Disjoint and external partial difference families and cyclotomy

Laura Johnson

A thesis submitted for the degree of PhD
at the
University of St Andrews

2024

Candidate's declaration

I, Laura Johnson, do hereby certify that this thesis, submitted for the degree of PhD, which is approximately 60,000 words in length, has been written by me, and that it is the record of work carried out by me, or principally by myself in collaboration with others as acknowledged, and that it has not been submitted in any previous application for any degree. I confirm that any appendices included in my thesis contain only material permitted by the 'Assessment of Postgraduate Research Students' policy.

I was admitted as a research student at the University of St Andrews in September 2020.

I received funding from an organisation or institution and have acknowledged the funder(s) in the full text of my thesis.

Date 02/10/2024 Signature of candidate

Supervisor's declaration

I hereby certify that the candidate has fulfilled the conditions of the Resolution and Regulations appropriate for the degree of PhD in the University of St Andrews and that the candidate is qualified to submit this thesis in application for that degree. I confirm that any appendices included in the thesis contain only material permitted by the 'Assessment of Postgraduate Research Students' policy.

Date 02/10/2024 Signature of supervisor

Permission for publication

In submitting this thesis to the University of St Andrews we understand that we are giving permission for it to be made available for use in accordance with the regulations of the University Library for the time being in force, subject to any copyright vested in the work not being affected thereby. We also understand, unless exempt by an award of an embargo as requested below, that the title and the abstract will be published, and that a copy of the work may be made and supplied to any bona fide library or research worker, that this thesis will be electronically accessible for personal or research use and that the library has the right to migrate this thesis into new electronic forms as required to ensure continued access to the thesis.

I, Laura Johnson, confirm that my thesis does not contain any third-party material that requires copyright clearance.

The following is an agreed request by candidate and supervisor regarding the publication of this thesis:

Printed copy

No embargo on print copy.

Electronic copy

No embargo on electronic copy.

Date 02/10/2024 Signature of candidate

Date 02/10/2024 Signature of supervisor

Underpinning Research Data or Digital Outputs

Candidate's declaration

I, Laura Johnson, hereby certify that no requirements to deposit original research data or digital outputs apply to this thesis and that, where appropriate, secondary data used have been referenced in the full text of my thesis.

Date 02/10/2024 Signature of candidate

Abstract

In this Thesis, we introduce two new combinatorial objects known as Disjoint Partial Difference Families and External Partial Difference Families: these objects generalise Disjoint Difference Families (DDFs), External Difference Families (EDFs) and Partial Difference Sets (PDSs), which have all been well-studied in the literature. We demonstrate how DPDFs and EPDFs can be formed from PDSs and Relative Difference Sets (RDSs), presenting both cyclotomic and non-cyclotomic constructions of these objects.

We also develop two new cyclotomic frameworks within this Thesis, which allow us to identify new cyclotomic constructions of DPDFs and EPDFs along with other types of difference structures. The first of these cyclotomic frameworks relies upon a series of partition results, the second utilises natural connections between cyclotomic numbers and cyclotomic cosets. These frameworks remove the need to evaluate all cyclotomic numbers in a particular finite field.

We primarily use these frameworks to identify new DPDF and EPDF constructions, however, we also use the cyclotomic techniques underpinning these frameworks to establish a series of algorithms that compute the cyclotomic numbers in a given finite field. Further, we use one of these frameworks to prove that a PDS with Denniston parameters exists in the group $\mathbb{Z}_3^9$: as 3 is an odd prime, it was previously believed that such a PDS would not exist in this group.

Acknowledgements

First and foremost, I would like to thank my PhD supervisor Dr. Sophie Huczynska, for all of her support and encouragement over the past 4 years. Under her guidance, I have grown significantly both in confidence and in my mathematical ability. I have thoroughly enjoyed working on difference structures with Sophie over the past few years and I look forward to our future, related projects on the horizon.

Thank you also to my second supervisor Prof. Christopher Jefferson for his help during my PhD, particularly for his detailed comments on the algorithmic material in Chapter 4.

I would also like to thank my friends and family for motivating me and providing distractions from work when needed. I would especially like to thank Lizzie, Elisabeth, Victoria and Harry for always being there to cheer me on when I needed support. Thank you also to my parents and grandmother for their practical support throughout my PhD, and to my Uncle Mark for always expressing enthusiasm for my work.

Finally, I would like to thank to my partner Nicholas for keeping me going during my PhD. His help and gentle encouragement, especially during the last few months, has made this process a lot easier.

This work was supported by a University of St. Andrews Handsel Tuition Fee Scholarship.

Contents

1 **Introduction** **1**

1.1 Motivation and Outline 1

1.2 Preliminaries/notation 3

1.3 Difference families 5

1.4 Cyclotomy in finite fields 16

2 **Cyclotomic frameworks** **31**

2.1 Key cyclotomic number framework 32

2.1.1 Internal differences 32

2.1.2 External differences 44

2.1.3 Uniform cyclotomy 46

2.2 Cyclotomic orbit framework 52

2.2.1 Cyclotomic coset representatives 73

3 **Cyclotomic constructions of DPDFs and EPDFs** **75**

3.1 PDS constructions for small e 76

3.2 DPDF/EPDF constructions from unions of PDSs 81

3.3 DPDF/EPDF partition constructions 83

3.4 Explicit DPDF/EPDF constructions obtained by partitioning the squares into cyclotomic classes with small e 91

3.5 DPDF/EPDF constructions obtained by partitioning the squares into cyclotomic classes with small f 93

3.6 Cyclotomic DPDF construction obtained via the use of cyclotomic orbits 98

4 **A cyclotomic number algorithm and Denniston PDSs** **100**

4.1 Algorithm for computing cyclotomic numbers in large finite fields 100

4.1.1 The Wen et al. paper 101
4.1.2 Comments on Wen et al. algorithm 104
4.1.3 Adapted Wen et al. algorithm for computing internal cyclotomic numbers 106
4.1.4 Algorithm for computing external cyclotomic numbers . . 111
4.2 Denniston partial difference sets 114
4.2.1 Background 114
4.2.2 Proving that a PDS with Denniston parameters in which $r = 1$ exists in $\mathbb{Z}_3^9$ 116

5 Non-cyclotomic constructions of DPDFs and EPDFs 125
5.1 DPDF and EPDF constructions arising from non-cyclotomic PDSs 126
5.2 DPDF and EPDF constructions arising from Relative Difference Sets 130
5.2.1 Extension of Bose's construction to DPDFs/EPDFs 135
5.3 DPDFs that are not EPDFs and vice versa 137

6 Conclusion and further work 139

Appendices 147

A Cyclotomic numbers 148

B All cyclotomic DPDFs and EPDFs 152

C Cyclotomic numbers of order 13 in the finite field GF(729) 156

D Cyclotomic number calculations in GF(729) 157

Chapter 1

Introduction

1.1 Motivation and Outline

In this Thesis, we introduce two new combinatorial structures known as Disjoint Partial Difference Families (DPDFs) and External Partial Difference Families (EPDFs). These objects generalise three well-studied combinatorial objects in the literature, known as Disjoint Difference Families (DDFs), External Difference Families (EDFs) and Partial Difference Sets (PDSs).

We can group all of these objects together under the umbrella term “difference structure”. Difference structures first arose in the literature in the 1930s in the work of Paley [56] and Bose [7]. (These objects were implicitly defined in these papers; we now refer to these objects as Partial Difference Sets (PDSs) and Difference Sets respectively.) PDSs are closely connected to association schemes and strongly regular graphs. Bose’s motivations for constructing Difference Sets centred around design theoretic applications, specifically he wanted to identify new construction of balanced incomplete block designs (BIBDs). In the 1970s, Wilson demonstrated that PDSs can also be used to find constructions of block designs known as partial BIBDS (PBIBDs), in [66] he also defined Difference Families in this paper (DFs). DFs are a generalisation of Difference Sets: a DF with disjoint component sets is known as Disjoint Difference Family (DDF). DDFs have been particularly well-studied (see for example Novak’s conjecture [29],[54]). More recently, they have been studied for their various applications in information security and other areas of combinatorics (see [9],[10],[14],[32],[46],[53]).

In the early 2000s, Ogata et al. defined an external analogue of Disjoint Difference Families, known as an External Difference Family (EDF) [55]. EDFs are of particular interest to cryptographers, as they can be used to build a type of cryptographical tool, known as an authentication code, which protects against attacks from active adversaries (see [19],[55],[58]). Owing to their applications in information security, many variants of EDFs have been studied in the literature (see [2],[16],[21],[33],[37],[38],[58]). The objects introduced in this Thesis very naturally extend many of these structures.

A second theme of this Thesis is using and developing finite field cyclotomy to identify constructions of difference structures (including the first cyclotomic proof that a PDS with Denniston parameters exists an elementary abelian group in which p is an odd prim(e). Finite field cyclotomy was first studied by Gauss in the 1800s and continues to be studied, owing to the difficulty of determining concrete values of cyclotomic numbers in finite fields. Currently mathematicians have only been able to determine certain sporadic values of cyclotomic numbers of order up to 24 (see [5]), and as these results are expressed indirectly in terms of character sums, they can be hard for combinatorialists with no experience of character theory to interpret. This Thesis develops two new cyclotomic frameworks that identify alternative ways of working with finite field cyclotomy.

In the first Chapter of this Thesis, we introduce DPDFs and EPDFs, as well as necessary group theoretic and cyclotomic results. The second Chapter is concerned with developing two cyclotomic frameworks for establishing new DPDF and EPDF constructions: the first framework relies upon a series of partition results to identify certain structural properties which yield new DPDF and EPDF constructions, while the second framework establishes a connection between cyclotomic numbers and cyclotomic cosets. In Chapter 3, we use the frameworks developed in Chapter 2 to establish new constructions of DPDFs and EPDFs. In Chapter 4, we apply the cyclotomic techniques developed in Chapter 2 to more general problems in this area of combinatorics, namely we develop a series of algorithms that may be used to compute cyclotomic numbers in large finite fields, and we discuss how cyclotomy may be used to prove that PDSs with Denniston parameters (see [23]) exist for odd primes.

Finally, in Chapter 5 we present a series of non-cyclotomic DPDF and EPDF constructions, which use group rather than field properties. We also present the first examples of DPDFs that are not EPDFs and vice versa.

1.2 Preliminaries/notation

Before we move on to the main themes of this Thesis, we must first cover some of the common notation used in this area of combinatorics, as well as some important preliminary results. For further information on all of the classic combinatorial structures discussed throughout this Thesis, see [17].

Let G be a group, which we write additively, unless otherwise stated the identity of G is 0. Throughout this Thesis, the notation G^* be used to denote the set $\mathrm{G}\backslash\{0\}$ (this is consistent with notation used in literature on difference families). For an element $g \in \mathrm{G}$, we will consistently use the notation $\langle g \rangle$ to denote the subgroup generated by $g \in \mathrm{G}$.

Throughout this Thesis we introduce various sets: note that capital italic letters will henceforth only be used to describe sets. For the purposes of this Thesis, we assume that S^* denotes the non-zero elements of the set S. We also introduce various multisets throughout this body of work: note that the symbols $\Delta(D)$, $\Delta(D_1, D_2)$, $\mathrm{Int}(D)$ and $\mathrm{Ext}(D)$ (where D, D_1 and D_2 are sets) will be exclusively used to describe multisets. Below we introduce the multisets $\Delta(D)$ and $\Delta(D_1, D_2)$; the multisets $\mathrm{Int}(D)$ and $\mathrm{Ext}(D)$ will be introduced in a later part of this Chapter.

Definition 1.2.1. *(i) For a subset $D \subseteq \mathrm{G}$, we define the multiset*

$$\Delta(D) = \{x - y : x \neq y \in D\}.$$

(ii) For two subsets $D_1, D_2 \subseteq \mathrm{G}$, we define the multiset

$$\Delta(D_1, D_2) = \{x - y : x \in D_1, y \in D_2\}.$$

In the literature, it is often specified that $D_1, D_2 \subseteq \mathrm{G}$ must be disjoint subsets of a group G. As in Chapter 4 we will look at a special case in which we allow $D_1, D_2 \subseteq \mathrm{G}$ to be non-disjoint sets, we specify that it is possible for D_1 and D_2 to be non-disjoint in Definition 1.2.1. Finally, for a subset $D \subseteq \mathrm{G}$ and a non-negative integer λ, we denote the multiset conisting of λ copies of the set D by the notation λD. With the multisets $\Delta(D)$ and $\Delta(D_i, D_j)$ defined, we note the following.

Remark 1.2.2. *Let* G *be a group and D be a k-subset of* G*, then*

$$\Delta(D,D) = \Delta(D) \cup k\{0\}.$$

We now establish some new notation which is used throughout this Thesis.

Definition 1.2.3. *Let $S' = \{D_1, \ldots, D_m\}$ denote a collection of m (usually pairwise disjoint) subsets of* G*. We define the following multisets:*

(i) $\mathrm{Int}(S') = \bigcup_{i=1}^{m} \Delta(D_i)$

(ii) $\mathrm{Ext}(S') = \bigcup_{\substack{1 \le i,j \le m \\ i \ne j}} \Delta(D_i, D_j).$

We refer to $\mathrm{Int}(S')$ *as the* ***internal differences*** *of $S' = \{D_1, \ldots, D_m\}$ and* $\mathrm{Ext}(S')$ *as the* ***external differences*** *of $S' = \{D_1, \ldots, D_m\}$.*

The following lemma plays an important role in many subsequent results.

Lemma 1.2.4. *Let S be a subset of elements of a group* G*, partitioned by $S' = \{D_1, \ldots, D_m\}$, where S' is a collection of m disjoint subsets. Then the following multiset equation holds*

$$\mathrm{Int}(S') \cup \mathrm{Ext}(S') = \Delta(S).$$

Proof. Since S' is a partition of S into m disjoint subsets, we may write

$$\Delta(S) = \Delta(D_1 \cup D_2 \cup \ldots \cup D_m) = \bigcup_{i=1}^{m} \Delta(D_i) \cup \bigcup_{\substack{1 \le i,j \le m \\ i \ne j}} \Delta(D_i, D_j) = \mathrm{Int}(S') \cup \mathrm{Ext}(S').$$

□

Some results within this Thesis rely upon translating subsets of a group. The formal definition of a translate is given below.

Definition 1.2.5. *Let* G *be an additive group, $g \in$* G *and $S \subseteq$* G*. The* ***translate*** *of S by g is defined by the set $g+S = \{g+s | s \in S\}$. Suppose* G *is a multiplicative group, then the* ***translate*** *of S by g is the set $gS = \{gs | s \in S\}$.*

1.3 Difference families

Disjoint and External Partial Difference Families are relatively new combinatorial objects, that I first defined at the outset of my PhD. My supervisor and I formally define these objects in our joint paper [34]. Both of these objects are types of difference structures. In this Section, we cover the definitions and applications of related difference structures, and we also explore how the new objects that I have defined fit into this area of combinatorics.

In essence, the term difference family refers to a combinatorial object with certain uniform difference properties. The study of objects with interesting uniform difference properties began in the 1930s, when in [56] Paley recorded the an infinite construction of a family of objects, which exist in any finite field $\mathrm{GF}(q)$ of order $q \equiv 3 \mod 4$. These structures are now known as Partial Difference Sets.

Definition 1.3.1. *Let* G *be a group of order* n *and* P *be a* k*-subset of* G*. Then* P *is an* (n, k, λ, μ)***-Partial Difference Set*** *(or* (n, k, λ, μ)***-PDS****) if the following multiset equation is satisfied:*

$$\Delta(P) = \lambda(P^*) \cup \mu(\mathrm{G}^* \backslash P),$$

for some non-negative integers λ, μ*. We say that* P *is* ***proper*** *if* $\lambda \neq \mu$ *and that* P *is* ***regular*** *if* $P = -P$ *and* $0 \notin P$*.*

PDSs are now well-researched combinatorial objects (see [49],[61],[63]), owing to their links with association schemes and strongly regular graphs ([48],[61]), their connections with combinatorial designs ([47],[66]) and their applications in coding theory ([22],[39]).

Paley's construction in [56] also yields an infinite construction of another type of difference family known as a Difference Set.

Definition 1.3.2. *Let* G *be a group of order* n *and* D *be a* k*-subset of* G*. Then* D *is an* (n, k, λ)***-Difference Set*** *if the following multiset equation is satisfied:*

$$\Delta(D) = \lambda(\mathrm{G}^*),$$

for some non-negative integer λ*.*

Difference Sets were later generalised to structures known as Difference Families in [66].

Definition 1.3.3. *Let G be a group of order n and $S' = \{D_1, \dots, D_m\}$ be a collection of k-subsets of G. Then S' is an (n, m, k, λ)-**Difference Family** (or (n, m, k, λ)-**DF**) if the following multiset equation is satisfied:*

$$\mathrm{Int}(S') = \lambda(\mathrm{G}^*).$$

*We say that a difference family is **disjoint** if S' is a collection of disjoint subsets. Throughout this thesis, we often use **DDF** as an abbreviation of Disjoint Difference Family. We say that a DDF is **near-complete** if its sets partition G^*.*

In fact, the following remark demonstrates that both PDSs and (D)DFs can be thought of as generalisations of Difference Sets.

Remark 1.3.4. *Let D be an (n, k, λ)-Difference Set in the group G observe that we can also view D as being*

(i) an (n, k, λ, λ)-PDS,

(ii) an $(n, 1, k, \lambda)$-DDF.

Example 1.3.5. *In the group $\mathbb{Z}_7$, the set $D = \{1, 2, 4\}$ forms a $(7, 3, 1)$-Difference Set. To see this observe that*

$$\Delta(D) = \{1-2, 1-4, 2-1, 2-4, 4-1, 4-2\} = \{6, 4, 1, 5, 3, 2\}$$

The set $D = \{1, 2, 4\}$ is thus consistent with the definition of $(7, 3, 1)$-Difference Set since it is a subset of size 3 in the group $\mathbb{Z}_7$, in which every element of $\mathbb{Z}_7$ occurs once in the multiset $\Delta(D)$. Notice that this is also consistent with the definition of a $(7, 3, 1, 1)$-Partial Difference Set, as all of the elements in the set $D = \{1, 2, 4\}$ occur with frequency 1 in the multiset $\Delta(D)$, and all of the elements in $\mathrm{G} \backslash D = \{3, 5, 6\}$ also occur with frequency 1 in $\Delta(D)$. Similarly, we can view D as a $(7, 1, 3, 1)$-DDF. For an example of a PDS that is not also a Difference Set, observe that the set $\{(0, 1), (0, 2)\}$ forms a $(9, 2, 1, 0)$-PDS in the group $\mathbb{Z}_3 \times \mathbb{Z}_3$. The collection of subsets $S' = \{\{1, 2, 4\}, \{3, 5, 6\}\}$ in $\mathbb{Z}_7$ is an example of a $(7, 2, 3, 2)$-DDF that is not simultaneously a Difference Set.

Difference Sets and Difference Families (particularly DDFs) have also attracted a lot of attention from the combinatorial community, owing to their applications in various areas of combinatorics. In fact, Difference Sets and Difference Families were first defined by Bose and Wilson respectively (in [7] and [66]) to identify new constructions of balanced incomplete block designs. In more recent years, the connection between these objects and partitions of complete multipartite graphs have been well-studied ([12],[57]). The applications of these objects in information security have also attracted recent attention (see [11],[52],[53]).

External Difference Families (or EDFs) are another type of difference family that have been well-researched in recent years. First defined in [55] and [19], these objects are essentially external analogues of DDFs.

Definition 1.3.6. *Let G be a group of order n and $S' = \{D_1, \dots, D_m\}$ be a collection of disjoint k-subsets of G. Then S' is an (n, m, k, λ)-**External Difference Family** (or (n, m, k, λ)-**EDF**) if the following multiset equation is satisfied*

$$\mathrm{Ext}(S') = \lambda(\mathrm{G}^*).$$

*We say that an EDF is **near-complete** if its sets partition G^*.*

Example 1.3.7. *In $\mathbb{Z}_5$, let $S' = \{\{1, 4\}, \{2, 3\}\}$. The first subtraction table below contains the elements of the multiset $\Delta(\{1, 4\}, \{2, 3\})$, and the second subtraction table contains the elements of the multiset $\Delta(\{2, 3\}, \{1, 4\})$.*

$-$	2	3
1	4	3
4	2	1

$-$	1	4
2	1	3
3	2	4

Notice that since $\mathrm{Ext}(S') = \Delta(\{1, 4\}, \{2, 3\}) \cup \Delta(\{2, 3\}, \{1, 4\})$, it follows that every non-identity element of $\mathbb{Z}_5$ occurs twice in the multiset union $\mathrm{Ext}(S')$ hence S' is a $(5, 2, 2, 2)$-EDF.

EDFs have attracted much attention in recent years, predominantly due to their applications in cryptography: they can be used to design cryptographical tools that meet particular optimality constraints. They can also be used to build cryptographical tools with perfect secrecy. A cryptographical tool is said to have **perfect secrecy** if each encoded message reveals no information about the plaintext source that has been encrypted. In the paper [58], many variants of EDFs are detailed, all of which have their own interesting applications in information security.

As EDFs and DDFs are analogues of one another, there are interesting connections between these objects. In what follows, we cover a result of [14] that highlights the connections between DDFs and EDFs that partition the non-identity elements of a group G. Before we arrive at this result, we require an intermediary Proposition.

Proposition 1.3.8. *Let G be a group of order n, then $\Delta(\mathrm{G}^*) = (n-2)\mathrm{G}^*$ and G^* is an $(n, n-1, n-2)$-Difference Set.*

We can now prove the following result of Chang and Ding detailed in [14]. Note that a similar result is also given in [21]: in this paper the authors show that any partition S' of G^* is a near-complete DDF if and only if it is a near-complete EDF.

Proposition 1.3.9. *Let $(G, +)$ be an abelian group of order n and $S' = \{D_1, \ldots, D_m\}$ be a collection of k-subsets of G. If S' is a partition of G^*, then S' is an $(n, m, k, n-k-1)$-EDF in G if and only if it is an $(n, m, k, k-1)$-DDF in G.*

Proof. By Proposition 1.3.8, it follows that $\Delta(\mathrm{G}^*) = (n-2)\mathrm{G}^*$. Since S' partitions G^*, when S' is an $(n, m, k, n-k-1)$-EDF, it follows by Proposition 1.2.4 that

$$(n-k-1)\mathrm{G}^* \cup \mathrm{Int}(S') = (n-2)\mathrm{G}^*,$$

and hence, $\mathrm{Int}(S') = (k-1)\mathrm{G}^*$. It therefore follows by Definition 1.3.3 that S' is a $(n, m, k, k-1)$-DDF when S' is an $(n, m, k, n-k-1)$-EDF. It analogously follows that if S' is a $(n, m, k, k-1)$-DDF then S' is also an $(n, m, k, n-k-1)$-EDF. □

Observe that for any DDF S' partitioning G^*, the multiset union $\mathrm{Int}(S')$ must consist of precisely $k-1$ copies of each non-identity element of G^*. To see this, note that $|\mathrm{Int}(S')| = mk(k-1)$, where $mk = n-1$ as the m k-subsets of S' partition the elements of G^*. As $\mathrm{Int}(S')$ must comprise an equal number of copies of each element of G^*, it follows that $\mathrm{Int}(S') = (k-1)\mathrm{G}^*$. Hence, the DDF and EDF parameters in Proposition 1.3.9 apply to any DDF or EDF that partitions G^* when G is an additive abelian group.

Moreover, notice that the relationship between the multiset unions $\mathrm{Int}(S')$ and $\mathrm{Ext}(S')$ in Proposition 1.3.9 depends upon the multiset $\Delta(\mathrm{G}^*)$ containing precisely $n-2$ copies of each non-identity element of G^* in the above proof. By replacing G^* by a general (n, k, λ)-Difference Set, S, where clearly $\Delta(S) = \lambda\mathrm{G}^*$, we can see that it is possible to partition any Difference Set into a collection of disjoint subsets that is simultaneously a DDF and an EDF (it should be noted that this change will alter the DDF and EDF parameters). However, this property does not hold for a proper (n, m, k, λ, μ)-Partial Difference Set, P, since $\Delta(P) = \lambda(P) \cup \mu(\mathrm{G}^*\backslash P)$ by definition. The following remark therefore establishes an equivalent relationship between the multiset unions $\mathrm{Int}(S')$ and $\mathrm{Ext}(S')$ for S' partitioning an (n, m, k, λ, μ)-PDS. This remark motivates the definitions of Disjoint Partial Difference Families (or DPDFs) and External Partial Difference Families (or EPDFs), as we will see presently.

Remark 1.3.10. *Let G be a group of order n, and let S be an (n, k, λ, μ)-PDS and suppose $S' = \{D_1, \ldots, D_m\}$ is a collection of subsets that partition S, then*

(i) if S' is an (n, m, k, λ')-DDF, by Lemma 1.2.4,

$$\mathrm{Ext}(S') = (\lambda - \lambda')(S^*) \cup (\mu - \lambda')(\mathrm{G}^*\backslash S).$$

(ii) if S' is an (n, m, k, λ')-EDF, it follows by Lemma 1.2.4 that

$$\mathrm{Int}(S') = (\lambda - \lambda')(S^*) \cup (\mu - \lambda')(\mathrm{G}^*\backslash S).$$

Remark 1.3.10 therefore demonstrates that in order to study partitions of PDSs, new combinatorial objects must be defined, in which the internal/external differences produce each non-identity of a group G at one of two frequencies, dependant upon membership/non-membership of the PDS. Hence, this Remark lead me to define DPDFs and EPDFs, which are objects with precisely these structural properties.

These seemed like natural objects to define since similar analogues of Difference Sets (namely DDFs and EDFs) had already been defined, and proven to have many interesting applications to other areas of combinatorics (see abov(e). Formal definitions of these objects first appear in my joint paper with my supervisor [34].

Definition 1.3.11. *Let G be a group of order n, $S' = \{D_1, \ldots, D_m\}$ be a collection of disjoint k-subsets of* G^* *and $S = \cup_{i=1}^{m} D_i$. Then S' is an (n, m, k, λ, μ)-**Disjoint Partial Difference Family** (or (n, m, k, λ, μ)-**DPDF**) if the following multiset equation is satisfied*

$$\mathrm{Int}(S') = \lambda(S^*) \cup \mu(\mathrm{G}^* \backslash S).$$

*If $\lambda \neq \mu$ then S' is called **proper**.*

Definition 1.3.12. *Let G be a group of order n, $S' = \{D_1, \ldots, D_m\}$ be a collection of disjoint k-subsets of* G^* *and $S = \cup_{i=1}^{m} D_i$. Then S' is an (n, m, k, λ, μ)-**External Partial Difference Family** (or (n, m, k, λ, μ)-**EPDF**) if the following multiset equation is satisfied*

$$\mathrm{Ext}(S') = \lambda(S^*) \cup \mu(\mathrm{G}^* \backslash S).$$

*If $\lambda \neq \mu$ then S' is called **proper**.*

Example 1.3.13. *In the group $\mathbb{Z}_3^2$, let $S' = \{D_1, D_2\}$, where $D_1 = \{(0, 1), (0, 2)\}$, and $D_2 = \{(1, 2), (2, 1)\}$. S' is both a $(9, 2, 2, 1, 0)$-DPDF and a $(9, 3, 2, 0, 2)$-EPDF. To highlight this, I have included two subtraction tables below the first table contains the internal differences between elements in D_1 and D_2, and the second table contains all external differences between these sets.*

$-$	$(0,1)$	$(0,2)$	$(1,2)$	$(2,1)$
$(0,1)$	-	$(0,2)$		
$(0,2)$	$(0,1)$	-		
$(1,2)$			-	$(2,1)$
$(2,1)$			$(1,2)$	-

$-$	$(0,1)$	$(0,2)$	$(1,2)$	$(2,1)$
$(0,1)$			$(2,2)$	$(1,0)$
$(0,2)$			$(2,0)$	$(1,1)$
$(1,2)$	$(1,1)$	$(1,0)$		
$(2,1)$	$(2,0)$	$(2,2)$		

From these tables, it is clear that $\mathrm{Int}(S') = \{(0, 1), (0, 2), (1, 2), (2, 1)\}$ *and* $\mathrm{Ext}(S')$ *contains two copies of each of the elements* $\{(1, 1), (2, 2), (1, 0), (2, 0)\}$. *As $D_1 \cup D_2 = \{(0, 1), (0, 2), (1, 2), (2, 1)\}$ and $(\mathbb{Z}_3^2)^* \backslash \{D_1 \cup D_2\} = \{(1, 0), (2, 0), (1, 1), (2, 2)\}$, it follows by Definitions 1.3.11 and 1.3.12 that S' is both a $(9, 2, 2, 1, 0)$-DPDF and a $(9, 3, 2, 0, 2)$-EPDF.*

Some related structures to DPDFs and EPDFs have previously been explored in the literature. For example, Almost Difference Families, first studied in [27], are structures in which every non-identity element of a group G, occurs either λ or $\lambda+1$ times in the multiset $\mathrm{Int}(S')$: note that the frequency at which an element occurs as a difference in $\mathrm{Int}(S')$ is not determined by whether it is contained within one of the subsets of S'. Another related, existing structure, also known as an External Partial Difference Family, was defined in [21]. Under the definition of an External Partial Difference Family given in [21], if a collection of m disjoint k-subsets $S' = \{D_1, \ldots, D_u\}$ is an External Partial Difference Family, then S' must partition G^* and the frequency at which an element of G^* occurs in $\mathrm{Ext}(S')$ depends upon membership/non-membership of the collection of subsets $\cup_{i=1}^{\gamma} D_i$ for $\gamma \in \{1, \ldots, u-1\}$. Finally, in [52], the authors implicitly explore various EPDF constructions in order to construct a type of combinatorial object known as a Difference System of Sets. These objects are all similar to DPDFs/EPDFs but do not naturally subsume other difference family definitions: in following results, we see that other varieties of difference families can be thought of as DPDFs/EPDFs that meet particular constraints.

We now observe an important result about the parameters of a DPDF/EPDF.

