Equivalence Problems of Almost Perfect Nonlinear Functions and Disjoint Difference Families

Dissertation

zur Erlangung des akademischen Grades

doctor rerum naturalium
(Dr. rer. nat.)

von Christian Kaspers, M. Ed.,

geb. am 16.12.1988 in Lahnstein

genehmigt durch die Fakultät für Mathematik
der Otto-von-Guericke-Universität Magdeburg

Gutachter: Prof. Dr. Alexander Pott
Prof. Dr. Anne Canteaut
apl. Prof. Dr. Alfred Wassermann

eingereicht am: 24.11.2020

Verteidigung am: 22.03.2021

Zusammenfassung

In der vorliegenden Arbeit untersuchen wir Äquivalenzprobleme zweier Objekte aus der diskreten Mathematik: disjunkte Differenzfamilien und fast perfekt-nichtlineare Funktionen (APN-Funktionen, aus dem Englischen: *almost perfect nonlinear*).

Eine disjunkte Differenzfamilie ist eine Sammlung disjunkter Teilmengen gleicher Kardinalität einer Gruppe G, sodass jedes Nichtnullelement aus G gleich häufig als Differenz zweier Elemente derselben Teilmenge auftritt. Differenzfamilien spielen eine wichtige Rolle in der Designtheorie, finden aber auch in der Kodierungstheorie Anwendung. Wird eine neue Differenzfamilienkonstruktion vorgestellt, so stellt sich natürlicherweise die Frage, ob die resultierenden Objekte wirklich neu sind oder ob sie isomorph zu bereits bekannten Differenzfamilien sind.

In dieser Arbeit untersuchen wir drei solche Isomorphieprobleme: Wir vergleichen eine klassische Konstruktion in endlichen Körpern (Wilson 1972) mit drei Konstruktionen in Galoisringen – zwei davon sind bekannt (Davis, Huczynska und Mullen 2017, sowie Momihara 2017), die dritte führen wir neu ein. Diese Isomorphieprobleme sind besonders interessant, da alle drei Galoisring-Konstruktionen auf demselben Ansatz wie Wilsons Konstruktion basieren. Indem wir ausgewählte Schnittzahlen der assoziierten kombinatorischen Designs bestimmen, zeigen wir, dass die beiden bekannten Differenzfamilien und Wilsons Differenzfamilien in fast allen Fällen nichtisomorph sind. Für unsere neuen Differenzfamilien geben wir eine partielle Lösung des Isomorphieproblems an.

APN-Funktionen sind vektorielle Boolesche Funktionen von $\mathbb{F}_2^n$ nach $\mathbb{F}_2^n$ mit optimalen differenziellen Eigenschaften. Sie wurden 1994 von Nyberg eingeführt. Die Auseinandersetzung mit diesen Funktionen wird primär aus der Kryptographie heraus motiviert, denn APN-Funktionen bieten den bestmöglichen Schutz gegen differenzielle Kryptoanalyse. Weitere Anwendungen finden sich in der Kodierungstheorie und in der endlichen Geometrie. Obwohl APN-Funktionen seit ihrer Einführung intensiv untersucht wurden, sind bisher nur wenige inäquivalente APN-Funktionen bekannt: einige sporadische Beispiele, mehrere APN-Potenzfunktionen und gegenwärtig 13 unendliche Familien von APN-Nichtpotenzfunktionen. Gänzlich offen ist die Frage, wie viele inäquivalente APN-Funktionen es auf $\mathbb{F}_2^n$ für ein gegebenes n gibt. Auch Computersuchen liefern nur für $n \leq 8$ zufriedenstellende Resultate.

In der vorliegenden Arbeit präsentieren wir die erste nichttriviale untere Schranke für die Anzahl der inäquivalenten APN-Funktionen auf $\mathbb{F}_2^n$ für gerade $n = 2m$. Für zwei sorgfältig ausgewählte unendliche Familien von APN-Funktionen, die auf Zhou und Pott (2013) und Taniguchi (2019) zurückgehen, ermitteln wir jeweils exakt, unter welchen Bedingungen die Funktionen jeder dieser Klassen äquivalent sind. Aus diesen Resultaten leiten wir ab, dass es auf $\mathbb{F}_2^{2m}$ mindestens $\frac{\varphi(m)}{2}\left\lceil\frac{2^m+1}{3m}\right\rceil$

inäquivalente APN-Funktionen gibt, wobei φ die Eulersche Phi-Funktion bezeichne. Darüber hinaus präsentieren wir einige Resultate über Gold APN-Funktionen und über eine unendliche Familie von APN-Funktionen, die von Carlet (2011) eingeführt wurde. Zudem bestimmen wir die Automorphismengruppen aller genannten APN-Funktionen.

Abstract

In this thesis, we study equivalence problems of two objects from discrete mathematics: disjoint difference families and almost perfect nonlinear (APN) functions.

Disjoint difference families are collections of same-sized disjoint subsets of a group G such that each nonzero element of G occurs equally often as the difference of two elements from the same subset. Difference families play an important role in design theory, and they also have applications in coding theory. Whenever a new construction of a difference family is presented, it is a natural question to ask whether the construction provides completely new objects or whether its instances are isomorphic to already known difference families.

In this thesis, we study three such isomorphism problems: we compare each of three different constructions of difference families in Galois rings, two of which were introduced by Davis, Huczynska, and Mullen (2017) and by Momihara (2017), and one of which is new, with a classical construction in finite fields by Wilson (1972). These isomorphism problems are particularly intriguing as Wilson's construction served as an inspiration for all three Galois ring constructions. To compare such difference families from different groups, we study the block intersection numbers of their associated combinatorial designs. For both known difference families, we show that they are in almost all cases nonisomorphic to Wilson's difference families. For our new difference family, we present a partial solution to the isomorphism problem.

APN functions are vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$ with optimal differential properties. They were introduced in 1994 by Nyberg. The main motivation to study these functions lies in cryptography as APN functions provide the strongest resistance against differential cryptanalysis, but they also have applications in coding theory and finite geometry. Although APN functions have been extensively studied since their introduction, only a limited number of inequivalent APN functions are known: except for some sporadic examples, we know several power APN functions and currently 13 infinite families of non-power APN functions. Up to now, it has been completely unknown, how many inequivalent APN functions exist on $\mathbb{F}_2^n$ for any given n. Satisfactory results from computer searches only exist for $n \leq 8$.

In this thesis, we present the first nontrivial lower bound on the total number of inequivalent APN functions on $\mathbb{F}_2^n$ where $n = 2m$ is even. We carefully pick two infinite families of non-power APN functions introduced by Zhou and Pott (2013) and Taniguchi (2019), and we completely determine the equivalence of the instances of these classes. We derive that on $\mathbb{F}_2^{2m}$, there exist at least $\frac{\varphi(m)}{2}\left\lceil\frac{2^m+1}{3m}\right\rceil$ inequivalent APN functions, where φ denotes Euler's totient function. We add some results about Gold APN functions and about an infinite family of APN functions by Carlet (2011), and we determine the automorphism groups of all these APN functions.

Contents

1 Introduction

Two focal points of research in combinatorics are the construction and the enumeration of interesting combinatorial configurations. When considering a certain combinatorial configuration, it is a natural problem to find as many examples of this object as possible since we need a certain number of candidates to study it in detail. In the best case, there are several powerful constructions that provide huge infinite families of these objects. In general, however, there exist one or even several equivalence relations on the structure the objects are embedded in that preserve the relevant properties of the configuration. Consequently, it often happens that many instances of the same infinite family are equivalent or that two classes that seem to be different at first actually provide equivalent examples. Hence, it is not only important to find new constructions of a combinatorial configuration, but it is an equally essential task to enumerate these objects by carefully studying their equivalence.

In this thesis, we contribute to this task for two kinds of objects: difference families, which are combinatorial configurations in abelian groups closely related to combinatorial designs, and almost perfect nonlinear functions, APN functions in brief, which are vectorial Boolean functions with optimal differential properties. We study several isomorphism problems about difference families from different constructions in finite fields and Galois rings, and we completely determine the equivalence of two infinite families of APN functions. The latter result enables us to establish the first nontrivial lower bound on the total number of APN functions.

This thesis is structured as follows. In this introduction, we present a short overview of difference families and APN functions, and we explain further what motivates our work. Afterwards, the thesis is separated into two parts one can read separately: in Chapter 2 and Chapter 3, we focus on difference families and their associated designs, and in Chapter 4 and Chapter 5, we study APN functions. In both these parts, the respective first chapters, Chapter 2 and Chapter 4, contain basic definitions and results that are mostly known, while the respective second chapters, Chapter 3 and Chapter 5, contain our main results. In detail:

In Chapter 2, we introduce difference families and combinatorial designs together with their equivalence relations, and we give a short overview of Galois rings. Moreover, we present the constructions of difference families that are relevant for this thesis, including a new construction of difference families in Galois rings, and we introduce a new family of divisible difference families. In Chapter 3, we study three isomorphism problems concerning these infinite classes of difference families. We tackle these problems using block intersection numbers.

In Chapter 4, we give an overview of vectorial Boolean functions and, in particular, APN functions. Moreover, we introduce the relevant equivalence relations of vectorial

Boolean functions that preserve the APN property, and we present the infinite families of APN functions that we study in detail. In Chapter 5, we completely determine the equivalence of two classes of APN functions introduced by Zhou and Pott [109] and by Taniguchi [100], respectively. From these results, we obtain the first nontrivial lower bound on the total number of inequivalent APN functions. Additionally, we determine the full automorphism groups of these functions.

Eventually, in Chapter 6, we will summarize our results, and we will give an outlook on open problems that we encounter in the course of our work.

Finally, we remark that Chapter 2 and Chapter 3 are based on two papers by Pott and the present author [75, 76] and Chapter 4 and Chapter 5 are based on two papers by Zhou and the present author [77, 78].

1.1 Difference families

If G is an additively written abelian group of order v and $D_1, D_2, \dots, D_b$ are subsets of cardinality k of G, or k-subsets of G, in brief, then we call the collection $\{D_1, D_2, \dots, D_b\}$ a (v, k, λ) difference family in G if for every nonzero element $g \in G$, there are λ distinct pairs of elements d, d', where $d, d' \in D_i$ for some $i \in \{1, 2, \dots, b\}$, such that $d - d' = g$.

Example 1.1. The collection

$$D = \{\{1, 5, 8, 12\}, \{2, 3, 10, 11\}, \{4, 6, 7, 9\}\}$$

is a $(13, 4, 3)$ difference family in the cyclic group $\mathbb{Z}_{13}$. Any nonzero element of $\mathbb{Z}_{13}$ is represented exactly three times as the difference of two elements from the same subset in $D = \{D_1, D_2, D_3\}$. For example, for $4 \in \mathbb{Z}_{13}$, we have $5 - 1 \equiv 12 - 8 \equiv 4 \pmod{13}$ from D_1, and $2 - 11 \equiv 4 \pmod{13}$ from D_2, and no difference from D_3.

Difference families are a generalization of difference sets, which are basically difference families with $b = 1$, and there is very rich theory on difference sets. We refer to the introduction by Jungnickel and Pott [73] and the survey by Jungnickel [72] for an overview. Still, various types of difference families have also long been studied in combinatorial literature. The term *difference family* was introduced in 1972 by Wilson [102], yet the concept of difference families can be traced back much further: in 1852 and 1853, Anstice [4, 5] used similar ideas to construct an infinite family of combinatorial designs. Unaware of Anstice's work, it was Bose [15] in 1939 who, in his paper, which is essentially the foundation of design theory, established difference methods as tools to systematically construct combinatorial designs. For an overview of difference families, we refer to the surveys by Abel and Buratti [1] and Beth, Jungnickel, and Lenz [10, Chapter VII].

In the past 25 years, research also included different generalizations or specifications of difference families, such as relative [28], strong [29], disjoint [84], near-complete [43], partitioned [31, 50], divisible [85], external [88] and strong external difference families [71, 89]. In this thesis, we will mostly deal with near-complete disjoint difference families, which, using the notation from above, are difference families such that the subsets $D_1, D_2, \ldots, D_b$ are disjoint and partition the nonzero elements of G.

As pointed out by Ng and Paterson [86], the different types of difference families have applications in design theory, cryptography, coding theory and communications and information security, and they have connections to many other combinatorial objects including association schemes, difference matrices, zero difference balance functions, sequences, strongly regular graphs, and difference systems of sets; see also the work by Abel and Buratti [1], Beth, Jungnickel, and Lenz [10], and Buratti and Jungnickel [31].

In this thesis, in particular, the connections to design theory play an important role as we can define an equivalence relation of difference families using the associated combinatorial 2-designs. If P is a set with v elements, which we call points, then a collection of k-subsets of P, which we call blocks, is a 2-(v, k, λ) design if every two points are contained in exactly λ blocks. From any (v, k, λ) difference family $\{D_1, D_2, \ldots, D_b\}$, we can easily obtain a 2-(v, k, λ) design by taking all the translates $D_i + g$, where $i \in \{1, 2, \ldots, b\}$ and $g \in G$.

Combinatorial designs have been extensively studied since the first half of the 19th century: Plücker [91] in 1835, Kirkman [79] in 1847, and Steiner [97] in 1853 all worked on combinatorial problems that today we would call design theoretical problems. For a historical account, we refer to Wilson [103] and Anderson, Colbourn, Dinitz, and Griggs [3]. Since these beginnings, countless publications have lead to very rich literature about combinatorial designs and their applications in, for example, group theory, finite geometry, and cryptography. We refer to Beth, Jungnickel, and Lenz [10] and Colbourn and Dinitz [41] for an extensive overview of design theory.

One of the focal points of research on difference families is finding new instances and new constructions of these objects. While difference families are not particularly rare, this task is still important since we may find difference families with new parameters or in new groups. In 2017, each Davis, Huczynska, and Mullen [43] and Momihara [84] introduced new constructions of difference families in the additive group of a Galois ring. In this thesis, we derive another new construction of difference families in this particular group from the construction by Davis, Huczynska, and Mullen [43]. Furthermore, we present a new construction of divisible difference families that is derived from Momihara's [84] work.

Even though the aforementioned constructions are new, this does not necessarily imply that they provide completely new difference families since there exist two basic equivalence relations between difference families: two difference families can be *equivalent* or *isomorphic*. To be equivalent, two difference families need to be defined in the same group. However, difference families in different groups may still be isomorphic as this concept makes use of the associated designs, for which we forget about the underlying groups.

So when a new construction of difference families is presented, we are naturally interested in the question whether these difference families are new or whether they are equivalent or isomorphic to already known ones. Of course, it does not make sense to randomly choose two difference families and compare them—this selection has to be carefully motivated. In the case of both the constructions in Galois rings by Davis, Huczynska, and Mullen [43] and Momihara [84], the authors state that their work was inspired by a popular construction of difference families in the additive group of a finite field by Wilson [102]. As the constructions in Galois rings and those in finite fields provide difference families with the exact same parameters, these classes are natural candidates for studying their isomorphism problem. Davis, Huczynska, and Mullen [43] even point out this question explicitly for their difference family.

In this thesis, we are going to solve these problems. We show that Momihara's [84] and Wilson's [102] difference families are always nonisomorphic, and we prove that, with one exception, the same holds for the difference families by Davis, Huczynska, and Mullen [43] and by Wilson [102]. As our new construction of difference families in Galois rings also has an analogue in finite fields from Wilson's [102] construction, we also study this isomorphism problem. Here, we present a partial solution.

1.2 Almost perfect nonlinear functions

A vectorial Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, where $\mathbb{F}_2^n$ denotes the n-dimensional vector space over the finite field $\mathbb{F}_2$ with 2 elements, is called *almost perfect nonlinear* (APN) if the equation

$$f(x+a)+f(x)=b$$

has exactly 0 or 2 solutions for any $b \in \mathbb{F}_2^n$ and any nonzero $a \in \mathbb{F}_2^n$. Note that the term *almost* in almost perfect nonlinear is misleading in the sense that APN functions actually are optimally nonlinear. A *perfect* nonlinear function is a function $f\colon \mathbb{F}_p^n \to \mathbb{F}_p^n$ such that the equation $f(x+a)-f(x)=b$ has exactly one solution for any $b \in \mathbb{F}_p^n$ and any nonzero $a \in \mathbb{F}_p^n$. Such functions are also called *planar functions.* However, over fields with characteristic 2, we have

$$f(x+a)+f(x)=f((x+a)+a)+f(x+a),$$

which means that if x solves the above equation, so does $x+a$. Consequently, there are no perfect nonlinear functions on $\mathbb{F}_2^n$, and APN functions are as close to perfect nonlinearity as possible.

We once again start with an example. Note that we identify the vector space $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$ here. This is something we will regularly do throughout this thesis as it allows us to use finite field operations.

Example 1.2. The function

$$f(x)=x^3$$

is APN on $\mathbb{F}_{2^n}$ for all positive integers n. As $f(x+a)+f(x)=ax^2+a^2x+a^3=b$ is a quadratic equation, it has 0, 1 or 2 solutions for any $a,b \in \mathbb{F}_{2^n}$ where $a \neq 0$. However, as pointed out above, one solution is not possible. Consequently, it has 0 or 2 solutions, and f is APN.

APN functions were introduced in 1994 by Nyberg [87]. She defined them as the mappings with the highest resistance to differential cryptanalysis, which is one of the most important cryptanalysis tools for block ciphers and was introduced in 1991 by Biham and Shamir [11]. APN functions are also strongly connected with coding theory and finite geometry. In particular, quadratic APN functions are equivalent to a special type of dimensional dual hyperovals; see the work by Yoshiara [104], Edel [56], and Dempwolff and Edel [44] for more details. Since their introduction, APN functions have been studied intensively. For an extended overview of these functions, we refer to the surveys by Pott [92], who mainly focuses on the geometrical aspects of APN and planar functions, and Blondeau and Nyberg [12], who provide an overview of theoretical results and applications of APN functions in cryptography.

For a long time, only very few APN functions were known, all of which were power functions of the form $x \mapsto x^d$ as in Example 1.2. Only in 2006, Edel, Kyureghyan, and Pott [55] reported the first two examples of non-power APN functions on $\mathbb{F}_2^{10}$ and $\mathbb{F}_2^{12}$. Since then, much research has been centered around finding new non-power APN functions, and rightfully so as quite a few infinite families of such functions have been discovered. Budaghyan, Calderini, and Villa [24, Table 3] recently listed the 13 known families. In Section 4.3, we give a short overview of the known APN functions.

In recent years, research about APN functions has focused on three big problems:

1. The Big APN Problem. When n is odd, several known APN functions on $\mathbb{F}_2^n$ are bijective. For example, all the known power APN functions permute the elements of $\mathbb{F}_2^n$ where n is odd. It had been a long-standing unanswered question whether there exists an APN permutation on $\mathbb{F}_2^n$ where n is even. In 2006, Hou [69] conjectured that there was none. However, in 2009, his conjecture, which many believed to be true, was refuted: Browning, Dillon, McQuistan, and Wolfe [21] presented the first instance of an APN permutation on $\mathbb{F}_2^n$ with n even on $\mathbb{F}_2^6$. Until now, this is the only known sporadic example, and since its discovery, the most intriguing question regarding APN functions is whether there are more such functions. Despite many attempts to tackle this so-called *Big APN Problem*, for example by Yu, Wang, and Li [108], Calderini, Sala, and Villa [32], Perrin, Udovenko, and Biryukov [90], and Canteaut, Perrin, and Tian [35], no additional APN permutation on an even-dimensional vector space $\mathbb{F}_2^n$ has been found yet.

2. Finding non-quadratic APN functions. Except for one sporadic example on $\mathbb{F}_2^6$, which was discovered by Edel and Pott [58] in 2009 using the so-called switching method, every known non-power APN function is equivalent to a quadratic APN function. That is an APN function that can be written in the form

$$\sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j} + \sum_{0 \le i \le n-1} b_i x^{2^i} + c$$

with $a_{i,j}, b_i, c \in \mathbb{F}_{2^n}$ for $i, j = 0, 1, \dots, n-1$ and not all $a_{i,j} = 0$. Since then, almost no progress has been made in finding more non-power APN functions that are not equivalent to a quadratic function.

Using a completely different approach than Edel and Pott [58], Carlet [36] actually also found a non-quadratic APN function on $\mathbb{F}_2^6$—but it turned out to be equivalent to the one already known. While several power APN functions are non-quadratic, it is an open problem whether there exist more than one non-quadratic non-power APN function.

3. Determining the number of inequivalent APN functions. APN functions are extremely rare: when randomly choosing a function on $\mathbb{F}_2^n$ where $n \geq 4$, chances that it is APN are basically 0. Completely classifying the APN functions on $\mathbb{F}_2^4$ and $\mathbb{F}_2^5$, Brinkmann and Leander [20] showed in 2008 that on these vector spaces, approximately $1.9 \cdot 10^{13}$ and $1.1 \cdot 10^{23}$ APN functions, respectively, exist. While these numbers seem to be large, they actually account for only approximately $1.0 \cdot 10^{-4}$ and $7.6 \cdot 10^{-24}$ percent, respectively, of all functions on these vector spaces. This percentage certainly drops much further for greater n. Hence, it is of great interest to find new constructions of these functions.

However, as there exist several equivalence relations for functions on $\mathbb{F}_2^n$ that preserve the APN property, it is an equally important task to study how many inequivalent functions do exist. Considering the most general notion of equivalence, the so-called CCZ-equivalence, it turns out there are not so many:

Brinkmann and Leander [20] showed that on $\mathbb{F}_2^4$, all APN functions are pairwise equivalent, and that on $\mathbb{F}_2^5$, all APN functions fall into three equivalence classes. On $\mathbb{F}_2^6$, currently 14 equivalence classes are known: the non-quadratic one mentioned above and 13 quadratic functions listed by Browning, Dillon, Kibler, and McQuistan [22]. It was confirmed by Edel [57] that this list is complete, but it is unknown whether there exist more non-quadratic APN functions on $\mathbb{F}_2^6$. For $n = 7$ and $n = 8$, according to Beierle and Leander [7], at the moment, 491 and 21 113 inequivalent functions are known, respectively. Most of these functions do not fall into one of the known infinite families, but were found by computer searches by Yu, Wang, and Li [108] in 2014, and by Beierle and Leander [7] in 2020.

For $n \geq 9$, however, hardly any results about the number of inequivalent APN functions exist. There are mainly two reasons for this. First, searching for new functions computationally becomes very hard and resource consuming for greater n: for example, the approach by Beierle and Leander [7], which yielded 12 923 new APN functions on $\mathbb{F}_2^8$, only lead to five new APN functions on $\mathbb{F}_2^{10}$ so far. Second, up to now, there are only few theoretical results about the equivalence of the infinite families of non-power APN functions. Power APN functions are relatively well studied, but they only provide very few inequivalent examples. As far as non-power APN functions are concerned, the 13 known classes seem to be mutually inequivalent, but it is not known how many inequivalent members each of these classes contains. It would be particularly useful to have one construction that provides a plethora of inequivalent functions.

In this thesis, we make an important contribution to the last of the aforementioned problems: for n even, we present the first nontrivial lower bound on the total number of inequivalent APN functions. In general, it is a very hard problem to prove the inequivalence of two functions on $\mathbb{F}_2^n$. As mentioned above, even computationally, it becomes difficult to check whether two APN functions are equivalent for $n \geq 9$. Consequently, for larger n, these problems need to be tackled theoretically. We will carefully pick two infinite families of non-power APN functions, which were introduced by Zhou and Pott [109] in 2013 and by Taniguchi [100] in 2019, and completely solve the equivalence problem for the members of these classes. We will add some similar results about a third infinite family of APN functions introduced by Carlet [36].

First, we prove that the family by Zhou and Pott [109] contains $\frac{1}{2}\varphi(m)\left(\lfloor \frac{m}{4} \rfloor + 1\right)$ inequivalent APN functions on $\mathbb{F}_2^{2m}$ with m even, where φ denotes Euler's totient function. Using the same approach for Taniguchi's [100] APN functions, we considerably improve this first lower bound and extend it to $\mathbb{F}_2^{2m}$ for any $m \geq 2$. We show that the number of inequivalent APN functions on $\mathbb{F}_2^{2m}$ is at least

$$\frac{\varphi(m)}{2} \left\lceil \frac{2^m + 1}{3m} \right\rceil .$$

As a corollary, our results enable us to determine the automorphism groups of the Zhou-Pott and the Taniguchi APN functions as well as of the Gold APN functions and, for m even, the Carlet APN functions.

2 Difference families and combinatorial designs

In this chapter, we focus on the two important combinatorial objects the first part of this thesis is centered around: difference families and combinatorial designs. In Section 2.1, we introduce these objects. We present some of their important properties, and, in particular, we point out the connection between them: we demonstrate that every difference family gives rise to a combinatorial design.

In Section 2.2, we define when two difference families are equivalent or isomorphic. As three of the difference families for which we tackle the isomorphism problem exist in a special local commutative ring called Galois ring, we give an introduction to Galois rings in Section 2.3. In Section 2.4, we eventually present the constructions of the difference families in finite fields and Galois rings that we study in this thesis. While the difference family in finite fields and two of the three difference families in Galois rings are well known, we also present one new construction in Galois rings. We conclude this chapter by introducing a new divisible difference family in Galois rings in Section 2.5.

2.1 Difference families and t-designs

We start by introducing some helpful notations. Let G be an abelian group, $A, B \subseteq G$ and $g \in G$. We define multisets

$$\begin{aligned} \Delta A &:= \{a - a' : a, a' \in A, a \neq a'\}, \\ \Delta_+ A &:= \{a + a' : a, a' \in A, a \neq -a'\}, \\ A - B &:= \{a - b : a \in A, b \in B, a \neq b\}, \\ A + B &:= \{a + b : a \in A, b \in B, a \neq -b\}, \\ A + g &:= \{a + g : a \in A\}. \end{aligned}$$

In the course of this paper, we will sometimes use these notations to denote sets, not multisets. It will be clear from the context if we mean the multiset or the respective set.

We recall the definition of a difference family from Section 1.1 using the new notations from above, and we introduce some additional properties of difference families.

Definition 2.1. Let G be an abelian group of order v, and let $D_1, D_2, \ldots, D_b$ be k-subsets of G. The collection $D = \{D_1, D_2, \ldots, D_b\}$ is called a (v, k, λ) *difference* *family in G* if each nonzero element of G occurs exactly λ times in the multiset union

$$\bigcup_{i=1}^{b} \Delta D_i.$$

We call $D_1, D_2, \ldots, D_b$ the *base blocks* of D. If the base blocks are mutually disjoint, we say D is a *disjoint difference family.* If $b = 1$, one speaks of a (v, k, λ) *difference set.* We call D *near-complete* if the base blocks partition $G \setminus \{0\}$.

Using these new denotations, the difference family we presented in Example 1.1 is a near-complete $(13, 4, 3)$ disjoint difference family. We remark that the number b of base blocks in a (v, k, λ) difference family is given by $b = \frac{\lambda(v-1)}{k(k-1)}$, which is the quotient of the number of total differences and the number of differences per block. Hence,

$$\lambda(v-1) \equiv 0 \pmod{k(k-1)}$$

is a necessary condition for the existence of a (v, k, λ) difference family. Using this condition, it is easy to confirm that there exists no *complete* disjoint difference family, which is a difference family whose base blocks partition G. Such difference families are often also called partitioned difference families, they are considered when we allow base blocks of different cardinalities.

In this thesis, all the difference families we study are near-complete $(v, k, k-1)$ disjoint difference families. Note that any disjoint difference family with parameters $(v, k, k-1)$ is near-complete. Nevertheless, to point out the near-completeness, we will usually also mention this property. Clearly, such difference families consist of $b = \frac{v-1}{k}$ base blocks.

Near-complete $(v, k, k-1)$ disjoint difference families are closely related to external difference families. As the name suggests, in an external difference family, we do not consider the differences of elements within one set but the differences of elements from distinct sets. Since Davis, Huczynska, and Mullen [43] actually constructed external difference families, we will take a closer look at these objects and their connection to disjoint difference families.

Definition 2.2. Let G be an abelian group of order v, and let $D_1, D_2, \ldots, D_b$ be mutually disjoint k-subsets of G, which we call base blocks. The collection $D = \{D_1, D_2, \ldots, D_b\}$ is called a (v, k, λ) *external difference family* if each nonzero element of G occurs exactly λ times in the multiset union

$$\bigcup_{\substack{1 \le i,j \le b \\ i \neq j}} (D_i - D_j)\,.$$

We call D *near-complete* if the base blocks partition the nonzero elements of G.

Proposition 2.1 shows that under certain conditions a disjoint difference family is also an external difference family. This result was observed by Momihara [84], and, for near-complete disjoint difference families, it was also mentioned by Chang and Ding [39] and Davis, Huczynska, and Mullen [43]. We will add a short proof.

Proposition 2.1. *Let G be an abelian group of order v, let $\lambda' \geq 2$ be an integer, and let $D = \{D_1, D_2, \dots, D_b\}$ be a collection of disjoint k-subsets of G such that their union $\bigcup_{i=1}^{b} D_i$ is a (v, bk, λ') difference set in G. Then D is a (v, k, λ) disjoint difference family in G for some positive integer $\lambda < \lambda'$ if and only if D is a $(v, k, \lambda' - \lambda)$ external difference family in G.*

Proof. Let G be an abelian group of order v, and let $D = \{D_1, D_2, \dots, D_b\}$ be a collection of mutually disjoint k-subsets of G whose union $\bigcup_{i=1}^{b} D_i$ is a (v, bk, λ') difference set for some integer $\lambda' \geq 2$. We can split all the differences in $\Delta(\bigcup_{i=1}^{b} D_i)$ in the following way into the internal and the external differences of the $D_1, D_2, \dots, D_b$:

$$\Delta\left(\bigcup_{i=1}^{b} D_i\right) = \bigcup_{i=1}^{b} \Delta D_i \cup \bigcup_{\substack{1 \leq i,j \leq b \\ i \neq j}} (D_i - D_j).$$

Since $\bigcup_{i=1}^{b} D_i$ is a difference set, each element $g \in G \backslash \{0\}$ occurs with multiplicity λ' in $\Delta(\bigcup_{i=1}^{b} D_i)$. It follows that each nonzero element in G is represented as λ differences in $\bigcup_{i=1}^{b} \Delta D_i$ if and only if it is represented $\lambda' - \lambda$ times in $\bigcup_{1 \leq i,j \leq b,\, i \neq j} (D_i - D_j)$. Consequently, D is a (v, k, λ) disjoint difference family if and only if D is a $(v, k, \lambda' - \lambda)$ external difference family. □

The next result follows immediately from Proposition 2.1.

Corollary 2.2. *Let G be an abelian group. A collection $D = \{D_1, D_2, \dots, D_b\}$ of k-subsets of G is a near-complete $(v, k, k-1)$ disjoint difference family in G if and only if D is a near-complete $(v, k, v-k-1)$ external difference family in G.*

Proof. If D is near-complete, then $\bigcup_{i=1}^{b} D_i = G \setminus \{0\}$, and $G \setminus \{0\}$ is a $(v, v-1, v-2)$ difference set in G. The result now follows from Proposition 2.1. □

For extended background on $(v, k, k-1)$ disjoint difference families, the reader is referred to Buratti [30] who gives an overview of difference families with these parameters and summarizes several constructions, including the one by Davis, Huczynska, and Mullen [43].

As mentioned before, every difference family gives rise to a combinatorial design. Note that while a difference family requires the structure of a group, combinatorial designs exist on sets.

Definition 2.3. Let P be a set with v elements, which we call *points*. A *t-(v, k, λ) design $\mathcal{D}$* or *t-design $\mathcal{D}$*, in brief, is a collection of k-subsets of P, which we call *blocks*, such that each t-subset of P is contained in exactly λ blocks. We call P the *point set* of $\mathcal{D}$. If $\mathcal{D}$ has no repeated blocks, we say that $\mathcal{D}$ is *simple*.

The most famous example of a combinatorial design is the *Fano plane*:

Example 2.4. The collection

$$\mathcal{D} = \{\{1,2,7\},\ \{1,3,6\},\ \{1,4,5\},\ \{2,3,4\},\ \{2,5,6\},\ \{3,5,7\},\ \{4,6,7\}\}$$

is a 2-$(7,3,1)$ design with point set $P = \{1,2,\ldots,7\}$. Every 2-subset of P is contained in exactly one block.

The designs associated to difference families are 2-designs, which are often referred to as *balanced incomplete block designs (BIBD)*. Note that a 2-(v,k,λ) design $\mathcal{D}$ consists of $\frac{vr}{k}$ blocks, where $r = \frac{\lambda(v-1)}{k-1}$ denotes the *repetition number* of $\mathcal{D}$, which is the number of blocks each point is contained in. In Definition 2.5 and Proposition 2.3, we describe how to construct a 2-design from a difference family.

Definition 2.5. Let G be an abelian group, and let $D = \{D_1, D_2, \ldots, D_b\}$ be a collection of subsets of G. The *development* $\mathrm{dev}(D)$ of D is the collection

$$\{D_i + g : D_i \in D, g \in G\}$$

of all the translates of the subsets contained in D. The sets $D_1, D_2, \ldots, D_b$ are called the *base blocks* of $\mathrm{dev}(D)$.

In other words: The development $\mathrm{dev}(D)$ of D contains the orbits of the base blocks of D under the action of G. Hence, $\mathrm{dev}(D)$ consists of vb blocks. Note that these blocks are not necessarily distinct. If $D_i + g = D_j$ for two base blocks D_i, D_j and some $g \in G$, or if the orbit of a base block does not have full length, we obtain repeated blocks, and $dev(D)$ is not simple. In this thesis, all the designs we consider are simple. The following Proposition 2.3 is well known. We add a proof for completeness.

Proposition 2.3. *Let D be a (v,k,λ) difference family in an abelian group G. The development $\mathrm{dev}(D)$ of D forms a 2-(v,k,λ) design with point set G.*

Proof. Let $D = \{D_1, D_2, \ldots, D_b\}$ be a (v,k,λ) difference family in G, and let $\mathcal{D} = \mathrm{dev}(D)$ be the development of D. We take an arbitrary 2-subset $T = \{t_1, t_2\}$ of G, and we denote by n the number of blocks of $\mathcal{D}$ containing T. Recall that the blocks of $\mathcal{D}$ are the translates $D_i + g$.

We first show that $n \geq \lambda$. Let $d = t_1 - t_2$. Since d is nonzero, d has exactly λ representations as a difference $d = d' - d''$ where $d', d'' \in D_i$ for some $i \in \{1,2,\ldots,b\}$. Obviously, $\Delta D_i = \Delta(D_i + g)$ for all $i = 1,2,\ldots,b$ and all $g \in G$. This implies that if $d \in \Delta D_i$, then $d \in \Delta(D_i + g)$ for all $g \in G$. Hence, if we take $d', d'' \in D_i$ with $d' - d'' = d$ and set $g = t_1 - d'$, then $d' + g = t_1$ and $d'' + g = t_2$. Consequently, $T \subseteq D_i + g$. Since there are λ pairs d', d'' with $d' - d'' = d$, we find λ blocks containing the set T this way.

Now suppose by way of contradiction that $n > \lambda$. This means that besides the λ blocks mentioned above there is an additional block $D_j + g$ for some $j \in \{1,2,\ldots,b\}$ and $g \in G$ that contains T. Then $d \in \Delta(D_j + g)$ and it follows that $d \in \Delta D_j$. Hence, we have $\lambda+1$ representations of the element d as a difference $d'-d''$, where $d', d'' \in D_i$ for some $i = 1, 2, \ldots, b$. This contradicts our assumption that D is a (v, k, λ) difference family. Consequently, $n = \lambda$. □

2.2 Equivalent and isomorphic difference families

In this section, we introduce the notions of *equivalent* and *isomorphic* difference families. While both concepts enable us to enumerate difference families, it is important to distinguish them. We start by defining when two difference families are equivalent.

Definition 2.6. Let G be an abelian group. We call two (v, k, λ) difference families $D = \{D_1, D_2, \ldots, D_b\}$ and $D' = \{D'_1, D'_2, \ldots, D'_b\}$ in G *equivalent* if there exists a group automorphism α of G such that D'_i is a translate of $\alpha(D_i) = \{\alpha(d) : d \in D_i\}$ for all $i = 1, \ldots, b$.

In the following example, we present two equivalent difference families.

Example 2.7. The $(13, 4, 3)$ difference family

$$D' = \{\{3, 4, 11, 12\}, \{6, 8, 9, 11\}, \{2, 4, 8, 11\}\}$$

in the cyclic group $\mathbb{Z}_{13}$ is equivalent to the difference family

$$D = \{D_1, D_2, D_3\} = \{\{1, 5, 8, 12\}, \{2, 3, 10, 11\}, \{4, 6, 7, 9\}\}$$

from Example 1.1 since $D' = \{2D_1 + 1,\ 2D_2 + 2,\ 2D_3 + 3\}$.

To define isomorphic difference families, we make use of the following definition about isomorphic combinatorial designs.

Definition 2.8. Two 2-(v, k, λ) designs $\mathcal{D}$ and $\mathcal{D}'$ with point sets P and P', respectively, are *isomorphic* if there exists a bijection $\alpha \colon P \to P'$ such that

(i) $\mathcal{D}' = \{\alpha(B) : B \in \mathcal{D}\}$, where $\alpha(B) = \{\alpha(p) : p \in B\}$, and

(ii) $p \in B$ if and only if $\alpha(p) \in \alpha(B)$ for any point $p \in P$.

From Proposition 2.3, we know that every difference family can be uniquely associated with a combinatorial designs. We use these associated 2-designs to define isomorphic difference families.

Definition 2.9. Two (v, k, λ) difference families D and D' in abelian groups G and G', respectively, are *isomorphic* if their associated 2-(v, k, λ) designs $\operatorname{dev}(D)$ and $\operatorname{dev}(D')$ are isomorphic.

Note that equivalent difference families are isomorphic, which can be seen as follows. Assume $D = \{D_1, D_2, \ldots, D_b\}$ and $D' = \{D'_1, D'_2, \ldots, D'_b\}$ are equivalent difference families in an abelian group G. Then for any $i \in \{1, 2, \ldots, b\}$, the base block D'_i is a translate of $\alpha(D_i)$ for some group automorphism α of G. As the associated designs $\mathrm{dev}(D)$ and $\mathrm{dev}(D')$ consist of all the translates of the base blocks of D and D', respectively, it is clear that α describes an isomorphism of $\mathrm{dev}(D)$ and $\mathrm{dev}(D')$.

The converse, however, is in general not true: isomorphic difference families are not necessarily equivalent. While this is obvious when D and D' are difference families in different groups, it also holds for difference families in the same group as the following example by Colbourn [40] demonstrates.

Example 2.10 ([40, Remark 2.28])**.** The collections

$$\begin{aligned} D &= \{\{0,1,2\},\{0,2,9\},\{0,3,6\},\{0,4,8\},\{0,5,10\}\},\\ D' &= \{\{0,1,3\},\{0,1,6\},\{0,2,7\},\{0,3,10\},\{0,4,8\}\},\\ D'' &= \{\{0,1,7\},\{0,1,10\},\{0,2,5\},\{0,2,13\},\{0,4,8\}\} \end{aligned}$$

are $(16,3,2)$ difference families in the cyclic group $\mathbb{Z}_{16}$. They are pairwise isomorphic: D and D' are isomorphic by the permutation $(1\ 13)(2\ 14)(4\ 12)(5\ 9)(6\ 10)(7\ 15)$ of the point set $\mathbb{Z}_{16}$, and D and D'' are isomorphic by $(2\ 10)(3\ 11)(6\ 14)(7\ 15)$. However, it can be confirmed computationally that all three difference families are mutually inequivalent. As an example: every difference family equivalent to D has the structure $\{uD_i + g_i : i = 1,\dots,5\}$, where u is a unit in the integer ring $\mathbb{Z}_{16}$ and $g_i \in \mathbb{Z}_{16}$ for $i = 1,\dots,5$. However, for D' and D'' there are no such u and $g_1,\dots,g_5$.

In Chapter 3, we compare difference families in different groups. Hence, we will only study isomorphism and no equivalence problems. However, one could argue that combinatorial designs are, in comparison to difference families, the more relevant combinatorial objects. Thus, it generally might be more interesting to study isomorphism problems. In most cases, though, it is a very hard problem to prove whether two designs are isomorphic or not. We will discuss some strategies to attack such isomorphism problems at the beginning of Chapter 3.

2.3 Galois rings

As the difference families by Davis, Huczynska, and Mullen [43] and Momihara [84] we are focusing on in this thesis are constructed in the additive group of a Galois ring, we give a short introduction to Galois rings in this section. We present some of their well-known properties; for extended general background on Galois rings, we refer to the work by McDonald [82] and Wan [101]. Roughly speaking, Galois rings are finite commutative rings that are relatively close to finite fields as they, for example, have a large unit group.

Let p be a prime, and denote by $\mathbb{Z}_p[X]$ the univariate polynomial ring over $\mathbb{Z}_p$. Let $P(X) \in \mathbb{Z}_{p^m}[X]$ be a *monic basic irreducible polynomial* of degree $r \geq 1$, where basic irreducible means that the image of $P(X)$ modulo p in the polynomial ring $\mathbb{F}_p[X]$ is irreducible. The factor ring

$$\mathbb{Z}_{p^m}[X]/(P(X))$$

is called a *Galois ring* of characteristic p^m and extension degree r, and it is denoted by $\mathrm{GR}(p^m, r)$. Its order is p^{mr}. Since any two Galois rings of the same characteristic and order are isomorphic, we speak of *the* Galois ring $\mathrm{GR}(p^m, r)$. If $m = 1$, then $\mathrm{GR}(p, r)$ is the finite field $\mathbb{F}_{p^r}$. For the remainder of this section, denote $R = \mathrm{GR}(p^m, r)$.

Galois rings are local commutative rings. The unique maximal ideal of R is

$$\mathcal{I} = pR = \{pr : r \in R\}.$$

The additive group of R is isomorphic to $\mathbb{Z}_{p^m}^r$. The unit group of R contains exactly the elements of $R \setminus \mathcal{I}$. We denote the unit group by R^*. It has order $p^{mr} - p^{(m-1)r}$, and it is the direct product of a cyclic group of order $p^r - 1$, called the *Teichmüller group* $\mathcal{T}^*$ of R, and the so-called *group of principal units* $\mathbb{P} = 1 + \mathcal{I}$ of order $p^{(m-1)r}$. If p is odd or if $p = 2$ and $m \leq 2$, then $\mathbb{P}$ is a direct product of r cyclic groups of order p^{m-1}. If $p = 2$ and $m \geq 3$, then $\mathbb{P}$ is a direct product of a cyclic group of order 2, a cyclic group of order 2^{m-2}, and $r - 1$ cyclic groups of order 2^{m-1}.

The factor ring $R/\mathcal{I}$ is isomorphic to the finite field $\mathbb{F}_{p^r}$ with p^r elements. Let ξ be a generator of $\mathcal{T}^*$, which means ξ is an element of multiplicative order $p^r - 1$ in R^*. As a system of representatives of $R/\mathcal{I}$, we take the *Teichmüller set*

$$\mathcal{T} = \{0, 1, \xi, \ldots, \xi^{p^r-2}\}.$$

Every $r \in R$ has a unique *p-adic representation* $r = \alpha_0 + p\alpha_1 + \cdots + p^{m-1}\alpha_{m-1}$, where $\alpha_0, \alpha_1, \ldots, \alpha_{m-1} \in \mathcal{T}$.

We remark that it is convenient to choose $P(X)$ as a *monic basic primitive polynomial* of degree r in $\mathbb{Z}_{p^m}[X]$, which means that the image of $P(X)$ modulo p is primitive in $\mathbb{F}_p[X]$. Then ξ is a root of order $p^r - 1$ of $P(X)$, and we may set $\xi = X + (P(X))$.

In this thesis, we will only consider Galois rings of characteristic p^2. In this case, the product of two principle units

$$(1 + p\alpha)(1 + p\beta) = 1 + p(\alpha + \beta)$$

for any $\alpha, \beta \in \mathcal{T}$, and every unit $u \in \mathrm{GR}(p^2, r)^*$ has a unique representation

$$u = \alpha_0(1 + p\alpha_1),$$

where $\alpha_0 \in \mathcal{T}^*$ and $\alpha_1 \in \mathcal{T}$. Moreover, the group of principal units $\mathbb{P}$ is a direct product of r cyclic groups of order p and thus has the structure of an elementary abelian group of order p^r.

In the following example, we describe the Galois ring $\mathrm{GR}(9, 2)$ and its important structures. In Section 2.4 and Section 2.5, we will show examples of several constructions of difference families in this particular Galois ring $\mathrm{GR}(9, 2)$.

Example 2.11. Define the Galois ring $\mathrm{GR}(9, 2)$ of characteristic 9 and extension degree 2 as the factor ring $\mathbb{Z}_9[X]/(X^2 + 5X + 8)$. It contains 81 elements. Note that

$P(X) = X^2 + 5X + 8$ is a monic basic primitive polynomial in $\mathbb{Z}_9[X]$ since the image of $P(X)$ in $\mathbb{F}_3[X]$ is the primitive polynomial $X^2 + 2X + 2$.

Set $\xi = X + (P(X))$. Then the Teichmüller group of $\mathrm{GR}(9,2)$ is

$$\mathcal{T}^* = \{1, \xi, \xi^2, \ldots, \xi^7\} = \{1,\ \xi,\ 4\xi + 1,\ 8\xi + 4,\ 8,\ 8\xi,\ 5\xi + 8,\ \xi + 5\},$$

the maximal ideal is given as

$$\mathcal{I} = p\mathrm{GR}(9,2) = \{0,\ 3,\ 6,\ 3\xi,\ 6\xi,\ 3\xi + 3,\ 3\xi + 6,\ 6\xi + 3,\ 6\xi + 6\},$$

and the group of principle units is

$$\mathbb{P} = 1 + \mathcal{I} = \{1,\ 4,\ 7,\ 3\xi + 1,\ 6\xi + 1,\ 3\xi + 4,\ 3\xi + 7,\ 6\xi + 4,\ 6\xi + 7\}.$$

The unit group of $\mathrm{GR}(9,2)$ is $\mathrm{GR}(9,2)^* = \mathrm{GR}(9,2) \setminus \mathcal{I}$. It is the direct product of $\mathcal{T}^*$ and $\mathbb{P}$. Every $u \in \mathrm{GR}(9,2)^*$ can be uniquely represented in the form $\xi^i(1 + 3\xi^j)$ for some $i, j \in \{0, 1, \ldots, 7\}$. For example, $6\xi + 5 = \xi^4(1 + 3\xi^2)$.

2.4 Constructions of difference families in finite fields and Galois rings

There are dozens of constructions of various types of difference families. In this section, we describe several constructions of *near-complete* $(v, k, k-1)$ *disjoint difference families* we will study in this thesis. We begin with a classical construction in finite fields by Wilson [102]. Afterwards, we restate a very general construction in commutative rings with an identity by Furino [62]. Furino's work forms a framework for two constructions in Galois rings, which we present next: the first one is due to Davis, Huczynska, and Mullen [43], and the second one is a new construction. Eventually, we present another construction in Galois rings introduced by Momihara [84].

For completeness, we add short proofs of the constructions by Wilson [102] and by Davis, Huczynska, and Mullen [43], which we present in Theorem 2.4 and Theorem 2.6. We will also give a proof for our new construction in Theorem 2.7. For the extensive and technical proof of Momihara's construction from Theorem 2.8, we refer to his original work [84, Theorem 1]. We remark that Davis, Huczynska, and Mullen [43, Theorem 2.1] actually showed that the disjoint difference family in Theorem 2.6 is an external difference family.

In Theorem 2.4, we present Wilson's construction of disjoint difference families in finite fields. It makes use of the cyclotomy of the e-th powers in a finite field. The idea goes back to Bose [15], who used this approach to construct 2-$(v, 3, 2)$ designs. A similar approach was also used by Hanani [67].

Theorem 2.4. *Let $\mathbb{F}_q$ be the finite field with q elements, and let α be a primitive element of $\mathbb{F}_q$. Moreover, let $e, f \geq 2$ be integers satisfying $ef = q - 1$, and let*

$$C_0 = \{1, \alpha^e, \alpha^{2e}, \ldots, \alpha^{(f-1)e}\}$$

be the unique subgroup of index e and order f of $\mathbb{F}_q^*$, which is formed by the e-th powers of α. For $i = 1, 2, \ldots, e-1$, let $C_i = \alpha^i C_0$ be the i-th coset of C_0. Then the collection $C = \{C_0, C_1, \ldots, C_{e-1}\}$ is a near-complete $(q, f, f-1)$ disjoint difference family in the additive group of $\mathbb{F}_q$.

Proof. Let x, y be distinct elements of $\mathbb{F}_q^*$, and suppose there exist $c, c' \in C_i$ for some $i \in \{0, 1, \ldots, e-1\}$ such that $x = c - c'$. Let $z = \frac{y}{x}$. Then $y = zc - zc'$. Obviously, zc and zc' are elements of the same coset C_j for some $j \in \{0, 1, \ldots, e-1\}$. Hence, we have found a representation of y as the difference of two elements from the same coset. Vice versa, every such difference representation of y gives a difference representation for x. Consequently, every element of $\mathbb{F}_q^*$ has the same number of difference representations.

As there are e cosets C_i, all of cardinality f, and every C_i provides $f(f-1)$ differences, we have $ef(f-1)$ total differences. They are distributed equally over all $q - 1 = ef$ elements of $\mathbb{F}_q^*$. Consequently, every $x \in \mathbb{F}_q^*$ has exactly $f - 1$ representations $x = c - c'$ where $c, c' \in C_i$ for some $i \in \{0, 1, \ldots, e-1\}$. □

Note that, according to Proposition 2.1, the collection C from Theorem 2.4 also forms a near-complete $(q, f, q-f-1)$ external difference family in the additive group of $\mathbb{F}_q$. Moreover, we remark that when we write $q = p^n$ for a prime p and an integer n, we may understand C as a difference family in $\mathbb{Z}_p^n$ as this group is isomorphic to the additive group of $\mathbb{F}_q$.

Example 2.12. The near-complete $(13, 4, 3)$ disjoint difference family in the cyclic group $\mathbb{Z}_{13}$ from Example 1.1 has been constructed using Theorem 2.4. Consider the finite field $\mathbb{F}_{13}$ with 13 elements. Then 2 is primitive in $\mathbb{F}_{13}$, and D contains exactly the subgroup of the third powers of 2 and its cosets:

$$D = \{\{2^0, 2^3, 2^6, 2^9\}, \{2^1, 2^4, 2^7, 2^{10}\}, \{2^2, 2^5, 2^8, 2^{11}\}\}.$$

In Theorem 2.5, we present Furino's [62] construction of difference families in commutative rings with an identity. His approach is a generalization of Wilson's construction in finite fields from Theorem 2.4. In this thesis, we only restate the special case of difference families with parameters $(v, k, k-1)$ of Furino's construction, for which we add a short proof. In general, his construction provides $(v, k, e(k-1))$ disjoint difference families for some integer e dividing k.

Theorem 2.5 ([62, Theorem 3.3 and Corollary 3.5]). *Let R be a commutative ring with an identity. Define $v = |R|$, and denote the unit group of R by R^*. Let B be a subgroup of R^* of order k such that $\Delta B \subseteq R^*$. Denote by S a system of representatives of the cosets of B in $R \setminus \{0\}$. The collection $\{sB : s \in S\}$ is a near complete $(v, k, k-1)$ disjoint difference family in the additive group of R.*

Proof. Note that, by definition, the sets sB, where $s \in S$, partition $R \setminus \{0\}$. We first show that $|sB| = k$ for all $s \in S$. Let $s \in S$. If $s \in R^*$, then clearly $|sB| = k$ since B is a subgroup of R^* and $|B| = k$. Now suppose $s \notin R^*$, and recall that $s \neq 0$.

Assume, by way of contradiction, that $|sB| < k$. This implies there are distinct $b, b' \in B$ such that $sb = sb'$ or, equivalently, $s(b - b') = 0$. Since $\Delta B \subseteq R^*$, we have $b - b' \in R^*$, which, in particular, implies $b - b' \neq 0$. It follows that $s = 0$, which is a contradiction. Hence, also if s is not a unit, $|sB| = k$.

It remains to show that every nonzero element of R has $k-1$ representations $b - b'$ where $b, b' \in sB$ for some $s \in S$. Write

$$\Delta sB = \bigcup_{\substack{b \in B \\ b \neq 1}} (b-1)sB.$$

Then, as the sets sB partition $R \setminus \{0\}$, the multiset union

$$\bigcup_{s \in S} \Delta sB = \bigcup_{\substack{b \in B \\ b \neq 1}} (b-1)\left(R \setminus \{0\}\right).$$

As we have $k-1$ choices for $b \in B$ such that $b \neq 1$, the above multiset union consists of $k-1$ copies of $R \setminus \{0\}$. □

Note that, by abuse of denotation, we also call a set sB where s is not a unit a coset of the subgroup B. Furthermore, we remark that the construction by Furino [62] was generalized in the case $(v, k, k-1)$ by Buratti [30] to so-called *Ferrero pairs* (G, A), where G is a group, and A is a non-trivial group of automorphisms of G acting semiregularly on $G \setminus \{0\}$.

We next present the construction of difference families in Galois rings by Davis, Huczynska, and Mullen [43]. Inspired by Wilson's [102] construction from Theorem 2.4, the aforementioned authors found a cyclotomic construction of a near-complete $(p^{2r}, p^r - 1, p^{2r} - p^r)$ external difference family in the Galois ring $\mathrm{GR}(p^2, r)$ of characteristic p^2. According to Proposition 2.1, their near-complete external difference family is also a near-complete disjoint difference family. When seen in this way, the construction fits into the general framework of Theorem 2.5 as we will show in the proof of Theorem 2.6. We remark that the result may also be proved directly by a similar approach as in Theorem 2.4 or using the Ferrero pairs by Buratti [30].

Theorem 2.6 ([43, Theorem 4.1])**.** *Let p be a prime, and let r be a positive integer such that $p^r \geq 3$. Let $\mathcal{T}$ be the Teichmüller set of the Galois ring $\mathrm{GR}(p^2, r)$, and let $\mathcal{T}^* = \mathcal{T} \setminus \{0\}$. Moreover, denote by $\mathbb{P} = \{1 + p\alpha : \alpha \in \mathcal{T}\}$ the group of principal units of $\mathrm{GR}(p^2, r)$, and let $S = \mathbb{P} \cup \{p\}$. The collection*

$$D = \{s\mathcal{T}^* : s \in S\}$$

forms a near-complete $(p^{2r}, p^r - 1, p^r - 2)$ disjoint difference family in the additive group of $\mathrm{GR}(p^2, r)$.

Proof. We show that D meets the conditions of Theorem 2.5. Denote by $\mathcal{I} = p\mathrm{GR}(p^2, r)$ the maximal ideal of $\mathrm{GR}(p^2, r)$. The Teichmüller set $\mathcal{T}$ is a system of representatives of $\mathrm{GR}(p^2,r)/\mathcal{I}$. As we have pointed out in Section 2.3, this factor ring is isomorphic to the finite field $\mathbb{F}_{p^r}$. Consequently, the difference of two distinct elements of the Teichmüller group $\mathcal{T}^*$ is a unit, hence $\Delta\mathcal{T}^* \subseteq \mathrm{GR}(p^2,r)^*$. Clearly, S is a system of representatives of the cosets of $\mathcal{T}^*$ in $\mathrm{GR}(p^2,r) \setminus \{0\}$. As $|\mathcal{T}^*| = p^r - 1$, by Theorem 2.5, D is a (p^{2r}, p^r-1, p^r-2) disjoint difference family. □

Note that for $p = 2$ and $r = 1$, the collection D from Theorem 2.6 is not a difference family in $\mathrm{GR}(4,1) \cong \mathbb{Z}_4$ since, in this case, $|\mathcal{T}^*| = 1$. Moreover, we remark that D can be considered as a difference family in $\mathbb{Z}_{p^2}^r$.

Example 2.13. Consider the Galois ring $\mathrm{GR}(9,2)$ that we presented in Example 2.11 with its Teichmüller group $\mathcal{T}^*$ and its group of principle units $\mathbb{P}$. Let $S = \mathbb{P} \cup \{3\}$. Then $D = \{s\mathcal{T}^* : s \in S\}$ forms a near-complete $(81,8,7)$ disjoint difference family in the additive group of $\mathrm{GR}(9,2)$.

Inspired by Theorem 2.6 and the work by Furino [62], we noticed that if p is odd, we obtain a new disjoint difference family in the additive group of $\mathrm{GR}(p^2,r)$ by collecting the cosets of the group of *Teichmüller squares.*

Theorem 2.7. *Let p be an odd prime, and let r be a positive integer such that $p^r \geq 5$. Moreover, let $\mathcal{T}^* = \{1, \xi, \xi^2, \ldots, \xi^{p^r-2}\}$ be the Teichmüller group of the Galois ring* $\mathrm{GR}(p^2,r)$*, and let $\mathcal{T} = \mathcal{T}^* \cup \{0\}$. Denote by*

$$\mathcal{T}_Q^* = \{1, \xi^2, \ldots, \xi^{p^r-3}\}$$

the subgroup of squares of $\mathcal{T}^*$ and by $\mathbb{P} = \{1 + p\alpha : \alpha \in \mathcal{T}\}$ the group of principle units of $\mathrm{GR}(p^2,r)$*. Let*

$$S = \mathbb{P} \cup \xi\mathbb{P} \cup \{p, p\xi\}.$$

The collection

$$D = \{s\mathcal{T}_Q^* : s \in S\}$$

forms a near-complete $\left(p^{2r}, \frac{p^r-1}{2}, \frac{p^r-3}{2}\right)$ disjoint difference family in the additive group of $\mathrm{GR}(p^2,r)$*.*

Proof. First, as $|\mathcal{T}^*| = p^r - 1$ is even, exactly half of the elements of $\mathcal{T}^*$ are squares. Hence, $|\mathcal{T}_Q^*| = \frac{p^r-1}{2}$. We show that D meets the conditions of Theorem 2.5. In the proof of Theorem 2.6, we showed that $\Delta\mathcal{T}^* \subseteq \mathrm{GR}(p^2,r)^*$. As $\mathcal{T}_Q^* \subseteq \mathcal{T}^*$, it follows that also $\Delta\mathcal{T}_Q^* \subseteq \mathrm{GR}(p^2,r)^*$. Clearly, S is a system of representatives of the cosets of $\mathcal{T}_Q^*$ in $\mathrm{GR}(p^2,r)$. Consequently, by Theorem 2.5, D is a $(p^{2r}, \frac{p^r-1}{2}, \frac{p^r-3}{2})$ disjoint difference family in the additive group of $\mathrm{GR}(p^2,r)$. □

Note that in the Galois ring $\mathrm{GR}(p^2,r)$ where p is odd, the difference family from Theorem 2.7 can be obtained by cutting the base blocks of the difference family from Theorem 2.6 into halves.

Example 2.14. Consider the Galois ring $\mathrm{GR}(9,2)$ that we presented in Example 2.11 with its Teichmüller group $\mathcal{T}^*$ and its group of principle units $\mathbb{P}$. Let

$$\mathcal{T}_Q^* = \{1, \xi^2, \xi^4, \xi^6\} = \{1,\ 4\xi+1,\ 8,\ 5\xi+8\}$$

be the group of Teichmüller squares. Define $S = \mathbb{P} \cup \xi\mathbb{P} \cup \{3, 3\xi\}$. The collection $D = \{s\mathcal{T}_Q^* : s \in S\}$ forms a near-complete $(81,4,3)$ disjoint difference family in the additive group of $\mathrm{GR}(9,2)$.

Furthermore, we remark that for the difference families from both Theorem 2.6 and Theorem 2.7 in $\mathrm{GR}(p^2,r)$, there exists a difference family from Theorem 2.4 in the finite field $\mathbb{F}_{p^{2r}}$ with the same parameters. For the parameters from Theorem 2.6, it can be constructed by taking the subgroup of (p^r+1)-th powers in $\mathbb{F}_{p^{2r}}^*$ and its cosets as the base blocks. For the parameters from Theorem 2.7, we take the subgroup of $2(p^r+1)$-th powers and its cosets.

To conclude this section, we present a construction of disjoint difference families in the Galois ring $\mathrm{GR}(p^2,2n)$ of characteristic p^2 and even extension degree $2n$ for some positive integer n that was introduced by Momihara [84]. We need the following notations first.

Denote by R_{2n} the Galois ring $\mathrm{GR}(p^2,2n) = \mathbb{Z}_{p^2}[X]/(P(X))$, where $P(X)$ is a monic basic primitive polynomial of degree $2n$. Denote by $\mathcal{I}_{2n}$ the maximal ideal and by $\mathbb{P}_{2n} = 1 + \mathcal{I}_{2n}$ the group of principal units of R_{2n}. Let ξ be a root of order $p^{2n}-1$ of $P(X)$, and let

$$\mathcal{T}_{2n} = \{0, 1, \xi, \dots, \xi^{p^{2n}-2}\}$$

be the Teichmüller set of R_{2n}. Recall that each element of R_{2n} has a unique p-adic representation $\alpha_0 + p\alpha_1$, where $\alpha_0, \alpha_1 \in \mathcal{T}_{2n}$.