Lemma 1.3.14. *(i) If S' is a $(n, m, k, \lambda_1, \mu_1)$-DPDF, then*

$$mk(k-1) = \lambda_1 mk + \mu_1(n-1-mk).$$

(ii) If S' is a $(n, m, k, \lambda_2, \mu_2)$-EPDF, then

$$m(m-1)k^2 = \lambda_2 mk + \mu_2(n-1-mk).$$

Proof. (i) Suppose that $S' = \{D_1, \ldots, D_m\}$, and let $S = \cup_{i=1}^{m} D_i$. By definition, since S' is a DPDF, then the following multiset equation must hold $\mathrm{Int}(S') = \lambda_1(S) \cup \mu_1(\mathrm{G}^* \backslash S)$. We may then write $|\mathrm{Int}(S')| = \lambda_1|S| + \mu_1|(\mathrm{G}^*\backslash S)|$. As $\mathrm{Int}(S')$ comprises s multisets of the form $\Delta(D_i)$, where $D_i \in S'$, and each multiset $\Delta(D_i)$ has cardinality $k(k-1)$, it follows that $|\mathrm{Int}(S')| = mk(k-1)$. Moreover, since S comprises the union of m pairwise disjoint k-subsets, it is clear that $|S| = mk$, and from this we can obtain $|\mathrm{G}^*\backslash S| = n-1-mk$.

(ii) The proof of this result is analogous to the proof of part (i). □

Remark 1.3.15. *Let G be a group and suppose that S' is a collection of m disjoint k-subsets, then*

(i) every (n, k, λ, μ)-PDS is an $(n, 1, k, \lambda, \mu)$-DPDF.

(ii) every (n, m, k, λ)-DDF is an $(n, m, k, \lambda, \lambda)$-DPDF,

(iii) every (n, m, k, λ)-EDF is an $(n, m, k, \lambda, \lambda)$-EPDF.

With DPDFs and EPDFs defined, we are able to partition both Difference Sets and PDSs into DDFs/EDFs/DPDFs/EPDFs.

Theorem 1.3.16. *In a group G of order n, let $S' = \{D_1, \dots, D_m\}$ be a collection of m disjoint k-subsets and suppose that $S = \cup_{i=1}^{m} D_i$ is an (n, mk, λ)-Difference Set. Then*

(i) S' is an (n, m, k, λ')-DDF if and only if S' is an $(n, m, k, \lambda - \lambda')$-EDF,

(ii) S' is an $(n, m, k, \lambda', \mu')$-DPDF if and only if S' is an $(n, m, k, \lambda - \lambda', \mu - \mu')$-EPDF.

Proof. (i) It follows by Remark 1.3.4 that we can think of a DS as being a PDS in which $\lambda = \mu$. This result then immediately follows from Remark 1.3.10.

(ii) When S is an (n, m, k, λ) Difference Set, by Definition 1.3.2, $\Delta(S) = \lambda(G^*)$. If we then assume that S' is an $(n, m, k, \lambda', \mu')$-DPDF, this means that $\mathrm{Int}(S') = \lambda'(S^*) \cup \mu'(\mathrm{G}^* \backslash S)$. It then follows by Lemma 1.2.4 that

$$(\lambda'(S^*) \cup \mu'(\mathrm{G}^* \backslash S)) \cup \mathrm{Ext}(S') = \lambda \mathrm{G}^*$$
$$\Leftrightarrow \mathrm{Ext}(S') = (\lambda - \lambda')(S^*) \cup (\lambda - \mu')(\mathrm{G}^* \backslash S).$$

By Definition 1.3.12, this then implies that S' is an $(n, m, k, \lambda - \lambda', \mu - \mu')$-EPDF. The reverse direction is analogous. □

Theorem 1.3.17. *In a group G of order n, let $S' = \{D_1, \dots, D_m\}$ be a collection of m disjoint k-subsets and suppose that $S = \cup_{i=1}^{m} D_i$ is an (n, mk, λ, μ)-PDS. Then*

(i) S' is an $(n, m, k, \lambda', \mu')$-DPDF if and only if S' is an $(n, m, k, \lambda - \lambda', \mu - \mu')$-EPDF,

(ii) S' *is an* (n, m, k, λ')*-DDF if and only if* S' *is an* $(n, m, k, \lambda - \lambda', \mu - \lambda')$*-EPDF,*

(iii) S' *is an* (n, m, k, σ)*-EDF if and only if* S' *is an* $(n, m, k, \lambda', \mu')$*-DPDF, where* $\lambda - \lambda' = \mu - \mu' = \sigma$*.*

Proof. By Definition 1.3.1, as S is an (n, mk, λ, μ)-PDS, this means that $\Delta(S) = \lambda(S) \cup \mu(\mathrm{G}^*\backslash S)$. Moreover, if we assume that S' is an $(n, m, k, \lambda', \mu')$-DPDF, by Definition 1.3.11, $\mathrm{Int}(S') = \lambda'(S) \cup \mu'(\mathrm{G}^*\backslash S)$. By Lemma 1.2.4, this means that

$$\begin{aligned}\lambda'(S^*) \cup \mu'(\mathrm{G}^*\backslash S) \cup \mathrm{Ext}(S') &= \lambda(S^*) \cup \mu(\mathrm{G}^*\backslash S)\\ \Leftrightarrow \mathrm{Ext}(S') &= (\lambda - \lambda')(S^*) \cup (\mu - \mu')(\mathrm{G}^*\backslash S).\end{aligned}$$

It then follows by Definition 1.3.12 that S' is an $(n, m, k, \lambda - \lambda', \mu - \mu')$-EPDF. By Lemma 1.3.15, parts (ii) and (iii) are special cases of part (i), in which $\lambda' = \mu'$ and $\lambda - \lambda' = \mu - \mu'$ respectively. □

Lemma 1.2.4 highlights a clear, bidirectional relationship between the internal/external differences of a collection of subsets, S', that partition a larger set S and the behaviour of the multiset $\Delta(S)$. In the previous result, we looked at how we can partition PDSs into DPDFs and EPDFs. We now see that if we have a collection of subsets, S', that simultaneously is a DPDF and an EPDF, the union of these subsets in S' must be a PDS.

Theorem 1.3.18. *Let* G *be a group, and* $S' = \{D_1, \dots, D_m\}$ *be a collection of* k*-subsets of* G*. Suppose* S' *partitions a set* S*, then if* S' *is both an* $(n, m, k, \lambda', \mu')$*-DPDF and an* (n, m, k, λ, μ)*-EPDF, then* S *is always an* $(n, mk, \lambda+\lambda', \mu+\mu')$*-PDS and an* $(n, m, k, \lambda + \lambda')$*-Difference Set in the case where* $\lambda + \lambda' = \mu + \mu'$*.*

Proof. By Definitions 1.3.11 and 1.3.12, when S' is both an (n, m, k, λ, μ)-DPDF and an $(n, m, k, \lambda', \mu')$-EPDF, this means that $\mathrm{Int}(S') = \lambda(S^*) \cup \mu(\mathrm{G}^*\backslash S)$ and $\mathrm{Ext}(S') = \lambda'(S^*) \cup \mu'(\mathrm{G}^*\backslash S)$. It therefore follows by Lemma 1.2.4 that

$$\begin{gathered}(\lambda(S^*) \cup \mu(\mathrm{G}^*\backslash S)) \cup (\lambda'(S^*) \cup \mu'(\mathrm{G}^*\backslash S)) = \Delta(S) \Leftrightarrow\\ (\lambda + \lambda')S^* \cup (\mu + \mu')(\mathrm{G}^*\backslash S) = \Delta(S).\end{gathered}$$

It then follows by Definition 1.3.1 that S is an $(n, mk, \lambda+\lambda', \mu+\mu')$-PDS. □

We have seen so far in this Section that DPDFs and EPDFs subsume the definitions of various other difference structures. We have also demonstrated that these structures can also be used to partition both Difference Sets and PDSs into interesting sub-structures. We now close this Section by further motivating DPDFs and EPDFs by demonstrating that constructions of DPDFs and EPDFs naturally arise from existing constructions of PDSs. Before we get onto these results, we require the following Theorem, which summarises a series of results in [47], and is recorded in a similar format in [34].

Theorem 1.3.19. *Let G be a group of order n. Let $S \subseteq G$, such that S has cardinality k and S is an (n, k, λ, μ)-PDS.*

(i) If S is not proper (i.e. S is a Difference Set), its complement $\mathrm{G}\backslash S$ is also a Difference Set.

(ii) If S is a proper PDS, then $S = -S$.

(iii) If S is a regular PDS then $S \cup \{0\}$, $\mathrm{G}^{*}\backslash S$, $\mathrm{G}\backslash S$ and $(\mathrm{G}\backslash S)\backslash\{0\}$ are all also PDSs.

(iv) If S is a non-regular proper PDS, then $S\backslash\{0\}$, $\mathrm{G}^{*}\backslash S$ $\mathrm{G}\backslash S$ and $(\mathrm{G}\backslash S) \cup \{0\}$ are also PDSs.

(v) If S is a non-trivial subgroup of G, then it is a $(n, k, k-1, 0)$-PDS.

(vi) If $\lambda \neq 0$ and $\mu = 0$, then $S \cup \{0\}$ is a subgroup of G.

The following results from [34] demonstrate how DPDFs and EDPFs can be obtained from existing PDS constructions.

Theorem 1.3.20. *Let G be a group of order n, $S' = \{D_1, \ldots, D_m\}$ be a collection of disjoint k-subsets of G and $S = \cup_{i=1}^{m} D_i$. Suppose that each $D_i \in S'$ is an (n, k, λ, μ)-PDS. Then*

(i) S' is an $(n, m, k, \lambda(m-1)\mu, m\mu)$-DPDF,

(ii) if S is an (n, mk, η, ν)-PDS, then S' is also an $(n, m, k, \eta-(\lambda(m-1)\mu), \nu-m\mu)$-EPDF.

Proof. (i) It follows by Definition 1.2.3 that

$$\mathrm{Int}(S') = \bigcup_{i=1}^{m} \Delta(D_i).$$

Since each $D_i \in S'$ is an (n, k, λ, μ)-PDS, it follows by Definition 1.3.1 that

$$\begin{aligned}\mathrm{Int}(S') &= (\lambda(D_1) \cup \mu(\mathrm{G}^*\backslash D_1)) \cup (\lambda(D_2) \cup \mu(\mathrm{G}^*\backslash D_2)) \cup \ldots \cup \\ &\qquad (\lambda(D_m) \cup \mu(\mathrm{G}^*\backslash D_m)) \\ &= (\lambda(D_1) \cup \mu(D_2 \cup \ldots \cup D_m)) \cup (\lambda(D_2) \cup \mu(D_1 \cup D_3 \cup \ldots D_m)) \cup \\ &\qquad \ldots \cup (\lambda(D_m) \cup \mu(D_1 \cup \ldots D_{m-1})).\end{aligned}$$

The above multiset union, $\mathrm{Int}(S')$, is broken up into precisely m expressions, with each expression corresponding to the elements of a multiset of the form $\Delta(D_i)$, where $D_i \in S'$. Notice that for every $D_i \in S'$, D_i occurs at frequency μ in precisely $m-1$ of these expressions, while in the expression corresponding to the multiset $\Delta(D_i)$, D_i occurs at frequency λ. For every $a \in \mathrm{G}^*\backslash S$, where $S = D_1 \cup D_2 \cup \ldots \cup D_m$, a occurs at frequency μ in each of the m expressions in $\mathrm{Int}(S')$. Since $D_1 \cup D_2 \cup \ldots \cup D_m = S$, we may rewrite this multiset union as;

$$\mathrm{Int}(S') = (\lambda + (m-1)\mu)S \cup m\mu(\mathrm{G}^*\backslash S),$$

and therefore S' is an $(n, m, k, \lambda + (m-1)\mu, m\mu)$-DPDF.

(ii) It follows by Lemma 1.2.4, Definition 1.3.11 and Definition 1.3.1 that when S' is an $(n, m, k, \lambda + (m-1)\mu, m\mu)$-DPDF and S is an (n, mk, η, ν)-PDS, this implies

$$(\lambda + (m-1)\mu)S \cup m\mu(\mathrm{G}^*\backslash S) \cup \mathrm{Ext}(S') = \eta(S) \cup \nu(\mathrm{G}^*\backslash S).$$

Notice that this expression is equivalent to

$$\mathrm{Ext}(S') = (\eta - (\lambda + (m-1)\mu))S \cup (\nu - m\mu)(\mathrm{G}^*\backslash S).$$

By Definition 1.3.12, the above equation implies that S' is also an $(n, m, k, \eta - (\lambda + (m-1)\mu), \nu - m\mu)$-EPDF.

□

Theorem 1.3.21. *Let G be a group of order n and let $S' = \{D_1, \dots, D_m\}$ be a collection of disjoint k-subsets, where each $D_i \in S'$ is an (n, k, λ, μ)-PDS. Moreover, suppose that $S = \cup_{i=1}^{m} D_i$. If*

(i) $\mathrm{G} \backslash S$ *is a PDS or*

(ii) $\mathrm{G}^* \backslash S$ *is a PDS (providing $0 \notin S$),*

then S' is a DPDF which is also an EPDF.

Proof. (i) It follows by Theorem 1.3.19 that when $\mathrm{G}\backslash S$ is a PDS (irrespective of whether $\mathrm{G}\backslash S$ is proper or regular) then its complement, S, is also a PDS. It then follows by Theorem 1.3.20 that since each $D_i \in S'$ is a PDS, and S' partitions the PDS S, that S' is both a DPDF and an EPDF.

(ii) The proof of this result is analogous to the proof of part (i). □

1.4 Cyclotomy in finite fields

Throughout the majority of this Thesis, I use a technique known as finite field cyclotomy to find new constructions of disjoint and external partial difference families, as well as other related combinatorial structures. The book [60], by Thomas Storer, is the earliest known source to explore the connections between between Difference Sets and cyclotomic classes since this book was written, cyclotomy has been used as a standard technique for developing constructions of various types of difference family (see [2],[34],[65],[66]).

Many cyclotomic constructions of difference families utilise formulas for computing the cyclotomic numbers of order e in a finite field of order q (see for example the constructions of a sub-classification of EDFs, known as SEDFs, in [2]) to take many of these results further, formulas for computing the cyclotomic numbers of order e in general finite fields of order q need to be extended to larger values of e. Generally speaking, identifying the cyclotomic numbers of order e in any finite field of order q is a hard problem to resolve, and is indeed a problem that has received a lot of attention since it was first approached by Gauss. In [60] Storer determines a formula for the cyclotomic numbers of order 2 and 3 also giving selective formulas for cyclotomic numbers of orders 4, 6 and 8, in [43] Emma Lehmer derives formulas for all cyclotomic numbers of order 8, and between the papers [25], [42] and [50] formulas for selective cyclotomic numbers of order up to $e = 12$ are detailed. In [5], the cyclotomic numbers were resolved for order up to 24 but we have not come across explicit cyclotomic number formulas in the literature for $e \geq 24$. Uniform cyclotomy can be used to determine cyclotomic numbers of order e in particular finite fields, even when e is greater than or equal to 22, but uniform cyclotomy is only applicable if e meets certain criteria. Due to the difficult nature of determining formulas for cyclotomic numbers of order e in general finite fields, a feature of Storer's work in [60] is seeking alternative methods for simplifying the computation of cyclotomic numbers. In this Thesis, I apply some Storer's techniques to identify cyclotomic constructions of disjoint and external partial difference families and I also develop some new techniques that may be used to evaluate cyclotomic numbers in certain cases.

In this Section, we use [60], [34] and [4], to set up a series of definitions and preliminary results which are later used to find cyclotomic constructions of disjoint and external difference families in later chapters. Before we cover these results, we must first cover some basic algebraic results.

The Fundamental Theorem of Finite Fields.

(1) There is a field with exactly q elements if and only if $q = p^s$ for a prime p and $s \geq 1$.

(2) Any two finite fields with the same cardinality are isomorphic.

(3) For any finite field $\mathbb{F}$ of order p^s, where p is prime

 (a) the additive group $(\mathbb{F}, +) \cong ((\mathbb{Z}_p)^s, +)$,

 (b) the multiplicative group $(\mathbb{F}^*, \cdot)$ is cyclic and a generator of the multiplicative subgroup is called a primitive element of $\mathbb{F}$.

Throughout this Thesis, we will use the notation $\mathrm{GF}(q)$ to denote the unique (up to isomorphism) finite field of order $q = p^s$.

The Fundamental Theorem for Cyclic Groups

(1) Every subgroup of a cyclic group is cyclic.

(2) In a finite cyclic group G of order n, if $\mathrm{H} \leq \mathrm{G}$ then the order of H divides n.

(3) For each $m \mid n$, there is exactly one cyclic subgroup $\mathrm{H} \leq \mathrm{G}$ of order m.

We can now define cyclotomic classes and cyclotomic numbers. In [60], Storer defines a cyclotomic class as follows:

Definition 1.4.1. *In a finite field* $\mathrm{GF}(q)$ *of order* $q = p^m = ef + 1$ *(where p is prime and $e, f \in \mathbb{N}$), we define the cyclotomic class of order e,* $C_i^{e,m}$, *in* $\mathrm{GF}(q)$ *to be the set:*

$$C_i^{e,m} = \alpha^i \langle \alpha^e \rangle,$$

where α is a primitive element of $\mathrm{GF}(q)$ *and $i \in \mathbb{Z}_e$. Notice that each cyclotomic class comprises f distinct elements.*

The reader should observe that the elements of each cyclotomic class of order e depend upon the primitive element chosen.

Example 1.4.2. *Note that $\alpha = 3$ and $\alpha = 6$ are two distinct primitive elements of the finite field* $\mathrm{GF}(17)$. *When $\alpha = 3$, the cyclotomic classes of order 4 in* $\mathrm{GF}(17)$ *are as follows*

$$\begin{aligned} C_0^{4,1} &= \{\alpha^0, \alpha^4, \alpha^8, \alpha^{12}\} = \{1, 13, 16, 4\} \\ C_1^{4,1} &= \{\alpha, \alpha^5, \alpha^9, \alpha^{13}\} = \{3, 5, 14, 12\} \\ C_2^{4,1} &= \{\alpha^2, \alpha^6, \alpha^{10}, \alpha^{14}\} = \{9, 15, 8, 2\} \\ C_3^{4,1} &= \{\alpha^3, \alpha^7, \alpha^{11}, \alpha^{15}\} = \{10, 11, 7, 6\}. \end{aligned}$$

When $\alpha = 6$, the cyclotomic classes of order 4 in $\mathrm{GF}(17)$ *are as follows*

$$\begin{aligned} C_0^{4,1} &= \{\alpha^0, \alpha^4, \alpha^8, \alpha^{12}\} = \{1, 4, 16, 13\} \\ C_1^{4,1} &= \{\alpha, \alpha^5, \alpha^9, \alpha^{13}\} = \{6, 7, 11, 10\} \\ C_2^{4,1} &= \{\alpha^2, \alpha^6, \alpha^{10}, \alpha^{14}\} = \{2, 8, 9, 15\} \\ C_3^{4,1} &= \{\alpha^3, \alpha^7, \alpha^{11}, \alpha^{15}\} = \{12, 14, 5, 3\}. \end{aligned}$$

Surprisingly, cyclotomic classes, which are in essence multiplicative structures, have some inherent additive properties. The study of finite field cyclotomy explores the additive relationships between elements contained within the same or distinct cyclotomic classes in the finite field $\mathrm{GF}(q)$. To understand these additive properties, we study the cyclotomic numbers of order e in a given finite field $\mathrm{GF}(q)$. The following definition of a cyclotomic number is again based on a definition given in [60]. Note that if $i_1 \equiv i_2 \bmod e$ and $j_1 \equiv j_2 \bmod e$ then the number of solutions for $\alpha^{es+i_1} + 1 = \alpha^{et+j_1}$ is the same as the number for $\alpha^{es+i_2} + 1 = \alpha^{et+j_2}$; for this reason we assume that i and j in the following definition lie in $\mathbb{Z}_e$.

Definition 1.4.3. *Let $\mathrm{GF}(q)$ be a finite field of order $q = p^m = ef + 1$ and let α be a primitive element of $\mathrm{GF}(q)$. For fixed integers $i, j \in \mathbb{Z}_e$, the **cyclotomic number** $(i,j)_e$ (of order e) is the number of ordered pairs (s,t) (where $0 \leq s, t \leq f-1$) such that*

$$\alpha^{es+i} + 1 = \alpha^{et+j},$$

where $\alpha^{es+i} \in C_i^{e,m}$ and $\alpha^{et+j} \in C_j^{e,m}$.

The reader should note here that there are two different ways of viewing the 2-tuple (i,j) which indexes the cyclotomic number $(i,j)_e$. One can either view i and j as element of $\mathbb{Z}_e$ or as two integers that lie in the following interval: $0 \leq i, j \leq e-1$. It is clear that these two viewpoints are analogous to one another, but we point this out as we will change the convention used across the various Sections and Chapters of this Thesis. In this Chapter, we will view $(i,j) \in \mathbb{Z}_e \times \mathbb{Z}_e$ and we will follow this same convention in Section 2 of Chapter 2, however in Section 1 of Chapter 2, Chapter 3 and Chapter 4, we will follow the convention that $0 \leq i, j \leq e-1$. Our reasoning for this is that in Chapter 1 and Section 2 of Chapter 2, we gain additional insight into certain proofs by viewing i and j as elements of the group $\mathbb{Z}_e$, whereas we follow the standard cyclotomic number convention in the other Sections. This is because the other Sections contain published material, and we keep the notation in these Sections in-line with the notation used in the original papers that these Sections are based upon.

The reader should also note that the cyclotomic numbers of order e depend upon the primitive element chosen as the generator for the cyclotomic class $C_0^{e,m}$. Whilst the cyclotomic numbers vary for different primitive elements, the cyclotomic numbers will always be equivalent up to isomorphism. We demonstrate this property with an example.

Example 1.4.4. *In Example 1.4.2, the elements of each of the cyclotomic classes of order* 4 *when* $\alpha = 3$ *are recorded. Notice that from the cyclotomic classes generated by* $\alpha = 3$*, we obtain the following sets (where the notation* $C_i^{e,m} - 1$ *denotes usual subtraction)*

$$\begin{aligned} C_0^{4,1} - 1 &= \{0, 12, 15, 3\} \\ C_1^{4,1} - 1 &= \{2, 4, 13, 11\} \\ C_2^{4,1} - 1 &= \{8, 14, 7, 1\} \\ C_3^{4,1} - 1 &= \{9, 10, 6, 5\}. \end{aligned}$$

From the above sets, we obtain that the cyclotomic numbers of order 4 *are as follows when* $\alpha = 3$*:* $(0,0)_4 = (3,0)_4 = (1,1)_4 = (0,3)_3 = 0$*,* $(2,0)_4 = (2,1)_4 = (3,1)_4 = (0,2)_4 = (1,2)_4 = (2,2)_4 = (3,2)_4 = (1,3)_4 = (2,3)_4 = 1$ *and* $(1,0)_4 = (0,1)_4 = (3,3)_4 = 2$.
By undergoing the same process with the cyclotomic classes of order 4 *generated by the primitive element* $\alpha = 6$ *in the finite field* $\mathrm{GF}(17)$*, we obtain the following cyclotomic numbers:* $(0,0)_4 = (1,0)_4 = (0,1)_4 = (3,3)_4 = 0$*,* $(2,0)_4 = (2,1)_4 = (0,2)_4 = (1,2)_4 = (2,2)_4 = (3,2)_4 = (3,1)_4 = (1,3)_4 = (2,3)_4 = 1$ *and* $(3,0)_4 = (1,1)_4 = (0,3)_4 = 2$.
This illustrates the well known fact (see page 24 *of [60]) that the cyclotomic numbers are determined up to choice of primitive element.*

We will now split the cyclotomic numbers into the following sub-classifications.

Definition 1.4.5. *For all* $i, j \in \mathbb{Z}_e$*, the cyclotomic numbers of the form* $(i,i)_e$*,* $(i,0)_e$ *and* $(0,i)_e$ *are referred to as **internal** cyclotomic numbers, and all cyclotomic numbers of the form* $(i,j)_e$*, where* $0 \neq i \neq j \neq 0$*, are referred to as **external** cyclotomic numbers.*

We require these sub-classifications because, as we see in a later Chapter on cyclotomic orbits, we can establish identities between collections of internal cyclotomic numbers and collections of external cyclotomic numbers. The following Definition and Theorem, first recorded in [4], demonstrate that in certain finite fields, we can in fact take this further, and demonstrate that internal (respectively external) cyclotomic numbers are equal to one another.

Definition 1.4.6. *The cyclotomic numbers in* $\mathrm{GF}(q)$ *are said to be* ***uniform*** *if* $(i,i)_e = (i,0)_e = (0,i)_e = (1,1)_e$ *for all* $i \in \mathbb{Z}_e$ *(the internal cyclotomic numbers have the same value) and if* $(i,j)_e = (1,2)_e$ *for all* $i \neq j \in \mathbb{Z}_e$ *(the external cyclotomic numbers have the same value).*

Theorem 1.4.7. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^r = ef + 1$*, where* p *is prime and* $e \geq 3$*. The cyclotomic numbers of order* e *are uniform if and only if* -1 *is a power of* p *modulo* e*. When the cyclotomic numbers are uniform either* p *is odd and* f *is even or* $p = 2$*. Moreover, when the cyclotomic numbers are uniform* $q = s^2$*, where* $s \equiv 1 \mod e$*, and we may express the cyclotomic numbers of order* e *as follows*

$$\begin{aligned}(0,0)_e &= \left(\frac{s-1}{e}\right)^2 - (e-3)\left(\frac{s-1}{e}\right) - 1,\\ (0,i)_e = (i,0)_e = (i,i)_e &= \left(\frac{s-1}{e}\right)^2 + \left(\frac{s-1}{e}\right) \text{ for } i \neq 0,\\ (i,j)_e &= \left(\frac{s-1}{e}\right)^2 \text{ for } 0 \neq i \neq j.\end{aligned}$$

Example 1.4.8. *In the finite field* $\mathrm{GF}(9)$*, let* $e = 4$ *and observe that* $p = 3$*. Notice that* $3 \equiv -1 \mod 4$*, and moreover* $f = \frac{9-1}{4} = 2$ *is even. It therefore follows that the cyclotomic numbers of order* 4 *are uniform in* $\mathrm{GF}(9)$*. Observe that* $s = -3$ *satisfies both* $s \equiv 1 \mod 4$ *and* $s^2 = 9$*. It follows from Theorem 1.4.7 that as* $s = -3$ *when* $e = 4$*, this means* $(0,0)_4 = 1$*,* $(i,0)_4 = (i,i)_4 = (0,i)_4 = 0$ *for all* $1 \leq i \leq 3$ *and* $(i,j)_4 = 1$ *for all* $1 \leq i \neq j \leq 3$*.*

To verify this, observe that in $\mathrm{GF}(9)$*,* $C_0^{4,2} = \{1,2\}$*. By definition,* $(0,0)_4$ *is the number of elements in* $\alpha^{4s} \in C_0^{4,2}$ $(1 \leq s \leq 2)$ *such that* $\alpha^{4s} - 1 \in C_0^{4,2}$ *and the cyclotomic number* $(0,i)_e$ *is the number of elements in* $\alpha^{4s} \in C_0^{4,2}$ $(1 \leq s \leq 2)$ *such that* $\alpha^{4s} - 1 \in C_i^{4,2}$ $(1 \leq i \leq 3)$*. Since* $2 - 1 = 1$*, we can directly compute* $(0,0)_4 = 1$ *and* $(0,i)_e = 0$*. We can similarly verify the other cyclotomic numbers of order* 4 *in the finite field* $\mathrm{GF}(9)$ *by directly computing the elements of each cyclotomic class. This is left to the reader.*

We return to the notions of internal/external cyclotomic numbers in later Chapters to establish cyclotomic constructions of DPDFs and EPDFs.

In the remainder of this Section, we establish identities between individual cyclotomic numbers. Before we present these identities, we must first define the Frobenius automorphism: a well-known endomorphism of finite fields of characteristic p, which is an automorphism when the field is finite (see [64] for further details).

Definition 1.4.9. *Let* $\mathrm{GF}(q)$ *be a finite field of characteristic* p*. The Frobenius automorphism* $\phi : \mathrm{GF}(q) \to \mathrm{GF}(q)$ *is defined by* $\phi(\omega) = \omega^p$*, for every* $\omega \in \mathrm{GF}(q)$*.*

We also require the following Lemma (often referred to as Freshman's Exponentiation Lemma) to derive later results in this chapter. For a proof of the following result, see [64].

Lemma 1.4.10. *Let* $\mathrm{GF}(q)$ *be a finite field of characteristic* p*. For any elements* $a, b \in \mathrm{GF}(q)$*,* $(a + b)^p = a^p + b^p$*.*

Finally, we require the following Lemma, originally proven by Storer in [60].

Lemma 1.4.11. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^m = ef + 1$*, where* p *is prime and* $m \in \mathbb{N}$*. Moreover, for each* $i \in \mathbb{Z}_e$*, let* $C_i^{e,m} = \alpha^i \langle \alpha^e \rangle$*, where* α *is a primitive element of* $\mathrm{GF}(q)$*. When*

(i) e *and* f *are both odd,* $-1 \in C_0^{e,m}$*,*

(ii) f *is even,* $-1 \in C_0^{e,m}$*,*

(iii) e *is even and* f *is odd,* $-1 \in C_{\frac{e}{2}}^{e,m}$*.*

Proof. (i) When e and f are both odd, this implies that $q = p^m = ef + 1$ is even, meaning that $p = 2$. When $p = 2$, $1 \equiv -1 \mod p$.

(ii) When f is even, $q = p^m = ef + 1$ is odd, meaning $p \neq 2$. As a consequence of Lagrange's Theorem, $\alpha^{\frac{ef}{2}} = -1$. When f is even, $\frac{f}{2}$ is an integer, hence $\alpha^{e\frac{f}{2}} = -1 \in C_0^{e,m}$.

(iii) As in part (ii), when e is even and f is odd, $q - 1 = ef$ is even and so $\alpha^{\frac{ef}{2}} = -1 \in \mathrm{GF}(q)$. When f is odd, $\frac{f}{2}$ is not an integer, but $\frac{e}{2}$ is an integer. Observe that we may write $\alpha^{f\frac{e}{2}} = \alpha^{(f-1)\frac{e}{2}+\frac{e}{2}} = \alpha^{\frac{(f-1)}{2}e+\frac{e}{2}} = -1$, since we have expressed -1 as a power of the form $\alpha^{se+\frac{e}{2}}$, where $0 \leq s = \frac{f-1}{2} \leq f-1$, it is clear that $-1 \in C_{\frac{e}{2}}^{e,m}$. □

With the preliminary results and definitions outlined, we are now able to prove all known identities between cyclotomic numbers. The following Theorem is based on the cyclotomic number identities introduced in [60] and [65] and also includes a new result in part (e) on the summation of all cyclotomic numbers with $i = j$.

Theorem 1.4.12. *Let $q = p^m$, where $m \geq 1$, p is prime and $q - 1 = ef$ ($e \geq 2$). Let $(i, j)_e$ be the cyclotomic numbers of order e in $\mathrm{GF}(q)$, then*

(a) $(i, j)_e = (e - i, j - i)_e$,

(b) $(i, j)_e = (ip, jp)_e$,

(c) suppose p is a prime, then

$$(i, j)_e = \begin{cases} (j, i)_e, \text{ if } p = 2 \text{ or } f \text{ is even} \\ (j + \frac{e}{2}, i + \frac{e}{2})_e, \text{ if } f \text{ is odd,} \end{cases}$$

(d) *(i) when either $p = 2$ or f is even,*

$$\sum_{i=0}^{e-1} (i, 0)_e = \sum_{i=0}^{e-1} (0, i)_e = \sum_{i=0}^{e-1} (e - i, e - i)_e = f - 1,$$

(ii) when e is even and f is odd,

$$\sum_{i=0}^{e-1} (i, 0)_e = \sum_{i=0}^{e-1} (\frac{e}{2}, i)_e = \sum_{i=0}^{e-1} (e - i, e - i)_e = f - 1,$$

(e) *(i) for any $j \neq 0 \in \mathbb{Z}_e$, $\sum_{i=0}^{e-1} (i, j)_e = f$,*

(ii) when either $p = 2$ or f is even, for any $i \neq 0 \in \mathbb{Z}_e$, $\sum_{j=0}^{e-1} (i, j)_e = f$,

(iii) when e is even and f is odd, for any $i \neq \frac{e}{2} \in \mathbb{Z}_e$, $\sum_{j=0}^{e-1} (i, j)_e = f$.

Proof. By Definition 1.4.3, for all $i, j \in \mathbb{Z}_e$ the cyclotomic number $(i, j)_e$ is precisely the number of solutions $(s, t) \in \mathbb{Z}_f \times \mathbb{Z}_f$ to the following equation

$$\alpha^{se+i} + 1 = \alpha^{te+j}. \tag{1.1}$$

Analogously, for all $I, J \in \mathbb{Z}_e$, the cyclotomic number $(I, J)_e$ is precisely the number of solutions $(s', t') \in \mathbb{Z}_f \times \mathbb{Z}_f$ to the following equation

$$\alpha^{s'e+I} + 1 = \alpha^{t'e+J}. \tag{1.2}$$

In subsequent parts of this proof, we aim to establish a bijection between the solution sets of (1.1) and (1.2). This will demonstrate the solution sets have the same size and thus $(i,j)_e = (I,J)_e$ for appropriate $I, J \in \mathbb{Z}_e$.

(a) Let $I = e - i$ and $J = j - i$. We define a mapping $g : \mathbb{Z}_f \times \mathbb{Z}_f \to \mathbb{Z}_f \times \mathbb{Z}_f$ by $g(s,t) = (f-1-s, t-s)$. We will prove that $g : \mathbb{Z}_f \times \mathbb{Z}_f \to \mathbb{Z}_f \times \mathbb{Z}_f$ is a bijection, show that g maps solutions of (1.1) to solutions of (1.2) and demonstrate that g^{-1} maps solutions of (1.2) to solutions of (1.1).
We begin this process by demonstrating that g is an injective mapping. Let $s_1, s_2, t_1, t_2 \in \mathbb{Z}_f$ and suppose that $g(s_1,t_1) = g(s_2,t_2)$, it then follows from the definition of g that the following equations must hold

$$f - 1 - s_1 = f - 1 - s_2, \tag{1.3}$$
$$t_1 - s_1 = t_2 - s_2. \tag{1.4}$$

It is immediate from (1.3) that $s_1 = s_2$ and it then naturally follows from (1.4) that $t_1 = t_2$. We can therefore conclude that g is an injective mapping and hence a surjective mapping as set sizes are equal. We now determine the inverse of g. Suppose that $(X,Y) \in \mathbb{Z}_f \times \mathbb{Z}_f$; we now find $(x,y) \in \mathbb{Z}_f \times \mathbb{Z}_f$ such that $g(x,y) = (X,Y)$. If we assume that $g(x,y) = (X,Y)$, then this requires $(X,Y) = (f-x-1, y-x)$, which would mean that $X = f-1-x$ and $Y = y-x$, hence we may then write $x = f-1-X$ and $y = Y + x = f-1-X+Y$.
By applying g^{-1} to (X,Y) we obtain

$$g^{-1}(X,Y) = (x,y) = (f-1-X, f-1-X+Y).$$

We now demonstrate that g maps every solution (s,t) of (1.1) to a solution $g(s,t)$ of (1.2). Suppose that $(s,t) \in \mathbb{Z}_f \times \mathbb{Z}_f$ belongs to solution set of (1.1), it then follows that

$$\alpha^{se+i} + 1 = \alpha^{te+j}.$$

By multiplying this equation by $\alpha^{(f-1-s)e+(e-i)}$ (the inverse of α^{se+i}) we obtain

$$\alpha^{se+i+fe-e-se+e-i} + \alpha^{(f-1-s)e+(e-i)} = \alpha^{te+j+fe-e-se+e-i}.$$

Since $\alpha^{fe} = 1$ by Lagrange's Theorem, it follows that

$$1 + \alpha^{(f-1-s)e+(e-i)} = \alpha^{(t-s)e+(j-i)}.$$

Since g is a bijective mapping, every solution (s, t) in the solution set of (1.1) corresponds to a solution $g(s, t) = (f - 1 - s, t - s)$ of (1.2).
We now demonstrate that g^{-1} maps a solution of (1.2) to a solution of (1.1). Suppose that (s', t') is in the solution set of (1.2), then this implies that

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

By multiplying this equation by $\alpha^{(f-1-s')e+i}$

$$\alpha^{s'e+e-i+fe-e+s'+i} + \alpha^{(f-1-s')e+i} = \alpha^{t'e+j-i+fe-e-s'e+i},$$
$$1 + \alpha^{(f-1-s')e+i} = \alpha^{(f-1-s'+t')e+j}.$$

It is then immediate that g^{-1} maps each solution (s', t') in the solution set of (1.2) to a solution $g^{-1}(s', t') = (f - 1 - s', f - 1 - s' + t')$ of (1.1).

(b) This is immediate by properties of the Frobenius automorphism (see Definition 1.4.9 and Lemma 1.4.10).

(c) By Lemma 1.4.11, $1 = -1$ when $p = 2$, thus

$$\alpha^{se+i} + 1 = \alpha^{te+j} \Leftrightarrow \alpha^{te+j} + 1 = \alpha^{se+i}.$$

It then immediately follows from Definition 1.4.3 that when $p = 2$, $(i, j)_e = (j, i)_e$. When p is an odd prime the situation is more complicated. In what follows, we will tackle the cases for f even and f odd when p is an odd prime. To do this, we will establish two bijections h_1 and h_2 and demonstrate that these bijections map solutions of (1.1) onto solutions of (1.2) in the case where f is even and f is odd respectively.

When f is even, we define a bijection h_1 between the solution set of (1.1) and the solution set of (1.2). In this instance, suppose $I = j$ and $J = i$. We define the mapping $h_1 : \mathbb{Z}_f \times \mathbb{Z}_f \to \mathbb{Z}_f \times \mathbb{Z}_f$ by $h_1(s,t) = (t + \frac{f}{2}, s + \frac{f}{2})$. We will prove that $h_1 : \mathbb{Z}_f \times \mathbb{Z}_f \to \mathbb{Z}_f \times \mathbb{Z}_f$ is a bijection, show that h_1 maps solutions of (1.1) to solutions of (1.2) and demonstrate that h_1^{-1} maps solutions of (1.2) to solutions of (1.1).

We begin this process by demonstrating that h_1 is an injective mapping. Let $s_1, s_2, t_1, t_2 \in \mathbb{Z}_f$ and suppose that $h_1(s_1, t_1) = h_1(s_2, t_2)$, it then follows from the definition of h_1 that the following equations must hold

$$t_1 + \frac{f}{2} = t_2 + \frac{f}{2}, \tag{1.5}$$

$$s_1 + \frac{f}{2} = s_2 + \frac{f}{2}. \tag{1.6}$$

It is immediate from (1.5) that $t_1 = t_2$ and it is similarly immediate from (1.6) that $s_1 = s_2$. We can therefore conclude that $h_1 : \mathbb{Z}_f \times \mathbb{Z}_f \to \mathbb{Z}_f \times \mathbb{Z}_f$ is an injective mapping, and hence a surjective mapping, since set sizes are equal.

We next determine h_1^{-1}. Suppose $(X, Y) \in \mathbb{Z}_f \times \mathbb{Z}_f$; we find $(x, y) \in \mathbb{Z}_f \times \mathbb{Z}_f$ such that $h_1(x, y) = (X, Y)$. If we assume that $h_1(x, y) = (X, Y)$ then this implies that $(X, Y) = (y + \frac{f}{2}, x + \frac{f}{2})$, meaning $x = Y - \frac{f}{2}$ and $Y = X - \frac{f}{2}$. By applying h^{-1} to (X, Y) we obtain

$$h^{-1}(X, Y) = (x, y) = (Y - \frac{f}{2}, X - \frac{f}{2}).$$

We will now demonstrate that when $I = j$, $J = i$ and f is even, the bijection h_1 guarentees that we can map every solution in the solution set of (1.1) to a solution in the solution set of (1.2). Suppose that $(s, t) \in \mathbb{Z}_f \times \mathbb{Z}_f$ belongs to the solution set of (1.1), it then follows that

$$\alpha^{se+i} + 1 = \alpha^{te+j}.$$

We will now multiply both sides of this equation by the element $-1 \in \mathrm{GF}(q)^*$. Notice that since we are in the case where f is even, $-1 = \alpha^{\frac{ef}{2}} = \alpha^{e\frac{f}{2}}$, hence when we multiply each term of the above expression by -1, we obtain

$$\alpha^{se+i+e\frac{f}{2}} - 1 = \alpha^{te+j+e\frac{f}{2}}.$$

By rearranging this equation, we obtain

$$\alpha^{(t+\frac{f}{2})e+j} + 1 = \alpha^{(s+\frac{f}{2})e+i}.$$

As h_1 is a bijective mapping, every solution (s, t) in the solution set of (1.1) corresponds to precisely one solution $h_1(s, t) = (t + \frac{f}{2}, s + \frac{f}{2})$ in the solution set of (1.2).

We will now demonstrate that h_1^{-1} maps every solution of (1.2) to a solution in the solution set of (1.1). Suppose that $(s', t') \in \mathbb{Z}_f \times \mathbb{Z}_f$ in the solution set of (1.2), then this implies that

$$\alpha^{s'e+j} + 1 = \alpha^{t'e+i}.$$

We will now multiply the equation through by -1. As above, since we are assuming f is even, this means that $-1 = \alpha^{e\frac{f}{2}}$. We therefore obtain the following equation when we multiply this equation by -1

$$\alpha^{(s'+\frac{f}{2})e+j} - 1 = \alpha^{(t'+\frac{f}{2})e+i}.$$

We can then rearrange this equation to give

$$\alpha^{(t'+\frac{f}{2})e+i} = \alpha^{(s'+\frac{f}{2})e+i} + 1.$$

Since h_1 is a bijection, h_1^{-1} maps every solution $(s', t') \in \mathbb{Z}_f \times \mathbb{Z}_f$ of (1.2) to a solution $h_1^{-1}(s', t') = (t' - \frac{f}{2}, s' - \frac{f}{2})$ of (1.1), so the solution sets must have the same size and therefore $(i, j)_e = (j, i)_e$ when f is even.

We now define a bijection $h_2 : \mathbb{Z}_f \times \mathbb{Z}_f \to \mathbb{Z}_f \times \mathbb{Z}_f$ by $h_2(s, t) = (t + \frac{f-1}{2}, s + \frac{f-1}{2})$. Owing to the similarities between the mappings h_1 and h_2, we will leave it up to the reader to prove for themselves that h_2 is a bijection, but we will note that the inverse mapping $h_2^{-1} : \mathbb{Z}_f \times \mathbb{Z}_f \to \mathbb{Z}_f \times \mathbb{Z}_f$ is defined by $h_2^{-1}(X, Y) = (x, y) = (Y - \frac{f-1}{2}, X - \frac{f-1}{2})$ for any two pairs $(X, Y) \in \mathbb{Z}_f \times \mathbb{Z}_f$ in the solution set of (1.2) and any $(x, y) \in \mathbb{Z}_f \times \mathbb{Z}_f$ in the solution set of

(1.1).

We will now prove, using the bijection h_2, that when $I = j + \frac{e}{2}$, $J = i + \frac{e}{2}$ and f is odd, every solution in the solution set (1.1) maps to precisely one solution in the solution set (1.2). To see this, suppose $(s,t) \in \mathbb{Z}_f \times \mathbb{Z}_f$ is in the solution set of (1.1). It then follows that $(s,t) \in \mathbb{Z}_f \times \mathbb{Z}_f$ satisfy

$$\alpha^{se+i} + 1 = \alpha^{te+j}.$$

We will now multiply the terms of this equation through by -1. As f is odd in this instance, we can write $-1 = \alpha^{\frac{ef}{2}} = \alpha^{e\frac{f-1}{2}+\frac{e}{2}}$. We therefore obtain the following equation when we multiply each term of the above equation by -1

$$\alpha^{(s+\frac{f-1}{2})e+(i+\frac{f}{2})} - 1 = \alpha^{(t+\frac{f-1}{2})e+(j+\frac{f}{2})}.$$

Which we can then rearrange to

$$\alpha^{(t+\frac{f-1}{2})e+(j+\frac{f}{2})} + 1 = \alpha^{(s+\frac{f-1}{2})e+(i+\frac{f}{2})}.$$

As h_2 is a bijection, every solution of $(s,t) \in \mathbb{Z}_f \times \mathbb{Z}_f$ in the solution set of (1.1) maps to precisely one solution $h(s,t) = (t + \frac{f-1}{2}, s + \frac{f-1}{2})$ in the solution set of (1.2).

Finally, we will demonstrate that h_2^{-1} maps every solution $(s',t') \in \mathbb{Z}_f \times \mathbb{Z}_f$ in the solution set of (1.2) to a solution in the solution set of (1.1) in the case where f is odd. Suppose $(s',t') \in \mathbb{Z}_f \times \mathbb{Z}_f$ is in the solution set of (1.2), then

$$\alpha^{s'e+(j+\frac{e}{2})} + 1 = \alpha^{t'e+(i+\frac{e}{2})}.$$

We will now multiply each term of this equation through by -1. As above, since f is odd, we may write $-1 = \alpha^{e\frac{f-1}{2}+\frac{e}{2}}$. Multiplying each term of the above equation through by -1 therefore yields

$$\alpha^{(s'+\frac{f-1}{2})e+j} - 1 = \alpha^{(t'+\frac{f-1}{2})e+i},$$

which can be rewritten as

$$\alpha^{(t'+\frac{f-1}{2})e+i} + 1 = \alpha^{(s'+\frac{f-1}{2})e+j}.$$

As h_2 is a bijection, h_2^{-1} maps every solution $(s',t') \in \mathbb{Z}_f \times \mathbb{Z}_f$ of (1.2) to a solution $h_2^{-1}(s',t') = (t' - \frac{f-1}{2}, s' - \frac{f-1}{2})$ of (1.1), so the solution sets of (1.1) and (1.2) must be of the same size, and therefore $(i,j)_e = (j + \frac{e}{2}, i + \frac{e}{2})_e$ when f is odd.

(d) By Definition 1.4.3, the cyclotomic number $(i,0)_e$ denotes the number of pairs $(s,t) \in \mathbb{Z}_f \times \mathbb{Z}_f$, such that:

$$\alpha^{se+i} + 1 = \alpha^{te}.$$

This can be rewritten as:

$$\alpha^{se+i} = \alpha^{te} - 1,$$

or the number of elements of $C_i^{e,m}$ (where $i \in \mathbb{Z}_e$) that be expressed as an element of the set $C_0^{e,m} - 1 = \{\alpha^{te} - 1 \,|\, t \in \mathbb{Z}_f\}$. This means that $\sum_{i=0}^{e-1}(i,0)_e$ is the number of elements in $C_0^{e,m} - 1$ that are contained in some cyclotomic class $C_i^{e,m}$ for $i \in \mathbb{Z}_e$.
There are precisely f distinct elements in the cyclotomic class $C_0^{e,m} = \langle \alpha^e \rangle$. As the element $1 \in C_0^{e,m}$ (since $1 = \alpha^{ef}$), this means that $0 \in C_0^{e,m} - 1$. Since the element 0 is the only element of $\mathrm{GF}(q)$ not contained within one of the cyclotomic classes of order e, this means that precisely $f-1$ elements of the set $C_0^{e,m} - 1$ can be expressed as an element of one of the cyclotomic classes of order e. Therefore $\sum_{i=0}^{e-1}(i,0)_e = f - 1$.
Moreover it follows from part a) that for every $i \in \mathbb{Z}_e$, $(i,0)_e = (e-i, e-i)_e$, therefore $\sum_{i=0}^{e-1}(e-i,e-i)_e = f-1$. Notice that by part (b) $(i,0)_e = (ip,0)_e$, however the sum $\sum_{i=0}^{e-1}(ip,0)_e$ counts the same cyclotomic numbers as the sum $\sum_{i=0}^{e-1}(i,0)_e$ since $i, ip \in \mathbb{Z}_e$, so no new information is gained from this identity.

(i) When either e and f are both odd or when f is even it follows from part (c) $(i,0)_e = (0,i)_e$ for all $i \in \mathbb{Z}_e$, which implies that $\sum_{i=0}^{e-1}(0,i)_e = f-1$.

(ii) When e is even and f is odd by part (c) $(i,0)_e = (\frac{e}{2}, i + \frac{e}{2})_e$, hence $\sum_{i=0}^{e-1}(\frac{e}{2}, i + \frac{e}{2})_e = f - 1$. Observe that by part a), $(\frac{e}{2}, i + \frac{e}{2})_e = (\frac{e}{2}, i)_e$, however as $i, \frac{e}{2}, i + \frac{e}{2} \in \mathbb{Z}_e$, the sums $\sum_{i=0}^{e-1}(\frac{e}{2}, i + \frac{e}{2})_e$ and $\sum_{i=0}^{e-1}(\frac{e}{2}, i)_e$

count the same cyclotomic numbers, so no new information is gained from this identity.

(e) (i) By Definition 1.4.3 the cyclotomic number $(i,j)_e$ is the number of pairs $(s,t) \in \mathbb{Z}_f \times \mathbb{Z}_f$ such that:

$$\alpha^{se+i} = \alpha^{te+j} - 1.$$

In other words, $\sum_{i=0}^{e-1}(i,j)_e$ is the number of elements in $C_j^{e,m} - 1 = \{\alpha^{te+j} - 1 \,|\, t \in \mathbb{Z}_f\}$ that lie in some cyclotomic class $C_i^{e,m}$, where $i \in \mathbb{Z}_e$. Note that for each $i \in \mathbb{Z}_e$ and $j \in \mathbb{Z}_e^*$, the cyclotomic classes $C_i^{e,m}$ and $C_j^{e,m}$ consist of f distinct elements of $\mathrm{GF}(q)^*$. As in part (d), for a fixed $j \in \mathbb{Z}_e^*$, we can therefore think of $\sum_{i=0}^{e-1}(i,j)$ as being the number of non-zero elements of $\mathrm{GF}(q)$ contained within the set $C_j^{e,m} - 1$. As $j \in \mathbb{Z}_e^*$ (i.e. $j \neq 0$) this means that $1 \notin C_j^{e,m}$, and therefore $0 \notin C_j^{e,m} - 1$. This means all f of the elements in $C_j^{e,m} - 1$ are non-zero element of $\mathrm{GF}(q)$, and therefore $\sum_{i=0}^{e-1}(i,j) = f$.

(ii) As above, by Definition 1.4.3 the cyclotomic number $(i,j)_e$ is the number of pairs $(s,t) \in \mathbb{Z}_f \times \mathbb{Z}_f$ such that:

$$\alpha^{se+i} = \alpha^{te+j} - 1.$$

It follows from this that $\sum_{j=0}^{e-1}(i,j)_e$ counts the number of elements $\alpha^{te+j} \in \cup_{j=0}^{e-1} C_j^{e,m} = \mathrm{GF}(q)^*$ satisfying $\alpha^{se+i} + 1 = \alpha^{te+j}$, where $\alpha^{se+i} \in C_i^{e,m}$. In other words, $\sum_{j=0}^{e-1}(i,j)_e$ is the equivalent to the number of elements in the intersection $C_i^{e,m} \cap (\mathrm{GF}(q)^* \backslash \{-1\})$, where $\mathrm{GF}(q)^* \backslash \{-1\} = \{\alpha^{te+j} - 1 \,|\, j \in \mathbb{Z}_e,\, t \in \mathbb{Z}_f\}$. By Lemma 1.4.11, when either e and f are both odd or when f is even, $-1 \in C_0^{e,m}$, meaning that for all $i \in \mathbb{Z}_e$, $|C_i^{e,m} \cap (\mathrm{GF}(q)^* \backslash \{-1\})| = f$ and so $\sum_{j=0}^{e-1}(i,j)_e = f$ for all $i \in \mathbb{Z}_e$.

(iii) By Lemma 1.4.11 when e is even and f is odd, $-1 \in C_{\frac{e}{2}}^{e,m}$. This means that when $i \neq \frac{e}{2} \in \mathbb{Z}_e$, $|C_i^{e,m} \cap (\mathrm{GF}(q) \backslash \{-1\})| = f$. By part (e)(ii) it follows that $\sum_{j=0}^{e-1}(i,j)_e = f$ for all $i \neq \frac{e}{2} \in \mathbb{Z}_e$. □

Chapter 2

Cyclotomic frameworks

In this Chapter, we establish two new cyclotomic frameworks that can be deployed in different ways to find new constructions of difference families, as well as being of independent interest. In the beginning of this Chapter, we present the cyclotomic framework established in [34], that combines the partition results introduced in Chapter 1 and finite field cyclotomy to obtain new cyclotomic techniques that can be used to construct PDSs, DPDFs and EPDFs. The paper [34] is a joint paper with my supervisor Dr Sophie Huczynska. The key ideas of the paper were mine but I worked closely with my supervisor to refine and express these ideas. In Chapter 4 we will demonstrate how these techniques can be used to find new cyclotomic constructions of PDSs, DPDFs and EPDFs.

In the second half of this Chapter, we outline a framework for determining of cyclotomic orbits of order e for a particular finite field $\mathrm{GF}(q)$. In Chapter 4, it is demonstrated that this framework can be used to establish a more sophisticated algorithm for computing the internal cyclotomic numbers of order e, where $e \geq 5$ is prime and f is even (for further details see Algorithm 2 in Chapter 4). The results in Section 2 of this Chapter are new results that I obtained myself whilst developing the algorithms in Chapter 4: working on these algorithms highlighted the necessity of idenitfying the equivalent cyclotomic numbers in a given finite field.

2.1 Key cyclotomic number framework

2.1.1 Internal differences

Throughout this Subsection, it is assumed that q is a prime power and can be expressed by $q = p^s = ef+1$, where p is prime, $s \in \mathbb{N}$ and e, f are integers greater than 1, unless otherwise stated. We also use the notation $C_i^{e,s}$ to denote the i^{th} cyclotomic class of order e in the finite field $\mathrm{GF}(q)$. Finally, it is assumed for all results that α is a primitive element of $\mathrm{GF}(q)$. All results in this Subsection are included in my joint paper with my supervisor [34].

In this Subsection, we establish tools for determining the elements contained within each multiset of the form $\Delta(C_i^{e,s})$, where $C_i^{e,s}$ is a cyclotomic class. We begin this subsection with stating the definition of a transversal of the multiset $\Delta(C_i^{e,s})$.

Definition 2.1.1. *(i) For each $1 \leq r \leq f-1$, we define*

$$T_r := \{\alpha^{ne} - \alpha^{me} : n - m \equiv r \bmod f,\ 0 \leq n \neq m \leq f-1\}.$$

*Notice that $T_r \subseteq \Delta(C_0^{e,s})$ (as defined in Chapter 1). We refer to T_r as a **transversal** of $\Delta(C_0^{e,s})$ (these are also simply referred to as transversals throughout this Thesis). Each transversal T_r is simply a cyclotomic class of order e, therefore $|T_r| = f$ (see Lemma 2.1.2 below).*

(ii) For each $1 \leq r \leq f-1$, let $a_r \in \{0, \dots, e-1\}$ be such that $\alpha^{re} - 1 \in C_{a_r}^{e,s}$.

The following Lemma demonstrates how transversals can be used to split the multiset $\Delta(C_i^{e,s})$ up into a series of cyclotomic classes, since each transversal is effectively a copy of the cyclotomic class $C_{a_r}^{e,s}$, where $a_r \in \{0, 1, \dots, e-1\}$.

Lemma 2.1.2. *(i) For $1 \leq r \leq f-1$, $T_r \subseteq \Delta(C_0^{e,s})$. We may write the set T_r as follows: $T_r = (\alpha^{re}-1)C_0^{e,s} = C_{a_r}^{e,s}$.*

(ii) $\Delta(C_0^{e,s}) = \bigcup_{r=1}^{f-1} T_r = \bigcup_{r=1}^{f-1} C_{a_r}^{e,s} = \bigcup_{i=0}^{e-1} (i,0)_e C_i^{e,s}$.

(iii) For $0 \leq j \leq e-1$, $\Delta(C_j^{e,s}) = \alpha^j \Delta(C_0^{e,s}) = \bigcup_{p=1}^{f-1} \alpha^j T_r = \bigcup_{i=0}^{e-1} (i-j,0)_e C_i^{e,s}$.

Proof. (i) It follows from Definition 2.1.1 (i) that for each $1 \leq r \leq e-1$

$$T_r = \{\alpha^{ne} - \alpha^{me} : 0 \leq m \leq f-1\}.$$

Note that since $0 \leq n \neq m \leq f-1$, we may write $n \equiv m + r \mod f$. We may then write

$$T_r = \{\alpha^{(m+r)e} - \alpha^{me} : 0 \leq m \leq f-1\} = \{\alpha^{me}(\alpha^{re} - 1) : 0 \leq m \leq f-1\}$$
$$= (\alpha^{re} - 1)C_0^{e,s}.$$

By Definition 2.1.1 (ii), this means $T_r = C_{a_r}^{e,s}$.

(ii) By Definition 1.4.3, for $0 \leq j \leq e-1$, the elements of the cyclotomic class $C_j^{e,s}$ can be written in the form α^{et+j}, where α is a primitive element of $\mathrm{GF}(q)$ and $0 \leq t \leq f-1$. This means that $\Delta(C_0^{e,s}) = \{\alpha^{ne} - \alpha^{me} : 0 \leq n \neq m \leq f-1\}$. Since for each pair $0 \leq n \neq m \leq f-1$, there is a unique up to modulo f value of $1 \leq r \leq f-1$ such that $n \equiv m + r \mod f$, we may rewrite this multiset as

$$\Delta(C_0^{e,s}) = \{\alpha^{(m+r)e} - \alpha^{me} : 1 \leq r \leq f-1, 0 \leq m \leq f-1\}$$
$$= \bigcup_{r=1}^{f-1} \{\alpha^{(m+r)e} - \alpha^{me} : 0 \leq m \leq f-1\} = \bigcup_{r=1}^{f-1} T_r = \bigcup_{r=1}^{f-1} (\alpha^{re} - 1)C_0^{e,s}$$

by part (i). By Definition 1.4.3, for each $0 \leq i \leq e-1$ there are precisely $(i,0)_e$ values of $1 \leq r \leq f-1$ such that $\alpha^{re} - 1 \in C_i^{e,s}$. This means that for $0 \leq i \leq e-1$ the cyclotomic class $C_i^{e,s}$ occurs $(i,0)_e$ times in the multiset union $\Delta(C_0^{e,s}) = \bigcup_{r=1}^{f-1} (\alpha^{re} - 1)C_0^{e,s}$, hence

$$\Delta(C_0^{e,s}) = \bigcup_{r=1}^{f-1} (\alpha^{re} - 1)C_0^{e,s} = \bigcup_{r=1}^{f-1} C_{a_r}^{e,s} = \bigcup_{i=0}^{e-1} (i,0)_e C_i^{e,s}.$$

(iii) As in part (ii), we can use Definition 1.4.3 to write the elements of the multiset $\Delta(C_j^{e,s})$ as follows

$$\begin{aligned}\Delta(C_j^{e,s}) &= \{\alpha^{en+j} - \alpha^{me+j} : 0 \leq n \neq m \leq f-1\} \\ &= \{\alpha^j(\alpha^{en} - \alpha^{me}) : 0 \leq n \neq m \leq f-1\} \\ &= \alpha^j \Delta(C_0^{e,s}).\end{aligned}$$

It then follows by part (ii) that

$$\Delta(C_j^{e,s}) = \alpha^j \Delta(C_0^{e,s}) = \bigcup_{p=1}^{f-1} \alpha^j(T_r) = \bigcup_{r=1}^{f-1} \alpha^j(C_{a_r}^{e,s}) = \bigcup_{i=0}^{e-1} (i,0)_e(\alpha^j C_i^{e,s}).$$

Notice that we may rewrite

$$\bigcup_{i=0}^{e-1} (i,0)_e(\alpha^j C_i^{e,s}) = \bigcup_{i=0}^{e-1} (i,0)_e(C_{i+j}^{e,s}) = \bigcup_{i=0}^{e-1} (i-j,0)_e(C_i^{e,s}). \qquad \square$$

Using the above result, we are able to show that if the cyclotomic numbers of order e meet certain conditions (i.e. all cyclotomic numbers of the form $(a,0)_e$ where $1 \leq a \leq e-1$ are equal) then each multiset of the form $\Delta(C_j^{e,s})$ (where $0 \leq j \leq e-1$) is automatically a PDS. Moreover, any collection, S', of distinct cyclotomic classes satisfying the above property will be a DPDF. We demonstrate this in the following result.