According to Wan [101, Theorem 14.24], the Galois ring R_{2n} contains a unique Galois ring $\mathrm{GR}(p^2,n)$ of characteristic p^2 and extension degree n as a subring. We denote this subring by R_n. It can be constructed in the following way [101, Corollary 14.28]. The element $\xi^{p^n+1} \in \mathcal{T}_{2n}^*$ has order p^n-1 in $\mathcal{T}_{2n}^*$. Hence, it generates a subgroup of order p^n-1 of $\mathcal{T}_{2n}^*$, which is the Teichmüller group $\mathcal{T}_n^*$ of R_n. Hence,

$$\mathcal{T}_n = \{0, 1, \xi^{p^n+1}, \xi^{2(p^n+1)}, \dots, \xi^{(p^n-2)(p^n+1)}\}$$

is the Teichmüller set of R_n, and we may describe R_n as

$$R_n = \{\alpha_0 + p\alpha_1 : \alpha_0, \alpha_1 \in \mathcal{T}_n\}.$$

Then

$$R_n^* = \{\alpha_0(1+p\alpha_1) : \alpha_0 \in \mathcal{T}_n^*, \alpha_1 \in \mathcal{T}_n\}$$

is the unit group of R_n. Analogously to the notations for R_{2n}, denote by $\mathcal{I}_n = pR_n$ the maximal ideal and by $\mathbb{P}_n = 1 + \mathcal{I}_n$ the group of principal units of R_n. Then R_n^* is the direct product of $\mathcal{T}_n^*$ and $\mathbb{P}_n$.

Now, let $S \subseteq \mathcal{T}_{2n}$ such that pS is a system of representatives of $\mathcal{I}_{2n}/\mathcal{I}_n$. Then $1 + pS$ is a system of representatives of $\mathbb{P}_{2n}/\mathbb{P}_n$. We enumerate the elements of S in an arbitrary order and write $S = \{\alpha_0, \alpha_1, \dots, \alpha_{p^n-1}\}$. Finally, we define a subset P of $\mathcal{I}_{2n}$ as

$$P = \{p\xi^{p^n}, p\xi^{(p^n+1)+p^n}, p\xi^{2(p^n+1)+p^n}, \dots, p\xi^{(p^n-2)(p^n+1)+p^n}\}.$$

We are now able to describe Momihara's [84] difference family.

Theorem 2.8 ([84, Theorem 1])**.** *Let p be a prime, and let n be a positive integer. Using the notations from above, for $i = 0, 1, \dots, p^n$, define subsets*

$$D_i = \xi^i \left(P \cup \left(\bigcup_{j=0}^{p^n-1} \xi^j (1 + p\alpha_j) R_n^* \right) \right)$$

of the Galois ring $\mathrm{GR}(p^2, 2n)$. The collection $D = \{D_0, D_1, \dots, D_{p^n}\}$ forms a near-complete $\left(p^{4n},\, p^{3n} - p^{2n} + p^n - 1,\, p^{3n} - p^{2n} + p^n - 2\right)$ disjoint difference family in the additive group of $\mathrm{GR}(p^2, 2n)$.

We remark that the construction from Theorem 2.8 does not meet the conditions from Furino's [62] Theorem 2.5. For the extensive and technical proof of Theorem 2.8, the reader is referred to Momihara [84].

Example 2.15. Consider the Galois ring $R_2 = \mathrm{GR}(9, 2)$ that we presented in Example 2.11 with its Teichmüller group $\mathcal{T}_2^*$ and its group of principle units $\mathbb{P}_2$. The Galois ring R_2 contains the Galois ring $R_1 = \mathrm{GR}(9, 1) = \mathbb{Z}_9$ as a subring. Then

$$\mathcal{T}_1^* = \{1, 8\}, \qquad \mathcal{I}_1 = \{0, 3, 6\}, \qquad \text{and} \qquad \mathbb{P}_1 = \{1, 4, 7\}$$

are the Teichmüller group, the maximal ideal, and the group of principal units of R_1, respectively. Moreover, the unit group of R_1 is

$$R_1^* = \{1, 2, 4, 5, 7, 8\}.$$

If we define

$$S = \{0, \xi, \xi^5\},$$

then $1 + pS$ is a system of representatives of $\mathbb{P}_{2n}/\mathbb{P}_n$. Eventually, let

$$P = \{3\xi^3, 3\xi^7\}.$$

For $i = 0, 1, 2, 3$, define

$$D_i = \xi^i \left(P \cup R_1^* \cup \xi(1 + 3\xi) R_1^* \cup \xi^2 (1 + 3\xi^5) R_1^* \right).$$

Then the collection $D = \{D_0, D_1, \dots, D_3\}$ is a near-complete $(81, 20, 19)$ disjoint difference family in $\mathrm{GR}(9, 2)$.

In his paper, Momihara [84] mentions that for given p and n, since $p^{3n} - p^{2n} + p^n - 1 = (p^{2n}+1)(p^n-1)$ divides $p^{4n}-1$, there exists a disjoint difference family in the additive group of the finite field $\mathbb{F}_{p^{4n}}$ with the same parameters as in Theorem 2.8. We can construct this difference family using Theorem 2.4 by taking the subgroup of the (p^n+1)-th powers in $\mathbb{F}^*_{p^{4n}}$ and its cosets as the base blocks.

2.5 A new divisible difference family in Galois rings

Motivated by our study of Momihara's [84] disjoint difference families from Theorem 2.8, we found a new infinite family of *divisible difference families* in the Galois ring $\mathrm{GR}(p^2, 2n)$.

Definition 2.16. Let G be an abelian group of order v, and let N be a subgroup of G. Let $D_1, D_2, \ldots, D_b$ be k-subsets of G. The collection $D = \{D_1, D_2, \ldots, D_b\}$ is called a *divisible difference family with parameters* $(G, N, k, \lambda_1, \lambda_2)$ if each nonzero element of N occurs exactly λ_1 times and each element of $G \setminus N$ occurs exactly λ_2 times in the multiset union

$$\bigcup_{i=1}^{b} \Delta D_i.$$

If $N = \{0\}$, then D is a (v, k, λ_2) difference family. If $b = 1$ and if we set $|N| = n$ and $m = \frac{v}{n}$, then D is a $(m, n, k, \lambda_1, \lambda_2)$ divisible difference set. If $\lambda_1 = 0$, we say that D is a (G, N, k, λ_2) relative difference family.

Divisible difference families were first introduced by Momihara and Yamada [85]. We use the notation we introduced before Theorem 2.8, and we consider the Galois ring $\mathrm{GR}(p^2, 2n)$ again.

Theorem 2.9. *Let p be a prime, and let n be a positive integer. Denote by R_{2n} the Galois ring $\mathrm{GR}(p^2, 2n)$. We define a subgroup T of the unit group R^*_{2n} as the direct product of the Teichmüller group $\mathcal{T}^*_n$ of the subring R_n and the group of principle units $\mathbb{P}_{2n}$ of R_{2n}, in short: $T = \{\alpha_0(1 + p\alpha_1) : \alpha_0 \in \mathcal{T}^*_n, \alpha_1 \in \mathcal{T}_{2n}\}$. The collection*

$$\{T, \xi T, \ldots, \xi^{p^n} T\}$$

is a $((R_{2n}, +)$, $\mathcal{I}_{2n}$, $p^{3n} - p^{2n}$, $p^{4n} - p^{2n}$, $p^{3n} - 2p^{2n})$ divisible difference family.

Proof. Since $|\mathcal{T}^*_n| = p^n - 1$ and $|\mathbb{P}_{2n}| = p^{2n}$, clearly $|T| = p^{2n}(p^n - 1)$. Rewrite T as $T = \{\alpha_0 + p\alpha_1 : \alpha_0 \in \mathcal{T}^*_n, \alpha_1 \in \mathcal{T}_{2n}\}$. In ΔT, we consider differences of the type

$$\alpha_0 + p\alpha_1 - (\beta_0 + p\beta_1), \tag{2.1}$$

where $\alpha_0, \beta_0 \in \mathcal{T}^*_n$ and $\alpha_1, \beta_1 \in \mathcal{T}_{2n}$ such that $(\alpha_0, \alpha_1) \neq (\beta_0, \beta_1)$. We show that ΔT consists of $p^{2n}(p^n - 1)$ copies of $\mathcal{I}_{2n} \setminus \{0\}$ and $p^{2n}(p^n - 2)$ copies of T. We separate two cases.

First, suppose $\alpha_0 = \beta_0$, which implies $\alpha_1 \neq \beta_1$. Then (2.1) becomes

$$p(\alpha_1 - \beta_1),$$

which is a nonzero element of $\mathcal{I}_{2n}$. There are $p^n - 1$ possible choices for $\alpha_0 \in \mathcal{T}_n^*$ and $p^{2n}(p^{2n} - 1)$ possible choices for (α_1, β_1) where $\alpha_1, \beta_1 \in \mathcal{T}_{2n}$ and $\alpha_1 \neq \beta_1$. As $\mathcal{T}_{2n}$ is a system of representatives of the factor ring $R_{2n}/\mathcal{I}_{2n}$, which is isomorphic to $\mathbb{F}_{p^{2n}}$, the differences $p(\alpha_1 - \beta_1)$ cover each of the $p^{2n} - 1$ elements of $\mathcal{I}_{2n} \setminus \{0\}$ exactly $p^{2n}(p^n - 1)$ times.

Now, assume $\alpha_0 \neq \beta_0$. We first show that in this case, the difference from (2.1) is an element of T. Rewrite (2.1) as

$$\alpha_0 - \beta_0 + p(\alpha_1 - \beta_1). \tag{2.2}$$

In the proof of Theorem 2.6, we showed that $\Delta\mathcal{T}_n^* \subseteq R_n^*$. Consequently, for every distinct $\alpha_0, \beta_0 \in \mathcal{T}_n^*$, there are $\gamma_0 \in \mathcal{T}_n^*$ and $\gamma_1 \in \mathcal{T}_n$ such that $\alpha_0 - \beta_0 = \gamma_0 + p\gamma_1$. Hence, (2.2) can be written in the form

$$\gamma_0 + p(\gamma_1 + \alpha_1 - \beta_1), \tag{2.3}$$

where $\gamma_0 \in \mathcal{T}_n^*$ and $p(\gamma_1 + \alpha_1 - \beta_1) \in \mathcal{I}_{2n}$. This implies that for $\alpha_0 \neq \beta_0$, the difference from (2.1) is an element of T.

Next, we rewrite (2.2) with respect to all distinct $\alpha_0, \beta_0 \in \mathcal{T}_n^*$ and $\alpha_1, \beta_1 \in \mathcal{T}_{2n}$ as

$$\Delta\mathcal{T}_n^* + p\Delta\mathcal{T}_{2n}.$$

Since $\mathcal{T}_n$ is a system of representatives of $R_n/\mathcal{I}_n$, which is isomorphic to $\mathbb{F}_{p^n}$, the multiset $\Delta\mathcal{T}_n^*$ contains the same number of elements from every coset $\alpha + \mathcal{I}_n$, where $\alpha \in \mathcal{T}_n^*$. It follows that in (2.3), every $\gamma_0 \in \mathcal{T}_n^*$ occurs equally often. Consequently, the differences from (2.2) cover every element of T equally often. There are $p^{4n}(p^n - 1)(p^n - 2)$ distinct ways to choose $\alpha_0, \alpha_1, \beta_0, \beta_1$ in (2.2), and $|T| = p^{2n}(p^n - 1)$. It follows that each element of T is represented $p^{2n}(p^n - 2)$ times as the difference of two distinct elements of T.

Having studied the structure of ΔT, we easily obtain similar results for the structure of $\Delta\xi^s T$ for all $s = 0, 1, \ldots, p^n$. Since $\Delta\xi^s T = \xi^s \Delta T$, the multiset $\Delta\xi^s T$ contains $p^{2n}(p^n - 1)$ copies of $\xi^s \mathcal{I}_{2n} = \mathcal{I}_{2n}$ and $p^{2n}(p^n - 2)$ copies of $\xi^s T$. As we have $p^n + 1$ sets $\xi^s T$, the multiset union $\bigcup_{s=0}^{p^n} \Delta\xi T$ contains $p^{2n}(p^n - 1)(p^n + 1) = p^{4n} - p^{2n}$ copies of $\mathcal{I}_{2n}$. Note that $\bigcup_{s=0}^{p^n} \xi T = R_{2n}^*$. Consequently, every element of $R_{2n}^* = R_{2n} \setminus \mathcal{I}_{2n}$ occurs with multiplicity $p^{2n}(p^n - 2) = p^{3n} - 2p^{2n}$ in $\bigcup_{s=0}^{p^n} \Delta\xi T$. □

We illustrate Theorem 2.9 in the following example.

Example 2.17. We consider the Galois ring $R_2 = \mathrm{GR}(9, 2)$ and its subring $R_1 = \mathrm{GR}(9, 1)$ that we introduced in Example 2.11 and Example 2.15, respectively. Denote the maximal ideal of R_2 by $\mathcal{I}_2$. If we define T as the direct product of $\mathcal{T}_1^*$ and $\mathbb{P}_2$, then the collection

$$\{T, \xi T, \xi^2 T, \xi^3 T\}$$

is a $((R_2, +), \mathcal{I}_2, 18, 72, 9)$ divisible difference family. The multiset $\bigcup_{s=0}^{3} \Delta \xi^s T$ consists of 72 copies of $\mathcal{I}_{2n}$ and 9 copies of $R_{2n} \setminus I_{2n} = R_{2n}^*$.

3 Solving isomorphism problems of disjoint difference families

As mentioned in Section 2.4, for each of the difference families in the Galois ring $\mathrm{GR}(p^2, r)$ from Theorem 2.6, Theorem 2.7 and Theorem 2.8, there exists a difference family with the same parameters in the finite field $\mathbb{F}_{p^{2r}}$ from Theorem 2.4. Note that two difference families in the additive groups of $\mathrm{GR}(p^2, r)$ and $\mathbb{F}_{p^{2r}}$, respectively, cannot be equivalent as they are defined in different groups $\mathbb{Z}_p^{2r}$ and $\mathbb{Z}_{p^2}^{r}$. However, as pointed out in Section 2.2, the difference families could still be isomorphic. Since all three constructions in Galois rings are inspired by the concept of cyclotomy used in Wilson's [102] construction, it is natural to ask whether the difference families are mutually isomorphic or not.

In this chapter, we are going to answer this question. We study three isomorphism problems about the difference families from Section 2.4: we examine whether Wilson's [102] difference families in finite fields from Theorem 2.4 are isomorphic to the difference families in Galois rings from Theorem 2.6, Theorem 2.7 and Theorem 2.8.

If we want to solve an isomorphism problem about difference families, we need to decide whether two combinatorial designs are isomorphic or not. This is, in general, a hard problem. If two designs are isomorphic, one can simply present the corresponding isomorphism. If they are nonisomorphic, however, we have to show that there is no such isomorphism. Usually, this is quite difficult. In this case, it is often promising to look for a suitable isomorphism invariant that discriminates the designs.

One popular approach is to study the ranks or the p-ranks of the incidence matrices of the designs. But for the isomorphism problems we study, all the ranks are full. When checking examples computationally, it often helps to compute the automorphism groups of the designs. Computer algebra systems like `Magma` [16] have built-in functions to do so. It is a hard problem though, to determine the automorphism group of a combinatorial design theoretically.

The approach we follow is to calculate so-called block intersection numbers of our 2-designs. In Section 3.1, we give an overview of these numbers. While this technique has its limitations as well, it will be helpful in the cases we study: we will completely solve the isomorphism problems for Wilson's [102] difference families and the difference families by Momihara [84] and by Davis, Huczynska, and Mullen [43] in Section 3.2 and Section 3.4, respectively, and we will present a partial solution to the isomorphism problem for Wilson's [102] difference family and our new difference family from Theorem 2.7 in Section 3.3. In Chapter 6, we will eventually take a closer look at the limitations of our block intersection number approach.

3.1 Block intersection numbers

We begin by defining block intersection numbers of a combinatorial design.

Definition 3.1. Let $\mathcal{D}$ be a t-(v, k, λ)-design. We call a nonnegative integer N a *block intersection number* or, in brief, *intersection number* of $\mathcal{D}$ if $\mathcal{D}$ contains two distinct blocks B and B' that intersect in exactly N points. If N is a block intersection number of $\mathcal{D}$, we denote by $n(N)$ the *multiplicity* of N, which is the number of pairs of distinct blocks B, B' of $\mathcal{D}$ such that $|B \cap B'| = N$.

Block intersection numbers have often been used to study combinatorial designs. For example, a 2-design with only one intersection number is symmetric: the number of blocks equals the number of points. Block intersection numbers can be easily computed in the following way:

Remark 3.1. Let M denote the incidence matrix of a t-design $\mathcal{D}$ with the rows of M corresponding to the points and the columns of M corresponding to the blocks of $\mathcal{D}$. The entry (i, j) of the matrix $M^T M$ equals the cardinality $|B_i \cap B_j|$ of the intersection of the blocks B_i and B_j that correspond to the columns i and j of M. Since $B_i \cap B_j$ equals $B_j \cap B_i$ and $|B_i \cap B_i| = |B_i|$ is no block intersection number, we describe all the block intersection numbers of $\mathcal{D}$ as the multiset of the matrix entries (i, j), where $i < j$, of $M^T M$.

In our case, all designs will be developments of difference families. In this situation, there is a strong connection between differences and block intersection numbers.

Remark 3.2. Let $D = \{D_1, D_2, \dots, D_b\}$ be a difference family in an abelian group G, and let $\mathcal{D} = \text{dev}(D)$. Let $D_i, D_j \in D$ be two not necessarily distinct base blocks of $\mathcal{D}$, and let $d \in G$ be a difference occurring with multiplicity N_d in the multiset $D_i - D_j$. Then N_d is the block intersection number $|D_i \cap (D_j + d)|$ of the blocks D_i and $D_j + d$ of $\mathcal{D}$. Hence, we may determine the block intersection number $|D_i \cap (D_j + d)|$ by calculating the multiplicity N_d of d in $D_i - D_j$. Note that in this case, N_d is also the intersection number of the blocks $D_i + d'$ and $D_j + (d + d')$ for all $d' \in G$.

Block intersection numbers of combinatorial designs clearly are invariant under isomorphism: if B, B' are blocks of a t-design $\mathcal{D}$ with $|B \cap B'| = N$ and α is a permutation of the point set of $\mathcal{D}$, then $|\alpha(B) \cap \alpha(B')| = N$. So, to prove that two designs $\mathcal{D}$ and $\mathcal{D}'$ are nonisomorphic, it is sufficient to show that $\mathcal{D}$ has one block intersection number different from the block intersection numbers of $\mathcal{D}'$. Note, however, that there also exist designs that have the exact same block intersection numbers but are nonisomorphic. We will present one such case in Example 3.4 in Section 3.3. The designs in this example are pairwise nonisomorphic, but they all share the same intersection numbers.

By the same argument as above, not only the block intersection numbers of a combinatorial design, but also their multiplicities are isomorphism invariants. Thus, when possible, we will also present the multiplicities of the intersection numbers we determine in this chapter. Although we will not directly use these multiplicities to solve isomorphism problems, they might be useful for further research. We determine the multiplicities of the block intersection numbers in the way we describe in the following remark.

Remark 3.3. To determine the multiplicity of an intersection number N of a design $\mathcal{D}$, we first count the number of pairs (i, j) such that two blocks B_i and B_j of $\mathcal{D}$ intersect in N elements without considering that $B_i \cap B_j = B_j \cap B_i$. In the end, we divide this number by 2.

Since we compare all three difference families in Galois rings from Theorem 2.6, Theorem 2.7 and Theorem 2.8 to Wilson's difference families in finite fields from Theorem 2.4, we finish this section by pointing out an important connection between Wilson's difference families and the so-called cyclotomic numbers.

Definition 3.2. Let $\mathbb{F}_q$ be the finite field with q elements, and let e be a positive integer dividing $q-1$. Let C_0 be the subgroup of the e-th powers of $\mathbb{F}_q^*$, and denote by $C_1, C_2, \dots, C_{e-1}$ the cosets of C_0 in $\mathbb{F}_q^*$. For fixed non-negative integers $i, j \leq e-1$, the *cyclotomic number* $(i, j)_e$ *of order* e is defined as

$$(i, j)_e = |(C_i + 1) \cap C_j|.$$

In the following Proposition 3.1, we show that the block intersection numbers of the associated design of Wilson's difference families are precisely the so-called cyclotomic numbers. Moreover, we determine the multiplicities of the intersection numbers dependent on the multiplicities of the cyclotomic numbers.

Proposition 3.1. *Let $e, f \geq 2$ be integers such that $ef = q-1$, and let C be a $(q, f, f-1)$ disjoint difference family in the additive group of $\mathbb{F}_q$ constructed with Theorem 2.4. Let $M_e = \{(i, j)_e : i, j = 0, \dots, e-1\}$ be the multiset of the cyclotomic numbers of order e in $\mathbb{F}_q$, and denote by $n_e(N)$ the multiplicity of the cyclotomic number N in M_e.*

The block intersection numbers of $\mathrm{dev}(C)$ *are* 0 *and all N with $N \in M$. They have multiplicities*

$$n(N) = \begin{cases} \frac{1}{2}q(q-1)n_e(0) + \frac{1}{2}qe(e-1) & \text{if } N = 0, \\ \frac{1}{2}q(q-1)n_e(N) & \text{otherwise.} \end{cases}$$

Proof. Let α be primitive in $\mathbb{F}_q$, and let $C = \{C_0, C_1, \dots, C_{e-1}\}$ be a disjoint difference family from Theorem 2.4 in the additive group of $\mathbb{F}_q$. Take two arbitrary distinct blocks $C_i + a$ and $C_j + b$, where $i, j \in \{0, 1, \dots, e-1\}$ and $a, b \in \mathbb{F}_q$, of $\mathrm{dev}(C)$. To calculate their block intersection number

$$|(C_i + a) \cap (C_j + b)|,$$

we need to determine the number of solutions (s, t) of the equation

$$\alpha^{se+i} + a = \alpha^{te+j} + b. \tag{3.1}$$

If $a = b$, then obviously only the case $i \neq j$ is relevant. As then C_i and C_j are disjoint, (3.1) has no solutions. Consequently,

$$|(C_i + a) \cap (C_j + a)| = 0.$$

Since there are q choices for a and $e(e-1)$ choices for (i, j) such that $i \neq j$, the block intersection number 0 occurs $qe(e-1)$ times in this case. Removing repeated intersections, this multiplicity reduces to $\frac{qe(e-1)}{2}$.

If $a \neq b$, then $a - b = \alpha^r$ for some $r \in \{0, \ldots, q-1\}$. Write $r = me + r'$ for nonnegative integers m and r' such that $r' \leq e - 1$. Now, we can rewrite (3.1) as

$$\alpha^{(s-m)e+(i-r')} + 1 = \alpha^{(t-m)e+(j-r')}.$$

Consequently,

$$|(C_i + a) \cap (C_j + b)| = |(C_{i-r'} + 1) \cap C_{j-r'}|, \tag{3.2}$$

where the subscripts of C are calculated modulo e. The right-hand side of (3.2) is exactly the cyclotomic number $(i - r', j - r')_e$. We have $q(q-1)$ choices for (a, b) such that $a \neq b$, and the difference $a - b$ covers all the elements of $\mathbb{F}_q^*$ equally often. Consequently, each cyclotomic number $(i, j)_e$ that equals N contributes with $q(q-1)$ to the multiplicity of the block intersection number N. Removing repeated intersections, this contribution reduces to $\frac{q(q-1)}{2}$. □

It follows from the previous result that we can completely determine the block intersection numbers of the design associated to a difference family from Theorem 2.4 by determining the respective cyclotomic numbers. It is, however, in general a hard number theoretic problem to determine these cyclotomic numbers, and there is rich literature about them dating back to the 1930s, when they were first studied by Dickson [45, 46]. For a long time, the problem to determine cyclotomic numbers had been solved only in single cases for small e; see for example the work by Storer [98] from 1967. In 1982, Baumert, Mills, and Ward [6] eventually proved that when -1 is a power of p modulo e, where p is the characteristic of $\mathbb{F}_q$, the cyclotomic numbers of order e can be calculated quite easily. As, in this case, there are only three distinct cyclotomic numbers, Baumert, Mills, and Ward [6] speak of *uniform* cyclotomic numbers. In Proposition 3.2, we restate their result.

Proposition 3.2 ([6, Theorems 1 and 4]). *Consider the finite field $\mathbb{F}_{p^n}$. Let $e \geq 3$ be a divisor of $p^n - 1$. If -1 is a power of p modulo e, then either $p = 2$ or $f = \frac{p^n-1}{e}$ is even, $p^n = s^2$ and $s \equiv 1 \pmod{e}$, and the cyclotomic numbers of order e are*

$$\begin{aligned} (0,0)_e &= \eta^2 - (e-3)\eta - 1, & & \\ (0,i)_e = (i,0)_e = (i,i)_e &= \eta^2 + \eta & &\text{for } i \neq 0, \\ (i,j)_e &= \eta^2 & &\text{for } i \neq j \text{ and } i,j \neq 0, \end{aligned} \tag{3.3}$$

where $\eta = \frac{s-1}{e}$.

In the following sections, we show that the parameters of the difference families from Theorem 2.6 and Theorem 2.8 meet the conditions of Proposition 3.2. Hence, in these cases, we can completely determine the intersection numbers of the development of Wilson's difference families from Theorem 2.4 by combining Proposition 3.1 and Proposition 3.2. Although the parameters from Theorem 2.7 do not meet the conditions of Proposition 3.2, we will be able to determine the intersection numbers of the respective design coming from finite fields in this case as well.

In summary, in all three isomorphism problems, we completely determine the block intersection numbers of the designs associated to the difference families in finite fields from Theorem 2.4. This implies that for the difference families in Galois rings, we only need to show that their developments have at least one block intersection number different from the respective cyclotomic numbers.

3.2 Isomorphism problem I: Wilson vs. Davis, Huczynska, and Mullen

In this section, we solve the isomorphism problem for Wilson's [102] difference families in finite fields from Theorem 2.4 and the difference families in Galois rings from Theorem 2.6 that were introduced by Davis, Huczynska, and Mullen [43]. As pointed out before, the problem was raised by these authors. We will show that the difference families from Theorem 2.4 and those from Theorem 2.6 are nonisomorphic in all but one case. We obtain this result comparing the block intersection numbers of the associated designs.

Throughout this section, we denote by C the (p^{2r}, p^r-1, p^r-2) disjoint difference family in the additive group of $\mathbb{F}_{p^{2r}}$ from Theorem 2.4 that is constructed by taking the subgroup of (p^r+1)-th powers of $\mathbb{F}_{p^{2r}}^*$ and its cosets, and we denote by D the disjoint difference family with the same parameters in the additive group of $\mathrm{GR}(p^2, r)$ from Theorem 2.6. Moreover, we denote $\mathcal{C} = \mathrm{dev}(C)$ and $\mathcal{D} = \mathrm{dev}(D)$.

First note that block intersection numbers seem to be a good isomorphism invariant to attack this problem as the following example demonstrates.

Example 3.3. From Theorem 2.4 and Theorem 2.6, we obtain $(81, 8, 7)$ disjoint difference families C and D in the additive groups of $\mathbb{F}_{3^4}$ and $\mathrm{GR}(9, 2)$, respectively. The associated designs $\mathcal{C}$ and $\mathcal{D}$ have the following intersection numbers: for $\mathcal{C}$, they are $0, 1, 7$ with multiplicities $91\,125$, $233\,280$ and $3\,240$, respectively; for $\mathcal{D}$, they are $0, 1, 2, 3, 7$ with multiplicities $129\,033$, $148\,716$, $43\,740$, $5\,832$ and 324, respectively. Consequently, C and D are nonisomorphic.

As mentioned in Section 3.1, we can completely determine the intersection numbers of $\mathcal{C}$ and their multiplicities using Proposition 3.1 and Proposition 3.2 since the respective cyclotomic numbers are uniform.

Proposition 3.3. *The 2-(p^{2r}, p^r-1, p^r-2) design $\mathcal{C}$ has exactly the block intersection numbers 0, 1 and p^r-2. These numbers occur with the following multiplicities:*

$$\begin{aligned} n(0) &= \tfrac{1}{2}(3p^{5r} + p^{4r} - 2p^{3r}), \\ n(1) &= \tfrac{1}{2}(p^{6r} - p^{5r} - p^{4r} + p^{3r}), \\ n(p^r-2) &= \tfrac{1}{2}(p^{4r} - p^{2r}). \end{aligned}$$

Proof. According to Proposition 3.1, the block intersection numbers of $\mathcal{C}$ equal the cyclotomic numbers of order p^r+1 in $\mathbb{F}_{p^{2r}}$. Using the notation from Proposition 3.2, we have $e = p^r+1$. Since $-1 \equiv p^r \pmod{p^r+1}$, we can determine the required cyclotomic numbers with the help of Proposition 3.2. From $p^{2r} = s^2$ and $s \equiv 1 \pmod{p^r+1}$, it follows that $s = -p^r$. Thus, $\eta = \frac{-p^r-1}{p^r+1} = -1$, and we obtain the cyclotomic numbers

$$\begin{aligned} (0,0)_{p^r+1} &= p^r - 2, && \\ (0,i)_{p^r+1} = (i,0)_{p^r+1} = (i,i)_{p^r+1} &= 0 && \text{for } i \neq 0, \\ (i,j)_{p^r+1} &= 1 && \text{for } i \neq j \text{ and } i,j \neq 0. \end{aligned} \tag{3.4}$$

These are the intersection numbers of $\mathcal{C}$.

To obtain their multiplicities, denote by $n_{p^r+1}(N)$ the number of cyclotomic numbers of order p^r+1 that equal N. In $\mathbb{F}_{p^{2r}}$, according to (3.4), we have

$$n_{p^r+1}(0) = 3p^r, \qquad n_{p^r+1}(1) = p^r(p^r-1) \qquad \text{and} \qquad n_{p^r+1}(p^r-2) = 1. \tag{3.5}$$

We multiply these numbers with the factor $\frac{1}{2}p^{2r}(p^{2r}-1)$ from Proposition 3.1. This gives us the multiplicities of the block intersection numbers 1 and p^r-2. To obtain the multiplicity of 0, according to Proposition 3.1, we additionally need to add $\frac{1}{2}p^{2r}(p^r+1)p^r$. □

We add an interesting observation about the cyclotomic number $(0,0)_{p^r+1}$ from the above theorem.

Remark 3.4. The finite field $\mathbb{F}_{p^{2r}}$ contains a unique subfield $\mathbb{F}_{p^r}$. Thus, the subgroup C_0 of order p^r-1 of $\mathbb{F}^*_{p^{2r}}$, which is the first base block of the disjoint difference family C, is exactly the multiplicative group of the subfield $\mathbb{F}_{p^r}$. Hence, ΔC_0 contains precisely the elements of C_0, each with multiplicity (p^r-2). It follows that $(C_0+1) \cap C_0 = C_0 \setminus \{-1\}$, and, thus, $(0,0)_{p^r+1} = p^r-2$.

We next study the block intersection numbers of $\mathcal{D}$, the design coming from the difference family D in the Galois ring $\mathrm{GR}(p^2, r)$. Recall from Remark 3.2 that the intersection numbers of the development of a difference family occur as the multiplicities of differences between or within base blocks.

Consider $\mathrm{GR}(p^2, r)$. As before, let $\mathcal{T}$ denote the Teichmüller set, and let $\mathcal{T}^* = \mathcal{T} \setminus \{0\}$ denote the cyclic Teichmüller group of order p^r-1. Furthermore, denote by $\mathcal{I} = p\mathrm{GR}(p^2, r)$ the maximal ideal and by $\mathbb{P} = 1 + \mathcal{I}$ the group of principal units. We start with three short lemmas.

Lemma 3.4. *Consider the Galois ring* $\mathrm{GR}(p^m, r)$*. If* p *is odd, then* $-1 \in \mathcal{T}^*$*, hence* $\mathcal{T}^* = -\mathcal{T}^*$*. If* $p = 2$*, then* -1 *is a principal unit, hence* $\mathbb{P} = -\mathbb{P}$*.*

Proof. Recall from Section 2.3 that the unit group $\mathrm{GR}(p^m, r)^*$ is the direct product of $\mathbb{P}$ and $\mathcal{T}^*$, and that $|\mathbb{P}| = p^{(m-1)r}$ and $|\mathcal{T}^*| = p^r - 1$. Let ξ be a generator of $\mathcal{T}^*$. If p is odd, then $\mathcal{T}^*$ has even order, and $\mathbb{P}$ is a direct product of r cyclic groups, each of odd order p^{m-1}; see Section 2.3. Consequently, there are only two second roots of unity in $\mathrm{GR}(p^m, r)$, namely 1 and -1. Hence, $-1 = \xi^{\frac{p^r-1}{2}}$ is an element of $\mathcal{T}^*$. If $p = 2$, all the even integers in $\mathbb{Z}_{2^m} \subseteq \mathrm{GR}(2^m, r)$ are elements of the maximal ideal $\mathcal{I} = 2\mathrm{GR}(2^m, r)$. Since $\mathbb{P} = 1 + \mathcal{I}$ and -1 is odd, it follows that $-1 \in \mathbb{P}$. □

Lemma 3.5 is well known; see, for example, Wan [101, Theorem 14.8].

Lemma 3.5. *Let* $u = \alpha_0(1 + p\alpha_1)$ *and* $u' = \alpha_0'(1 + p\alpha_1')$*, where* $\alpha_0, \alpha_0' \in \mathcal{T}^*$ *and* $\alpha_1, \alpha_1' \in \mathcal{T}$*, be two units in the Galois ring* $\mathrm{GR}(p^2, r)$*. The difference* $u - u'$ *is a unit if and only if* $\alpha_0 \neq \alpha_0'$*.*

Proof. The statement follows from the fact that the Teichmüller set $\mathcal{T}$ is a system of representatives of $\mathrm{GR}(p^2, r)/\mathcal{I}$, which is isomorphic to $\mathbb{F}_{p^r}$. Consequently,

$$u - u' = \alpha_0 - \alpha_0' + p(\alpha_1 - \alpha_1')$$

is not a unit, if and only if $\alpha_0 - \alpha_0' = 0$. □

Lemma 3.6. *Let* $d \in \mathrm{GR}(p^m, r)$*. If* $d \in \Delta\mathcal{T}^*$*, then* $d\mathcal{T}^* \subseteq \Delta\mathcal{T}^*$*, and all the elements of* $d\mathcal{T}^*$ *occur with the same multiplicity in* $\Delta\mathcal{T}^*$*.*

Proof. Assume d occurs with multiplicity n in $\Delta\mathcal{T}^*$, which means there exist n distinct pairs $(\alpha_1, \alpha_1'), \dots, (\alpha_n, \alpha_n')$, where $\alpha_1, \alpha_1', \dots, \alpha_n, \alpha_n' \in \mathcal{T}^*$, such that $\alpha_1 - \alpha_1' = \dots = \alpha_n - \alpha_n' = d$. For every $\gamma \in \mathcal{T}^*$, we obtain $\gamma\alpha_i - \gamma\alpha_i' = \gamma d$ for all $i = 1, \dots, n$. Since $\gamma\alpha_i, \gamma\alpha_i' \in \mathcal{T}^*$, the set $d\mathcal{T}^* = \{d\gamma : \gamma \in \mathcal{T}^*\}$ is contained in $\Delta\mathcal{T}^*$, and every element of $d\mathcal{T}^*$ occurs with multiplicity n. □

In the following statements Lemma 3.7 to Lemma 3.10, we focus on the case $p = 2$. These results will help us to determine a block intersection number of $\mathcal{D}$. It follows from Lemma 3.4 that in $\mathrm{GR}(4, r)$, the element -1 is a principal unit. Consequently, for every base block $(1 + 2\alpha)\mathcal{T}^*$, where $\alpha \in \mathcal{T}$, of D, the set $-(1 + 2\alpha)\mathcal{T}^*$ of its additive inverses is also a base block of D, and the two sets are disjoint. We also need the following result:

Lemma 3.7. *In the Galois ring* $\mathrm{GR}(4, r)$*, where* $r \geq 2$*, the Teichmüller set* $\mathcal{T}$ *is the set of all squares.*

Proof. Since $\mathcal{T} = \mathcal{T}^* \cup \{0\}$ and $\mathcal{T}^*$ is a cyclic group of odd order $2^r - 1$, all the elements of $\mathcal{T}$ are squares. Now, let $x \in \mathrm{GR}(4, r)$. If $x \in \mathcal{I}$, we write $x = p\alpha$ for some $\alpha \in \mathcal{T}$. As $p^2 = 0$, it follows that $x^2 = 0$, hence $x^2 \in \mathcal{T}$. If x is a unit, we write $x = \alpha_0(1 + p\alpha_1)$ for some $\alpha_0 \in \mathcal{T}^*$ and $\alpha_1 \in \mathcal{T}$. Recall from Section 2.3 that in $\mathrm{GR}(4, r)$, every principal unit has order 2. Hence, $(1 + p\alpha_1)^2 = 1$, which means $x^2 = \alpha_0^2$ and thereby $x^2 \in \mathcal{T}^*$. □

We additionally use the well-known result that in the Galois ring $\mathrm{GR}(4,r)$ of characteristic 4, the Teichmüller set is a relative difference set; see, for example, Bonnecaze and Duursma [14, Lemma 3]. We add a proof in Proposition 3.8 but first, we define this combinatorial object. Let G be a group of order mn that contains a normal subgroup N of order n. We call a k-subset D of G an (m,n,k,λ)*-relative difference set* in G relative to N if each element of $G \setminus N$ occurs exactly λ times in ΔD and the elements of N do not occur in ΔD.

Proposition 3.8. *In* $\mathrm{GR}(4,r)$*, where* $r \geq 2$*, the Teichmüller set* $\mathcal{T}$ *is a* $(2^r, 2^r, 2^r, 1)$*-relative difference set in the additive group of* $\mathrm{GR}(4,r)$ *relative to the maximal ideal* $\mathcal{I} = 2\mathrm{GR}(4,r)$*.*

Proof. Let $\beta, \beta' \in \mathcal{T}$. From the proof of Theorem 2.6, it follows that if $\beta \neq \beta'$, the difference $\beta - \beta'$ is a unit. Hence, the elements of $\mathcal{I}$ do not occur in $\Delta\mathcal{T}$. As $|\Delta\mathcal{T}| = |\mathrm{GR}(4,r)^*| = 4^r - 2^r$, it remains to show that every $u \in \mathrm{GR}(4,r)^*$ can be represented in the form $u = \beta - \beta'$ for some $\beta, \beta' \in \mathcal{T}$. Recall from Section 2.3 that u has a unique 2-adic representation $u = \alpha_0 + 2\alpha_1$, where $\alpha_0 \in \mathcal{T}^*$ and $\alpha_1 \in \mathcal{T}$. We need to find $\beta, \beta' \in \mathcal{T}$ such that

$$\alpha_0 + 2\alpha_1 = \beta - \beta'.$$

This equation is solved by

$$\beta = \alpha_0^{-1}(\alpha_0 + \alpha_1)^2 \qquad \text{and} \qquad \beta' = \alpha_0^{-1}\alpha_1^2.$$

Clearly, $\beta' \in \mathcal{T}$. As according to Lemma 3.7, the Teichmüller set $\mathcal{T}$ is the set of all the squares in $\mathrm{GR}(4,r)$, also $\beta \in \mathcal{T}$. □

In Proposition 3.8, we studied the Teichmüller set $\mathcal{T}$. This result immediately implies the following statement about the Teichmüller group $\mathcal{T}^*$.

Corollary 3.9. *In* $\mathrm{GR}(4,r)$*, where* $r \geq 2$*, we have*

$$\Delta\mathcal{T}^* = \mathrm{GR}(4,r)^* \setminus (\mathcal{T}^* \cup -\mathcal{T}^*),$$

and each element of $\mathrm{GR}(4,r)^* \setminus (\mathcal{T}^* \cup -\mathcal{T}^*)$ *occurs with multiplicity* 1 *in* $\Delta\mathcal{T}^*$*.*

Proof. According to Proposition 3.8, the Teichmüller set $\mathcal{T}$ is a $(2^r, 2^r, 2^r, 1)$-relative difference set in the additive group of $\mathrm{GR}(4,r)$ relative to $\mathcal{I}$. Hence, by removing 0 from $\mathcal{T}$ to obtain $\mathcal{T}^*$, we remove differences of the type $\mathcal{T}^* - 0 = \mathcal{T}^*$ and $0 - \mathcal{T}^* = -\mathcal{T}^*$ from $\Delta\mathcal{T}$ to obtain $\Delta\mathcal{T}^*$. □

For our purpose to calculate a block intersection number of $\mathcal{D}$, we need the following Lemma 3.10. A more detailed analysis of the differences and sums in the Teichmüller set in $\mathrm{GR}(4,r)$, which includes the following result in a slightly different way, is given by Hammons et al. [66, Section III.–C.] and Bonnecaze and Duursma [14, Theorem 1]. Arguments of this type have also been used by Ghinelli and Jungnickel [64] and

Resmini, Ghinelli, and Jungnickel [95] in the theory of difference sets to obtain ovals in the development of a difference set and by Pott and Zhou [93] to construct Cayley graphs.

Lemma 3.10. *In* $\mathrm{GR}(4, r)$*, where* $r \geq 2$*, an element* s *of the multiset* $\Delta_+\mathcal{T}^*$ *has multiplicity* 2 *if* s *is a unit and multiplicity* 1 *if* $s \in \mathcal{I} \setminus \{0\}$*.*

Proof. Let β, γ be two distinct elements of the Teichmüller group $\mathcal{T}^*$. Since $2\mathcal{T} = \mathcal{I}$, it follows that $\beta + \beta = 2\beta \neq 2\gamma = \gamma + \gamma$. Hence, the elements of $\mathcal{I} \setminus \{0\}$ are represented once as the sum of two elements of $\mathcal{T}^*$. We now consider sums of the type $\beta + \gamma$, where $\beta \neq \gamma$. Clearly, each sum $s = \beta + \gamma$ has at least two representations: $\beta + \gamma$ and $\gamma + \beta$. To prove that there are no more than those two representations, we suppose by way of contradiction that there exist elements $\beta', \gamma' \in \mathcal{T}^*$ such that $\beta', \gamma' \notin \{\beta, \gamma\}$ and $\beta + \gamma = \beta' + \gamma'$. This equation is equivalent to $\beta - \beta' = \gamma' - \gamma$. However, according to Corollary 3.9, all the differences of two distinct elements of $\mathcal{T}^*$ are distinct. This is a contradiction. □

We remark that Corollary 3.9 and Lemma 3.10 not only hold for $\mathcal{T}^*$ but also for any coset $(1 + 2\alpha)\mathcal{T}^*$, where $\alpha \in \mathcal{T}$, of $\mathcal{T}^*$. In Theorem 3.13, we will use Lemma 3.10 to prove that 2 is a block intersection number of $\mathcal{D}$ if $p = 2$. But first, we study the case that p is odd.

For odd p, the following two lemmas will help us bound an intersection number of $\mathcal{D}$. We will formulate the results for the Teichmüller group $\mathcal{T}^*$. As in the case $p = 2$, these results also hold for any of its cosets $(1 + p\alpha)\mathcal{T}^*$, where $\alpha \in \mathcal{T}$. According to Lemma 3.4, if p is odd, then $\mathcal{T}^* = -\mathcal{T}^*$. Hence, the Teichmüller group consists of pairs of elements and their additive inverses, and we write

$$\mathcal{T}^* = \left\{1, \xi, \xi^2, \ldots, \xi^{(p^r-3)/2}, -1, -\xi, -\xi^2, \ldots, -\xi^{(p^r-3)/2}\right\},$$

where ξ is a generator of $\mathcal{T}^*$.

Lemma 3.11. *In* $\mathrm{GR}(p^2, r)$*, where* p *is odd, let* $d \in \Delta\mathcal{T}^*$ *be the difference of two distinct elements of* $\mathcal{T}^*$*. The difference* d *has odd multiplicity if and only if* $d \in 2\mathcal{T}^*$*. If* $d \notin 2\mathcal{T}^*$*, then* d *has even multiplicity at least* 2*.*

Proof. Let $\alpha, \alpha' \in \mathcal{T}^*$ be two distinct Teichmüller elements, and let $d = \alpha - \alpha'$, which means $d \in \Delta\mathcal{T}^*$. According to Lemma 3.4, also $-\alpha, -\alpha' \in \mathcal{T}^*$. If $\alpha' \neq -\alpha$, then $-\alpha' - (-\alpha) = d$ is a second representation of d in $\Delta\mathcal{T}^*$. If $\alpha' = -\alpha$, then $d = \alpha - (-\alpha) = 2\alpha$, and it is not guaranteed that d has more than this single representation in $\Delta\mathcal{T}^*$. However, in both of the above cases, it is possible that there exist more distinct pairs $(\alpha_1, \alpha'_1), \ldots, (\alpha_\ell, \alpha'_\ell)$, where $\alpha_1, \alpha'_1, \ldots, \alpha_\ell, \alpha'_\ell \in \mathcal{T}^* \setminus \{\pm\alpha, \pm\alpha'\}$, such that $\alpha_i - \alpha'_i = -\alpha'_i - (-\alpha_i) = d$ for all $i = 1, \ldots, \ell$. In this situation, d has multiplicity $2\ell + 2$ in $\Delta\mathcal{T}^*$ if $d \notin 2\mathcal{T}^*$ and multiplicity $2\ell + 1$ if $d \in 2\mathcal{T}^*$. It is not clear, however, under which conditions such additional representations occur. □

In Lemma 3.12, we establish an upper bound on the multiplicity of the differences in the multiset $\Delta\mathcal{T}^*$. Recall from Remark 3.3 that these multiplicities are directly connected to the block intersection numbers of $\mathcal{D}$.

Lemma 3.12. *In* $\mathrm{GR}(p^2, r)$*, where* p *is odd and* $p^r > 3$*, every difference* $d \in \Delta\mathcal{T}^*$ *occurs with multiplicity less than* $p^r - 2$*.*

Proof. Note that, counting multiplicities, $\Delta\mathcal{T}^*$ contains $(p^r - 1)(p^r - 2)$ elements. We showed in Lemma 3.6 that if $\Delta\mathcal{T}^*$ contains one element of a coset of $\mathcal{T}^*$, then it contains all its elements, and they all have the same multiplicity. This implies, first, that $\Delta\mathcal{T}^*$ contains at least $p^r - 1$ distinct elements, and, second, that $p^r - 2$ is the maximum multiplicity an element of $\Delta\mathcal{T}^*$ can occur with. Now, suppose by way of contradiction that there is an element $d \in \Delta\mathcal{T}^*$ having multiplicity $p^r - 2$. Since p is odd, $p^r - 2$ is odd, and it follows from Lemma 3.11 that $d \in 2\mathcal{T}^*$. By Lemma 3.6, the whole set $2\mathcal{T}^*$ is contained in $\Delta\mathcal{T}^*$ with multiplicity $p^r - 2$. Consequently, $\Delta\mathcal{T}^* = 2\mathcal{T}^*$. Note that, as $2 < p$, clearly 2 is invertible.

Now let $\alpha \in \mathcal{T}^* \setminus \{-1, 1\}$. Note that such an element exists as the condition $p^r > 3$ guarantees that $|\mathcal{T}^*| > 2$. Then $\alpha - 1 \in \Delta\mathcal{T}^*$, which means $\alpha - 1 \in 2\mathcal{T}^*$. Hence, there is an element $\beta \in \mathcal{T}^*$ such that $\alpha - 1 = 2\beta$. By Lemma 3.4, $-1 \in \mathcal{T}^*$, which implies that $\alpha + 1$ is also contained in $\Delta\mathcal{T}^*$, and we have $\alpha + 1 = 2\beta + 2 = 2(\beta + 1)$. It follows that $\beta + 1 \in \mathcal{T}^*$. However, if both β and $\beta + 1 = \beta - (-1)$ are elements of $\mathcal{T}^*$, then $\Delta\mathcal{T}^* = \mathcal{T}^*$. In other words, $\mathcal{T}^*$ needs to be an additive $(p^{r-1}, p^{r-2}, p^{r-2})$ difference set in $\mathcal{T} = \mathcal{T}^* \cup \{0\}$. This is only the case if $\mathcal{T}$ forms an additive group. As $1 \in \mathcal{T}$, it follows that $p \in \mathcal{T}$. Since p is not a unit, this is a contradiction. Hence, there is no $d \in \mathcal{T}^*$ with multiplicity $p^r - 2$. □

Summarizing the previous results and adding the results for two special cases, we obtain Theorem 3.13, which solves the isomorphism problem for the difference families C and D.

Theorem 3.13. *Let* C *be a* $(p^{2r}, p^r - 1, p^r - 2)$ *disjoint difference family in the additive group of the finite field* $\mathbb{F}_{p^{2r}}$ *constructed with Theorem 2.4, and let* D *be a disjoint difference family with the same parameters in the additive group of the Galois ring* $\mathrm{GR}(p^2, r)$ *constructed with Theorem 2.6. The difference families* C *and* D *are isomorphic if* $p = 3$ *and* $r = 1$*, and they are nonisomorphic in every other case.*

Proof. As before, denote by $\mathcal{C}$ and $\mathcal{D}$ the associated designs of C and D, respectively. We show that $\mathcal{D}$ has a block intersection number different from the intersection numbers of $\mathcal{C}$. Recall from Proposition 3.3 that the block intersection numbers of $\mathcal{C}$ are $0, 1$ and $p^r - 2$.

We first study $\mathcal{D}$ for $p = 2$, which means D is a difference family in $\mathrm{GR}(4, r)$. Let $d \in \mathrm{GR}(4, r)$. By combining Corollary 3.9 and Lemma 3.10, we obtain the following block intersection numbers of $\mathcal{D}$:

$$|(\mathcal{T}^* + d) \cap \mathcal{T}^*| = \begin{cases} 1 & \text{if } d \in \Delta\mathcal{T}^*, \\ 0 & \text{in any other case,} \end{cases}$$

$$|(\mathcal{T}^* + d) \cap -\mathcal{T}^*| = \begin{cases} 2 & \text{if } d \in (\Delta_+(-\mathcal{T}^*)) \setminus \mathcal{I}, \\ 1 & \text{if } d \in \mathcal{I} \setminus \{0\}, \\ 0 & \text{in any other case.} \end{cases}$$

Hence, 2 is an intersection number of $\mathcal{D}$. For $r \geq 3$, this number is different from the intersection numbers of $\mathcal{C}$ and the designs are nonisomorphic. If $p = 2$ and $r = 2$, however, $\mathcal{D}$ and $\mathcal{C}$ share the same block intersection numbers together with their multiplicities: for both designs, the block intersection numbers are 0, 1, and 2 with multiplicities 1600, 1440 and 120, respectively. We solve this case by computing the automorphism groups of the designs using `Magma` [16]. The automorphism group of $\mathcal{D}$ has order 384 while the automorphism group of $\mathcal{C}$ is of order 5760. If $\mathcal{D}$ and $\mathcal{C}$ were isomorphic, their automorphism groups would have the same order. Hence, the two designs are nonisomorphic.

Now, let p be an odd prime, and let r be an integer such that $p^r > 3$. The case $p = 3$ and $r = 1$ will be considered separately as in this case, Lemma 3.12 does not hold. We show that if $p^r > 3$, the design $\mathcal{D}$ has an intersection number N such that $1 < N < p^r - 2$. First, Lemma 3.11 gives us a lower bound: for any $d \in (\Delta\mathcal{T}^* \setminus 2\mathcal{T}^*)$, the block intersection number $|\mathcal{T}^* \cap (\mathcal{T}^* + d)| \geq 2$. From Lemma 3.12, it follows that $|\mathcal{T}^* \cap (\mathcal{T}^* + d)| < p^r - 2$ for all $d \in \Delta\mathcal{T}^*$. Combining both bounds, we obtain

$$1 < |\mathcal{T}^* \cap (\mathcal{T}^* + d)| < p^r - 2$$

for all $d \in (\Delta\mathcal{T}^* \setminus 2\mathcal{T}^*)$. Consequently, C and D are nonisomorphic if p is odd and $p^r > 3$.

Eventually, let $p = 3$ and $r = 1$. In this case, the 2-$(9, 2, 1)$-designs $\mathcal{C}$ and $\mathcal{D}$ are isomorphic. Note that $\mathrm{GR}(9, 1) \cong \mathbb{Z}_9$ and $(\mathbb{F}_9, +) \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. An isomorphism between $\mathcal{D}$ and $\mathcal{C}$ computed by the computer algebra system `Magma` [16] is the following map from $\mathbb{Z}_9$, the point set of $\mathcal{D}$, to $\mathbb{Z}_3 \times \mathbb{Z}_3$, the point set of $\mathcal{C}$, given by

$$\begin{array}{lllll} 0 \mapsto (0,0), & 1 \mapsto (0,1), & 2 \mapsto (1,2), & 3 \mapsto (1,1), & 4 \mapsto (2,2) \\ 5 \mapsto (2,0), & 6 \mapsto (1,0), & 7 \mapsto (2,1), & 8 \mapsto (0,2). & \end{array}$$

□

3.3 Isomorphism problem II: Wilson vs. Kaspers and Pott

In this section, we partially solve the isomorphism problem for Wilson's [102] difference families in finite fields from Theorem 2.4 and our new difference families in Galois rings that we introduced Theorem 2.7. As pointed out in Theorem 2.7, these difference families only exist if p is odd. Hence, throughout this section, let p be an odd prime, and let r be a positive integer.

Since we will use some results from Section 3.2 in this section, we introduce the following notations first. As in Section 3.2, denote by C and by D the $(p^{2r}, p^r - 1, p^r - 2)$ difference families in the additive groups of $\mathbb{F}_{p^{2r}}$ and $\mathrm{GR}(p^2, r)$, respectively, constructed with Theorem 2.4 and Theorem 2.6, and denote the associated designs by $\mathcal{C}$ and $\mathcal{D}$. We denote by C^H and by D^H the $(p^{2r}, \frac{p^r-1}{2}, \frac{p^r-3}{2})$ difference families in the additive groups of $\mathbb{F}_{p^{2r}}$ and $\mathrm{GR}(p^2, r)$, respectively, which are constructed using Theorem 2.4 and Theorem 2.7. They can be obtained by cutting the base blocks of C and D into halves. We denote the associated designs of C^H and D^H by $\mathcal{C}^H$ and $\mathcal{D}^H$.

In Section 3.2, we solved the isomorphism problem for C and D. We showed that the difference families are nonisomorphic for all combinations of p and r except $p = 3$ and $r = 1$. However, the fact that C and D are nonisomorphic does not automatically imply that the same holds for C^H and D^H. In general, the fact that two designs $\mathcal{D}_1, \mathcal{D}_2$ are nonisomorphic does not imply that two designs $\mathcal{D}_1^H, \mathcal{D}_2^H$ that are obtained by cutting the blocks of $\mathcal{D}_1$ and $\mathcal{D}_2$ into smaller blocks are nonisomorphic. This is demonstrated in the following example, which was given by Feng and Xiang [61, Example 3.3] in the context of skew Hadamard difference sets.

Example 3.4. Consider the finite field $\mathbb{F}_{11^3}$, and let α be primitive in $\mathbb{F}_{11^3}$. Denote by C_0 the subgroup of the 14-th powers in $\mathbb{F}_{11^3}^*$, and, analogously to Theorem 2.4, let $C_i = \alpha^i C_0$ denote the i-th coset of C_0 for $i = 1, 2, \ldots, 13$. According to Theorem 2.4, the collection $C = \{C_0, C_1, \ldots, C_{13}\}$ is a disjoint difference family in the additive group of $\mathbb{F}_{11^3}$. Moreover, it can be verified that the collections

$$\begin{aligned} D_1 = \{&\{C_0 \cup C_2 \cup C_4 \cup C_6 \cup C_8 \cup C_{10} \cup C_{12}\},\\ &\{C_1 \cup C_3 \cup C_5 \cup C_7 \cup C_9 \cup C_{11} \cup C_{13}\}\},\\ D_2 = \{&\{C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_6\},\\ &\{C_7 \cup C_8 \cup C_9 \cup C_{10} \cup C_{11} \cup C_{12} \cup C_{13}\}\},\\ D_3 = \{&\{C_0 \cup C_1 \cup C_3 \cup C_4 \cup C_5 \cup C_6 \cup C_9\},\\ &\{C_2 \cup C_7 \cup C_8 \cup C_{10} \cup C_{11} \cup C_{12} \cup C_{13}\}\}. \end{aligned}$$

are also disjoint difference families in the additive group of $\mathbb{F}_{11^3}$. Consider their associated designs $\mathrm{dev}(D_1), \mathrm{dev}(D_2), \mathrm{dev}(D_3)$. Their full automorphism groups $\mathcal{A}_1, \mathcal{A}_2, \mathcal{A}_3$ have orders $|\mathcal{A}_1| = 5310690, |\mathcal{A}_2| = 252890$ and $|\mathcal{A}_3| = 758670$. Thus, the designs are pairwise nonisomorphic. However, it is clear that from each of the three difference families, we can obtain the difference family C by cutting the base blocks into the cyclotomic cosets $C_0, C_1, \ldots, C_{13}$. Hence, from the nonisomorphic designs $\mathrm{dev}(D_1), \mathrm{dev}(D_2), \mathrm{dev}(D_3)$, we can obtain the exact same design $\mathrm{dev}(C)$ by cutting their blocks into smaller blocks.

Note that all three designs share the block intersection numbers $0, 332, 333$ with multiplicities $1\,331$, $2\,655\,345$ and $885\,115$, respectively. Hence, in this example, neither the intersection numbers nor their multiplicities distinguish the designs.

Unlike in the above example, our designs $\mathcal{C}^H$ and $\mathcal{D}^H$ apparently can be distinguished by their block intersection numbers as the following example indicates. Hence, these numbers seem to be a useful isomorphism invariant.

Example 3.5. Theorem 2.4 and Theorem 2.7 yield $(625, 12, 11)$ disjoint difference families C^H and D^H in the additive groups of $\mathbb{F}_{5^4}$ and $\mathrm{GR}(25, 2)$, respectively. The associated 2-$(625, 12, 11)$ designs have the following block intersection numbers: for $\mathcal{C}^H$, they are $0, 1, 5, 6$ with multiplicities $410\,328\,750$, $117\,000\,000$, $195\,000$, and $585\,000$, respectively; for $\mathcal{D}^H$, they are $0, 1, 2, 5, 6$ with multiplicities $417\,078\,750$, $100\,687\,500$, $10\,312\,500$, $7\,500$, and $22\,500$, respectively. Hence, the difference families are nonisomorphic.

Our approach to attack the isomorphism problem for C^H and D^H is similar to the approach in Section 3.2: we first determine the block intersection numbers and their multiplicities of the design $\mathcal{C}^H$. Afterwards, we establish bounds on the intersection numbers of $\mathcal{D}^H$. This will lead to a partial solution of the isomorphism problem.

We determine the cyclotomic numbers of order $2(p^r + 1)$ in $\mathbb{F}_{p^{2r}}$, which are the intersection numbers of $\mathcal{C}^H$. Unfortunately, these cyclotomic numbers are not uniform as their parameters do not meet the conditions of Proposition 3.2, the result we used to obtain the cyclotomic numbers of order $p^r + 1$. Nevertheless, we can deduce the cyclotomic numbers of order $2(p^r + 1)$ from the cyclotomic numbers of order $p^r + 1$ that we presented in Proposition 3.3. To do so, we need the following well-known lemma by Dickson [47]. In the precise form of this thesis, it was also given by Ralston [94].

Lemma 3.14 ([47, §67], [94, Theorem 2]). *Let p be an odd prime, and let r be a positive integer. Let Q be the set of nonzero squares, and let N be the set of non-squares in the finite field $\mathbb{F}_{p^r}$. Denote by QQ the number of squares $s \in Q$ for which $s + 1$ is a nonzero square and by QN the number of $s \in Q$ for which $s + 1$ is not a square. Moreover, let NN denote the number of non-squares $n \in N$ for which $n + 1$ is not a square and NQ the number of $n \in N$ for which $n + 1$ is a nonzero square.*

- *If $p^r - 1 \equiv 0 \pmod 4$, then*

$$QQ = \frac{p^r - 5}{4}, \qquad QN = \frac{p^r - 1}{4}, \qquad NN = \frac{p^r - 1}{4}, \qquad NQ = \frac{p^r - 1}{4}.$$

- *If $p^r - 1 \equiv 2 \pmod 4$, then*

$$QQ = \frac{p^r - 3}{4}, \qquad QN = \frac{p^r + 1}{4}, \qquad NN = \frac{p^r - 3}{4}, \qquad NQ = \frac{p^r - 3}{4}.$$

Combining Lemma 3.14 with Proposition 3.3, we obtain the following result.