Lemma 2.1.3. *Let* GF(q) *be a finite field of order* $q = p^s = ef+1$.

(i) For $0 \leq i \leq e-1$, *each* $C_i^{e,s}$ *is a* $(q, \frac{q-1}{e}, A, B)$*-PDS if and only if there are integers* A *and* B *satisfying* $A = (0,0)_e$ *and* $B = (j,0)_e$ *for all* $1 \leq j \leq e-1$. *The PDS is proper precisely when* $A \neq B$.

(ii) Suppose that there exist integers A *and* B *satisfying* $A = (0,0)_e$ *and* $B = (i,0)_e$ *for all* $1 \leq i \leq e-1$. *Let* $\mathcal{D}' = \{C_j^{e,s}\}_{j \in R}$ *be a collection of* u *cyclotomic classes of order* e, *where* $R \subseteq \{0,1,\ldots,e-1\}$. *Then* $\mathcal{D}'$ *is a* $(q, u, \frac{q-1}{e}, A+(u-1)B, uB)$*-DPDF, which is proper precisely when* $A \neq B$.

Proof. (i) Assume that $C_i^{e,s}$ is a PDS, then by Definition 1.3.1

$$\Delta(C_i^{e,s}) = A(C_i^{e,s}) \cup B(\mathrm{G}^* \backslash C_i^{e,s}).$$

By Lemma 2.1.2 (iii), we may then write

$$\Delta(C_i^{e,s}) = A(C_i^{e,s}) \cup B(\mathrm{G}^*\backslash C_i^{e,s}) = \bigcup_{i'=0}^{e-1}(i'-i,0)C_{i'}^{e,s}.$$

When $i' = i$, it follows that $(i-i,0)_e = (0,0)_e = A$, moreover for all $i' \neq i$, it's clear that $(i'-i,0)_e = B$. In other words, for all $1 \leq j \leq e-1$, $(j,0) = B$.

For the reverse direction; by Lemma 2.1.2 (iii), when $A = (0,0)_e$ and $B = (j,0)_e$ for all $1 \leq j \leq e-1$, then

$$\Delta(C_i^{e,s}) = (0,0)_e(C_i^{e,s}) \cup (j,0)_e(\mathrm{G}^*\backslash C_i^{e,s}).$$

By Definition 1.3.1 it is then immediate that $C_i^{e,s}$ is a $(q, \frac{q-1}{e}, A, B)$-PDS, where $A = (0,0)_e$ and $B = (j,0)_e$ for all $1 \leq j \leq e-1$. Since $A = (0,0)_e$ counts the number of occurrences of the elements of $C_i^{e,s}$ in $\Delta(C_i^{e,s})$, and $B = (j,0)_e$ counts the occurrences of all other non-zero elements of $\mathrm{GF}(q)$ then by Definition 1.3.1 this implies that $C_i^{e,s}$ is a proper PDS when $A \neq B$.

(ii) In part (i) it was demonstrated that when $A = (0,0)_e$ and $B = (j,0)_e$ for all $1 \leq j \leq e-1$, then $C_i^{e,s}$ is a $(q, u, \frac{q-1}{e}, A+(u-1)B, uB)$-DPDF. It then follows as a direct consequence of Theorem 1.3.20 that if $\mathcal{D}'$ comprises a collection of u of these cyclotomic classes then $\mathcal{D}'$ is a $(q, u, \frac{q-1}{e}, A+(u-1)B, uB)$-DPDF. □

Note that Lemma 2.1.3 (i) is stronger than Lemma 2.1.3 (ii) (i.e. part (i) is an if and only if statement, whereas part (ii) is an if statement). This is because for a PDS, S, the multiset of internal differences $\mathrm{Int}(S)$ comprises only of the multiset $\Delta(C_i^{e,s})$, meaning that each element of $\mathrm{G}^*\backslash\{C_i^{e,s}\}$ must occur equally often in the multiset $\Delta(C_i^{e,s})$. For a DPDF, S', comprising of more than one cyclotomic class, $\mathrm{Int}(S')$ comprises multiple multisets of the form $\Delta(C_i^{e,s})$ (where $0 \leq i \leq e-1$), this means that $B \neq (j,0)_e$, where $0 \leq j \leq e-1$ is no longer a requirement. However, when $B = (j,0)_e$ for all $1 \leq j \leq e-1$, this means that each of the component sets of the DPDF is an individual PDS.

We now turn our attention to the following Lemma, which demonstrates how we can partition cyclotomic classes into unions of smaller cyclotomic classes.

Lemma 2.1.4. *Let $q = ef + 1 = \epsilon\rho + 1$, where $\epsilon \mid e$. Then*

(i) $C_0^{\epsilon,s} = \bigcup_{i=0}^{e/\epsilon-1} C_{i\epsilon}^{e,s}$,

(ii) for $0 \leq j \leq \epsilon - 1$, $C_j^{\epsilon,s} = \bigcup_{i=0}^{e/\epsilon-1} C_{i\epsilon+j}^{e,s}$

Proof. (i) The cyclotomic class $C_0^{\epsilon,s}$ consists of ϵ^{th} powers of α, where α is a primitive element, while the cyclotomic class $C_0^{e,s}$ consists of all e^{th} powers of α. As $\epsilon \mid e$, it is clear that $C_0^{e,s} \subseteq C_0^{\epsilon,s}$, and moreover that for $0 \leq i \leq \epsilon-1$, $C_{i\epsilon}^{e,s} \subseteq C_0^{\epsilon,s}$. It then naturally follows that

$$C_0^{\epsilon,s} = \bigcup_{i=0}^{e/\epsilon-1} C_{i\epsilon}^{e,s}$$

(ii) Immediate from part (i). □

Building upon the idea of partitioning larger cyclotomic classes into smaller cyclotomic classes, we are able to extend the notion of transversals to structures which, for a collection of cyclotomic classes S', contain elements of every multiset $\Delta(C_i^{e,s}) \subset \mathrm{Int}(S')$ (where $0 \leq i \leq e-1$). We call these new structures diagonals of transversals. Establishing a definition of these new objects will simplify the process of computing the elements of $\mathrm{Int}(S')$, which will in turn allow us to build machinery that is more easily able to identify cyclotomic constructions of DPDFs in which the component sets are not individually PDSs.

Definition 2.1.5. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = ef + 1 = \epsilon\rho + 1$, *where* $\epsilon \mid e$. *For* $1 \leq r \leq f - 1$, *we define*

$$D_r := \bigcup_{i=0}^{e/\epsilon-1} \alpha^{i\epsilon} T_r.$$

We refer to D_r *as a* ***diagonal of a transversal****.*

We now replicate the results of Lemma 2.1.2 for diagonals of transversals.

Lemma 2.1.6. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^s = ef + 1 = \epsilon\rho + 1$ *such that* $\epsilon \mid e$. *Moreover, let* $S' = \{C_0^{e,s}, C_\epsilon^{e,s}, \ldots, C_{e-\epsilon}^{e,s}\}$.

(i) $\mathrm{Int}(S') = \bigcup_{r=1}^{f-1} D_r$.

For each $1 \leq r \leq f - 1$

(ii) $D_r = (\alpha^{re} - 1)C_0^{\epsilon,s}$,

(iii) $D_r = C_{a'_r}^{\epsilon,s}$, *where* a'_r *is defined by* $\alpha^{re} - 1 \in C_{a'_r}^{\epsilon,s}$.

Proof. (i) By Defintion 1.2.3 and Lemma 2.1.2 (iii), it follows that

$$\mathrm{Int}(S') = \bigcup_{i=0}^{e/\epsilon-1} \Delta(C_{i\epsilon}^{e,s}) = \bigcup_{i=0}^{e/\epsilon-1} \alpha^{i\epsilon}\Delta(C_0^{e,s}).$$

Moreover, by Lemma 2.1.2 (ii)

$$\mathrm{Int}(S') = \bigcup_{i=0}^{e/\epsilon-1} \alpha^{i\epsilon}\left(\bigcup_{r=1}^{f-1} T_r\right) = \bigcup_{r=1}^{f-1}\left(\bigcup_{i=0}^{e/\epsilon-1} \alpha^{i\epsilon}T_r\right) = \bigcup_{r=1}^{f-1} D_r.$$

(ii) It follows by Lemma 2.1.2 (i) that for each $1 \leq r \leq f-1$, $T_r = (\alpha^{re}-1)C_0^{e,s}$, thus by Definition 2.1.5

$$D_r = \bigcup_{i=0}^{e/\epsilon-1} \alpha^{i\epsilon}(\alpha^{re} - 1)C_0^{e,s} = (\alpha^{re} - 1) \bigcup_{i=0}^{e/\epsilon-1} C_{i\epsilon}^{e,s}.$$

The result then follows by Lemma 2.1.4.

(iii) Since $\alpha^{re} - 1 \in \mathrm{GF}(q)$ (by the additive closure of $\mathrm{GF}(q)$), there exist values of $0 \leq u \leq \rho - 1$ and $0 \leq a'_r \leq \epsilon - 1$ such that $\alpha^{re} - 1 = \alpha^{u\epsilon + a'_r}$, hence it follows by part (ii) of this result that

$$D_r = (\alpha^{re} - 1)C_0^{\epsilon,s} = \alpha^{u\epsilon + a'_r}C_0^{\epsilon,s}.$$

Moreover, observe that since $\alpha^{u\epsilon} \in C_0^{\epsilon,s}$, we may write $\alpha^{u\epsilon+a'_r}C_0^{\epsilon,s} = \alpha^{a'_r}C_0^{\epsilon,s}$. The result is then immediate by Definition 1.4.1. □

With these results replicated for diagonals of transversals, we now set up further machinery to identify relationships between diagonals of transversals. This will further aid in the process of establishing new cyclotomic DPDF constructions. We start by establishing a quantity ϕ_i which, for each $0 \leq i \leq \epsilon - 1$, counts the number of diagonals of transversals in the multiset $\mathrm{Int}(S')$ (where $S' = \{C_0^{e,s}, C_\epsilon^{e,s}, \ldots, C_{e-\epsilon}^{e,s}\}$) that are copies of the cyclotomic class $C_i^{\epsilon,s}$.

Definition 2.1.7. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^s = ef + 1 = \epsilon\rho + 1$*, such that* $\epsilon \mid e$*. Let* α *be a primitive element of* $\mathrm{GF}(q)$*,* $C_i^{\epsilon,s} = \alpha^i \langle \alpha^\epsilon \rangle$ *for* $0 \leq i \leq \epsilon - 1$ *and* $C_0^{e,s} = \langle \alpha^e \rangle$*. We then define, for* $0 \leq i \leq \epsilon - 1$*,*

$$\Phi_i := \{x \in C_0^{e,s} : x \neq 1, x - 1 \in C_i^{\epsilon,s}\} \,\mathrm{and}\, \phi_i = |\Phi_i|.$$

Proposition 2.1.8. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = ef + 1 = \epsilon\rho + 1$ *such that* $\epsilon \mid e$*, then for* $0 \leq j \leq \epsilon - 1$*,*

$$\phi_j = \sum_{i=0}^{e/\epsilon - 1} (\epsilon i + j, 0)_e$$

Proof. By Lemma 2.1.4, it follows that $C_j^{\epsilon,s} = \bigcup_{i=0}^{e/\epsilon-1} C_{i\epsilon+j}^{e,s}$, where $0 \leq j \leq \epsilon - 1$. This means

$$\Phi_j = \{x \in C_0^{e,s} : x - 1 \in C_j^{\epsilon,s}\} = \{x \in C_0^{e,s} : x - 1 \in \cup_{i=0}^{e/\epsilon-1} C_{i\epsilon+j}^{e,s}\}.$$

By Definition 1.4.3, this implies $\phi_j = \sum_{i=0}^{e/\epsilon-1} (i\epsilon + j, 0)_e$. □

Theorem 2.1.9. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = ef + 1 = \epsilon\rho + 1$*, such that* $\epsilon \mid e$*. Moreover, let* $(C_0^{\epsilon,s})' = \{C_0^{e,s}, C_\epsilon^{e,s}, \ldots, C_{e-\epsilon}^{e,s}\}$*.*

(i) If $\phi_1 = \ldots = \phi_{\epsilon-1}$*, then* $\mathrm{Int}((C_0^{\epsilon,s})') = \phi_0(C_0^{\epsilon,s}) + \phi_1(\mathrm{G}^* \backslash C_0^{\epsilon,s})$ *meaning* $(C_0^{\epsilon,s})'$ *is a DPDF (or PDS if* $\epsilon = e$*).*

(ii) If $\phi_0 = \phi_1 = \ldots = \phi_{\epsilon-1}$*, then* $\mathrm{Int}((C_0^{\epsilon,s})') = \mathrm{G}^*$ *meaning* $(C_0^{\epsilon,s})'$ *is a DDF (or DS when* $\epsilon = e$*).*

(iii) If $\phi_i \neq \phi_j$ *for some distinct* $i, j \in \{1, \ldots, \epsilon - 1\}$ *then* $(C_0^{\epsilon,s})'$ *is not a DPDF (and therefore not a DDF).*

Proof. The proofs of both (i) and (ii) follow by Definition 2.1.7 and Lemma 2.1.6. In part (iii), suppose that there exist values of $i, j \in \{1, \ldots, \epsilon - 1\}$ such that $\phi_i \neq \phi_j$. This implies that $\mathrm{Int}((C_0^{\epsilon,s})')$ contains ϕ_i copies of $C_i^{\epsilon,s}$ and ϕ_j copies of $C_j^{\epsilon,s}$. Since $C_i^{\epsilon,s}, C_j^{\epsilon,s} \in \mathrm{GF}(q)^*\backslash C_0^{\epsilon,s}$, where $C_0^{\epsilon,s} = \sum_{a=0}^{\frac{e}{\epsilon}-1} C_{a\epsilon}^{e,s}$, it is immediate by Definition 1.3.11 that $(C_0^{\epsilon,s})'$ is not a DPDF. □

In the following Theorem and Corollary, we observe that the transversals and diagonals of transversals naturally pair up with one another.

Proposition 2.1.10. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^s = ef+1 = \epsilon\rho+1$, $C_0^{e,s} = \langle \alpha^e \rangle$ *and* $C_0^{\epsilon,s} = \langle \alpha^\epsilon \rangle$.

(i) For each $1 \leq r \leq f-1$, $T_{f-r} = -T_r$.

(ii) For each $1 \leq r \leq f-1$, $D_{f-t} = -D_t$.

Proof. (i) By Lemma 2.1.2 (i), for each $1 \leq r \leq f-1$, $-T_r = -(\alpha^{re}-1)C_0^{e,s} = (1-\alpha^{re})C_0^{e,s}$. By Lagrange's Theorem $\alpha^{ef} = 1$, we can therefore rewrite $-T_r = (\alpha^{ef} - \alpha^{re})C_0 = \alpha^{re}(\alpha^{ef-re} - 1)C_0^{e,s} = \alpha^{re}(\alpha^{e(f-r)} - 1)C_0^{e,s}$. Since $\alpha^{re} \in C_0^{e,s}$, which is closed under multiplication, it follows that $-T_r = (\alpha^{e(f-r)} - 1)C_0^{e,s} = T_{f-r}$.

(ii) It follows by Lemma 2.1.6 that $-D_r = -(\alpha^{re} - 1)C_0^{\epsilon,s}$. The proof of this result is then analogous to the proof of part (i). □

Corollary 2.1.11. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^s = ef+1 = \epsilon\rho+1$, *where* $\epsilon \mid e$. *Moreover, let* $C_0^{\epsilon,s} = \langle \alpha^\epsilon \rangle$ *and* $C_0^{e,s} = \langle \alpha^e \rangle$, *where* α *is a primitive element of* $\mathrm{GF}(q)$.

(a) Suppose that $T_r = C_{a_r}^{e,s}$ *(as definied in Definition 2.1.1) for* $1 \leq r \leq f-1$, *then*

(i) if either f *is even or* $p = 2$, *then* $T_{f-r} = C_{a_r}^{e,s}$ *(note that when* $r = \frac{f}{2}$, *trivially* $T_{f-\frac{f}{2}} = T_{\frac{f}{2}}$*).*

(ii) if e *is even but* f *is odd, then* $T_{f-r} = C_{a_r+\frac{e}{2}}^{e,s}$.

(b) Suppose that $D_r = C_{a_r'}^{\epsilon,s}$ *(as definied in Lemma 2.1.6.) for* $1 \leq r \leq f-1$, *then*

(i) *if either ρ is even or $p = 2$, then $D_{f-r} = C^{\epsilon,s}_{a'_r}$ (again, when $r = \frac{\rho}{2}$, trivially $D_{f-\frac{f}{2}} = D_{\frac{f}{2}}$).*

(ii) *if ϵ is even but ρ is odd, then $D_{f-r} = C^{\epsilon,s}_{a'_r+\frac{\epsilon}{2}}$.*

(c) *When f is even $T_{\frac{f}{2}} = (2)C^{e,s}_0$ and $D_{\frac{f}{2}} = (2)C^{\epsilon,s}_0$.*

Proof. (a) By Proposition 2.1.10, $T_{f-r} = -C^{e,s}_{a_r}$. It follows immediately by Lemma 1.4.11 that when f is even or $p = 2$, $-1 \in C^{e,s}_0$, hence $T_{f-r} = -C^{e,s}_{a_r} = C^{e,s}_{a_r}$, as multiplying an element of $C^{e,s}_{a_r}$ (a coset of $C^{e,s}_0$) by an element of $C^{e,s}_0$ trivially returns an element of $C^{e,s}_{a_r}$. When f is odd and e is even, it follows by Lemma 1.4.11 that $-1 = \alpha^{\frac{f-1}{2}e+\frac{e}{2}} \in C^{e,s}_{\frac{e}{2}}$. By choosing a particular coset representative $\alpha^{ev+a_r} \in C^{e,s}_{a_r}$ (where $v \in \mathbb{Z}_f$), we may then write $T_{f-r} = -C^{e,s}_{a_r} = \alpha^{\frac{f-1}{2}e+\frac{e}{2}}\alpha^{ev+a_r}C^{e,s}_0 = \alpha^{(\frac{f-1}{2}+v)e+(a_r+\frac{e}{2})}C^{e,s}_0$. Since $\alpha^{(\frac{f-1}{2}+v)e} \in C^{e,s}_0$, it follows that we may write $T_{f-r} = \alpha^{a_r+\frac{e}{2}}C^{e,s}_0$, and hence by Definition 1.4.1, when f is odd and e is even, $T_{f-r} = C^{e,s}_{a_r+\frac{e}{2}}$.

(b) Similarly, it follows from Lemma 1.4.11 that when ρ is even or $p = 2$, then $-1 \in C^{\epsilon,s}_0$, and when ρ is odd but ϵ is even, $-1 = \alpha^{\frac{\rho-1}{2}\epsilon+\frac{\epsilon}{2}} \in C^{\epsilon,s}_{\frac{\epsilon}{2}}$. The proof is then analogous to part (a).

(c) By Lemma 2.1.2 (i), $T_{\frac{f}{2}} = (\alpha^{\frac{f}{2}e}-1)C^{e,s}_0$. Moreover, by Lagrange's Theorem, $\alpha^{\frac{f}{2}e} = -1$, therefore $T_{\frac{f}{2}} = (-1-1)C^{e,s}_0 = (-2)C^{e,s}_0$. As f is even, it follows by Lemma 1.4.11 that $-1 \in C^{e,s}_0$, so therefore $T_{\frac{f}{2}} = (2)C^{e,s}_0$. When f is even, it is immediate that ρ must be even (since $f \mid \rho$), therefore $-1 \in C^{\epsilon,s}_0$ when f is even. It then follows by similar reasoning that $D_{\frac{f}{2}} = (2)C^{\epsilon,s}_0$. □

In what follows, we refer to $T_{\frac{f}{2}}$ as the **central transversal** and $D_{\frac{f}{2}}$ as the **central diagonal**.

In the case where $\epsilon = 2$, we have the following useful cyclotomic result from [60] (can be found in Theorem 4 of the $e = 2$ chapter, which can be found on page 31 of the book [60]).

Lemma 2.1.12. *Let* GF(q) *be a finite field, where $q = p^s = 2\rho + 1$ and suppose ρ is even, then*

(i) *if $q \equiv 1 \mod 8$, then $2 \in C^{2,s}_0$,*

(ii) *if $q \equiv 5 \mod 8$, then $2 \in C^{2,s}_1$.*

The next result then follows as an immediate consequence of Corollary 2.1.11(c) and Lemma 2.1.12.

Corollary 2.1.13. *Let* $\mathrm{GF}(q)$ *be a finite field, where* $q = p^s = ef + 1 = 2\rho + 1$. *Let* e *and* f *be even, then*

(i) if $q \equiv 1 \mod 8$, $D_{\frac{f}{2}} = C_0^{2,s}$,

(ii) if $q \equiv 5 \mod 8$, $D_{\frac{f}{2}} = C_1^{2,s}$.

We now establish a quantity ψ_i, which we will subsequently use to count the number of paired diagonals of transversals in $\mathrm{Int}(S')$, where $S' = \{C_0^{e,s}, C_\epsilon^{e,s}, \dots, C_{e-\epsilon}^{e,s}\}$ is a partition of the cyclotomic class $C_0^{\epsilon,s}$.

Definition 2.1.14. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = ef+1 = \epsilon\rho+1$, *such that* $\epsilon \mid e$. *For* $0 \le i \le \epsilon - 1$, *let*

$$\Psi_i := \{1 \le r < \frac{f}{2} : \alpha^{re} \in \Phi_i\} \text{ and } \psi_i := |\Psi_i|.$$

In the final results of this subsection, we demonstrate how the machinery that we have built can be used to find new constructions of PDSs, DPDFs and EPDFs.

Theorem 2.1.15. *Let* $\mathrm{GF}(q)$ *be a finite of order* $q = p^s = ef+1 = \epsilon\rho+1$, *where* $\epsilon \mid e$. *Moreover, let* $(C_0^{\epsilon,s})' = \{C_0^{e,s}, C_\epsilon^{e,s}, \dots, C_{e-\epsilon}^{e,s}\}$.

(a) Suppose that ρ *is even (i.e.* p *is odd) and* $\phi_1 = \phi_j$ *for all* $1 \le j \le \epsilon - 1$, *then* $(C_0^{\epsilon,s})'$ *is a* $(q, \frac{e}{\epsilon}, f, \phi_0, \phi_1)$*-DPDF (or* $(q, \rho, \phi_0, \phi_1)$*-PDS when* $\epsilon = e$*).*

(i) If f *is odd then* $\phi_0 = 2\psi_0$ *and* $\phi_1 = 2\psi_1$.

(ii) If f *is even and* $\epsilon > 2$, *then* $\phi_0 = 2\psi_0 + 1$ *and* $\phi_1 = 2\psi_1$.

(iii) If $\epsilon = 2$ *and* $q \equiv 1 \mod 8$, *then* $\phi_0 = 2\psi_0 + 1$ *and* $\phi_1 = 2\psi_1$.

(iv) If $\epsilon = 2$ *and* $q \equiv 5 \mod 8$, *then* $\phi_0 = 2\psi_0$ *and* $\phi_1 = 2\psi_1 + 1$.

(b) Let $p = 2$ *and suppose that* $\phi_1 = \phi_j$ *for all* $1 \le j \le \epsilon - 1$. *Then* $\phi_0 = 2\psi_0$, $\phi_1 = 2\psi_1$ *and* $(C_0^{\epsilon,s})'$ *is a* $(q, \frac{e}{\epsilon}, f, \phi_0, \phi_1)$*-DPDF (or* $(q, \rho, \phi_0, \phi_1)$*-PDS when* $\epsilon = e$*).*

(c) Let ϵ *be even and* ρ *be odd, and suppose* $\phi_1 = \phi_j$ *for all* $1 \le j \le \epsilon - 1$, *then* $\phi_0 = \phi_1$ *and* $(C_0^{\epsilon,s})'$ *is a* $(q, \frac{e}{\epsilon}, f, \phi_0)$*-DDF (or* (q, ρ, ϕ_0)*-Difference Set when* $\epsilon = e$*).*

Proof. As $q = ef + 1 = \epsilon\rho + 1$ such that $\epsilon \mid e$, then this implies that $f \mid \rho$.

(a) It follows by Corollary 2.1.11 (b)(i) that when ρ is even, if $D_r = C_i^{\epsilon,s}$ for $1 \leq r \leq f - 1$ (note $0 \leq i \leq \epsilon - 1$), then $D_{f-r} = C_i^{\epsilon,s}$. This means that if for some $1 \leq r \leq \frac{f}{2}$, $r \in \Psi_i$ (where $0 \leq i \leq \epsilon - 1$), then $\alpha^{re} \in \Phi_i$ and $\alpha^{(f-r)e} \in \Phi_i$. By Corollary 2.1.11(c), it follows that if f is even, then $D_{\frac{f}{2}} = C_k^{\epsilon,s}$ (where $0 \leq k \leq \epsilon - 1$) if $2 \in C_k^{\epsilon,s}$. We can therefore conclude that $\phi_i = 2\psi_i$ (where $0 \leq i \leq \epsilon - 1$) if $2 \notin C_i^{\epsilon,s}$ and $\phi_i = 2\psi_i + 1$ if $2 \in C_i^{\epsilon,s}$.

Note that when ρ is even, $f \mid \rho$ can be odd or even.

(i) It follows from the above that when f is odd, there is no central diagonal $D_{\frac{f}{2}}$, so $\phi_0 = 2\psi_0$ and $\phi_1 = 2\psi_1$.

(ii) Suppose that $\epsilon > 2$ and $2 \in C_l^{\epsilon,s}$ for $1 \leq l \leq \epsilon - 1$, it then follows from part (i) that $D_{\frac{f}{2}} = C_l^{e,s}$ and thus $\phi_l = 2\psi_l + 1$. This contradicts $\phi_1 = \phi_j$ for all $1 \leq j \leq \epsilon - 1$, since for all $1 \leq i \neq l \leq \epsilon - 1$, it was demonstrated in part (i) that $\phi_i = 2\psi_i$. This means that if $\phi_1 = \phi_i$ for all $1 \leq i \leq \epsilon - 1$, then $2 \in C_0^{\epsilon,s}$ and thus $\phi_0 = 2\psi_0 + 1$.

When f is even and $\epsilon = 2$, the only values of $0 \leq i \leq \epsilon - 1$ are $i = 0, 1$. This means that when $\epsilon = 2$, the above contradiction does not hold. This result is then immediate from Corollary 2.1.13.

(b) When ρ is odd, $\frac{f}{2}$ is not an integer meaning that there is no central diagonal, therefore each D_r (where $1 \leq r \leq f - 1$) pairs up with a distinct D_{f-r}. The proof of this result is otherwise analogous to the proof of part (a).

(c) As above, since ρ is odd, there is no central diagonal, therefore each D_r (where $1 \leq r \leq f - 1$) pairs up with a distinct D_{f-r}. By Corollary 2.1.11, when ρ is odd, if $D_r = C_i^{\epsilon,s}$ for some $0 \leq i \leq \epsilon - 1$ and $1 \leq r \leq \epsilon - 1$ then $D_{f-r} = C_i^{\epsilon,s}$. This then means that if for some $1 \leq r < \frac{f}{2}$, $r \in \Psi_i$ then $\alpha^{re} \in \Phi_i$ and $\alpha^{(f-r)e} \in \Phi_{i+\frac{\epsilon}{2}}$ (where $0 \leq i \leq \epsilon - 1$). It then follows that $\phi_i = \phi_{i+\frac{\epsilon}{2}}$ for all $0 \leq i \leq \epsilon - 1$: in particular, $\phi_0 = \phi_{\frac{\epsilon}{2}}$. Finally, since $\phi_1 = \phi_j$ for all $1 \leq j \leq \epsilon - 1$, $\phi_1 = \phi_{\frac{\epsilon}{2}} = \phi_0$. □

Corollary 2.1.16. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = ef + 1 = \epsilon\rho + 1$, *where* $\epsilon \mid e$. *Let* $(C_0^{\epsilon,s})' = \{C_0^{e,s}, C_\epsilon^{e,s}, \ldots, C_{e-\epsilon}^{e,s}\}$.

(a) Assume that ρ *is even.*

- *(i) If* $C_0^{\epsilon,s}$ *is a PDS, then it must be proper (and therefore regular).*
- *(ii) Suppose* f *is even, then if* $(C_0^{\epsilon,s})'$ *is a DPDF, then it must be proper.*

Suppose $\epsilon > 2$.

- *(iii) If* $C_0^{\epsilon,s}$ *is a proper PDS then* $2 \in C_0^{\epsilon,s}$.
- *(iv) Let* f *be even, then if* $(C_0^{\epsilon,s})'$ *is a proper DPDF, then* $2 \in C_0^{\epsilon,s}$.

(b) Let ϵ *be even and* ρ *be odd, then*

- *(i)* $C_0^{\epsilon,s}$ *is either a Difference Set, or it is not a PDS.*
- *(ii)* $(C_0^{\epsilon,s})'$ *is either a DDF, or it is not a DPDF.*

Proof. (a) Assume that $\epsilon > 2$. Since $C_0^{\epsilon,s}$ is a PDS, we apply $\epsilon = e$ and $\rho = f$ to Theorem 2.1.15 (a)(ii). As ρ is even, it follows by Theorem 2.1.15 (a)(ii) that $\phi_0 = 2\psi_0 + 1$ and $\phi_1 = 2\psi_1$. When we assume $\epsilon = 2$, it follows by Theorem (a)(ii) that either $\phi_0 = 2\psi_0 + 1$ and $\phi_1 = 2\psi_1$ or $\phi_0 = 2\psi_0$ and $\phi_1 = 2\psi_1 + 1$. In all cases, ϕ_0 and ϕ_1 have opposing parity, and therefore $C_0^{\epsilon,s}$ is a proper PDS. Since $C_0^{\epsilon,s}$ comprises the elements of a cyclotomic class, $0 \notin C_0^{\epsilon,s}$ and so $C_0^{\epsilon,s}$ is a regular PDS.

The proof of (ii) is analgous to the above here we simply assume that $e > \epsilon$. Parts (iii) and (iv) are immediate from the proof of part (ii) of Theorem 2.1.15.

(b) When $C_0^{e,s}$ is a PDS, we apply $\epsilon = e$ and $\rho = f$ to Theorem 2.1.15 (c) and obtain that $\phi_0 = \phi_j$ for $1 \le j \le \epsilon - 1$. It is immediate from this that $C_0^{\epsilon,s}$ must be a Difference Set, and cannot be proper PDS. We can analogously prove that $(C_0^{\epsilon,s})'$ is always a DDF. □

2.1.2 External differences

We can define similar tools for analysing the relationships between elements contained within multisets of the form $\Delta(C_i^{e,s}, C_j^{e,s})$ (where $0 \leq i \neq j \leq e-1$) which we refer to as external multisets. Note that the results in this subsection are also recorded in my joint paper with my supervisor [34].

We begin this Subsection by establishing an external analogue of a transversal.

Definition 2.1.17. *Let α be a primitive element of* $\mathrm{GF}(q)$*, where $q = p^s = ef+1$.*

(i) Let $T_{(r,l)} \subseteq \Delta(C_l^{e,s}, C_0^{e,s})$ (where $1 \leq l \leq e-1$) then for $0 \leq r \leq f-1$,

$$T_{(r,l)} := \{\alpha^{ne+l} - \alpha^{me} : n - m \equiv r \mod f, 0 \leq n, m \leq f-1\}.$$

We refer to the set $T_{(r,l)}$ as an ***external transversal*** *of $\Delta(C_l^{e,s}, C_0^{e,s})$ (or simply external transversal). Note that $|T_{(r,l)}| = f$.*

(ii) For each $0 \leq r \leq f-1$ and $1 \leq l \leq e-1$, let $a_{(r,l)} \in \{0, \dots, e-1\}$ be such that $\alpha^{re} - 1 \in C_{a_{(r,l)}}^{e,s}$.

The following Lemma demonstrates that, like transversals, we can use external transversals to split the multiset $\Delta(C_i^{e,s}, C_j^{e,s})$ into individual cylotomic classes.

Lemma 2.1.18. *Let* $\mathrm{GF}(q)$ *be a finite field of order $q = p^s = ef+1$*

(i) For $0 \leq r \leq f-1$ and $1 \leq l \leq e-1$, each external transversal $T_{(r,l)} = (\alpha^{re+l} - 1)C_0^{e,s}$ is a copy of $C_{a_{(r,l)}}^{e,s}$.

(ii) For $0 \leq r \leq f-1$, $\Delta(C_l^{e,s}, C_0^{e,s}) = \bigcup\limits_{r=1}^{f} T_{(r,l)} = \bigcup\limits_{r=0}^{f-1} C_{a_{(r,l)}}^{e,s} = \bigcup\limits_{k=0}^{e-1} (k,l)_e C_k^{e,s}$.

(iii) For $0 \leq i \neq j \leq e-1$, $\Delta(C_i^{e,s}, C_j^{e,s}) = \alpha^j \Delta(C_l, C_0) = \bigcup\limits_{r=0}^{f-1} \alpha^j T_{(r,l)} = \bigcup\limits_{k=0}^{e-1} (k-j, l)_e C_k^{e,s}$, where $l \equiv i - j \mod e$.

Proof. The proof of this result is analogous to the proof of Lemma 2.1.2. □

We now demonstrate that we can use the above machinery to establish new EPDF constructions when the cyclotomic numbers meet certain criteria. Note that in the following proof, we refer to the cyclotomic classes $C_r^{e,s}$ and $C_t^{e,s}$ as the

components of the multiset $\Delta(C_r^{e,s}, C_t^{e,s})$. An element that is not a component of the multiset $\Delta(C_r^{e,s}, C_t^{e,s})$ is referred to as a **non-component**.

Proposition 2.1.19. *Let* $\mathrm{GF}(q)$ *be a finite field, where* $q = p^s = ef + 1$. *Let* $I \subset \{0, 1, \ldots, e-1\}$ *(where* $|I| = u$, $2 \leq u \leq e-1$*) and* $D' = \{C_i^{e,s}\}_{i \in I}$. *If there exist integers* B *and* X *such that* $B = (i, 0)_e = (i, i)_e$ *and* $X = (i, j)_e$ *for all* $1 \leq i \neq j \leq e-1$, *then*

(i) $\Delta(C_r^{e,s}, C_t^{e,s}) = B(C_r^{e,s} \cup C_t^{e,s}) \cup X(\mathrm{G}^* \backslash (C_r^{e,s} \cup C_t^{e,s}))$.

(ii) D' *is a* $(q, u, \frac{q-1}{e}, 2B(u-1) + X(u-1)(u-2), Xu(u-1))$*-EPDF (which is proper if* $B \neq X$*).*

Proof. (i) It follows from Lemma 2.1.18 (iii) that

$$\Delta(C_r^{e,s}, C_t^{e,s}) = \alpha^t \Delta(C_{r-t}^{e,s}, C_0^{e,s}) = \bigcup_{k=0}^{e-1} (k-t, r-t)_e C_0^{e,s}.$$

Notice that the cyclotomic number $(k-t, r-t)_e$ is an external cyclotomic number except when $k = r$ or $k = t$. Since all internal cyclotomic numbers have value B, and all external cyclotomic numbers have value X, this means that we can rewrite $\Delta(C_r^{e,s}, C_t^{e,s})$ as

$$\Delta(C_r^{e,s}, C_t^{e,s}) = B(C_r^{e,s} \cup C_t^{e,s}) \cup X(\mathrm{G}^* \backslash (C_r^{e,s} \cup C_t^{e,s})).$$

(ii) It follows by Definition 1.2.3 that

$$\mathrm{Ext}(D') = \bigcup_{r,t \in I : r \neq t} \Delta(C_r^{e,s}, C_t^{e,s}).$$

By part (i), the components $C_r^{e,s}$ and $C_t^{e,s}$ of the multiset $\Delta(C_r^{e,s}, C_t^{e,s})$ occur at frequency B in this multiset $\Delta(C_r^{e,s}, C_t^{e,s})$, while each the non-components occurs at frequency X. There are precisely $u(u-1)$ multisets in $\mathrm{Ext}(D')$. For each $r \in I$, $C_r^{e,s}$ is a component of precisely $u-1$ multisets of the form $\Delta(C_r^{e,s}, C_t^{e,s})$ (where $t \in I$ and $t \neq r$), and is also a component of precisely $u-1$ multisets of the form $\Delta(C_t^{e,s}, C_r^{e,s})$ (where similarly, $t \in I$ and $t \neq r$) there are no further multisets for which $C_r^{e,s}$ is a component.

This means that there are $2(u-1)$ multisets in which (for $r \in I$) $C_r^{e,s}$ has frequency B and a remaining $u(u-1)-2(u-1)=(u-1)(u-2)$ multisets in which $C_r^{e,s}$ has frequency X. For any $v \notin I$, it follows by part (i) that $C_v^{e,s}$ has frequency X in all multisets in $\mathrm{Ext}(D')$. It then follows that D' is a $(q, u, \frac{q-1}{e}, 2B(u-1)+X(u-1)(u-2), Xu(u-1))$-EPDF, which is proper when $B \neq X$. □

Notice that we have not defined an external analogue of a diagonal of a transversal in this Subsection. This is because diagonals of transversals are only able to establish connections between unions of transversals and copies of cyclotomic classes of order ϵ, if the transversals partition a cyclotomic class of order ϵ. This means that if the multiset $\mathrm{Int}(S')$, where $S' = \{C_0^{e,s}, C_\epsilon^{e,s}, \ldots, C_{e-\epsilon}\}$, can be split into a collection of diagonals of transversals, then we can partition results in Section 1 to establish the elements contained in the multiset $\mathrm{Ext}(S')$, since we know that S' partitions the cyclotomic class $C_0^{\epsilon,s}$. In other words, an external analogue of a diagonal of a transversal would give us no extra information. It is, however, still useful to define an external transversal, since we may use external transversals to determine the behaviour of multisets of the form $\Delta(C_i^{e,s}, C_j^{e,s})$ (where $0 \leq i \neq j \leq e-1$), when the cyclotomic classes $C_i^{e,s}, C_j^{e,s} \in S'$, where S' is a collection of cyclotomic classes that does not partition a larger cyclotomic class. We see this machinery in action in Section 6.

2.1.3 Uniform cyclotomy

The concept of uniform cyclotomic numbers was defined in Chapter 1. We now close this Section of Chapter 2 by looking at how this concept can be used to find constructions of cyclotomic DPDFs and EPDFs. We begin this Section with the following results from [34].

Lemma 2.1.20. *Let* $\mathrm{GF}(q')$ *be a finite field of order* $q' = p^s = ef+1$*, where* p *is prime and* $e \geq 3$*. The following conditions are equivalent*

(i) -1 *is a power of* p *modulo* e*,*

(ii) there exists a prime power q *such that* $q' = q^{2b}$ $(b \in \mathbb{N})$ *and* $e|q+1$*.*

Proof. For the forwards direction, notice that $p^s \equiv 1 \mod e$, since $e \mid p^s - 1$. If we then suppose that p^t is the smallest positive integer satisfying $p^t \equiv -1$

mod e, we can see that $2t \mid s$, and so $s = 2tb$ for some $b \in \mathbb{N}$. This then means that $q' = p^s = p^{2tb} = (p^t)^{2b}$, where $e \mid p^t + 1$. For the reverse direction, note that $q \equiv -1 \mod e$ and we may write $q = p^c$, where $c \in \mathbb{N}$. □

The following result recorded in [34] demonstrates that we can use uniform cyclotomy to find new constructions of PDSs, DPDFs and EPDFs. Note that as a special case of Theorem 2.1.21 part (iii), we obtain the result of Calderbank and Kantor in Section 9 of [13], which is also presented in Section 10 of the survey paper [49]. Calderbank and Kantor demonstrated that the set D is a PDS when $e = q + 1$. Moreover, Theorem 2.1.21 part (iii) also subsumes a result of [26], an alternative proof of which is given in [4]. In [26] and [4], both sets of authors demonstrate that D is a Difference Set when η, e and u meet certain criterion.

Theorem 2.1.21. *Let* $\mathrm{GF}(q')$ *be a finite field of order* $q' = q^{2\beta} = ef + 1$, *where* $\beta \in \mathbb{N}$ *and* $q = p^{2m}$ *for some prime* p *and* $m \in \mathbb{N}$. *Let* $e \mid q + 1$ *and let* $\eta = \left(\frac{(-q)^{\beta}-1}{e}\right)$. *For any* $I \subseteq \{0, 1, \ldots, e-1\}$ *(where* $|I| = u$ *for some* u *with* $2 \leq u \leq e-1$*) let* $\mathcal{D}' = \{C_i^{e,4m\beta}\}_{i \in I}$. *Then*

(i) each $C_i^{e,2m}$ *is a (regular)* $(q', \frac{q'-1}{e}, \eta^2 - (e-3)\eta - 1, \eta^2 + \eta)$*-PDS,*

(ii) $\mathcal{D}'$ *is a* $(q', u, \frac{q'-1}{e}, u\eta^2 + (u+2-e)\eta - 1, u(\eta^2+\eta))$*-DPDF and a* $(q', u, \frac{q-1}{e}, u(u-1)\eta^2 + 2(u-1)\eta, u(u-1)\eta^2)$*-EPDF,*

(iii) $D = \bigcup_{i \in I} C_i^{e,2m}$ *is a (regular)* $(q', u\frac{(q'-1)}{e}, u^2\eta^2 + (3u-e)\eta - 1, u^2\eta^2 + u\eta)$*-PDS, which is proper except when* $\eta = 1 = 2u - e$ *and* $\eta = -1 = 2u - e$.

Proof. (i) As $e \mid q + 1$ for a prime power q satisfying $q' = q^{2\beta}$, where $\beta \in \mathbb{N}$, it follows, by Lemma 2.1.20 and Theorem 1.4.7, that the cyclotomic numbers of order e are uniform in the finite field $\mathrm{GF}(q')$. Moreover, by Theorem 1.4.7, for all $1 \leq i \neq j \leq e-1$

$$(0,0)_e = \left(\frac{s-1}{e}\right)^2 - (e-3)\left(\frac{s-1}{e}\right) - 1,$$

$$(i,0)_e = (0,i)_e = (i,i)_e = \left(\frac{s-1}{e}\right)^2 + \left(\frac{s-1}{e}\right),$$

$$(i,j)_e = \left(\frac{s-1}{e}\right)^2,$$

where for $q' = s^2$, $s \equiv 1 \mod e$. Notice that since $e \mid q+1$, this implies that $q \equiv -1 \mod e$ and therefore that $-q \equiv 1 \mod e$. Since $q' = s^2$ and $q' = q^{2\beta}$, it follows from the above that $s = (-q)^\beta$. We can therefore write

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

where $1 \leq i \neq j \leq e-1$ and $\eta = \frac{(-q)^\beta - 1}{e}$. It is then immediate from Lemma 2.1.3 (i) that for each $0 \leq l \leq e-1$, $C_l^{e,2m}$ is a $(q', \frac{q'-1}{e}, \eta^2-(e-3)\eta-1, \eta^2+\eta)$-PDS.

(ii) This is immediate from the above and Lemma 2.1.3 (ii).

(iii) This result is similarly immediate from the above and Proposition 2.1.19 (ii). Notice that when $u^2\eta^2 + (3u-e)\eta - 1 = u^2\eta^2 + u\eta$, then D is a Difference Set. We can rearrange the above to give

$$u\eta^2 + (3u-e)\eta - 1 = u^2\eta^2 + u\eta \Leftrightarrow (2u-e)\eta = 1.$$

It follows that the only solutions to this are $\eta = 2u-e = 1$ and $\eta = 2u-e = -1$. □

The following result is a new proof of a result in Section 8 of [4].

Corollary 2.1.22. *Let* $\mathrm{GF}(q')$ *be a finite field of order* $q' = q^{2\beta} = ef+1$*, where* $\beta \in \mathbb{N}$ *and* $q = p^r$ *for some prime* p *(i.e.* q *is a prime power). Let* $e \mid q+1$ *and let* $\eta = \left(\frac{(-q)^\beta - 1}{e}\right)$*. For any* $I \subset \{0,1,\ldots,e-1\}$ *(where* $|I| = u$ *for some* u *such that* $2 \leq u \leq e-1$*) let* $D = \bigcup_{i\in I} C_i^{e,2r\beta}$*, then* D *is a proper PDS unless*

(i) $e = 3$*,* $u = 2$ *and* $\eta = 1$*, in which case* D *is a* $(16,10,6)$*-Difference Set,*

(ii) $e = 2^a+1$*,* $u = 2^{a-1}$ *and* $\eta = -1$*, in which case* D *is a* $(4u^2, u(2u-1), u(u-1))$*-Difference Set.*

Proof. As demonstrated in the proof of Theorem 2.1.21 (iii), D is a proper PDS, except when $\eta = 2u-e = 1$ and $\eta = 2u-e = -1$. In both of these cases $(2u-e)\eta = 1$: we can rearrange this to give

$$2u\eta = e\eta + 1. \tag{2.1}$$

Observe that

$$e\eta + 1 = e\left(\frac{(-q)^{\beta} - 1}{e}\right) + 1 = (-q)^{\beta}. \tag{2.2}$$

It follows from the above that $2u\eta = (-q)^{\beta}$, and since $q' = ((-q)^{\beta})^2$, it follows that q' is a power of 2 (as q' is a prime power). We therefore write $q' = 2^{2a}$, where $m \in \mathbb{N}$.

(i) When $\eta = 1$, it follows from the above that

$$e + 1 = (-q)^{\beta} \Leftrightarrow e = (-q)^{\beta} - 1.$$

As e is a positive integer, note that this means $\beta \geq 2$ must be an even integer. Assuming that β is even, we may rewrite this $e = q^{\beta} - 1$. Moreover, as $e \mid q + 1$, this means that $e = q + 1$, since if $e < q + 1$, then it is not possible for $e = q^{\beta} - 1$, where $\beta \geq 2$ is an integer. Observe that $e = q^{\beta} - 1$ and $e = q + 1$ can only both be satisfied if $e = 3$, $q = 2$ and $\beta = 2$ (since q is a power of 2). Since $\beta = 2$, it follows that $q' = q^{2\beta} = 16$. Moreover, it follows that as $\eta = 1$, $2u = (-2)^2$, meaning $u = 2$ thus $\frac{u(q'-1)}{e} = \frac{2(15)}{3} = 10$ and $u^2\eta + u\eta = 4(1) + 2(1) = 6$. It is then immediate that D is a $(16, 10, 6)$-Difference Set when $\eta = 1$.

(ii) When $\eta = -1$, it follows from the above that

$$-e + 1 = (-q)^{\beta} \Leftrightarrow e = 1 - (-q)^{\beta}.$$

As e is a positive integer, it follows that $\beta \geq 1$ is an odd integer, and so $e = q^{\beta} + 1$. As $e \mid q + 1$, it follows that $e = q + 1$ and $\beta = 1$. Since $q' = 2^{2a} = (q)^{2\beta} = q^2$, it follows that $q = 2^{2m}$, and so $e = 2^m + 1$.

Moreover, since $q = 2^m$, this implies $(-q)^1 = -2^m$. By combining this fact with Equations (2.1) and (2.2) we obtain

$$2u\eta = -2^m \Leftrightarrow -2u = -2^m \Leftrightarrow u = 2^{m-1},$$

where $m \in \mathbb{N}$. It then follows that since $e = 2^m - 1$, $u = 2^{m-1}$ and $\eta = -1$ that $\frac{u(q'-1)}{e} = \frac{2^{m-1}(2^{2m}-1)}{2^m+1} = 2^{m-1}(2^m - 1) = u(2u-1)$, $u^2\eta^2 + u\eta = u^2 - u =$

$u(u-1)$ and $q' = 2^{2m} = 4(2^{2(m-1)}) = 4u^2$. It therefore follows that D is a $(4u^2, u(2u-1), u(u-1))$-Difference Set. □

As demonstrated in my joint paper with my supervisor [34] further to Corollary 2.1.22, we can also use Theorem 2.1.21 to obtain the recursive construction below. As demonstrated by the result below, this recursive construction only produces an EDF when the component sets partition the non-identity elements of $\mathrm{GF}(q')^*$. (Here the term recursive construction refers to the fact that component sets are PDSs that can be individually partioned into DPDFs/EPDFs.) This means that non-trivial DPDF/EPDF constructions obtained from the following result do not encompass any pre-existing cyclotomic DDF/EDF constructions in the literature.

Theorem 2.1.23. *Let* $\mathrm{GF}(q')$ *be a finite field of order* $q' = q^{2\beta} = p^{2m}$, *where* $m, \beta \in \mathbb{N}$. *For* $e \geq 3$, *let* $e|q+1$ *and* $\eta = \frac{(-q)^{\beta}-1}{e}$. *Let* $u, w \in \mathbb{N}$ *such that* $wu \leq e$ *and for* $1 \leq a \leq w$, *let* $I_a \subset \{0, 1, \ldots, e-1\}$ *such that* $|I_a| = u$ *and* $I_a \cap I_b = \emptyset$ *for all* $1 \leq a \neq b \leq w$. *Let* $D_a = \bigcup_{i \in I_a} C_i^{e,2m}$ *and* $\mathcal{W}' = \{D_1, D_2, \ldots, D_w\}$. *Then*

(i) $\mathcal{W}'$ *is a* $(q', w, u\frac{q'-1}{e}, u^2\eta^2 + (3u-e)\eta - 1 + (w-1)(u^2\eta^2 + u\eta), w(u^2\eta + u\eta))$-*DPDF.*

(ii) when $w \geq 2$, $\mathcal{W}'$ *is a* $(q', w, u\frac{q'-1}{e}, w(w-1)u^2\eta^2 + 2(w-1)u\eta, w(w-1)u^2\eta^2)$-*EPDF.*

(iii) if $\mathcal{W}'$ *does not partition* $\mathrm{GF}(q')$, *then* $\mathcal{W}'$ *is a DDF if and only if each* D_a *is a Difference Set.* $\mathcal{W}'$ *is only a DDF with* $w \geq 2$ *when* $e = 2^a + 1$, $u = 2^{a-1}$, $\eta = -1$ *and* $w = 2$.

(iv) Let $w \geq 2$. *If* $\mathcal{W}'$ *does partition* $\mathrm{GF}(q')$, *then* $\mathcal{W}'$ *is not an EDF.*

Proof. (i) By Theorem 2.1.21 (iii), each $D_a = \bigcup_{i \in I_a} C_i^{e,2m}$ is a $(q', \frac{u(q'-1)}{e}, u^2\eta^2 + (3u-e)\eta - 1, u^2\eta^2 + u\eta)$-PDS. It is then immediate from Theorem 1.3.20 (i) that $\mathcal{W}'$ is a $(q', w, u\frac{q'-1}{e}, u^2\eta^2 + (3u-e)\eta - 1 + (w-1)(u^2\eta^2 + u\eta), w(u^2\eta^2 + u\eta))$-DPDF.

(ii) Let $w \geq 2$ and $W = \cup_{a=1}^{w} D_a$, where $D_a \in \mathcal{W}'$. As $D_a = \cup_{i \in I_a} C_i^{e,2m}$, we may write $W = \cup_{a=1}^{w}(\cup_{i \in I_a} C_i^{e,m})$. Notice that this means that W is a collection of uw cyclotomic classes of order e. It then follows by Theorem 2.1.21

that W is a $(q', wu\frac{q'-1}{e}, (uw)^2\eta^2 + (3uw - e)\eta - 1, (uw)^2\eta^2 + uw\eta))$-PDS. Therefore, by Theorem 1.3.20, $\mathcal{W}'$ is also an EPDF.

By Lemma 1.2.4 as $\text{Int}(\mathcal{W}') = (u^2\eta^2 + (3u - e)\eta - 1 + (w - 1)(u^2\eta^2 + u\eta))\mathcal{W}' \cup w(u^2\eta + u\eta)(\text{GF}(q')*)$ and $\Delta(\mathcal{W}') = ((uw)^2\eta^2 + (3uw - e)\eta - 1)\mathcal{W}' \cup (uw)^2\eta^2 + uw\eta)(\text{GF}(q')^*\backslash\mathcal{W}')$, it follows that $\text{Ext}(W') = (w(w - 1)u^2\eta^2 + 2(w-1)u\eta)\mathcal{W}' \cup w(w-1)u^2\eta^2(\text{GF}(q')^*\backslash\mathcal{W}')$. It is then clear that when $w \geq 2$, $\mathcal{W}'$ is a $(q', w, u\frac{q'-1}{e}, w(w-1)u^2\eta^2+2(w-1)u\eta, w(w-1)u^2\eta^2)$-EPDF.

(iii) For the forwards direction $\mathcal{W}'$ is a DDF when $u^2\eta^2 + (3u - e)\eta - 1 + (w - 1)(u^2\eta^2 + u\eta) = w(u^2\eta + u\eta)$ this happens precisely when $(2u - e)\eta = 1$. By Theorem 2.1.21, when $(2u-e)\eta = 1$, then each $D_a \in \mathcal{W}'$ is a Difference Set. The reverse direction is immediate, since any collection of disjoint Difference Sets forms a DDF.

By Corollary 2.1.22, there are two cases for which a set $D_a = \cup_{i\in I_a} C_i^{e,2m}$ forms a Difference Set this happens when either $e = 3$, $u = 2$ and $\eta = 1$ or when $e = 2^a + 1$, $u = 2^{a-1}$ and $\eta = -1$. In the first case, we may apply the recursive construction when $w = 1$, since if $w \geq 2$, $wu \geq 4$, which is greater than $e = 3$. Therefore, in the first case, the recursive construction produces the $(16, 10, 6)$-Difference Set found by Corollary 2.1.22. In the second case, notice that $w \in \{1, 2\}$, since when $w = 2$, $wu = 2^a$, where $2^a < 2^a + 1 = e$. Notice if $w > 2$, then $wu > e$. In the case where $w = 2$, we obtain a $(4u^2, 2, u(2u-1), 2u(u-1))$-DDF (using the parameters given Corollary 2.1.22).

(iv) Let $w \geq 2$. If $\mathcal{W}'$ is an EPDF, then $w(w-1)u^2\eta^2+2(w-1)u\eta = w(w-1)u^2\eta^2$ must hold. In order for this equation to hold $(w-1)u\eta = 0$ must be true, but if $(w-1)u\eta = 0$ then either $u = 0$, $\eta = 0$ or $w - 1 = 0$. Since u and η have to be non-zero integers, and $w \geq 2$, $\mathcal{W}'$ is always a proper EPDF. □

Example 2.1.24. *In the finite field* GF(16)*, where* $16 = 2^4$*, let* $q = 4$ *and* $e = 5$*. When* $u = 2$ *and* $w = 2$*,* $\mathcal{W}' = \{D_1, D_2\}$*, where* $D_1 \cap D_2 = \emptyset$ *and* D_1 *and* D_2 *comprise elements of two distinct cyclotomic classes of order* 5*. For example, we can choose* $D_1 = C_0^{5,4} \cup C_4^{5,4}$ *and* $D_2 = C_1^{5,4} \cup C_3^{5,4}$*. By Corollary 2.1.22,* D_1 *and* D_2 *are individually* $(16, 6, 2)$*-Difference Sets, so naturally if* $\mathcal{W}' = \{D_1, D_2\}$ *then*

$\mathcal{W}'$ is a $(16,2,6,4)$-DDF. It then naturally follows by Theorem 2.1.23 that $\mathcal{W}'$ is also a $(16,2,6,4,8)$-EPDF. It is left up to the reader to check this.

2.2 Cyclotomic orbit framework

In this Section, we introduce a new cyclotomic tool, which we refer to as a cyclotomic orbit. Essentially, cyclotomic orbits are equivalence classes, in which any two cyclotomic numbers, indexed by distinct values of $(i,j) \in \mathbb{Z}_e \times \mathbb{Z}_e$, are related to each other under a collection of the identities outlined in Theorem 1.4.12. Note that whilst there is an inherent group action underpinning the relationship between each pair of cyclotomic numbers contained within the same cyclotomic orbit, in this Section we will be studying these objects from a purely combinatorial point of view.

The work in this Section enables us to identify the number of cyclotomic numbers of e, indexed by distinct values of $(i,j) \in \mathbb{Z}_e \times \mathbb{Z}_e$, that have the same value when $e \geq 5$ and f is even. This addresses a gap in the literature as there is currently no way of enurmerating the number of distinct cyclotomic numbers of order e in a given finite field. The machinery developed in this Section is used to identify a new method for constructing DPDFs in Chapter 3.6 and to create a more efficient algorithm for computing the cyclotomic numbers in large finite fields in Chapter 4.1.

Throughout this Section, we will use a combinatorial object known as a cyclotomic coset to understand more about the structure of cyclotomic orbits. Cyclotomic cosets have only previously been used in coding theory (see [45]). The relationship between cyclotomic cosets and cyclotomic orbits, explored in this Section, inherently will establish a connection between cyclotomic cosets and cyclotomic numbers. No such connection between cyclotomic cosets and cyclotomic numbers has previously been explored in the literature.

Definition 2.2.1. *(i) A **cyclotomic orbit**, $\mathrm{Orb}_{\mathfrak{R}}(i,j)_e$ is the set of cyclotomic numbers equivalent to the cyclotomic number $(i,j)_e$ $((i,j) \in \mathbb{Z}_e \times \mathbb{Z}_e)$ under a collection of cyclotomic relations, $\mathfrak{R}$.*

*(ii) The **orbit representative** of $\mathrm{Orb}_{\mathfrak{R}}(i,j)_e$ is the lexicographically smallest cyclotomic number $(a,b)_e$ such that $d = |b-a|$, where $d = \min_{(x,y)_e \in \mathrm{Orb}_{\mathfrak{R}}(i,j)_e}$*

$|y-x|$. *Throughout the rest of this document, we write the orbit as* $\mathrm{Orb}_{\mathfrak{R}}(a,b)_e$.

The reasoning behind the rigid definition of the cyclotomic representative of the cyclotomic orbit $\mathrm{Orb}(i,j)_e$ will become clear later. As each indiviudal cyclotomic orbit is defined under a particular collection of relations, $\mathfrak{R}$, we will need to highlight the particular collection of relations that we are referring to in each subsequent result/example. We therefore define the three special sets of relations which will be used throughout subsequent results.

Definition 2.2.2. *(i)* $\mathfrak{R}_1 := \{(i,j)_e = (ip,jp)_e\}$,

(ii) $\mathfrak{R}_2 := \{(i,j)_e = (j,i)_e, (i,j)_e = (e-i,j-i)_e\}$,

(iii) $\mathfrak{R}_3 := \{(i,j)_e = (j,i)_e, (i,j)_e = (e-i,j-i)_e, (i,j)_e = (ip,jp)_e\}$.

With these sets of relations defined, we will now look at an example of the Definition 2.2.1.