Proposition 3.15. *Let p be an odd prime, and let $e = p^r + 1$ for some positive integer r. In the finite field $\mathbb{F}_{p^{2r}}$, the cyclotomic numbers of order $2e$ are as follows:*

- *If* $p^r - 1 \equiv 0 \pmod 4$*, then*

$$\begin{aligned}(0,0)_{2e} &= \frac{p^r-5}{4},\\ (0,e)_{2e} = (e,0)_{2e} = (e,e)_{2e} &= \frac{p^r-1}{4}.\end{aligned}$$

- *If* $p^r - 1 \equiv 2 \pmod 4$*, then*

$$\begin{aligned}(0,e)_{2e} &= \frac{p^r+1}{4},\\ (0,0)_{2e} = (e,0)_{2e} = (e,e)_{2e} &= \frac{p^r-3}{4}.\end{aligned}$$

In both of the above cases,

$$\begin{aligned}(0,i)_{2e} &= (i,0)_{2e} = (i,i)_{2e} = (i,e)_{2e}\\ &= (e,i)_{2e} = (i,e+i)_{2e} = (e+i,i)_{2e} = 0 \qquad \textit{for } i \notin \{0,e\}.\end{aligned}$$

Out of the remaining cyclotomic numbers

$$(i,j)_{2e}, (i,j+e)_{2e}, (i+e,j)_{2e}, (i+e,j+e)_{2e}, \qquad \textit{where } i,j \neq 0 \textit{ and } i \neq j,$$

for fixed i *and* j*, exactly one cyclotomic number is* 1 *and the other three cyclotomic numbers are* 0*, but it is not known which one is* 1*.*

Proof. Let $e = p^r + 1$. Let C_0 be the unique subgroup of order $p^r - 1$ of $\mathbb{F}^*_{p^{2r}}$ formed by the e-th powers, and let $C_0, C_1, \dots, C_{p^r}$ be the cosets of C_0. Moreover, let α be primitive in $\mathbb{F}_{p^{2r}}$. The finite field $\mathbb{F}_{p^{2r}}$ contains a unique subfield $\mathbb{F}_{p^r}$ with p^r elements. Hence, C_0 is the multiplicative group $\mathbb{F}^*_{p^r}$ of $\mathbb{F}_{p^r}$. As p^r is odd, C_0 consists of $\frac{1}{2}(p^r-1)$ squares and non-squares in $\mathbb{F}_{p^r}$ each. Consequently,

$$C_0 = C_0^H \cup C_e^H,$$

where

$$C_0^H = \{1, \alpha^{2e}, \dots, \alpha^{(p^r-3)e}\}$$

is the set of nonzero squares and

$$C_e^H = \{\alpha^e, \alpha^{3e}, \dots, \alpha^{(p^r-2)e}\}$$

is the set of non-squares in $\mathbb{F}^*_{p^r}$. The values of the cyclotomic numbers $(i,j)_{2e}$, where $i,j \in \{0,e\}$, now follow from Lemma 3.14.

Note that C_0^H is a subgroup of $\mathbb{F}^*_{p^{2r}}$ itself. Consequently, in the same way as for C_0, we can divide each of the cosets $C_0, C_1, \dots, C_{p^r}$ of C_0 into two cosets C_i^H and C_{e+i}^H of C_0^H. Since

$$C_i = C_i^H \cup C_{e+i}^H$$

for all $i = 0, 1, \ldots, p^r$, we obtain

$$(C_i + 1) \cap C_j = \bigcup_{\substack{k \in \{i, e+i\}, \\ \ell \in \{j, e+j\}}} (C_k^H + 1) \cap C_\ell^H$$

for $0 \leq i, j \leq p^r$. In terms of cyclotomic numbers, this means

$$(i, j)_e = \sum_{\substack{k \in \{i, e+i\}, \\ \ell \in \{j, e+j\}}} (k, \ell)_{2e} \tag{3.6}$$

for $0 \leq i, j \leq p^r$. Recall that we determined the cyclotomic numbers of order $e = p^r + 1$ in $\mathbb{F}_{p^{2r}}$ in the proof of Proposition 3.3. The values of the cyclotomic numbers $(i, j)_{2e}$, where $i, j \notin \{0, e\}$, now follow from combining (3.6) with (3.4). □

Unfortunately, the exact values of the cyclotomic numbers $(i, j)_{2e}$, $(i, j + e)_{2e}$, $(i + e, j)_{2e}$, $(i + e, j + e)_{2e}$, where $i, j \neq 0$ and $i \neq j$, in $\mathbb{F}_{p^{2r}}$ are not known in general. It is an open problem to determine those.

Nevertheless, from Proposition 3.15, we can completely derive the block intersection numbers of the 2-design $\mathcal{C}^H$ as well as their multiplicities.

Proposition 3.16. *Let C^H be a $(p^{2r}, \frac{p^r-1}{2}, \frac{p^r-3}{2})$ difference family in the additive group of $\mathbb{F}_{p^{2r}}$ constructed with Theorem 2.4. The associated 2-design $\mathcal{C}^H$ has exactly the following block intersection numbers.*

- *If $p^r - 1 \equiv 0 \pmod 4$, the intersection numbers are $0, 1, \frac{p^r-5}{4}$, and $\frac{p^r-1}{4}$, and they occur with multiplicities*

$$\begin{aligned} n(0) &= \tfrac{1}{2}(3p^{6r} + 9p^{5r} + p^{4r} - 3p^{3r} + 2p^{2r}), \\ n(1) &= \tfrac{1}{2}(p^{6r} - p^{5r} - p^{4r} + p^{3r}), \\ n(\tfrac{p^r-5}{4}) &= \tfrac{1}{2}(p^{4r} - p^{2r}), \\ n(\tfrac{p^r-1}{4}) &= \tfrac{1}{2}(3p^{4r} - 3p^{2r}). \end{aligned}$$

- *If $p^r - 1 \equiv 2 \pmod 4$, the intersection numbers are $0, 1, \frac{p^r-3}{4}$, and $\frac{p^r+1}{4}$. The multiplicities $n(0)$ and $n(1)$ are as above and*

$$\begin{aligned} n(\tfrac{p^r-3}{4}) &= \tfrac{1}{2}(3p^{4r} - 3p^{2r}), \\ n(\tfrac{p^r+1}{4}) &= \tfrac{1}{2}(p^{4r} - p^{2r}). \end{aligned}$$

Proof. Let $e = p^r + 1$. It follows from Proposition 3.1 that the block intersection numbers of $\mathcal{C}^H$ are exactly 0 and the cyclotomic numbers from Proposition 3.15. We obtain their multiplicities using (3.6) from the proof of Proposition 3.15:

Every cyclotomic number $(i, j)_e$ of order e that equals 0 gives four cyclotomic numbers of order $2e$ that equal 0. Every cyclotomic number of order e that takes the value 1 splits into three cyclotomic numbers of order $2e$ that equal 0 and one cyclotomic number of order $2e$ that equals 1. If $p^r - 1 \equiv 0 \pmod 4$, the unique cyclotomic number of order e that equals $p^r - 2$ provides one cyclotomic number of order $2e$ that equals $\frac{p^r-5}{4}$ and three cyclotomic numbers of order $2e$ that equal $\frac{p^r-1}{4}$. If $p^r - 1 \equiv 2 \pmod 4$, we obtain $\frac{p^r-3}{4}$ three times and $\frac{p^r+1}{4}$ once from $p^r - 2$.

For $i \in \{e, 2e\}$, denote by $n_i(N)$ the number of cyclotomic numbers of order i that equal N. By the above argumentation, we obtain the following values for $n_{2e}(N)$. If $p^r - 1 \equiv 0 \pmod 4$, then

$$\begin{aligned} n_{2e}(0) &= 4n_e(0) + 3n_e(1), \\ n_{2e}(1) &= n_e(1) \\ n_{2e}(\tfrac{p^r-5}{4}) &= n_e(p^r-2), \\ n_{2e}(\tfrac{p^r-1}{4}) &= 3n_e(p^r-2). \end{aligned} \tag{3.7}$$

If $p^r - 1 \equiv 2 \pmod 4$, then $n_{2e}(0)$ and $n_{2e}(1)$ are as above and

$$\begin{aligned} n_{2e}(\tfrac{p^r-3}{4}) &= 3n_e(p^r-2), \\ n_{2e}(\tfrac{p^r+1}{4}) &= n_e(p^r-2). \end{aligned} \tag{3.8}$$

We now obtain the multiplicities of the block intersection numbers of $\mathcal{C}^H$ by combining (3.7) and (3.8) with (3.5) from the proof of Proposition 3.3 and Proposition 3.1. In (3.5), we presented the values of $n_e(N)$ for $N \in \{0, 1, p^r - 2\}$. According to Proposition 3.1, we need to multiply the numbers from (3.7) and (3.8) with $\frac{1}{2}p^{2r}(p^{2r} - 1)$ to obtain the multiplicities of the respective block intersection numbers. For the block intersection number 0 we additionally need to add $\frac{1}{2}p^{2r}(2p^{2r} + 2)(2p^{2r} + 1)$. □

Next, we examine the intersection numbers of $\mathcal{D}^H$, the design associated to the disjoint difference family D^H in the Galois ring $\mathrm{GR}(p^2, r)$ from Theorem 2.7. As in Section 3.2, we use the connection between intersection numbers and multiplicities of differences that we explained in Remark 3.2 to study these intersection numbers.

Let ξ denote a generator of the Teichmüller group $\mathcal{T}^*$, and let $\mathcal{T} = \mathcal{T}^* \cup \{0\}$. As in Theorem 2.7, we denote by $\mathcal{T}_Q^*$ the subgroup of Teichmüller squares in $\mathrm{GR}(p^2, r)^*$, and we further denote by $\mathcal{T}_N^*$ the set of Teichmüller non-squares. Furthermore, we call a coset of type

$$(1 + p\alpha)\mathcal{T}_Q^*,$$

where $\alpha \in \mathcal{T}$, a *square coset of* $\mathcal{T}_Q^*$, and a coset of type

$$(1 + p\alpha)\mathcal{T}_N^* = (1 + p\alpha)\xi\mathcal{T}_Q^*,$$

where $\alpha \in \mathcal{T}$, a *non-square coset of* $\mathcal{T}_Q^*$.

In the remainder of this section, we establish bounds on block intersection numbers of $\mathcal{D}^H$ that come from the multisets $\Delta\mathcal{T}_Q^*$ and $\mathcal{T}_Q^* - \mathcal{T}_N^*$. To obtain these bounds we need to analyze the structure of those multisets first.

Lemma 3.17. *Let p be an odd prime. Using the same notations as above, consider the multisets $\Delta\mathcal{T}_Q^*$ and $\mathcal{T}_Q^* - \mathcal{T}_N^*$ in the Galois ring $\mathrm{GR}(p^2, r)$.*

- *If $p^r - 1 \equiv 0 \pmod 4$, then $\Delta\mathcal{T}_Q^*$ contains $\frac{p^r-5}{4}$ square cosets and $\frac{p^r-1}{4}$ non-square cosets of $\mathcal{T}_Q^*$, and $\mathcal{T}_Q^* - \mathcal{T}_N^*$ contains $\frac{p^r-1}{4}$ square and non-square cosets of $\mathcal{T}_Q^*$ each.*
- *If $p^r - 1 \equiv 2 \pmod 4$, then $\Delta\mathcal{T}_Q^*$ contains $\frac{p^r-3}{4}$ square and non-square cosets of $\mathcal{T}_Q^*$ each, and $\mathcal{T}_Q^* - \mathcal{T}_N^*$ contains $\frac{p^r-3}{4}$ square cosets and $\frac{p^r+1}{4}$ non-square cosets of $\mathcal{T}_Q^*$.*

Proof. Denote by $\mathcal{I}$ the maximal ideal of $\mathrm{GR}(p^2, r)$. The Teichmüller set $\mathcal{T}$ is a system of representatives of $\mathrm{GR}(p^2, r)/\mathcal{I}$, which is isomorphic to the finite field $\mathbb{F}_{p^r}$. Hence, when considered modulo $\mathcal{I}$, differences of elements of Teichmüller squares and Teichmüller non-squares act in the same way as the respective differences of squares and non-squares in $\mathbb{F}_{p^r}$ that we studied in Lemma 3.14.

We show the result for $\Delta\mathcal{T}_Q^*$. The result for $\mathcal{T}_Q^* - \mathcal{T}_N^*$ can be obtained analogously. By the same arguments as in Lemma 3.6, $\Delta\mathcal{T}_Q^*$ consists of $\frac{p^r-3}{2}$ not necessarily distinct cosets of $\mathcal{T}_Q^*$, each of cardinality $\frac{p^r-1}{2}$. Moreover, note that $(1+p\alpha)\mathcal{T}_Q^* \equiv \mathcal{T}_Q^*$ mod $\mathcal{I}$ for any square coset of $\mathcal{T}_Q^*$, and $(1+p\alpha)\mathcal{T}_N^* \equiv \mathcal{T}_N^*$ mod $\mathcal{I}$ for any non-square coset of $\mathcal{T}_Q^*$. Let $d \in \Delta\mathcal{T}_Q^*$. Then there are $s, s' \in \mathcal{T}_Q^*$ such that

$$d = s - s'. \tag{3.9}$$

According to the proof of Theorem 2.7, d is a unit. Hence, we may write $d = \alpha_0 + p\alpha_1$ for unique $\alpha_0 \in \mathcal{T}^*$ and $\alpha_1 \in \mathcal{T}$. Dividing (3.9) by α_0 and considering this equation modulo $\mathcal{I}$, we obtain

$$\frac{s'}{\alpha_0} + 1 \equiv \frac{s}{\alpha_0} \mod \mathcal{I}. \tag{3.10}$$

Note that, as $\mathcal{T}_Q^*$ is a group, $\frac{1}{\alpha_0}$ is a square, and thereby $\frac{s'}{\alpha_0}$ and $\frac{s}{\alpha_0}$ are squares, if and only if α_0 is a square. Using the notation from Lemma 3.14, equation (3.10) has QQ solutions for s, s' if $\alpha_0 \in \mathcal{T}_Q^*$ and NN solutions if $\alpha_0 \in \mathcal{T}_N^*$. Consequently, if we consider $\Delta\mathcal{T}_Q^*$ modulo $\mathcal{I}$, this multiset contains QQ copies of $\mathcal{T}_Q^*$ and NN copies of $\mathcal{T}_N^*$, which means that $\Delta\mathcal{T}_Q^*$ consists of QQ square cosets and NN non-square cosets of $\mathcal{T}_Q^*$. □

Furthermore, we need the following properties of squares and non-squares in the Galois ring $\mathrm{GR}(p^2, r)$.

Proposition 3.18. *Consider the Galois ring $\mathrm{GR}(p^2, r)$, where p is odd.*

(a) If $p^r - 1 \equiv 0 \pmod 4$, then $-1 \in \mathcal{T}_Q^*$, and $\mathcal{T}_Q^* = -\mathcal{T}_Q^*$ and $2\mathcal{T}_Q^* \subseteq \Delta\mathcal{T}_Q^*$.

If $p^r - 1 \equiv 2 \pmod 4$, then $-1 \in \mathcal{T}_N^*$, and $\mathcal{T}_Q^* = -\mathcal{T}_N^*$ and $2\mathcal{T}_Q^* \subseteq \mathcal{T}_Q^* - \mathcal{T}_N^*$.

(b) *If* $p^r - 1 \equiv 0 \pmod{12}$, *then* $1 \in \Delta\mathcal{T}_Q^*$, *and* $\mathcal{T}_Q^* \subseteq \Delta\mathcal{T}_Q^*$.
If $p^r - 1 \equiv 6 \pmod{12}$, *then* $1 \in \mathcal{T}_N^* - \mathcal{T}_Q^*$, *and* $\mathcal{T}_Q^* \subseteq \mathcal{T}_N^* - \mathcal{T}_Q^*$.

(c) *If* $p^r - 1 \equiv 0$ *or* $6 \pmod 8$, *then* 2 *is a square, and* $2\mathcal{T}_Q^*$ *is a square coset of* $\mathcal{T}_Q^*$.
If $p^r - 1 \equiv 2$ *or* $4 \pmod 8$, *then* 2 *is a non-square, and* $2\mathcal{T}_Q^*$ *is a non-square coset of* $\mathcal{T}_Q^*$.

Proof. Let ξ be a generator of the Teichmüller group $\mathcal{T}^*$ in the Galois ring $\mathrm{GR}(p^2, r)$.

(a) In Lemma 3.4, we showed that if p is odd, $-1 \in \mathcal{T}^*$, in particular $-1 = \xi^{\frac{p^r-1}{2}}$. The exponent $\frac{p^r-1}{2}$ is even if $p^r - 1 \equiv 0 \pmod 4$; then -1 is a square in $\mathcal{T}^*$. If $p^r - 1 \equiv 2 \pmod 4$, the exponent $\frac{p^r-1}{2}$ is odd, and -1 is a non-square in $\mathcal{T}^*$.

(b) If $p^r - 1 \equiv 0 \pmod 6$, the equation $x^6 = 1$ has exactly six solutions in the Teichmüller group $\mathcal{T}^*$, namely $\xi^{\frac{k(p^r-1)}{6}}$ for $k = 0, 1, \ldots, 5$. We show that the sum of these elements is 0. It is easy to see that

$$\xi^{\frac{p^r-1}{6}} \sum_{k=0}^{5} \xi^{\frac{k(p^r-1)}{6}} = \sum_{k=0}^{5} \xi^{\frac{k(p^r-1)}{6}}.$$

Hence,

$$\left(\xi^{\frac{p^r-1}{6}} - 1\right) \sum_{k=0}^{5} \xi^{\frac{k(p^r-1)}{6}} = 0.$$

As $\xi^{\frac{p^r-1}{6}} - 1$ is the difference of two distinct Teichmüller elements, it is a unit; see the proof of Theorem 2.6. It follows that

$$\sum_{k=0}^{5} \xi^{\frac{k(p^r-1)}{6}} = 0. \tag{3.11}$$

By the same reasoning, $\sum_{k=0}^{2} \xi^{\frac{k(p^r-1)}{3}} = 0$. Consequently, we can rewrite (3.11) as

$$\xi^{\frac{5(p^r-1)}{6}} - \xi^{\frac{2(p^r-1)}{3}} = 1.$$

If $p^r - 1 \equiv 0 \pmod{12}$, the elements $\xi^{\frac{5(p^r-1)}{6}}$, and $\xi^{\frac{2(p^r-1)}{3}}$ are squares and, consequently, $1 \in \Delta\mathcal{T}_Q^*$. If $p^r - 1 \equiv 6 \pmod{12}$, then $\xi^{\frac{5(p^r-1)}{6}}$ is a non-square and $\xi^{\frac{2(p^r-1)}{3}}$ is a square, hence $1 \in \mathcal{T}_N^* - \mathcal{T}_Q^*$.

(c) We first consider $r = 1$. Note that $\mathrm{GR}(p^2, 1) = \mathbb{Z}_{p^2}$. The following classical results about quadratic residues were first systematically given by Gauß [63]. A positive integer a coprime to an odd prime p is a square in the integer ring $\mathbb{Z}_{p^m}$, where $m \geq 1$, if and only if a is a square in $\mathbb{Z}_p$. In $\mathbb{Z}_p$, the element 2 is a square if $p - 1 \equiv 0$ or $6 \pmod 8$, and 2 is a non-square if $p - 1 \equiv 2$ or $4 \pmod 8$. This solves the case $r = 1$.

Now, let $r \geq 2$. Let

$$\mathcal{T}_1^* = \{1, \zeta, \zeta^2, \ldots, \zeta^{p-2}\}$$

denote the Teichmüller group of $\mathrm{GR}(p^2, 1)$, and let $\mathcal{T}_1 = \mathcal{T}_1^* \cup \{0\}$. For a fixed prime p, the Galois ring $\mathrm{GR}(p^2, 1)$ is a subring of $\mathrm{GR}(p^2, r)$ for all $r \geq 1$. If $\mathcal{T}^* = \{1, \xi, \xi^2, \ldots, \xi^{p^r-2}\}$ is the Teichmüller group of $\mathrm{GR}(p^2, r)$, then $\mathcal{T}_1^*$ is a subgroup of $\mathcal{T}^*$ with $\zeta = \xi^{\frac{p^r-1}{p-1}}$. Thus, we may write

$$\mathcal{T}_1^* = \left\{1, \xi^{\frac{p^r-1}{p-1}}, \xi^{\frac{2(p^r-1)}{p-1}}, \ldots, \xi^{\frac{(p-2)(p^r-1)}{p-1}}\right\}.$$

Since 2 is a unit in $\mathrm{GR}(p^2, 1)$, there exist unique $\alpha_0 \in \mathcal{T}_1^*$ and $\alpha_1 \in \mathcal{T}_1$ such that $\alpha_0(1 + p\alpha_1) = 2$. It follows that $\alpha_0 = \zeta^\ell$ for some $\ell \in \{0, 1, \ldots, p-2\}$. In $\mathrm{GR}(p^2, r)$, we consequently obtain

$$2 = (1 + p\alpha_1)\, \xi^{\frac{\ell(p^r-1)}{p-1}}.$$

Hence, 2 is a square, and thereby $2\mathcal{T}_Q^*$ is a square coset of $\mathcal{T}_Q^*$, if ℓ or $\frac{p^r-1}{p-1}$ is even. The later is even if and only if r is even. In this case, $p^r - 1 \equiv 0 \pmod 8$. Hence, if r is odd, then ℓ needs to be even. This implies that 2 is a square in $\mathrm{GR}(p^2, 1)$, which, according to the case $r = 1$, holds whenever $p - 1 \equiv 0$ or $6 \pmod 8$. If r is odd, $p^r \equiv p \pmod 8$. The result follows. □

Note that it follows from Proposition 3.18 (b) that if $p^r - 1 \equiv 6 \pmod{12}$, then $\mathcal{T}_N^* \subseteq \mathcal{T}_Q^* - \mathcal{T}_N^*$. By combining all three results from Proposition 3.18, we obtain the following corollary.

Corollary 3.19. *Consider the Galois ring* $\mathrm{GR}(p^2, r)$*, where* p *is odd.*

- *If* $p^r - 1 \equiv 0 \pmod{12}$*, then* $\Delta\mathcal{T}_Q^*$ *contains both* $\mathcal{T}_Q^*$ *and* $2\mathcal{T}_Q^*$*. Moreover,* $2\mathcal{T}_Q^*$ *is a square coset of* $\mathcal{T}_Q^*$ *if and only if* $p^r - 1 \equiv 0 \pmod{24}$*.*
- *If* $p^r - 1 \equiv 6 \pmod{12}$*, then* $\mathcal{T}_Q^* - \mathcal{T}_N^*$ *contains both* $\mathcal{T}_N^*$ *and* $2\mathcal{T}_Q^*$*. Moreover,* $2\mathcal{T}_Q^*$ *is a non-square coset of* $\mathcal{T}_Q^*$ *if and only if* $p^r - 1 \equiv 18 \pmod{24}$*.*

Note that $p^r - 1 \equiv 0 \pmod{24}$ holds whenever $p \geq 5$ and r is even. To continue, we need to study under which conditions 2 is a Teichmüller square.

Lemma 3.20. *Consider the Galois ring* $\mathrm{GR}(p^2, r)$*, where* p *is odd. Then*

- $\mathcal{T}_Q^* = 2\mathcal{T}_Q^*$ *if and only if* $p^r - 1 \equiv 0$ *or* $6 \pmod 8$ *and* $2^{p-1} \equiv 1 \pmod{p^2}$*,*
- $\mathcal{T}_N^* = 2\mathcal{T}_Q^*$ *if and only if* $p^r - 1 \equiv 2$ *or* $4 \pmod 8$ *and* $2^{p-1} \equiv 1 \pmod{p^2}$*.*

Proof. The equation $\mathcal{T}_Q^* = 2\mathcal{T}_Q^*$ holds if and only if $2 \in \mathcal{T}_Q^*$, which means 2 is a square in the Teichmüller group $\mathcal{T}^*$. According to Proposition 3.18 (c), the element 2 is a square in $\mathrm{GR}(p^2, r)^*$ if and only if $p^r - 1 \equiv 0$ or $6 \pmod 8$. Recall that $\mathrm{GR}(p^2, r)^*$ is the direct product of $\mathcal{T}^*$, which is a cyclic group of order $p^r - 1$, and the group of principal units $\mathbb{P}$, which is elementary abelian of order p^r. Consequently, $2 \in \mathcal{T}^*$ if and only if $2^{p^r-1} \equiv 1 \pmod{p^2}$. Since 2 is an element of $\mathbb{Z}_{p^2} = \mathrm{GR}(p^2, 1)$, which is a subring of $\mathrm{GR}(p^2, r)$, we can reduce this condition to $2^{p-1} \equiv 1 \pmod{p^2}$.

On the other hand, the equation $\mathcal{T}_N^* = 2\mathcal{T}_Q^*$ holds if and only if $2 \in \mathcal{T}_N^*$. The second statement now follows from Proposition 3.18 (c) by analogous reasoning as above. □

A prime p solving the congruence $2^{p-1} \equiv 1 \pmod{p^2}$ from Lemma 3.20 is called a *Wieferich prime.* So far, the only known Wieferich primes are 1093 and 3511; we refer to Crandall, Dilcher, and Pomerance [42], Knauer and Richstein [80], and Dorais and Klyve [54] for some background on the search for more Wieferich primes. Thus, the only known Galois rings of characteristic p^2 with $\mathcal{T}_Q^* = 2\mathcal{T}_Q^*$ are $\mathrm{GR}(1093^2, r)$, where r is even, and $\mathrm{GR}(3511^2, r)$ for arbitrary r. The only known Galois ring of characteristic p^2 where $\mathcal{T}_N^* = 2\mathcal{T}_Q^*$ is $\mathrm{GR}(1093^2, r)$, where r is odd.

With the help of Proposition 3.18 (a), we now establish a lower bound on the multiplicities of certain elements in $\Delta\mathcal{T}_Q^*$ and $\mathcal{T}_Q^* - \mathcal{T}_N^*$. The proof follows the same approach as in Lemma 3.11.

Lemma 3.21. *Consider the Galois ring* $\mathrm{GR}(p^2, r)$*, where p is odd.*

- *If $p^r - 1 \equiv 0 \pmod 4$, then every $d \in \Delta\mathcal{T}_Q^*$ with $d \notin 2\mathcal{T}_Q^*$ has even multiplicity at least* 2.
- *If $p^r - 1 \equiv 2 \pmod 4$, then every $d \in \mathcal{T}_Q^* - \mathcal{T}_N^*$ with $d \notin 2\mathcal{T}_Q^*$ has even multiplicity at least* 2.

Proof. We prove the first result. The second statement can be shown analogously. Let p be a prime, and let r be a positive integer such that $p^r - 1 \equiv 0 \pmod 4$. Moreover, let $d \in \Delta\mathcal{T}_Q^*$, which means there exist distinct $s, s' \in \mathcal{T}_Q^*$ such that $d = s - s'$. According to Proposition 3.18 (a), $\mathcal{T}_Q^* = -\mathcal{T}_Q^*$. Hence, if $s' \neq s$, then $(-s') - (-s) = d$ is a second representation of d in $\Delta\mathcal{T}_Q^*$. If $s' = -s$, however, the two representations are the same, and $d = 2s$, thus $d \in 2\mathcal{T}_Q^*$. By the same reasoning as in the proof of Lemma 3.11, there might be pairs of elements $s_1, s_1', s_2, s_2', \ldots, s_\ell, s_\ell' \in \mathcal{T}_Q^*$ such that $s_i - s_i' = -s_i' - (-s_i) = d$ for all $i \in \{1, 2, \ldots, \ell\}$, but all these differences occur in pairs. □

In Lemma 3.22, we establish an upper bound on the multiplicity of certain differences in $\Delta\mathcal{T}_Q^*$ and $\mathcal{T}_Q^* - \mathcal{T}_N^*$. For our main theorem of this section, only the first part of the lemma is relevant. However, we also state the second part as it is easily obtained from the previous results.

Lemma 3.22. *Let p be an odd prime such that $2^{p-1} \not\equiv 1 \pmod{p^2}$. Consider the Galois ring* $\mathrm{GR}(p^2, r)$.

- *If $p^r - 1 \equiv 0 \pmod{24}$, then every square $d \in \Delta\mathcal{T}_Q^*$ occurs with multiplicity less than $\frac{p^r-5}{4}$.*

- *If* $p^r - 1 \equiv 18 \pmod{24}$*, then every* $d \in \mathcal{T}_Q^* - \mathcal{T}_N^*$ *occurs with multiplicity less than* $\frac{p^r+1}{4}$*.*

Proof. The condition $2^{p-1} \not\equiv 1 \pmod{p^2}$ guarantees that $\mathcal{T}_Q^* \neq 2\mathcal{T}_Q^*$ and $\mathcal{T}_N^* \neq 2\mathcal{T}_Q^*$ as shown in Lemma 3.20. Assume $p^r - 1 \equiv 0 \pmod{24}$. Let d be a square in $\Delta\mathcal{T}_Q^*$, and denote its multiplicity by N_d. From Lemma 3.17, we know that $\Delta\mathcal{T}_Q^*$ contains $\frac{p^r-5}{4}$ not necessarily distinct square cosets of $\mathcal{T}_Q^*$. It follows that $N_d \leq \frac{p^r-5}{4}$, and $N_d = \frac{p^r-5}{4}$ if and only if $\Delta\mathcal{T}_Q^*$ contains exactly one square coset of $\mathcal{T}_Q^*$ with multiplicity $\frac{p^r-5}{4}$. Assume $N_d = \frac{p^r-5}{4}$. As $p^r - 1 \equiv 0 \pmod{24}$, according to Corollary 3.19, both $\mathcal{T}_Q^*, 2\mathcal{T}_Q^* \subseteq \Delta\mathcal{T}_Q^*$, and $2\mathcal{T}_Q^*$ is a square coset of $\mathcal{T}_Q^*$. This is a contradiction.

Now, assume $p^r - 1 \equiv 18 \pmod{24}$. Let d be a non-square in $\mathcal{T}_Q^* - \mathcal{T}_N^*$, and denote its multiplicity by N_d. Analogously to above, we conclude from Lemma 3.17 that $N_d \leq \frac{p^r+1}{4}$, and $N_d = \frac{p^r+1}{4}$ if and only if $\mathcal{T}_Q^* - \mathcal{T}_N^*$ contains only exactly one non-square coset of $\mathcal{T}_Q^*$. Assume $N_d = \frac{p^r+1}{4}$. If $p^r - 1 \equiv 18 \pmod{24}$, then both $\mathcal{T}_N^*$ and $2\mathcal{T}_Q^*$ are contained in $\mathcal{T}_Q^* - \mathcal{T}_N^*$, and $2\mathcal{T}_Q^*$ is a non-square coset of $\mathcal{T}_Q^*$. Again, we obtain a contradiction. □

As we have mentioned in Remark 3.2, the multiplicity of a difference $d \in \Delta\mathcal{T}_Q^*$ corresponds directly to the block intersection number $|\mathcal{T}_Q^* \cap (\mathcal{T}_Q^* \cap d)|$. Hence, we obtain from the previous lemmas the following result, which partially solves the isomorphism problem for the difference families C^H and D^H.

Theorem 3.23. *Let p be an odd prime such that $2^{p-1} \not\equiv 1 \pmod{p^2}$. Let C^H be a $(p^{2r}, \frac{p^r-1}{2}, \frac{p^r-3}{2})$ disjoint difference family in the additive group of the finite field $\mathbb{F}_{p^{2r}}$ constructed with Theorem 2.4, and let D^H be a disjoint difference family with the same parameters in the additive group of the Galois ring $\mathrm{GR}(p^2, r)$ constructed with Theorem 2.7. If $p^r - 1 \equiv 0 \pmod{24}$, then C^H and D^H are nonisomorphic.*

Proof. Let p be an odd prime, and let r be an integer such that $p^r - 1 \equiv 0 \pmod{24}$. Recall from Proposition 3.16 that, in this case, the block intersection numbers of the design $\mathcal{C}^H$ are $0, 1, \frac{p^r-5}{4}, \frac{p^r-1}{4}$. Now, consider the Galois ring $\mathrm{GR}(p^2, r)$, and denote by $\mathcal{T}_Q^*$ the set of Teichmüller squares. By combining Lemma 3.21 and Lemma 3.22, we obtain

$$1 < |\mathcal{T}_Q^* \cap (\mathcal{T}_Q^* + d)| < \frac{p^r-5}{4}$$

for all squares $d \in \Delta\mathcal{T}_Q^* \backslash 2\mathcal{T}_Q^*$. Note that it follows from Corollary 3.19 and Lemma 3.20 that $\mathcal{T}_Q^* \subseteq \Delta\mathcal{T}_Q^*$ and $\mathcal{T}_Q^* \neq 2\mathcal{T}_Q^*$. Hence, such a square d always exists. Consequently, the design $\mathcal{D}^H$ has an intersection number different from the intersection numbers of $\mathcal{C}^H$, and the designs are nonisomorphic. □

We remark that the condition $p^r - 1 \equiv 0 \pmod{24}$ from Theorem 3.23 is not as restrictive as it sounds since it holds for all p and r where $p \geq 5$ and r is even.

Furthermore, we note that Theorem 3.23 also holds for the Wieferich primes 1093 and 3511, which satisfy the condition $2^{p-1} \equiv 1 \pmod{p^2}$. For both primes, we used `Magma` [16] to compute $\Delta\mathcal{T}_Q^*$ in the case $r = 1$, and we confirmed that $\Delta\mathcal{T}_Q^*$ contains more than one square coset of $\mathcal{T}_Q^*$. Hence, there are at least as many square cosets of $\mathcal{T}_Q^*$ in $\Delta\mathcal{T}_Q^*$ for $r > 1$, and, if $p^r - 1 \equiv 0 \pmod{24}$, which means for even r, the bound established in the previous proof holds.

To conclude this section, we demonstrate in Example 3.6 why our intersection number approach fails if $p^r - 1 \not\equiv 0 \pmod{24}$. We choose the case $p^r - 1 \equiv 18 \pmod{24}$ since, in the previous lemmas, we already obtained several results about this case, which followed immediately from the results for $p^r - 1 \not\equiv 0 \pmod{24}$.

Example 3.6. Let p and r such that $p^r - 1 \equiv 18 \pmod{24}$. In this case, according to Proposition 3.16, the block intersection numbers of the design $\mathcal{C}^H$ are 0, 1, $\frac{p^r-3}{4}$, $\frac{p^r+1}{4}$. For the design $\mathcal{D}^H$, using Lemma 3.21 and Lemma 3.22, we obtain

$$1 < |\mathcal{T}_Q^* \cap (\mathcal{T}_N^* + d)| < \tfrac{p^r+1}{4}$$

for all $d \in (\mathcal{T}_Q^* - \mathcal{T}_N^*) \setminus 2\mathcal{T}_Q^*$. However, this result is of little use as it is still possible that there exists some $d \in (\mathcal{T}_Q^* - \mathcal{T}_N^*) \setminus 2\mathcal{T}_Q^*$ such that $|\mathcal{T}_Q^* \cap (\mathcal{T}_N^* + d)| = \frac{p^r-3}{4}$, or that two completely different blocks intersect in $\frac{p^r+1}{4}$ elements. In fact, the multiset $p\mathcal{T}_Q^* - p\mathcal{T}_N^*$ contains the sets $p\mathcal{T}_N^*$ and $p\mathcal{T}_Q^*$ with multiplicities $\frac{p^r+1}{4}$ and $\frac{p^r-3}{4}$, respectively. Hence, these two numbers actually occur as the block intersection numbers

$$|p\mathcal{T}_Q^* \cap (p\mathcal{T}_N^* + d)|,$$

where $d \in \mathcal{I} \setminus \{0\}$. Consequently, with our approach, we cannot show the existence of an intersection number N such that $1 < N < \frac{p^r-3}{4}$.

3.4 Isomorphism problem III: Wilson vs. Momihara

In this section, we solve the isomorphism problem for Wilson's [102] difference families in finite fields from Theorem 2.4 and Momihara's [84] difference families in Galois rings from Theorem 2.8. We show that these difference families are always nonisomorphic.

Recall from Theorem 2.8 that Momihara's [84] difference families only exist in Galois rings of characteristic p^2 with even extension degree. Hence, throughout this section, we consider the finite field $\mathbb{F}_{p^{4n}}$ and the Galois ring $\mathrm{GR}(p^2, 2n)$, where p is a prime and n is a positive integer. Using the same notations as in the previous sections, we denote by C the $\big(p^{4n}, p^{3n} - p^{2n} + p^n - 1, p^{3n} - p^{2n} + p^n - 2\big)$ disjoint difference family in the additive group of $\mathbb{F}_{p^{4n}}$ and by D the disjoint difference family with the same parameters in the additive group of $\mathrm{GR}(p^2, 2n)$. Moreover, let $\mathcal{C} = \mathrm{dev}(C)$ and $\mathcal{D} = \mathrm{dev}(D)$.

To show that C and D are nonisomorphic, we study the block intersection numbers of the associated designs $\mathcal{C}$ and $\mathcal{D}$. The following example demonstrates that these numbers apparently distinguish the designs.

Example 3.7. From Theorem 2.4 and Theorem 2.8, we obtain $(2401, 300, 299)$ disjoint difference families C and D in the additive groups of $\mathbb{F}_{7^4}$ and $\mathrm{GR}(49, 2)$, respectively. The associated 2-$(2401, 300, 299)$ designs have the following intersection numbers: for $\mathcal{C}$, they are $0, 5, 36, 42$ with multiplicities 67 228, 2 881 200, 121 010 400, and 60 505 200, respectively. For $\mathcal{D}$, they are $0, 5, 32, 36, 40, 42, 65$ with multiplicities 67 228, 57 624, 50 824 368, 36 303 120, 84 707 280, 9 680 832, and 2 823 576, respectively. Hence, the difference families are nonisomorphic.

We first determine the block intersection numbers of $\mathcal{C}$, as shown in Proposition 3.1, by calculating the cyclotomic numbers of order p^n+1 in $\mathbb{F}_{p^{4n}}$. Since these cyclotomic numbers are uniform, we can directly use Proposition 3.2.

Proposition 3.24. *The* 2-$(p^{4n}, p^{3n}-p^{2n}+p^n-1, p^{3n}-p^{2n}+p^n-2)$ *design* $\mathcal{C}$ *has precisely the block intersection numbers* 0, p^n-2, $p^{2n}-2p^n+1$ *and* $p^{2n}-p^n$. *These intersection numbers occur with the following multiplicities:*

$$\begin{aligned} n(0) &= \tfrac{1}{2}(p^{6n}+p^{5n}), \\ n(p^n-2) &= \tfrac{1}{2}(p^{8n}-p^{4n}), \\ n(p^{2n}-2p^n+1) &= \tfrac{1}{2}(p^{10n}-p^{9n}-p^{6n}+p^{5n}), \\ n(p^{2n}-p^n) &= \tfrac{1}{2}(3p^{9n}-3p^{5n}). \end{aligned} \tag{3.12}$$

Proof. The difference family C consists of the subgroup of the (p^n+1)-th powers of $\mathbb{F}^*_{p^{4n}}$ and all its cosets. We show that C meets the conditions of Proposition 3.2. Using the notation from Proposition 3.2, $e = p^n+1$, so $-1 \equiv p^n \pmod{p^n+1}$. Moreover, from $p^{4n} = s^2$, it follows that $s = p^{2n} \equiv 1 \pmod{p^n+1}$. Consequently, $\eta = \frac{p^{2n}-1}{p^n+1} = p^n-1$. We now use (3.3) to obtain the cyclotomic numbers

$$\begin{aligned} (0,0)_{p^n+1} &= p^n-2, && \\ (0,i)_{p^n+1} = (i,0)_{p^n+1} = (i,i)_{p^n+1} &= p^n(p^n-1) && \text{for } i \neq 0, \\ (i,j)_{p^n+1} &= (p^n-1)^2 && \text{for } i \neq j \text{ and } i,j \neq 0, \end{aligned} \tag{3.13}$$

that occur as intersection numbers of $\mathcal{C}$. Additionally, according to Proposition 3.1, 0 is an intersection number of $\mathcal{C}$ since the base blocks of C are disjoint.

We next determine the multiplicities of these intersection numbers. Denote by $n_{p^n+1}(N)$ the number of cyclotomic numbers of order p^n+1 in $\mathbb{F}_{p^{4n}}$ that equal N. Counting the numbers in (3.13), we obtain

$$\begin{aligned} n_{p^n+1}(0) &= 0, \\ n_{p^n+1}(p^n-2) &= 1, \\ n_{p^n+1}(p^{2n}-2p^n+1) &= p^n(p^n-1), \\ n_{p^n+1}(p^{2n}-p^n) &= 3p^n. \end{aligned} \tag{3.14}$$

The multiplicities of the block intersection numbers of $\mathcal{C}$ can now be obtained by combining (3.14) with Proposition 3.1. □

To examine the intersection numbers of the design $\mathcal{D}$, we need some preparatory work. First, we present a result about $\Delta\mathrm{GR}(p^2,r)^*$.

Lemma 3.25. *For any Galois ring* $\mathrm{GR}(p^2,r)$*, the multiset* $\Delta\mathrm{GR}(p^2,r)^*$ *contains every nonzero element of* $\mathcal{I}$ *with multiplicity* $p^{2r}-p^r$ *and every element of* $\mathrm{GR}(p^2,r)^*$ *with multiplicity* $p^{2r}-2p^r$*.*

Proof. Let $u,u' \in \mathrm{GR}(p^2,r)^*$, and write $u=\alpha_0+p\alpha_1$ and $u'=\alpha_0'+p\alpha_1'$ for unique $\alpha_0,\alpha_0' \in \mathcal{T}^*$ and $\alpha_1,\alpha_1' \in \mathcal{T}$. In Lemma 3.5, we showed that $u-u'$ is not invertible if and only if $\alpha_0=\alpha_0'$. Consequently, there are $(p^r-1)p^{2r}$ ways to choose $\alpha_0,\alpha_0',\alpha_1,\alpha_1'$ such that $u-u' \in \mathcal{I}$. By similar reasoning as in the proof of Theorem 2.4, these differences are evenly distributed. As $|\mathcal{I}\setminus\{0\}|=p^r-1$, every nonzero element of $\mathcal{I}$ has multiplicity $p^{2r}-p^r$ in $\Delta\mathrm{GR}(p^2,r)^*$. Analogously, there are $(p^r-1)(p^r-2)p^{2r}$ ways to choose $\alpha_0,\alpha_0',\alpha_1,\alpha_1'$ such that $u-u' \in \mathrm{GR}(p^2,r)^*$. As these differences are evenly distributed again and $|\mathrm{GR}(p^2,r)^*|=p^r(p^r-1)$, every unit of $\mathrm{GR}(p^2,r)$ occurs with multiplicity $p^{2r}-2p^r$ in $\Delta\mathrm{GR}(p^2,r)^*$. □

As in Theorem 2.8, denote $R_{2n}=\mathrm{GR}(p^2,2n)$ and $R_n=\mathrm{GR}(p^2,n)$, and use the subscripts $2n$ and n also for the respective subsets of these rings. Let ξ be a generator of the Teichmüller group $\mathcal{T}_{2n}^*$, and let $S=\{\alpha_0,\alpha_1,\ldots,\alpha_{p^n-1}\}$ such that $1+pS$ is a system of representatives of $\mathbb{P}_{2n}/\mathbb{P}_n$, where $\mathbb{P}_{2n}$ and $\mathbb{P}_n$ are the groups of principal units of R_{2n} and R_n, respectively. Define

$$P=\{p\xi^{p^n},p\xi^{(p^n+1)+p^n},p\xi^{2(p^n+1)+p^n},\ldots,p\xi^{(p^n-2)(p^n+1)+p^n}\}.$$

Furthermore, define subsets U and V of R_{2n}^* as

$$U=\bigcup_{j=0}^{p^n-1}\xi^j(1+p\alpha_j)R_n^* \qquad \text{and} \qquad V=\bigcup_{j=0}^{p^n-1}(1+p\alpha_j)R_n^*. \tag{3.15}$$

Note that for every base block D_i of D, we have $D_i=\xi^i(P\cup U)$. Moreover, V is the direct product of $\mathcal{T}_n^*$ and $\mathbb{P}_{2n}$, and $\bigcup_{i=0}^{p^n}\xi^iV=R_{2n}^*$. We additionally need the following helpful lemmas.

Lemma 3.26. *In* R_{2n}*, we have* $R_n^*=-R_n^*$ *and* $P=-P$*.*

Proof. First, suppose p is odd. Then Lemma 3.4 implies that $-1=\xi^{\frac{(p^n-1)(p^n+1)}{2}}$. As p^n-1 is even and $\mathcal{T}_n^*=\{\xi^{i(p^n+1)}:i=0,1,\ldots,p^n-2\}$, clearly $-1\in\mathcal{T}_n^*$. The results now follow from considering that $\mathcal{T}_n^*\subseteq R_n^*$ and rewriting P as $P=p\xi^{p^n}\mathcal{T}_n^*$.

Now, assume $p=2$. According to Lemma 3.4, now $-1\in\mathbb{P}_{2n}$. Note that $-1\equiv 3 \pmod 4$. Since we can write $3=1\cdot(1+2\cdot 1)$ and $1\in\mathcal{T}_n$, this implies $-1\in\mathbb{P}_n$. Therefore, $-1\in R_n^*$, which implies $R_n^*=-R_n^*$. Furthermore, from $\mathcal{I}_{2n}=2R_{2n}$ and $-2\equiv 2 \pmod 4$, it follows that $x=-x$ for all $x\in\mathcal{I}_{2n}$. As $P\subseteq\mathcal{I}_{2n}$, we have $-P=P$. □

For the proof of the following Lemma 3.27, we refer to Momihara [84].

Lemma 3.27 ([84, Lemma 3])**.** *Let $s \leq p^{2n}-2$ be a nonnegative integer, let $r \in R_{2n}$, and let V be as defined in (3.15). If $\xi^s(1+pr) \notin R_n$ and $\xi^s \notin \mathcal{T}_n$, then*

$$R_n^* + \xi^s(1+pr)R_n^* = R_{2n}^* \setminus (V \cup \xi^s V)\,.$$

We can now state the main theorem of this section. Since we have completely determined the block intersection numbers of $\mathcal{C}$ in Proposition 3.24, we can prove that $\mathcal{C}$ and $\mathcal{D}$ are nonisomorphic by showing that $\mathcal{D}$ has an intersection number different from the ones of $\mathcal{C}$. We remark that the proof of Theorem 3.28 has a similar structure as the proofs by Momihara [84, Lemmas 4–7], but unlike Momihara, we will not consider all the base blocks $D_0, D_1, \dots, D_b$ of the difference family D, but only D_0. Thus, our approach requires a more detailed analysis of the differences in ΔD_0.

Theorem 3.28. *Let C be a $\big(p^{4n}, p^{3n}-p^{2n}+p^n-1, p^{3n}-p^{2n}+p^n-2\big)$ disjoint difference family in the additive group of the finite field $\mathbb{F}_{p^{4n}}$ constructed with Theorem 2.4, and let D be a disjoint difference family with the same parameters in the additive group of the Galois ring $\mathrm{GR}(p^2, 2n)$ constructed with Theorem 2.8. Then C and D are nonisomorphic.*

Proof. For $p^n \geq 3$, we will prove Theorem 3.28 by showing that $\mathcal{D}$ has the block intersection number $|(D_0+u) \cap D_0| = 2p^{2n} - 5p^n + 2$ for all $u \in U$, where U is as defined in (3.15). The case $p = 2$ and $n = 1$ will be solved computationally.

Suppose $p^n \geq 3$. As pointed out in Remark 3.2, the statement $|(D_0+u) \cap D_0| = 2p^{2n} - 5p^n + 2$ for $u \in U$ is equivalent to the statement that every $u \in U$ occurs with multiplicity $(2p^n-1)(p^n-2)$ in the multiset ΔD_0. Regarding the structure of

$$D_0 = P \cup U = P \cup \left(\bigcup_{j=0}^{p^n-1} \xi^j (1+p\alpha_j) R_n^* \right),$$

we can divide the differences in ΔD_0 into four different types:

Type 1: $\xi^s(1+p\alpha_s)R_n^* - \xi^t(1+p\alpha_t)R_n^*$, where $s,t \in \{0,1,\dots,p^n-1\}$ and $s \neq t$,

Type 2: $\Delta\xi^s(1+p\alpha_s)R_n^*$, where $s \in \{0,1,\dots,p^n-1\}$,

Type 3: $\xi^s(1+p\alpha_s)R_n^* - P$, where $s \in \{0,1,\dots,p^n-1\}$,

Type 4: ΔP.

Note that it follows from Lemma 3.26 that $\xi^s(1+p\alpha_s)R_n^* - P = P - \xi^s(1+p\alpha_s)R_n^*$ for all $s \in \{0,1,\dots,p^n-1\}$. Hence, we summarize both these types of differences in *Type 3*.

From now on, fix $u \in U$. We determine the multiplicity of u in ΔD_0 by counting its occurrences in each of the four types of multisets defined above. We first show that u occurs with multiplicity $p^{2n} - 3p^n + 2$ in the union of all *Type 1* multisets and with multiplicity $p^{2n} - 2p^n$ in the union of all *Type 2* multisets. Afterwards, we prove that u does not occur in multisets of *Type 3* and *Type 4*.

We start our proof by addressing differences of *Type 1*. Fix $s, t \in \{0, 1, \dots, p^n - 1\}$ such that $s \neq t$. From Lemma 3.26, it follows that

$$\xi^s(1 + p\alpha_s)R_n^* - \xi^t(1 + p\alpha_t)R_n^* = \xi^s(1 + p\alpha_s)R_n^* + \xi^t(1 + p\alpha_t)R_n^*.$$

Factoring out $\xi^s(1 + p\alpha_s)$ gives

$$\xi^s(1 + p\alpha_s)(R_n^* + \xi^{t-s}(1 + p(\alpha_t - \alpha_s))R_n^*),$$

which, applying Lemma 3.27 and using the definition of V from (3.15), equals

$$\xi^s(1 + p\alpha_s)(R_{2n}^* \setminus (V \cup \xi^{t-s}V)).$$

Since $(1 + pr)V = V$ for any $r \in R_{2n}$, we may omit $(1 + p\alpha_s)$ and write a *Type 1* multiset in the form

$$\xi^s(1 + p\alpha_s)R_n^* - \xi^t(1 + p\alpha_t)R_n^* = R_{2n}^* \setminus (\xi^s V \cup \xi^t V). \tag{3.16}$$

Now, we count differences. The set D_0 contains p^n distinct subsets $\xi^s(1 + p\alpha_s)R_n^*$. Consequently, ΔD_0 contains $p^n(p^n - 1)$ *Type 1* multisets. Recall that $\bigcup_{i=0}^{p^n} \xi^i V = R_{2n}^*$. Since $s, t \leq p^n - 1$, according to (3.16), every *Type 1* multiset contains the set $\xi^{p^n}V$, whereas any element of $\bigcup_{j=0}^{p^n-1} \xi^j V = R_{2n}^* \setminus \xi^{p^n}V$ occurs only in $(p^n - 1)(p^n - 2)$ *Type 1* multisets. Since $U \subseteq R_{2n}^* \setminus \xi^{p^n}V$, we count, $p^{2n} - 3p^n + 2$ occurrences of u in ΔD_0 coming from *Type 1* multisets.

Next, we study differences of *Type 2*: $\Delta\xi^s(1 + p\alpha_s)R_n^*$. Note that

$$\Delta\xi^s(1 + p\alpha_s)R_n^* = \xi^s(1 + p\alpha_s)\Delta R_n^*.$$

It follows from Lemma 3.25 that $\xi^s(1 + p\alpha_s)\Delta R_n^*$ contains $p^{2n} - p^n$ copies of $\mathcal{I}_n$ and $p^{2n} - 2p^n$ copies of $\xi^s(1 + p\alpha_s)R_n^*$. By (3.15), $u \in \xi^s(1 + p\alpha_s)R_n^*$ for some $s \in \{0, 1, \dots, p^n - 1\}$. Hence, u occurs $p^{2n} - 2p^n$ times in ΔD_0 as a difference of *Type 2*.

Now, we examine differences of *Type 3*: $\xi^s(1 + p\alpha_s)R_n^* - P$. First, we take arbitrary elements $\xi^{k(p^n+1)}(1 + p\beta) \in R_n^*$, where $k \in \{0, 1, \dots, p^n - 2\}$ and $\beta \in \mathcal{T}_n$, and $-p\xi^{\ell(p^n+1)+p^n} \in P$, where $\ell \in \{0, 1, \dots, p^n - 2\}$. Recall from Lemma 3.26 that $P = -P$. Moreover, fix $s \in \{0, 1, \dots, p^n - 1\}$. We study

$$\xi^s(1 + p\alpha_s)\xi^{k(p^n+1)}(1 + p\beta) + p\xi^{\ell(p^n+1)+p^n}.$$

Factoring out $\xi^{s+k(p^n+1)}$ and summarizing, we obtain

$$\xi^{s+k(p^n+1)}(1 + p\alpha_s)(1 + p\beta)(1 + p\xi^{(\ell-k)(p^n+1)+p^n-s}). \tag{3.17}$$

Writing (3.17) with respect to all $0 \leq k, \ell \leq p^n - 2$ and all $\beta \in \mathcal{T}_n$, gives

$$\xi^s(1 + p\alpha_s)\mathcal{T}_n^*\mathbb{P}_n(1 + p\xi^{p^n-s}\mathcal{T}_n^*). \tag{3.18}$$

Note that $1 + p\xi^{p^n-s}\mathcal{T}_n^* \subseteq \mathbb{P}_{2n}$ and $|1 + p\xi^{p^n-s}\mathcal{T}_n^*| = p^n - 1$. Since $\xi^{p^n-s} \notin \mathcal{T}_n$, it is clear that the sets $\mathbb{P}_n = 1 + p\mathcal{T}_n$ and $1 + p\xi^{p^n-s}\mathcal{T}_n^*$ are disjoint. We show that from each of the $p^n - 1$ other cosets in $\mathbb{P}_{2n}/\mathbb{P}_n$ exactly one element is contained in $1 + p\xi^{p^n-s}\mathcal{T}_n^*$. This is equivalent to showing that $p\xi^{p^n-s}\mathcal{T}_n$ contains exactly one element of every coset in $\mathcal{I}_{2n}/\mathcal{I}_n$, except for $\mathcal{I}_n = p\mathcal{T}_n^*$ itself. By way of contradiction, suppose $p\xi^{p^n-s}\mathcal{T}_n^*$ contains two distinct elements x, x' of the same coset in $\mathcal{I}_{2n}/\mathcal{I}_n$. Then $x - x'$ is an element of $\mathcal{I}_n$. However, for two distinct integers k, ℓ, the difference

$$p\xi^{p^n-s+k(p^n+1)} - p\xi^{p^n-s+\ell(p^n+1)} = \xi^{p^n-s}(p\xi^{k(p^n+1)} - p\xi^{\ell(p^n+1)})$$

is not contained in $\mathcal{I}_n$ since $\xi^{p^n-s} \notin \mathcal{T}_n$ and $p\xi^{k(p^n+1)} - p\xi^{\ell(p^n+1)} \in \mathcal{I}_n$. This is a contradiction.

Consequently, (3.18) equals

$$\xi^s(1 + p\alpha_s)\mathcal{T}_n^* \left(\mathbb{P}_{2n} \setminus \mathbb{P}_n\right).$$

Hence, with the definition of V from (3.15), we can write a *Type 3* multiset as

$$\xi^s(1 + p\alpha_s)R_n^* - P = \xi^s \left(V \setminus (1 + p\alpha_s)R_n^*\right).$$

Recall from (3.15) that $U = \bigcup_{j=0}^{p^n-1} \xi^j(1 + p\alpha_j)R_n^*$. Hence, $u \in U$ does not occur in multisets of *Type 3*.

Eventually, we examine differences of *Type 4*: ΔP. As $P \subseteq \mathcal{I}_{2n}$, it follows that $\Delta P \subseteq \Delta\mathcal{I}_{2n}$. Hence, ΔP contains no units and, thus, provides no representations of u.

Consequently, $|(D_0 + u) \cap D_0| = (p^{2n} - 3p^n + 2) + (p^{2n} - 2p^n) = 2p^{2n} - 5p^n + 2$. For $p^n \geq 3$, this number does not equal any of the block intersection numbers 0, $p^n - 2$, $p^{2n} - 2p^n + 1$ and $p^{2n} - p^n$ of $\mathcal{C}$ from Proposition 3.24. We conclude that C and D are nonisomorphic if $p^n \geq 3$.

In the case $p = 2$ and $n = 1$, however, $|(D_0+u)\cap D_0| = 0$, and the block intersection numbers of $\mathcal{D}$ and their multiplicities match those of $\mathcal{C}$: both 2-$(16, 5, 4)$ designs have the intersection numbers 0, 1 and 2 with multiplicities 168, 240 and 720, respectively. To complete our proof, we computed the full automorphism groups $\mathrm{Aut}(\mathcal{C})$ and $\mathrm{Aut}(\mathcal{D})$ of $\mathcal{C}$ and $\mathcal{D}$, respectively, using `Magma` [16]. We obtained $|\mathrm{Aut}(\mathcal{C})| = 960$ and $|\mathrm{Aut}(\mathcal{D})| = 192$. Hence, C and D are also nonisomorphic if $p = 2$ and $n = 1$. □

As we only needed to calculate the block intersection number $2p^{2n} - 5p^n + 2$ of $\mathcal{D}$ to prove Theorem 3.28, we did not try to determine additional block intersection numbers of this design. However, unlike for the difference families from Theorem 2.6 and Theorem 2.7, our computations show that for the difference families from Theorem 2.8, the block intersection numbers appear to be very structured. From our computational results with Magma [16], we conjecture that $\mathcal{D}$ has the block intersection numbers listed in the following remark. We leave the task to theoretically confirm these results to future work. To tackle this problem, it seems promising to follow an approach similar to the proof of Theorem 3.28.

Remark 3.5. We conjecture that $\mathcal{D}$ has precisely the seven block intersection numbers 0, p^n-2, $p^{2n}-3p^n+4$, $p^{2n}-2p^n+1$, $p^{2n}-2p^n+5$, $p^{2n}-p^n$ and $2p^{2n}-5p^n+2$. Moreover, we conjecture that these intersection numbers have the following multiplicities:

$$\begin{aligned} n(0) &= \tfrac{1}{2}(p^{6n}+p^{5n}), \\ n(p^n-2) &= \tfrac{1}{2}(p^{6n}-p^{4n}), \\ n(p^{2n}-3p^n+4) &= \tfrac{1}{2}(3p^{9n}-3p^{8n}-3p^{7n}+3p^{6n}), \\ n(p^{2n}-2p^n+1) &= \tfrac{1}{2}(2p^{9n}-p^{8n}-3p^{7n}+p^{6n}+p^{5n}), \\ n(p^{2n}-2p^n+5) &= \tfrac{1}{2}(p^{10n}-3p^{9n}+p^{8n}+3p^{7n}-2p^{6n}), \\ n(p^{2n}-p^n) &= \tfrac{1}{2}(3p^{8n}+3p^{7n}-3p^{6n}-3p^{5n}), \\ n(2p^{2n}-5p^n+2) &= \tfrac{1}{2}(p^{8n}-p^{6n}). \end{aligned} \tag{3.19}$$

We have computationally confirmed that the above numbers are block intersection numbers of $\mathcal{D}$ for all p and n with $p^n \leq 97$, and we have confirmed that these numbers are all the block intersection numbers of $\mathcal{D}$ and that they occur with the multiplicities given in (3.19) for all p and n with $p^n \leq 9$.

Furthermore, we add an interesting observation about the connection between the multiplicities of the intersection numbers of $\mathcal{C}$ and $\mathcal{D}$. Recall the intersection numbers of $\mathcal{C}$ from Proposition 3.24. If we denote the multiplicity of an intersection number N of $\mathcal{C}$ by $n_{\mathcal{C}}(N)$ and the multiplicity of an intersection number N of $\mathcal{D}$ by $n_{\mathcal{D}}(N)$, then it follows from comparing (3.12) and (3.19) that

$$\begin{aligned} n_{\mathcal{C}}(0) &= n_{\mathcal{D}}(0), \\ n_{\mathcal{C}}(p^n-2) &= n_{\mathcal{D}}(p^n-2)+n_{\mathcal{D}}(2p^{2n}-5p^n+2), \\ n_{\mathcal{C}}(p^{2n}-2p^n+1) &= n_{\mathcal{D}}(p^{2n}-2p^n+1)+n_{\mathcal{D}}(p^{2n}-2p^n+5), \\ n_{\mathcal{C}}(p^{2n}-p^n) &= n_{\mathcal{D}}(p^{2n}-p^n)+n_{\mathcal{D}}(p^{2n}-3p^n+4). \end{aligned}$$

4 Almost perfect nonlinear functions

In this chapter, we introduce APN functions, and we give all the definitions and basic results needed for the presentation of our main results in Chapter 5. In Section 4.1, we introduce vectorial Boolean functions and, in particular, APN functions. In Section 4.2, we present the different notions of equivalence between vectorial Boolean functions, and we introduce some approaches to study them. Finally, in Section 4.3, we give an overview of the known classes of APN functions. In this section, we will also present the two classes of APN functions by Zhou and Pott [109] and by Taniguchi [100] that we will study extensively in Chapter 5.