Example 2.2.3. *In the finite field* $\mathrm{GF}(81)$*, there are 10 orbits under the relations of* $\mathfrak{R}_3$*:*

$\mathrm{Orb}_{\mathfrak{R}_3}(0,0)_8 = \{(0,0)_8\}$
$\mathrm{Orb}_{\mathfrak{R}_3}(1,1)_8 = \{(1,1)_8, (3,3)_8, (7,0)_8, (5,0)_8, (0,7)_8, (0,5)_8\}$
$\mathrm{Orb}_{\mathfrak{R}_3}(2,2)_8 = \{(2,2)_8, (6,6)_8, (6,0)_8, (2,0)_8, (0,6)_8, (0,2)_8\}$
$\mathrm{Orb}_{\mathfrak{R}_3}(4,4)_8 = \{(4,4)_8, (4,0)_8, (0,4)_8\}$
$\mathrm{Orb}_{\mathfrak{R}_3}(5,5)_8 = \{(5,5)_8, (7,7)_8, (3,0)_8, (1,0)_8, (0,3)_8, (0,1)_8\}$
$\mathrm{Orb}_{\mathfrak{R}_3}(1,2)_8 = \{(1,2)_8, (3,6)_8, (2,1)_8, (6,3)_8, (7,1)_8, (5,3)_8, (1,7)_8, (3,5)_8, (6,7)_8,$
$(2,5)_8, (7,6)_8, (5,2)_8\}$
$\mathrm{Orb}_{\mathfrak{R}_3}(1,3)_8 = \{(1,3)_8, (3,1)_8, (7,2)_8, (5,6)_8, (2,7)_8, (6,5)_8\}$
$\mathrm{Orb}_{\mathfrak{R}_3}(3,4)_8 = \{(1,4)_8, (3,4)_8, (4,1)_8, (4,3)_8, (7,3)_8, (5,1)_8, (3,7)_8, (1,5)_8, (4,5)_8,$
$(4,7)_8, (5,4)_8, (7,4)_8\}$
$\mathrm{Orb}_{\mathfrak{R}_3}(2,3)_8 = \{(1,6)_8, (3,2)_8, (6,1)_8, (2,3)_8, (7,5)_8, (5,7)_8\}$
$\mathrm{Orb}_{\mathfrak{R}_3}(2,4)_8 = \{(2,4)_8, (6,4)_8, (4,2)_8, (4,6)_8, (6,2)_8, (2,6)_8\}$

Definition 2.2.4. *Any two cyclotomic numbers* $(a,b)_e$ *and* $(x,y)_e$ *contained within the same orbit* $\mathrm{Orb}_{\mathfrak{R}}(i,j)_e$ *are said to be* ***co-orbital****. (Note that for* $i,j \in \mathbb{Z}_e$*,* $(i,j)_e$ *is the orbit representative of* $\mathrm{Orb}_{\mathfrak{R}}(i,j)_e$*.) Two co-orbital cyclotomic numbers* $(a,b)_e$ *and* $(x,y)_e$*, indexed by* $(a,b),(x,y) \in \mathbb{Z}_e \times \mathbb{Z}_e$*, are said* *to be* ***identical*** *if $a = x$ and $b = y$, and* ***distinct*** *otherwise. We define the* ***order*** *of a cyclotomic orbit* $\mathrm{Orb}_{\mathfrak{R}}(i,j)_e$ *to be the number of distinct co-orbital cyclotomic numbers it contains.*

Notice that for any cyclotomic number $(i,j)_e$, indexed by $(i,j) \in \mathbb{Z}_e \times \mathbb{Z}_e$, we can view the elements i and j individually as elements of $\mathbb{Z}_e$. This viewpoint allows us to learn more about the impact of the cyclotomic number relations on cyclotomic numbers, and thus understand more about size of individual cyclotomic orbits. The following definition of a cyclotomic coset, which is based upon the definition given in [45], allows us to understand more about the structure of cyclotomic orbits under the relation in $\mathfrak{R}_1$.

Definition 2.2.5. *Let p be a prime such that* $\gcd(e,p) = 1$ *and let* $\mathbb{Z}_e = \{0, 1, \dots, e-1\}$ *be the ring of integers modulo e. Then the cyclotomic coset $\mathbb{C}_i$, where $i \in \mathbb{Z}_e$, is defined by the set*

$$\mathbb{C}_i = \{ip^x \,(\mathrm{mod}\, e) | 0 \leq x < y\},$$

where y is the smallest positive integer such that $ip^y \equiv i \,(\mathrm{mod}\, e)$.

Definition 2.2.6. *The smallest positive integer k, such that $p^k \equiv 1 \mod e$ is denoted* $\mathrm{ord}_e(p)$*. Notice that this is the size of the cyclotomic coset $\mathbb{C}_1$.*

Example 2.2.7. *Let $e = 8$ and $p = 3$. It is clear that the* $\gcd(8,3) = 1$ *and the cyclotomic cosets in $\mathbb{Z}_8$ are as follows; $\mathbb{C}_0 = \{0\}$, $\mathbb{C}_1 = \{1,3\} = \mathbb{C}_3$, $\mathbb{C}_2 = \{2,6\} = \mathbb{C}_6$, $\mathbb{C}_4 = \{4\}$, $\mathbb{C}_5 = \{5,7\} = \mathbb{C}_7$.*

Note that in [45], as well as many other papers in the literature, the definition of a cyclotomic coset is often given in terms of a prime power q. For the purposes of this Thesis, the definition is given in terms of a prime p, as we want to use the behaviour of the cyclotomic cosets to study the cyclotomic number relation $(i,j)_e = (ip, jp)_e$.

Throughout following results, we use the notation $\mathrm{U}(\mathbb{Z}_e)$ to refer to the group of units of the ring $\mathbb{Z}_e$. As any element $x \in \mathbb{Z}_e$ is a unit if $\gcd(x,e) = 1$, we can observe that there is an interesting connection between the cyclotomic coset $\mathbb{C}_1$ and the group $\mathrm{U}(\mathbb{Z}_e)$.

Remark 2.2.8. *Since* $\gcd(e,p) = 1$*, $p \in \mathrm{U}(\mathbb{Z}_e)$. By Definition 2.2.5, it follows that $\mathbb{C}_1 = \{1, p, \dots, p^{\mathrm{ord}_e(p)-1}\}$ is a multiplicative subgroup of $\mathrm{U}(\mathbb{Z}_e)$, comprising*

$\mathrm{ord}_e(p)$ *elements. Moreover, as* $p \in \mathrm{U}(\mathbb{Z}_e)$, *for each* $i \in \mathbb{Z}_e^*$, ip *is a unique element of* $\mathbb{Z}_e^*$.

Having established that the cyclotomic coset $\mathbb{C}_1$ is a subgroup of $\mathrm{U}(\mathbb{Z}_e)$, we can use this relationship to determine the order of each cyclotomic coset $\mathbb{C}_i$, where $2 \leq i \leq e-1$. To do this, we require the following preliminary Lemma.

Lemma 2.2.9. *Let* $e \in \mathbb{N}$, *where* $\gcd(e,p) = 1$ *for some prime* p. *For* $i \in \mathbb{Z}_e$, *let* n_i *be the smallest positive integer* $ip^{n_i} \equiv i \mod e$. *Then*

(i) for every $w \in \mathbb{N}$, $ip^{wn_i} \equiv i \mod e$,

(ii) if for $x \in \mathbb{N}$ $ip^x \equiv i \mod e$, *then this implies* $n_i \mid x$.

Proof. (i) We show inductively that $ip^{wn_i} \equiv i \mod e$ for every $w \in \mathbb{N}$. The base case $ip^{n_i} \equiv i \mod e$ is true by definition.

Assume for some $v \in \mathbb{N}$ that $ip^{vn_i} \equiv i \mod e$. It then follows that $ip^{(v+1)n_i} \equiv ip^{vn_i + n_i} \equiv ip^{vn_i}p^{n_i} \equiv ip^{n_i} \mod e$ by the inductive hypothesis. Therefore, we have proven by induction that $ip^{wn_i} \equiv i \mod e$ for every $w \in \mathbb{N}$.

(ii) Since n_i is the smallest positive integer satisfying $ip^{n_i} \equiv i \mod e$, we assume that $x \geq n_i$. Assume $n_i \nmid x$, this implies that $x = qn_i + r$, where $q = \frac{x-r}{n_i}$ and $1 \leq r \leq n_i - 1$. Then $i \equiv ip^x \equiv ip^{qn_i + r} \equiv ip^{qn_i}p^r \mod e$. It follows from part (i) that $ip^{qn_i} \equiv i \mod e$, therefore $ip^{qn_i}p^r \equiv ip^r \equiv i \mod e$. This is a contradiction as $r < n_i$ and n_i is the smallest positive integer satisfying $ip^{n_i} \equiv i \mod e$. □

We can now use this result to prove that the order of any cyclotomic coset $\mathbb{C}_i$ (where $i \in \mathbb{Z}_e$) must divide the order of $\mathbb{C}_1$.

Proposition 2.2.10. *Let* $\{1, p, p^2, \ldots, p^{\mathrm{ord}_e(p)-1}\} \subseteq \mathbb{Z}_e^*$, *where* p *be is a prime and* $\gcd(e,p) = 1$. *Moreover, let* $\mathbb{C}_i = \{i, ip, ip^2, \ldots, ip^{\mathrm{ord}_e(p)-1}\}$ *for* $i \in \mathbb{Z}_e$, *then*

(i) when $i \in \mathrm{U}(\mathbb{Z}_e)$, $|\mathbb{C}_i| = \mathrm{ord}_e(p)$,

(ii) when $i \notin \mathrm{U}(\mathbb{Z}_e)$, $|\mathbb{C}_i|$ *divides* $|\mathbb{C}_1| = \mathrm{ord}_e(p)$.

Proof. (i) It is immediate from Remark 2.2.8 that $\mathbb{C}_1 = \{1, p, \ldots, p^{\text{ord}_e(p)-1}\}$ is a multiplicative subgroup of $\mathbb{Z}_e$ consisting of $\text{ord}_e(p)$ distinct elements. Now suppose that for $i \neq 1 \in \mathbb{Z}_e$, $i \in \text{U}(\mathbb{Z}_e)$ then $\mathbb{C}_i = \{i, ip, \ldots, ip^{\text{ord}_e(p)-1}\} = i(\mathbb{C}_1)$. As $\mathbb{C}_1 \subseteq \text{U}(\mathbb{Z}_e)$ and $i \in \text{U}(\mathbb{Z}_e)$, it follows that $\mathbb{C}_i = i(\mathbb{C}_1)$ is a multiplicative coset of $\mathbb{C}_1$ in the group $\text{U}(\mathbb{Z}_e)$, and therefore $\mathbb{C}_i$ also has order $\text{ord}_e(p)$.

(ii) When $i = 0$, observe that $\mathbb{C}_0 = \{0\}$ and therefore $|\mathbb{C}_0| = 1$, so the statement is true for $i = 0$.

Now suppose that for $2 \leq i \leq e-1$, $i \notin \text{U}(\mathbb{Z}_e)$. Since $p \in \text{U}(\mathbb{Z}_e)$, there are no zero divisors under multiplication by p in the ring $\mathbb{Z}_e$. This means that for $i \notin \text{U}(\mathbb{Z}_e)$, there exists some $s \in \mathbb{N}$ that is the smallest positive integer satisfying $ip^s \equiv i \mod e$. It follows directly from Lemma 2.2.9 that $s \mid \text{ord}_e(p)$, and thus $|\mathbb{C}_i|$ divides $\text{ord}_e(p)$. □

Example 2.2.11. *In the ring* $\mathbb{Z}_8$, $\text{U}(\mathbb{Z}_8) = \{1, 3, 5, 7\}$ *and the elements of* $\mathbb{Z}_8$ *not contained within the group of units are the elements* $\{0, 2, 4, 6\}$*. It was demonstrated in Example 2.2.7 that when* $p = 3$ *and* $e = 8$, $\mathbb{C}_1 = \langle 3 \rangle = \{1, 3\} = \mathbb{C}_3$*. As the elements* $\{5, 7\}$ *are also units, it is clear that the cyclotomic coset* $\mathbb{C}_5 = 5\langle 3 \rangle = \{5, 7\} = \mathbb{C}_7$ *is a multiplicative coset of* $\mathbb{C}_1$ *in the group* $\text{U}(\mathbb{Z}_8)$*.*

It follows from Proposition 2.2.10 that each of the non-units is contained within a cyclotomic coset, $\mathbb{C}_i$*, whose order divides* $|\mathbb{C}_1| = 2$*. Observe that* $|\mathbb{C}_0| = 1$, $|\mathbb{C}_2| = |\mathbb{C}_6| = 2$ *and* $|\mathbb{C}_4| = 1$*, all of which divide* 2*.*

Using the above Proposition, we can establish an interesting connection between the cyclotomic classes of order e in the finite field $\text{GF}(q)$ ($q = p^s = ef + 1$) and certain cyclotomic classes in the finite field $\text{GF}(e)$ when e and p are both prime.

Corollary 2.2.12. *Let* $\langle p \rangle \subseteq \mathbb{Z}_e^*$*, where* e *and* p *are distinct primes. For each* $i \in \mathbb{Z}_e$*, let* $\mathbb{C}_i = \{i, ip, \ldots, ip^{n_i - 1}\} \subseteq \mathbb{Z}_e$*. Then*

(i) $|\mathbb{C}_0| = 1$*,*

(ii) for $i \in \mathbb{Z}_e^*$, $|\mathbb{C}_i| = \text{ord}_e(p)$*,*

(iii) for each $i \in \mathbb{Z}_e^*$, the cyclotomic coset $\mathbb{C}_i$ is equivalent to the cyclotomic class $C_j^{\epsilon,1} \subset \mathrm{GF}(e)$, where $\epsilon = \frac{e-1}{\mathrm{ord}_e(p)}$ and $i \in C_j^{\epsilon,1}$ for some $j \in \mathbb{Z}_\epsilon$.

Proof. (i) This result is immediate by Proposition 2.2.10.

(ii) When e is prime, the group $\mathrm{U}(\mathbb{Z}_e)$ comprises all the elements of $\mathbb{Z}_e^*$. It therefore follows from Proposition 2.2.10 (i) that since every element of $\mathbb{Z}_e^*$ is a unit, each cyclotomic coset must have order $\mathrm{ord}_e(p)$.

(iii) When e is prime, the ring $\mathbb{Z}_e$ is equivalent to the finite field $\mathrm{GF}(e)$. It then follows from Remark 2.2.8 that $\mathbb{C}_1$ is a multiplicative subgroup of order $\mathrm{ord}_e(p)$ in $\mathrm{GF}(e)^*$. By the fundamental theorem of cyclic groups, as $\mathrm{GF}(e)^*$ is a cyclic group, each subgroup of $\mathrm{GF}(e)^*$ is unique. This means that, irrespective of the generator chosen, the subgroup of order $\mathrm{ord}_e(p)$ in $\mathrm{GF}(e)^*$ contains the elements $\{1, p, \ldots, p^{\mathrm{ord}_e(p)-1}\}$, and thus $\mathbb{C}_1$ is equivalent to the cyclotomic class $C_0^{\epsilon,1} = \langle \alpha^\epsilon \rangle$, where α is a primitive element of $\mathrm{GF}(e)$ and $\epsilon = \frac{e-1}{\mathrm{ord}_e(p)}$. Moreover, for $2 \leq i \leq e-1$, $\mathbb{C}_i = i\mathbb{C}_1$ is a multiplicative coset of $\mathbb{C}_1$. As $i \in \mathrm{GF}(e)^*$, there exists a $j \in \mathbb{Z}_\epsilon$ and an $0 \leq s \leq \mathrm{ord}_e(p) - 1$ such that $\alpha^{\epsilon s + j} = i$ (where α is a primitive element of $\mathrm{GF}(e)$ as above). Observe that $\alpha^{\epsilon s+j} \in C_j^{\epsilon,1}$, therefore the cyclotomic coset $\mathbb{C}_i$, where $1 \leq i \leq e-1$, is equivalent to the cyclotomic class $C_j^{\epsilon,1}$. □

Let $(i,j) \in \mathbb{Z}_e \times \mathbb{Z}_e$ denote the ordered 2-tuple which indexes an arbitrary cyclotomic number $(i,j)_e$. In the following results, we demonstrate that by viewing i and j as individual elements of the group $\mathbb{Z}_e$, in particular viewing i as an element of the cyclotomic coset $\mathbb{C}_i$ and j as an element of the cyclotomic coset $\mathbb{C}_j$, allows us to compute number of distinct co-orbital cyclotomic numbers lying in each $\mathrm{Orb}_{\mathfrak{R}_1}(i,j)_e$.

Proposition 2.2.13. *In $\mathbb{Z}_e$, let p be a prime such that the $\gcd(e,p) = 1$. Moreover, suppose that $\mathbb{C}_i = i\langle p \rangle$ and $\mathbb{C}_j = j\langle p \rangle$ are cyclotomic cosets, where $|\mathbb{C}_i| = n_i$, $|\mathbb{C}_j| = n_j$ and $i, j \in \mathbb{Z}_e$. The smallest positive integer $z_{i,j} \mid \mathrm{ord}_e(p)$ for which $ip^{z_{i,j}} = i$ and $jp^{z_{i,j}} = j$ is $z_{i,j} = \mathrm{lcm}(n_i, n_j)$.*

Proof. It follows from Lemma 2.2.9 that $z_{i,j} = \mathrm{lcm}(n_i, n_j)$ satisfies $ip^{z_{i,j}} \equiv i \mod e$ and $jp^{z_{i,j}} \equiv \mod e$. As a further consequence of Lemma 2.2.9, any integer $0 \leq z < z_{i,j}$ can satisfy $ip^{z_{i,j}} \equiv i \mod e$ and $jp^{z_{i,j}} \equiv \mod e$ simultaneously if and only if $n_i \mid z$ and $n_j \mid z$. Since $z_{i,j} = \frac{n_i n_j}{\gcd(n_i,n_j)}$ is the lowest common multiple of n_i and n_j, no integer $0 < z < z_{i,j}$ can satisfy both $ip^{z_{i,j}} \equiv i \mod e$ and $jp^{z_{i,j}} \equiv \mod e$ simultaneously. □

Lemma 2.2.14. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^n = ef + 1$*, where* p *is an odd prime (note that* $\gcd(e,p) = 1$*). Suppose that for* $i, j \in \mathbb{Z}_e$*,* $\mathbb{C}_i$ *and* $\mathbb{C}_j$ *denote the* i^{th} *and* j^{th} *cyclotomic cosets modulo* e*, where* $|\mathbb{C}_i| = n_i$ *and* $|\mathbb{C}_j| = n_j$*. Then the* $\mathrm{Orb}_{\mathfrak{R}_1}(i,j)_e$ *has order* $z_{i,j}$*, where* $z_{i,j} = \mathrm{lcm}(n_i, n_j)$ *and* $z_{i,j} \mid \mathrm{ord}_e(p)$*.*

Proof. All cyclotomic numbers contained within the cyclotomic orbit $\mathrm{Orb}_{\mathfrak{R}_1}(i,j)_e$ are of the form $(ip^r, jp^r)_e$, where $ip^r \in \mathbb{C}_i$, $jp^r \in \mathbb{C}_j$ and $r \in \mathbb{Z}$. To determine the order of $\mathrm{Orb}_{\mathfrak{R}_1}(i,j)_e$ for a particular $(i,j) \in \mathbb{Z}_e \times \mathbb{Z}_e$, we therefore need to determine the number of distinct cyclotomic numbers that can be written in the form $(ip^r, jp^r)_e$, where $r \in \mathbb{Z}$, $ip^r \in \mathbb{C}_i$ and $jp^r \in \mathbb{C}_j$. By Proposition 2.2.13, the smallest positive integer r satisfying $ip^r \equiv i \mod e$ and $jp^r \equiv j \mod e$ simultaneously is $z_{i,j} = \mathrm{lcm}(n_i, n_j)$, where $|\mathbb{C}_i| = n_i$ and $|\mathbb{C}_j| = n_j$. Since $ip^{z_{i,j}} \equiv i \mod e$ and $jp^{z_{i,j}} \equiv j \mod e$, the cyclotomic numbers $(ip^{z_{i,j}}, jp^{z_{i,j}})_e$ and $(i,j)_e$ are identical. Further, assume that two cyclotomic numbers $(ip^{r_1}, jp^{r_1})_e$ and $(ip^{r_2}, jp^{r_2})_e$, where $0 \le r_1 < r_2 \le z_{i,j} - 1$, are identical to one another. This is true if and only if $ip^{r_1} \equiv ip^{r_2} \mod e$ and $jp^{r_1} \equiv jp^{r_2} \mod e$ which in turn is true if and only if $ip^{r_2 - r_1} \equiv i \mod e$ and $jp^{r_2 - r_1} \equiv j \mod e$. Notice that $0 \le r_2 - r_1 \le z_{i,j} - 1$, so it follows by Proposition 2.2.13 that there are no values $0 \le r_1 < r_2 \le z_{i,j} - 1$ satisfying $ip^{r_2 - r_1} \equiv i \mod e$ and $jp^{r_2 - r_1} \equiv j \mod e$ simultaneously, therefore the cyclotomic numbers $(ip^{r_1}, jp^{r_1})_e$ and $(ip^{r_2}, jp^{r_2})_e$, where $0 \le r_1 < r_2 \le z_{i,j} - 1$ must be distinct. Finally, for $t > z_{i,j}$, observe that we may write $t = uz_{i,j} + s$, where $u = \frac{t-s}{z_{i,j}}$ and $0 \le s \le z_{i,j} - 1$. Since by Proposition 2.2.13 $ip^{z_{i,j}} \equiv i \mod e$ and $jp^{z_{i,j}} \equiv j \mod e$, it follows by Lemma 2.2.9 that $ip^t = ip^{uz_{i,j}}p^s \equiv ip^s \mod e$ and $jp^t = jp^{uz_{i,j}}p^s \equiv jp^s \mod e$. This means that each cyclotomic number $(ip^t, jp^t)_e$, where $t > z_{i,j}$ is equivalent to the cyclotomic number $(ip^s, jp^s)_e$, where $t = uz_{i,j} + s$ for $0 \le s \le z_{i,j} - 1$ and $u = \frac{t-s}{z_{i,j}}$ (as above). □

We now demonstrate that when e is an odd prime, all cyclotomic orbits under the relation $(i,j)_e = (ip, jp)_e$ have order $\mathrm{ord}_e(p)$.

Corollary 2.2.15. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^n = ef + 1$*, where* e *and* p *are distinct primes. Then* $\mathrm{Orb}_{\mathfrak{R}_1}(i,j)_e$ *has order* $\mathrm{ord}_e(p)$ *for all* $(i,j) \in \mathbb{Z}_e \times \mathbb{Z}_e^*$.

Proof. By Lemma 2.2.14 that $|\mathrm{Orb}_{\mathfrak{R}_1}(i,j)_e| = z_{i,j}$, where, for $n_i = |\mathbb{C}_i|$ and $n_j = |\mathbb{C}_j|$, $z_{i,j} = \mathrm{lcm}(n_i, n_j)$. It then follows by Corollary 2.2.12 that $|\mathbb{C}_i| = |\mathbb{C}_j| = \mathrm{ord}_e(p)$ for all $i, j \in \mathbb{Z}_e^*$. □

Remark 2.2.16. *As a direct consequence of Corollary 2.2.15, we can say that when* e *and* p *are distinct primes, the relation* $(i,j)_e = (ip, jp)_e$ *maps each cyclotomic number* $(a,b)_e$ *(where* $(a,b) \in \mathbb{Z}_e \times \mathbb{Z}_e$*) to* $\mathrm{ord}_e(p)$ *cyclotomic numbers of the form* (ap^x, bp^x)*, where* $0 \leq x \leq \mathrm{ord}_e(p) - 1$. *It is evident from the proof of Lemma 2.2.14 that the cyclotomic numbers* (ap^x, bp^x) *are all distinct for* $0 \leq x \leq \mathrm{ord}_e(p) - 1$.

Lemma 2.2.17. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^n = ef + 1$*, where* p *is an odd prime and* f *is even. Suppose that* $i, j \in \mathbb{Z}_e$. *Then the cyclotomic orbit* $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ *has order at most 6.*

Proof. By Lemma 1.4.12, when f is even, the following relations $(i,j)_e = (j,i)_e$ and $(i,j)_e = (e-i, j-i)_e$ hold for all $i, j \in \mathbb{Z}_e^*$. It is immediately clear that the relation $(i,j)_e = (j,i)_e$ is self-inverse. It is less clear that $(i,j)_e = (e-i, j-i)_e$ is self-inverse, but observe that under relation:

$$(e-i, j-i)_e = (e-(e-i), (j-i)-(e-i))_e = (i, j-e)_e = (i,j)_e.$$

It is immediately clear from the above relations that the cyclotomic numbers $(i,j)_e, (j,i)_e, (e-i, j-i)_e \subseteq \mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$. To find further cyclotomic numbers contained within $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$, the cyclotomic relations $(i,j)_e = (j,i)_e$ and $(i,j)_e = (e-i, j-i)_e$ must be applied in combination with one another. Note the relations $(i,j)_e = (e-i, j-i)_e$ and $(i,j)_e = (j,i)_e$ must be applied alternately, as both relations are self-inverse.

By first applying the relation $(i,j)_e = (e-i, j-i)_e$ to the cyclotomic number $(i,j)_e$, followed by the relation $(i,j)_e = (j,i)_e$, we obtain the cyclotomic number $(j-i, e-i)_e$. By then applying the relation $(i,j)_e = (e-i, j-i)_e$ to the cyclotomic number $(j-i, e-i)_e$, we obtain the cyclotomic number:

$$(j-i, e-i)_e = (e-(j-i), (e-i)-(j-i))_e = (e+i-j, e-j)_e = (i-j, e-j)_e.$$

Applying the relation $(i,j)_e = (j,i)_e$ to the cyclotomic number $(i-j,e-j)_e$ yields the cyclotomic number $(e-j,i-j)_e$. Applying the relation $(i,j)_e = (e-i,j-i)_e$ for a final time to $(i,j)_e = (e-j,i-j)_e$ gives:

$$(e-j,i-j)_e = (e-(e-j),(i-j)-(e-j))_e = (j,i-e)_e = (j,i)_e,$$

which is an existing cyclotomic number in the cyclotomic orbit $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$. Since both relations are symmetric, applying the relations in the reverse direction produces a series cyclotomic numbers, already contained in the cyclotomic orbit $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$. Hence, $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e = \{(i,j)_e,(j,i)_e,(e-i,j-i)_e,(j-i,e-i)_e,(i-j,e-j)_e,(e-j,i-j)_e\}$. Therefore $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ has order exactly 6 when the cyclotomic numbers $(i,j)_e$, $(j,i)_e$, $(e-i,j-i)_e$, $(j-i,e-i)_e$, $(i-j,e-j)_e$ and $(e-j,i-j)_e$ are all distinct cyclotomic numbers, and order less than 6 when any collection of these cyclotomic numbers are identical. □

Next we look to identify the size of each orbit $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$. We first identify the conditions under which certain pairs of elements from the orbit $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ are identical, and the conditions under which pairs of elements in $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ are always distinct.

As demonstrated in the proof of Lemma 2.2.17, each distinct cyclotomic number in $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ can be written as at least one of the following cyclotomic numbers $(i,j)_e$, $(j,i)_e$, $(e-i,j-i)_e$, $(e-j,i-j)_e$, $(j-i,e-i)_e$, $(i-j,e-j)_e$. To determine the number of identical/distinct co-orbital cyclotomic numbers in the orbit $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$, we need to determine whether each pair of 2-tuples $((a,b),(c,d)) \in \mathbb{Z}_e \times \mathbb{Z}_e$ indexing the elements of $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ is identical/distinct under certain conditions. As there are 6 distinct 2-tuples $(a,b) \in \mathbb{Z}_e \times \mathbb{Z}_e$ indexing the co-orbital cyclotomic numbers of $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$, we need to consider all $\binom{6}{2} = 15$ possible pairs of indicies $((a,b),(c,d)) \in \mathbb{Z}_e \times \mathbb{Z}_e$.

Lemma 2.2.18. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = ef+1 = p^n$*, where* p *is an odd prime and* f *is even. Let* $i,j \in \mathbb{Z}_e$*. Under the relations in* $\mathfrak{R}_2$*, the pairs of indicies of co-orbital cyclotomic numbers in* $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ *satisfy the following*

(i) $\{(i,j),(e-i,j-i)\}$, $\{(i,j),(i-j,e-j)\}$, $\{(j,i),(e-j,i-j)\}$, $\{(j,i),(j-i,e-i)\}$, $\{(e-i,j-i),(j-i,e-i)\}$ *and* $\{(e-j,i-j),(i-j,e-j)\}$ *are always distinct from one another.*

(ii) $\{(i,j),(j,i)\}$, $\{(e-i,j-i),(e-j,i-j)\}$ *and* $\{(j-i,e-i),(i-j,e-j)\}$, *are identical when* $i=j$ *and distinct otherwise,*

(iii) $\{(i,j),(e-j,i-j)\}$, $\{(i,j),(j-i,e-i)\}$, $\{(e-j,i-j),(j-i,e-i)\}$, $\{(j,i),(e-i,j-i)\}$, $\{(j,i),(i-j,e-j)\}$ *and* $\{(e-i,j-i),(i-j,e-j)\}$ *are identical when the conditions* $i \equiv 2j \mod e$ *and* $3j \equiv 0 \mod e$ *are both satisfied, and distinct otherwise. Observe that this case can only arise if* $3 \mid e$.

Proof. (i) Observe that for all $i,j \in \mathbb{Z}_e^*$ we have $j \neq j-i$, and analogously, for all $i,j \in \mathbb{Z}_e^*$, $i \neq i-j$. This means that the following pairs of indicies must always be distinct: $\{(i,j),(e-i,j-i)\}$, $\{(i,j),(i-j,e-j)\}$, $\{(j,i),(e-j,i-j)\}$ and $\{(j,i),(j-i,e-i)\}$. Note that for all $i,j \in \mathbb{Z}_e^*$, $e-j \neq i-j$, since if $e-j=i-j$ this implies $i=e$, meaning that i is outside of the set range of integer values. Analogously for all $1 \leq i,j \leq e-1$, $e-i \neq j-i$. This means that the following pairs of indicies are always distinct: $\{(e-i,j-i),(j-i,e-i)\}$ and $\{(e-j,i-j),(i-j,e-j)\}$.

(ii) When $i=j \in \mathbb{Z}_e$, observe that the following pairs of indicies are identical $\{(i,j),(j,i)\}$, $\{(e-i,j-i),(e-j,i-j)\}$ and $\{(i-j,e-j),(j-i,e-i)\}$. Moreover, when $i \neq j \in \mathbb{Z}_e^*$, then $i \neq j$, $e-i \neq e-j$ and $j-i \neq i-i$, therefore the above pairs of cyclotomic numbers are not identical when $i \neq j \in \mathbb{Z}_e^*$.

(iii) Finally, when for $i \neq j \in \mathbb{Z}_e^*$, $i \equiv 2j \mod e$ and $3j \equiv 0 \mod e$ hold, this means:

$$\begin{aligned}
(i,j) &= (2j,j)\\
(e-j,i-j) &= (3j-j,2j-j) = (2j,j)\\
(j-i,e-i) &= (j-2j,3j-2j) = (2j,j)\\
(j,i) &= (j,2j)\\
(e-i,j-i) &= (e-2j,j-2j) = (j,2j)\\
(i-j,e-j) &= (2j-j,e-j) = (j,2j).
\end{aligned}$$

It then immediately follows from the above that when, for $i \neq j \in \mathbb{Z}_e$, $i \equiv 2j \mod e$ and $3j \equiv 0 \mod e$, the following pairs of indicies are identical

$\{(i,j),(e-j,i-j)\}$, $\{(i,j),(j-i,e-i)\}$, $\{(e-j,i-j),(j-i,e-i)\}$, $\{(j,i),(e-i,j-i)\}$, $(j,i),(i-j,e-j)\}$ and $\{(e-i,j-i),(i-j,e-j)\}$.

We now prove that the pairs of indicies $\{(i,j),(e-j,i-j)\}$ and $\{(j,i),(i-j,e-j)\}$ are only identical when, for $i \neq j \in \mathbb{Z}_e^*$, $i \equiv 2j \mod e$ and $3j \equiv 0 \mod e$. The above pairs of cyclotomic numbers are only identical if $i = e-j$ and $j = i-j$ from the second condition, we obtain that $2j \equiv i \mod e$, therefore immediately follows that if $i \not\equiv 2j \mod e$, then these pairs of cyclotomic numbers are not equal. Moreover, suppose $i \equiv 2j \mod e$, but $3j \not\equiv 0 \mod e$, then it is clear that $i \not\equiv e-j \mod e$, and so the pairs of indicies, $\{(i,j),(e-j,i-j)\}$ and $\{(j,i),(i-j,e-j)\}$, cannot be identical when $i \not\equiv 2j \mod e$ or $3j \not\equiv 0 \mod e$.

Using an analogous proof strategy, we can demonstrate that the following pairs of indicies are identical only if $i \equiv 2j \mod e$ and $3j \equiv 0 \mod e$ $\{(i,j),(j-i,e-i)\}$, $\{(j,i),(e-i,j-i)\}$, $\{(e-j,i-j),(j-i,e-i)\}$ and $\{(e-i,j-i),(i-j,e-j)\}$.

□

Remark 2.2.19. *In case (ii), observe that as* $i = j$*, the orbit representative is automatically the cyclotomic number* $(i,i)_e$*. In case (iii), there are only two elements in* $(i,j)_e$ *and* $(j,i)_e$ *in the orbit* $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ *notice that* $i \equiv 2j \mod e$ *and* $3j \equiv 0 \mod e$ *if and only if* $j \equiv 2i \mod e$ *and* $3i \equiv 0 \mod e$.

As we have determined when the indicies of the cyclotomic numbers in $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ are identical, and when they are distinct, we can now determine the size of each orbit $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$.

Lemma 2.2.20. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = ef+1 = p^n$*, where* p *is an odd prime and* f *is even. The cyclotomic orbit* $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ *has size* 6 *except for in the following cases:*

(i) $i = j = 0$*, in which case* $|\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e| = 1$*,*

(ii) $i = j \neq 0$*, in which case* $|\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e| = 3$*,*

(iii) $i \equiv 2j \mod e$ *and* $3j \equiv 0 \mod e$*, in which case* $|\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e| = 2$

Proof. Notice that $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e = \{(i,j)_e,(j,i)_e,(e-i,j-i)_e,(e-j,i-j)_e,(j-i,e-i)_e,(i-j,e-j)_e\}$. This result is then immediate from Lemma 2.2.18. □

In the remaining part of this Subsection, we build upon previous results to determine the size of each cyclotomic orbit $\mathrm{Orb}_{\mathfrak{R}_3}(i,j)_e$. Throughout all subsequent results, it will be assumed that f is even. Note that the set $\mathfrak{R}_3$ contains all known cyclotomic numbers relations listed for f even in Theorem 1.4.12, therefore these orbits under the relations of $\mathfrak{R}_3$ are the most useful orbits explored in this Subsection when it comes to establishing new cyclotomic constructions of combinatorial objects in the f even case. In the result below, we establish the maximum possible size of each orbit $\mathrm{Orb}_{\mathfrak{R}_3}(i,j)_e$.

Theorem 2.2.21. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^n = ef + 1$, *where* $e \geq 5$ *and* p *are both odd primes and* f *is even. In the finite field* $\mathrm{GF}(e)$, *let* $C_0^{\epsilon,1} = \langle \alpha^\epsilon \rangle \cong \langle p \rangle$, *where* α *is a primitive root of* $\mathrm{GF}(e)$ *and* $n_1 = |C_0^{\epsilon,1}| = \mathrm{ord}_e(p)$ *is odd.*

- *(i) Each cyclotomic number in the orbit* $\mathrm{Orb}_{\mathfrak{R}_3}(i,j)_e$ *can be written in the form* $(ap^r, bp^r)_e$, *where* $(a,b) \in \mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ *and* $0 \leq r \leq n_1 - 1$.
- *(ii) Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = ef+1 = p^n$, *where* p *is an odd prime and* e *is prime. Then the cyclotomic orbit* $\mathrm{Orb}_{\mathfrak{R}_3}(i,j)_e$ *has order at most* $6n_1$, *where* $n_1 = \mathrm{ord}_e(p)$.

Proof. (i) By applying the relation $(i,j)_e = (ip,jp)_e$ to the cyclotomic numbers contained in the cyclotomic orbit $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ we obtain all co-orbital cyclotomic numbers of the form $(ip^u, jp^u)_e$, $(jp^v, ip^v)_e$, $((e-i)p^w, (j-i)p^w)_e$, $((e-j)p^x, (i-j)p^x)_e$, $((j-i)p^y, (e-i)p^y)_e$ and $((i-j)p^z, (e-j)p^z)_e$, where $0 \leq u, v, w, x, y, z \leq n_1 - 1$. These are precisely the cyclotomic numbers contained within the cyclotomic orbit $\mathrm{Orb}_{\mathfrak{R}_3}(i,j)_e$. To see this, observe that we may write all of the cyclotomic numbers above as a cyclotomic number in $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ with the cyclotomic relation $(i,j)_e = (ip,jp)_e$ applied to it, as a cyclotomic number of the form $(ap^r, bp^r)_e$, where $(a,b) \in \mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ and $0 \leq r \leq n_1 - 1$. By applying the relation $(i,j)_e = (j,i)_e$ to the cyclotomic number $(ap^r, bp^r)_e$, we obtain the cyclotomic number $(bp^r, ap^r)_e$, which has already been obtained by applying the relation $(i,j)_e = (ip,jp)_e$ to the element $(b,a)_e$ of the orbit $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$. Similarly, by applying the relation $(i,j)_e = (e-i, j-i)_e$ to $(ap^r, bp^r)_e$, we obtain $((e-a)p^r, (b-a)p^r)_e$, which has also already been determined by applying $(i,j)_e = (ip,jp)_e$ to an element of $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$.

(ii) By Lemma 2.2.17, the cyclotomic orbit $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ comprises at most 6 cyclotomic numbers it therefore follows by Remark 2.2.16 that $\mathrm{Orb}_{\mathfrak{R}_3}(i,j)_e$ comprises at most $6n_1$ cyclotomic numbers, where $n_1 = \mathrm{ord}_e(p)$. □

As the maximum size of each orbit $\mathrm{Orb}_{\mathfrak{R}_3}(i,j)_e$ has now been established, we now seek to determine the exact size of each orbit. Before we can do this, we require a few preliminary results.

Proposition 2.2.22. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^n = ef+1$*, where* p *is prime,* e *is prime and* f *is even. Let* n_1*, as it is definied statement of Theorem 2.2.21, be odd and let* $1 \leq m \leq e-1$*, then*

(i) if $m \in C_r^{\epsilon,1}$*, then* $-m \in C_{r+\frac{\epsilon}{2}}^{\epsilon,1}$*, where* $0 \leq r \leq \epsilon - 1$*.*

(ii) for all $0 \leq x, y \leq n_1 - 1$*,* $mp^x \not\equiv (-m)p^y \mod e$*.*

(iii) for all $1 \leq x \leq n_1 - 1$*,* $mp^{2x} \not\equiv m \mod e$*.*

Proof. (i) As $|C_0^{\epsilon,1}| = n_1$ is odd, it follows by Lemma 1.4.11 that $-1 \in C_{\frac{\epsilon}{2}}^{\epsilon,1}$. This means that if $m \in C_r^{\epsilon,1}$, then $-m = (-1)m \in C_{r+\frac{\epsilon}{2}}^{\epsilon,1}$ where $0 \leq r \leq \epsilon - 1$.

(ii) Since $C_0^{\epsilon,1} \cong \langle p \rangle$, there exist integers $0 \leq x, y \leq n_1 - 1$ such that $mp^x \equiv (-m)p^y \mod e$, if m and $-m$ are contained within the same cyclotomic class. By part (i), m and $-m$ are in distinct cyclotomic classes, we see that $mp^x \not\equiv (-m)p^y \mod e$ for all $0 \leq x, y \leq n_1 - 1$.

(iii) As $1 \leq m \leq e-1$, $m \in C_r^{\epsilon,1}$, where $0 \leq r \leq \epsilon - 1$. By Corollary 2.2.12, $|C_r^{\epsilon,1}| = \mathrm{ord}_e(p) = n_1$ meaning that n_1 is the smallest positive integer such that $mp^{n_1} \equiv m \mod e$. As n_1 is odd, there is no integer $1 \leq x \leq n_1 - 1$ such that $2x \equiv 0 \mod n_1$ by Lemma 2.2.9 as $n_1 \nmid 2x$ for $1 \leq x \leq n_1 - 1$, this means $mp^{2x} \not\equiv m \mod e$ for all $1 \leq x \leq n_1 - 1$. □

We can now use the above result to identify the conditions under which certain pairs of co-orbital cyclotomic numbers are identical to each other under the relations in $\mathfrak{R}_3$ as well as when pairs of co-orbital cyclotomic numbers are always distinct from one another under the relations in $\mathfrak{R}_3$.

Recall from Lemma 2.2.21 that for each cyclotomic number $(ap^r, bp^r)_e \in \mathrm{Orb}_{\mathfrak{R}_3}(i,j)_e$, indexed by $(ap^r, bp^r) \in \mathbb{Z}_e \times \mathbb{Z}_e$, the 2-tuple (a,b) indexes a cyclotomic number $(a,b)_e \in \mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$. Therefore, if a pair of cyclotomic numbers $((ap^r, bp^r)_e, (cp^s, dp^s)_e) \in \mathrm{Orb}_{\mathfrak{R}_3}(i,j)_e \times \mathrm{Orb}_{\mathfrak{R}_3}(i,j)_e$, then $(a,b)_e, (c,d)_e \in$

$\text{Orb}_{\mathfrak{R}_2}(i,j)_e$ and $0 \leq r, s \leq n_1 - 1$. Note that, for any pair of co-orbital cyclotomic numbers $((ap^r, bp^r)_e, (cp^s, cp^s)_e) \in \text{Orb}_{\mathfrak{R}_3}(i,j)_e \times \text{Orb}_{\mathfrak{R}_3}(i,j)_e$, there are 4 possibilities

(i) $(a,b) = (c,d) \in \text{Orb}_{\mathfrak{R}_2}(i,j)_e$ and $0 \leq r = s \leq n_1 - 1$,

(ii) $(a,b) = (c,d) \in \text{Orb}_{\mathfrak{R}_2}(i,j)_e$ and $0 \leq r \neq s \leq n_1 - 1$,

(iii) $(a,b) \neq (c,d) \in \text{Orb}_{\mathfrak{R}_2}(i,j)_e$ and $0 \leq r = s \leq n_1 - 1$,

(iv) $(a,b) \neq (c,d) \in \text{Orb}_{\mathfrak{R}_2}(i,j)_e$ and $0 \leq r \neq s \leq n_1 - 1$.

Case (i) is trivial as any cyclotomic number is identical to itself, however, determining whether a pair of cyclotomic numbers satisfying Cases (ii)-(iv) is distinct/identical requires more work. Over the next three results, we identify all pairs of co-orbital cyclotomic numbers in Cases (ii)-(iv) that are distinct under the relations in $\mathfrak{R}_3$, and we also identify when certain pairs of co-orbital cyclotomic numbers in Cases (ii)-(iv) are identical under the relations in $\mathfrak{R}_3$. Each Lemma below covers one of Cases (ii)-(iv) outlined above.

Lemma 2.2.23. *Let* $\text{GF}(q)$ *be a finite field of order* $q = ef + 1 = p^n$*, where* p *is an odd prime,* $e \geq 5$ *is prime and* f *is even. In the finite field* $\text{GF}(e)$*, let* $C_0^{\epsilon,1} = \langle \alpha^\epsilon \rangle \cong \langle p \rangle$ *and suppose* $n_1 = |C_0^{\epsilon,1}| = \text{ord}_e(p)$ *is odd. Let* $(a,b) \in \text{Orb}_{\mathfrak{R}_2}(i,j)_e$ *and let* $0 \leq r \neq s \leq n_1 - 1$*. Then the cyclotomic numbers* $(ap^r, bp^r)_e, (ap^s, bp^s)_e \in \text{Orb}_{\mathfrak{R}_3}(i,j)_e$ *are distinct.*

Proof. This result is immediate from Remark 2.2.16. □

Lemma 2.2.24. *Let* $\text{GF}(q)$ *be a finite field of order* $q = ef + 1 = p^n$*, where* p *is an odd prime,* $e \geq 5$ *is prime and* f *is even. In the finite field* $\text{GF}(e)$*, let* $C_0^{\epsilon,1} = \langle \alpha^\epsilon \rangle \cong \langle p \rangle$ *and suppose* $n_1 = |C_0^{\epsilon,1}| = \text{ord}_e(p)$ *is odd. Let* $(a,b) \neq (c,d) \in \text{Orb}_{\mathfrak{R}_2}(i,j)_e$ *and let* $0 \leq r \leq n_1 - 1$*. Then the cyclotomic numbers* $(ap^r, bp^r)_e, (cp^r, dp^r)_e \in \text{Orb}_{\mathfrak{R}_3}(i,j)_e$ *are distinct if*

(i) $\{(a,b),(c,d)\}$ *is a pair in Case (i) of Lemma 2.2.18,*

(ii) $\{(a,b),(c,d)\}$ *is a pair in Case (ii) of Lemma 2.2.18 and* $i \neq j$*,*

(iii) $\{(a,b),(c,d)\}$ *is a pair in Case (iii) of of Lemma 2.2.18.*

If $\{(a,b),(c,d)\}$ is a pair in Case (ii) of Lemma 2.2.18 and $i=j$ then $(ap^r,bp^r)_e$, $(cp^r,dp^r)_e \in \mathrm{Orb}_{\mathfrak{R}}(i,j)_e$ are identical.

Proof. Let $(ap^r,bp^r)_e,(cp^r,dp^r)_e$ be any two cyclotomic numbers satisfying $0 \leq r \leq n_1-1$, where $(a,b) \neq (c,d) \in \{(i,j),(j,i),(e-i,j-i),(e-j,i-j),(j-i,e-i),(i-j,e-j)\}$. The cyclotomic numbers $(ap^r,bp^r)_e$ and $(cp^r,dp^r)_e$ are identical if and only if $ap^r \equiv cp^r \mod e$ and $bp^r \equiv dp^r \mod e$, which is true if and only if $ap^{r-r} \equiv c \mod e$ and $bp^{r-r} \equiv d \mod e$. We can see that $ap^{r-r}=a$ and $bp^{r-r}=b$, therefore, the cyclotomic numbers $(ap^r,bp^r)_e$ and $(cp^r,dp^r)_e$ are identical if and only if the cyclotomic numbers $(a,b)_e$ and $(c,d)_e$ are identical.

Since f is even and p is prime, parts (i) and (ii) are immediate from Lemma 2.2.20.

For part (iii) notice that the pairs in Lemma 2.2.20 are identical precisely when $i \equiv 2j \mod e$ and $3j \equiv 0 \mod e$, however the second condition requires $e \mid 3j$, which is not possible since $e \geq 5$ and e is prime. This means that these pairs are not identical pairs under the above conditions. □

Theorem 2.2.25. *Let $\mathrm{GF}(q)$ be a finite field of order $q=ef+1=p^n$, where p is an odd prime, $e \geq 5$ is prime and f is even. In the finite field $\mathrm{GF}(e)$, let $C_0^{\epsilon,1} = \langle \alpha^\epsilon \rangle \cong \langle p \rangle$ and suppose $n_1 = |C_0^{\epsilon,1}| = \mathrm{ord}_e(p)$ is odd. Let $(ap^r,bp^r)_e$ and $(cp^s,dp^s)_e$ be two co-orbital cyclotomic numbers in the cyclotomic orbit $\mathrm{Orb}_{\mathfrak{R}_3}(i,j)_e$ such that $(a,b) \neq (c,d) \in \mathbb{Z}_e \times \mathbb{Z}_e$ index two cyclotomic numbers $(a,b)_e,(c,d)_e \in \mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ and $0 \leq r \neq s \leq n_1-1$. Then if*

(i) $\{(a,b),(c,d)\} \in \{(i,j),(e-i,j-i)\},\{(i,j),(i-j,e-j)\},\{(j,i)_e,(e-j,i-j)\},\{(j,i),(j-i,e-i)\}$ the cyclotomic numbers $(ap^r,bp^r)_e$ and $(cp^s,dp^s)_e$ are distinct.

(ii) $\{(a,b),(c,d)\} \in \{\{(i,j),(j,i)\},\{(e-i,j-i),(j-i,e-i)\},\{(e-j,i-j),(i-j,e-j)\}\}$ the cyclotomic numbers $(ap^r,bp^r)_e$ and $(cp^s,dp^s)_e$ are distinct.

(iii) $\{(a,b),(c,d)\} \in \{\{(e-i,j-i),(e-j,i-j)\},\{(j-i,e-i),(i-j,e-j)\}\}$ the cyclotomic numbers $(ap^r,bp^r)_e$ and $(cp^s,dp^s)_e$ are distinct.

(iv) (a) For $\{(a,b),(c,d)\} \in \{\{(i,j),(e-j,i-j)\},\{(e-j,i-j),(j-i,e-i)\},\{(j,i),(i-j,e-j)\}\}$ we have $(ap^r,bp^r)_e = (cp^s,dp^s)$ precisely if $i \equiv (-j)p^{s-r} \mod e$ and $j \equiv i(p^{s-r}+1) \mod e$.

(b) *For* $\{(a,b),(c,d)\} \in \{\{(i,j),(j-i,e-i)\},\{(j,i),(e-i,j-i)\},\{(e-i,j-i),(i-j,e-j)\}\}$ *we have* $(ap^r,bp^r)_e = (cp^s,dp^s)$ *precisely if* $i \equiv (-j)p^{r-s} \mod e$ *and* $j \equiv i(p^{r-s}+1) \mod e$.

Proof. As $0 \leq r \neq s \leq e-1$ are arbitrary, the number of distinct cases $((ap^r,bp^r)_e,(cp^s,dp^s)_e \in \mathrm{Orb}_{\mathfrak{R}_3}(i,j)_e$ depends only on the number of distinct pairs $((a,b),(c,d)) \in \mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e \times \mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$. Since there are 6 different elements in the cyclotomic orbit $\mathrm{Orb}_{\mathfrak{R}'}(i,j)_e$, there are $\binom{6}{2} = 15$ different pairs of cyclotomic numbers $(ap^r,bp^r)_e$ and $(cp^s,dp^s)_e$ in $\mathrm{Orb}_{\mathfrak{R}_3}(i,j)_e$ for which $(a,b) \neq (c,d) \in \mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ and $0 \leq r \neq s \leq n_1-1$. We account for 4 of the possibilities in part (i), 3 of the possibilities in part (ii), 2 of the possibilities in part (iii) and 6 of the possibilities in part (iv) thus all 15 possible cases of cyclotomic numbers $(ap^r,bp^r)_e$ and $(cp^s,dp^s)_e$ where $(a,b) \neq (c,d) \in \mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ and $0 \leq r \neq s \leq n_1-1$ are accounted for in this result.

(i) The cyclotomic numbers $(ip^r,jp^r)_e$ and $((e-i)p^s,(j-i)p^s)_e$, where $0 \leq r \neq s \leq n_1-1$, are identical if and only if $ip^r \equiv (e-i)p^s \mod e$ and $jp^r \equiv (j-i)p^s \mod e$. By Proposition 2.2.22, for all $0 \leq r \neq s \leq n_1-1$, $ip^r \not\equiv (e-i)p^s \mod e$ (since $e-i=-i$) this means that the cyclotomic numbers $(ip^r,jp^r)_e$ and $((e-i)p^s,(j-i)p^s)_e$ are always distinct. We can also see that this implies that the cyclotomic numbers $(jp^r,ip^r)_e$ and $((j-i)p^s,(e-i)p^s)_e$ are always distinct. Similarly, by Proposition 2.2.22, for all $0 \leq r \neq s \leq n_1-1$ $jp^r \not\equiv (e-j)p^s$ this implies that the pairs of cyclotomic numbers $\{(ip^r,jp^r)_e,((i-j)p^s,(e-j)p^s)_e\}$ and $\{(jp^r,ip^r)_e,((e-j)p^s,(i-j)p^s)_e\}$ are always distinct.

(ii) Assume that for $0 \leq r \neq s \leq n_1-1$, the cyclotomic numbers $(ip^r,jp^r)_e$ and $(jp^s,ip^s)_e$ are identical. This means that $ip^r \equiv jp^s \mod e$ and $jp^r \equiv ip^s \mod e$. By rearranging these expressions, we obtain $ip^{r-s} \equiv j \mod e$ and $j \equiv ip^{s-r} \mod e$. We can then combine the resultant equalities to give $ip^{r-s} \equiv ip^{s-r} \mod e$, which we can then multiply through by p^{r-s} to give $ip^{2(r-s)} \equiv i \mod e$. As $0 \leq r \neq s \leq n_1-1$, either $0 \leq r < s \leq n_1-1$ or $0 \leq s < r \leq n_1-1$. In the first case, $1 \leq r-s \leq n_1-1$ and so by Proposition 2.2.22, $ip^{2(r-s)} \not\equiv i \mod e$. In the second case, $-(n_1-1) \leq r-s \leq -1$. Since $p^{n_1} \equiv 1 \mod e$, $p^{r-s+n_1} \equiv p^{r-s} \mod e$, where $1 \leq r-s+n_1 \leq n_1-1$.

By Proposition 2.2.22, as $1 \leq r-s+n_1 \leq n_1-1$, $ip^{2(r-s+n_1)} \equiv ip^{2(r-s)} \not\equiv i \mod e$. Therefore, $(ip^r, jp^s)_e$ and $(jp^r, ip^s)_e$ must always be distinct.

An analogous argument can be used to show that the ensuing pairs of cyclotomic numbers must also be distinct $\{((e-i)p^r, (j-i)p^r)_e, ((j-i)p^s, (e-i)p^s)_e\}$ and $\{((e-j)p^r, (i-j)p^r)_e, ((i-j)p^s, (e-j)p^s)_e\}$ for all $0 \leq r \neq s \leq n_1-1$.

(iii) Assume that the cyclotomic numbers $((e-i)p^r, (j-i)p^r)_e$ and $((e-j)p^s, (i-j)p^s)_e$ are identical for $0 \leq r \neq s \leq n_1-1$, then this means that $(e-i)p^r \equiv (e-j)p^s \mod e$ and $(j-i)p^r \equiv (i-j)p^s \mod e$. Observe that if $0 \leq i \neq j \leq e-1$, $j-i = -(i-j)$, and so by Proposition 2.2.22 (ii) $(j-i)p^r \not\equiv (i-j)p^s \mod e$, which is a contradiction. This means that if $(j-i)p^r \equiv (i-j)p^s \mod e$ then $0 \leq i = j \leq n_1-1$. When $0 \leq i = j \leq n_1-1$, $(e-j)p^s = (e-i)p^s$ and therefore $(e-i)p^r \equiv (e-i)p^s \mod e$. By Remark 2.2.16 $(e-i)p^r \not\equiv (e-i)p^s \mod e$ for any $0 \leq r \neq s \leq n_1-1$, so therefore the cyclotomic numbers $((e-i)p^r, (j-i)p^r)_e$ and $((e-j)p^s, (i-j)p^s)_e$ are always distinct when $0 \leq r \neq s \leq n_1-1$. The same argument can be used to show that the cyclotomic numbers $((j-i)p^r, (e-i)p^r)_e$ and $((i-j)p^s, (e-j)p^s)_e$ are always distinct.

(iv) In case (a), the cyclotomic numbers $(ip^r, jp^r)_e$ and $((e-j)p^s, (i-j)p^s)_e$ are identical for $0 \leq r \neq s \leq n_1-1$, precisely if $ip^r \equiv (e-j)p^s \mod e$ and $jp^r \equiv (i-j)p^s \mod e$. These conditions can rearranged to give $i \equiv (e-j)p^{r-s} \mod e$ and $j \equiv (i-j)p^{r-s} \mod e$, which is equivalent to $i \equiv -jp^{s-r} \mod e$ and $j \equiv ip^{r-s} + i \mod e$. All other cases follow analogously. □

Remark 2.2.26. *It can be shown that $(i, j)_e$ satisfies the conditions of Theorem 2.2.25 (iv) precisely if $(a, b)_e$ also satisfies these conditions for any other $(a, b)_e$ in the orbit. Hence the condition does not depend on the choice of $(i, j)_e$.*

As we have found all pairs of conditionally identical/distinct cyclotomic numbers under the relations in $\mathfrak{R}_3$ between the three results above, we can determine the size of all cyclotomic orbits under the relations in $\mathfrak{R}_3$.

Theorem 2.2.27. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = ef + 1 = p^n$*, where* p *is an odd prime,* f *is even and* $e \geq 5$ *is prime. Moreover, in the finite field* $\mathrm{GF}(e)$*, let* $C_0^{\epsilon,1} = \langle \alpha^\epsilon \rangle \cong \langle p \rangle$*, where* $|C_0^{\epsilon,1}| = \mathrm{ord}_e(p) = n_1$ *is odd. The cyclotomic orbit* $\mathrm{Orb}_{\mathfrak{R}_3}(i,j)_e$ *has order* $6n_1$ *except in the following cases:*

(i) when $i = j = 0$*,* $\mathrm{Orb}_{\mathfrak{R}}(i,j)_e$ *has order* 1*,*

(ii) when $i = j \in \mathbb{Z}_e^*$*,* $\mathrm{Orb}_{\mathfrak{R}}(i,j)_e$ *has order* $3n_1$*,*

(iii) when $i \equiv -jp^x \mod e$ *and* $j \equiv i(p^x + 1) \mod e$ *for* $1 \leq x \leq n_1 - 1$*,* $\mathrm{Orb}_{\mathfrak{R}}(i,j)_e$ *has order* $2n_1$*.*

Proof. Part (i) follows from Lemma 2.2.20; notice that when $i = j = 0$, $\mathrm{Orb}_{\mathfrak{R}_2}(i,j)_e$ contains only 1 element, the element $(0,0)_e$. Applying the cyclotomic number relation $(i,j)_e = (ip, jp)_e$ to the cyclotomic number $(0,0)_e$ only returns the cyclotomic number $(0,0)_e$. Part (ii) is immediate from above. For part (iii) by Theorem 2.2.25 (iv) it is immediate that if there is some $0 \leq x \leq n_1 - 1$ such that $i \equiv -jp^x \mod e$ and $j \equiv i(p^x + 1) \mod e$ then

- $(ap^r, bp^r)_e = (cp^{r+x}, dp^{r+x})_e$ for $\{(a,b),(c,d)\} \in \{\{(i,j),(e-j,i-j)\},\{(e-j,i-j),(j-i,e-i)\},\{(j,i),(i-j,e-j)\}$.
- $(ap^r, bp^r)_e = (cp^{r-x}, dp^{r-x})_e$ for $\{(a,b),(c,d)\} \in \{\{(i,j),(j-i,e-i)\},\{(j,i),(e-i,j-i)\},\{(e-i,j-i),(i-j,e-j)\}$. □

I now introduce a final new definition, this is the definition of internal and external cyclotomic orbits. It is important distinguish between internal and external cyclotomic orbits as internal cyclotomic orbits can be used as tools to find new constructions of disjoint partial difference families, whilst external cyclotomic orbits may be used to construct external partial difference families. Note that the following definition discusses internal and external cyclotomic numbers; for a formal definition of these concepts, we refer the reader back to Definition 1.4.5.

Definition 2.2.28. *When a cyclotomic orbit comprises only internal cyclotomic numbers, this cyclotomic orbit is referred to as an* ***internal cyclotomic orbit****. Similarly, a cyclotomic orbit that comprises only external cyclotomic numbers, is referred to as an* ***external cyclotomic orbit****.*

Note that it is not always possible to cleanly partition the cyclotomic orbits into internal cyclotomic orbits and external cyclotomic orbits. Whilst in the f even case every orbit is either an internal cyclotomic orbit or external cyclotomic orbit, since the relations $(i,j)_e = (j,i)_e$, $(i,j)_e = (e-i, j-i)_e$ and $(i,j)_e = (ip, jp)_e$ (which are the only cyclotomic number relations that hold when f is even) relate internal cyclotomic numbers to internal cyclotomic numbers and external cyclotomic numbers to external cyclotomic numbers, the same is not true in the case where f is odd. When f is odd is the relation $(i,j)_e = (j+\frac{e}{2}, i+\frac{e}{2})_e$ relates internal cyclotomic numbers to external cyclotomic numbers (for details, see Theorem 1.4.12), therefore we can only classify cyclotomic orbits as internal and external cyclotomic orbits when f is even.