4.1 Vectorial Boolean functions

Let $\mathbb{F}_2$ be the finite field with two elements, and denote by $\mathbb{F}_2^n$ the n-dimensional vector space over $\mathbb{F}_2$. A function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$ is called a *vectorial Boolean function* if $m \geq 2$ or simply a *Boolean function* if $m = 1$. In this thesis, we consider vectorial Boolean functions from $\mathbb{F}_2^n$ to $\mathbb{F}_2^n$, we say functions *on* $\mathbb{F}_2^n$. Note that we will regularly identify the vector space $\mathbb{F}_2^n$ over $\mathbb{F}_2$ with the finite field $\mathbb{F}_{2^n}$ with 2^n elements as this allows us to use the properties, operations, and notations of the finite field.

Vectorial Boolean functions can be represented in various ways: the most popular representations are the *univariate* and the *multivariate* description. If n is even, the *bivariate* description is another important representation. We describe all three representations.

Let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$. When we consider f as a function on $\mathbb{F}_{2^n}$, then f can be uniquely written as a univariate polynomial mapping

$$f(x) = \sum_{i=0}^{2^n-1} a_i x^i,$$

where $a_i \in \mathbb{F}_{2^n}$ for $i = 0, 1, \ldots, 2^n - 1$, of degree at most $2^n - 1$.

For the multivariate representation, we write f in the standard way to write mappings on vector spaces using n Boolean coordinate functions $f_1, \ldots, f_n\colon \mathbb{F}_2^n \to \mathbb{F}_2$, which is

$$f(x_1, \ldots, x_n) = \begin{pmatrix} f_1(x_1, \ldots, x_n) \\ \vdots \\ f_n(x_1, \ldots, x_n) \end{pmatrix}.$$

To obtain a unique multivariate representation, we need the *algebraic normal form* of f. This term was originally introduced for Boolean functions, but it can be easily extended to vectorial Boolean functions. If f is a Boolean function, $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$, then f has a unique representation as a multivariate polynomial mapping of the form

$$f(x_1, \dots, x_n) = \sum_{u \in \mathbb{F}_2^n} a_u \prod_{i=1}^{n} x_i^{u_i}, \tag{4.1}$$

where $a_u \in \mathbb{F}_2$ for all $u \in \mathbb{F}_2^n$. If every coordinate function $f_1, \dots, f_n\colon \mathbb{F}_2^n \to \mathbb{F}_2$ of a vectorial Boolean function f on $\mathbb{F}_2^n$ is given in its algebraic normal form, then we call this multivariate representation the algebraic normal form of f.

Now, assume n is even. Write $n = 2m$ for a positive integer m. We identify $\mathbb{F}_2^{2m}$ with the 2-dimensional vector space $\mathbb{F}_{2^m}^2$ over $\mathbb{F}_{2^m}$. For the bivariate description, we write f as a mapping on $\mathbb{F}_{2^m}^2$ defined by two functions $f_1, f_2\colon \mathbb{F}_{2^m}^2 \to \mathbb{F}_{2^m}$, which means

$$f(x, y) = (f_1(x, y), f_2(x, y)).$$

As f_1 and f_2 can be uniquely represented by a bivariate polynomial mapping

$$f_k(x, y) = \sum_{i,j=0}^{2^m-1} a_{k,i,j} x^i y^j,$$

where $k = 1, 2$ and $a_{k,i,j} \in \mathbb{F}_{2^m}$ for $k = 1, 2$ and $i, j = 0, 1, \dots, 2^m - 1$, we can also obtain a unique bivariate representation. Note that in order to switch between the different descriptions, the choice of a basis is relevant. Mesnager [83] gives an overview of how to get one representation from another one.

Example 4.1. In this thesis, we will often consider functions given in bivariate representation. One example is the function $f\colon \mathbb{F}_4^2 \to \mathbb{F}_4^2$ defined by

$$f(x, y) = (x^3 + \beta y^3,\ xy),$$

where β is primitive in $\mathbb{F}_4$. It is included in the class of APN functions we present in Theorem 4.6. The multivariate description of f as a function on the vector space $\mathbb{F}_2^4$ is given by its algebraic normal form

$$f(x_1, \dots, x_4) = \begin{pmatrix} x_3x_4 + x_3 + x_4 \\ x_1x_2 + x_1 + x_2 \\ x_1x_3 + x_2x_4 \\ x_1x_4 + x_2x_3 + x_2x_4 \end{pmatrix}.$$

Its univariate description as a function on $\mathbb{F}_{16}$ is

$$f(x) = \alpha x^{12} + \alpha^{14} x^9 + \alpha^8 x^8 + \alpha^9 x^6 + \alpha^5 x^5 + \alpha^{10} x^3 + \alpha^8 x^2 + \alpha x,$$

where α is primitive in $\mathbb{F}_{16}$. To compute this example, we chose standard bases and representations of finite fields implemented in `Magma` [16]: we constructed $\mathbb{F}_4$ as the splitting field of the irreducible polynomial $X^2 + X + 1 \in \mathbb{F}_2[X]$ and $\mathbb{F}_{16}$ as the splitting field of $X^4 + X + 1 \in \mathbb{F}_2[X]$.

If $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is given in its multivariate representation, and $v \in \mathbb{F}_2^n$ is nonzero, then we call the Boolean function $f_v\colon \mathbb{F}_2^n \to \mathbb{F}_2$ with

$$f_v(x) = \langle v, f(x)\rangle, \tag{4.2}$$

where $\langle\,,\rangle$ denotes a scalar product on $\mathbb{F}_2^n$, a *component function* of f. In univariate representation, we replace the scalar product on $\mathbb{F}_2^n$ with a scalar product on $\mathbb{F}_{2^n}$: the canonical choice is the *absolute trace function* $\mathrm{tr}\colon \mathbb{F}_{2^n} \to \mathbb{F}_2$ defined by

$$\mathrm{tr}(x) = x + x^2 + x^{2^2} + \cdots + x^{2^{n-1}}.$$

In this case, the component functions of $f\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are the mappings

$$f_a(x) = \mathrm{tr}(af(x))$$

for any nonzero $a \in \mathbb{F}_{2^n}$.

An important parameter of a vectorial Boolean function is its *algebraic degree*. We define this term for Boolean functions first. Let $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$ be a Boolean function given in its algebraic normal form; see (4.1). The degree of a monomial $x \mapsto \prod_{i=1}^n x_i^{u_i}$ is $u_1 + \cdots + u_n$, and the maximal degree of all monomials with a nonzero coefficient in (4.1) is called the algebraic degree of f. Now let f be a vectorial Boolean function on $\mathbb{F}_2^n$. We define the algebraic degree of f as the largest degree of all its coordinate functions in its algebraic normal form. We call a function of algebraic degree 2 *quadratic* and a function of algebraic degree 1 *affine*. If f is affine and has no constant term, we say f is *linear*. Note that the algebraic degree of a vectorial Boolean function must not be confused with the polynomial degree of its univariate description. Moreover, we remark that the algebraic degree of f is also the largest degree of all its component functions, which we described in (4.2).

We can also determine the algebraic degree of f from its univariate and its bivariate representation. For any nonnegative integer $s \le 2^{n-1}$, we define the *weight* $w(s)$ of s as the number of nonzero coefficients in its binary expansion $s = \sum_{j=0}^{n-1} s_j 2^j$, hence, $w(s) = \sum_{j=0}^{n-1} s_j$. If f is given in its univariate description $f(x) = \sum_{i=0}^{2^n-1} a_i x^i$, then the algebraic degree of f is

$$\max_{s:a_s \neq 0} w(s).$$

If f is given in its bivariate description with two coordinate functions $f_k(x,y) = \sum_{i,j=0}^{2^m-1} a_{k,i,j} x^i y^j$ for $k = 1,2$, then the algebraic degree of f_k is

$$\max_{(s,t):a_{s,t}\neq 0} (w(s) + w(t)),$$

and the algebraic degree of f is the largest degree of the coordinate functions.

All the APN functions we consider in this thesis are quadratic. If f is a quadratic function on $\mathbb{F}_2^n$, then its univariate representation on $\mathbb{F}_{2^n}$ is of the form

$$f(x) = \sum_{0 \le i < j \le n-1} a_{i,j} x^{2^i + 2^j} + \sum_{0 \le i \le n-1} b_i x^{2^i} + c,$$

where not all $a_{i,j} = 0$. If f is affine, then

$$f(x) = \sum_{i=0}^{n-1} b_i x^{2^i} + c,$$

where not all $b_i = 0$. If f is affine and $c = 0$, then f is linear.

Example 4.2. The function from Example 4.1 on $\mathbb{F}_2^4$ is quadratic as in its algebraic normal form, the coordinate functions have degree at most 2. The function $f(x) = x^3$ on $\mathbb{F}_{2^n}$ is quadratic for all n. Since $3 = 1 \cdot 2 + 1 \cdot 1$, we have $w(3) = 2$.

As mentioned above, functions on $\mathbb{F}_{2^n}$ are polynomial mappings. In this thesis, we often use *linearized polynomials.* Denote by $\mathbb{F}_{2^n}[X]$ the univariate polynomial ring over $\mathbb{F}_{2^n}$. A polynomial of the form

$$P(X) = \sum_{i \ge 0} a_i X^{2^i},$$

where not all $a_i = 0$, is called a linearized polynomial. Note that there is a one-to-one correspondence between linear functions on $\mathbb{F}_2^n$ and linearized polynomials in the factor ring $\mathbb{F}_{2^n}[X]/(X^{2^n} - X)$. In the same way as for univariate polynomials, we define a linearized polynomial in the multivariate polynomial ring $\mathbb{F}_{2^n}[X_1, \ldots, X_r]$ as a polynomial of the form

$$P(X_1, \ldots, X_r) = \sum_{j=1}^{r} \Big(\sum_{i \ge 0} a_{i,j} X_j^{2^i} \Big),$$

where not all $a_{i,j} = 0$.

Vectorial Boolean functions play an important role in cryptography. From a cryptographic view, one desirable property of a vectorial Boolean function is being as nonlinear as possible. There are mainly two important approaches to measure this nonlinearity: via the *differential uniformity* and via the *Walsh spectrum.*

For a function f on $\mathbb{F}_2^n$, we call the mapping

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

where $a \in \mathbb{F}_2^n$ is nonzero, a *differential mapping* or a *derivative* of f. It is easy to see that if f is linear, all the derivatives of f are 2^n-to-1; their image sets all have cardinality 1. Consequently, functions whose derivatives have a huge image set are, in some sense, the opposite of linear. This makes them appealing for cryptography.

We call a function f on $\mathbb{F}_2^n$ *differentially k-uniform* if the equation

$$f(x+a)+f(x)=b$$

has at most k solutions for any $b \in \mathbb{F}_2^n$ and any nonzero $a \in \mathbb{F}_2^n$. The multiset containing the number of solutions to the above equation for all a and b is called the *differential spectrum* of f. In Section 1.2, we have already pointed out why on $\mathbb{F}_2^n$, the derivative of any function f can never be a permutation. This means there are no differentially 1-uniform functions on $\mathbb{F}_2^n$. Hence, a vectorial Boolean function on $\mathbb{F}_2^n$ with optimal differential properties is differentially 2-uniform. We call such functions almost perfect nonlinear, and we recall their definition from Section 1.2.

Definition 4.3. A function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called *almost perfect nonlinear* or APN, in brief, if the equation

$$f(x+a)+f(x)=b$$

has exactly 0 or 2 solutions for all nonzero $a \in \mathbb{F}_2^n$ and all $b \in \mathbb{F}_2^n$.

There are several equivalent definitions of almost perfect nonlinearity, which are summarized in the work by Budaghyan [23]. We only restate one using the derivative here: a function f on $\mathbb{F}_2^n$ is APN if and only if for every nonzero $a \in \mathbb{F}_2^n$, its derivative $x \mapsto f(x+a)+f(x)$ is a 2-to-1 mapping or, equivalently, the image set of each derivative has cardinality 2^{n-1}.

As mentioned above, we will only consider quadratic APN functions in this thesis. Quadratic functions on $\mathbb{F}_2^n$ have the property that the mapping

$$x \mapsto f(x+a)+f(x)+f(a)+f(0) \tag{4.3}$$

is linear for all nonzero $a \in \mathbb{F}_2^n$. Hence, the problem to find the number of solutions to the equation $f(x+a)+f(x)=b$ for any $b \in \mathbb{F}_2^n$ reduces to checking the dimension of the kernel of the linear map in (4.3). If the dimension is 1, then we have 0 or 2 solutions. Consequently, if the dimension of the kernel is 1 for all nonzero $a \in \mathbb{F}_2^n$, then f is APN.

We have already shown in Example 1.2 that $f(x)=x^3$ is APN on $\mathbb{F}_{2^n}$ for all n. We will give an overview of the known APN functions in Section 4.3.

The second important nonlinearity parameter of a (vectorial) Boolean functions is its *Walsh spectrum*. For a Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$, the *Walsh transform* $\hat{f}$ is the integer valued function

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

where $\langle\,,\rangle$ denotes a scalar product on $\mathbb{F}_2^n$; for functions from $\mathbb{F}_{2^n}$ to $\mathbb{F}_2$, we may take the trace function again. The values $\hat{f}(u)$ are called the *Walsh coefficients* of f, and the set or sometimes the multiset

$$\mathcal{W}_f=\{\hat{f}(u) : u \in \mathbb{F}_2^n\}$$

of all Walsh coefficients is called the *Walsh spectrum* of f. We say that the set or the multiset of the absolute values of the Walsh coefficients is the *extended Walsh spectrum* of f. The Walsh coefficient $\hat{f}(u)$ is used to measure the distance of f and the affine functions $x \mapsto \langle u, x\rangle$ and $x \mapsto \langle u, x\rangle + 1$. Consequently, the Walsh spectrum indicates how well a Boolean function can be approximated by an affine function.

For a vectorial Boolean function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, the *Walsh spectrum* $\mathcal{W}_f$ of f is the union of the Walsh spectra of all the component functions of f, which means

$$\mathcal{W}_f = \bigcup_{v \in \mathbb{F}_2^n} \mathcal{W}_{f_v},$$

where $v \in \mathbb{F}_2^n$ is nonzero, and f_v is defined as in (4.2). As above, the *extended Walsh spectrum* contains the absolute values of the elements of $\mathcal{W}_f$. The *linearity* of f, which is important to measure the resistance of a vectorial Boolean function against linear cryptanalysis, is

$$\mathcal{L}(f) = \max_{W \in \mathcal{W}_f} |W|.$$

If f is a function from $\mathbb{F}_2^n$ to $\mathbb{F}_2^m$, it can be shown using Parseval's relation that $\mathcal{L}(f) \geq 2^{\frac{n}{2}}$. Functions achieving this lower bound with equality are called *bent.* We refer to Mesnager [83] for an extended overview of bent functions. Bent vectorial functions exist if and only if n is even and $m \leq \frac{n}{2}$. Consequently, functions on $\mathbb{F}_2^n$, in particular APN functions, cannot be bent. If f is a function on $\mathbb{F}_2^n$, then $\mathcal{L}(f) \geq 2^{\frac{n+1}{2}}$ as was shown by Sidel'nikov [96] and Chabaud and Vaudenay [38]. Functions for which equality holds are called *almost bent* or AB, in brief. They exist only if n is odd, and their Walsh spectrum $\mathcal{W}_f = \{0, \pm 2^{\frac{n+1}{2}}\}$ is called the *classical Walsh spectrum* for odd n. It is well known that any AB function is APN [38].

If n is even, AB functions do not exist, and the lowest possible linearity is unknown. For even n, we say that $\mathcal{W}_f = \{0, \pm 2^{\frac{n}{2}}, \pm 2^{\frac{n}{2}+1}\}$ is the *classical Walsh spectrum.* It is the Walsh spectrum of all known infinite families of quadratic APN functions on $\mathbb{F}_2^n$, where n is even. However, there are numerous examples of quadratic APN function with a non-classical Walsh spectrum; the first one was presented by Dillon [48] on $\mathbb{F}_2^6$. On $\mathbb{F}_2^8$, the currently known APN functions admit six different Walsh spectra, three of which were only recently found to be valid Walsh spectra of APN functions by Beierle and Leander [7].

4.2 Equivalence of vectorial Boolean functions

There are several important equivalence relations between vectorial Boolean functions that preserve the APN property. We list them in the following definition.

Definition 4.4. Two functions $f, g\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ are called

- *Carlet-Charpin-Zinoviev equivalent* (CCZ-equivalent) if there is an affine permutation C on $\mathbb{F}_2^n \times \mathbb{F}_2^n$ such that

$$C(G_f) = G_g,$$

where $G_f = \{(x, f(x)) : x \in \mathbb{F}_2^n\}$ denotes the graph of f,

- *extended affine equivalent* (EA-equivalent) if there exist three affine functions $A_1, A_2, A_3 \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$, where A_1 and A_2 are permutations, such that

$$f(A_1(x)) = A_2(g(x)) + A_3(x),$$

- *extended linearly equivalent* (EL-equivalent) if they are EA-equivalent and A_1, A_2, and A_3 are linear,
- *affine equivalent* if they are EA-equivalent and $A_3(x) = 0$,
- *linearly equivalent* if they are EL-equivalent and $A_3(x) = 0$.

In the case of EL- or linear equivalence, we usually write L, N, M instead of A_1, A_2, A_3 to underline that these functions are linear. CCZ-equivalence is the most general known equivalence relation of vectorial Boolean functions preserving the APN property. Obviously, linear equivalence implies affine equivalence, and affine equivalence implies EA-equivalence. Similarly, linear equivalence implies EL-equivalence, which, in turn, implies EA-equivalence. Moreover, it is well known that EA-equivalence implies CCZ-equivalence but, in general, the converse is not true as was shown by Budaghyan, Carlet, and Pott [27]. Note that the algebraic degree of a function is preserved under EA-equivalence, but this is, in general, not the case for CCZ-equivalence.

In most cases, solving equivalence problems of APN functions is a difficult task. For small values of n, we can check the equivalence of two functions computationally. This is usually done by using a connection of vectorial Boolean functions to coding theory and checking for code equivalence as proposed by Browning, Dillon, Kibler, and McQuistan [22] and Edel and Pott [60]. We refer to MacWilliams and Sloane [81] for more background on coding theory.

With any vectorial Boolean function f on $\mathbb{F}_2^n$, we can associate a linear code $\mathcal{C}_f$ with parity-check matrix

$$H_f = \begin{bmatrix} 1 \\ x \\ f(x) \end{bmatrix}_{x \in \mathbb{F}_2^n}.$$

This means

$$\mathcal{C}_f = \{v \in \mathbb{F}_2^n : H_f \cdot v = 0\}. \tag{4.4}$$

Two functions f and g are CCZ-equivalent if and only if their associated codes $\mathcal{C}_f$ and $\mathcal{C}_g$ are equivalent. So to investigate the equivalence of two functions, we simply compute the associated codes and use the built-in `Magma` [16] function to check for code equivalence. For EA- and affine equivalence, similar codes were introduced by

Edel and Pott [60]. To check for EA-equivalence, for instance, we need to consider the code $\mathcal{C}_f^{EA}$ with parity-check matrix

$$H_f^{EA} = \begin{bmatrix} 1 & 0 \\ x & 0 \\ f(x) & y \end{bmatrix}_{x\in\mathbb{F}_2^n,\ y\in\mathbb{F}_2^n\setminus\{0\}}.$$

While testing for code equivalence is an effective method to determine the equivalence of two functions on $\mathbb{F}_2^n$ for small values of n computationally, this approach becomes too resource consuming for larger n.

Hence, when studying whether two functions are equivalent or not, it makes sense to check some equivalence invariants first. Some useful invariants of vectorial Boolean functions under CCZ-equivalence are their extended Walsh spectrum, their Γ-rank, their Δ-rank, and the size of their automorphism group. Recently, Canteaut and Perrin [34] additionally presented a new EA-invariant for quadratic functions using so-called ortho-derivatives. We shortly introduce these invariants. Concerning the automorphism group, we will go into more detail since we will determine the automorphism group of several quadratic APN functions in Section 5.5.

We defined the extended Walsh spectrum in Section 4.1. Note that, in contrast to the extended Walsh spectrum, the Walsh spectrum is not invariant under CCZ-equivalence. As mentioned in Section 4.1, on $\mathbb{F}_2^n$ with n even, all currently known quadratic APN functions that are part of an infinite family share the classical Walsh spectrum. Consequently, these functions cannot be distinguished by their extended Walsh spectra.

The Γ- and the Δ-rank of a vectorial Boolean function make use of a connection between said functions and design theory; see Section 2.1 for a short introduction to combinatorial designs. We refer to Beth, Jungnickel, and Lenz [10] and Colbourn and Dinitz [41] for more background on this topic.

Definition 4.5. Let f be a function on $\mathbb{F}_2^n$. Denote by G_f the graph of f, which means

$$G_f = \{(x, f(x)) : x \in \mathbb{F}_2^n\},$$

and denote by D_f the set

$$D_f = \{(a, f(x+a) + f(x)) : x, a \in \mathbb{F}_2^n, a \neq 0\}.$$

We define the Γ-*rank* of f as the $\mathbb{F}_2$-rank of the incidence matrix of the development $\mathrm{dev}(G_f)$ of G_f, and we define the Δ-*rank* of f as the $\mathbb{F}_2$-rank of the incidence matrix of $\mathrm{dev}(D_f)$.

If f and g are CCZ-equivalent functions, then their associated incidence structures $\mathrm{dev}(G_f)$ and $\mathrm{dev}(G_g)$ are isomorphic, which implies that the Γ-ranks of f and g are equal. The same holds for $\mathrm{dev}(D_f)$ and $\mathrm{dev}(D_g)$ and the Δ-ranks of f and g. Note, however, that there exist many CCZ-inequivalent APN functions that have the same Γ-rank or the same Δ-rank. Moreover, it seems difficult to theoretically determine these ranks for a given function. Nevertheless, for small n, computing the Γ-rank or the Δ-rank of APN functions is an effective method to check for CCZ-inequivalence.

Remark 4.1. The incidence structures we describe in Definition 4.5 are, in general, no t-designs as defined in Definition 2.3. If f is an APN function, then $\operatorname{dev}(G_f)$ is a so-called semibiplane: any two points are contained in either none or in exactly two blocks, and any two blocks intersect in either none or in exactly two points. If f is an AB function, then $\operatorname{dev}(D_f)$ is a 2-design since, in this case, D_f is a Hadamard difference set; see Edel and Pott [59] for more details. If f is APN but not AB, then there may not be a nice characterization of $\operatorname{dev}(D_f)$.

The *ortho-derivative* of a quadratic APN function f on $\mathbb{F}_2^n$ is defined as the unique function $\Pi_f \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ with $\Pi_f(0) = 0$ such that for all nonzero $a \in \mathbb{F}_2^n$, the equation

$$\langle \Pi_f(a),\ f(x) + f(x+a) + f(a) + f(0) \rangle = 0$$

holds for all $x \in \mathbb{F}_2^n$. The differential spectrum and the extended Walsh spectrum of Π_f are invariant under EA-equivalence of f. Since for quadratic functions, CCZ-equivalence implies EA-equivalence, these invariants also indicate CCZ-equivalence. First results by Canteaut and Perrin [34] and Beierle and Leander [7] suggest that these invariants are easy to compute and strongly discriminate quadratic APN functions. They will not help for non-quadratic functions, though.

Before introducing automorphisms of vectorial Boolean functions, we characterize some of the mappings that define an equivalence of two functions in the sense of Definition 4.4 in more detail. Let f and g be functions on $\mathbb{F}_2^n$, and denote their graphs by G_f and G_g, respectively. We call an affine permutation C on $\mathbb{F}_2^n \times \mathbb{F}_2^n$ such that $C(G_f) = G_g$ a *CCZ-mapping* from g to f. Similarly to Canteaut and Perrin [33], we define an *EL-mapping* $C_{EL} = (L, M, N)$ from g to f as a linear CCZ-mapping from g to f satisfying

$$f(L(x)) = N(g(x)) + M(x),$$

where L, N are linear permutations and M is a linear map on $\mathbb{F}_2^n$. Such an EL-mapping C_{EL} from g to f may be represented as a formal matrix

$$C_{EL} = \begin{bmatrix} L & 0 \\ M & N \end{bmatrix}$$

corresponding to the calculation

$$\begin{bmatrix} L & 0 \\ M & N \end{bmatrix} \begin{bmatrix} x \\ g(x) \end{bmatrix} = \begin{bmatrix} L(x) \\ N(g(x)) + M(x) \end{bmatrix} = \begin{bmatrix} y \\ f(y) \end{bmatrix}.$$

Moreover, we define an *EA-mapping* $C_{EA} = (L, M, N, a, b)$ from g to f as a CCZ-mapping from g to f whose linear part is an EL-mapping. It is characterized by linear maps L, M, N as above and two elements $a, b \in \mathbb{F}_2^n$ such that

$$f(L(x) + a) = N(g(x)) + M(x) + b.$$

Now, an automorphism of f is an equivalence mapping from f to f, which is a mapping on $\mathbb{F}_2^n \times \mathbb{F}_2^n$ that preserves the graph of f.

Definition 4.6. For a function $f\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ with graph G_f, we call an affine permutation $\mathcal{A}$ on $\mathbb{F}_2^n \times \mathbb{F}_2^n$ with $\mathcal{A}(G_f) = G_f$ an *automorphism* of f. We denote the set of all such mappings by $\mathrm{Aut}(f)$. If $\mathcal{A}$ is an EA-mapping, we say that $\mathcal{A}$ is an *EA-automorphism* of f, and we denote the set of all EA-automorphisms by $\mathrm{Aut}_{EA}(f)$. Analogously, if $\mathcal{A}$ is an EL-mapping, we say that $\mathcal{A}$ is an *EL-automorphism* of f, and we denote the set of all EL-automorphisms by $\mathrm{Aut}_{EL}(f)$.

Note that $\mathrm{Aut}(f), \mathrm{Aut}_{EA}(f)$ and $\mathrm{Aut}_{EL}(f)$ each form a group under composition, see Canteaut and Perrin [33], and $\mathrm{Aut}_{EL}(f)$ is a subgroup of $\mathrm{Aut}_{EA}(f)$, which, in turn, is a subgroup of $\mathrm{Aut}(f)$. Hence, we simply call $\mathrm{Aut}(f)$ the *automorphism group* of f, and we call $\mathrm{Aut}_{EA}(f)$ and $\mathrm{Aut}_{EL}(f)$ the automorphism group of f under EA- or EL-equivalence, respectively.

To compute the automorphism group of a vectorial Boolean function, usually the aforementioned connection to coding theory is used: the automorphism group $\mathrm{Aut}(f)$ of f is isomorphic to the automorphism group of the code $\mathcal{C}_f$ from (4.4); for $\mathrm{Aut}_{EA}(f)$, we consider $\mathcal{C}_f^{EA}$ instead. For small values of n, the codes $\mathcal{C}_f$ and $\mathcal{C}_f^{EA}$ and their automorphism groups can be easily computed with `Magma` [16], and we may use the order of the respective automorphism group to check for CCZ- or EA-inequivalence. However, as for the Γ-rank and the Δ-rank, there are many inequivalent functions whose automorphism groups are of the same order. Furthermore, it is often difficult to theoretically determine the automorphism group of a given function.

Because of all their limitations, the aforementioned equivalence invariants may be useful to check the equivalence of particular examples of APN functions, but they will most certainly not help to determine the equivalence between all functions from an infinite family. In this thesis, we will use another approach to completely solve several CCZ-equivalence problems: we directly determine under which conditions there exists an equivalence mapping between given functions. While, at first, this approach might look like an uphill battle, we will see that the situation becomes easier to handle as all the functions we study are quadratic and have no constant term. First, there is the following result by Yoshiara [106].

Theorem 4.1 ([106, Theorem 1])**.** *Let f and g be quadratic APN functions on $\mathbb{F}_2^n$ with $n \geq 2$. Then f is CCZ-equivalent to g if and only if f is EA-equivalent to g.*

As it is much easier to study EA-equivalence than CCZ-equivalence, Theorem 4.1 is a very helpful result. For quadratic functions with no constant term, we can simplify the problem even more. In this case, two EA-equivalent functions are also EL-equivalent as we show in Proposition 4.2.[1]

[1] The present author was made aware of the result in Proposition 4.2 by one of the anonymous reviewers of [78].

Proposition 4.2. *Suppose f and g are EA-equivalent quadratic functions on $\mathbb{F}_2^n$ with $f(0) = g(0) = 0$, and denote by $C_{EA} = (L, M, N, a, b)$ an EA-mapping from g to f. Define a mapping $D_{f,L,a}$ on $\mathbb{F}_2^n$ as*

$$D_{f,L,a}(x) = f(L(x) + a) + f(L(x)) + f(a).$$

Then $b = f(a)$, the functions f and g are EL-equivalent, and C_{EA} uniquely defines an EL-mapping $C_{EL} = (L, \tilde{M}, N)$ from g to f, where $\tilde{M} = M + D_{f,L,a}$.

Proof. Recall from the definition of an EA-mapping that C_{EA} satisfies the equation

$$f(L(x) + a) = N(g(x)) + M(x) + b. \tag{4.5}$$

As f is quadratic and $f(0) = 0$, it is easy to confirm that the mapping $D_{f,L,a}$ is linear for $a \neq 0$ and zero for $a = 0$; see also (4.3). Combining (4.5) with the definition of $D_{f,L,a}$, we obtain

$$f(L(x)) = N(g(x)) + M(x) + D_{f,L,a}(x) + b + f(a).$$

As $f(0) = g(0) = 0$ and $L, N, M, D_{f,L,a}$ have no constant part either, it follows that $b = f(a)$. Hence,

$$f(L(x)) = N(g(x)) + M(x) + D_{f,L,a}(x).$$

Thus, f and g are EL-equivalent, and C_{EA} corresponds to an EL-mapping C_{EL} from g to f of the shape

$$\begin{bmatrix} L & 0 \\ M + D_{f,L,a} & N \end{bmatrix}$$

that is uniquely determined by C_{EA}. □

Thanks to Theorem 4.1 and Proposition 4.2, we can study the CCZ-equivalence of the functions in this thesis by restricting ourselves on their EL-equivalence. As many of the functions we deal with are given in bivariate description, we next present a general framework to study the EL-equivalence of such functions.

Two functions $f, g \colon \mathbb{F}_{2^m}^2 \to \mathbb{F}_{2^m}^2$ defined by

$$f(x, y) = (f_1(x, y), f_2(x, y)) \qquad \text{and} \qquad g(x, y) = (g_1(x, y), g_2(x, y))$$

for coordinate functions $f_1, f_2, g_1, g_2 \colon \mathbb{F}_{2^m}^2 \to \mathbb{F}_{2^m}$ are EL-equivalent, if there exist linear functions $L, N, M \colon \mathbb{F}_{2^m}^2 \to \mathbb{F}_{2^m}^2$, where L and N are bijective, such that

$$f(L(x, y)) = N(g(x, y)) + M(x, y).$$

Write

$$L(x, y) = (L_A(x, y), L_B(x, y)) \qquad \text{and} \qquad M(x, y) = (M_A(x, y), M_B(x, y))$$

for linear functions $L_A, L_B, M_A, M_B \colon \mathbb{F}_{2^m}^2 \to \mathbb{F}_{2^m}$ and

$$N(x,y) = (N_1(x) + N_3(y),\ N_2(x) + N_4(y))$$

for linear functions $N_1, \dots, N_4 \colon \mathbb{F}_{2^m} \to \mathbb{F}_{2^m}$. In terms of these newly defined functions, f and g are EL-equivalent if both

$$f_1(L_A(x,y), L_B(x,y)) = N_1(g_1(x,y)) + N_3(g_2(x,y)) + M_A(x,y), \tag{4.6}$$
$$f_2(L_A(x,y), L_B(x,y)) = N_2(g_1(x,y)) + N_4(g_2(x,y)) + M_B(x,y) \tag{4.7}$$

hold. They are linearly equivalent if $M(x,y) = 0$.

Equations (4.6) and (4.7) will form the framework in the proofs of our main results in Chapter 5. We will then regard L, M and N as linearized polynomials in the respective polynomial rings.

We close this section by showing that for a quadratic function f with no constant part, Proposition 4.2 allows us to establish a connection between the automorphism groups $\mathrm{Aut}_{EA}(f)$ and $\mathrm{Aut}_{EL}(f)$ of f under EA- and EL-equivalence. We need the definition of a semidirect product first. Let G be a group with identity element e. Let H and N be two subgroups of G. If N is normal, $G = NH$ and $N \cap H = \{e\}$, then we say G is a *semidirect product* of N and H and write

$$G = N \rtimes H.$$

Proposition 4.3 may be well known.[2] Edel and Pott [58] and Bracken, Byrne, McGuire, and Nebe [18] showed that the automorphism group of a quadratic function on $\mathbb{F}_2^n$ contains the additive group of $\mathbb{F}_{2^n}$.

Proposition 4.3. *Let f be a quadratic function on $\mathbb{F}_2^n$ with $f(0) = 0$. Then*

$$\mathrm{Aut}_{EA}(f) = T_f \rtimes \mathrm{Aut}_{EL}(f),$$

where T_f is isomorphic to the additive group $(\mathbb{F}_{2^n}, +)$ of $\mathbb{F}_{2^n}$.

Proof. By Proposition 4.2, every EA-automorphism of f given by (L, M, N, a, b) can be uniquely written as the composition of an EL-automorphism φ of the shape

$$\varphi\colon \begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} L & 0 \\ \tilde{M} & N \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}, \tag{4.8}$$

where $\tilde{M} = M + D_{f,L,a}$ for $D_{f,L,a}$ as defined in Proposition 4.2, and a map τ_a of the shape

$$\tau_a\colon \begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} I & 0 \\ D_{f,I,a} & I \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} a \\ f(a) \end{bmatrix},$$

where I is the identity map on $\mathbb{F}_2^n$.

[2] The proof of Proposition 4.3 is mainly due to Yue Zhou.

Note that the set of all φ is $\mathrm{Aut}_{EL}(f)$. Clearly, τ_a is also an EA-automorphism of f mapping $(x, f(x))$ to $(x+a, f(x+a))$ for any $x \in \mathbb{F}_2^n$. The set of all τ_a with $a \in \mathbb{F}_2^n$ forms a subgroup T_f of $\mathrm{Aut}_{EA}(f)$ that is isomorphic to $(\mathbb{F}_{2^n}, +)$. Hence, $\mathrm{Aut}_{EA}(f) = T_f \mathrm{Aut}_{EL}(f)$. Moreover, it is obvious that the identity map on $\mathbb{F}_2^n \times \mathbb{F}_2^n$ is the unique common element of T_f and $\mathrm{Aut}_{EL}(f)$.

It remains to show that T_f is a normal subgroup of $\mathrm{Aut}_{EA}(f)$. We do so by verifying that

$$\tau_a \circ \varphi = \varphi \circ \tau_{L^{-1}(a)}. \tag{4.9}$$

A similar result was given by Dempwolff and Edel [44, Lemma 2.5]. The left-hand side of (4.9), $\tau_a \circ \varphi$, is exactly the EA-automorphism (L, M, N, a, b) we decomposed above. The right-hand side of (4.9), $\varphi \circ \tau_{L^{-1}(a)}$, maps $(x, f(x))$ to

$$\begin{aligned} \varphi \circ \tau_{L^{-1}(a)} \begin{bmatrix} x \\ f(x) \end{bmatrix} &= \begin{bmatrix} L & 0 \\ \tilde{M} & N \end{bmatrix} \begin{bmatrix} x + L^{-1}(a) \\ f(x + L^{-1}(a)) \end{bmatrix} \\ &= \begin{bmatrix} L(x) + a \\ N(f(x + L^{-1}(a))) + \tilde{M}(x + L^{-1}(a)) \end{bmatrix}. \end{aligned} \tag{4.10}$$

We consider

$$N(f(x + L^{-1}(a))) + \tilde{M}(x + L^{-1}(a)). \tag{4.11}$$

Adding $N(f(x)) + N(f(L^{-1}(a)))$ twice and using the definition of $\tilde{M}$, (4.11) equals

$$\begin{aligned} &N(f(x)) + M(x) + N(f(L^{-1}(a)) + M(L^{-1}(a)) \\ &\quad + D_{f,L,a}(x) + N(f(x + L^{-1}(a))) + N(f(x)) + N(f(L^{-1}(a))) + D_{f,L,a}(L^{-1}(a)). \end{aligned}$$

First, note that $D_{f,L,a}(L^{-1}(a)) = 0$. Second, as $N(f(x)) = f(L(x)) + M(x) + D_{f,L,a}(x)$ by the definition of φ, it follows that

$$\begin{aligned} &N(f(x + L^{-1}(a))) + N(f(x)) + N(f(L^{-1}(a))) \\ &\qquad = f(L(x) + a) + f(L(x)) + f(a) = D_{f,L,a}(x). \end{aligned}$$

Third, using the same reasoning as before and recalling that $D_{f,L,a}(L^{-1}(a)) = 0$, we have

$$N(f(L^{-1}(a)) + M(L^{-1}(a)) = f(a) + D_{f,L,a}(L^{-1}(a)) = f(a).$$

Consequently, we obtain

$$N(f(x + L^{-1}(a))) + \tilde{M}(x + L^{-1}(a)) = N(f(x)) + M(x) + f(a),$$

which, considering (4.10), means that $\varphi \circ \tau_{L^{-1}(a)}$ also describes the EA-automorphism (L, M, N, a, b). Therefore, by definition, $\mathrm{Aut}_{EA}(f) = T_f \rtimes \mathrm{Aut}_{EL}(f)$. □

We remark that Proposition 4.3 enables us to determine the automorphism group $\mathrm{Aut}_{EA}(f)$ under EA-equivalence of any quadratic function f on $\mathbb{F}_2^n$, also if $f(0) \neq 0$. To obtain $\mathrm{Aut}_{EA}(f)$, we then only have to apply a conjugation of a translation on the automorphism group $\mathrm{Aut}_{EA}(f+f(0))$ of the quadratic function $f+f(0)$, which, as $f+f(0)$ has no constant part, we can determine using Proposition 4.3.

We add an interesting remark about the connection of the automorphism groups of quadratic APN functions under EA- and CCZ-equivalence.

Remark 4.2. Without formal proof, Satoshi Yoshiara and Ulrich Dempwolff pointed out to Yue Zhou and the present author that if f is a quadratic APN function on $\mathbb{F}_2^n$, where $n \geq 4$, then

$$\mathrm{Aut}(f) = \mathrm{Aut}_{EA}(f). \tag{4.12}$$

It seems that a proof of this result requires techniques quite different from those used in this thesis. Therefore, we did not try to extract a proof from the group theoretic papers by the aforementioned authors [44, 105, 106].

Since no proof of (4.12) has been published yet, we will formulate our results about the automorphism groups of several quadratic APN functions in Section 5.5 in terms of EA-equivalence. A formal proof of (4.12) would imply that our results can be directly transferred to the automorphism groups of the respective functions under CCZ-equivalence.

4.3 Known families of almost perfect nonlinear functions

In this section, we give a short overview of the currently known APN functions. Note that, from now on, we will usually identify the vector space $\mathbb{F}_2^n$ with the finite field $\mathbb{F}_{2^n}$, and we will denote the multiplicative group of $\mathbb{F}_{2^n}$ by $\mathbb{F}_{2^n}^*$.

In Table 4.1, we present the known power APN functions $x \mapsto x^d$. According to Pott [92], this list is sometimes believed to be complete. Power APN functions and their equivalence relations are very well studied. We refer to Yoshiara [107] for a complete characterization of the CCZ-equivalence relations among these functions. It is, for example, known that Gold functions are inequivalent for different values of i; see Budaghyan, Carlet, and Leander [26]. In Section 5.1, we will take a careful look at the equivalence relations between distinct Gold functions as they will play an important role in the proofs of our main theorems.

Table 4.1: List of the known power APN functions $x \mapsto x^d$ on $\mathbb{F}_{2^n}$ [92, Table 3].

	Exponents d	Conditions	Reference
Gold functions	2^i+1	$\gcd(i,n)=1,\ i \leq \lfloor \frac{n}{2} \rfloor$	[65, 87]
Kasami functions	$2^{2i}-2^i+1$	$\gcd(i,n)=1,\ i \leq \lfloor \frac{n}{2} \rfloor$	[70, 74]
Welch function	2^k+3	$n=2k+1$	[52]
Niho function	$2^k+2^{\frac{k}{2}}-1$	$n=2k+1$, k even	[51]
	$2^k+2^{\frac{3k+1}{2}}-1$	$n=2k+1$, k odd	
Inverse function	$2^{2k}-1$	$n=2k+1$	[9, 87]
Dobbertin function	$2^{4k}+2^{3k}+2^{2k}+2^k-1$	$n=5k$	[53]

Studying the power APN functions from Table 4.1, it is obvious, though, that none of these classes provides many inequivalent functions. There are simply not enough possible choices for the relevant parameters. Hence, power APN functions are not well suited to establish a good lower bound on the total number of inequivalent APN functions.

As far as non-power APN functions are concerned, the situation becomes much less clear. Several infinite families of non-power APN functions have been found, but not much is known about their equivalence relations. This includes equivalence relations both between functions from different classes as well as between functions coming from the same class. Recently, Budaghyan, Calderini, and Villa [24] actually reduced the number of known classes of non-power APN functions by proving that several of them coincide. The authors present an updated list [24, Table 3] of 13 currently known infinite families of quadratic APN functions that are CCZ-inequivalent to power functions. Note that in their list, Budaghyan, Calderini, and Villa [24] give all functions in univariate description. We will only use bivariate descriptions in this thesis as the functions we consider have much simpler forms in this representation.

In the remainder of this section, we present the APN functions we study in this thesis. The main focus lies on the classes presented in Theorem 4.6 and Theorem 4.8, which were introduced by Zhou and Pott [109] in 2013 and by Taniguchi [100] in 2019, respectively. In the aforementioned list [24, Table 3], these are the families F10 and F12. We add some information on the background of these infinite families first.

Both the Zhou-Pott and the Taniguchi functions have a similar form: they fit into a general non-explicit construction introduced by Carlet [36, 37], who showed that a function $f\colon \mathbb{F}_{2^m}^2 \to \mathbb{F}_{2^m}^2$ with bivariate description

$$f(x,y) = (g(x,y),\, xy),$$

is APN if and only if

1. for every $y \in \mathbb{F}_{2^m}$, the function $x \mapsto g(x,y)$ on $\mathbb{F}_{2^m}$ is APN,
2. for every $x \in \mathbb{F}_{2^m}$, the function $y \mapsto g(x,y)$ on $\mathbb{F}_{2^m}$ is APN, and
3. for every $(a,b) \in \mathbb{F}_{2^m}^* \times \mathbb{F}_{2^m}^*$ and for every $c \in \mathbb{F}_{2^m}$, the function $x \mapsto g(ax, bx+c)$ on $\mathbb{F}_{2^m}$ is APN.

From his result, Carlet [36] derived the following class of APN functions.

Theorem 4.4 ([36, Theorem 1]). *Let m be a positive integer, and let i, j be integers such that $\gcd(m, i-j) = 1$. Moreover, let $s, t \in \mathbb{F}_{2^m}^*$ and $u, v \in \mathbb{F}_{2^m}$. The function $f\colon \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^{2m}}$ defined by*

$$f(x,y) = \left(sx^{2^i+2^j} + ux^{2^i}y^{2^j} + vx^{2^j}y^{2^i} + ty^{2^i+2^j},\ xy\right)$$

is APN if and only if the polynomial $sX^{2^i+2^j} + uX^{2^i} + vX^{2^j} + t$ has no root in $\mathbb{F}_{2^m}$.

Carlet [36] additionally showed that the class from Theorem 4.4 contains several known families of APN functions that were introduced by Budaghyan and Carlet [25] and by Bracken, Byrne, Markin, and McGuire [17]. They are summarized in the family F4 in [24, Table 3].

Taniguchi [100] observed that the functions from Theorem 4.4 are CCZ-equivalent to a family with a simpler representation. Since we are only interested in inequivalent APN functions, we will from now on only consider the functions from Proposition 4.5 and call these Carlet APN functions.

Proposition 4.5 ([100, Corollary 2]). *Let $m \geq 2$ and k be positive integers such that* $\gcd(k,m) = 1$. *Let $\alpha \in \mathbb{F}_{2^m}$ and $\beta \in \mathbb{F}_{2^m}^*$. The function $f_{k,\alpha,\beta}\colon \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^{2m}}$ defined by*

$$f_{k,\alpha,\beta}(x,y) = \left(x^{2^k+1} + \alpha x y^{2^k} + \beta y^{2^k+1},\ xy\right)$$

is APN if and only if the polynomial $X^{2^k+1} + \alpha X + \beta$ has no root in $\mathbb{F}_{2^m}$.

Taniguchi [100] also showed that any function $f_{k,\alpha,\beta}$ from Proposition 4.5 with $\alpha \neq 0$ is CCZ-equivalent to a function $f_{k,1,\beta'}$ from the same family with $\alpha = 1$. In Lemma 5.7, we will restate this result and add a short proof. Consequently, only Carlet APN functions with $\alpha = 0$ and $\alpha = 1$ are relevant to us.

Independently of Carlet's [36] general construction from above, Zhou and Pott [109] discovered a class of APN functions of a similar form, which they derived from a new infinite family of commutative semifields. In Theorem 4.6, we restate their result, which was later improved by Anbar, Kalaycı, and Meidl [2].

Theorem 4.6 ([109, Corollary 2] and [2, Proposition 3.5]). *Let $m \geq 2$ be an even integer, and let k, s be positive integers such that k is coprime to m. Let $\alpha \in \mathbb{F}_{2^m}^*$. The function $f_{k,s,\alpha}\colon \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^{2m}}$ defined by*

$$f_{k,s,\alpha}(x,y) = \left(x^{2^k+1} + \alpha y^{(2^k+1)2^s},\ xy\right)$$

is APN if and only if s is even and α is a non-cube.

Zhou and Pott [109] showed that the restrictions on the parameters s and α in Theorem 4.6, namely on s to be even and on α to be a non-cube, are sufficient for the function to be APN. Anbar, Kalaycı, and Meidl [2] then observed that these conditions are also necessary.

Having learned of the Zhou-Pott APN functions, Carlet [37] generalized his family from Theorem 4.4 so that it also contains the functions from Theorem 4.6.

Theorem 4.7 ([37, Theorem 4.2]). *Let m be a positive integer, and let k be coprime to m. Let $h_1, \ldots, h_4$ be linear maps on $\mathbb{F}_{2^m}$. The function $f\colon \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^{2m}}$ defined by*

$$f(x,y) = (h_1(x^{2^k+1}) + h_2(x^{2^k}y) + h_3(xy^{2^k}) + h_4(y^{2^k+1}),\ xy)$$

is APN if and only if for every $a, b \in \mathbb{F}_{2^m}$ such that $(a,b) \neq (0,0)$, the linear function

$$t_{a,b}(y) = h_1(a^{2^k+1}y) + h_2(a^{2^k}by) + h_3(ab^{2^k}y) + h_4(b^{2^k+1}y)$$

is bijective if m is odd, and satisfies $\ker t_{a,b} \cap \{u^{2^k+1}(v^{2^k}+v) : u \in \mathbb{F}_{2^m}^*, v \in \mathbb{F}_{2^m}\} = \{0\}$ *if m is even.*

Setting $h_1(x) = x$, $h_2(x) = 0$, $h_3(x) = \alpha x$ and $h_4(x) = \beta x$, we obtain the Carlet APN functions from Proposition 4.5, choosing $h_1(x) = x$, $h_2(x) = h_3(x) = 0$ and $h_4(x) = \alpha x^{2^s}$, we obtain the Zhou-Pott APN functions from Theorem 4.6.

In Theorem 4.8, we present Taniguchi's [100] construction. The author proved the almost perfect nonlinearity of these functions using the three criteria on $g(x, y)$ by Carlet [36] we mentioned above.

Theorem 4.8 ([100, Theorem 3])**.** *Let $m \geq 2$ be a positive integer, and let k be an integer coprime to m. Let $\alpha \in \mathbb{F}_{2^m}$ and $\beta \in \mathbb{F}_{2^m}^*$. The function $f_{k,\alpha,\beta} \colon \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^{2m}}$ defined by*

$$f_{k,\alpha,\beta}(x, y) = \left(x^{2^{2k}(2^k+1)} + \alpha x^{2^{2k}} y^{2^k} + \beta y^{2^k+1},\ xy\right)$$

is APN if and only if the polynomial $X^{2^k+1} + \alpha X + \beta$ has no root in $\mathbb{F}_{2^m}$.

Anbar, Kalaycı, and Meidl [2] remarked that the Taniguchi APN functions from Theorem 4.8 are also a special case of the functions from Theorem 4.7: we need to choose $h_1(x) = x^{2^{2k}}$, $h_2(x) = \alpha x^{2^k}$, $h_3(x) = 0$ and $h_4(x) = \beta x$. Analogously to the functions from Proposition 4.5, Taniguchi [100] showed that any function $f_{k,\alpha,\beta}$ from Theorem 4.8 with $\alpha \neq 0$ is CCZ-equivalent to a function $f_{k,1,\beta'}$ from the same class with $\alpha = 1$. We will restate this result in Proposition 5.12 and add a proof.

Note that all the functions from Theorem 4.4, Proposition 4.5, Theorem 4.6 and Theorem 4.8 are quadratic. Moreover, Tan, Qu, Ling, and Tan [99] and Anbar, Kalaycı, and Meidl [2] showed that all these functions have the classical Walsh spectrum $\mathcal{W}_f = \{0, \pm 2^m, \pm 2^{m+1}\}$.

We close this section by specifying the case $\alpha = 0$ for Carlet and Taniguchi APN functions with the help of the following lemma.

Lemma 4.9. *Let m be a positive integer, let k be coprime to m, and let $\beta \in \mathbb{F}_{2^m}^*$. The polynomial $P(X) = X^{2^k+1} + \beta$ has no root in $\mathbb{F}_{2^m}$ if and only if m is even and β is a non-cube.*

Proof. It is well known that if m and k are coprime, then

$$\gcd(2^k + 1, 2^m - 1) = \begin{cases} 1 & \text{if } m \text{ is odd,} \\ 3 & \text{if } m \text{ is even.} \end{cases}$$

Consequently, if m is odd, then $P(X)$ is a permutation polynomial and, thus, always has a root. If m is even, then $P(X)$ has a root if and only if β is a cube. □

From Lemma 4.9, we immediately obtain the following corollary.

Corollary 4.10. *(a) A Carlet function $f_{k,0,\beta}$ on $\mathbb{F}_{2^{2m}}$ from Proposition 4.5 is APN if and only if m is even and β is a non-cube in $\mathbb{F}_{2^m}^*$.*

(b) *A Taniguchi function $f_{k,0,\beta}$ on $\mathbb{F}_{2^{2m}}$ from Theorem 4.8 is APN if and only if m is even and β is a non-cube in $\mathbb{F}_{2^m}^*$.*

It follows that Carlet APN functions with $\alpha = 0$ from Proposition 4.5 coincide with Zhou-Pott APN functions with $s = 0$ from Theorem 4.6.

5 Solving equivalence problems of almost perfect nonlinear functions

In this chapter, we study the equivalence relations of the functions introduced in Section 4.3. In Section 5.1, we present a new proof to a well-known result about the equivalence of Gold APN functions that we need in the following sections. In Section 5.2, we completely determine the equivalence of Zhou-Pott APN functions. In Section 5.3, we show that on $\mathbb{F}_{2^{2m}}$ where m is even, Carlet APN functions are included in the Zhou-Pott class. In Section 5.4, we almost completely determine the equivalence of Taniguchi APN functions.

Afterwards, in Section 5.5, we derive the automorphism groups of all the aforementioned APN functions under EA- and EL-equivalence from the precise shape of the admissible equivalence mappings. Using these results, we add the final piece to completely determine the equivalence of Taniguchi APN functions, and we completely determine the equivalence between Zhou-Pott and Taniguchi APN functions. Eventually, we use all these results in Section 5.6 to determine the total number of inequivalent functions in the families by Zhou-Pott and by Taniguchi. This allows us to establish the first nontrivial lower bound on the total number of inequivalent APN functions on $\mathbb{F}_{2^n}$ where n is even.

5.1 Equivalence of Gold APN functions

Before we tackle the equivalence problems of the Zhou-Pott and the Taniguchi APN functions in the following sections, we state a well-known result about the equivalence of Gold APN functions $x \mapsto x^{2^k+1}$ on $\mathbb{F}_{2^n}$, where k is coprime to n, in Theorem 5.1. We present a new proof for this result that allows us to determine the precise shape of the equivalence mappings of Gold APN functions. We will need these equivalence mappings in the proofs of Theorem 5.4 and Theorem 5.13.

Note that Gold functions are quadratic and have no constant term. Hence, by Theorem 4.1 and Proposition 4.2, two Gold functions are CCZ-equivalent if and only if they are EL-equivalent. Moreover, for any k coprime to n, the Gold APN functions $x \mapsto x^{2^k+1}$ and $x \mapsto x^{2^{-k}+1}$ are linearly equivalent on $\mathbb{F}_{2^n}$ since for the linearized polynomials $L(X) = X$ and $N(X) = X^{2^k}$, the equation

$$(L(x))^{2^k+1} = N(x^{2^{-k}+1})$$

holds for all $x \in \mathbb{F}_{2^n}$. Consequently, we only need to consider Gold APN functions with $k < \frac{n}{2}$.

Our new proof shows that for $n \geq 5$, all equivalence mappings from one Gold APN function to another are monomials. The case $n = 4$ will be considered separately in Proposition 5.2. For $n \leq 3$, the Gold APN function $x \mapsto x^3$ is the unique APN function up to EA-equivalence. Hence, this case may not be interesting and will not be considered in this thesis.

Theorem 5.1. *Let $n \geq 5$, and let k, ℓ be integers coprime to n such that $0 < k, \ell < \frac{n}{2}$. Two Gold APN functions $f, g \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$, where*

$$f(x) = x^{2^k+1} \qquad \textit{and} \qquad g(x) = x^{2^\ell+1},$$

are CCZ-equivalent if and only if $k = \ell$. In this case, the functions are linearly equivalent, and the equation $f(L(x)) = N(g(x))$ holds for all $x \in \mathbb{F}_{2^n}$ if and only if $L(X) = a_u X^{2^u}$ and $N(X) = a_u^{2^k+1} X^{2^u}$ for some $u \in \{0, \dots, n-1\}$ and $a_u \in \mathbb{F}_{2^n}^*$.

Proof. If $k = \ell$, the functions f and g coincide and, thus, are linearly equivalent and thereby CCZ-equivalent. We will show that EL-equivalence, and thereby CCZ-equivalence, of f and g implies $k = \ell$ and that f and g are linearly equivalent. Assume f and g are EL-equivalent. Then there exist linearized polynomials $L(X), N(X), M(X) \in \mathbb{F}_{2^n}[X]$, where $N(X)$ and $L(X)$ are permutation polynomials, such that

$$(L(x))^{2^k+1} = N(x^{2^\ell+1}) + M(x) \tag{5.1}$$

for all $x \in \mathbb{F}_{2^n}$. Let $x \in \mathbb{F}_{2^n}$. Writing $L(X) = \sum_{i=0}^{n-1} a_i X^{2^i}$ and $N(X) = \sum_{i=0}^{n-1} b_i X^{2^i}$, and rearranging the left-hand side of (5.1), we obtain

$$\sum_{i=0}^{n-1} a_{i-k}^{2^k} a_i x^{2^{i+1}} + \sum_{\substack{i,j=0,\\ j\neq i+k}}^{n-1} a_i^{2^k} a_j x^{2^{i+k}+2^j} = \sum_{i=0}^{n-1} b_i x^{(2^\ell+1)2^i} + M(x). \tag{5.2}$$

As the first sum on the left-hand side of (5.2) is a linearized polynomial and the second sum on the left-hand side does not include any linear parts, it follows that

$$M(X) = \sum_{i=0}^{n-1} a_{i-k}^{2^k} a_i X^{2^{i+1}}. \tag{5.3}$$

We omit the linear parts and rewrite the second sum on the left-hand side of (5.2). We obtain

$$\sum_{0\leq i<j\leq n-1} (a_{i-k}^{2^k} a_j + a_{j-k}^{2^k} a_i) x^{2^i+2^j} = \sum_{i=0}^{n-1} b_i x^{2^i+2^{i+\ell}},$$

where the subscripts of a are calculated modulo n. It follows that

$$a_{i-k}^{2^k} a_{i+\ell} + a_{i+\ell-k}^{2^k} a_i = b_i \qquad \text{for all } i, \tag{5.4}$$

$$a_{i-k}^{2^k} a_j + a_{j-k}^{2^k} a_i = 0 \qquad \text{for } j \neq i, i \pm \ell. \tag{5.5}$$

Since $N(X)$ cannot be zero, there exists some $u \in \{0, \dots, n-1\}$ such that $b_u \neq 0$. Then, by (5.4), a_{u-k} and a_u cannot be zero at the same time. We will consider the two cases that, first, exactly one of a_{u-k} and a_u is nonzero and, second, both a_{u-k} and a_u are nonzero.

Case 1. We divide this case into two subcases: first, we assume $a_u \neq 0$ and $a_{u-k} = 0$, and second, we assume $a_u = 0$ and $a_{u-k} \neq 0$.

Case 1.1. Suppose $a_u \neq 0$ and $a_{u-k} = 0$. Then (5.4) with $i = u$ implies $a_{u+\ell-k} \neq 0$, and (5.5) reduces to

$$a_{j-k}^{2^k} a_u = 0 \qquad \text{for } j \neq u, u \pm \ell.$$

Consequently, $a_{j-k} = 0$ for $j \neq u, u \pm \ell$, and besides a_u and $a_{u+\ell-k}$, the only coefficient of $L(X)$ that is possibly nonzero is $a_{u-\ell-k}$.

Assume $k \neq \ell$. Then $L(X) = a_u X^{2^u} + a_{u-\ell-k} X^{2^{u-\ell-k}} + a_{u+\ell-k} X^{2^{u+\ell-k}}$. If we plug this polynomial into (5.1), we obtain on the left-hand side

$$\begin{aligned}
&a_u^{2^k+1} x^{2^u(2^k+1)} + a_{u-\ell-k}^{2^k+1} x^{2^{u-\ell-k}(2^k+1)} + a_{u+\ell-k}^{2^k+1} x^{2^{u+\ell-k}(2^k+1)} \\
&\quad + a_u^{2^k} a_{u-\ell-k} x^{2^{u-\ell-k}(2^{2k+\ell}+1)} + a_u^{2^k} a_{u+\ell-k} x^{2^{u+\ell-k}(2^{2k-\ell}+1)} \\
&\quad + a_{u-\ell-k}^{2^k} a_u x^{2^{u-\ell}(2^\ell+1)} + a_{u-\ell-k}^{2^k} a_{u+\ell-k} x^{2^{u+\ell-k}(2^{k-2\ell}+1)} \\
&\quad + a_{u+\ell-k}^{2^k} a_u x^{2^u(2^\ell+1)} + a_{u+\ell-k}^{2^k} a_{u-\ell-k} x^{2^{u-\ell-k}(2^{k+2\ell}+1)}.
\end{aligned} \tag{5.6}$$

Note that the first and the third summand of (5.6) have nonzero coefficients and, since $k \not\equiv \pm\ell \pmod{n}$, they can neither cancel each other nor can they be canceled by any of the other terms. However, as $k \neq \ell$, these two terms cannot be represented on the right-hand side of (5.1). This is a contradiction.

Now suppose $k = \ell$. Then a_u and $a_{u+\ell-k}$ coincide, and $L(X) = a_u X^{2^u} + a_{u-2k} X^{2^{u-2k}}$. Plugging this polynomial into the left-hand side of (5.1), we obtain

$$\begin{aligned}
&a_u^{2^{k+1}} x^{2^u(2^k+1)} + a_{u-2k}^{2^{k+1}} x^{2^{u-2k}(2^k+1)} \\
&\quad + a_u^{2^k} a_{u-2k} x^{2^{u-2k}(2^{3k}+1)} + a_{u-2k}^{2^k} a_u x^{2^{u-k}(2^k+1)}.
\end{aligned} \tag{5.7}$$

As $n \geq 5$, we have $3k \not\equiv \pm k \pmod{n}$. Hence, the third term of (5.7) neither can be canceled nor can it be represented in the form $x^{2^i(2^k+1)}$ on the right-hand side of (5.1). Consequently, its coefficient has to be zero. Since $a_u \neq 0$, it follows that $a_{u-2k} = 0$, which means $L(X) = a_u X^{2^u}$ is a monomial. Thus, $N(X) = b_u X^{2^u}$ is also a monomial, and it follows from (5.4) that $b_u = a_u^{2^k+1}$. Furthermore, (5.3) now implies $M(X) = 0$, which means f and g are linearly equivalent.

Case 1.2. Assume $a_{u-k} \neq 0$ and $a_u = 0$. Now (5.4) implies $a_{u+\ell} \neq 0$. Moreover, (5.5) with $i = u$ becomes

$$a_{u-k}^{2^k} a_j = 0 \qquad \text{for } j \neq u, u \pm \ell.$$

Consequently, $a_j = 0$ for $j \neq u, u \pm \ell$, and besides a_{u-k} and $a_{u+\ell}$, the only coefficient of $L(X)$ that is possibly nonzero is $a_{u-\ell}$.

If we suppose $k \neq \ell$, we obtain, by similar reasoning as above, the same contradiction as in Case 1.1. The case $k = \ell$ is also similar, but will lead to a contradiction now. If $k = \ell$, then $L(X) = a_{u-k}X^{2^{u-k}} + a_{u+k}X^{2^{u+k}}$, where both coefficients are nonzero. Plugging this polynomial into (5.1), the left-hand side becomes

$$a_{u-k}^{2^{k+1}} x^{2^{u-k}(2^k+1)} + a_{u+k}^{2^{k+1}} x^{2^{u+k}(2^k+1)} + a_{u-k}^{2^k} a_{u+k} x^{2^u(2^k+1)} + a_{u+k}^{2^k} a_{u-k} x^{2^{u-k}(2^{3k}+1)}.$$

Similarly to (5.7), the fourth term cannot be represented in the form $x^{2^i(2^k+1)}$ on the right-hand side of (5.1). As its coefficient is nonzero, this is a contradiction.

Case 2. Assume both a_u and a_{u-k} are nonzero. First, suppose $k \neq \ell$. Since $0 < k, \ell < \frac{n}{2}$, it follows that $u - k \not\equiv u \pm \ell \pmod{n}$. Hence, we may consider (5.5) for $i = u$ and $j = u - k$ and obtain

$$a_{u-k}^{2^k+1} + a_{u-2k}^{2^k} a_u = 0.$$

Consequently, $a_{u-2k} \neq 0$. If we now consider (5.5) for $(i, j) = (u - k, u - 2k), (u - 2k, u - 3k), \ldots, (u - (n-1)k, u)$ and recall that $\gcd(k, n) = 1$, then it follows that $a_i \neq 0$ for all $i = 0, \ldots, n-1$. Moreover, this sequence of equations implies that the quotient

$$\frac{a_{i-k}^{2^k}}{a_i} = \frac{a_{u-k}^{2^k}}{a_u} =: \Delta$$

is constant for all $i = 0, \ldots, n-1$. We consider (5.4) for $i = u$:

$$a_{u-k}^{2^k} a_{u+\ell} + a_{u+\ell-k}^{2^k} a_u = b_u. \tag{5.8}$$

If we divide (5.8) by $a_u a_{u+\ell}$, we obtain

$$\frac{a_{u-k}^{2^k}}{a_u} + \frac{a_{u+\ell-k}^{2^k}}{a_{u+\ell}} = \frac{b_u}{a_u a_{u+\ell}}.$$

This is a contradiction as the left-hand side is $\Delta + \Delta = 0$ and the right-hand side is nonzero.

Now, assume $k = \ell$. In this case, (5.4) becomes

$$a_{u-k}^{2^k} a_{u+k} + a_u^{2^k+1} = b_u \tag{5.9}$$

for $i = u$. We consider (5.5) for $i = u - k$ and $j = u + k$:

$$a_{u-2k}^{2^k} a_{u+k} + a_u^{2^k} a_{u-k} = 0.$$

Recall that $a_{u-k}, a_u \neq 0$, thus $a_{u-2k}, a_{u+k} \neq 0$. From additionally considering (5.5) for $(i, j) = (u - 2k, u), (u - 3k, u - k), \ldots, (u, u + 2k)$, it follows that $a_i \neq 0$ for all

$i = 0, \dots, n-1$. Furthermore, we obtain from these equations that

$$\frac{a_{u-ik}^{2^k}}{a_{u-(i+1)k}} = \begin{cases} \dfrac{a_u^{2^k}}{a_{u+k}} =: \Delta_1 & \text{for } i \text{ even,} \\[2ex] \dfrac{a_{u-k}^{2^k}}{a_u} =: \Delta_2 & \text{for } i \text{ odd.} \end{cases}$$

Note that $u - k \not\equiv u + 3k \pmod{n}$ as $n \geq 5$. Hence, considering (5.5) with $i = u$ and $j = u + 3k$, we obtain

$$a_{u-k}^{2^k} a_{u+3k} + a_{u+2k}^{2^k} a_u = 0,$$

which implies $\Delta_1 = \Delta_2 =: \Delta$. If we now divide (5.9) by $a_u a_{u+k}$, we obtain the same kind of contradiction as in the case $k \neq \ell$. Hence, Case 2 does not provide any solutions for $L(X), N(X)$ and $M(X)$.

In summary, f and g are EL-equivalent if and only if $k = \ell$, and the only possible EL-mappings from g to f are described by the polynomials $L(X) = a_u X^{2^u}$, $N(X) = a_u^{2^k+1} X^{2^u}$ and $M(X) = 0$ for arbitrary $u \in \{0, \dots, n-1\}$ and $a_u \in \mathbb{F}_{2^n}^*$. □

For completeness, we also consider Gold functions on $\mathbb{F}_{2^4}$. Note that on $\mathbb{F}_2^4$, it was shown by Brinkmann and Leander [20] that the Gold function $f(x) = x^3$ is the unique APN function up to CCZ-equivalence. The authors additionally showed that there are two EA-classes of APN functions, though: the class containing the Gold function, and a second class that was found by Budaghyan, Carlet, and Pott [27] and whose functions are EA-inequivalent to power functions.

If $n = 4$, some of the arguments used in the proof of Theorem 5.1 do not hold. Unlike in the case $n \geq 5$, this leads to additional EL-mappings from f to f that are not monomials. We describe these EL-automorphisms of f in the following proposition. This result can be verified computationally, for example with `Magma` [16].

Proposition 5.2. *The set* $\mathrm{Aut}_{EL}(f)$ *of EL-automorphisms of the unique Gold APN function* $f \colon \mathbb{F}_{2^4} \to \mathbb{F}_{2^4}$ *defined by* $f(x) = x^3$ *consists of the linearized monomials from Theorem 5.1 together with the linearized polynomials*

$$\begin{aligned} L(X) &= a_1 X^2 + a_3 X^8 \quad &\text{and} \quad N(X) &= a_3^2 a_1 X + a_1^3 X^2 + a_1^2 a_3 X^4 + a_3^3 X^8, \\ L(X) &= a_0 X + a_2 X^4 \quad &\text{and} \quad N(X) &= a_0^3 X + a_0^2 a_2 X^2 + a_2^3 X^4 + a_2^2 a_0 X^8, \end{aligned}$$

for coefficients $a_1, \dots, a_4 \in \mathbb{F}_{2^n}^*$ *such that* $\frac{a_1}{a_3}$ *and* $\frac{a_0}{a_2}$*, respectively, are non-cubes.*

Proof. It is easy to confirm that the monomial EL-mappings we presented in Theorem 5.1 for $n \geq 5$, also establish a linear equivalence for $n = 4$. Suppose $n = 4$. Using the same approach and the same notations as in the proof of Theorem 5.1, we obtain (5.4) and (5.5) for $k = \ell = 1$. More precisely, we have the following equations of type (5.4):

$$a_3^2 a_1 + a_0^3 = b_0, \quad a_0^2 a_2 + a_1^3 = b_1, \quad a_1^2 a_3 + a_2^3 = b_2, \quad a_2^2 a_0 + a_3^3 = b_3. \qquad (5.10)$$

Note that we now only have two equations of type (5.5), namely

$$a_1^2 a_0 + a_3^2 a_2 = 0 \qquad \text{and} \qquad a_0^2 a_3 + a_2^2 a_1 = 0. \qquad (5.11)$$

We may assume that $b_u \neq 0$ for some $u \in \{0, \dots, 3\}$, and we separate the same cases as in the proof of Theorem 5.1:

Case 1. First, suppose $a_u \neq 0$ and $a_{u-1} = 0$. The case $a_u = 0$ and $a_{u-1} \neq 0$ may be solved analogously. If $a_u \neq 0$ and $a_{u-1} = 0$, it follows from (5.11) that $a_{u+1} = 0$ and $a_{u-2} \neq 0$. However, unlike in the proof of Theorem 5.1, we do not obtain a contradiction from (5.7) now, as $x^{2^{3k}+1} = x^9$ can be written as $x^{2^{3k}(2^k+1)} = x^{2^3 \cdot 3}$. Hence, the equation

$$L(x)^3 = N(x^3)$$

holds not only for the linearized monomials from Theorem 5.1, but also for the linearized polynomials

$$L(X) = a_1 X^2 + a_3 X^8 \qquad \text{and} \qquad N(X) = a_3^2 a_1 X + a_1^3 X^2 + a_1^2 a_3 X^4 + a_3^3 X^8,$$

which we obtain choosing $u = 1$ or 3, and

$$L(X) = a_0 X + a_2 X^4 \qquad \text{and} \qquad N(X) = a_0^3 X + a_0^2 a_2 X^2 + a_2^3 X^4 + a_2^2 a_0 X^8,$$

for which we choose $u = 0$ or $u = 2$.

In the final step, we need to check under which conditions $L(X)$ and $N(X)$ are permutation polynomials. Since $L(X)$ and $N(X)$ are linearized, it is sufficient to show that they have no nonzero roots. For $x \neq 0$, the equation $L(x) = 0$ can be rearranged to $\frac{a_1}{a_3} = x^6$ and $\frac{a_0}{a_2} = x^3$, respectively. These equations have no solution if and only if $\frac{a_1}{a_3}$ and $\frac{a_0}{a_2}$ are non-cubes. It is routine to verify that $N(X)$ also is a permutation polynomial in these cases.

Case 2. Now, let both a_{u-1} and a_u be nonzero. In this case, it follows from (5.11) that $a_1, \dots, a_4$ are nonzero, and that $\frac{a_1}{a_3}$ and $\frac{a_2}{a_0}$ have to be cubes satisfying $(\frac{a_1}{a_3})^2 = \frac{a_2}{a_0}$. Consequently, by (5.10), the coefficients $b_1, \dots, b_4$ are also nonzero, which implies $a_0^3 \neq a_3^2 a_1$. Taking all these conditions into consideration, we obtain 15 choices for a_1, five choices for a_3, twelve choices for a_0, and a_2 is finally uniquely determined by the other coefficients. Thus, we obtain a total of 900 possible distinct polynomials $L(X)$. However, it can be verified that none of them is a permutation polynomial. Hence, Case 2 does not provide any solutions. □

5.2 Equivalence of Zhou-Pott APN functions

In this section, we study the equivalence of the Zhou-Pott APN functions on $\mathbb{F}_{2^{2m}}$, where m is even, that we introduced in Theorem 4.6. We will answer the question for which values of the parameters k, s, α two Zhou-Pott APN functions $f_{k,s,\alpha}$ are CCZ-inequivalent. Recall from Section 4.3 that these functions are quadratic and have no constant term. Hence, by Theorem 4.1 and Proposition 4.2, two Zhou-Pott APN functions are CCZ-equivalent if and only if they are EL-equivalent. We begin by proving some obvious equivalences:

Proposition 5.3. *Let m be an even integer. Let k, ℓ be integers coprime to m such that $0 < k, \ell < m$, and let s, t be even integers with $0 \leq s, t \leq m$. Let $\alpha, \beta \in \mathbb{F}_{2^m}^*$ be non-cubes. The following Zhou-Pott APN functions on $\mathbb{F}_{2^{2m}}$ from Theorem 4.6 are linearly equivalent:*

(a) $f_{k,s,\alpha}$ and $f_{k,s,\beta}$,

(b) $f_{k,s,\alpha}$ and $f_{-k,s,\beta}$,

(c) $f_{k,s,\alpha}$ and $f_{k,-s,\beta}$,

(d) $f_{k,s,\alpha}$ and $f_{-k,-s,\beta}$.

Proof. By (4.6) and (4.7), the Zhou-Pott functions $f_{k,s,\alpha}$ and $f_{\ell,t,\beta}$ are linearly equivalent if there exist invertible mappings L, N on $\mathbb{F}_{2^m}^2$, represented by linearized polynomials $L_A(X,Y), L_B(X,Y) \in \mathbb{F}_{2^m}[X,Y]$ and $N_1(X), \ldots, N_4(X) \in \mathbb{F}_{2^m}[X]$, respectively, such that the two equations

$$\begin{aligned} L_A(x,y)^{2^k+1} + \alpha L_B(x,y)^{(2^k+1)2^s} &= N_1(x^{2^\ell+1} + \beta y^{(2^\ell+1)2^t}) + N_3(xy), \\ L_A(x,y) L_B(x,y) &= N_2(x^{2^\ell+1} + \beta y^{(2^\ell+1)2^t}) + N_4(xy) \end{aligned}$$

hold for all $x, y \in \mathbb{F}_{2^m}$. Note that in all the following cases, $N_2(X) = N_3(X) = 0$. Hence we will omit these polynomials in the remainder of the proof. Let $x, y \in \mathbb{F}_{2^m}$.

(a) Suppose $k = \ell$ and $s = t$, and denote by γ a primitive element of $\mathbb{F}_{2^m}$. For the non-cubes $\alpha, \beta \in \mathbb{F}_{2^m}^*$ write $\alpha = \gamma^a$ and $\beta = \gamma^b$ for some integers $a, b \in \{0, \ldots, 2^m - 1\}$ such that $a, b \not\equiv 0 \pmod 3$. We separate the cases $a \equiv b \pmod 3$ and $a \not\equiv b \pmod 3$. First, assume $a \equiv b \pmod 3$. Then f_{k,s,γ^a} and f_{k,s,γ^b} are linearly equivalent by

$$L_A(X,Y) = X, \quad L_B(X,Y) = \gamma^c Y, \quad N_1(X) = X, \quad N_4(X) = \gamma^c X,$$

where $c \in \{0, \ldots, 2^m - 1\}$ such that

$$(2^k + 1) 2^s c \equiv b - a \pmod{2^m - 1}.$$

Such an integer c always exists as $\gcd((2^k+1)2^s, 2^m-1) = 3$ and $b-a \equiv 0 \pmod 3$. If $a \not\equiv b \pmod 3$, then f_{k,s,γ^a} and f_{k,s,γ^b} are linearly equivalent by

$$L_A(X,Y) = X^2, \quad L_B(X,Y) = \gamma^c Y^2, \quad N_1(X) = X^2, \quad N_4(X) = \gamma^c X^2,$$

where c satisfies

$$(2^k+1)2^s c \equiv 2b-a \pmod{2^m-1}.$$

By the same reasoning as before and considering that $2b-a \equiv 0 \pmod 3$, such an integer c always exists.

(b) According to (a), $f_{-k,s,\beta}$ is linearly equivalent to $f_{-k,s,\alpha}$. The function $f_{k,s,\alpha}$ is also linearly equivalent to $f_{-k,s,\alpha}$ via the equivalence mapping given by

$$L_A(X,Y) = X^{2^{-k}}, \quad L_B(X,Y) = Y^{2^{-k}}, \quad N_1(X) = X, \quad N_4(X) = X^{2^{-k}}.$$

(c) Let $\beta' = \frac{1}{\alpha^{2^{-s}}}$. According to (a), $f_{k,-s,\beta}$ is linearly equivalent to $f_{k,-s,\beta'}$. We show that $f_{k,s,\alpha}$ is also linearly equivalent to $f_{k,-s,\beta'}$. This can be seen choosing

$$L_A(X,Y) = Y, \qquad L_B(X,Y) = X, \qquad N_1(X) = \alpha X^{2^s}, \qquad N_4(X) = X.$$

(d) Combining (b) and (c), it follows that $f_{k,s,\alpha}$ is linearly equivalent to $f_{-k,-s,\beta}$. □

Thanks to Proposition 5.3, we can, from now on, fix the non-cube α and restrict the parameters k and s to $0 < k < \frac{m}{2}$ and $0 \leq s \leq \frac{m}{2}$.

In Theorem 5.4, we completely determine the equivalence of Zhou-Pott APN functions. Note that for $m = 2$, all Zhou-Pott APN functions are CCZ-equivalent since, as mentioned above, there is only one CCZ-class of APN functions on $\mathbb{F}_{2^4}$. The result for the case $m = 4$ was already given by Zhou and Pott [109], we restate it at the beginning of our proof. We remark that our approach to prove Theorem 5.4 is motivated by Zhou and Pott [109], who used a similar technique to determine under which conditions the semifields, from which they obtained their APN functions, are non-isotopic.

Theorem 5.4. *Let $m \geq 4$ be an even integer. Let k, ℓ be integers coprime to m such that $0 < k, \ell < \frac{m}{2}$, let s, t be even integers with $0 \leq s, t \leq \frac{m}{2}$, and let $\alpha, \beta \in \mathbb{F}_{2^m}^*$ be non-cubes. Two Zhou-Pott APN functions $f_{k,s,\alpha}, f_{\ell,t,\beta} \colon \mathbb{F}_{2^{2m}} \to \mathbb{F}_{2^{2m}}$ from Theorem 4.6 defined by*

$$f_{k,s,\alpha}(x,y) = \left(x^{2^k+1} + \alpha y^{(2^k+1)2^s},\ xy\right)$$

and

$$f_{\ell,t,\beta}(x,y) = \left(x^{2^\ell+1} + \beta y^{(2^\ell+1)2^t},\ xy\right)$$

are CCZ-equivalent if and only if $k = \ell$ and $s = t$.

Proof. As shown in Proposition 5.3 (a), $f_{\ell,t,\beta}$ is linearly equivalent and thereby CCZ-equivalent to $f_{\ell,t,\alpha}$. Hence, we only consider $f_{k,s,\alpha}$ and $f_{\ell,t,\alpha}$ from now on. Write $f_{k,s}$ and $f_{\ell,t}$ for these functions. We show that if $f_{k,s}$ and $f_{\ell,t}$ are CCZ-equivalent, which implies the functions are EL-equivalent, then $k=\ell$ and $s=t$.

For $m=4$, the only admissible parameters are $k=1$ and $s\in\{0,2\}$. Zhou and Pott [109] showed that the functions $f_{1,0}$ and $f_{1,2}$ on $\mathbb{F}_{2^4}$ are CCZ-inequivalent. The authors computed the Γ-rank of these functions as 13200 and 13642, respectively.

For the remainder of this proof, let $m\geq 6$. Suppose the functions $f_{k,s}$ and $f_{\ell,t}$ are EL-equivalent. Similar to the the proof of Proposition 5.3, this implies that there exist linearized polynomials $L_A(X,Y)$, $L_B(X,Y)$, $M_A(X,Y)$, $M_B(X,Y)\in\mathbb{F}_{2^m}[X,Y]$ and $N_1(X),\dots,N_4(X)\in\mathbb{F}_{2^m}[X]$, where

$$L(X,Y)=(L_A(X,Y),L_B(X,Y))$$

and

$$N(X,Y)=(N_1(X)+N_3(Y),\ N_2(X)+N_4(Y))$$

are invertible, such that the equations

$$\begin{aligned}L_A(x,y)^{2^k+1}\ &+\ \alpha L_B(x,y)^{(2^k+1)2^s}\\ &=N_1(x^{2^\ell+1}+\alpha y^{(2^\ell+1)2^t})+N_3(xy)+M_A(x,y),\end{aligned}\tag{5.12}$$

$$L_A(x,y)L_B(x,y)=N_2(x^{2^\ell+1}+\alpha y^{(2^\ell+1)2^t})+N_4(xy)+M_B(x,y)\tag{5.13}$$

hold for all $x,y\in\mathbb{F}_{2^m}$. We write $L_A(X,Y)=L_1(X)+L_3(Y)$ and $L_B(X,Y)=L_2(X)+L_4(Y)$ for linearized polynomials $L_1(X),\dots,L_4(X)\in\mathbb{F}_{2^m}[X]$. Hence,

$$L(X,Y)=(L_1(X)+L_3(Y),\ L_2(X)+L_4(Y)).$$

Write

$$L_1(X)=\sum_{i=0}^{m-1}a_iX^{2^i},\qquad\qquad L_2(X)=\sum_{i=0}^{m-1}b_iX^{2^i},$$

and

$$L_3(Y)=\sum_{i=0}^{m-1}\overline{a}_iY^{2^i},\qquad\qquad L_4(Y)=\sum_{i=0}^{m-1}\overline{b}_iY^{2^i}.$$

Analogously, define linearized polynomials $M_1(X),\dots,M_4(X)\in\mathbb{F}_{2^m}[X]$ such that

$$M(X,Y)=(M_1(X)+M_3(Y),M_2(X)+M_4(Y)).$$

For the remainder of the proof, let $x,y\in\mathbb{F}_{2^m}$. We first prove the following claim.

Claim 5.1. *If $f_{k,s}$ and $f_{\ell,t}$ are EL-equivalent, then $k=\ell$ and each of the linearized polynomials $L_1(X),L_2(X),L_3(Y),L_4(Y)$ is either a binomial, a monomial or zero.*

We will prove the result for $y = 0$, hence we only consider $L_1(X)$ and $L_2(X)$. By proceeding analogously, it can be shown that the statement also holds for $x = 0$ and the polynomials $L_3(Y)$ and $L_4(Y)$. Suppose $y = 0$. Then (5.12) and (5.13) can be reduced to

$$L_1(x)^{2^k+1} + \alpha L_2(x)^{(2^k+1)2^s} = N_1(x^{2^\ell+1}) + M_1(x), \tag{5.14}$$

$$L_1(x)L_2(x) = N_2(x^{2^\ell+1}) + M_2(x) \tag{5.15}$$

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

$$N_1(X) = \sum_{i=0}^{m-1} c_i X^{2^i} \qquad \text{and} \qquad N_2(X) = \sum_{i=0}^{m-1} d_i X^{2^i}.$$

Since $L(X, Y)$ needs to be a permutation polynomial, it is not possible that both $L_1(X)$ and $L_2(X)$ are zero. We first consider the case that one of $L_1(X)$ or $L_2(X)$ is zero. Assume $L_1(X) \neq 0$ and $L_2(X) = 0$. In this case, the left-hand side of (5.15) is zero, and it follows that $N_2(X) = M_2(X) = 0$. Moreover, (5.14) becomes

$$L_1(x)^{2^k+1} = N_1(x^{2^\ell+1}) + M_1(x), \tag{5.16}$$

which implies that the Gold APN functions $x \mapsto x^{2^k+1}$ and $x \mapsto x^{2^\ell+1}$ are EL-equivalent. According to Theorem 5.1, this holds if and only if $k = \ell$. It additionally follows from Theorem 5.1 that, as $m \geq 6$, the polynomial $L_1(X)$ is a linearized monomial. In summary, we obtain

$$L_1(X) = a_u X^{2^u} \qquad \text{and} \qquad L_2(X) = 0 \tag{5.17}$$

for some $u \in \{0, \dots, m-1\}$ and $a_u \in \mathbb{F}_{2^m}^*$. If we consider the case $L_1(X) = 0$ and $L_2(X) \neq 0$, we analogously obtain

$$L_1(X) = 0 \qquad \text{and} \qquad L_2(X) = b_u X^{2^u} \tag{5.18}$$

for some $u \in \{0, \dots, m-1\}$ and $b_u \in \mathbb{F}_{2^m}^*$. In both cases, $M_1(X) = M_2(X) = 0$.

Now, let both $L_1(X)$ and $L_2(X)$ be nonzero. Then (5.15) becomes

$$\sum_{i=0}^{m-1} a_i b_i x^{2^{i+1}} + \sum_{\substack{i,j=0,\\ j\neq i}}^{m-1} a_i b_j x^{2^i+2^j} = \sum_{i=0}^{m-1} d_i x^{(2^\ell+1)2^i} + M_2(x). \tag{5.19}$$

The first sum on the left-hand side of (5.19) is a linearized polynomial and the second sum does not contain linear parts. Hence, $M_2(X) = \sum_{i=0}^{m-1} a_i b_i X^{2^{i+1}}$. Omitting the linear parts, we rewrite (5.19) as

$$\sum_{0 \leq i < j \leq m-1} (a_i b_j + a_j b_i) x^{2^i+2^j} = \sum_{i=0}^{m-1} d_i x^{2^i+2^{i+\ell}}$$

and obtain

$$a_i b_{i+\ell} + a_{i+\ell} b_i = d_i \qquad \text{for all } i, \tag{5.20}$$

$$a_i b_j + a_j b_i = 0 \qquad \text{for } j \neq i, i \pm \ell, \tag{5.21}$$

where the subscripts are calculated modulo m. We separate the proof into two cases: first, the case that $d_i = 0$ for all $i = 0, \ldots, m-1$ and, second, the case that $d_u \neq 0$ for some $u \in \{0, \ldots, m-1\}$.

Case 1. In this case, we show that if $d_i = 0$ for all $i = 0, \ldots, m-1$, similarly to (5.16), the problem can be reduced to the Gold APN case. We will demonstrate that this implies $k = \ell$ and that $L_1(X)$ and $L_2(X)$ are monomials of the same degree.

Assume $d_i = 0$ for all $i = 0, \ldots, m-1$, which means $N_2(X) = 0$. In this case, (5.20) and (5.21) combine to

$$a_i b_j + a_j b_i = 0 \qquad \text{for } j \neq i. \tag{5.22}$$

As $L_1(X), L_2(X) \neq 0$, there exist $u, u' \in \{0, \ldots, m-1\}$ such that the coefficients $a_u, b_{u'}$ are nonzero. If $u = u'$, then the corresponding term $a_u b_u X^{2^{u+1}}$ is linearized. Hence, in (5.15), it is a part of $M_2(X)$, not of $N_2(X)$. If $u \neq u'$, then, by (5.22),

$$a_u b_{u'} + a_{u'} b_u = 0.$$

Consequently, $a_{u'}, b_u \neq 0$ and $a_u, a_{u'}, b_u, b_{u'}$ need to satisfy $\frac{a_u}{b_u} = \frac{a_{u'}}{b_{u'}}$. Define $\Delta = \frac{a_u}{b_u}$, and note that $\Delta \neq 0$. It follows from (5.22) that all pairs (a_j, b_j) satisfy either

$$a_j = b_j = 0 \qquad \text{or} \qquad \frac{a_j}{b_j} = \Delta. \tag{5.23}$$

Hence, $b_j = \delta a_j$, where $\delta = \frac{1}{\Delta}$, for all $j = 0, \ldots, m-1$, and $L_2(X)$ is a multiple of $L_1(X)$, namely

$$L_2(X) = \delta L_1(X). \tag{5.24}$$

Considering (5.15), it is obvious that $L_1(X)L_2(X) = \delta L_1(X)^2$ is a linearized polynomial, hence $N_2(X) = 0$ and $M_2(X) = \delta L_1(X)^2$.

Next, we plug $L_1(X)$ and $L_2(X) = \delta L_1(X)$ into (5.14) and obtain

$$L_1(x)^{2^k+1} + \alpha \delta^{(2^k+1)2^s} L_1(x)^{(2^k+1)2^s} = N_1(x^{2^\ell+1}) + M_1(x). \tag{5.25}$$

If $s = 0$, then (5.25) becomes

$$(1 + \alpha \delta^{(2^k+1)2^s}) L_1(x)^{2^k+1} = N_1(x^{2^\ell+1}) + M_1(x),$$

which again implies that the Gold APN functions $x \mapsto x^{2^k+1}$ and $x \mapsto x^{2^\ell+1}$ are EL-equivalent. According to Theorem 5.1, it follows that $k = \ell$ and that $L_1(X)$ is a monomial. Consequently, $L_2(X) = \delta L_1(X)$ is also a monomial, it has the same degree as $L_1(X)$.

If $s \neq 0$, we define a polynomial $T(X) \in \mathbb{F}_{2^m}[X]$ by

$$T(X) = X + \alpha\delta^{(2^k+1)2^s} X^{2^s}$$

and rewrite the left hand side of (5.25) as $T(L_1(x)^{2^k+1})$. We show that $T(X)$ is a permutation polynomial. Since $T(X)$ is linearized, it is sufficient to show that it has no nonzero root. If $T(X)$ had a nonzero root, it would solve the equation

$$\alpha^{-1} = \delta^{(2^k+1)2^s} x^{2^s-1}. \tag{5.26}$$

We show that this equation can never be true. Its left-hand side is obviously a non-cube. Since $\gcd(2^k+1, 2^m-1) = 3$, the first factor on the right-hand side, $\delta^{(2^k+1)2^s}$, is a cube. As $\gcd(2^s-1, 2^m-1) = 2^{\gcd(s,m)} - 1 = 2^{2\gcd(\frac{s}{2}, \frac{m}{2})} - 1$ is divisible by 3, the second factor, x^{2^s-1}, is also a cube. Hence, we have a cube on the right-hand side and a non-cube on the left-hand side of (5.26), which is a contradiction.

Denote by $T^{-1}(X)$ the inverse of $T(X)$ and rewrite (5.25) as

$$L_1(x)^{2^k+1} = T^{-1}(N_1(x^{2^\ell+1})) + T^{-1}(M_1(x)). \tag{5.27}$$

As $T^{-1}(X)$ is also linearized, (5.27) leads us to the equivalence problem of the Gold APN functions $x \mapsto x^{2^k+1}$ and $x \mapsto x^{2^\ell+1}$ again, and it follows from Theorem 5.1 that $k = \ell$ and that $L_1(X)$ is a monomial. Because of (5.24), $L_2(X)$ is also a monomial, it has the same degree as $L_1(X)$.

In summary, from Case 1, we obtain

$$L_1(X) = a_u X^{2^u} \qquad \text{and} \qquad L_2(X) = b_u X^{2^u}. \tag{5.28}$$

Moreover, $M_1(X) = 0$ and $M_2(X) = a_u b_u X^{2^{u+1}}$.

Case 2. Consider (5.20) and (5.21) again, and assume $d_u \neq 0$ for some $u \in \{0, \ldots, m-1\}$, which means $N_2(X) \neq 0$. We show that this assumption implies that $k = \ell$ and that $L_1(X)$ and $L_2(X)$ are either both monomials, but this time of different degrees 2^u and 2^{u+k}, or, for $s = 0$, are both binomials consisting of monomials of the same degrees 2^u and 2^{u+k} with some special conditions on the coefficients.

If $d_u \neq 0$ for some $u \in \{0, \ldots, m-1\}$, then, by (5.20), a_u and b_u cannot be zero at the same time. We will separate the proof of Case 2 into two subcases: first, Case 2.1, where both a_u and b_u are nonzero, and second, Case 2.2, where exactly one of a_u and b_u is nonzero. Both these cases will be separated into several subcases again.

Case 2.1. Assume $a_u \neq 0$ and $b_u \neq 0$. Then, from (5.21), it follows that all pairs (a_j, b_j) with $j \neq u, u \pm \ell$ satisfy (5.23). We first show that the only coefficients that are possibly nonzero are a_j, b_j for $j = u, u \pm \ell, u \pm 2\ell$.

By way of contradiction, suppose there exists $\ell' \neq 0, \pm\ell, \pm 2\ell$ such that $a_{u+\ell'}$ and $b_{u+\ell'}$ are nonzero. Considering (5.23), this implies $\frac{a_{u+\ell'}}{b_{u+\ell'}} = \Delta$. Since $u + \ell' \pm \ell \neq u \pm \ell$, it follows from (5.21) with $i = u + \ell'$ that both $(a_{u+\ell}, b_{u+\ell})$ and $(a_{u-\ell}, b_{u-\ell})$ also have to satisfy one of the equations in (5.23). Hence, (5.23) holds for all pairs (a_j, b_j) with $j = 0, \dots, m-1$, which means $L_2(X)$ is a multiple of $L_1(X)$. It now follows from (5.15) that $N_2(X) = 0$. This is a contradiction.

Hence, for the remainder of Case 2.1, suppose $a_j = b_j = 0$ for $j \neq u, u \pm \ell, u \pm 2\ell$. We separate Case 2.1 into two subcases. In Case 2.1.1, we assume $a_{u\pm 2\ell} = b_{u\pm 2\ell} = 0$, and we will see that provided $k = \ell$ and $s = 0$, there exist binomials $L_1(X)$ and $L_2(X)$ satisfying (5.14) and (5.15). In Case 2.1.2, we suppose that at least one of the coefficients $a_{u\pm 2\ell}, b_{u\pm 2\ell}$ is nonzero. This case will lead to a contradiction.

Case 2.1.1. Assume $a_{u\pm 2\ell} = b_{u\pm 2\ell} = 0$. In this case, we obtain only one equation from (5.21), namely

$$a_{u-\ell} b_{u+\ell} + a_{u+\ell} b_{u-\ell} = 0.$$

Hence, either

(i) $a_{u-\ell} = a_{u+\ell} = 0$ or $b_{u-\ell} = b_{u+\ell} = 0$, meaning that one of $L_1(X)$ and $L_2(X)$ is a monomial and the other one has at most three nonzero coefficients, or

(ii) $a_{u-\ell} = b_{u-\ell} = 0$ or $a_{u+\ell} = b_{u+\ell} = 0$, meaning that both $L_1(X)$ and $L_2(X)$ have at most two nonzero coefficients, or

(iii) $a_{u\pm\ell}, b_{u\pm\ell} \neq 0$ and $\frac{a_{u-\ell}}{b_{u-\ell}} = \frac{a_{u+\ell}}{b_{u+\ell}}$, meaning that both $L_1(X)$ and $L_2(X)$ are trinomials.

We will consider each of these three subcases separately.

Case 2.1.1. (i) Assume $b_{u-\ell} = b_{u+\ell} = 0$. The case $a_{u-\ell} = a_{u+\ell} = 0$ follows by symmetry. We consider polynomials

$$L_1(X) = a_{u-\ell} X^{2^{u-\ell}} + a_u X^{2^u} + a_{u+\ell} X^{2^{u+\ell}} \qquad \text{and} \qquad L_2(X) = b_u X^{2^u},$$

where a_u and b_u are nonzero. Moreover, we may assume that at least one of $a_{u-\ell}$ and $a_{u+\ell}$ is nonzero as otherwise $L_1(X)$ and $L_2(X)$ are monomials of the same degree implying $N_2(X) = 0$. This contradicts the assumption of Case 2.

We plug $L_1(X)$ and $L_2(X)$ into the left-hand side of (5.14) and obtain

$$\begin{aligned} L_1(x)^{2^k+1} &= a_{u-\ell}^{2^k+1} x^{2^{u-\ell}(2^k+1)} + a_u^{2^k+1} x^{2^u(2^k+1)} + a_{u+\ell}^{2^k+1} x^{2^{u+\ell}(2^k+1)} \\ &\quad + a_{u-\ell}^{2^k} a_u x^{2^u(2^{k-\ell}+1)} + a_u^{2^k} a_{u+\ell} x^{2^{u+\ell}(2^{k-\ell}+1)} \\ &\quad + a_{u+\ell}^{2^k} a_{u-\ell} x^{2^{u-\ell}(2^{k+2\ell}+1)} + a_{u-\ell}^{2^k} a_{u+\ell} x^{2^{u+\ell}(2^{k-2\ell}+1)} \\ &\quad + a_u^{2^k} a_{u-\ell} x^{2^{u-\ell}(2^{k+\ell}+1)} + a_{u+\ell}^{2^k} a_u x^{2^u(2^{k+\ell}+1)} \end{aligned} \tag{5.29}$$

and

$$\alpha L_2(x)^{2^s(2^k+1)} = \alpha b_u^{2^s(2^k+1)} x^{2^{s+u}(2^k+1)}. \tag{5.30}$$

Recall that the right-hand side of (5.14) is

$$\sum_{i=0}^{m-1} c_i x^{2^i(2^\ell+1)} + M_1(x).$$

We show that the first three summands of (5.29), whose exponents all contain the factor 2^k+1, cannot be canceled simultaneously. As $0 < \ell < \frac{m}{2}$, they cannot cancel each other. If $\ell = \frac{m}{2} - k$, the exponent of the sixth term contains the factor 2^k+1, it can be written as $2^{u-\frac{m}{2}}(2^k+1)$. However, by the same reasoning as above, this term cannot cancel any of the first three terms. The only possibility that one of these summands may be canceled is the following: if $\ell = k$, the seventh and the second term can be summarized and could potentially cancel each other. But since $a_{u-\ell}$ or $a_{u+\ell}$ is nonzero, for arbitrary k and ℓ, there is at least one term with a nonzero coefficient in (5.29) whose exponent contains the factor 2^k+1. Note that this term cannot be canceled by the term from (5.30): as m and s are even and $\gcd(\ell, m) = 1$, it follows that $s \not\equiv \pm\ell \pmod{m}$.

We now compare the left-hand side and the right-hand side of (5.14). Since the left-hand side contains a term of the shape $a_i x^{2^i(2^k+1)}$, it follows that $k = \ell$. Note that in this case, the fourth and fifth summand of (5.29) become linearized, hence

$$M_1(X) = a_{u-k}^{2^k} a_u X^{2^{u+1}} + a_u^{2^k} a_{u+k} X^{2^{u+k+1}}.$$

Now, consider the sixth, eighth and ninth summand of (5.29):

$$a_{u+k}^{2^k} a_{u-k} x^{2^{u-k}(2^{3k}+1)}, \qquad a_u^{2^k} a_{u-k} x^{2^{u-k}(2^{2k}+1)}, \qquad a_{u+k}^{2^k} a_u x^{2^u(2^{2k}+1)}.$$

As $m \geq 6$, we have $2k \not\equiv \pm k \pmod{m}$ and $3k \not\equiv \pm k \pmod{m}$. Hence, these terms cannot be represented in the form $c_i x^{2^i(2^k+1)}$, which means their coefficients have to be zero. As $a_u \neq 0$, it follows that $a_{u-k} = a_{u+k} = 0$. This is a contradiction.

Case 2.1.1. (ii) Assume $a_{u-\ell} = b_{u-\ell} = 0$. The case $a_{u+\ell} = b_{u+\ell} = 0$ follows by symmetry. In our case,

$$L_1(X) = a_u X^{2^u} + a_{u+\ell} X^{2^{u+\ell}} \qquad \text{and} \qquad L_2(X) = b_u X^{2^u} + b_{u+\ell} X^{2^{u+\ell}}.$$

As in Case 2.1.1. (i), a_u and b_u are nonzero, and we may assume that at least one of $a_{u+\ell}$ and $b_{u+\ell}$ is nonzero. For the left-hand side of (5.14), we obtain

$$\begin{aligned} L_1(x)^{2^k+1} = {} & a_u^{2^k+1} x^{2^u(2^k+1)} + a_{u+\ell}^{2^k+1} x^{2^{u+\ell}(2^k+1)} \\ & + a_u^{2^k} a_{u+\ell} x^{2^{u+\ell}(2^{k-\ell}+1)} + a_{u+\ell}^{2^k} a_u x^{2^u(2^{k+\ell}+1)}. \end{aligned} \tag{5.31}$$

and

$$\begin{aligned} \alpha L_2(x)^{2^s(2^k+1)} = {} & \alpha b_u^{2^s(2^k+1)} x^{2^{s+u}(2^k+1)} + \alpha b_{u+\ell}^{2^s(2^k+1)} x^{2^{s+u+\ell}(2^k+1)} \\ & + \alpha b_u^{2^{s+k}} b_{u+\ell}^{2^s} x^{2^{s+u+\ell}(2^{k-\ell}+1)} + \alpha b_{u+\ell}^{2^{s+k}} b_u^{2^s} x^{2^{s+u}(2^{k+\ell}+1)}. \end{aligned} \tag{5.32}$$

As in Case 2.1.1. (i), the first two terms of (5.31) and (5.32), respectively, cannot cancel each other. We separate the cases $s \neq 0$ and $s = 0$.

First, assume $s \neq 0$. As $s \not\equiv \pm\ell \pmod{m}$, the terms in (5.31) and in (5.32) cannot cancel each other if we add both expressions. Consequently, from comparing the left-hand side of (5.14) with its right-hand side, it follows that $k = \ell$. Using the same argument as in Case 2.1.1. (i), we obtain $a_{u+\ell} = b_{u+\ell} = 0$, which is a contradiction.

Next, assume $s = 0$. Now, the corresponding terms in (5.31) and (5.32) can be summarized. We show that the coefficient of the first summand,

$$(a_u^{2^k+1} + \alpha b_u^{2^k+1}) x^{2^u(2^k+1)}, \tag{5.33}$$

is nonzero. As $a_u, b_u \neq 0$, the coefficient is zero, if and only if

$$\alpha = \left(\frac{a_u}{b_u}\right)^{2^k+1}.$$

However, as $\gcd(2^k + 1, 2^m - 1) = 3$, this implies that α is a cube, which is a contradiction. Hence, the term from (5.33) occurs with a nonzero coefficient on the left-hand side of (5.14), and we need $k = \ell$ to represent it as $c_i x^{2^i(2^\ell+1)}$ on the right-hand side of (5.14). If $k = \ell$, the second term in the sum of (5.31) and (5.32) can also be represented in this way, and the third term is linearized, which means

$$M_1(X) = (a_u^{2^k} a_{u+k} + \alpha b_u^{2^k} b_{u+k}) X^{2^{u+k+1}}.$$

We consider the fourth summand:

$$\left(a_{u+k}^{2^k} a_u + \alpha b_{u+k}^{2^k} b_u\right) x^{2^u(2^{2k}+1)}.$$

As $2k \not\equiv \pm k \pmod{m}$, it cannot be represented as $c_i x^{2^i(2^k+1)}$. Hence, its coefficient has to be zero. As at least one of a_{u+k} and b_{u+k} is nonzero, this is only the case if

$$\left(\frac{a_u}{b_u}\right)\left(\frac{a_{u+k}}{b_{u+k}}\right)^{2^k} = \alpha. \tag{5.34}$$

Hence, for $s = 0$, we obtain binomials $L_1(X)$ and $L_2(X)$ of the form

$$L_1(X) = a_u X^{2^u} + a_{u+k} X^{2^{u+k}} \qquad \text{and} \qquad L_2(X) = b_u X^{2^u} + b_{u+k} X^{2^{u+k}}, \tag{5.35}$$

where the coefficients satisfy (5.34). This implies $\frac{a_u}{b_u} \neq \frac{a_{u+k}}{b_{u+k}}$ since otherwise, α would be a cube. Moreover, we obtain $M_1(X) = (a_u^{2^k} a_{u+k} + \alpha b_u^{2^k} b_{u+k}) X^{2^{u+k+1}}$ and $M_2(X) = a_u b_u X^{2^{u+1}} + a_{u+k} b_{u+k} X^{2^{u+k+1}}$.

Case 2.1.1. (iii) Now,

$$\begin{aligned} L_1(X) &= a_{u-\ell}X^{2^{u-\ell}} + a_u X^{2^u} + a_{u+\ell}X^{2^{u+\ell}} \\ \text{and } L_2(X) &= b_{u-\ell}X^{2^{u-\ell}} + b_u X^{2^u} + b_{u+\ell}X^{2^{u+\ell}}, \end{aligned}$$

where all coefficients are nonzero and $\frac{a_{u-\ell}}{b_{u-\ell}} = \frac{a_{u+\ell}}{b_{u+\ell}}$. We plug these polynomials into (5.14). Then $L_1(x)^{2^k+1}$ is as in (5.29), and $\alpha L_2(x)^{(2^k+1)2^s}$ looks basically the same: just replace a by b, multiply every coefficient by α and apply the automorphism $x \mapsto x^{2^s}$ on every summand. Furthermore, what we mentioned below (5.30) for the coefficients of $L_1(x)^{2^k+1}$ still holds, now for the coefficients of both $L_1(x)^{2^k+1}$ and $\alpha L_2(x)^{(2^k+1)2^s}$. As in Case 2.1.1. (ii), we separate the cases $s \neq 0$ and $s = 0$.

Assume $s \neq 0$. Like before, terms from $L_1(x)^{2^k+1}$ and from $\alpha L_2(x)^{(2^k+1)2^s}$ cannot cancel each other, and it follows that $k = \ell$. We obtain

$$M_1(X) = a_{u-k}^{2^k} a_u X^{2^{u+1}} + a_u^{2^k} a_{u+k} X^{2^{u+k+1}} + \alpha b_{u-k}^{2^{s+k}} b_u^{2^s} X^{2^{s+u+1}} + \alpha b_u^{2^{s+k}} a_{u+k}^{2^s} X^{2^{s+u+k+1}}.$$

By the same argument as in Case 2.1.1. (i), the sixth, eighth and ninth term of (5.29), which now contain the factors $x^{2^{3k}+1}$ or $x^{2^{2k}+1}$, cannot be represented as $x^{2^i(2^k+1)}$ on the right-hand side of (5.14). The same holds for the corresponding terms in $\alpha L_2(x)^{2^s(2^k+1)}$. As a consequence, the coefficients of these terms, which are

$$a_{u+k}^{2^k} a_{u-k},\ a_u^{2^k} a_{u-k},\ a_{u+k}^{2^k} a_u, \qquad \text{and} \qquad \alpha b_{u+k}^{2^{k+s}} b_{u-k}^{2^s},\ \alpha b_u^{2^{k+s}} b_{u-k}^{2^s},\ \alpha b_{u+k}^{2^{k+s}} b_u^{2^s},$$

have to be zero. As $a_u, b_u \neq 0$, it follows that $a_{u\pm k} = b_{u\pm k} = 0$, which contradicts our assumption that all coefficients are nonzero.

Now, suppose $s = 0$. In this case, we can summarize the corresponding terms of $L_1(x)^{2^k+1}$ and $\alpha L_2(x)^{2^s(2^k+1)}$ and obtain the same term as in (5.33) on the left-hand side of (5.14). By the same argument as in Case 2.1.1. (ii), it follows that $k = \ell$. Now, consider the term

$$(a_{u+k}^{2^k} a_{u-k} + \alpha b_{u+k}^{2^{k+s}} b_{u-k}^{2^s}) x^{2^{u-k}(2^{3k}+1)},$$

which, as $3k \not\equiv \pm k \pmod m$, cannot be represented as $c_i x^{2^i(2^k+1)}$. Hence, its coefficient has to be zero. As $a_{u\pm k}$ and $b_{u\pm k}$ are nonzero, this is only the case if

$$\left(\frac{a_{u-k}}{b_{u-k}}\right)\left(\frac{a_{u+k}}{b_{u+k}}\right)^{2^k} = \alpha.$$

However, as $\frac{a_{u-k}}{b_{u-k}} = \frac{a_{u+k}}{b_{u+k}}$ and $\gcd(2^k+1, 2^m-1) = 3$, this contradicts the condition that α is a non-cube. In summary, we cannot obtain possible polynomials $L_1(X)$ and $L_2(X)$ from Case 2.1.1. (iii).

Case 2.1.2. Now, assume $a_j = b_j = 0$ for $j \neq u, u \pm \ell, u \pm 2\ell$. Recall that all pairs (a_j, b_j) where $j \neq u, u \pm \ell$ have to satisfy (5.23). If $a_{u\pm 2\ell} = b_{u\pm 2\ell} = 0$, we are in Case 2.1.1. Hence, assume that $a_{u+2\ell}$ and $b_{u+2\ell}$ are nonzero. One can obtain an almost identical result by symmetry when assuming that $a_{u-2\ell}$ and $b_{u-2\ell}$ are nonzero.

If $a_{u+2\ell}, b_{u+2\ell} \neq 0$, then, by (5.23), $\frac{a_{u+2\ell}}{b_{u+2\ell}} = \Delta$. It follows from (5.21) that also $(a_{u-2\ell}, b_{u-2\ell})$ and $(a_{u-\ell}, b_{u-\ell})$ have to satisfy (5.23). However, (5.21) does not provide any restriction on the value of $(a_{u+\ell}, b_{u+\ell})$. If $(a_{u+\ell}, b_{u+\ell})$ satisfies (5.23), then all (a_j, b_j) do and we are in the case described at the beginning of Case 2.1. If $(a_{u+\ell}, b_{u+\ell})$ does not satisfy (5.23), then it follows from (5.21) that $a_j = b_j = 0$ for $j = u-\ell, u-2\ell$. Hence,

$$\begin{aligned} L_1(X) &= a_u X^{2^u} + a_{u+\ell} X^{2^{u+\ell}} + a_{u+2\ell} X^{2^{u+2\ell}} \\ \text{and } L_2(X) &= b_u X^{2^u} + b_{u+\ell} X^{2^{u+\ell}} + b_{u+2\ell} X^{2^{u+2\ell}}. \end{aligned}$$

As $\frac{a_u}{b_u} = \frac{a_{u+2\ell}}{b_{u+2\ell}}$, this case is similar to Case 2.1.1. (iii) when shifting all coefficients by ℓ, with the only difference that now exactly one of the middle coefficients $a_{u+\ell}$ and $b_{u+\ell}$ may be zero. However, the arguments used in Case 2.1.1. (iii) still hold. Consequently, Case 2.1.2 does not provide possible polynomials $L_1(X)$ and $L_2(X)$.

Case 2.2. Assume exactly one of a_u and b_u is nonzero. We show the case $a_u \neq 0$ and $b_u = 0$. The case $a_u = 0$ and $b_u \neq 0$ can be proved analogously. So, assume $a_u \neq 0$ and $b_u = 0$. From (5.20) with $i = u$, we then obtain the equation

$$a_u b_{u+\ell} = d_u.$$

As $d_u \neq 0$, it follows that $b_{u+\ell} \neq 0$. Moreover, from (5.21) with $i = u$, we obtain

$$a_u b_j = 0 \qquad \text{for } j \neq u, u \pm \ell.$$

Consequently, $b_j = 0$ for $j \neq u \pm \ell$. It now follows from (5.21) with $i = u + \ell$ that

$$a_j b_{u+\ell} = 0 \qquad \text{for } j \neq u-\ell, u, u+\ell, u+2\ell.$$

Consequently, $a_j = 0$ for $j \neq u-\ell, u, u+\ell, u+2\ell$.

We will separate the proof of Case 2.2 into two subcases: in Case 2.2.1, we consider $b_{u-\ell} \neq 0$, and in Case 2.2.2, we consider $b_{u-\ell} = 0$. Recall that $b_{u+\ell} \neq 0$.

Case 2.2.1. Suppose $b_{u-\ell} \neq 0$. From (5.21) with $i = u-\ell$ and $j = u+2\ell$, we obtain

$$a_{u+2\ell} b_{u-\ell} = 0,$$

which implies $a_{u+2\ell} = 0$. Moreover, for $i = u - \ell$ and $j = u + \ell$, we obtain

$$a_{u-\ell} b_{u+\ell} + a_{u+\ell} b_{u-\ell} = 0,$$

which, recalling that $b_{u+\ell}$ is nonzero, implies either $a_{u-\ell} = a_{u+\ell} = 0$ or $a_{u-\ell}, a_{u+\ell} \neq 0$ and $\frac{a_{u-\ell}}{b_{u-\ell}} = \frac{a_{u+\ell}}{b_{u+\ell}}$. We separate these two subcases:

Case 2.2.1. (i) Assume $a_{u-\ell} = a_{u+\ell} = 0$. Then

$$L_1(X) = a_u X^{2^u} \qquad \text{and} \qquad L_2(X) = b_{u-\ell} X^{2^{u-\ell}} + b_{u+\ell} X^{2^{u+\ell}},$$

where all coefficients are nonzero. We plug $L_1(X)$ and $L_2(X)$ into (5.14) and obtain on the left-hand side

$$L_1(x)^{2^k+1} = a_u^{2^k+1} x^{2^u(2^k+1)} \tag{5.36}$$

and

$$\begin{aligned} \alpha L_2(x)^{(2^k+1)2^s} &= \alpha b_{u-\ell}^{2^{s+k+1}} x^{2^{s+u-\ell}(2^k+1)} + \alpha b_{u+\ell}^{2^{s+k+1}} x^{2^{s+u+\ell}(2^k+1)} \\ &\quad + \alpha b_{u-\ell}^{2^{s+k}} b_{u+\ell}^{2^s} x^{2^{s+u+\ell}(2^{k-2\ell}+1)} + \alpha b_{u+\ell}^{2^{s+k}} b_{u-\ell}^{2^s} x^{2^{s+u-\ell}(2^{k+2\ell}+1)}. \end{aligned} \tag{5.37}$$

Recall that the right-hand side of (5.14) is

$$\sum_{i=0}^{m-1} c_i x^{2^i(2^\ell+1)} + M_1(x).$$

Since $s \not\equiv \pm\ell \pmod{m}$, the terms containing x^{2^k+1} cannot be canceled with each other. Hence, they can only be represented as $c_i x^{2^i(2^\ell+1)}$ if $k = \ell$. In this case, however, the last term of (5.37) contains $x^{2^{3k}+1}$, which cannot be represented in the form $c_i x^{2^i(2^k+1)}$ since $m \geq 6$ implies $3k \not\equiv \pm k \pmod{m}$. Consequently, the corresponding coefficient has to be zero, which implies that $b_{u-\ell} = 0$ or $b_{u+\ell} = 0$. This is a contradiction.

Case 2.2.1. (ii) Assume $a_{u-\ell}, a_{u+\ell} \neq 0$ and $\frac{a_{u-\ell}}{b_{u-\ell}} = \frac{a_{u+\ell}}{b_{u+\ell}}$. Then

$$\begin{aligned} L_1(X) &= a_{u-\ell} X^{2^{u-\ell}} + a_u X^{2^u} + a_{u+\ell} X^{2^{u+\ell}} \\ \text{and } L_2(X) &= b_{u-\ell} X^{2^{u-\ell}} + b_{u+\ell} X^{2^{u+\ell}}, \end{aligned}$$

where all coefficients are nonzero. We plug these polynomials into (5.14). Then $L_1(x)^{2^k+1}$ is as in (5.29) and $\alpha L_2(x)^{(2^k+1)2^s}$ is as in (5.37). Since $a_u^{2^k+1} x^{2^u(2^k+1)}$ can never be canceled by any of the terms in (5.37), it follows that $k = \ell$. However, now the expressions $a_u^{2^k} a_{u-k} x^{2^{u-k}(2^{2k}+1)}$ and $a_{u+k}^{2^k} a_u x^{2^u(2^{2k}+1)}$ occur on the left-hand side of (5.14), and they cannot be represented in the form $c_i x^{2^i(2^k+1)}$ on its right-hand side. As the corresponding coefficients are nonzero, this is a contradiction.

Case 2.2.2. Assume $b_{u-\ell} = 0$. Then, by (5.21) with $i = u + \ell$ and $j = u - \ell$, we have

$$a_{u-\ell} b_{u+\ell} = 0,$$

which implies $a_{u-\ell} = 0$. We obtain

$$L_1(X) = a_u X^{2^u} + a_{u+\ell} X^{2^{u+\ell}} + a_{u+2\ell} X^{2^{u+2\ell}} \qquad \text{and} \qquad L_2(X) = b_{u+\ell} X^{2^{u+\ell}},$$

where a_u and $b_{u+\ell}$ are nonzero. We consider (5.14) for these polynomials. The expression $L_1(x)^{2^k+1}$ is now similar to (5.29), we only need to replace u by $u+\ell$. Moreover,

$$\alpha L_2(x)^{(2^k+1)2^s} = b_{u+\ell}^{2^s(2^k+1)} x^{2^{s+u+l}(2^k+1)}.$$

Since terms containing $x^{2^u(2^k+1)}$ and $x^{2^{u+2\ell}(2^k+1)}$ cannot be canceled on the left-hand side of (5.14), but have to be represented on its right-hand side, it follows that $k=\ell$. If $k=\ell$, the summands

$$a_{u+2k}^{2^k} a_u x^{2^u(2^{3k}+1)}, \qquad a_{u+k}^{2^k} a_u x^{2^u(2^{2k}+1)}, \qquad a_{u+2k}^{2^k} a_{u+k} x^{2^{u+k}(2^{2k}+1)}$$

on the left-hand side cannot be represented as $c_i x^{2^i(2^k+1)}$ on the right-hand side. As $a_u \neq 0$, it follows that $a_{u+k} = a_{u+2k} = 0$. Consequently, $L_1(X)$ and $L_2(X)$ are monomials of the form

$$L_1(X) = a_u X^{2^u} \qquad \text{and} \qquad L_2(X) = b_{u+k} X^{2^{u+k}}, \tag{5.38}$$

and $M_1(X) = M_2(X) = 0$.

Note that if we consider Case 2.2 with $a_u = 0$ and $b_u \neq 0$, we obtain

$$L_1(X) = a_{u+k} X^{2^{u+k}} \qquad \text{and} \qquad L_2(X) = b_u X^{2^u} \tag{5.39}$$

and $M_1(X) = M_2(X) = 0$ from Case 2.2.2.

This concludes the proof of **Claim 5.1**. We summarize the results we have obtained so far. If the APN functions $f_{k,s}$ and $f_{\ell,t}$ are EL-equivalent, then $k=\ell$, and $L_1(X)$ and $L_2(X)$ are of the form

$$L_1(X) = a_u X^{2^u} + a_{u+k} X^{2^{u+k}} \qquad \text{and} \qquad L_2(X) = b_u X^{2^u} + b_{u+k} X^{2^{u+k}}$$

for some $u \in \{0, \ldots, m-1\}$. If $L_1(X)$ is a binomial, then, by (5.35), $L_2(X)$ is as well. Moreover, this case is only possible if $s=0$ and the coefficients of $L_1(X)$ and $L_2(X)$ satisfy (5.34). If $L_1(X)$ is a monomial of degree 2^u, then, $L_2(X)$ is either zero, see (5.17), or a monomial of degree 2^u or $2^{u\pm k}$, see (5.28), (5.38), and (5.39). If $L_1(X) = 0$, then, by (5.18), $L_2(X)$ is a monomial.

Vice versa, the same statements hold for $L_3(Y)$ and $L_4(Y)$, where

$$L_3(Y) = \overline{a}_w Y^{2^w} + \overline{a}_{w+k} Y^{2^{w+k}} \qquad \text{and} \qquad L_4(Y) = \overline{b}_w Y^{2^w} + \overline{b}_{w+k} Y^{2^{w+k}}$$

for some $w \in \{0, \ldots, m-1\}$.

It remains to show that EL-equivalence of $f_{k,s}$ and $f_{k,t}$ implies $s=t$. Combining the results on $L_1(X), \ldots, L_4(X)$ we mentioned above, the following combinations of $L_A(X,Y) = L_1(X) + L_3(Y)$ and $L_B(X,Y) = L_2(X) + L_4(Y)$ are possible:

(a) $L_A(X,Y) = a_u X^{2^u} + a_{u+k} X^{2^{u+k}} + \overline{a}_w Y^{2^w} + \overline{a}_{w+k} Y^{2^{w+k}}$
and $L_B(X,Y) = b_u X^{2^u} + b_{u+k} X^{2^{u+k}} + \overline{b}_w Y^{2^w} + \overline{b}_{w+k} Y^{2^{w+k}}$,

(b) $L_A(X,Y) = a_u X^{2^u} + a_{u+k} X^{2^{u+k}} + \overline{a}_w Y^{2^w}$ and $L_B(X,Y) = b_u X^{2^u} + b_{u+k} X^{2^{u+k}} + \overline{b}_w Y^{2^w}$,

(c) $L_A(X,Y) = a_u X^{2^u} + a_{u+k} X^{2^{u+k}} + \overline{a}_w Y^{2^w}$ and $L_B(X,Y) = b_u X^{2^u} + b_{u+k} X^{2^{u+k}} + \overline{b}_{w+k} Y^{2^{w+k}}$,

(d) $L_A(X,Y) = a_u X^{2^u} + a_{u+k} X^{2^{u+k}} + \overline{a}_{w+k} Y^{2^{w+k}}$ and $L_B(X,Y) = b_u X^{2^u} + b_{u+k} X^{2^{u+k}} + \overline{b}_w Y^{2^w}$,

(e) $L_A(X,Y) = a_u X^{2^u} + \overline{a}_w Y^{2^w} + \overline{a}_{w+k} Y^{2^{w+k}}$ and $L_B(X,Y) = b_u X^{2^u} + \overline{b}_w Y^{2^w} + \overline{b}_{w+k} Y^{2^{w+k}}$,

(f) $L_A(X,Y) = a_u X^{2^u} + \overline{a}_w Y^{2^w} + \overline{a}_{w+k} Y^{2^{w+k}}$ and $L_B(X,Y) = b_{u+k} X^{2^{u+k}} + \overline{b}_w Y^{2^w} + \overline{b}_{w+k} Y^{2^{w+k}}$,

(g) $L_A(X,Y) = a_{u+k} X^{2^{u+k}} + \overline{a}_w Y^{2^w} + \overline{a}_{w+k} Y^{2^{w+k}}$ and $L_B(X,Y) = b_u X^{2^u} + \overline{b}_w Y^{2^w} + \overline{b}_{w+k} Y^{2^{w+k}}$,

(h) $L_A(X,Y) = a_u X^{2^u} + \overline{a}_w Y^{2^w}$ and $L_B(X,Y) = b_u X^{2^u} + \overline{b}_w Y^{2^w}$,

(i) $L_A(X,Y) = a_u X^{2^u} + \overline{a}_w Y^{2^w}$ and $L_B(X,Y) = b_u X^{2^u} + \overline{b}_{w+k} Y^{2^{w+k}}$,

(j) $L_A(X,Y) = a_u X^{2^u} + \overline{a}_{w+k} Y^{2^{w+k}}$ and $L_B(X,Y) = b_u X^{2^u} + \overline{b}_w Y^{2^w}$,

(k) $L_A(X,Y) = a_u X^{2^u} + \overline{a}_w Y^{2^w}$ and $L_B(X,Y) = b_{u+k} X^{2^{u+k}} + \overline{b}_w Y^{2^w}$,

(l) $L_A(X,Y) = a_{u+k} X^{2^{u+k}} + \overline{a}_w Y^{2^w}$ and $L_B(X,Y) = b_u X^{2^u} + \overline{b}_w Y^{2^w}$,

(m) $L_A(X,Y) = a_u X^{2^u} + \overline{a}_w Y^{2^w}$ and $L_B(X,Y) = b_{u+k} X^{2^{u+k}} + \overline{b}_{w+k} Y^{2^{w+k}}$,

(n) $L_A(X,Y) = a_u X^{2^u} + \overline{a}_{w+k} Y^{2^{w+k}}$ and $L_B(X,Y) = b_{u+k} X^{2^{u+k}} + \overline{b}_w Y^{2^w}$,

(o) $L_A(X,Y) = a_{u+k} X^{2^{u+k}} + \overline{a}_w Y^{2^w}$ and $L_B(X,Y) = b_u X^{2^u} + \overline{b}_{w+k} Y^{2^{w+k}}$,

(p) $L_A(X,Y) = a_{u+k} X^{2^{u+k}} + \overline{a}_{w+k} Y^{2^{w+k}}$ and $L_B(X,Y) = b_u X^{2^u} + \overline{b}_w Y^{2^w}$.

Note that, as $L(X,Y) = (L_A(X,Y), L_B(X,Y))$ has to be a permutation polynomial, it is neither possible that $L_A(X,Y)$ or $L_B(X,Y)$ is zero nor that both $L_A(X,Y)$ and $L_B(X,Y)$ depend only on X or only on Y. We will show that all cases listed above either lead to a contradiction or to the conclusion that $s = t$ and $L_A(X,Y)$ and $L_B(X,Y)$ need to be monomials of the same degree.

Considering that, according to Claim 5.1, EL-equivalence of $f_{k,s}$ and $f_{\ell,t}$ implies $k = \ell$, we rewrite (5.12) and (5.13) as

$$\begin{aligned} L_A(x,y)^{2^k+1} \; + \; & \alpha L_B(x,y)^{(2^k+1)2^s} \\ & = N_1(x^{2^k+1} + \alpha y^{(2^k+1)2^t}) + N_3(xy) + M_A(x,y), \end{aligned} \tag{5.40}$$

$$L_A(x,y) L_B(x,y) = N_2(x^{2^k+1} + \alpha y^{(2^k+1)2^t}) + N_4(xy) + M_B(x,y). \tag{5.41}$$

We will check for all the possible combinations **(a)**–**(p)** if (5.40) and (5.41) can hold. We begin with cases **(a)**–**(g)**. Note that in these cases, $L_1(X)$ and $L_2(X)$ or $L_3(Y)$ and $L_4(Y)$ are binomials. Hence, these cases require $s = 0$, and the coefficients of the binomials are nonzero and have to satisfy (5.34).

We first consider **(c)**. As $L_1(X)$ and $L_2(X)$ are binomials, the coefficients a_u, a_{u+k}, b_u and b_{u+k} are nonzero. If we plug the polynomials of **(c)** into the left-hand side of (5.41), we obtain

$$\begin{aligned} L_A(x,y)L_B(x,y) = {} & a_u b_u x^{2^{u+1}} + a_{u+k} b_{u+k} x^{2^{u+k+1}} \\ & + (a_u b_{u+k} + a_{u+k} b_u) x^{2^u(2^k+1)} + \overline{a}_w \overline{b}_{w+k} y^{2^w(2^k+1)} \\ & + a_u \overline{b}_{w+k} x^{2^u} y^{2^{w+k}} + a_{u+k} \overline{b}_{w+k} x^{2^{u+k}} y^{2^{w+k}} \\ & + b_u \overline{a}_w x^{2^u} y^{2^w} + b_{u+k} \overline{a}_w x^{2^{u+k}} y^{2^w}. \end{aligned} \tag{5.42}$$

Note that the first and the second term of (5.42) are linearized. We focus on the last four summands. At least one of $\overline{a}_w$ and $\overline{b}_{w+k}$ needs to be nonzero, as otherwise $L(X,Y)$ is no permutation polynomial. Consequently, (5.42) must contain the fifth and the sixth or the seventh and the eighth summand. However, no matter how we choose u and w, we can never represent $x^{2^u} y^{2^{w+k}}$ and $x^{2^{u+k}} y^{2^{w+k}}$ or $x^{2^u} y^{2^w}$ and $x^{2^{u+k}} y^{2^w}$ simultaneously in the form $x^{2^i} y^{2^i}$ on the right-hand side of (5.41). Hence, **(c)** leads to a contradiction. Similar arguments also lead to contradictions in cases **(d)**, **(f)** and **(g)**.

We next consider **(b)**. Recall that, in this case, a_u, a_{u+k}, b_u and b_{u+k} are nonzero and, by the arguments below (5.35), satisfy $\frac{a_u}{b_u} \neq \frac{a_{u+k}}{b_{u+k}}$. Plugging $L_A(X,Y)$ and $L_B(X,Y)$ into (5.41), we obtain on the left-hand side

$$\begin{aligned} L_A(x,y)L_B(x,y) = {} & a_u b_u x^{2^{u+1}} + a_{u+k} b_{u+k} x^{2^{u+k+1}} \\ & + (a_u b_{u+k} + a_{u+k} b_u) x^{2^u(2^k+1)} + \overline{a}_w \overline{b}_w y^{2^{w+1}} \\ & + (a_u \overline{b}_w + b_u \overline{a}_w) x^{2^u} y^{2^w} + (a_{u+k} \overline{b}_w + b_{u+k} \overline{a}_w) x^{2^{u+k}} y^{2^w}. \end{aligned} \tag{5.43}$$

Now the first, second and fourth term of (5.43) are linearized. Note that the coefficient $a_u b_{u+k} + a_{u+k} b_u$ of the third term of (5.43) is nonzero, as otherwise $\frac{a_u}{b_u} = \frac{a_{u+k}}{b_{u+k}}$. To represent this term on the right-hand side of (5.41), we need $N_2(X) \neq 0$. This implies that there is a term containing the factor $\alpha^{2^i} y^{2^{t+i}(2^k+1)}$ on the right-hand of (5.41). However, there is no corresponding term on the left-hand side, see (5.43). This is a contradiction. By proceeding analogously, we obtain a similar contradiction in case **(e)**.

Next, consider **(a)**. Recall that this case is only possible for $s = 0$. Since in this case, $L_1(X), \dots, L_4(X)$ are binomials, all the coefficients of $L_A(X,Y)$ and $L_B(X,Y)$ have to be nonzero and satisfy the inequalities $\frac{a_u}{b_u} \neq \frac{a_{u+k}}{b_{u+k}}$ and $\frac{\overline{a}_w}{\overline{b}_w} \neq \frac{\overline{a}_{w+k}}{\overline{b}_{w+k}}$ as shown below (5.35). If we plug $L_A(X,Y)$ and $L_B(X,Y)$ into (5.41), the following four terms occur on the left-hand side of this equation:

$$\begin{aligned} &(a_u\overline{b}_w + b_u\overline{a}_w)x^{2^u}y^{2^w}, \quad (a_u\overline{b}_{w+k} + b_u\overline{a}_{w+k})x^{2^u}y^{2^{w+k}}, \\ \text{and} \quad &(a_{u+k}\overline{b}_w + b_{u+k}\overline{a}_w)x^{2^{u+k}}y^{2^w}, \quad (a_{u+k}\overline{b}_{w+k} + b_{u+k}\overline{a}_{w+k})x^{2^{u+k}}y^{2^{w+k}}. \end{aligned} \tag{5.44}$$

We show that the coefficients of the second and the third term have to be zero. Suppose, the coefficient of the second term is nonzero. Then we need $u = w + k$ to represent it on the right-hand side of (5.41). It is easy to see that now none of the other terms in (5.44) can be represented on the right-hand side of (5.41), which means their coefficients have to be zero. However, if all three coefficients are zero, it follows that $\frac{a_u}{b_u} = \frac{a_{u+k}}{b_{u+k}} = \frac{\overline{a}_w}{\overline{b}_w} = \frac{\overline{a}_{w+k}}{\overline{b}_{w+k}}$. This is a contradiction. Analogously, the assumption that the third term does not vanish leads to the same contradiction.

Hence, assume $\frac{a_u}{b_u} = \frac{\overline{a}_{w+k}}{\overline{b}_{w+k}}$ and $\frac{a_{u+k}}{b_{u+k}} = \frac{\overline{a}_w}{\overline{b}_w}$. Then the second and third term of (5.44) vanish, and the coefficients of the first and the fourth term are nonzero. If we now compare the left-hand side and the right-hand side of (5.41), it follows that $u = w$. Next, we use (5.40). On the left-hand side of (5.40), we obtain the summand

$$(a_{u+k}^{2^k}\overline{a}_u + \alpha b_{u+k}^{2^k}\overline{b}_u)x^{2^{u+2k}}y^{2^u},$$

which cannot be represented on the corresponding right-hand side. Consequently, its coefficient has to be zero, which implies

$$\alpha = \frac{a_{u+k}^{2^k}\overline{a}_u}{b_{u+k}^{2^k}\overline{b}_u}.$$

However, as $\frac{\overline{a}_u}{\overline{b}_u} = \frac{a_{u+k}}{b_{u+k}}$ and $\gcd(2^k + 1, 2^m - 1) = 3$, this implies that α is a cube. Hence, case **(a)** leads to a contradiction.

We next study the cases **(h)**–**(p)**, where $L_1(X), \ldots, L_4(X)$ are monomials. We consider **(i)** first. If $L_A(X,Y)$ and $L_B(X,Y)$ are as in **(i)**, the left-hand side of (5.41) is

$$\begin{aligned} L_A(x,y)L_B(x,y) = a_u b_u x^{2^{u+1}} &+ \overline{a}_w\overline{b}_{w+k}y^{2^w(2^k+1)} \\ &+ a_u\overline{b}_{w+k}x^{2^u}y^{2^{w+k}} + b_u\overline{a}_w x^{2^u}y^{2^w}. \end{aligned} \tag{5.45}$$

The first term of (5.45) is linearized. Since (5.45) does not contain a term with x^{2^k+1}, we need $N_2(X) = 0$ on the right-hand side of (5.41). It follows that the second summand of (5.45) cannot be represented on the right-hand side of (5.41), which means $\overline{a}_w$ or $\overline{b}_{w+k}$ has to be zero.

Case 1. Suppose $\overline{a}_w = 0$. Note that this implies $a_u \neq 0$ and $\overline{b}_{w+k} \neq 0$ as otherwise $L(X,Y)$ would not be a permutation polynomial. If $\overline{a}_w = 0$, the fourth summand of (5.45) vanishes, and the third summand can only be represented on the right-hand side of (5.41) if $u = w + k$. We consider the left-hand side of (5.40) with $u = w + k$

and obtain

$$\begin{aligned} &L_A(x,y)^{2^k+1} + \alpha L_B(x,y)^{(2^k+1)2^s} \\ &\quad = a_u^{2^k+1} x^{2^u(2^k+1)} + \alpha b_u^{2^s(2^k+1)} x^{2^{u+s}(2^k+1)} + \alpha \bar{b}_u^{2^s(2^k+1)} y^{2^{u+s}(2^k+1)} \\ &\qquad + \alpha b_u^{2^{k+s}} \bar{b}_u^{2^s} x^{2^{u+k+s}} y^{2^{u+s}} + \alpha \bar{b}_u^{2^{k+s}} b_u^{2^s} x^{2^{u+s}} y^{2^{u+k+s}}. \end{aligned} \tag{5.46}$$

The fourth and the fifth summand of (5.46) cannot be canceled by any of the other terms, and they cannot be represented on the right-hand side of (5.40). As $\alpha, \bar{b}_u \neq 0$, it follows that $b_u = 0$. This means, $L_A(X,Y)$ and $L_B(X,Y)$ are monomials of the same degree,

$$L_A(X,Y) = a_u X^{2^u} \qquad \text{and} \qquad L_B(X,Y) = \bar{b}_u Y^{2^u}. \tag{5.47}$$

Case 2. Suppose $\bar{b}_{w+k} = 0$. By the same arguments as above, this implies $b_u \neq 0$ and $\bar{a}_w \neq 0$. Now (5.45) holds for $u = w$. We consider (5.40) with $u = w$:

$$\begin{aligned} L_A(x,y)^{2^k+1} + \alpha L_B(x,y)^{(2^k+1)2^s} &= a_u^{2^k+1} x^{2^u(2^k+1)} + \bar{a}_u^{2^k+1} y^{2^u(2^k+1)} \\ &\quad + a_u^{2^k} \bar{a}_u x^{2^k} y + \bar{a}_u^{2^k} a_u x y^{2^k} \\ &\quad + \alpha b_u^{2^s(2^k+1)} x^{2^{u+s}(2^k+1)} \end{aligned} \tag{5.48}$$

Now, the third and the fourth summand of (5.48) cannot be represented on the right-hand side of (5.40). As $\bar{a}_u \neq 0$, it follows that $a_u = 0$. Consequently, $L_A(X,Y)$ and $L_B(X,Y)$ are monomials of the same degree,

$$L_A(X,Y) = \bar{a}_u Y^{2^u} \qquad \text{and} \qquad L_B(X,Y) = b_u X^{2^u}. \tag{5.49}$$

By symmetry, the same results can be obtained from cases **(j)**–**(l)**.

We study **(m)** next. With $L_A(X,Y)$ and $L_B(X,Y)$ from **(m)**, the left-hand side of (5.41) becomes

$$\begin{aligned} L_A(x,y)L_B(x,y) &= a_u b_{u+k} x^{2^u(2^k+1)} + \bar{a}_w \bar{b}_{w+k} y^{2^w(2^k+1)} \\ &\quad + a_u \bar{b}_{w+k} x^{2^u} y^{2^{w+k}} + \bar{a}_w b_{u+k} x^{2^{u+k}} y^{2^w}. \end{aligned} \tag{5.50}$$

As $k \not\equiv \pm k$, the third and the fourth term of (5.50) cannot be represented simultaneously in the shape $x^{2^i} y^{2^i}$ on the right-hand side of (5.41). Consequently, at least one of $a_u, b_{u+k}, \bar{a}_w$ and $\bar{b}_{w+k}$ needs to be zero.

Suppose $a_u = 0$, which implies $\bar{a}_w$ and b_{u+k} are nonzero. Now the first term of (5.50) vanishes. It follows that $N_2(X) = 0$. Hence, we cannot represent the second term of (5.50) on the right-hand side of (5.41), and we need $\bar{b}_{w+k} = 0$. The only remaining term of (5.50) is the fourth one. To represent it on the right-hand side of (5.41), we need $w = u + k$. Consequently $L_A(X,Y)$ and $L_B(X,Y)$ are monomials of the same degree as in (5.49). We obtain the same result if we assume $\bar{b}_{w+k} = 0$. When supposing $b_{u+k} = 0$ or $\bar{a}_w = 0$, we obtain that $L_A(X,Y)$ and $L_B(X,Y)$ are monomials of the same degree as in (5.47). By symmetry, **(p)** leads to identical results.

We consider **(n)**. If we plug $L_A(X, Y)$ and $L_B(X, Y)$ of **(n)** into (5.41), the left-hand side becomes

$$\begin{aligned} L_A(x,y)L_B(x,y) = a_u b_{u+k} x^{2^u(2^k+1)} &+ \overline{a}_{w+k}\overline{b}_w y^{2^w(2^k+1)} \\ &+ a_u\overline{b}_w x^{2^u} y^{2^w} + b_{u+k}\overline{a}_{w+k} x^{2^{u+k}} y^{2^{w+k}}. \end{aligned} \tag{5.51}$$

Clearly, the third and the fourth term cannot vanish simultaneously since otherwise $L(X, Y)$ would not be a permutation polynomial. To represent the third or the fourth term on the right-hand side of (5.41), we need $u = w$. We plug $L_A(X, Y)$ and $L_B(X, Y)$ with $u = w$ into (5.40). The left-hand side of (5.40) then contains the two summands

$$a_u\overline{a}_{u+k}^{2^k} x^{2^u} y^{2^{u+2k}} \qquad \text{and} \qquad \alpha b_{u+k}^{2^{s+k}} \overline{b}_u^{2^s} x^{2^{s+u+2k}} y^{2^{s+u}},$$

which neither can be canceled, nor can be represented on the right-hand side of (5.40). Consequently, one of a_u and $\overline{a}_{u+k}$ and one of b_{u+k} and $\overline{b}_u$ have to be zero, which means that $L_A(X, Y)$ and $L_B(X, Y)$ are monomials. The only combinations so that $L(X, Y)$ is a permutation polynomial are $L_A(X, Y)$ and $L_B(X, Y)$ as in (5.47) or (5.49). By symmetry, we obtain the same result for case **(o)**.

Eventually, we study **(h)**: For this case, we obtain

$$L_A(x,y)L_B(x,y) = a_u b_u x^{2^{u+1}} + \overline{a}_w\overline{b}_w y^{2^{w+1}} + (a_u\overline{b}_w + b_u\overline{a}_w) x^{2^u} y^{2^w} \tag{5.52}$$

on the left-hand side of (5.41). We consider two cases: in Case 1, the third term of (5.52) vanishes, in Case 2, its coefficient is nonzero.

Case 1. Suppose $a_u, b_u, \overline{a}_w$ and $\overline{b}_w$ are nonzero and satisfy $\frac{a_u}{b_u} = \frac{\overline{a}_w}{\overline{b}_w}$. Note that this is the only possibility such that $a_u\overline{b}_w + b_u\overline{a}_w = 0$ as $a_u\overline{b}_w = b_u\overline{a}_w = 0$ implies that $L(X, Y)$ is not a permutation polynomial. In our case, the left-hand side of (5.41) is a linearized polynomial, and it follows that $N_2(X) = N_4(X) = 0$.

We plug $L_A(X, Y)$ and $L_B(X, Y)$ into (5.40). Then the left-hand side of (5.40) contains the four summands

$$\begin{aligned} &a_u^{2^k}\overline{a}_w x^{2^{u+k}} y^{2^w}, \quad \alpha b_u^{2^{k+s}} \overline{b}_w^{2^s} x^{2^{s+u+k}} y^{2^{s+w}} \\ \text{and} \quad &a_u\overline{a}_w^{2^k} x^{2^u} y^{2^{w+k}}, \quad \alpha b_u^{2^s} \overline{b}_w^{2^{s+k}} x^{2^{s+u}} y^{2^{s+w+k}}. \end{aligned} \tag{5.53}$$

If $s \neq 0$, these terms cannot be represented on the right-hand side of (5.40). Hence, the corresponding coefficients need to be zero, which is a contradiction. If $s = 0$, we can summarize the terms of (5.53) and obtain

$$(a_u^{2^k}\overline{a}_w + \alpha b_u^{2^k}\overline{b}_w) x^{2^{u+k}} y^{2^w} \qquad \text{and} \qquad (a_u\overline{a}_w^{2^k} + \alpha b_u\overline{b}_w^{2^k}) x^{2^u} y^{2^{w+k}}. \tag{5.54}$$

The coefficients of these terms are zero if both

$$\alpha = \frac{a_u^{2^k}\overline{a}_w}{b_u^{2^k}\overline{b}_w} \qquad \text{and} \qquad \alpha = \frac{a_u\overline{a}_w^{2^k}}{b_u\overline{b}_w^{2^k}} \tag{5.55}$$

hold. As $\frac{a_u}{b_u} = \frac{\overline{a}_w}{\overline{b}_w}$, both equations are identical and we obtain

$$\alpha = \left(\frac{a_u}{b_u}\right)^{2^k+1}.$$

Since $\gcd(2^k+1, 2^m-1) = 3$, this implies α is a cube, which is a contradiction.

Case 2. Now, assume $a_u\overline{b}_w + b_u\overline{a}_w \neq 0$. We need $u = w$ to represent the third term of (5.52) on the right-hand side of (5.41). Assuming $u = w$, we plug $L_A(X,Y)$ and $L_B(X,Y)$ into (5.40). Then its left-hand side contains the summands from (5.53), where $u = w$.

As in Case 1, if $s \neq 0$, these terms cannot be represented on the right-hand side of (5.40). Hence, either a_u and $\overline{b}_u$ or $\overline{a}_u$ and b_u need to be zero, which implies that $L_A(X,Y)$ and $L_B(X,Y)$ are monomials of the same degree as in (5.47) and (5.49). If $s = 0$, the results from the case $s \neq 0$ are also possible. But additionally, we can summarize the terms from (5.53) in the same way as in (5.54) with $u = w$. The coefficients of these terms are zero if both equations from (5.55) with $u = w$ hold. This is only the case if

$$\left(\frac{a_u\overline{b}_u}{b_u\overline{a}_u}\right)^{2^k-1} = 1. \tag{5.56}$$

Since k and m are coprime, we obtain $\gcd(2^k-1, 2^m-1) = 2^{\gcd(k,m)} - 1 = 1$. Consequently, (5.56) implies $\frac{a_u}{b_u} = \frac{\overline{a}_u}{\overline{b}_u}$. As $u = w$, this contradicts our assumption $\frac{a_u}{b_u} \neq \frac{\overline{a}_w}{\overline{b}_w}$.

In summary, the only possible choices for $L_A(X,Y)$ and $L_B(X,Y)$ are that both polynomials are monomials of the same degree as in (5.47) or (5.49). We will show that both cases imply $s = t$.

First, consider $L_A(X,Y) = a_uX^{2^u}$ and $L_B(X,Y) = \overline{b}_uY^{2^u}$. It follows from (5.41) that, in this case, $N_2(X) = 0$, $N_4(X) = a_u\overline{b}_uX^{2^u}$, and $M_B(X,Y) = 0$. Plugging $L_A(X,Y)$ and $L_B(X,Y)$ into (5.40), we obtain

$$\begin{aligned} &(a_ux^{2^u})^{2^k+1} + \alpha(\overline{b}_uy^{2^u})^{(2^k+1)2^s} \\ &\qquad = N_1(x^{2^k+1} + \alpha y^{(2^k+1)2^t}) + N_3(xy) + M_A(x,y). \end{aligned} \tag{5.57}$$

Clearly, $M_A(X,Y) = 0$ and $N_3(X) = 0$. Moreover, $N_1(X)$ has to be a monomial of degree 2^u, and $s = t$. Writing $N_1(X) = c_uX^{2^u}$ and considering $s = t$, (5.57) becomes

$$a_u^{2^k+1}x^{2^u(2^k+1)} + \alpha\overline{b}_u^{2^s(2^k+1)}y^{2^{s+u}(2^k+1)} = c_ux^{2^u(2^k+1)} + \alpha^{2^u}c_uy^{2^{s+u}(2^k+1)}.$$

It follows that the coefficients have to satisfy the equations

$$a_u^{2^k+1} = c_u \qquad \text{and} \qquad \alpha \bar{b}_u^{2^s(2^k+1)} = \alpha^{2^u} c_u. \tag{5.58}$$

Clearly, we can find admissible coefficients.

Next, we consider $L_A(X,Y) = \bar{a}_u Y^{2^u}$ and $L_B(X,Y) = b_u X^{2^u}$. Now, (5.41) implies $N_2(X) = 0$, $N_4(X) = b_u \bar{a}_u X^{2^u}$, and $M_B(X,Y) = 0$. Moreover, (5.40) becomes

$$\begin{aligned}(\bar{a}_u y^{2^u})^{2^k+1} &+ \alpha(b_u x^{2^u})^{(2^k+1)2^s} \\ &= N_1(x^{2^k+1} + \alpha y^{(2^k+1)2^t}) + N_3(xy) + M_A(x,y).\end{aligned} \tag{5.59}$$

It follows that $M_A(X,Y) = 0$ and $N_3(X) = 0$. Moreover, $N_1(X)$ has to be a monomial of degree 2^{u+s}, and we need $s + t \equiv 0 \pmod{m}$. As $0 \le s, t \le \frac{m}{2}$, this congruence only holds for $s = t = 0$ and $s = t = \frac{m}{2}$. Writing $N_1(X) = c_{u+s} X^{2^{u+s}}$ and considering $s = t = 0$ or $\frac{m}{2}$, (5.59) becomes

$$\alpha b_u^{2^s(2^k+1)} x^{2^{s+u}(2^k+1)} + \bar{a}_u^{2^k+1} y^{2^u(2^k+1)} = c_{u+s} x^{2^{s+u}(2^k+1)} + \alpha^{2^{u+s}} c_{u+s} y^{2^u(2^k+1)}.$$

Consequently, the coefficients have to meet the conditions

$$\alpha b_u^{2^s(2^k+1)} = c_{u+s} \qquad \text{and} \qquad \bar{a}_u^{2^k+1} = \alpha^{2^{u+s}} c_{u+s}. \tag{5.60}$$

As before, we can find admissible coefficients. This concludes our proof. □

In Theorem 5.15, we will take a closer look at the coefficients satisfying (5.58) and (5.60), respectively, to determine the automorphism groups of Zhou-Pott functions under EL- and EA-equivalence. In Corollary 5.20, we use Theorem 5.4 to determine the exact number of inequivalent Zhou-Pott functions.

5.3 Equivalence of Carlet APN functions

In this section, we add a few results about the equivalence relations of Carlet APN functions from Proposition 4.5. In Theorem 5.8, we show that for even m, any Carlet APN function on $\mathbb{F}_{2^{2m}}$ is EL-equivalent to a Zhou-Pott APN function from Theorem 4.6. From this result, we determine the equivalence of Carlet APN functions on $\mathbb{F}_{2^{2m}}$ where m is even. Note that we do not consider the case that m is odd in this thesis.

First, we need the following three results. In Lemma 5.5, we summarize several observations about polynomials of the shape $X^{2^k+1} + \alpha X + \beta$ that may be well known.

Lemma 5.5. *Let $m \ge 2$ and $k < m$ be positive integers, and let $\alpha, \beta \in \mathbb{F}_{2^m}^*$.*

(a) The polynomial $P(X) = X^{2^k+1} + \alpha X + \beta$ has no root in $\mathbb{F}_{2^m}$ if and only if $P'(X) = X^{2^k+1} + X + \frac{\beta}{\alpha^{2^{-k}+1}}$ has no root in $\mathbb{F}_{2^m}$.

(b) *The polynomial* $P(X) = X^{2^k+1} + X + \beta$ *has no root in* $\mathbb{F}_{2^m}$ *if and only if* $P'(X) = X^{2^k+1} + X + \beta^{2^i}$ *has no root in* $\mathbb{F}_{2^m}$ *for* $i \in \{0, \dots, m-1\}$*.*

(c) *The polynomial* $P(X) = X^{2^k+1} + X + \beta$ *has no root in* $\mathbb{F}_{2^m}$ *if and only if* $P'(X) = X^{2^{-k}+1} + X + \beta$ *has no root in* $\mathbb{F}_{2^m}$*.*

Proof. (a) Substitute X by $\alpha^{2^{-k}}X$ in $P(X)$ to obtain $\alpha^{2^{-k}+1}X^{2^k+1} + \alpha^{2^{-k}+1}X + \beta$. Factoring out $\alpha^{2^{-k}+1}$ gives the result.

(b) For any $i \in \{0, \dots, m-1\}$, we can transform $P(X)$ into $P'(X)$ by applying the automorphism $x \mapsto x^{2^i}$ on the coefficients of $P(X)$.

(c) We can transform $P'(X)$ into $P(X)$ using the substitution $X \mapsto (X+1)^{2^k}$. □

The next result is by Bracken, Tan, and Tan [19]. It specifies the values of $\beta \in \mathbb{F}_{2^m}^*$ such that the polynomial $X^{2^k+1} + X + \beta$ has no root in $\mathbb{F}_{2^m}$.

Lemma 5.6 ([19, Theorem 2.1])**.** *Let* m *be a positive integer, and let* k *be coprime to* m*. Denote by* C *the set of non-cubes in* $\mathbb{F}_{2^m}^*$*, and define a function* $t\colon C \to \mathbb{F}_{2^m}$ *by*

$$t(\gamma) = \frac{\gamma(\gamma+1)^{2^k+2^{-k}}}{(\gamma+\gamma^{2^{-k}})^{2^k+1}}.$$

The polynomial $X^{2^k+1} + X + \beta \in \mathbb{F}_{2^m}[X]$ *has no root if and only if* $\beta \in \operatorname{Im}(t)$*.*

Lemma 5.7 is due to Taniguchi [100]. We add a short proof.

Lemma 5.7 (included in [100, Corollary 2])**.** *Let* m *be a positive integer, let* k *be an integer coprime to* m*, and let* $\alpha, \beta \in \mathbb{F}_{2^m}^*$ *such that the polynomial* $X^{2^k+1} + \alpha X + \beta$ *has no root in* $\mathbb{F}_{2^m}$*. Define* $\beta' = \frac{\beta}{\alpha^{2^{-k}+1}}$*. The Carlet APN functions* $f_{k,\alpha,\beta}$ *and* $f_{k,1,\beta'}$ *on* $\mathbb{F}_{2^{2m}}$ *from Proposition 4.5 are linearly equivalent.*

Proof. Note that, according to Lemma 5.5 (a), $f_{k,1,\beta'}$ is APN. By (4.6) and (4.7), the Carlet APN functions $f_{k,\alpha,\beta}$ and $f_{k,1,\beta'}$ are linearly equivalent if there exist invertible mappings L, N on $\mathbb{F}_{2^m}^2$, represented by linearized polynomials $L_A(X,Y), L_B(X,Y) \in \mathbb{F}_{2^m}[X,Y]$ and $N_1(X), \dots, N_4(X) \in \mathbb{F}_{2^m}[X]$, respectively, such that the two equations

$$\begin{aligned} L_A(x,y)^{2^k+1} + \alpha L_A(x,y)L_B(x,y)^{2^k} + \beta L_B(x,y)^{2^k+1} \\ = N_1(x^{2^\ell+1} + xy^{2^\ell} + \beta' y^{2^\ell+1}) + N_3(xy), \\ L_A(x,y)L_B(x,y) = N_2(x^{2^\ell+1} + xy^{2^\ell} + \beta' y^{2^\ell+1}) + N_4(xy) \end{aligned}$$

hold for all $x, y \in \mathbb{F}_{2^m}$. These equations are satisfied for

$$L_A(X,Y) = X, \qquad L_B(X,Y) = \tfrac{1}{\alpha^{2^{-k}}}Y,$$
$$N_1(X) = X, \quad N_2(X) = 0, \quad N_3(X) = 0, \quad N_4(X) = \tfrac{1}{\alpha^{2^{-k}}}X. \qquad \square$$

With the help of Lemma 5.6 and Lemma 5.7, we are able to prove Theorem 5.8. This result may be well known. Note that Zhou-Pott and Carlet APN functions are quadratic and have no constant term, which, by Theorem 4.1 and Proposition 4.2, implies they are CCZ-inequivalent if and only if they are EL-equivalent. Thanks to Lemma 5.7, we only need to consider Carlet APN functions with $\alpha \in \{0, 1\}$.

Theorem 5.8. *Let $m \geq 2$ be an even integer, let k be an integer coprime to m, and let $\gamma \in \mathbb{F}_{2^m}^*$ be a non-cube. Moreover, let $\alpha \in \{0, 1\}$ and $\beta \in \mathbb{F}_{2^m}^*$ such that the polynomial $X^{2^k+1} + aX + \beta$ has no root in $\mathbb{F}_{2^m}$. On $\mathbb{F}_{2^{2m}}$, the Zhou-Pott APN function $f_{k,0,\gamma}$ from Theorem 4.6 is EL-equivalent to the Carlet APN function $g_{k,\alpha,\beta}$ from Proposition 4.5.*

Proof. For $\alpha = 0$, we have shown in Corollary 4.10 (a) that $g_{k,0,\beta} = f_{k,0,\beta}$. According to Proposition 5.3 (a), $f_{k,0,\beta}$ is linearly equivalent to $f_{k,0,\gamma}$.

Suppose $\alpha = 1$. We show that $f_{k,0,\gamma}$ is EL-equivalent to $g_{k,1,\beta}$. In a first step, we prove that $f_{k,0,\gamma}$ is EL-equivalent to $g_{k,\alpha',\beta'}$, where

$$\alpha' = \frac{\gamma^{2^k} + \gamma}{\gamma + 1} \qquad \text{and} \qquad \beta' = \frac{\gamma^{2^k+1} + \gamma}{\gamma + 1}.$$

According to (4.6) and (4.7), the functions $f_{k,0,\gamma}$ and $g_{k,\alpha',\beta'}$ are EL-equivalent if there exist linear mappings L, N, M on $\mathbb{F}_{2^m}^2$, where L, N are invertible, that are represented by linearized polynomials $L_A(X,Y)$, $L_B(X,Y)$, $M_A(X,Y)$, $M_B(X,Y) \in \mathbb{F}_{2^m}[X,Y]$ and $N_1(X), \ldots, N_4(X) \in \mathbb{F}_{2^m}[X]$, respectively, such that the two equations

$$\begin{aligned} L_A(x,y)^{2^k+1} &+ \gamma L_B(x,y)^{2^k+1} \\ &= N_1(x^{2^k+1} + \alpha' x y^{2^k} + \beta' y^{2^k+1}) + N_3(xy) + M_A(x,y), \\ L_A(x,y) L_B(x,y) &= N_2(x^{2^k+1} + \alpha' x y^{2^k} + \beta' y^{2^k+1}) + N_4(xy) + M_B(x,y) \end{aligned}$$

hold for all $x, y \in \mathbb{F}_{2^m}$. This is the case for

$$\begin{aligned} L_A(X,Y) = X + \gamma Y \qquad & L_B(X,Y) = X + Y, \\ N_1(X) = (\gamma+1)X, \quad N_2(X) = 0, \quad N_3(X) = 0, \quad & N_4(X) = (\gamma+1)X, \\ M_A(X,Y) = 0, \quad & M_B(X,Y) = X^2 + \gamma Y^2. \end{aligned}$$

It now follows from Lemma 5.7 that $g_{k,\alpha',\beta'}$, and thereby $f_{k,0,\gamma}$, is EL-equivalent to $g_{k,1,\beta''}$, where

$$\beta'' = \frac{\beta'}{\alpha'^{2^{-k}+1}} = \frac{\gamma(\gamma+1)^{2^k+2^{-k}}}{(\gamma + \gamma^{2^{-k}})^{2^k+1}}.$$

It remains to show that $f_{k,0,\gamma}$ is EL-equivalent to $g_{k,1,\beta}$. We consider β'' as a map from the set of non-cubes of $\mathbb{F}_{2^m}^*$ to $\mathbb{F}_{2^m}$. According to Lemma 5.6, as $X^{2^k+1} + X + \beta$ has no root in $\mathbb{F}_{2^m}$, there exists a non-cube $\gamma' \in \mathbb{F}_{2^m}^*$ such that $\beta''(\gamma') = \beta$. Hence, $f_{k,0,\gamma'}$ is EL-equivalent to $g_{k,1,\beta}$. By Proposition 5.3 (a), $f_{k,0,\gamma'}$ is also linearly equivalent to $f_{k,0,\gamma}$. It follows that $f_{k,0,\gamma}$ is EL-equivalent to $g_{k,1,\beta}$. □

Theorem 5.8 implies the following results about the equivalence of two Carlet APN functions on $\mathbb{F}_{2^{2m}}$ where m is even. Recall that for $m = 2$ all APN functions are CCZ-equivalent.

Corollary 5.9. *Let $m \geq 4$ be even.*

(a) Two Carlet APN functions $f_{k,\alpha,\beta}$ and $f_{-k,\alpha,\beta}$ on $\mathbb{F}_{2^{2m}}$ are CCZ-equivalent.

(b) Two Carlet APN functions $f_{k,\alpha,\beta}$ and $f_{\ell,\alpha',\beta'}$ on $\mathbb{F}_{2^{2m}}$ where $0 < k, \ell < \frac{m}{2}$ are CCZ-equivalent if and only if $k = \ell$.

Proof. Statement (a) follows from Lemma 5.7 and Theorem 5.8 in combination with Proposition 5.3 (b). Statement (b) follows from Lemma 5.7 and Theorem 5.8 in combination with Proposition 5.3 (a) and Theorem 5.4. □

We remark that our computations hint Corollary 5.9 may also hold for odd m.

5.4 Equivalence of Taniguchi APN functions

In this section, we study the equivalence of the Taniguchi APN functions on $\mathbb{F}_{2^{2m}}$ that we introduced in Theorem 4.6. We will answer the question for which values of the parameters two Taniguchi APN functions $f_{k,\alpha,\beta}$ and $f_{\ell,\alpha',\beta'}$ are CCZ-inequivalent. Our approach to tackle this equivalence problem is similar to the approach we used in Section 5.2 for the equivalence problem of the Zhou-Pott functions.

As pointed out before, Taniguchi APN functions are quadratic and have no constant term. Hence, by Theorem 4.1 and Proposition 4.2, two Taniguchi APN functions are CCZ-equivalent if and only if they are EL-equivalent. We begin by studying the case $\alpha = 0$. Recall from Corollary 4.10 (b) that a Taniguchi function $f_{k,0,\beta}$ on $\mathbb{F}_{2^{2m}}$ is APN if and only if m is even and $\beta \in \mathbb{F}_{2^m}^*$ is a non-cube.

Proposition 5.10. *Let $m \geq 2$ be an even integer, and let k be an integer coprime to m. Let $\beta, \gamma \in \mathbb{F}_{2^m}^*$ be non-cubes. The Taniguchi APN function $f_{k,0,\beta}$ on $\mathbb{F}_{2^{2m}}$ from Theorem 4.8 is linearly equivalent to the Zhou-Pott APN function $g_{k,2k,\gamma}$ on $\mathbb{F}_{2^{2m}}$ from Theorem 4.6.*

Proof. If $\beta \in \mathbb{F}_{2^m}^*$ is a non-cube, then $\frac{1}{\beta}$ is as well. From Proposition 5.3 (a), we know that the Zhou-Pott APN function $g_{k,2k,\gamma}$ is linearly equivalent to $g_{k,2k,\frac{1}{\beta}}$. We show that $f_{k,0,\beta}$ is also linearly equivalent to $g_{k,2k,\frac{1}{\beta}}$.

By (4.6) and (4.7) and the explanations below, the functions $f_{k,0,\beta}$ and $g_{k,2k,\frac{1}{\beta}}$ are linearly equivalent if there exist bijective mappings L, N on $\mathbb{F}_{2^m}^2$, represented by linearized polynomials $L_A(X,Y), L_B(X,Y) \in \mathbb{F}_{2^m}[X,Y]$ and $N_1(X), \ldots, N_4(X) \in \mathbb{F}_{2^m}[X]$, respectively, such that the two equations

$$\begin{aligned} L_A(x,y)^{2^{2k}(2^k+1)} + \beta L_B(x,y)^{(2^k+1)} &= N_1(x^{2^k+1} + \tfrac{1}{\beta} y^{2^{2k}(2^k+1)}) + N_3(xy), \\ L_A(x,y) L_B(x,y) &= N_2(x^{2^k+1} + \tfrac{1}{\beta} y^{2^{2k}(2^k+1)}) + N_4(xy) \end{aligned}$$

hold for all $x, y \in \mathbb{F}_{2^m}$. The functions $f_{k,0,\beta}$ and $g_{k,2k,\frac{1}{\beta}}$ are linearly equivalent by

$$L_A(X,Y) = Y, \qquad L_B(X,Y) = X,$$
$$N_1(X) = \beta X, \quad N_2(X) = 0, \quad N_3(X) = 0, \quad N_4(X) = X.$$

Consequently, $f_{k,0,\beta}$ is linearly equivalent to $g_{k,2k,\gamma}$. □

From Proposition 5.10, we immediately obtain the following results.

Corollary 5.11. *Let $m \geq 4$ be even.*

(a) Two Taniguchi APN functions $f_{k,0,\beta}$ and $f_{-k,0,\beta}$ on $\mathbb{F}_{2^{2m}}$ are CCZ-equivalent.

(b) Two Taniguchi APN functions $f_{k,0,\beta}$ and $f_{\ell,0,\beta'}$ on $\mathbb{F}_{2^{2m}}$ where $0 < k, \ell < \frac{m}{2}$ are CCZ-equivalent if and only if $k = \ell$.

Proof. Result (a) follows from combining Proposition 5.10 with Proposition 5.3 (b). Result (b) follows from Proposition 5.10 in combination with Theorem 5.4. □

From now on, we focus on the case $\alpha \neq 0$.

Proposition 5.12. *Let $m \geq 2$ be an integer. Let k be an integer coprime to m, and let $\alpha, \beta \in \mathbb{F}_{2^m}^*$ such that $X^{2^k+1} + \alpha X + \beta$ has no root in $\mathbb{F}_{2^m}$. Then the following pairs of Taniguchi APN functions on $\mathbb{F}_{2^{2m}}$ from Theorem 4.8 are linearly equivalent:*

(a) $f_{k,\alpha,\beta}$ and $f_{k,1,\beta'}$, where $\beta' = \frac{\beta}{\alpha^{2^{-k}+1}}$,

(b) $f_{k,1,\beta^{2^i}}$ and $f_{k,1,\beta}$ for $i \in \{0, \dots, m-1\}$,

(c) $f_{-k,1,\beta}$ and $f_{k,1,\beta}$.

Proof. Note that it follows from Lemma 5.5 that all the functions in Proposition 5.12 are APN. To study their equivalence, we use the framework established in (4.6) and (4.7). Two Taniguchi APN functions $f_{k,\alpha,\beta}$ and $f_{\ell,\alpha',\beta'}$ are linearly equivalent if there exist invertible mappings L, N on $\mathbb{F}_{2^m}^2$, represented by linearized polynomials $L_A(X,Y), L_B(X,Y) \in \mathbb{F}_{2^m}[X,Y]$ and $N_1(X), \dots, N_4(X) \in \mathbb{F}_{2^m}[X]$, respectively, such that the two equations

$$\begin{aligned} L_A(x,y)^{2^{2k}(2^k+1)} + \alpha L_A(x,y)^{2^{2k}} L_B(x,y)^{2^k} + \beta L_B(x,y)^{(2^k+1)} \\ = N_1(x^{(2^\ell+1)2^{2\ell}} + \alpha' x^{2^{2\ell}} y^{2^\ell} + \beta' y^{2^\ell+1}) + N_3(xy), \\ L_A(x,y) L_B(x,y) = N_2(x^{(2^\ell+1)2^{2\ell}} + \alpha' x^{2^{2\ell}} y^{2^\ell} + \beta' y^{2^\ell+1}) + N_4(xy) \end{aligned}$$

hold for all $x, y \in \mathbb{F}_{2^m}$. We will present such polynomials for (a)–(c). As in all three cases, $N_2(X) = N_3(X) = 0$, we will not restate these polynomials in every case.

(a) The functions $f_{k,\alpha,\beta}$ and $f_{k,1,\beta'}$ are linearly equivalent by

$$L_A(X,Y) = X, \quad L_B(X,Y) = \frac{1}{\alpha^{2^{-k}}} Y, \quad N_1(X) = X, \quad N_4(X) = \frac{1}{\alpha^{2^{-k}}} X.$$

(b) The functions $f_{k,1,\beta^{2i}}$ and $f_{k,1,\beta}$ are linearly equivalent by

$$L_A(X,Y) = X^{2^i}, \quad L_B(X,Y) = Y^{2^i}, \quad N_1(X) = X^{2^i}, \quad N_4(X) = X^{2^i}.$$

(c) We first show that $f_{-k,1,\beta}$ and $f_{k,\frac{1}{\beta},\frac{1}{\beta}}$ are linearly equivalent. Their equivalence is established by

$$L_A(X,Y) = Y^{2^{3k}}, \quad L_B(X,Y) = X^{2^{3k}}, \quad N_1(X) = \beta X, \quad N_4(X) = X^{2^{3k}}.$$

Using (a), it follows that $f_{k,\frac{1}{\beta},\frac{1}{\beta}}$ is linearly equivalent to $f_{k,1,\beta^{2^{-k}}}$, which, by (b), is linearly equivalent to $f_{k,1,\beta}$. Hence, $f_{-k,1,\beta}$ and $f_{k,1,\beta}$ are linearly equivalent. □

In the following Theorem 5.13, we completely solve the equivalence problem for Taniguchi APN functions $f_{k,\alpha,\beta}$ with $\alpha \neq 0$. As mentioned before, on $\mathbb{F}_{2^4}$, there exists only one APN function up to CCZ-equivalence. Consequently, we only consider $\mathbb{F}_{2^{2m}}$ with $m \geq 3$. According to Proposition 5.12, every Taniguchi APN function $f_{k,\alpha,\beta}$ with $\alpha \neq 0$ is linearly equivalent to a Taniguchi APN function $f_{k',1,\beta'}$ where $0 < k' < \frac{m}{2}$ and $\alpha = 1$. Hence, we will only consider functions $f_{k,1,\beta}$ where $0 < k < \frac{m}{2}$.

Note that the structure of the proof of Theorem 5.13 is similar to the structure of the proof of Theorem 5.4, some parts are almost identical. However, to keep the proof of Theorem 5.13 self-contained, we will not shorten it.

Theorem 5.13. *Let $m \geq 3$ be an integer, and let k, ℓ be integers coprime to m such that $0 < k, \ell < \frac{m}{2}$. Let $\beta, \beta' \in \mathbb{F}_{2^m}^*$ such that the polynomials $X^{2^k+1} + X + \beta$ and $X^{2^\ell+1} + X + \beta'$ have no root in $\mathbb{F}_{2^m}$. Two Taniguchi APN functions $f_{k,1,\beta}, f_{\ell,1,\beta'}$ on $\mathbb{F}_{2^{2m}}$ defined by*

$$f_{k,1,\beta} = (x^{2^{2k}(2^k+1)} + x^{2^{2k}} y^{2^k} + \beta y^{2^k+1},\ xy)$$

and

$$f_{\ell,1,\beta'} = (x^{2^{2\ell}(2^\ell+1)} + x^{2^{2\ell}} y^{2^\ell} + \beta' y^{2^\ell+1},\ xy)$$

are CCZ-equivalent if and only if $k = \ell$ and $\beta' = \beta^{2^i}$ for some $i \in \{0, \dots, m-1\}$.

Proof. We have shown in Proposition 5.12 (b) that $f_{k,1,\beta}$ and $f_{k,1,\beta^{2i}}$ are linearly equivalent and thereby CCZ-equivalent. We will now show the converse: if $f_{k,1,\beta}$ and $f_{\ell,1,\beta'}$ are CCZ-equivalent, then $k = \ell$ and $\beta' = \beta^{2^i}$ for some $i \in \{0, \dots, m-1\}$.

For $m = 3$ and $m = 4$, the result can be easily confirmed. If $m = 3$, then $k = 1$, and there are three distinct $\beta \in \mathbb{F}_{2^3}^*$ such that $X^3 + X + \beta$ has no root in $\mathbb{F}_{2^3}^*$. If β meets this condition, then, according to Lemma 5.5 (b), β^2 and β^4 do as well. It follows from Proposition 5.12 that for $m = 3$, all three Taniguchi APN functions belong to the same equivalence class. If $m = 4$, then $k = 1$, and there are five distinct $\beta \in \mathbb{F}_{2^4}^*$ such that $X^3 + X + \beta$ has no root, namely 1 and $\beta, \beta^2, \beta^4, \beta^8$ for some $\beta \neq 1$. Hence, for $m = 4$, there exist two equivalence classes: $f_{1,1,1}$ and $f_{1,1,\beta}$, where $\beta \neq 1$. Their inequivalence was shown by Taniguchi [100], who computed the Γ-ranks for these functions as 13 700 and 13 798, respectively.

For the remainder of the proof, let $m \geq 5$. Assume $f_{k,1,\beta}$ and $f_{\ell,1,\beta'}$ are CCZ-equivalent. By Theorem 4.1 and Proposition 4.2, this implies that the functions are also EL-equivalent. Hence, similarly to the proof of Proposition 5.12, there exist linearized polynomials $L_A(X,Y), L_B(X,Y), M_A(X,Y), M_B(X,Y) \in \mathbb{F}_{2^m}[X,Y]$ and $N_1(X), \dots, N_4(X) \in \mathbb{F}_{2^m}[X]$, where

$$L(X,Y) = (L_A(X,Y), L_B(X,Y))$$

and

$$N(X,Y) = (N_1(X) + N_3(Y),\ N_2(X) + N_4(Y))$$

are invertible, such that the equations

$$\begin{aligned} &L_A(x,y)^{2^{2k}(2^k+1)} + L_A(x,y)^{2^{2k}} L_B(x,y)^{2^k} + \beta L_B(x,y)^{2^k+1} \\ &\qquad = N_1(x^{(2^\ell+1)2^{2\ell}} + x^{2^{2\ell}} y^{2^\ell} + \beta' y^{2^\ell+1}) + N_3(xy) + M_A(x,y), \end{aligned} \tag{5.61}$$

$$\begin{aligned} &L_A(x,y) L_B(x,y) \\ &\qquad = N_2(x^{(2^\ell+1)2^{2\ell}} + x^{2^{2\ell}} y^{2^\ell} + \beta' y^{2^\ell+1}) + N_4(xy) + M_B(x,y) \end{aligned} \tag{5.62}$$

hold for all $x, y \in \mathbb{F}_{2^m}$. We write $L_A(X,Y) = L_1(X) + L_3(Y)$ and $L_B(X,Y) = L_2(X) + L_4(Y)$ for linearized polynomials $L_1(X), \dots, L_4(X) \in \mathbb{F}_{2^m}[X]$. Hence,

$$L(X,Y) = (L_1(X) + L_3(Y),\ L_2(X) + L_4(Y))\,.$$

Write

$$L_1(X) = \sum_{i=0}^{m-1} a_i X^{2^i}, \qquad\qquad L_2(X) = \sum_{i=0}^{m-1} b_i X^{2^i},$$

and

$$L_3(Y) = \sum_{i=0}^{m-1} \overline{a}_i Y^{2^i}, \qquad\qquad L_4(Y) = \sum_{i=0}^{m-1} \overline{b}_i Y^{2^i}.$$

Analogously, define linearized polynomials $M_1(X), \dots, M_4(X) \in \mathbb{F}_{2^m}[X]$ such that

$$M(X,Y) = (M_1(X) + M_3(Y), M_2(X) + M_4(Y)).$$

For the remainder of the proof, let $x, y \in \mathbb{F}_{2^m}$. We first prove the following claim.

Claim 5.2. *If $f_{k,1,\beta}$ and $f_{\ell,1,\beta'}$ are EL-equivalent, then $k = \ell$ and each of the linearized polynomials $L_1(X), L_2(X), L_3(Y), L_4(Y)$ is a monomial or zero.*

We will prove the result for $y = 0$ and obtain statements for $L_1(X)$ and $L_2(X)$. Using the same approach with $x = 0$, identical statements can be obtained for $L_3(Y)$

and $L_4(Y)$. Let $y = 0$. Then it follows from (5.61) and (5.62) that the equations

$$L_1(x)^{2^{2k}(2^k+1)} + L_1(x)^{2^{2k}} L_2(x)^{2^k} + \beta L_2(x)^{2^k+1} = N_1(x^{(2^\ell+1)2^{2\ell}}) + M_1(x), \quad (5.63)$$

$$L_1(x)L_2(x) = N_2(x^{(2^\ell+1)2^{2\ell}}) + M_2(x) \quad (5.64)$$

need to hold for all $x \in \mathbb{F}_{2^m}$. Write

$$N_1(X) = \sum_{i=0}^{m-1} c_i X^{2^i} \qquad \text{and} \qquad N_2(X) = \sum_{i=0}^{m-1} d_i X^{2^{i-2\ell}}.$$

Note that, for convenience, we shift the summation index of $N_2(X)$.

As $L(X, Y)$ has to be invertible, it is not possible that both $L_1(X)$ and $L_2(X)$ are zero. We first study the case that exactly one out of $L_1(X)$ and $L_2(X)$ is nonzero. Suppose $L_1(X) \neq 0$ and $L_2(X) = 0$. In this case, the left-hand side of (5.64) is zero, which implies $N_2(X) = M_2(X) = 0$. Moreover, (5.63) becomes

$$L_1(x)^{2^{2k}(2^k+1)} = N_1(x^{(2^\ell+1)2^{2\ell}}) + M_1(x). \quad (5.65)$$

This equation implies that the Gold APN functions $x \mapsto x^{2^k+1}$ and $x \mapsto x^{2^\ell+1}$ on $\mathbb{F}_{2^m}$ are EL-equivalent. According to Theorem 5.1, this holds if and only if $k = \ell$. We further showed that for $m \geq 5$, the associated equivalence mappings between two Gold APN functions with $k = \ell$ are linearized monomials. Consequently, we obtain

$$L_1(X) = a_u X^{2^u} \qquad \text{and} \qquad L_2(X) = 0 \quad (5.66)$$

for some $u \in \{0, \dots, m-1\}$ and $a_u \in \mathbb{F}_{2^m}^*$. If we suppose $L_1(X) = 0$ and $L_2(X) \neq 0$ and proceed analogously to the previous case, we obtain

$$L_1(X) = 0 \qquad \text{and} \qquad L_2(X) = b_u X^{2^u} \quad (5.67)$$

for some $u \in \{0, \dots, m-1\}$ and $b_u \in \mathbb{F}_{2^m}^*$. In both of the above cases, we have $M_1(X) = M_2(X) = 0$.

Now, assume that both $L_1(X)$ and $L_2(X)$ are nonzero. Then (5.64) becomes

$$\sum_{i=0}^{m-1} a_i b_i x^{2^{i+1}} + \sum_{\substack{i,j=0,\\ j\neq i}}^{m-1} a_i b_j x^{2^i+2^j} = \sum_{i=0}^{m-1} d_i x^{(2^\ell+1)2^i} + M_2(x). \quad (5.68)$$

Note that the first sum on the left-hand side of (5.68) is linearized. Hence, set $M_2(X) = \sum_{i=0}^{m-1} a_i b_i X^{2^{i+1}}$. We rewrite (5.68) as

$$\sum_{0 \leq i < j \leq m-1} (a_i b_j + a_j b_i) x^{2^i+2^j} = \sum_{i=0}^{m-1} d_i x^{2^i+2^{i+\ell}},$$

which implies that the equations

$$\begin{aligned} a_i b_{i+\ell} + a_{i+\ell} b_i &= d_i && \text{for all } i, && (5.69)\\ a_i b_j + a_j b_i &= 0 && \text{for } j \neq i, i \pm \ell, && (5.70) \end{aligned}$$

where the subscripts are calculated modulo m, have to hold. We separate the proof into two cases: first, the case that $d_i = 0$ for all $i = 0, \ldots, m-1$, and, second, the case that $d_u \neq 0$ for some $u \in \{0, \ldots, m-1\}$.

Case 1. In this case, we show that if $d_i = 0$ for all $i = 0, \ldots, m-1$, similarly to (5.65), the problem can be reduced to the equivalence problem of two Gold APN functions. Assume $d_i = 0$ for all $i = 0, \ldots, m-1$, which means $N_2(X) = 0$. In this case, (5.69) and (5.70) combine to

$$a_i b_j + a_j b_i = 0 \qquad \text{for } j \neq i. \tag{5.71}$$

As $L_1(X)$ and $L_2(X)$ are both nonzero, there exist $u, u' \in \{0, \ldots, m-1\}$ such that a_u and $b_{u'}$ are nonzero. If $u = u'$, the corresponding term $a_u b_u X^{2^u+1}$ on the left-hand side of (5.64) is linearized and only contributes to $M_2(X)$ on the respective right-hand side. If $u \neq u'$, then, by (5.71),

$$a_u b_{u'} + a_{u'} b_u = 0.$$

Consequently, $a_{u'}$ and b_u have to be nonzero as well, and $a_u, a_{u'}, b_u, b_{u'}$ have to meet the condition $\frac{a_u}{b_u} = \frac{a_{u'}}{b_{u'}}$. Define $\Delta = \frac{a_u}{b_u}$, and note that $\Delta \neq 0$. It follows from (5.71) that for all $j = 0, \ldots, m-1$, the coefficient pair (a_j, b_j) satisfies either

$$a_j = b_j = 0 \qquad\qquad \text{or} \qquad\qquad \frac{a_j}{b_j} = \Delta. \tag{5.72}$$

Consequently, $b_j = \delta a_j$, where $\delta = \frac{1}{\Delta}$, for all $j = 0, \ldots, m-1$, and $L_2(X)$ is a multiple of $L_1(X)$, namely

$$L_2(X) = \delta L_1(X). \tag{5.73}$$

We plug $L_1(X)$ and $L_2(X)$ into (5.63) and obtain

$$\begin{aligned} L_1(x)^{2^{2k}(2^k+1)} + \delta^{2^k} L_1(x)^{2^k(2^k+1)} \; + \; \beta\delta^{2^k+1} L_1(x)^{2^k+1} \\ = N_1(x^{(2^\ell+1)2^{2\ell}}) + M_1(x). \end{aligned} \tag{5.74}$$

Define a polynomial $T(X) \in \mathbb{F}_{2^m}[X]$ as

$$T(X) = X^{2^{2k}} + \delta^{2^k} X^{2^k} + \beta\delta^{2^k+1} X,$$

and rewrite the left-hand side of (5.74) as $T(L_1(x)^{2^k+1})$. We show that $T(X)$ is a permutation polynomial. Since $T(X)$ is linearized, it is sufficient to show that $T(X)$ has no nonzero roots. If $T(X)$ had a nonzero root, it would also be a root of the polynomial

$$T'(X) = X^{2^{2k}-1} + \delta^{2^k} X^{2^k-1} + \beta\delta^{2^k+1}.$$

Substitute X^{2^k-1} by X, and note that, as $\gcd(2^k-1, 2^m-1) = 2^{\gcd(k,m)} - 1 = 1$, this substitution is one-to-one. We obtain

$$T'(X) = X^{2^k+1} + \delta^{2^k} X + \beta\delta^{2^k+1}.$$

By Lemma 5.5 (a), the polynomial $T'(X)$ has no root if and only if $P(X) = X^{2^k+1} + X + \beta$ has no root in $\mathbb{F}_{2^m}$. This holds by the definition of β.

Hence, we denote by $T^{-1}(X)$ the inverse of $T(X)$ and rewrite (5.74) as

$$L_1(x)^{2^k+1} = T^{-1}(N_1(x^{(2^\ell+1)2^{2\ell}})) + T^{-1}(M_1(x)). \tag{5.75}$$

Since $T^{-1}(X)$ is also linearized, (5.75) describes the same equivalence problem of two Gold APN functions as in (5.65). It follows from Theorem 5.1 that $k = \ell$ and that $L_1(X)$ is a linearized monomial. Because of (5.73), the polynomials $L_1(X)$ and $L_2(X)$ are monomials of the same degree:

$$L_1(X) = a_u X^{2^u} \qquad \text{and} \qquad L_2(X) = b_u X^{2^u}. \tag{5.76}$$

Moreover, $M_2(X) = a_u b_u X^{2^{u+1}}$ and $M_1(X) = 0$.

Case 2. Consider (5.69) and (5.70) again, and assume $d_u \neq 0$ for some $u \in \{0, \ldots, m-1\}$, which means $N_2(X) \neq 0$. If $d_u \neq 0$, then, by (5.69), a_u and b_u cannot be zero at the same time. We will separate the proof of Case 2 into two subcases: first, Case 2.1, where both a_u and b_u are nonzero, and second, Case 2.2, where exactly one of a_u and b_u is nonzero. Both these cases will be separated into several subcases again.

We will show that Case 2.1 will lead to a contradiction, whereas Case 2.2 provides new possible solutions for $L_1(X)$ and $L_2(X)$ under the condition that $k = \ell$: the polynomials can be monomials of different degrees.

Case 2.1. Assume $a_u \neq 0$ and $b_u \neq 0$. It follows from (5.70) that all pairs (a_j, b_j), where $j \neq u, u \pm \ell$, satisfy (5.72). We will first show that the only possible nonzero coefficients are a_j, b_j for $j = u, u \pm \ell, u \pm 2\ell$.

By way of contradiction, suppose there exists $\ell' \neq 0, \pm\ell, \pm 2\ell$ such that $a_{u+\ell'}$ and $b_{u+\ell'}$ are nonzero. By (5.72), this implies $\frac{a_{u+\ell'}}{b_{u+\ell'}} = \Delta$. Since $u + \ell' \pm \ell \neq u \pm \ell$, it follows from (5.69) with $i = u + \ell'$ that both $(a_{u+\ell}, b_{u+\ell})$ and $(a_{u-\ell}, b_{u-\ell})$ also have to satisfy one of the equations in (5.72). Hence, (5.72) holds for all $j = 0, \ldots, m-1$, which means that $L_2(X)$ is a multiple of $L_1(X)$. However, now $L_1(X)L_2(X)$ is linearized, and (5.64) implies $N_2(X) = 0$. This is a contradiction.

Hence, we assume $a_j = b_j = 0$ for $j \neq u, u \pm \ell, u \pm 2\ell$ for the remainder of Case 2.1. We separate its proof into two subcases: in Case 2.1.1, we assume $a_{u\pm 2\ell} = b_{u\pm 2\ell} = 0$, in Case 2.1.2, we suppose that at least one of the coefficients $a_{u\pm 2\ell}, b_{u\pm 2\ell}$ is nonzero. Both these cases lead to contradictions.

Case 2.1.1. Suppose $a_{u\pm 2\ell} = b_{u\pm 2\ell} = 0$. In this case, we obtain only one equation from (5.69), namely

$$a_{u-\ell}b_{u+\ell} + a_{u+\ell}b_{u-\ell} = 0.$$

Hence, either

(i) $a_{u-\ell} = a_{u+\ell} = 0$ or $b_{u-\ell} = b_{u+\ell} = 0$, meaning that one of $L_1(X)$ and $L_2(X)$ is a monomial and the other one has at most three nonzero coefficients, or

(ii) $a_{u-\ell} = b_{u-\ell} = 0$ or $a_{u+\ell} = b_{u+\ell} = 0$, meaning that both $L_1(X)$ and $L_2(X)$ have at most two nonzero coefficients, or

(iii) $a_{u\pm\ell}, b_{u\pm\ell} \neq 0$ and $\frac{a_{u-\ell}}{b_{u-\ell}} = \frac{a_{u+\ell}}{b_{u+\ell}}$, meaning that both $L_1(X)$ and $L_2(X)$ are trinomials.

We will consider each of these three subcases separately.

Case 2.1.1. (i) Assume $b_{u-\ell} = b_{u+\ell} = 0$. The case $a_{u-\ell} = a_{u+\ell} = 0$ follows by symmetry. We consider polynomials

$$L_1(X) = a_{u-\ell}X^{2^{u-\ell}} + a_uX^{2^u} + a_{u+\ell}X^{2^{u+\ell}} \qquad \text{and} \qquad L_2(X) = b_uX^{2^u},$$

where $a_u, b_u \neq 0$. Moreover, we may assume that at least one of $a_{u-\ell}$ and $a_{u+\ell}$ is nonzero as otherwise $L_1(X)$ and $L_2(X)$ are monomials of the same degree, which implies $N_2(X) = 0$. This contradicts the assumption of Case 2. We plug $L_1(X)$ and $L_2(X)$ into the left-hand side of (5.63) and obtain

$$\begin{aligned} L_1(x)^{2^{2k}(2^k+1)} = {} & a_{u-\ell}^{2^{2k}(2^k+1)}x^{2^{u-\ell+2k}(2^k+1)} + a_u^{2^{2k}(2^k+1)}x^{2^{u+2k}(2^k+1)} \\ & + a_{u+\ell}^{2^{2k}(2^k+1)}x^{2^{u+\ell+2k}(2^k+1)} + a_{u-\ell}^{2^{3k}}a_u^{2^{2k}}x^{2^{u+2k}(2^{k-\ell}+1)} \\ & + a_u^{2^{3k}}a_{u+\ell}^{2^{2k}}x^{2^{u+\ell+2k}(2^{k-\ell}+1)} + a_{u+\ell}^{2^{3k}}a_{u-\ell}^{2^{2k}}x^{2^{u-\ell+2k}(2^{k+2\ell}+1)} \\ & + a_{u-\ell}^{2^{3k}}a_{u+\ell}^{2^{2k}}x^{2^{u+\ell+2k}(2^{k-2\ell}+1)} + a_u^{2^{3k}}a_{u-\ell}^{2^{2k}}x^{2^{u-\ell+2k}(2^{k+\ell}+1)} \\ & + a_{u+\ell}^{2^{3k}}a_u^{2^{2k}}x^{2^{u+2k}(2^{k+\ell}+1)} \end{aligned} \tag{5.77}$$

and

$$\begin{aligned} L_1(x)^{2^{2k}}L_2(x)^{2^k} = {} & a_{u-\ell}^{2^{2k}}b_u^{2^k}x^{2^{u+k}(2^{k-\ell}+1)} + a_u^{2^{2k}}b_u^{2^k}x^{2^{u+k}(2^k+1)} \\ & + a_{u+\ell}^{2^{2k}}b_u^{2^k}x^{2^{u+k}(2^{k+\ell}+1)} \end{aligned} \tag{5.78}$$

and

$$\beta L_2(x)^{2^k+1} = \beta b_u^{2^k+1}x^{2^u(2^k+1)}. \tag{5.79}$$

Recall that the right-hand side of (5.63) is

$$\sum_{i=0}^{m-1} c_i x^{2^{i+2\ell}(2^\ell+1)} + M_1(x).$$

Note that the second term of (5.77), whose coefficient is nonzero, can only be canceled by any of the other terms in (5.77), (5.78) and (5.79) if $k = \ell$. Then, it may be canceled by the seventh term of (5.77). For $k \neq \ell$ it cannot be canceled as, since $0 < \ell < \frac{m}{2}$, no other term will be of the shape $ax^{2^{u+2k}(2^k+1)}$. Assuming the second term of (5.77) cannot be canceled, it can only be represented on the right-hand side of (5.63) if $k = \ell$.

In summary, we may suppose $k = \ell$. Now, the fourth and the fifth summand of (5.77) as well as the first summand of (5.78) become linearized. Consequently,

$$M_1(X) = a_{u-k}^{2^{2k}} b_u^{2^k} X^{2^{u+k+1}} + a_{u-k}^{2^{3k}} a_u^{2^{2k}} X^{2^{u+2k+1}} + a_u^{2^{3k}} a_{u+k}^{2^{2k}} X^{2^{u+3k+1}}.$$

Next, consider the eighth and the ninth term of (5.77), where the eighth term can be summarized with the third term of (5.78):

$$a_{u+k}^{2^{3k}} a_u^{2^{2k}} x^{2^{u+2k}(2^{2k}+1)}, \qquad\qquad (a_u^{2^{3k}} a_{u-k}^{2^{2k}} + a_{u+k}^{2^{2k}} b_u^{2^k}) x^{2^{u+k}(2^{2k}+1)}.$$

As $m \geq 5$ and $\gcd(k, m) = 1$, we have $2k \not\equiv \pm k \pmod{m}$. Hence, these terms cannot be represented in the form $c_i x^{2^{i+2k}(2^k+1)}$ on the right-hand side of (5.63), which means that their coefficients have to be zero. As $a_u \neq 0$, it follows that $a_{u+k} = 0$, which, recalling that $b_u \neq 0$, then implies $a_{u-k} = 0$. This contradicts our assumption that at least one of a_{u-k} and a_{u+k} is nonzero.

Case 2.1.1. (ii) Assume $a_{u-\ell} = b_{u-\ell} = 0$. The case $a_{u+\ell} = b_{u+\ell} = 0$ follows by symmetry. In our case,

$$L_1(X) = a_u X^{2^u} + a_{u+\ell} X^{2^{u+\ell}} \qquad \text{and} \qquad L_2(X) = b_u X^{2^u} + b_{u+\ell} X^{2^{u+\ell}}.$$

As in Case 2.1.1. (i), a_u and b_u are nonzero, and we may assume that at least one of $a_{u+\ell}$ and $b_{u+\ell}$ is nonzero. For $L_1(X)$ and $L_2(X)$ as above, the the left-hand side of (5.63) consists of

$$\begin{aligned} L_1(x)^{2^{2k}(2^k+1)} = {} & a_u^{2^{2k}(2^k+1)} x^{2^{u+2k}(2^k+1)} + a_{u+\ell}^{2^{2k}(2^k+1)} x^{2^{u+\ell+2k}(2^k+1)} \\ & + a_u^{2^{3k}} a_{u+\ell}^{2^{2k}} x^{2^{u+\ell+2k}(2^{k-\ell}+1)} + a_{u+\ell}^{2^{3k}} a_u^{2^{2k}} x^{2^{u+2k}(2^{k+\ell}+1)} \end{aligned}$$

and

$$\begin{aligned} L_1(x)^{2^{2k}} L_2(x)^{2^k} = {} & a_u^{2^{2k}} b_u^{2^k} x^{2^{u+k}(2^k+1)} + a_{u+\ell}^{2^{2k}} b_{u+\ell}^{2^k} x^{2^{u+\ell+k}(2^k+1)} \\ & + a_u^{2^{2k}} b_{u+\ell}^{2^k} x^{2^{u+\ell+k}(2^{k-\ell}+1)} + a_{u+\ell}^{2^{2k}} b_u^{2^k} x^{2^{u+k}(2^{k+\ell}+1)} \end{aligned}$$

and

$$\begin{aligned} \beta L_2(x)^{2^k+1} = {} & \beta b_u^{2^k+1} x^{2^u(2^k+1)} + \beta b_{u+\ell}^{2^k+1} x^{2^{u+\ell}(2^k+1)} \\ & + \beta b_u^{2^k} b_{u+\ell} x^{2^{u+\ell}(2^{k-\ell}+1)} + \beta b_{u+\ell}^{2^k} b_u x^{2^u(2^{k+\ell}+1)}. \end{aligned}$$

By similar reasoning as in Case 2.1.1. (i), not all summands containing the factor x^{2^k+1} can be canceled simultaneously. Consequently, we need $k = \ell$ for these terms to be represented on the right-hand side of (5.63). If $k = \ell$, the following terms, which cannot be canceled, occur on the left-hand side of (5.63):

$$a_{u+k}^{2^{3k}} a_u^{2^{2k}} x^{2^{u+2k}(2^{2k}+1)}, \qquad a_{u+k}^{2^{2k}} b_u^{2^k} x^{2^{u+k}(2^{2k}+1)}, \qquad \beta b_{u+k}^{2^{2k}} b_u x^{2^u(2^{2k}+1)}.$$

Note that least one of these terms has a nonzero coefficient as a_u, b_u and at least one of a_{u+k} and b_{u+k} are nonzero. However, none of these terms can be represented in the form $c_i x^{2^{i+2k}(2^k+1)}$ on the right-hand side of (5.63). This is a contradiction.

Case 2.1.1. (iii) Now,

$$\begin{aligned} L_1(X) &= a_{u-\ell} X^{2^{u-\ell}} + a_u X^{2^u} + a_{u+\ell} X^{2^{u+\ell}} \\ \text{and } L_2(X) &= b_{u-\ell} X^{2^{u-\ell}} + b_u X^{2^u} + b_{u+\ell} X^{2^{u+\ell}}, \end{aligned}$$

where all coefficients are nonzero and satisfy $\frac{a_{u-\ell}}{b_{u-\ell}} = \frac{a_{u+\ell}}{b_{u+\ell}}$. We plug these polynomials into the left-hand side of (5.63). By similar reasoning as in Case 2.1.1. (i) and Case 2.1.1. (ii), not all terms containing the factor x^{2^k+1} can be canceled. Hence, $k = \ell$. Now, the left-hand side of (5.63) contains the following two summands that have nonzero coefficients and cannot be canceled:

$$a_{u+k}^{2^{3k}} a_u^{2^{2k}} x^{2^{u+2k}(2^{2k}+1)}, \qquad \beta b_u^{2^{2k}} b_{u-k} x^{2^{u-k}(2^{2k}+1)}.$$

As none of them can be represented on the right-hand side of (5.63), this is a contradiction.

Case 2.1.2. Suppose that not all of $a_{u\pm 2\ell}, b_{u\pm 2\ell}$ are zero. Recall that all pairs (a_j, b_j) where $j \neq u, u \pm \ell$ have to satisfy (5.72). We consider the case that $a_{u+2\ell}$ and $b_{u+2\ell}$ are nonzero. An almost identical result can be obtained by symmetry assuming that $a_{u-2\ell}$ and $b_{u-2\ell}$ are nonzero.

If $a_{u+2\ell}, b_{u+2\ell} \neq 0$, then, by (5.72), $\frac{a_{u+2\ell}}{b_{u+2\ell}} = \Delta$. It follows from (5.70) that $(a_{u-2\ell}, b_{u-2\ell})$ and $(a_{u-\ell}, b_{u-\ell})$ also have to satisfy (5.72). However, (5.70) does not provide any restriction on the values of $a_{u+\ell}$ and $b_{u+\ell}$. If $(a_{u+\ell}, b_{u+\ell})$ satisfies (5.72), then all (a_j, b_j) do, and we know from the beginning of Case 2.1 that this implies $N_2(X) = 0$. As before, this is a contradiction.

If $(a_{u+\ell}, b_{u+\ell})$ does not satisfy (5.72), then it follows from (5.70) that $a_j = b_j = 0$ for $j = u - \ell, u - 2\ell$. Hence,

$$\begin{aligned} L_1(X) &= a_u X^{2^u} + a_{u+\ell} X^{2^{u+\ell}} + a_{u+2\ell} X^{2^{u+2\ell}} \\ \text{and } L_2(X) &= b_u X^{2^u} + b_{u+\ell} X^{2^{u+\ell}} + b_{u+2\ell} X^{2^{u+2\ell}}. \end{aligned}$$

As $\frac{a_u}{b_u} = \frac{a_{u+2\ell}}{b_{u+2\ell}}$, this case is similar to Case 2.1.1. (iii), when we substitute u by $u + \ell$, with the only difference that now, precisely one of the middle coefficients $a_{u+\ell}, b_{u+\ell}$ may be zero. However, the arguments used in Case 2.1.1 leading to the conclusion $k = \ell$ still hold. If $k = \ell$, the left-hand side of (5.63) contains the following summands that have nonzero coefficients and cannot be canceled:

$$a_{u+2k}^{2^{3k}} a_u^{2^{2k}} x^{2^{u+2k}(2^{3k}+1)}, \qquad a_{u+2k}^{2^{2k}} b_u^{2^k} x^{2^{u+k}(2^{3k}+1)}, \qquad \beta b_{u+2k}^{2^k} b_u x^{2^u(2^{3k}+1)}.$$

As these terms cannot be represented on the right-hand side of (5.63), their coefficients need to be zero. This contradicts our assumption that $a_u, a_{u+2k}, b_u, b_{u+2k}$ are nonzero.

Case 2.2. Assume, exactly one of a_u and b_u is nonzero. We show the case $a_u \neq 0$ and $b_u = 0$. The case $a_u = 0$ and $b_u \neq 0$ can be proved analogously. So assume $a_u \neq 0$ and $b_u = 0$. From (5.69) with $i = u$, we obtain the equation

$$a_u b_{u+\ell} = d_u.$$

As $d_u \neq 0$, it follows that $b_{u+\ell} \neq 0$. From (5.70) with $i = u$, we obtain

$$a_u b_j = 0 \quad \text{for } j \neq u, u \pm \ell.$$

Consequently, $b_j = 0$ for $j \neq u \pm \ell$. Now, (5.70) with $i = u + \ell$ implies

$$a_j b_{u+\ell} = 0 \quad \text{for } j \neq u - \ell, u, u + \ell, u + 2\ell.$$

Hence, $a_j = 0$ for $j \neq u - \ell, u, u + \ell, u + 2\ell$. We will separate the remainder of Case 2.2 into two subcases: in Case 2.2.1, we consider $b_{u-\ell} \neq 0$, in Case 2.2.2, we suppose $b_{u-\ell} = 0$.

Case 2.2.1. Assume $b_{u-\ell} \neq 0$. From (5.70) with $i = u - \ell$ and $j = u + 2\ell$, we obtain

$$a_{u+2\ell} b_{u-\ell} = 0,$$

which implies $a_{u+2\ell} = 0$. If we consider (5.70) with $i = u - \ell$ and $j = u + \ell$, then

$$a_{u-\ell} b_{u+\ell} + a_{u+\ell} b_{u-\ell} = 0.$$

Recalling that $b_{u+\ell}$ is nonzero, this implies either $a_{u-\ell} = a_{u+\ell} = 0$ or $a_{u-\ell}, a_{u+\ell} \neq 0$ and $\frac{a_{u-\ell}}{b_{u-\ell}} = \frac{a_{u+\ell}}{b_{u+\ell}}$. We separate these two subcases:

Case 2.2.1. (i) Assume $a_{u-\ell} = a_{u+\ell} = 0$. Then

$$L_1(X) = a_u X^{2^u} \qquad \text{and} \qquad L_2(X) = b_{u-\ell} X^{2^{u-\ell}} + b_{u+\ell} X^{2^{u+\ell}},$$

where all coefficients are nonzero. We plug these polynomials into the left-hand side of (5.63) and obtain

$$L_1(x)^{2^{2k}(2^k+1)} = a_u^{2^{2k}(2^k+1)} x^{2^{u+2k}(2^k+1)}$$

and

$$L_1(x)^{2^{2k}} L_2(x)^{2^k} = a_u^{2^{2k}} b_{u-\ell}^{2^k} x^{2^{u-\ell+k}(2^{k+\ell}+1)} + a_u^{2^{2k}} b_{u+\ell}^{2^k} x^{2^{u+\ell+k}(2^{k-\ell}+1)}$$

and

$$\begin{aligned}\beta L_2(x)^{2^k+1} &= \beta b_{u-\ell}^{2^k+1} x^{2^{u-\ell}(2^k+1)} + \beta b_{u+\ell}^{2^k+1} x^{2^{u+\ell}(2^k+1)} \\ &\quad + \beta b_{u-\ell}^{2^k} b_{u+\ell} x^{2^{u+\ell}(2^{k-2\ell}+1)} + \beta b_{u+\ell}^{2^k} b_{u-\ell} x^{2^{u-\ell}(2^{k+2\ell}+1)}.\end{aligned} \tag{5.80}$$

As in previous cases, not all terms containing the factor x^{2^k+1} can be canceled simultaneously. Thus, we need $k = \ell$ to represent them on the right-hand side of (5.63). However, if $k = \ell$, the left-hand side of (5.63) contains the terms

$$a_u^{2^{2k}} b_{u-k}^{2^k} x^{2^u(2^{2k}+1)} \qquad \text{and} \qquad \beta b_{u+k}^{2^k} b_{u-k} x^{2^{u-k}(2^{3k}+1)},$$

which cannot be represented in the form $c_i x^{2^{i+2k}(2^k+1)}$ on the right-hand side of (5.63). Hence, their coefficients need to be zero, which is a contradiction.

Case 2.2.1. (ii) Assume $a_{u-\ell}, a_{u+\ell} \neq 0$ and $\frac{a_{u-\ell}}{b_{u-\ell}} = \frac{a_{u+\ell}}{b_{u+\ell}}$. Then

$$\begin{aligned}L_1(X) &= a_{u-\ell} X^{2^{u-\ell}} + a_u X^{2^u} + a_{u+\ell} X^{2^{u+\ell}} \\ \text{and } L_2(X) &= b_{u-\ell} X^{2^{u-\ell}} + b_{u+\ell} X^{2^{u+\ell}},\end{aligned}$$

where all coefficients are nonzero. We plug these polynomials into the left-hand side of (5.63). Then $L_1(x)^{2^{2k}(2^k+1)}$ is as in (5.77) and $\beta L_2(x)^{2^k+1}$ is as in (5.80). Moreover,

$$\begin{aligned}L_1(x)^{2^{2k}} L_2(x)^{2^k} &= a_{u-\ell}^{2^{2k}} b_{u-\ell}^{2^k} x^{2^{u-\ell+k}(2^k+1)} + a_{u+\ell}^{2^{2k}} b_{u+\ell}^{2^k} x^{2^{u+\ell+k}(2^k+1)} \\ &\quad + a_{u-\ell}^{2^{2k}} b_{u+\ell}^{2^k} x^{2^{u+\ell+k}(2^{k-2\ell}+1)} + a_u^{2^{2k}} b_{u-\ell}^{2^k} x^{2^{u-\ell+k}(2^{k+\ell}+1)} \\ &\quad + a_u^{2^{2k}} b_{u+\ell}^{2^k} x^{2^{u+\ell+k}(2^{k-\ell}+1)} + a_{u+\ell}^{2^{2k}} b_{u-\ell}^{2^k} x^{2^{u-\ell+k}(2^{k+2\ell}+1)}.\end{aligned} \tag{5.81}$$

By the same reasoning as in Case 2.2.1. (i), it follows that $k = \ell$. However, if $k = \ell$, then, for example, the fourth term of (5.81) neither can be canceled by any other terms on the left-hand side of (5.63), nor can it be represented on the right-hand side of (5.63). This implies $a_u = 0$ or $b_{u-\ell} = 0$, which contradicts our assumption.

Case 2.2.2. Assume $b_{u-\ell} = 0$. From (5.70) with $i = u + \ell$ and $j = u - \ell$, it follows that

$$a_{u-\ell} b_{u+\ell} = 0,$$

which, recalling that $b_{u+\ell} \neq 0$, implies $a_{u-\ell} = 0$. Then

$$L_1(X) = a_u X^{2^u} + a_{u+\ell} X^{2^{u+\ell}} + a_{u+2\ell} X^{2^{u+2\ell}} \qquad \text{and} \qquad L_2(X) = b_{u+\ell} X^{2^{u+\ell}},$$

where a_u and $b_{u+\ell}$ are nonzero. Plugging these polynomials into (5.63), the expressions $L_1(x)^{2^{2k}(2^k+1)}$, $L_1(x)^{2^{2k}} L_2(x)^{2^k}$ and $\beta L_2(x)^{2^k+1}$ are as in (5.77), (5.78) and (5.79), respectively, when substituting u by $u + \ell$. By the same reasoning as in Case 2.1.1. (i), it follows that $k = \ell$. If $k = \ell$, analogously to Case 2.1.1. (i), the following terms occur on the left-hand side of (5.63):

$$a_{u+2k}^{2^{3k}} a_u^{2^{2k}} x^{2^{u+2k}(2^{3k}+1)}, \qquad (a_{u+k}^{2^{3k}} a_u^{2^{2k}} + a_{u+2k}^{2^{2k}} b_{u+k}^{2^k}) x^{2^{u+2k}(2^{2k}+1)}.$$

As neither of them can be represented on the right-hand side of (5.63), their coefficients need to be zero. Since $a_u \neq 0$, it follows that $a_{u+2k} = 0$, and, consequently, $a_{u+k} = 0$. Hence, $L_1(X)$ and $L_2(X)$ are monomials of the form

$$L_1(X) = a_u X^{2^u} \qquad \text{and} \qquad L_2(X) = b_{u+k} X^{2^{u+k}}, \tag{5.82}$$

and we have $M_1(X) = a_u^{2^{2k}} b_{u+k}^{2^k} X^{2^{u+2k+1}}$ and $M_2(X) = 0$.

Note that if we consider Case 2.2 with $a_u = 0$ and $b_u \neq 0$, we obtain

$$L_1(X) = a_{u+k} X^{2^{u+k}} \qquad \text{and} \qquad L_2(X) = b_u X^{2^u} \tag{5.83}$$

together with $M_1(X) = a_{u+k}^{2^{2k}} b_u^{2^k} X^{2^{u+2k+1}}$ and $M_2(X) = 0$, from Case 2.2.2.

This concludes the proof of **Claim 5.2**. We summarize the results we have obtained so far. If the Taniguchi APN functions $f_{k,1,\beta}$ and $f_{\ell,1,\beta'}$ are EL-equivalent, then $k = \ell$, and the polynomials $L_1(X)$ and $L_2(X)$ are of the following shapes: either, one of $L_1(X)$ and $L_2(X)$ is zero and the other one is a monomial, see (5.66) and (5.67), or both $L_1(X)$ and $L_2(X)$ are monomials, either of the same degree or of degrees 2^u and 2^{u+k}, see (5.76), (5.82) and (5.83). Vice versa, the same statements hold for $L_3(Y)$ and $L_4(Y)$.

It remains to show that the EL-equivalence of $f_{k,1,\beta}$ and $f_{k,1,\beta'}$ implies $\beta' = \beta^{2^i}$ for some $i \in \{0, \ldots, m-1\}$. Combining the results on $L_1(X), L_2(X), L_3(Y), L_4(Y)$ mentioned above, it is clear that the polynomials $L_A(X,Y)$ and $L_B(X,Y)$ have to be of one of the following forms:

(a) $L_A(X,Y) = a_u X^{2^u} + \bar{a}_w Y^{2^w}$ and $L_B(X,Y) = b_u X^{2^u} + \bar{b}_w Y^{2^w}$,

(b) $L_A(X,Y) = a_u X^{2^u} + \bar{a}_w Y^{2^w}$ and $L_B(X,Y) = b_u X^{2^u} + \bar{b}_{w+k} Y^{2^{w+k}}$,

(c) $L_A(X,Y) = a_u X^{2^u} + \bar{a}_{w+k} Y^{2^{w+k}}$ and $L_B(X,Y) = b_u X^{2^u} + \bar{b}_w Y^{2^w}$,

(d) $L_A(X,Y) = a_u X^{2^u} + \bar{a}_w Y^{2^w}$ and $L_B(X,Y) = b_{u+k} X^{2^{u+k}} + \bar{b}_w Y^{2^w}$,

(e) $L_A(X,Y) = a_{u+k} X^{2^{u+k}} + \bar{a}_w Y^{2^w}$ and $L_B(X,Y) = b_u X^{2^u} + \bar{b}_w Y^{2^w}$,

(f) $L_A(X,Y) = a_u X^{2^u} + \bar{a}_w Y^{2^w}$ and $L_B(X,Y) = b_{u+k} X^{2^{u+k}} + \bar{b}_{w+k} Y^{2^{w+k}}$,

(g) $L_A(X,Y) = a_u X^{2^u} + \bar{a}_{w+k} Y^{2^{w+k}}$ and $L_B(X,Y) = b_{u+k} X^{2^{u+k}} + \bar{b}_w Y^{2^w}$,

(h) $L_A(X,Y) = a_{u+k} X^{2^{u+k}} + \bar{a}_w Y^{2^w}$ and $L_B(X,Y) = b_u X^{2^u} + \bar{b}_{w+k} Y^{2^{w+k}}$,

(i) $L_A(X,Y) = a_{u+k} X^{2^{u+k}} + \bar{a}_{w+k} Y^{2^{w+k}}$ and $L_B(X,Y) = b_u X^{2^u} + \bar{b}_w Y^{2^w}$.

Note that, as $L(X,Y) = (L_A(X,Y), L_B(X,Y))$ has to be a permutation polynomial, it is neither possible that $L_A(X,Y)$ or $L_B(X,Y)$ is zero nor that both $L_A(X,Y)$ and $L_B(X,Y)$ depend only on X or only on Y. We will show that all cases listed above lead to the conclusion that $L_A(X,Y)$ and $L_B(X,Y)$ need to be monomials of the same degree of the shape

$$L_A(X,Y) = a_u X^{2^u} \qquad \text{and} \qquad L_B(X,Y) = b_u Y^{2^u}. \tag{5.84}$$

We rewrite (5.61) and (5.62) considering $k = \ell$:

$$\begin{aligned} &L_A(x,y)^{2^{2k}(2^k+1)} + L_A(x,y)^{2^{2k}} L_B(x,y)^{2^k} + \beta L_B(x,y)^{2^k+1} \\ &\qquad = N_1(x^{2^{2k}(2^k+1)} + x^{2^{2k}} y^{2^k} + \beta' y^{2^k+1}) + N_3(xy) + M_A(x,y), \end{aligned} \tag{5.85}$$

$$\begin{aligned} &L_A(x,y) L_B(x,y) \\ &\qquad = N_2(x^{2^{2k}(2^k+1)} + x^{2^{2k}} y^{2^k} + \beta' y^{2^k+1}) + N_4(xy) + M_B(x,y). \end{aligned} \tag{5.86}$$

We will plug all the possible combinations **(a)**–**(i)** into these equations. We start with **(b)**. Plugging the polynomials of **(b)** into the left-hand side of (5.86), we obtain

$$\begin{aligned} L_A(x,y) L_B(x,y) = {}& a_u b_u x^{2^{u+1}} + \overline{a}_w \overline{b}_{w+k} y^{2^w(2^k+1)} \\ &+ a_u \overline{b}_{w+k} x^{2^u} y^{2^{w+k}} + \overline{a}_w b_u x^{2^u} y^{2^w}. \end{aligned} \tag{5.87}$$

Note that the first term of (5.87) is linearized. As there is no term containing the factor x^{2^k+1} in (5.89), we need $N_2(X) = 0$ on the right-hand side of (5.86). This implies, first, that the coefficient $\overline{a}_w \overline{b}_{w+k}$ of the second summand of (5.87) has to be zero, and second, that the third and the fourth summand of (5.87) cannot be represented simultaneously on the right-hand side of (5.86). The coefficient of the second summand of (5.87) is zero if $\overline{a}_w$ or $\overline{b}_{w+k}$ is zero. We separate the proof into two cases:

Case 1. Assume $\overline{a}_w = 0$. Note that this implies $a_u \neq 0$ and $\overline{b}_{w+k} \neq 0$ as otherwise $L(X,Y)$ would not be a permutation polynomial. If $\overline{a}_w = 0$, then (5.86) holds only if $u = w + k$. Set $u = w + k$, and plug $L_A(x,y)$ and $L_B(x,y)$ into the left-hand side of (5.85). We obtain

$$L_A(x,y)^{2^{2k}(2^k+1)} = a_u^{2^{2k}(2^k+1)} x^{2^{u+2k}(2^k+1)} \tag{5.88}$$

and

$$L_A(x,y)^{2^{2k}} L_B(x,y)^{2^k} = a_u^{2^{2k}} b_u^{2^k} x^{2^{u+k}(2^k+1)} + a_u^{2^{2k}} \overline{b}_u^{2^k} x^{2^{u+2k}} y^{2^{u+k}} \tag{5.89}$$

and

$$\begin{aligned} \beta L_B(x,y)^{2^k+1} = {}& \beta b_u^{2^k+1} x^{2^u(2^k+1)} + \beta \overline{b}_u^{2^k+1} y^{2^u(2^k+1)} \\ &+ \beta b_u^{2^k} \overline{b}_u x^{2^{u+k}} y^{2^u} + \beta \overline{b}_u^{2^k} b_u x^{2^u} y^{2^{u+k}}. \end{aligned} \tag{5.90}$$

The fourth summand of (5.90) cannot be canceled by any other summand of (5.88)–(5.90), and it cannot be represented on the right-hand side of (5.85). As $\beta, \overline{b}_u \neq 0$, it follows that $b_u = 0$. Consequently, $L_A(X, Y)$ and $L_B(X, Y)$ are monomials of the same degree as in (5.84).

Case 2. Assume $\overline{b}_{w+k} = 0$. By the same reasoning as in Case 1, this implies $b_u \neq 0$ and $\overline{a}_u \neq 0$. Now, (5.86) holds for $u = w$. Set $u = w$ and plug $L_A(x, y)$ and $L_B(x, y)$ into the left-hand side of (5.85). The expression $L_A(x, y)^{2^{2k}} L_B(x, y)^{2^k}$ contains the term

$$\overline{a}_u^{2^{2k}} b_u^{2^k} x^{2^{u+k}} y^{2^{u+2k}},$$

which has a nonzero coefficient and cannot be canceled by the other terms on the left-hand side of (5.85). However, it cannot be represented on the right-hand side of (5.85). This is a contradiction.

By proceeding analogously to **(b)**, the cases **(c)**–**(e)** lead to the same result: $L_A(X, Y)$ and $L_B(X, Y)$ need to be as in (5.84).

We next study **(f)**. If we plug $L_A(X, Y)$ and $L_B(X, Y)$ of **(f)** into (5.86), we obtain

$$\begin{aligned} L_A(x, y) L_B(x, y) = {} & a_u b_{u+k} x^{2^u(2^k+1)} + \overline{a}_w \overline{b}_{w+k} y^{2^w(2^k+1)} \\ & + a_u \overline{b}_{w+k} x^{2^u} y^{2^{w+k}} + \overline{a}_w b_{u+k} x^{2^{u+k}} y^{2^w}. \end{aligned} \tag{5.91}$$

If all coefficients are nonzero, we need $u = w + 2k$ to represent the first and the second summand of (5.91) on the right-hand side of (5.86). Then, however, the fourth term of (5.91) cannot be represented on the right-hand side of (5.86), which is a contradiction.

Now assume one of the coefficients is zero. We show the case $b_{u+k} = 0$. If $b_{u+k} = 0$, it follows that a_u and $\overline{b}_{w+k}$ are nonzero as otherwise $L(X, Y)$ would not be a permutation polynomial. Moreover, as the first term of (5.91) vanishes, we need $N_2(X) = 0$. Then, also the second term of (5.91) cannot be represented on the right-hand side of (5.86) and $\overline{a}_w \overline{b}_{w+k}$ has to be zero. As $\overline{b}_{w+k} \neq 0$, it follows that $\overline{a}_w = 0$. Moreover, we need $u = w + k$ to represent the third summand of (5.91) on the right-hand side of (5.86). Consequently, $L_A(X, Y)$ and $L_B(X, Y)$ are monomials as in (5.84).

If we suppose $a_u = 0$ instead of $b_{u+k} = 0$, we end up with the same contradiction as in the study of **(b)**, Case 2. Analogous results can be obtained when assuming $\overline{a}_w = 0$ or $\overline{b}_{w+k} = 0$. Note that, by symmetry, case **(i)** leads to the same results as **(f)**. Moreover, an analogous approach also provides identical results for cases **(g)** and **(h)**.

It remains to study **(a)**. If we plug $L_A(X, Y)$ and $L_B(X, Y)$ of **(a)** into (5.86), we obtain

$$L_A(x, y) L_B(x, y) = a_u b_u x^{2^{u+1}} + \overline{a}_w \overline{b}_w y^{2^{w+1}} + (a_u \overline{b}_w + \overline{a}_w b_u) x^{2^u} y^{2^w}. \tag{5.92}$$

We separate two cases: in Case 1, the third term of (5.92) vanishes, in Case 2, its coefficient is nonzero.

Case 1. We first show that the third term of (5.92) can only vanish if all coefficients are nonzero. Suppose $a_u = 0$. Then $\overline{a}_w b_u$ has to be zero as well. However, this is not possible, as $a_u = 0$ implies that $\overline{a}_w$ and b_u are nonzero. By symmetry, the same result is obtained if we assume that any other coefficient is zero.

Consequently, assume all coefficients are nonzero and $\frac{a_u}{b_u} = \frac{\overline{a}_w}{\overline{b}_w}$. Then (5.86) does not provide any more information about the coefficients, as the left-hand side is a linearized polynomial. We plug $L_A(X,Y)$ and $L_B(X,Y)$ into the left-hand side of (5.85) and obtain

$$\begin{aligned} L_A(x,y)^{2^{2k}(2^k+1)} = {} & a_u^{2^{2k}(2^k+1)} x^{2^{u+2k}(2^k+1)} + \overline{a}_w^{2^{2k}(2^k+1)} y^{2^{w+2k}(2^k+1)} \\ & + a_u^{2^{3k}} \overline{a}_w^{2^{2k}} x^{2^{u+3k}} y^{2^{w+2k}} + \overline{a}_w^{2^{3k}} a_u^{2^{2k}} x^{2^{u+2k}} y^{2^{w+3k}} \end{aligned} \tag{5.93}$$

and

$$\begin{aligned} L_A(x,y)^{2^{2k}} L_B(x,y)^{2^k} = {} & a_u^{2^{2k}} b_u^{2^k} x^{2^{u+k}(2^k+1)} + \overline{a}_w^{2^{2k}} \overline{b}_w^{2^k} y^{2^{w+k}(2^k+1)} \\ & + a_u^{2^{2k}} \overline{b}_w^{2^k} x^{2^{u+2k}} y^{2^{w+k}} + \overline{a}_w^{2^{2k}} b_u^{2^k} x^{2^{u+k}} y^{2^{w+2k}} \end{aligned} \tag{5.94}$$

and

$$\begin{aligned} \beta L_B(x,y)^{2^k+1} = {} & \beta b_u^{2^k+1} x^{2^u(2^k+1)} + \beta \overline{b}_w^{2^k+1} y^{2^w(2^k+1)} + \\ & + \beta b_u^{2^k} \overline{b}_w x^{2^{u+k}} y^{2^w} + \beta \overline{b}_w^{2^k} b_u x^{2^u} y^{2^{w+k}}. \end{aligned} \tag{5.95}$$

No matter how we choose u and w, the third and the fourth summand of (5.93) cannot be canceled by the terms of (5.93)–(5.95), and they cannot be represented simultaneously on the right-hand side of (5.85). Hence, at least one of the coefficients needs be zero, which is a contradiction.

Case 2. Assume $a_u \overline{b}_w + \overline{a}_w b_u \neq 0$. As there are no terms on the left-hand side of (5.86) containing the factors x^{2^k+1} and y^{2^k+1}, it follows that $N_2(X) = 0$, and we need $u = w$ to represent the third summand of (5.92) on the right-hand side of (5.86). We plug $L_A(X,Y)$ and $L_B(X,Y)$ into (5.85) and obtain the same expressions as in (5.93)–(5.95) with $u = w$. Analogously to Case 1, the third and the fourth term of (5.93) cannot be represented on the right-hand side of (5.85) at the same time. Hence, $a_u \overline{a}_w$ has to be zero. Assuming $\overline{a}_w = 0$, we obtain, by similar reasoning as in the previous cases, that $L_A(X,Y)$ and $L_B(X,Y)$ have to be monomials of the same degree as in (5.84). Assuming $a_u = 0$, we obtain the same contradiction as in the study of **(b)**, Case 2.

In summary, the only choice of $L_A(X,Y)$ and $L_B(X,Y)$ that may satisfy (5.85) and (5.86) is $L_A(X,Y) = a_u X^{2^u}$ and $L_B(x,y) = \overline{b}_u Y^{2^u}$. Considering (5.86) for these monomials, it follows that $N_2(X) = 0$, $N_4(X) = a_u \overline{b}_u X^{2^u}$ and $M_B(X,Y) = 0$. If we plug $L_A(X,Y)$ and $L_B(X,Y)$ into (5.85), we obtain

$$\begin{aligned} a_u^{2^{2k}(2^k+1)} x^{2^{u+2k}(2^k+1)} + a_u^{2^{2k}} \bar{b}_u^{2^k} x^{2^{u+2k}} y^{2^{u+k}} + \beta \bar{b}_u^{2^k+1} y^{2^u(2^k+1)} \\ = N_1(x^{2^{2k}(2^k+1)} + x^{2^{2k}} y^{2^k} + \beta' y^{(2^k+1)}) + N_3(xy) + M_A(x,y). \end{aligned} \tag{5.96}$$

Obviously, $N_3(X) = 0$ and $M_A(X,Y) = 0$, and $N_1(X)$ has to be a monomial of degree 2^u, the same degree as $L_A(X,Y)$ and $L_B(X,Y)$.

Write $N_1(X) = c_u X^{2^u}$. Then (5.96) becomes

$$\begin{aligned} a_u^{2^{2k}(2^k+1)} x^{2^{u+2k}(2^k+1)} + a_u^{2^{2k}} \bar{b}_u^{2^k} x^{2^{u+2k}} y^{2^{u+k}} + \beta \bar{b}_u^{2^k+1} y^{2^u(2^k+1)} \\ = c_u x^{2^{u+2k}(2^k+1)} + c_u x^{2^{u+2k}} y^{u+2^k} + c_u \beta'^{2^u} y^{2^u(2^k+1)}, \end{aligned}$$

and the coefficients a_u, b_u, c_u have to meet the following conditions:

$$a_u^{2^{2k}(2^k+1)} = c_u, \qquad a_u^{2^{2k}} \bar{b}_u^{2^k} = c_u, \qquad \beta \bar{b}_u^{2^k+1} = c_u \beta'^{2^u}. \tag{5.97}$$

The first two equations of (5.97) imply $\bar{b}_u = a_u^{2^{2k}}$ and $c_u = \bar{b}_u^{2^k+1}$. Combining the later result with the third equation of (5.97), it follows that $\beta = \beta'^{2^u}$. Clearly, we can now find $a_u, \bar{b}_u$ and c_u such that the equations in (5.97) are satisfied. This concludes our proof. □

In Theorem 5.17, we use Theorem 5.13 and, in particular, (5.97) to determine the automorphism groups of Taniguchi APN functions under EL- and EA-equivalence. In Theorem 5.28, we present the precise number of inequivalent Taniguchi functions.

After determining the automorphism groups, we will complete the solution to the equivalence problem of Taniguchi APN functions in Corollary 5.19 by showing that $f_{k,0,\beta}$ is CCZ-inequivalent to $f_{k,1,\beta'}$ for all admissible $\beta, \beta' \in \mathbb{F}_{2^m}^*$.

5.5 Automorphism groups of Gold, Zhou-Pott, Carlet and Taniguchi APN functions

In this section, we present the automorphism groups of Gold, Zhou-Pott, Carlet (for m even) and Taniguchi APN functions under EL- and under EA-equivalence. For any function f from these classes, we obtain $\mathrm{Aut}_{EL}(f)$ from the precise shape of the EL-mappings we determined in the previous sections. We then use Proposition 4.3 to determine $\mathrm{Aut}_{EA}(f)$. Recall that Remark 4.2 indicates that if f is a quadratic APN function on $\mathbb{F}_{2^n}$ with $n \geq 4$, we also have $\mathrm{Aut}(f) = \mathrm{Aut}_{EA}(f)$. Our results will eventually allow us to determine the equivalence between Zhou-Pott and Taniguchi APN functions. This will be the final piece needed to complete the study of the equivalence of Taniguchi APN functions.

We start with Gold APN functions $x \mapsto x^{2^k+1}$. Note that Corollary 5.14 is well known. These results were originally given by Berger and Charpin [8, Proposition 5] in a coding theory context. We restate their result to demonstrate how it can be derived from Theorem 5.1 and Proposition 5.2.

Corollary 5.14. *Let f be a Gold APN function on $\mathbb{F}_{2^n}$. If $n \geq 5$, then $\mathrm{Aut}_{EL}(f)$ is isomorphic to the general semi-linear group $\Gamma\mathrm{L}(1, 2^n)$ of degree 1 over $\mathbb{F}_{2^n}$, and*

$$|\mathrm{Aut}_{EL}(f)| = n(2^n - 1) \qquad \textit{and} \qquad |\mathrm{Aut}_{EA}(f)| = n2^n(2^n - 1).$$

If $n = 4$, then

$$|\mathrm{Aut}_{EL}(f)| = 360 \qquad \textit{and} \qquad |\mathrm{Aut}_{EA}(f)| = 5760.$$

Proof. In Theorem 5.1, we showed that for $n \geq 5$, the EL-automorphisms of a Gold APN function are precisely described by polynomials of the shape $L(X) = a_u X^{2^u}$, $N(X) = a_u^{2^k+1} X^{2^u}$ and $M(X) = 0$. As $u \in \{0, \dots, n-1\}$ and $a_u \in \mathbb{F}_{2^n}^*$, there exist $n(2^n - 1)$ distinct monomials $L(X)$. By fixing u and a_u, the monomial $N(X)$ is uniquely determined. Clearly, $\mathrm{Aut}_{EL}(f)$ is isomorphic to the semilinear group $\Gamma\mathrm{L}(1, 2^n)$, and $|\mathrm{Aut}_{EL}(f)| = n(2^n - 1)$.

If $n = 4$, we obtain the same number of monomial equivalence mappings as above: that is $4 \cdot (2^4 - 1) = 60$. Besides these monomials, we now additionally have the linearized polynomials presented in Proposition 5.2. The coefficients in both possible shapes of $L(X)$ and $N(X)$ only depend on some $a_u, a_{u+2} \in \mathbb{F}_{2^n}^*$, where $u \in \{0, 1\}$, such that $\frac{a_u}{a_{u+2}}$ is a non-cube. Consequently, for both polynomial pairs, we have 15 choices for a_u resulting in 10 choices for a_{u+2}. This gives us a total number of $300 = 2 \cdot 15 \cdot 10$ distinct pairs of $L(X)$ and $N(X)$. Adding this number to the number of distinct monomials, we obtain $|\mathrm{Aut}_{EL}(f)| = 60 + 300 = 360$.

In both of the above cases, the automorphism group $\mathrm{Aut}_{EA}(f)$ is obtained from $\mathrm{Aut}_{EL}(f)$ using Proposition 4.3. □

Berger and Charpin [8] actually showed that for $n = 4$, the automorphism group $\mathrm{Aut}_{EL}(f)$ of the unique Gold APN function $f(x) = x^3$ is isomorphic to the general semilinear group $\Gamma\mathrm{L}(2, 4)$. Furthermore, we remark that the automorphism group $\mathrm{Aut}_{EA}(f)$ under EA-equivalence of any quadratic APN function f on $\mathbb{F}_{2^4}$ has order 5760 since there is only one EA-class of quadratic APN functions on $\mathbb{F}_{2^4}$. Therefore, we will only consider $\mathbb{F}_{2^{2m}}$ with $m > 2$, when determining the automorphism groups of the Zhou-Pott, Carlet and Taniguchi functions in the remainder of this section.

We next study Zhou-Pott functions. From the proof of Theorem 5.4, we can deduce the order of their automorphism group under EL-equivalence.

Theorem 5.15. *Let $m \geq 4$ be even, and let $f_{k,s,\alpha}$ be a Zhou-Pott APN function on $\mathbb{F}_{2^{2m}}$ from Theorem 4.6. Then*

$$|\mathrm{Aut}_{EL}(f_{k,s,\alpha})| = \begin{cases} 3m(2^m - 1) & \textit{if } s \in \{0, \frac{m}{2}\}, \\ \frac{3}{2}m(2^m - 1) & \textit{otherwise}, \end{cases}$$

and

$$|\mathrm{Aut}_{EA}(f_{k,s,\alpha})| = \begin{cases} 3m2^{2m}(2^m-1) & \text{if } s \in \{0, \frac{m}{2}\}, \\ 3m2^{2m-1}(2^m-1) & \text{otherwise.} \end{cases}$$

Proof. We determine $|\mathrm{Aut}_{EL}(f_{k,\alpha,\beta})|$, then $|\mathrm{Aut}_{EA}(f_{k,\alpha,\beta})|$ follows from Proposition 4.3.

Using the same notation as in the proof of Theorem 5.4, we count the number of EL-mappings (L, M, N) that map $f_{k,s,\alpha}$ onto itself. For $m \geq 6$, we showed that $L_A(X,Y)$ and $L_B(X,Y)$ need to be monomials of the same degree 2^u as presented in (5.47), where $L_A(X,Y) = a_u X^{2^u}$ and $L_B(X,Y) = \overline{b}_u Y^{2^u}$, or, if $s \in \{0, \frac{m}{2}\}$, also as in (5.49), where $L_A(X,Y) = \overline{a}_u Y^{2^u}$ and $L_B(X,Y) = b_u X^{2^u}$. For both cases, we proved that $N_1(X)$ is also a monomial, $N_2(X) = N_3(X) = 0$, $N_4(X)$ is a monomial of degree 2^u that is uniquely determined by $L_A(X,Y)$ and $L_B(X,Y)$, and $M_A(X,Y) = M_B(X,Y) = 0$.

First, we consider the case $L_A(X,Y) = a_u X^{2^u}$ and $L_B(X,Y) = \overline{b}_u Y^{2^u}$. In this case, $N_1(X) = c_u X^{2^u}$. In the proof of Theorem 5.4, we showed that $u \in \{0,\dots,m-1\}$ and the coefficients $a_u, \overline{b}_u, c_u \in \mathbb{F}_{2^m}^*$ have to satisfy the equations $a_u^{2^k+1} = c_u$ and $\alpha \overline{b}_u^{2^s(2^k+1)} = \alpha^{2^u} c_u$ from (5.58). These conditions imply

$$\alpha^{2^u-1} a_u^{2^k+1} = \overline{b}_u^{2^s(2^k+1)}. \tag{5.98}$$

If we divide (5.98) by $a_u^{2^k+1}$, we have a cube on the right-hand side. Consequently, α^{2^u-1} also needs to be a cube. As $\gcd(2^u-1, 2^m-1) = 2^{\gcd(u,m)} - 1$ is divisible by 3 if and only if $\gcd(u,m)$ is even, α^{2^u-1} is a cube if and only if u is even. Since $u \in \{0,\dots,m-1\}$, we first have $\frac{m}{2}$ choices for u. Then we may choose a_u arbitrarily from $\mathbb{F}_{2^m}^*$, which means we have $2^m - 1$ choices for a_u. Every choice of a_u results in 3 choices for $\overline{b}_u$ since $x \mapsto x^{2^k+1}$ is a 3-to-1 mapping on $\mathbb{F}_{2^m}^*$ with m even. Finally, c_u is uniquely determined by a_u.

If $s \in \{0, \frac{m}{2}\}$, we can also choose $L_A(X,Y) = \overline{a}_u Y^{2^u}$ and $L_B(X,Y) = b_u X^{2^u}$. Then $N_1(X) = c_{u+s} X^{2^{u+s}}$, and $u \in \{0,\dots,m-1\}$ and the coefficients $\overline{a}_u, b_u, c_{u+s} \in \mathbb{F}_{2^m}^*$ have to satisfy the following equations that are given in (5.60): $\alpha b_u^{2^s(2^k+1)} = c_{u+s}$ and $\overline{a}_u^{2^k+1} = \alpha^{2^{u+s}} c_{u+s}$. From these conditions, it follows that

$$\overline{a}_u^{2^k+1} = \alpha^{2^{u+s}+1} b_u^{2^s(2^k+1)}. \tag{5.99}$$

Dividing (5.99) by $b_u^{2^s(2^k+1)}$, we obtain a cube on the left-hand side. Hence, $\alpha^{2^{u+s}+1}$ has to be a cube as well. Define $r = u + s$. Then α^{2^r+1} is a cube if and only if $\gcd(2^r+1, 2^m-1)$ is divisible by 3. It is well known that

$$\gcd(2^r+1, 2^m-1) = \frac{2^{\gcd(2r,m)}-1}{2^{\gcd(r,m)}-1}; \tag{5.100}$$

for a proof we refer to Zhou and Pott [109]. Write $m = 2^n \cdot q$ for a positive integer n

and odd q. Then

$$\gcd(2r, m) = \begin{cases} \gcd(r, m) & \text{if } 2^n \mid r, \\ 2\gcd(r, m) & \text{if } 2^n \nmid r. \end{cases} \tag{5.101}$$

Combining (5.100) with (5.101), it follows that

$$\gcd(2^r + 1, 2^m - 1) = \begin{cases} 1 & \text{if } 2^n \mid r, \\ 2^{\gcd(r,m)} + 1 & \text{if } 2^n \nmid r. \end{cases}$$

As m is even, 3 divides $2^{\gcd(r,m)} + 1$ if and only if r is odd. Recall that $r = u + s$. Consequently, if $s = 0$, then u has to be odd, and if $s = \frac{m}{2}$, then u has to be odd if $4 \mid m$, and u has to be even if $4 \nmid m$. In summary, in each of these three cases, either u has to be even or u has to be odd. As $u \in \{0, \dots, m-1\}$, we have, for both u even and u odd, $\frac{m}{2}$ choices for u. By the same arguments as above, we then have $2^m - 1$ possibilities to choose $\overline{a}_u$ resulting in 3 choices for b_u. Eventually, c_{u+s} is uniquely determined by the choice of $\overline{a}_u$. Hence, if $s \in \{0, \frac{m}{2}\}$, then there exist twice as many EL-automorphisms of $f_{k,s,\alpha}$ as in the case $s \notin \{0, \frac{m}{2}\}$.

We checked the case $m = 4$ computationally with `Magma` [16]. According to Theorem 5.4, there exist two equivalence classes of Zhou-Pott functions on $\mathbb{F}_{2^8}$, represented by $f_{1,0,\alpha}$ and $f_{1,2,\alpha}$ for an arbitrary non-cube $\alpha \in \mathbb{F}_{2^4}$. For both functions we obtained $|\mathrm{Aut}_{EA}(f_{k,s,\alpha})|$ by computing the automorphism group $\mathrm{Aut}(\mathcal{C}^{EA}_{f_{k,s,\alpha}})$ of the associated code $\mathcal{C}^{EA}_{f_{k,s,\alpha}}$ as described in Section 4.2. The value of $|\mathrm{Aut}_{EL}(f_{k,s,\alpha})|$ then follows from Proposition 4.3. Our computations confirm that for $m = 4$, the same formula as for $m \geq 6$ holds. □

From Theorem 5.15, we derive the automorphism group of Carlet APN functions on $\mathbb{F}_{2^{2m}}$ when m is even.

Corollary 5.16. *Let $m \geq 4$ be even, and let $f_{k,\alpha,\beta}$ be a Carlet APN function on $\mathbb{F}_{2^{2m}}$ from Proposition 4.5. Then*

$$|\mathrm{Aut}_{EL}(f_{k,\alpha,\beta})| = 3m(2^m - 1) \qquad \textit{and} \qquad |\mathrm{Aut}_{EA}(f_{k,\alpha,\beta})| = 3m2^{2m}(2^m - 1).$$

Proof. In Theorem 5.8, we showed that on $\mathbb{F}_{2^{2m}}$, where m is even, any Carlet APN function is EL-equivalent to a Zhou-Pott APN function with $s = 0$. Consequently, their automorphism groups under EL- and under EA-equivalence are isomorphic. The result now follows from Theorem 5.15. □

We now focus on Taniguchi APN functions. We can derive the order of their automorphism group under EL-equivalence from the proof of Theorem 5.13. Note that Theorem 5.17 only holds for $m \geq 4$. If $m = 3$, the unique Taniguchi APN function $f_{1,1,\beta}$ on $\mathbb{F}_{2^6}$ is EA-equivalent to the APN function $x \mapsto x^3 + ux^{24} + x^{10}$, where u is primitive in $\mathbb{F}_{2^6}$, that was presented by Browning, Dillon, Kibler, and McQuistan [22]. In this case, $|\mathrm{Aut}_{EA}(f_{1,1,\beta})| = 896$.

Theorem 5.17. *Let $m \geq 4$, and let $f_{k,\alpha,\beta}$ be a Taniguchi APN function on $\mathbb{F}_{2^{2m}}$ from Theorem 4.6. Define $\beta' = \frac{\beta}{\alpha^{2^{-k}+1}}$. Then*

$$|\mathrm{Aut}_{EL}(f_{k,\alpha,\beta})| = \begin{cases} 3m(2^m-1) & \textit{if } \alpha = 0 \textit{ and } m = 4, \\ \frac{3}{2}m(2^m-1) & \textit{if } \alpha = 0 \textit{ and } m \geq 6, \\ \dfrac{m(2^m-1)}{\min\{u \geq 1 : \beta'^{2^u} = \beta'\}} & \textit{if } \alpha \neq 0, \end{cases}$$

and

$$|\mathrm{Aut}_{EA}(f_{k,\alpha,\beta})| = \begin{cases} 3m2^{2m}(2^m-1) & \textit{if } \alpha = 0 \textit{ and } m = 4, \\ 3m2^{2m-1}(2^m-1) & \textit{if } \alpha = 0 \textit{ and } m \geq 6, \\ \dfrac{m2^{2m}(2^m-1)}{\min\{u \geq 1 : \beta'^{2^u} = \beta'\}} & \textit{if } \alpha \neq 0. \end{cases}$$

Proof. We determine $|\mathrm{Aut}_{EL}(f_{k,\alpha,\beta})|$, then $|\mathrm{Aut}_{EA}(f_{k,\alpha,\beta})|$ follows from Proposition 4.3.

If $\alpha = 0$, then m is even and, according to Proposition 5.10, the Taniguchi APN function $f_{k,0,\beta}$ is linearly equivalent to the Zhou-Pott APN function $g_{k,2k,\beta}$. Hence, their automorphism groups are isomorphic, and the result follows from Theorem 5.15. Note that if $m = 4$, then $k = 1$ and $2k = \frac{m}{2}$, whereas for $m \geq 6$, we always have $2k \neq \frac{m}{2}$ since k and m are coprime.

If $\alpha \neq 0$, we know from Proposition 5.12 (a) that $f_{k,\alpha,\beta}$ is linearly equivalent to $f_{k,1,\beta'}$. We study the case $\alpha = 1$. For $m = 4$ the results can be confirmed computationally with `Magma` [16] as described for the Zhou-Pott function in the proof of Theorem 5.15. Assume $m \geq 5$. Then the proof of Theorem 5.13 holds, we use the same notation. We count the number of EL-automorphisms (L, M, N) of $f_{k,1,\beta'}$. We showed that $L_A(X,Y) = a_u X^{2^u}$ and $L_B(X,Y) = \overline{b}_u Y^{2^u}$. Moreover, $M_A(X,Y) = M_B(X,Y) = 0$, $N_2(X) = N_3(X) = 0$, and $N_4(X) = a_u\overline{b}_u X^{2^u}$ is a uniquely determined monomial of degree 2^u. Furthermore, $N_1(X) = c_u X^{2^u}$. We next consider the conditions given in (5.97) that $u \in \{0, \dots, m-1\}$ and the coefficients $a_u, \overline{b}_u, c_u \in \mathbb{F}_{2^m}^*$ have to meet. We showed that

$$\overline{b}_u = a_u^{2^{2k}}, \qquad c_u = \overline{b}_u^{2^k+1}, \qquad \text{and} \qquad \beta'^{2^u} = \beta'.$$

The number of u such that $\beta'^{2^u} = \beta'$ is given by

$$\frac{m}{\min\{u \geq 1 : \beta'^{2^u} = \beta'\}}.$$

For every u, we have $2^m - 1$ choices for a_u. By fixing a_u, the coefficients $\overline{b}_u$ and c_u are uniquely determined. □

From Theorem 5.17, we easily derive the following result about the inequivalence of Taniguchi and Zhou-Pott APN functions. Recall that Zhou-Pott APN functions only exist on $\mathbb{F}_{2^{2m}}$ with m even and that we already solved the case $\alpha = 0$ in Proposition 5.10.

Corollary 5.18. *Let $m \geq 4$ be even. Let $f_{k,\alpha,\beta}$, where $\alpha \neq 0$, be a Taniguchi APN function on $\mathbb{F}_{2^{2m}}$ from Theorem 4.8, and let $g_{\ell,s,\gamma}$ be a Zhou-Pott APN function on $\mathbb{F}_{2^{2m}}$ from Theorem 4.6. Then $f_{k,\alpha,\beta}$ and $g_{\ell,s,\gamma}$ are CCZ-inequivalent.*

Proof. We determined the order of the automorphism group under EA-equivalence for Zhou-Pott and Taniguchi APN functions in Theorem 5.15 and Theorem 5.17, respectively. Clearly, $\frac{m}{\min\{u \geq 1 : \beta'^{2^u} = \beta'\}} < \frac{3}{2}m < 3m$, which implies $|\mathrm{Aut}_{EA}(f_{k,\alpha,\beta})| \neq |\mathrm{Aut}_{EA}(g_{\ell,s,\gamma})|$. Consequently, the functions are EA-inequivalent. It follows from Theorem 4.1 that they are also CCZ-inequivalent. □

From Corollary 5.18, we eventually derive the final piece to determine the complete equivalence of Taniguchi APN functions.

Corollary 5.19. *Let $m \geq 4$ be even. Two Taniguchi APN functions $f_{k,0,\beta}$ and $f_{\ell,\alpha',\beta'}$, where $\alpha' \neq 0$, on $\mathbb{F}_{2^{2m}}$ from Theorem 4.8 are CCZ-inequivalent.*

Proof. According to Proposition 5.10, $f_{k,0,\beta}$ is CCZ-equivalent to a Zhou-Pott APN function $g_{k,2k,\gamma}$ from Theorem 4.6. The result now follows from Corollary 5.18. □

5.6 On the number of inequivalent APN functions

In this section, we use the results about the equivalence of Zhou-Pott and Taniguchi APN functions we obtained in the previous sections to precisely determine the number of CCZ-inequivalent functions within each of these families. For even m, we add a result about the number of Carlet APN functions. For completeness, we remark that clearly on $\mathbb{F}_{2^n}$, there exist $\frac{\varphi(n)}{2}$ CCZ-inequivalent Gold APN functions, where φ denotes Euler's totient function.

We start with the Zhou-Pott functions. Recall that these functions are APN only if m is even. We obtain the following result immediately from Theorem 5.4.

Corollary 5.20. *On $\mathbb{F}_{2^{2m}}$, where $m \geq 4$ is even, there exist exactly*

$$\frac{\varphi(m)}{2}\left(\left\lfloor \frac{m}{4} \right\rfloor + 1\right)$$

CCZ-inequivalent Zhou-Pott APN functions $f_{k,s,\alpha}$ from Theorem 4.6, where φ denotes Euler's totient function.

Proof. According to Proposition 5.3, we may fix α and we only need to consider $0 < k < \frac{m}{2}$ and $0 \leq s \leq \frac{m}{2}$. We have shown in Theorem 5.4 that for $0 < k, \ell < \frac{m}{2}$ and $0 \leq s, t \leq \frac{m}{2}$, two Zhou-Pott APN functions $f_{k,s,\alpha}$ and $f_{\ell,t,\beta}$ on $\mathbb{F}_{2^{2m}}$, where m is even, are CCZ-inequivalent if and only if $k \neq \ell$ and $s \neq t$. We count the number of distinct parameter pairs (k, s) we can choose: as $0 \leq s \leq \frac{m}{2}$ and s is even, we have

$\lfloor \frac{m}{4} \rfloor$ nonzero choices for s plus the choice $s = 0$. As $0 < k < \frac{m}{2}$ and $\gcd(k, m) = 1$, we have $\frac{\varphi(m)}{2}$ choices for k. □

In Table 5.1, we present the result of Corollary 5.20 for small values of m. Note that from computational results, only the number of inequivalent Zhou-Pott APN functions for $m = 4$ was known.

In Figure 5.2, we illustrate Corollary 5.20 for $m \leq 1000$. The upper bound $\frac{m(m+4)}{16}$ on the number of inequivalent Zhou-Pott APN functions on $\mathbb{F}_{2^{2m}}$ holds for all $m \geq 4$. It is sharp whenever m is a power of 2. The lower bound $\frac{m\sqrt{m}}{2}$ holds for $m > 210$.

From Corollary 5.9, we easily obtain the number of inequivalent Carlet APN functions on $\mathbb{F}_{2^{2m}}$, where m is even. Our computations hint that Corollary 5.21 may also hold for m odd.

Corollary 5.21. *On $\mathbb{F}_{2^{2m}}$, where $m \geq 4$ is even, there exist precisely $\frac{\varphi(m)}{2}$ CCZ-inequivalent Carlet APN functions $f_{k,\alpha,\beta}$ from Proposition 4.5, where φ denotes Euler's totient function.*

Proof. In Corollary 5.9, we have shown that two Carlet APN functions $f_{k,\alpha,\beta}$ and $f_{\ell,\alpha',\beta'}$ on $\mathbb{F}_{2^{2m}}$, where m is even, are CCZ-equivalent if and only if $k \equiv \pm\ell \pmod{m}$. As $\gcd(k, m) = 1$, we have $\frac{\varphi(m)}{2}$ choices for k. □

Next, we focus on Taniguchi APN functions. Recall that unlike the Zhou-Pott APN functions, they exist on $\mathbb{F}_{2^{2m}}$ for any m. We present the precise number of CCZ-inequivalent Taniguchi APN functions on $\mathbb{F}_{2^{2m}}$ in Theorem 5.28. To determine this number, we count the combinations of admissible parameters that lead to inequivalent functions. This time, we need to do some preparatory work, though, as counting all valid β turns out to be quite complicated. Therefore, we remark that in Corollary 5.29, we give a nice and very good lower bound on the number of inequivalent Taniguchi APN functions that can be immediately obtained from Theorem 5.13 in combination with Lemma 5.23.

Recall from Proposition 5.12 that every Taniguchi APN function $f_{k,\alpha,\beta}$ with $\alpha \neq 0$ is CCZ-equivalent to a Taniguchi function $f_{k,1,\beta'}$ for some $\beta' \in \mathbb{F}_{2^m}^*$. Hence, we only need to consider functions with $\alpha = 0$ or $\alpha = 1$. As we have shown in Proposition 5.10 that $f_{k,0,\beta}$ is part of the Zhou-Pott family, for which we determined the number of inequivalent functions in Corollary 5.20, we focus on the case $\alpha = 1$ first.

In Theorem 5.13, we showed that two Taniguchi APN functions $f_{k,1,\beta}$ and $f_{k,1,\beta'}$ on $\mathbb{F}_{2^{2m}}$ are CCZ-equivalent if and only if $\beta' = \beta^{2^i}$ for some $i \in \{0, \dots, m-1\}$. Consequently, to obtain the exact number of β that provide inequivalent functions

Table 5.1: Number $n(m)$ of CCZ-inequivalent Zhou-Pott APN functions on $\mathbb{F}_{2^{2m}}$ for small values of m.

m	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34
$n(m)$	2	2	6	6	8	12	20	15	24	30	28	42	48	32	72	72

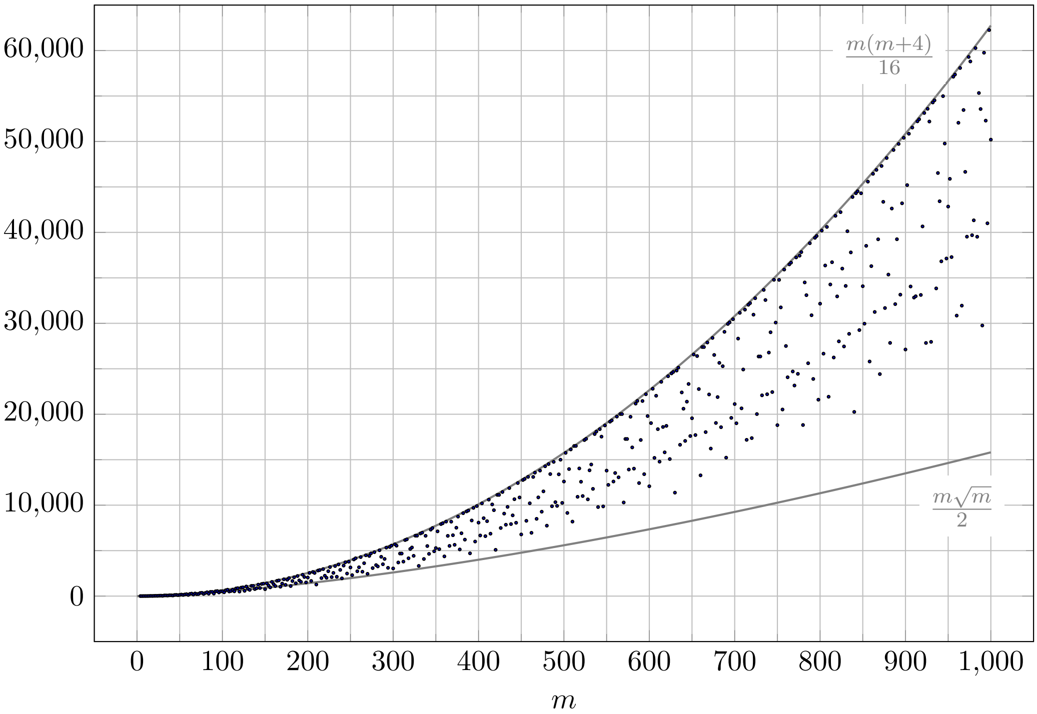

Figure 5.2: Number of CCZ-inequivalent Zhou-Pott APN functions on $\mathbb{F}_{2^{2m}}$ for $m \leq 1000$.

for fixed k, we need to determine the number of orbits of $\beta \in \mathbb{F}_{2^m}^*$ such that the polynomial $X^{2^k+1} + X + \beta$ has no root in $\mathbb{F}_{2^m}$ under the action of the Galois group $\mathrm{Gal}(\mathbb{F}_{2^m}/\mathbb{F}_2)$. We will do so in Proposition 5.27 with the help of the following series of lemmas.

First, in Lemma 5.22, we present a special case of a result by Bluher [13], who determined the possible numbers of roots of the polynomial $X^{p^k+1} + X + \beta$ in $\mathbb{F}_{p^m}$ for any prime p and integers k and m. We only restate her result for $p = 2$.

Lemma 5.22. *Let k, m be positive integers. For any $\beta \in \mathbb{F}_{2^m}^*$, the polynomial $P(X) = X^{2^k+1} + X + \beta$ has either none, one, two or $2^{\gcd(k,m)} + 1$ roots in $\mathbb{F}_{2^m}$. In particular, if $\gcd(k, m) = 1$, then $P(X)$ has either none, one or three roots in $\mathbb{F}_{2^m}$.*

Bluher [13, Theorem 5.6] additionally determined the number of $\beta \in \mathbb{F}_{p^m}^*$ such that $X^{p^k+1} + X + \beta$ has none, one, two or $p^{\gcd(k,m)} + 1$ roots in $\mathbb{F}_{p^m}$. In Lemma 5.23, we present her result for $p = 2$, $\gcd(k, m) = 1$ and $X^{2^k+1} + X + \beta$ having no root in $\mathbb{F}_{2^m}$. In this specific form, the result was also given by Helleseth and Kholosha [68, Theorem 1].

Lemma 5.23. *The number of $\beta \in \mathbb{F}_{2^m}^*$ such that the polynomial $X^{2^k+1} + X + \beta$ has no root in $\mathbb{F}_{2^m}$ is $\frac{2^m-1}{3}$ if m is even and $\frac{2^m+1}{3}$ if m is odd.*

To determine the number of orbits under the action of $\mathrm{Gal}(\mathbb{F}_{2^m}/\mathbb{F}_2)$ into which all β from Lemma 5.23 decompose, we need the following technical lemmas.[1]

Lemma 5.24. *If k is a positive integer coprime to 3, then $3k$ does not divide 2^k+1.*

Proof. Assume, by way of contradiction, that $3k \mid 2^k+1$. By the Chinese Remainder Theorem, $2^k \equiv -1 \pmod 3$, which means that k is odd. Write $k = p_1^{t_1} \cdots p_s^{t_s}$ for primes $p_1, \dots, p_s$ such that $3 < p_1 < p_2 < \cdots < p_s$ and integers $t_i \geq 1$ for $i = 1, \dots, s$. For convenience, set $p = p_1$ and $t = t_1$ for the remainder of this proof.

Using the Chinese Remainder Theorem again, we also obtain $2^k \equiv -1 \pmod{p^t}$. Denote Euler's totient function by φ. Since $2^{2k} \equiv 1 \pmod{p^t}$, and the unit group of the integer ring $\mathbb{Z}_{p^t}$ has order $\varphi(p^t)$, it follows that the multiplicative order $\mathrm{ord}_{p^t}(2)$ of 2 modulo p^t divides $\gcd(2k, \varphi(p^t))$. Note that $\varphi(p^t) = (p-1)p^{t-1}$. Clearly, $p-1$ is even. Moreover, $p-1$ is not divisible by p_i for any $i \in \{1, \dots, s\}$ as $p-1 < p_i$ for all i. Recalling that $k = p^t p_2^{t_2} \cdots p_s^{t_s}$, it follows that $\gcd(2k, \varphi(p^t)) = 2p^{t-1}$. Consequently, $2^{2p^{t-1}} - 1 \equiv 0 \pmod{p^t}$, which implies $4^{p^{t-1}} - 1 \equiv 0 \pmod p$. As $4^p \equiv 4 \pmod p$, we obtain $4 - 1 \equiv 0 \pmod p$, and it follows that $p = 3$. This contradicts the assumption that $3 < p$. □

Lemma 5.25. *Let k and m be positive integers satisfying $\gcd(k, m) = 1$. Write $m = pr$ for a prime p and an integer r. Let $\beta \in \mathbb{F}_{2^r}^*$ such that the polynomial $P(X) = X^{2^k+1} + X + \beta$ has no root in $\mathbb{F}_{2^r}$.*

(a) If $p \neq 3$, then $P(X)$ has no root in $\mathbb{F}_{2^m}$.

(b) If $p = 3$, then $P(X)$ has exactly three roots in $\mathbb{F}_{2^m}$.

Proof. Set $\sigma(x) = x^{2^r}$ for x in any extension of $\mathbb{F}_{2^r}$. We show (a) first. Let $p \neq 3$ be a prime such that $m = pr$ for some integer r. By way of contradiction, suppose that $P(X)$ has a root $x_0 \in \mathbb{F}_{2^m}$. Then $x_0, \sigma(x_0), \dots, \sigma^{p-1}(x_0)$ have to be p distinct roots of $P(X)$ in $\mathbb{F}_{2^m}$ because $\sigma(P(x_0)) = \sigma(x_0)^{2^k+1} + \sigma(x_0) + \beta = 0$ and p is prime. It follows from Lemma 5.23 that if $P(X)$ has more than one root in $\mathbb{F}_{2^m}$, then $P(X)$ has exactly three roots in $\mathbb{F}_{2^m}$. This contradicts the assumption that $p \neq 3$.

We next prove (b). Now $p = 3$, so $m = 3r$. If $P(X)$ has at least one root in $\mathbb{F}_{2^m}$, then by the proof of (a), it has exactly three roots in $\mathbb{F}_{2^m}$, and we are done.

Assume, by way of contradiction, that $P(X)$ has no root in $\mathbb{F}_{2^m}$. First, if $k = 1$, then $P(X)$ has degree 3 and is irreducible over $\mathbb{F}_{2^r}$. Therefore, $P(X)$ splits over $\mathbb{F}_{2^m}$, which contradicts our assumption.

From now on, suppose $k > 1$. We write $P(X) = P_1(X)P_2(X) \cdots P_s(X)$ for irreducible polynomials $P_1(X), \dots, P_s(X) \in \mathbb{F}_{2^m}[X]$. Since the degree 2^k+1 of $P(X)$ is odd, at least one of the polynomials $P_1(X), \dots, P_s(X)$ has odd degree. Let $j^* \in \{1, \dots, s\}$ such that $P_{j^*}(X)$ has odd degree and is of minimal degree among all polynomials $P_j(X)$ of odd degree. We denote $\ell = \deg(P_{j^*}(X))$ and remark that $\ell \geq 3$ since $P(X)$ has no root in $\mathbb{F}_{2^m}$. The polynomial $P_{j^*}(X)$ now splits over $\mathbb{F}_{2^{m\ell}}$,

[1] The results in Lemma 5.24–Proposition 5.27 are mainly based on the work by Yue Zhou.

which is an extension of $\mathbb{F}_{2^m}$ with $[\mathbb{F}_{2^{m\ell}} : \mathbb{F}_{2^m}] = \ell$. Consequently, $P(X)$ has at least ℓ roots in $\mathbb{F}_{2^{m\ell}}$, and there is no root of $P(X)$ in any proper subfield of $\mathbb{F}_{2^{m\ell}}$ containing $\mathbb{F}_{2^m}$.

As $\ell \geq 3$, it follows from Lemma 5.22 that $P(X)$ has exactly $2^{\gcd(m\ell,k)} + 1$ roots in $\mathbb{F}_{2^{m\ell}}$. Define $h = \gcd(m\ell, k)$, and note that this implies $h = \gcd(\ell, k)$. If $h = 1$, then $P(X)$ has three roots in $\mathbb{F}_{2^{m\ell}}$, and these roots are also elements of $\mathbb{F}_{2^m}$ since $m = 3r$. This contradicts our assumption that $P(X)$ has no root in $\mathbb{F}_{2^m}$. Hence, assume $h > 1$. We show that $3\ell \mid 2^h + 1$. We may regard σ as an element in $\mathrm{Gal}(\mathbb{F}_{2^{m\ell}}/\mathbb{F}_{2^r})$. If $3 \nmid \ell$, then it is clear that x_0, $\sigma(x_0)$, $\ldots, \sigma^{3\ell}(x_0)$ are pairwise distinct for any root x_0 of $P(X)$ in $\mathbb{F}_{2^{m\ell}}$. We show that this also holds if $3 \mid \ell$. Suppose $3 \mid \ell$ and $\sigma^j(x_0) = x_0$ for some $j < 3\ell$ with $j \mid 3\ell$. This means $[\mathbb{F}_{2^r}(x_0) : \mathbb{F}_{2^r}] = j$. Thus,

$$[\mathbb{F}_{2^m}(x_0) : \mathbb{F}_{2^m}] = \begin{cases} j & \text{if } 3 \nmid j, \\ j/3 & \text{if } 3 \mid j. \end{cases}$$

By definition, we have $\mathbb{F}_{2^{m\ell}} = \mathbb{F}_{2^m}(x_0)$. Consequently, if $3 \nmid j$, it follows that $j = \ell$, which is a contradiction to the assumption that $3 \mid \ell$. If $3 \mid j$, we obtain $\ell = j/3$, which contradicts the assumption $j < 3\ell$.

Therefore, 3ℓ divides $2^h + 1$. As $h \mid \ell$, we obtain in particular $3h \mid 2^h + 1$. By Lemma 5.24, this implies $\gcd(h, 3) > 1$. As $m = 3r$ and $h \mid k$, it follows that $\gcd(m, k) > 1$, which is a contradiction. □

For any two coprime positive integers k and m, define

$$\Phi(m) = \{\beta \in \mathbb{F}_{2^m}^* : X^{2^k+1} + X + \beta \text{ has no root in } \mathbb{F}_{2^m}\} \tag{5.102}$$

and

$$M(m) = |\Phi(m)|$$

and

$$N(m) = \left|\{\beta \in \Phi(m) : \beta \notin \mathbb{F}_{2^{m'}} \text{ for all } m' < m \text{ with } m' \mid m\}\right|. \tag{5.103}$$

According to Lemma 5.23,

$$M(m) = \frac{2^m + (-1)^{m+1}}{3}. \tag{5.104}$$

In the following Lemma 5.26, we determine the exact value of $N(m)$.

Lemma 5.26. *Let m be a positive integer. Write $m = 3^{n_0} \prod_{i=1}^{t} p_i^{n_i}$, where n_0 is a non-negative integer, $p_1, \ldots, p_t$ are distinct prime numbers, and $n_1, \ldots, n_t$ are positive integers. If $t = 0$, which means $m = 3^{n_0}$ and, in particular, includes the case $m = 1$, then*

$$N(m) = \frac{2^m + 1}{3}.$$

If $t \geq 1$, then

$$\begin{aligned} N(m) = \frac{1}{3}\Big(2^m - \sum_{i=1}^{t} 2^{\frac{m}{p_i}} + \sum_{\substack{i,j=1,\\ j\neq i}}^{t} 2^{\frac{m}{p_ip_j}} - \dots \\ \dots + (-1)^\ell \sum_{\substack{i_1,\dots,i_\ell=1\\ \textit{pairwise distinct}}}^{t} 2^{\frac{m}{p_{i_1}\cdots p_{i_\ell}}} + \dots + (-1)^t \cdot 2^{\frac{m}{p_1p_2\cdots p_t}} - \varepsilon\Big), \end{aligned} \tag{5.105}$$

where

$$\varepsilon = \begin{cases} 2 & \textit{if } t = 1 \textit{ and } m \equiv 2 \pmod 4, \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. By definition, to determine $N(m)$, we take $\Phi(m)$, and for every proper subfield $\mathbb{F}_{2^{m'}}$ of $\mathbb{F}_{2^m}$, we exclude each element in $\Phi(m) \cap \mathbb{F}_{2^{m'}}^*$ from $\Phi(m)$.

We first consider the case $t = 0$. If $n_0 = 1$, which means $m = 1$, then $X^{2^k+1} + X + \beta$ has no root in $\mathbb{F}_2$ if and only if $\beta = 1$. Hence, $N(1) = 1$. If $n_0 \geq 1$, by Lemma 5.25,

$$\Phi(m) \cap \mathbb{F}_{2^{m'}} = \begin{cases} \emptyset & \text{if } 3m' \mid m, \\ \Phi(m') & \text{if } 3m' \nmid m. \end{cases}$$

Consequently, we obtain $N(3^{n_0}) = M(3^{n_0})$ and, by (5.104), $M(3^{n_0}) = \frac{2^m+1}{3}$.

From now on, assume $t \geq 1$. Then, by the inclusion–exclusion principle,

$$\begin{aligned} N(m) = M(m) - \sum_{i=1}^{t} M\left(\frac{m}{p_i}\right) + \sum_{\substack{i,j=1,\\ j\neq i}}^{t} M\left(\frac{m}{p_ip_j}\right) - \cdots \\ \cdots + (-1)^\ell \sum_{\substack{i_1,\dots,i_\ell=1\\ \text{pairwise distinct}}}^{t} M\left(\frac{m}{p_{i_1}\cdots p_{i_\ell}}\right) + \cdots + (-1)^t M\left(\frac{m}{p_1\cdots p_t}\right). \end{aligned} \tag{5.106}$$

First, suppose $m \not\equiv 2 \pmod 4$, which means either m is odd or $4 \mid m$. If m is odd, then m' is odd for all $m' \mid m$. If $4 \mid m$, then m' is even for all $m' = \frac{m}{p_{i_1}\cdots p_{i_\ell}}$ that occur in (5.106). Consequently, in these two cases, by (5.104), we have

$$M(m') = \frac{2^{m'} + (-1)^{m+1}}{3} \tag{5.107}$$

for any $m' = \frac{m}{p_{i_1}\cdots p_{i_\ell}}$ occurring in (5.106). Plugging (5.107) into (5.106), we obtain

$$\begin{aligned} N(m) = \frac{1}{3}\Bigg(2^m - \sum_{i=1}^{t} 2^{\frac{m}{p_i}} + \sum_{\substack{i,j=1,\\ j\neq i}}^{t} 2^{\frac{m}{p_i p_j}} - \cdots + (-1)^t \cdot 2^{\frac{m}{p_1 p_2 \cdots p_t}}\Bigg) \\ + \frac{(-1)^{m+1}}{3}\left(1 - \binom{t}{1} + \binom{t}{2} - \cdots + (-1)^t\right). \end{aligned} \tag{5.108}$$

Note that the last sum of (5.108) equals zero, which can be seen using the binomial identity $(x+y)^n = \sum_{k=0}^{n}\binom{n}{k}x^{n-k}y^k$ with $x = 1$ and $y = -1$ (or vice versa).

If $m \equiv 2 \pmod 4$, we set $p_1 = 2$ and $n_1 = 1$. By (5.104),

$$M(m') = \begin{cases} \frac{2^{m'}+1}{3} & \text{if } m' = \frac{m}{2p_{i_2}\cdots p_{i_\ell}}, \\ \frac{2^{m'}-1}{3} & \text{if } m' = \frac{m}{p_{i_1}\cdots p_{i_\ell}} \text{ and } i_1, \ldots, i_\ell \neq 1. \end{cases} \tag{5.109}$$

Plugging (5.109) into (5.106), we obtain

$$\begin{aligned} N(m) = \frac{1}{3}\Bigg(2^m - \sum_{i=1}^{t} 2^{\frac{m}{p_i}} + \sum_{\substack{i,j=1,\\ j\neq i}}^{t} 2^{\frac{m}{p_i p_j}} - \cdots + (-1)^t \cdot 2^{\frac{m}{p_1 p_2 \cdots p_t}}\Bigg) \\ + \frac{1}{3}\sum_{i=0}^{t}(-1)^i\left(\binom{t-1}{i-1} - \binom{t-1}{i}\right). \end{aligned} \tag{5.110}$$

We show where the last sum of (5.110) is coming from and which values it can take. If $t = 1$, then $m = 3^{n_0} \cdot 2$. Note that m is even and $\frac{m}{2}$ is odd. Hence, in this case, $N(m) = M(m) - M(\frac{m}{2}) = 2^m - 2^{\frac{m}{2}} - 2$, and the last sum of (5.110) equals -2. Now assume $t > 1$. Consider

$$\sum_{\substack{i_1,\ldots,i_\ell=1\\ \text{pairwise distinct}}}^{t} M\left(\frac{m}{p_{i_1}\cdots p_{i_\ell}}\right) \tag{5.111}$$

from (5.106) for some $\ell \in \{1, \ldots, t\}$. This sum consists of $\binom{t}{\ell}$ terms. Assume $p_{i_1} < p_{i_2} < \cdots < p_{i_\ell}$. If $i_1 = 1$, which means $p_{i_1} = 2$, then $\frac{m}{2p_{i_2}\cdots p_{i_\ell}}$ is odd. In this case, there exist $\binom{t-1}{\ell-1}$ ways to choose $p_{i_2}, \ldots, p_{i_\ell}$. On the contrary, if $i_1 \neq 1$, then $\frac{m}{p_{i_1}\cdots p_{i_\ell}}$ is even, and we can choose $p_{i_1}, \ldots, p_{i_\ell}$ in $\binom{t-1}{\ell}$ ways. Combining these results with (5.109), the sum in (5.111) consists of $\binom{t-1}{\ell-1}$ terms of the form $\frac{2^{m'}+1}{3}$ and $\binom{t-1}{\ell}$ terms of the form $\frac{2^{m'}-1}{3}$. By similar reasoning as in the case $m \not\equiv 2 \pmod 4$, the last sum of (5.110) is zero if $t > 1$. □

In Proposition 5.27, we determine the number of orbits under the action of

$\mathrm{Gal}(\mathbb{F}_{2^m}/\mathbb{F}_2)$ into which $\Phi(m)$ decomposes.

Proposition 5.27. *Let m be positive integer. Let $\Phi(m)$ as in (5.102), and define*

$$B(m) = \left\{ \{\beta^{2^i} : i \in \{0, \dots, m-1\}\} : \beta \in \Phi(m) \right\}$$

as the set of orbits of $\beta \in \mathbb{F}_{2^m}^*$ for which $X^{2^k+1} + X + \beta$ has no root in $\mathbb{F}_{2^m}$ under the action of the Galois group $\mathrm{Gal}(\mathbb{F}_{2^m}/\mathbb{F}_2)$. Moreover, define $b(m) = |B(m)|$. Then

$$b(m) = \sum_{m' | m,\ 3 \nmid \frac{m}{m'}} \frac{N(m')}{m'},$$

where $N(m')$ is defined as in (5.103) and can be calculated as in Lemma 5.26.

Proof. In any subfield $\mathbb{F}_{2^{m'}}$ of $\mathbb{F}_{2^m}$, the number of orbits of $\beta \in \Phi(m) \cap \mathbb{F}_{2^{m'}}^*$ under the action of $\mathrm{Gal}(\mathbb{F}_{2^{m'}}/\mathbb{F}_2)$ that have full length m' is $\frac{N(m')}{m'}$. It follows from Lemma 5.25 that we only need to consider the orbits in $\mathbb{F}_{2^{m'}}$ with $3 \nmid [\mathbb{F}_{2^m} : \mathbb{F}_{2^{m'}}]$. Adding all these numbers gives $b(m)$. □

With the help of Proposition 5.27, we can eventually determine the precise number of CCZ-inequivalent Taniguchi APN functions on $\mathbb{F}_{2^{2m}}$.

Theorem 5.28. *Let $m \geq 3$, and denote by $n(m)$ the number of CCZ-inequivalent Taniguchi APN functions $f_{k,\alpha,\beta}$ on $\mathbb{F}_{2^{2m}}$ from Theorem 4.8. Then*

$$n(m) = \begin{cases} \dfrac{\varphi(m)b(m)}{2} & \text{if } m \text{ is odd,} \\ \dfrac{\varphi(m)(b(m)+1)}{2} & \text{if } m \text{ is even,} \end{cases}$$

where φ denotes Euler's totient function and $b(m)$ is as defined in Proposition 5.27.

Proof. Let $m \geq 3$. Thanks to Proposition 5.12, we only need to consider $\alpha \in \{0, 1\}$ and $0 < k < \frac{m}{2}$. We study functions with $\alpha = 1$ first. According to Theorem 5.13, for $0 < k, \ell < \frac{m}{2}$, two Taniguchi APN functions $f_{k,1,\beta}$ and $f_{\ell,1,\beta'}$ are CCZ-equivalent if and only if $k = \ell$ and $\beta = \beta'^{2^i}$ for some $i \in \{0, \dots, m-1\}$. We count the number of pairs (k, β) leading to inequivalent APN functions. As $0 < k < \frac{m}{2}$ and $\gcd(k, m) = 1$, we have $\frac{\varphi(m)}{2}$ choices for k. The number of admissible $\beta \in \mathbb{F}_{2^m}^*$ is given by $b(m)$ from Proposition 5.27. If m is odd, then these are all inequivalent Taniguchi APN functions.

If m is even, according to Corollary 4.10 (b), there also exist Taniguchi APN functions with $\alpha = 0$. In this case, it follows from Corollary 5.19 in combination with Corollary 5.11 that for every valid choice of k, there is additionally exactly one Taniguchi APN function $f_{k,0,\beta}$ up to CZZ-equivalence. It is inequivalent to all functions with $\alpha \neq 0$. As before, we have $\frac{\varphi(m)}{2}$ choices for k. □

Table 5.3: Number $n(m)$ of CCZ-inequivalent Taniguchi APN functions on $\mathbb{F}_{2^{2m}}$ for certain values of m.

m	4	5	6	7	8	9	10	11	12	13	14	15	16
$n(m)$	3	6	5	21	26	57	74	315	234	1 266	1 185	2 916	5 492
bound	2	6	4	21	22	57	70	315	228	1 266	1 173	2 916	5 464

m	17	18	19	20	21	22	23	24
$n(m)$	20 568	14 595	82 791	69 988	199 734	317 915	1 337 325	932 308
bound	20 568	14 565	82 791	69 908	199 734	317 755	1 337 325	932 068

m	25	30	40	50	100
$n(m)$	4 473 950	47 723 332	73 300 845 320	$\approx 7.5 \cdot 10^{13}$	$\approx 8.5 \cdot 10^{28}$
bound	4 473 930	47 721 860	73 300 775 192	$\approx 7.5 \cdot 10^{13}$	$\approx 8.5 \cdot 10^{28}$

In Corollary 5.29, we give a nice lower bound on the number from Theorem 5.28. It becomes obvious that the number of inequivalent quadratic APN functions on $\mathbb{F}_{2^{2m}}$ grows exponentially in m.

Corollary 5.29. *Let $m \geq 3$, and denote by $n(m)$ the number of CCZ-inequivalent Taniguchi APN functions on $\mathbb{F}_{2^{2m}}$ from Theorem 4.8. Then*

$$n(m) \geq \frac{\varphi(m)}{2} \left\lceil \frac{2^m + 1}{3m} \right\rceil,$$

where φ denotes Euler's totient function.

Proof. Define $B(m)$ and $b(m)$ as in Proposition 5.27. The value of $b(m)$ is minimal if all the orbits in $B(m)$ have full length m. By Lemma 5.23, this implies

$$b(m) \geq \begin{cases} \left\lceil \frac{2^m-1}{3m} \right\rceil & \text{if } m \text{ is even,} \\ \left\lceil \frac{2^m+1}{3m} \right\rceil & \text{if } m \text{ is odd.} \end{cases}$$

Clearly, $\left\lceil \frac{2^m-1}{3m} \right\rceil = \left\lceil \frac{2^m+1}{3m} \right\rceil$ for all $m \geq 3$. The result now follows from Theorem 5.28. □

In Table 5.3, we list the exact number of CCZ-inequivalent Taniguchi APN functions obtained from Theorem 5.28 for certain values of m. From computational results, this number was only known for $m \leq 4$. Recall that for $m = 2$ and $m = 3$, there is only one Taniguchi APN function up to CCZ-equivalence. We additionally compare these numbers to the lower bound established in Corollary 5.29. Clearly, the bound is very close to the actual number of Taniguchi APN functions.

6 Conclusion and outlook

6.1 Difference families

In this thesis, we studied the isomorphism problem for three pairs of near-complete $(v, k, k-1)$ disjoint difference families in Galois rings and finite fields. All the constructions in Galois rings were inspired by a well-known construction in finite fields that was introduced in 1972 by Wilson [102]. By carefully calculating and bounding block intersection numbers of the associated designs, we managed to completely solve two of the isomorphism problems, see Section 3.2 and Section 3.4, and partially solve the third one, see Section 3.3.

In general, isomorphism problems of combinatorial designs are hard problems. Our results demonstrate that the block intersection number approach to tackle these problems, while promising in some cases, has its limitations in general. To make the approach work, one needs designs that have a sufficiently strong algebraic structure. Only then, it is possible to calculate or at least bound these numbers.

In our case, we were able to use the existing rich theory about cyclotomic numbers to completely determine the block intersection numbers of the designs coming from finite fields. Fortunately, in all our cases, Wilson's [102] difference families provided uniform or almost uniform cyclotomic numbers, so that we could easily calculate them. Otherwise, their determination would have been difficult.

Thus, we knew the intersection numbers of the designs from finite fields, and we only needed to show that the designs from Galois rings have at least one block intersection number different from the intersection numbers of the finite fields designs. For Momihara's [84] difference family, which has the most structure among the Galois ring difference families we studied, we calculated such an intersection number and thereby solved the isomorphism problem. For the difference family by Davis, Huczynska, and Mullen [43], we were also able to determine one intersection number in the case $p = 2$, while for odd p we could bound an intersection number, so that we also solved this isomorphism problem. For our newly constructed difference family from Theorem 2.7, however, we were only able to partially solve the isomorphism problem by bounding an intersection number in the case $p^r - 1 \equiv 0 \pmod{24}$.

Despite these mixed results, we still consider the block intersection number approach promising to tackle isomorphism problems of combinatorial designs, especially if the designs are constructed as the development of some difference structure. The strong connection between block intersection numbers and multiplicities of differences that we emphasized in Remark 3.2 will often provide ways to obtain useful results about the intersection numbers.

We conclude by listing several interesting open problems about difference families and their developments that we stumbled upon in the course of our study:

- Our computations hint that Wilson's [102] difference family from Theorem 2.4 and our difference family from Theorem 2.7 are always nonisomorphic and not only in the case $p^r - 1 \equiv 0 \pmod{24}$ that we described in Theorem 3.23. We leave the task to prove this conjecture to future work.

- The construction of a disjoint difference family in the Galois ring $\mathrm{GR}(p^2, r)$ presented in Theorem 2.7 does not only work for the subgroup of squares in the Teichmüller group but for all its subgroups. Moreover, there will always be an analogous difference family in the finite field $\mathbb{F}_{p^{2r}}$. It would be interesting to study the isomorphism problem in all these cases. It might be possible to deduce more block intersection numbers from the ones given in Proposition 3.3 and Proposition 3.16.

- In Remark 3.5, we have conjectured all the block intersection numbers and their multiplicities of Momihara's [84] designs. Since it is always helpful to know isomorphism invariants of combinatorial objects, it would be nice to prove this conjecture.

- As mentioned before, Momihara's [84] difference family has a strong structure. In Section 2.5, we used this structure to obtain a new divisible difference family in Galois rings. A deeper study of the difference relations within and between the base blocks of Momihara's [84] difference family could lead to more interesting results and perhaps new types of difference families.

- As mentioned in Section 3.1, nonisomorphic designs can have the same block intersection numbers. To get a better understanding of how useful intersection numbers are as an isomorphism invariant, it would be interesting to find more difference families as in Example 3.4, for which the associated designs have the same intersection numbers but are still nonisomorphic.

6.2 Almost perfect nonlinear functions

In this thesis, we completely determined the equivalence of two infinite families of quadratic non-power APN functions of the form $f(x, y) = (g(x, y), xy)$ that were introduced by Zhou and Pott [109] and Taniguchi [100]. Moreover, we added some results about the equivalence of APN functions of a similar form introduced by Carlet [36]. In Table 6.1, we summarize our results for these three families.

From these results, we were able to derive the exact number of CCZ-inequivalent APN functions contained in the Zhou-Pott and in the Taniguchi family. By showing that the number of Taniguchi APN functions on $\mathbb{F}_{2^{2m}}$ grows exponentially in m, we established the first nontrivial lower bound on the total number of CCZ-inequivalent APN functions. Up to now, we have solely had computational results about this number, but only for $n \leq 8$. The only infinite families for which the equivalence had been completely determined were power APN functions.

Table 6.1: Equivalence of APN functions of the form $f(x,y) = (g(x,y), xy)$ on $\mathbb{F}_{2^{2m}}$

Class	$g(x,y)$	Conditions
Zhou-Pott [109, 2]	$x^{2^k+1} + \alpha y^{(2^k+1)2^s}$	m even, $\gcd(k,m) = 1$, s even, $\alpha \in \mathbb{F}_{2^m}^*$ not a cube
	$f_{k,s,\alpha} \overset{\text{CCZ}}{\sim} f_{\ell,t,\alpha'}$ iff $k \equiv \pm\ell \pmod{m}$ and $s \equiv \pm t \pmod{m}$	
Carlet [36, 100]	$x^{2^k+1} + \alpha x y^{2^k} + \beta y^{2^k+1}$	$\gcd(k,m) = 1$, $X^{2^k+1} + \alpha X + \beta$ has no root in $\mathbb{F}_{2^m}$
	if m even: $f_{k,\alpha,\beta} \overset{\text{CCZ}}{\sim} f_{\ell,\alpha',\beta'}$ iff $k \equiv \pm\ell \pmod{m}$, contained in Zhou-Pott	
Taniguchi [100]	$x^{2^{2k}(2^k+1)} + \alpha x^{2^{2k}} y^{2^k} + \beta y^{2^k+1}$	$\gcd(k,m) = 1$, $X^{2^k+1} + \alpha X + \beta$ has no root in $\mathbb{F}_{2^m}$

	if $\alpha, \alpha' \neq 0$: $f_{k,\alpha,\beta} \overset{\text{CCZ}}{\sim} f_{\ell,\alpha',\beta'}$ iff $k \equiv \pm\ell \pmod{m}$ and $\beta = \beta'^{2^i}$,
	inequivalent to Zhou-Pott
	if $\alpha = \alpha' = 0$: $f_{k,\alpha,\beta} \overset{\text{CCZ}}{\sim} f_{\ell,\alpha',\beta'}$ iff $k \equiv \pm\ell \pmod{m}$,
	contained in Zhou-Pott	

In the course of our study, the following problems remained open:

- As pointed out in Remark 4.2, it seems that on $\mathbb{F}_{2^n}$ with $n \geq 4$, for any quadratic APN function f, we have $\mathrm{Aut}(f) = \mathrm{Aut}_{EA}(f)$. This result apparently follows implicitly from Yoshiara's [106] proof of Theorem 4.1 in combination with a result by Dempwolff and Edel [44, Theorem 4.10]. It would be very helpful to have a direct proof of this result.
- In Corollary 5.21, we showed that for even m, there exist $\frac{\varphi(m)}{2}$ CCZ-inequivalent Carlet APN function on $\mathbb{F}_{2^{2m}}$, and in Corollary 5.16, we determined the automorphism group of Carlet APN functions for m even. Our computations hint that these results also hold if m is odd. As this would imply that the Carlet APN class contains only few inequivalent members, we did not pursue solving the equivalence problem for m odd any further. Nevertheless, it would be nice to have a complete characterization of the equivalence relations of Carlet functions.

More generally, our results may shift the focus of research on APN functions onto the following open problems:

- The lower bound on the total number of CCZ-inequivalent APN functions on the finite field $\mathbb{F}_{2^n}$ established in this thesis only holds for even n. It will be interesting to find a similar bound for n odd. Several of the infinite families in the list by Budaghyan, Calderini, and Villa [24, Table 3] also exist for odd n, so this may be a good starting point. Note, however, that for n odd, we cannot use the bivariate description that proved to be helpful in this thesis.

- Our results demonstrate that there are a great number quadratic APN functions on $\mathbb{F}_{2^{2m}}$, all of which have the classical Walsh spectrum. Thus, the efforts to find new APN functions may focus on the search for non-quadratic functions and functions with a non-classical Walsh spectrum. So far, only one non-power APN function that is not equivalent to a quadratic function is known, and lately, there was not much progress regarding this problem. Recent computational results by Beierle and Leander [7], however, show that there exist numerous APN functions with non-classical Walsh spectra. It would be great to find an infinite family that contains non-power APN functions with a non-classical Walsh spectrum.

- The APN permutation on $\mathbb{F}_{2^6}$ by Browning, Dillon, McQuistan, and Wolfe [21], which is the lone APN permutation on $\mathbb{F}_{2^n}$ with n even, is CCZ-equivalent to a quadratic function. Hence, it remains interesting to study quadratic APN functions with the goal of getting closer to a solution to The Big APN problem.

Bibliography

[1] R. J. R. Abel and M. Buratti. Difference families. In: *Handbook of Combinatorial Designs.* Ed. by C. J. Colbourn and J. H. Dinitz. 2nd ed. Boca Raton: Chapman & Hall/CRC Press, 2007, pp. 392–410.

[2] N. Anbar, T. Kalaycı, and W. Meidl. Determining the Walsh spectra of Taniguchi's and related APN-functions. In: *Finite Fields Appl.* 60 (2019), pp. 101577, 20.

[3] I. Anderson, C. J. Colbourn, J. H. Dinitz, and T. S. Griggs. Design theory: antiquity to 1950. In: *Handbook of Combinatorial Designs.* Ed. by C. J. Colbourn and J. H. Dinitz. 2nd ed. Boca Raton: Chapman & Hall/CRC Press, 2007, pp. 11–22.

[4] R. R. Anstice. On a problem in combinations. In: *Cambridge and Dublin Math. J* 7 (1852), pp. 279–292.

[5] R. R. Anstice. On a problem in combinations (continued). In: *Cambridge and Dublin Math. J* 8 (1853), pp. 149–154.

[6] L. D. Baumert, W. H. Mills, and R. L. Ward. Uniform cyclotomy. In: *J. Number Theory* 14.1 (1982), pp. 67–82.

[7] C. Beierle and G. Leander. *New instances of quadratic APN functions.* 2020. arXiv: `2009.07204 [cs.IT]`.

[8] T. P. Berger and P. Charpin. The permutation group of affine-invariant extended cyclic codes. In: *IEEE Trans. Inform. Theory* 42.6, part 2 (1996), pp. 2194–2209.

[9] T. Beth and C. Ding. On almost perfect nonlinear permutations. In: *Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993).* Vol. 765. Lecture Notes in Comput. Sci. Springer, Berlin, 1994, pp. 65–76.

[10] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory.* 2nd ed. Cambridge: Cambridge University Press, 1999.

[11] E. Biham and A. Shamir. Differential cryptanalysis of DES-like cryptosystems. In: *J. Cryptology* 4.1 (1991), pp. 3–72.

[12] C. Blondeau and K. Nyberg. Perfect nonlinear functions and cryptography. In: *Finite Fields Appl.* 32 (2015), pp. 120–147.

[13] A. W. Bluher. On $x^{q+1} + ax + b$. In: *Finite Fields Appl.* 10.3 (2004), pp. 285–305.

[14] A. Bonnecaze and I. M. Duursma. Translates of linear codes over $\mathbb{Z}_4$. In: *IEEE Trans. Inform. Theory* 43.4 (1997), pp. 1218–1230.

[15] R. C. Bose. On the construction of balanced incomplete block designs. In: *Ann. Eugenics* 9 (1939), pp. 353–399.

[16] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. In: *J. Symbolic Comput.* 24.3-4 (1997), pp. 235–265.

[17] C. Bracken, E. Byrne, N. Markin, and G. McGuire. New families of quadratic almost perfect nonlinear trinomials and multinomials. In: *Finite Fields Appl.* 14.3 (2008), pp. 703–714.

[18] C. Bracken, E. Byrne, G. McGuire, and G. Nebe. On the equivalence of quadratic APN functions. In: *Des. Codes Cryptogr.* 61.3 (2011), pp. 261–272.

[19] C. Bracken, C. H. Tan, and Y. Tan. On a class of quadratic polynomials with no zeros and its application to APN functions. In: *Finite Fields Appl.* 25 (2014), pp. 26–36.

[20] M. Brinkmann and G. Leander. On the classification of APN functions up to dimension five. In: *Des. Codes Cryptogr.* 49.1-3 (2008), pp. 273–288.

[21] 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.* Vol. 518. Contemp. Math. Amer. Math. Soc., Providence, RI, 2010, pp. 33–42.

[22] K. Browning, J. Dillon, R. Kibler, and M. McQuistan. APN polynomials and related codes. In: *J. Comb. Inform. Syst. Sci.* 34 (2009), pp. 135–159.

[23] L. Budaghyan. *Construction and Analysis of Cryptographic Functions.* Heidelberg: Springer, 2014.

[24] L. Budaghyan, M. Calderini, and I. Villa. On equivalence between known families of quadratic APN functions. In: *Finite Fields Appl.* 66 (2020), pp. 101704, 21.

[25] L. Budaghyan and C. Carlet. Classes of quadratic APN trinomials and hexanomials and related structures. In: *IEEE Trans. Inform. Theory* 54.5 (2008), pp. 2354–2357.

[26] L. Budaghyan, C. Carlet, and G. Leander. On inequivalence between known power APN functions. In: *Proceedings of the International Workshop on Boolean Functions: Cryptography and Applications, BFCA 2008.* Ed. by O. Masnyk-Hansen, J.-F. Michon, P. Valarcher, and J.-B. Yunès. Copenhagen, 2008, pp. 1–13.

[27] L. Budaghyan, C. Carlet, and A. Pott. New classes of almost bent and almost perfect nonlinear polynomials. In: *IEEE Trans. Inform. Theory* 52.3 (2006), pp. 1141–1152.

[28] M. Buratti. Recursive constructions for difference matrices and relative difference families. In: *J. Combin. Des.* 6.3 (1998), pp. 165–182.

[29] M. Buratti. Old and new designs via difference multisets and strong difference families. In: *J. Combin. Des.* 7.6 (1999), pp. 406–425.

[30] M. Buratti. On disjoint $(v, k, k-1)$ difference families. In: *Des. Codes Cryptogr.* 87.4 (2019), pp. 745–755.

[31] M. Buratti and D. Jungnickel. Partitioned difference families versus zero-difference balanced functions. In: *Des. Codes Cryptogr.* (2019), pp. 1–7.

[32] M. Calderini, M. Sala, and I. Villa. A note on APN permutations in even dimension. In: *Finite Fields Appl.* 46 (2017), pp. 1–16.

[33] A. Canteaut and L. Perrin. On CCZ-equivalence, extended-affine equivalence, and function twisting. In: *Finite Fields Appl.* 56 (2019), pp. 209–246.

[34] A. Canteaut and L. Perrin. *How to take a function apart with SboxU (also featuring some new results on ortho-derivatives)*. Slides from talk given at The 5th International Workshop on Boolean Functions and their Applications (BFA), held online. 2020.

[35] A. Canteaut, L. Perrin, and S. Tian. If a generalised butterfly is APN then it operates on 6 bits. In: *Cryptogr. Commun.* 11.6 (2019), pp. 1147–1164.

[36] C. Carlet. Relating three nonlinearity parameters of vectorial functions and building APN functions from bent functions. In: *Des. Codes Cryptogr.* 59.1-3 (2011), pp. 89–109.

[37] C. Carlet. More constructions of APN and differentially 4-uniform functions by concatenation. In: *Sci. China Math.* 56.7 (2013), pp. 1373–1384.

[38] F. Chabaud and S. Vaudenay. Links between differential and linear cryptanalysis. In: *Advances in Cryptology—EUROCRYPT '94 (Perugia)*. Vol. 950. Lecture Notes in Comput. Sci. Springer, Berlin, 1995, pp. 356–365.

[39] Y. Chang and C. Ding. Constructions of external difference families and disjoint difference families. In: *Des. Codes Cryptogr.* 40.2 (2006), pp. 167–185.

[40] C. J. Colbourn. Triple systems. In: *Handbook of Combinatorial Designs*. Ed. by C. J. Colbourn and J. H. Dinitz. 2nd ed. Boca Raton: Chapman & Hall/CRC Press, 2007, pp. 58–71.

[41] C. J. Colbourn and J. H. Dinitz, eds. *Handbook of Combinatorial Designs*. 2nd ed. Boca Raton: Chapman & Hall/CRC Press, 2007.

[42] R. Crandall, K. Dilcher, and C. Pomerance. A search for Wieferich and Wilson primes. In: *Math. Comp.* 66.217 (1997), pp. 433–449.

[43] J. A. Davis, S. Huczynska, and G. L. Mullen. Near-complete external difference families. In: *Des. Codes Cryptogr.* 84 (2017), pp. 415–424.

[44] U. Dempwolff and Y. Edel. Dimensional dual hyperovals and APN functions with translation groups. In: *J. Algebr. Comb.* 39.2 (2014), pp. 457–496.

[45] L. E. Dickson. Cyclotomy and trinomial congruences. In: *Trans. Amer. Math. Soc.* 37.3 (1935), pp. 363–380.

[46] L. E. Dickson. Cyclotomy, higher congruences, and Waring's problem. In: *Amer. J. Math.* 57.2 (1935), pp. 391–424.

[47] L. E. Dickson. *Linear Groups: With an Exposition of the Galois Field Theory.* New York: Dover Publications, 1958.

[48] J. F. Dillon. *APN polynomials and related codes.* Slides from talk given at the Polynomials over Finite Fields and Applications Workshop, held at Banff International Research Station. 2006.

[49] J. F. Dillon. *APN polynomials: an update.* Slides from talk given at The 9th International Conference on Finite Fields and their Applications, held at University College, Dublin, July 13-17, 2009. 2009.

[50] C. Ding and J. Yin. Combinatorial constructions of optimal constant-composition codes. In: *IEEE Trans. Inform. Theory* 51.10 (2005), pp. 3671–3674.

[51] H. Dobbertin. Almost perfect nonlinear power functions on $\mathrm{G}F(2^n)$: the Niho case. In: *Inform. and Comput.* 151.1-2 (1999), pp. 57–72.

[52] H. Dobbertin. Almost perfect nonlinear power functions on $\mathrm{G}F(2^n)$: the Welch case. In: *IEEE Trans. Inform. Theory* 45.4 (1999), pp. 1271–1275.

[53] H. Dobbertin. Almost perfect nonlinear power functions on $\mathrm{G}F(2^n)$: a new case for n divisible by 5. In: *Finite fields and Applications. Proceedings of The Fifth International Conference on Finite Fields and Applications Fq 5, held at the University of Augsburg, Germany, August 2–6, 1999.* Ed. by D. Jungnickel and H. Niederreiter. Berlin, Heidelberg: Springer, 2001, pp. 113–121.

[54] F. G. Dorais and D. Klyve. A Wieferich prime search up to 6.7×10^{15}. In: *J. Integer Seq.* 14.9 (2011), Article 11.9.2, 14.

[55] Y. Edel, G. Kyureghyan, and A. Pott. A new APN function which is not equivalent to a power mapping. In: *IEEE Trans. Inform. Theory* 52.2 (2006), pp. 744–747.

[56] Y. Edel. On quadratic APN functions and dimensional dual hyperovals. In: *Des. Codes Cryptogr.* 57.1 (2010), pp. 35–44.

[57] Y. Edel. Quadratic APN functions as subspaces of alternating bilinear forms. In: *Proceedings of the Contact Forum Coding Theory and Cryptography III.* Ed. by S. Nikova, B. Preneel, and L. Storme. Brussels: Royal Flemish Academy of Belgium for Science and the Arts, 2011, pp. 11–24.

[58] Y. Edel and A. Pott. A new almost perfect nonlinear function which is not quadratic. In: *Adv. Math. Commun.* 3.1 (2009), pp. 59–81.

[59] Y. Edel and A. Pott. On designs and multiplier groups constructed from almost perfect nonlinear functions. In: *Cryptography and Coding.* Vol. 5921. Lecture Notes in Comput. Sci. Springer, Berlin, 2009, pp. 383–401.

[60] Y. Edel and A. Pott. On the equivalence of nonlinear functions. In: *Enhancing Cryptographic Primitives with Techniques from Error Correcting Codes.* Vol. 23. NATO Sci. Peace Secur. Ser. D Inf. Commun. Secur. Amsterdam: IOS, 2009, pp. 87–103.

[61] T. Feng and Q. Xiang. Cyclotomic constructions of skew Hadamard difference sets. In: *J. Combin. Theory Ser. A* 119.1 (2012), pp. 245–256.

[62] S. Furino. Difference families from rings. In: *Discrete Math.* 97.1-3 (1991), pp. 177–190.

[63] C. F. Gauß. *Untersuchungen über höhere Arithmetik.* Trans. by H. Maser. New York: Chelsea Publishing Company, 1981.

[64] D. Ghinelli and D. Jungnickel. Finite projective planes with a large abelian group. In: *Surveys in Combinatorics, 2003 (Bangor).* Ed. by C. D. Wensley. Vol. 307. London Math. Soc. Lecture Note Ser. Cambridge Univ. Press, Cambridge, 2003, pp. 175–237.

[65] R. Gold. Maximal recursive sequences with 3-valued recursive cross-correlation functions. In: *IEEE Trans. Inform. Theory* 14.1 (1968), pp. 154–156.

[66] A. R. Hammons Jr., P. V. Kumar, A. R. Calderbank, N. J. A. Sloane, and P. Solé. The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. In: *IEEE Trans. Inform. Theory* 40.2 (1994), pp. 301–319.

[67] H. Hanani. Balanced incomplete block designs and related designs. In: *Discrete Math.* 11 (1975), pp. 255–369.

[68] T. Helleseth and A. Kholosha. On the equation $x^{2^l+1}+x+a=0$ over $\mathrm{GF}(2^k)$. In: *Finite Fields Appl.* 14.1 (2008), pp. 159–176.

[69] X.-d. Hou. Affinity of permutations of $\mathbb{F}_2^n$. In: *Discrete Appl. Math.* 154.2 (2006), pp. 313–325.

[70] H. Janwa and R. M. Wilson. Hyperplane sections of Fermat varieties in $\mathbf{P}^3$ in char. 2 and some applications to cyclic codes. In: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (San Juan, PR, 1993).* Vol. 673. Lecture Notes in Comput. Sci. Springer, Berlin, 1993, pp. 180–194.

[71] J. Jedwab and S. Li. Construction and nonexistence of strong external difference families. In: *J. Alg. Comb.* 49.1 (2019), pp. 21–48.

[72] D. Jungnickel. Difference sets. In: *Contemporary Design Theory.* New York: Wiley, 1992, pp. 241–324.

[73] D. Jungnickel and A. Pott. Difference sets: an introduction. In: *Difference Sets, Sequences and their Correlation Properties (Bad Windsheim, 1998).*

Vol. 542. NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci. Kluwer Acad. Publ., Dordrecht, 1999, pp. 259–295.

[74] T. Kasami. The weight enumerators for several classes of subcodes of the 2nd order binary Reed-Muller codes. In: *Information and Control* 18 (1971), pp. 369–394.

[75] C. Kaspers and A. Pott. Solving isomorphism problems about 2-designs from disjoint difference families. In: *J. Combin. Des.* 27.5 (2019), pp. 277–294.

[76] C. Kaspers and A. Pott. On solving isomorphism problems about 2-designs using block intersection numbers. In: *Finite Fields and their Applications. Proceedings of the 14th International Conference on Finite Fields and their Applications, Vancouver, June 3-7, 2019.* Ed. by J. A. Davis. Berlin, Boston: DeGruyter, 2020, pp. 51–70.

[77] C. Kaspers and Y. Zhou. *A lower bound on the number of inequivalent APN functions.* 2020. arXiv: `2002.00673 [math.CO]`.

[78] C. Kaspers and Y. Zhou. The number of almost perfect nonlinear functions grows exponentially. In: *J. Cryptology* 34.1 (2021), Paper No. 4, 37.

[79] T. Kirkman. On a problem in combinations. In: *Cambridge and Dublin Mathematical Journal* 2 (1847), pp. 191–204.

[80] J. Knauer and J. Richstein. The continuing search for Wieferich primes. In: *Math. Comp.* 74.251 (2005), pp. 1559–1563.

[81] F. J. MacWilliams and N. J. A. Sloane. *The theory of error-correcting codes.* North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

[82] B. R. McDonald. *Finite Rings with Identity.* New York: Marcel Dekker, Inc., 1974.

[83] S. Mesnager. *Bent functions.* Fundamentals and results. Cham: Springer, 2016.

[84] K. Momihara. Disjoint difference families from Galois rings. In: *Electron. J. Combin.* 24.3 (2017), P3.23.

[85] K. Momihara and M. Yamada. Divisible difference families from Galois rings $\mathrm{GR}(4, n)$ and Hadamard matrices. In: *Des. Codes Cryptogr.* 73.3 (2014), pp. 897–909.

[86] S.-L. Ng and M. B. Paterson. Disjoint difference families and their applications. In: *Des. Codes Cryptogr.* 78.1 (2016), pp. 103–127.

[87] K. Nyberg. Differentially uniform mappings for cryptography. In: *Advances in Cryptology—EUROCRYPT '93 (Lofthus, 1993).* Vol. 765. Lecture Notes in Comput. Sci. Berlin: Springer, 1994, pp. 55–64.

[88] W. Ogata, K. Kurosawa, D. R. Stinson, and H. Saido. New combinatorial designs and their applications to authentication codes and secret sharing schemes. In: *Discrete Math.* 279.1-3 (2004), pp. 383–405.

[89] M. B. Paterson and D. R. Stinson. Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families. In: *Discrete Math.* 339.12 (2016), pp. 2891–2906.

[90] L. Perrin, A. Udovenko, and A. Biryukov. Cryptanalysis of a theorem: decomposing the only known solution to the big APN problem. In: *Advances in Cryptology—CRYPTO 2016. Part II.* Vol. 9815. Lecture Notes in Comput. Sci. Springer, Berlin, 2016, pp. 93–122.

[91] J. Plücker. *System der analytischen Geometrie, auf neue Betrachtungsweisen gegründet, und insbesondere eine ausführliche Theorie der Curven dritter Ordnung enthaltend.* Berlin: Duncker und Humblot, 1835.

[92] A. Pott. Almost perfect and planar functions. In: *Des. Codes Cryptogr.* 78.1 (2016), pp. 141–195.

[93] A. Pott and Y. Zhou. Cayley graphs of diameter two from difference sets. In: *J. Graph Theory* 85.2 (2017), pp. 533–544.

[94] T. Ralston. On the distribution of squares in a finite field. In: *Geom. Dedicata* 8.2 (1979), pp. 207–212.

[95] M. J. de Resmini, D. Ghinelli, and D. Jungnickel. Arcs and ovals from abelian groups. In: *Des. Codes Cryptogr.* 26.1-3 (2002), pp. 213–228.

[96] V. M. Sidel'nikov. On mutual correlation of sequences. In: *Doklady Akademii Nauk.* Vol. 196. 3. Russian Academy of Sciences. 1971, pp. 531–534.

[97] J. Steiner. Combinatorische Aufgabe. In: *J. Reine Angew. Math.* 45 (1853), pp. 181–182.

[98] T. Storer. *Cyclotomy and Difference Sets.* Lectures in Advanced Mathematics, No. 2. Chicago: Markham Publishing Co., 1967.

[99] Y. Tan, L. Qu, S. Ling, and C. H. Tan. On the Fourier spectra of new APN functions. In: *SIAM J. Discrete Math.* 27.2 (2013), pp. 791–801.

[100] H. Taniguchi. On some quadratic APN functions. In: *Des. Codes Cryptogr.* 87.9 (2019), pp. 1973–1983.

[101] Z.-X. Wan. *Lectures on Finite Fields and Galois Rings.* Singapore: World Scientific, 2003.

[102] R. M. Wilson. Cyclotomy and difference families in elementary abelian groups. In: *J. Number Theory* 4.1 (1972), pp. 17–47.

[103] R. Wilson. The early history of block designs. In: *Rendiconti del Seminario Matematico di Messina, Serie II* 25.9 (2003), pp. 267–276.

[104] S. Yoshiara. Dimensional dual hyperovals associated with quadratic APN functions. In: *Innov. Incidence Geom.* 8 (2008), pp. 147–169.

[105] S. Yoshiara. Notes on APN functions, semibiplanes and dimensional dual hyperovals. In: *Des. Codes Cryptogr.* 56.2-3 (2010), pp. 197–218.

[106] S. Yoshiara. Equivalences of quadratic APN functions. In: *J. Algebr. Comb.* 35.3 (2012), pp. 461–475.

[107] S. Yoshiara. Equivalences of power APN functions with power or quadratic APN functions. In: *J. Algebraic Combin.* 44.3 (2016), pp. 561–585.

[108] Y. Yu, M. Wang, and Y. Li. A matrix approach for constructing quadratic APN functions. In: *Des. Codes Cryptogr.* 73.2 (2014), pp. 587–600.

[109] Y. Zhou and A. Pott. A new family of semifields with 2 parameters. In: *Adv. Math.* 234 (2013), pp. 43–60.

Tables and figures