With the above definition established, we can determine the order of all internal and external cyclotomic orbits.

Corollary 2.2.29. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = ef+1 = p^n$*, where* p *is an odd prime,* f *is even and* $e \geq 5$ *is prime. Moreover, let* n_1 *(as defined in the statement of Theorem 2.2.27) be odd. Then*

(i) *(a)* *we can index:* n_1 *of the cyclotomic numbers in each internal cyclotomic orbit by* $(i,i) \in \mathbb{Z}_e \times \mathbb{Z}_e$*,* n_1 *of the cyclotomic numbers by* $(e-i, 0) \times \mathbb{Z}_e \times \mathbb{Z}_e$ *and* n_1 *of the cyclotomic numbers by* $(0, e-i) \in \mathbb{Z}_e \times \mathbb{Z}_e$*.*

(b) *all internal cyclotomic numbers are contained in internal cyclotomic orbits of order* 1 *or* $3n_1$*.*

(c) *there is* 1 *internal orbit of order* 1 *and* ϵ *internal orbits of order* $3n_1$*.*

(ii) *all external cyclotomic numbers are contained in external cyclotomic orbits of order* $2n_1$ *or* $6n_1$*.*

Proof. (i) (a) This result is immediate from the proof of Theorem 2.2.21.

(b) It is clear that $\mathrm{Orb}_{\mathfrak{R}_3}(0,0)_e = \{(0,0)_e\}$, so the internal cyclotomic number $(0,0)_e$ is contained in an orbit of order 1.

By Definition 1.4.5 the remaining internal cyclotomic numbers of order e are indexed by one of the following; $(j,j) \in \mathbb{Z}_e^* \times \mathbb{Z}_e^*$, $(j,0)_e \in \mathbb{Z}_e^* \times \mathbb{Z}_e$ or $(0,j)_e \in \mathbb{Z}_e \times \mathbb{Z}_e^*$. It follows from part (i)(a) that all cyclotomic numbers, indexed by the above, are in internal orbits of length $3n_1$.

(c) The cyclotomic orbit $\mathrm{Orb}_{\mathfrak{R}_3}(0,0)_e$ has size 1. There are then a remaining $3(e-1)$ internal cyclotomic numbers. By part (i)(b), all other internal cyclotomic orbits have order $3n_1$. There are therefore $3(e-1)$ internal cyclotomic numbers contained in orbits of order $3n_1$. It follows from this that there are $\frac{3(e-1)}{3n_1} = \frac{\epsilon n_1}{n_1} = \epsilon$ internal cyclotomic orbits of order $3n_1$.

(ii) From part (i), all orbits of the form $\mathrm{Orb}_{\mathfrak{R}_3}(i,i)_e$ of order $3n_1$ only contain internal cyclotomic numbers. Further, the only orbit of order 1 contains an internal cyclotomic number. Since by Theorem 2.2.27, all orbits when e and p are both prime and n_1 is odd are of order 1, $2n_1$, $3n_1$ or $6n_1$, it follows that the orbits of order $2n_1$ and $6n_1$ must be external cyclotomic orbits. □

In Theorem 2.2.27 we demonstrate that external cyclotomic orbit $\mathrm{Orb}_{\mathfrak{R}_3}(i,j)_e$ has order $2n_1$ when $i = -jp^x$ and $j = i(p^x+1)$. In the following Corollary we demonstrate that i and j have to lie in particular cyclotomic classes in order for this phenomenon to occur.

Corollary 2.2.30. *If $1 \leq i, j \leq e-1$ satisfy the conditions of Theorem 2.2.27 then $i \in C_r^{\epsilon,1}$ and $j \in C_{r+\frac{\epsilon}{2}}^{\epsilon,1}$ for $0 \leq r \leq \epsilon - 1$.*

Proof. Recall that $e = \epsilon n_1 + 1$, where $e \geq 5$ is an odd prime and n_1 is odd. By Lemma 1.4.11, as n_1 is odd, this means that $-1 \in C_{\frac{\epsilon}{2}}^{\epsilon,1}$. As p generates the cyclotomic class $C_0^{\epsilon,1}$, we know that if $i = -jp^x$ and $i \in C_r^{\epsilon,1}$ for some $0 \leq r \leq \epsilon - 1$, then $j \in C_{r+\frac{\epsilon}{2}}^{\epsilon,1}$. □

In fact, I have been able to do more analysis of this type to determine further results about the structure of external orbits of order $2n_1$, but it is not included in this thesis due to time and space considerations.

We have now established the size and classification of each cyclotomic orbit in a finite field $\mathrm{GF}(q)$, in which $e \geq 5$ and p are both prime, f is even and $n_1 = |\langle p \rangle|$ is odd. In the following example, we use the above results to present the size and classification of each cyclotomic orbit in $\mathrm{GF}(243)$ under the relations of $\mathfrak{R}_3$ when $e = 11$.

Example 2.2.31. *In the finite field* $\mathrm{GF}(243)$*, it is clear that* $p = 3$*. Observe that* $243 = 11(22) + 1$*. If we choose* $e = 11$*, then we satisfy the conditions that* e *is a prime greater than 5 and* f *is even. Notice that* $\langle 3 \rangle = \{1, 3, 9, 5, 4\}$ *in* $\mathrm{GF}(11)$*, it therefore follows that the elements of* $\langle 3 \rangle$ *coincide with the cyclotomic class* $C_0^{2,1} \in \mathrm{GF}(11)$*. This means that* ϵ *is equal to 2, and as* $\langle 3 \rangle$ *comprises* 5 *distinct elements, this implies* $n_1 = 5$ *and thus, we meet all the conditions of Theorem 2.2.27 and Corollary 2.2.29. It is immediate from the proof of Corollary 2.2.29 that when* $e = 11$*, each internal cyclotomic orbit* $\mathrm{Orb}_{\mathfrak{R}}(i, j)_{11}$ *has order* $3n_1$*, except for the cyclotomic orbit containing the element* $(0, 0)_{11}$*, which has order* 1*. Excluding the cyclotomic number* $(0, 0)_{11}$*, there are* 30 *internal cyclotomic numbers of order* 11 *by Corollary 2.2.29 (i)(c), as* $\epsilon = 2$*, this means there are* 2 *internal orbits of order* $3n_1 = 15$*. As follows*

$$\begin{aligned}
\mathrm{Orb}_{\mathfrak{R}}(0,0)_{11} &= \{(0,0)_{11}\}\\
\mathrm{Orb}_{\mathfrak{R}}(1,1)_{11} &= \{(1,1)_{11},(3,3)_{11},(9,9)_{11},(5,5)_{11},(4,4)_{11},(10,0)_{11},(8,0)_{11},(2,0)_{11},\\
&\qquad (6,0)_{11},(7,0)_{11},(0,10)_{11},(0,8)_{11},(0,2)_{11},(0,6)_{11},(0,7)_{11}\},\\
\mathrm{Orb}_{\mathfrak{R}}(2,2)_{11} &= \{(2,2)_{11},(6,6)_{11},(7,7)_{11},(10,10)_{11},(8,8)_{11},(9,0)_{11},(5,0)_{11},\\
&\qquad (4,0)_{11},(1,0)_{11},(3,0)_{11},(0,9)_{11},(0,5)_{11},(0,4)_{11},(0,1)_{11},(0,3)_{11}\}.
\end{aligned}$$

From Corollary 2.2.30, we need to check where there are any $i \in C_0^{2,1} = \{1, 3, 9, 5, 4\}$ *and* $j \in C_1^{2,1} = \{2, 6, 7, 10, 8\}$ *such that* $i \equiv -j3^x \mod e$ *and* $j = i(3^x + 1)$*. As there are no elements of this type, there are zero external orbits of order* $2n_1 = 10$ *in this case. The remaining* 3 *orbits of size* $6n_1 = 30$ *are*

$$\begin{aligned}
\mathrm{Orb}_{\mathfrak{R}}(1,2)_{11} &= \{(1,2)_{11},(3,6)_{11},(9,7)_{11},(5,10)_{11},(4,8)_{11},(2,1)_{11},(6,3)_{11},(7,9)_{11},\\
&\qquad (10,5)_{11},(8,4)_{11},(10,1)_{11},(8,3)_{11},(2,9)_{11},(6,5)_{11},(7,4)_{11},(1,10)_{11},\\
&\qquad (3,8)_{11},(9,2)_{11},(5,6)_{11},(4,7)_{11},(9,10)_{11},(5,8)_{11},(4,2)_{11},(1,6)_{11},\\
&\qquad (3,7)_{11},(10,9)_{11},(8,5)_{11},(2,4)_{11},(6,1)_{11},(7,3)_{11}\}\\
\mathrm{Orb}_{\mathfrak{R}}(4,5)_{11} &= \{(1,3)_{11},(3,9)_{11},(9,5)_{11},(5,4)_{11},(4,1)_{11},(3,1)_{11},(9,3)_{11},(5,9)_{11},\\
&\qquad (4,5)_{11},(1,4)_{11},(10,2)_{11},(8,6)_{11},(2,7)_{11},(6,10)_{11},(7,8)_{11},(2,10)_{11},\\
&\qquad (6,8)_{11},(7,2)_{11},(10,6)_{11},(8,7)_{11},(8,9)_{11},(2,5)_{11},(6,4)_{11},(7,1)_{11},\\
&\qquad (10,3)_{11},(9,8)_{11},(5,2)_{11},(4,6)_{11},(1,7)_{11},(3,10)_{11}\}\\
\mathrm{Orb}_{\mathfrak{R}}(3,4)_{11} &= \{(1,5)_{11},(3,4)_{11},(9,1)_{11},(5,3)_{11},(4,9)_{11},(5,1)_{11},(4,3)_{11},(1,9)_{11},\\
&\qquad (3,5)_{11},(9,4)_{11},(10,4)_{11},(8,1)_{11},(2,3)_{11},(6,9)_{11},(7,5)_{11},(4,10)_{11},\\
&\qquad (1,8)_{11},(3,2)_{11},(9,6)_{11},(5,7)_{11},(6,7)_{11},(7,10)_{11},(10,8)_{11},(8,2)_{11},\\
&\qquad (2,6)_{11},(7,6)_{11},(10,7)_{11},(8,10)_{11},(2,8)_{11},(6,2)_{11}\}.
\end{aligned}$$

2.2.1 Cyclotomic coset representatives

In the previous subsection, we determined the number of cyclotomic orbits of order e in a finite field of characteristic p. In this subsection, we shift focus slightly and determine the orbit representatives of each cyclotomic orbit in a finite field $\mathrm{GF}(q)$, where for $q = p^m = ef + 1$, $e \geq 5$ is prime, p is prime, f is even and $|\langle p \rangle| \subseteq \mathrm{GF}(e)$ is odd. Ultimately, we are interested in doing this, because knowing the cyclotomic orbit representatives in these finite fields enables us to design an algorithm for computing the cyclotomic numbers in finite fields that meet these criteria in a later chapter.

We will use the following notation throughout this subsection.

Definition 2.2.32. *The notation $\alpha_{j,\epsilon}$ is used to denote the smallest positive integer in $\mathrm{GF}(e)$ that is contained within the cyclotomic class $C_j^{\epsilon,1} = \alpha^j \langle \alpha^\epsilon \rangle$, where $C_j^{\epsilon,1} \subseteq \mathrm{GF}(e)$ and e is a prime.*

Theorem 2.2.33. *Let $\mathrm{GF}(q)$ be a finite field of order $q = p^n = ef + 1$, where p is an odd prime, $e \geq 5$ is prime and for $\langle p \rangle \subseteq \mathrm{GF}(e)^*$, $|\langle p \rangle| = n_1$ is odd. Moreover, in the finite field $\mathrm{GF}(e)$, for all $0 \leq j \leq \epsilon - 1$, let $C_j^{\epsilon,1} = \alpha^j \langle \alpha^\epsilon \rangle = \alpha^j \langle p \rangle$. The representative of each internal cyclotomic orbit of order $3n_1$ is the cyclotomic number $(\alpha_{j,\epsilon}, \alpha_{j,\epsilon})_e$.*

Proof. It follows from the proof of Corollary 2.2.29 that when p is an odd prime, f is even, $e \geq 5$ is prime and n_1 is odd, all internal cyclotomic numbers, excluding $(0,0)_e$, are contained within a cyclotomic orbit of order $3n_1$. Further, each cyclotomic orbit of order $3n_1$ contains exactly n_1 elements of the form $(ip^r, ip^r)_e$, n_1 elements of the form $((e-i)p^r, 0)_e$ and n_1 elements of the form $(0, (e-i)p^r)_e$ (where $1 \leq i \leq e-1$ and $0 \leq r \leq n_1 - 1$). Notice that $d = |i - i| = 0$, therefore the cyclotomic number $(i,i)_e$ with smallest $0 \leq i \leq e-1$ is the representative of each orbit of order $3n_1$.

Moreover, it follows by the proof of Corollary 2.2.29 that two cyclotomic numbers $(ip^r, ip^r)_e$ and $(ip^s, ip^s)_e$ where $0 \leq r \neq s \leq n_1 - 1$ are only equivalent to one another under the relation $(i,j)_e = (ip, jp)_e$. It therefore follows that ip^r and ip^s (where $0 \leq r \neq s \leq n_1 - 1$) must be contained within the same cyclotomic coset $\mathbb{C}_i = \{i, ip, \ldots, ip^{n_1}\}$. By Corollary 2.2.12, each cyclotomic coset $\mathbb{C}_i$ is equivalent to some cyclotomic class $C_j^{\epsilon,1}$, where $\epsilon = \frac{e-1}{\mathrm{ord}_e(p)}$ and $i \in C_j^{\epsilon,1}$. It therefore follows that the smallest cyclotomic number $(i,i)_e$ in each cyclotomic orbit of order $3n_1$

corresponds to the cyclotomic number $(\alpha_{j,\epsilon}, \alpha_{j,\epsilon})$, where $\alpha_{j,\epsilon}$ is smallest element of the cyclotomic class $C_j^{\epsilon,1}$. □

Example 2.2.34. *Let* GF(243) *and choose* $e = 11$*. Note that in this finite field,* $p = 3$*. It follows from Example 2.2.31 that there are two internal orbits of order* $3n_1 = 15$*: the orbit representatives of these orbits are* $(1, 1)_{11}$ *and* $(2, 2)_{11}$*.*
Observe that in the finite field GF(11)*,* $\alpha = 6$ *is a primitive element of this finite field. Moreover,* $\alpha^2 = 3 \mod 11$*, therefore* $C_0^{2,1} = \langle \alpha^2 \rangle = \{3, 9, 5, 4, 1\} = \langle 3 \rangle$ *in* GF(11)*. It follows that in* GF(11)*,* $\alpha_{0,2} = 1$*, this corresponds to the orbit representative* $(1, 1)_{11}$*. Further, the only other cyclotomic class of order* 2 *in* GF(11) *is the cyclotomic class* $C_1^{2,1} = \{6, 7, 10, 8, 2\}$ *and it is clear that* $\alpha_{1,2} = 2$*, where* $(\alpha_{1,1}, \alpha_{1,1})_{11}$ *corresponds to the cyclotomic number* $(2, 2)_e$*.*

At this present time, I have not been able to replicate these results to find the cyclotomic orbit representatives for all external cyclotomic orbits.

Chapter 3

Cyclotomic constructions of DPDFs and EPDFs

In this Chapter, we utilise the cyclotomic frameworks developed in Chapter 2, to establish further DPDF and EPDF constructions. As mentioned in the introductory chapter, field cyclotomy has long since been an established tool for constructing various types of difference family with more recent papers in this area centering around finding new constructions of DDFs and EDFs (see for example [14],[16]). As DPDFs generalise DDFs and EDFs, the results in this Chapter extend previous DDF and EDF constructions. We also able to extend some more historic difference family results, for example, one of our results expands upon the main PDS result in [4].

This Chapter is organised as follows in the first Section of this Chapter, we explore cyclotomic PDS constructions, which we use in subsequent Sections to inform new DPDF and EPDF constructions. In the second Section of this Chapter, we utilise the PDS constructions found in Section 1 to identify new DPDF/EPDF constructions, in which the component sets of the DPDFs are individually PDSs. In Section 3, we construct DPDFs and EPDFs by partitioning cyclotomic PDSs into smaller cyclotomic classes. In Sections 4 and Section 5, we look at partitions of the squares into cyclotomic classes with small values of e and f respectively. Finally, in Section 6, we look at a standalone cyclotomic PDS/DPDF construction obtained using cyclotomic orbits. The results in Sections 1 to 4 are from the paper [34], while Section 5 largely contains results from the upcoming preprint [40].

3.1 PDS constructions for small e

As demonstrated in the Introduction, PDSs can be used to construct DPDFs and EPDFs in two different ways we can partition PDSs into DPDFs/EPDFs and we can also construct DPDFs (and EPDFs) from collections of PDSs. In this Section we therefore explore cyclotomic constructions of PDSs, as we utilise these results in later Sections to find new cyclotomic constructions of DPDFs and EPDFs.

Throughout this Section, we investigate when a particular cyclotomic class $C_0^{e,m} \subseteq \mathrm{GF}(q)$, where $q = ef + 1$, forms a PDS. (In a later Chapter we construct PDSs from unions of cyclotomic classes.) We begin this Section by looking at some key results in the papers [60] and [67] which provide insight into when C_0^e is/isn't a Difference Set. In the second part of this section, we explore the conditions under which C_0^e is a PDS for small, selected values of e (namely the values $e = 2, 3, 4, 6, 8$). Finally, in the last part of this Section, we include some more general PDS results that depend on the relation between e and f, as opposed to evaluating specific cyclotomic numbers. All results in this Section are recorded in my joint paper with my supervisor [34].

The result below is a concatenation of results from [60] and [67]. The book [60] is the earliest known resource to explore cyclotomic constructions of Difference Sets, and hence contains many interesting results about when $C_0^{e,m}$ is a Difference Set. However, in [60], most of the results are predicated on q being an odd prime power. The paper [67] is a more up to date resource which establishes new results, including results where q is an even prime power. (Note that since it was demonstrated by Remark 1.3.4 that we can view any cyclotomic Difference Set as being a PDS, we can also use Difference Sets to inform DPDF/EPDF constructions.)

Theorem 3.1.1. *Let $q = p^m = ef + 1$ be a prime power.*

(i) If q is even then $C_0^{e,m}$ is not a Difference Set for any value of e.

(ii) If q is odd and $C_0^{e,m}$ is a Difference Set, then e must be even and f must be odd.

(iii) If $q = 2f + 1 \equiv 3 \mod 4$, then $C_0^{2,m}$ is a Difference Set.

(iv) If $q = 4f + 1$ then $C_0^{4,m}$ is a Difference Set if and only if $q = 1 + 4t^2$ and t is odd.

(v) When $q = 6f + 1$ then $C_0^{6,m}$ is not a Difference Set.

(vi) If $q = 8f + 1$ then $C_0^{8,m}$ is a Difference Set if and only if q admits the simultaneous representations $q = 9 + 64y^2 = 1 + 8b^2$, where $y \equiv b \equiv 1 \mod 2$.

We now look at when $C_0^{e,m}$ is a PDS. We begin by looking at when $C_0^{e,m}$ is a PDS for small values of e.

The result below covers the case $e = 2$. (Notice that part Theorem 3.1.2(ii) is a rewriting of Theorem 3.1.1(iii).) Proposition 3.1.2 was first recorded in [60], but is essentially a rewrite of Paley's classical PDS construction in [56] in cyclotomic notation.

Proposition 3.1.2. *Let* GF(q) *be a finite field, where $q = p^s = 2f + 1$. Then $C_0^{2,s}$ is a*

(i) $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$-PDS if $q \equiv 1 \mod 4$,

(ii) $(q, \frac{q-1}{2}, \frac{q-3}{4})$-Difference Set if $q \equiv 3 \mod 4$.

We now establish similar results for $e \in \{3, 4, 6, 8\}$. The cycltomic number expressions quoted below in Theorem 3.1.3 have been taken from the following sources: [25], [42], [43], [60] and [67]. For a full list of internal cyclotomic number expressions when $e \in \{3, 4, 6, 8\}$ see Appendix A. The notion of a proper representation is a number theoretic technicality, for further information on proper representation, see the formal definition presented in Appendix A.

Theorem 3.1.3. *Let* GF(q) *be a finite field, where $q = p^m = ef + 1$. Suppose f is even:*

(i) when $e = 3$, then $q = p^m \equiv 1 \mod 3$ and $4q = c^2 + 27d^2$ is the unique proper representation of $4q$ with $c \equiv 1 \mod 3$. It follows that $C_0^{3,m}$ is a PDS if and only if $d = 0$. The parameters of this PDS are $(q, \frac{q-1}{3}, \frac{q-8+c}{9}, \frac{2q-4-c}{18})$ and $C_0^{3,m}$ is a proper PDS if it is non-trivial. The case $d = 0$ holds precisely when $q = p^m$, such that $p \equiv 2 \mod 3$ and m is even.

(ii) when $e = 4$, then $q = p^m \equiv 1 \mod 4$ and $q = s^2 + 4t^2$ is the unique proper representation of q with $s \equiv 1 \mod 4$. It follows that $C_0^{4,m}$ is a PDS if and

only if $t = 0$. *The parameters of this PDS are* $(q, \frac{q-1}{4}, \frac{q-11-6s}{16}, \frac{q-3+2s}{16})$. *The case* $t = 0$ *holds precisely when* $q = p^m$, *such that* $p \equiv 3 \mod 4$ *and* m *is even.*

(iii) when $e = 6$, *then* $q = p^m \equiv 1 \mod 6$ *and* $q = s^2 + 3t^2$ *is the unique proper representation of* q *with* $s \equiv 1 \mod 3$, *then* $C_0^{6,m}$ *is a proper PDS if and only if* $t = 0$. *The parameters of this PDS are* $(q, \frac{q-1}{6}, \frac{q-17-20s}{36}, \frac{q-5+4s}{36})$. *The case* $t = 0$ *holds precisely when* $q = p^m$, *such that* $p \equiv 5 \mod 6$ *and* m *is even.*

(iv) when $e = 8$, *then* $q = p^m \equiv 1 \mod 8$ *and* $q = x^2 + 4y^2 = a^2 + 2b^2$ *are the unique proper representations of* q *with* $x \equiv a \equiv 1 \mod 4$, *then* $C_0^{8,m}$ *is a proper PDS if and only if* $x = a$ *and* $y = b = 0$. *The parameters of this PDS are* $(q, \frac{q-1}{6}, \frac{q-23-42x}{64}, \frac{q-7+6x}{64})$. *The case* $x = a$ *and* $y = b = 0$ *holds precisely when* $q = p^m$, *such that* $p \equiv 7 \mod 8$ *and* m *is even.*

Proof. (i) For the forwards direction, note that if $C_0^{3,m}$ is a $(q, \frac{q-1}{3}, \lambda, \mu)$-PDS, then by Lemma 2.1.2 (ii), $\lambda = (0,0)_3$ and $\mu = (1,0)_3 = (2,0)_3$. By Theorem A.0.2, if $(1,0)_3 = (2,0)_3$ then this implies

$$\frac{2q-4-c-9d}{18} = \frac{2q-4-c+9d}{18}.$$

The above equality is satisfied precisely when $d = 0$. For the reverse direction, observe that if $d = 0$, by Theorem A.0.2, this means that $p \equiv 2 \mod 3$. This means that $p^1 \equiv -1 \mod 3$ and so it then follows by Lemma 2.1.20 and Theorem 1.4.7 that the cyclotomic numbers of order 3 are uniform in this case, and thus $C_0^{3,m}$ is a PDS. By Theorem A.0.2, when $d = 0$, $\lambda = (0,0)_3 = \frac{q-8+c}{9}$ and $\mu = (1,0)_3 = (2,0)_3 = \frac{2q-4-c}{18}$. It follows that $\lambda = \frac{q-8+c}{9} = \frac{2q-4-c}{18} = \mu$ only when $c = 4$, $q = 4$, which is the trivial case (meaning that $C_0^{3,m}$ is always proper except for in the trivial case).

(ii) For the forwards direction, take the appropriate case from Theorem A.0.3 the rest of the proof is then analogous to the proof of part (i). This result was stated without proof in [49].

(iii) By Corollary 2.1.16, if C_0^6 is a proper PDS, then $2 \in C_0^{6,m}$ this determines the cyclotomic number formulae that we require from Theorem A.0.4 for this proof. Both the forwards and reverse directions of this proof are then analogous to the proof of part (i). The parameters can be obtained from Theorem A.0.4.

(iv) It follows from Corollary 2.1.16 that if $C_0^{8,m}$ is a PDS, then f is even and $2 \in C_0^{8,m}$ this determines the cyclotomic formulae from Theorem A.0.5 that should be used in the forwards direction of this proof. For the reverse direction, observe that when $y = 0$, $p \equiv 3 \mod 4$ and when $b = 0$, $p \equiv 5, 7 \mod 8$, so $y = b = 0$ implies $p \equiv 7 \mod 8$. Both directions of this proof are otherwise analogous to the proof of part (i). The parameters can be obtained from Theorem A.0.5. □

We now end this Section with two results that depend upon the relation between e and f, and therefore do not require evaluation of small cyclotomic numbers.

Proposition 3.1.4. *(i) Let $q = p^m$, where $m > 1$. For $r \mid m$ (where $r \neq m$), let F_r be the subfield $\mathrm{GF}(p^r)$ of $\mathrm{GF}(q)$ then F_r^* is the cyclotomic class $C_0^{e,m}$ of $\mathrm{GF}(q)$, where $e = \frac{q-1}{p^r-1}$.*

(ii) Let $q = p^m = ef + 1$. Then $C_0^{e,m}$ is a $(q, f, f-1, 0)$-PDS if and only if $C_0^{e,m} \cup \{0\}$ is a subfield of $\mathrm{GF}(q)$. Here, q is a prime power, $e = \frac{q-1}{p^r-1}$ and $f = p^r - 1$.

Proof. (i) As F_r is a subfield of $\mathrm{GF}(q)$, it follows that F_r^* is a multiplicative subgroup of $\mathrm{GF}(q)^*$. As $\mathrm{GF}(q)^*$ is the multiplicative group of a finite field, $\mathrm{GF}(q)^*$ is cyclic. It then follows by the fundamental theorem of cyclic groups that F_r^* is the unique multiplicative subgroup of index e of $\mathrm{GF}(q)^*$ up to isomorphism. Moreover, since F_r has order p^r, F_r^* has order $p^r - 1$, and so $e = \frac{q-1}{p^r-1}$.

(ii) For the forwards direction, assume $C_0^{e,m}$ is a $(q, f, f-1, 0)$-PDS. It immediately follows by Theorem 1.3.19 (vi) that $C_0^{e,m} \cup \{0\}$ is an additive subgroup of $\mathrm{GF}(q)$. By definition, every cyclotomic class $C_0^{e,m}$ is a multiplicative subgroup of $\mathrm{GF}(q)^*$. It therefore follows that $C_0^{e,m} \cup \{0\}$ is a subfield of $\mathrm{GF}(q)$. For the reverse direction, notice that if $C_0^{e,m} \cup \{0\}$ is a subfield of $\mathrm{GF}(q)$, then we can view $C_0^{e,m} \cup \{0\}$ as an additive subgroup of $\mathrm{GF}(q)$. It then follows by Theorem 1.3.19 (v) that $C_0^{e,m} \cup \{0\}$ is a $(q, f+1, f+1, 0)$-PDS in GF(q). Since $\Delta(C_0^{e,m}, 0) = \Delta(C_0^{e,m}) \cup \Delta(C_0^{e,m}, 0) \cup \Delta(0, C_0^{e,m})\, (\cup\, \Delta(0,0))$, and $\Delta(C_0^{e,m}, 0) = \Delta(0, C_0^{e,m}) = C_0^{e,m}$, observe that $\Delta(C_0^{e,m}) = (f-1)C_0^{e,m}$. It therefore follows that $C_0^{e,m}$ is a $(q, f, f-1, 0)$-PDS. The values of e and f can be obtained from part (i). □

The final result in this Section demonstrates that a PDS must consist of the non-identity elements of a subfield of GF(q) if $e > f$ and $C_0^{e,m}$ cannot consist entirely of the non-identity elements of a subfield otherwise.

Theorem 3.1.5. *Let $q = p^m = ef + 1$. Suppose that $C_0^{e,m}$ is a proper (q, f, λ, μ)-PDS. Then*

(i) if $e > f$ then $C_0^{e,m} \cup \{0\}$ is a subfield of GF(q).

(ii) if $e < f$ then $C_0^{e,m} \cup \{0\}$ is not a subfield of GF(q) *and $\mu \geq 1$.*

(iii) the case where $e = f$ cannot occur for $f > 2$.

Proof. When $C_0^{e,m}$ is a proper (q, f, λ, μ)-PDS, the following multiset equation must hold

$$\Delta(C_0^{e,m}) = \lambda(C_0^{e,m}) \cup \mu(\mathrm{GF}(q)^* \backslash C_0^{e,m}).$$

Since the set $C_0^{e,m}$ has cardinality f, this means that $|\Delta(C_0^{e,m})| = f(f-1)$ and $|\mathrm{GF}(q)^* \backslash C_0^{e,m}| = q - 1 - f = (ef+1) - 1 - f = f(e-1)$. This then implies that

$$f(f-1) = \lambda(f) + \mu(f(e-1)).$$

By dividing each term by f, we find

$$f - 1 = \lambda + \mu(e-1). \tag{3.1}$$

(i) When $e > f$, as λ and μ are both non-negative integers, it follows immediately from Equation 3.1 that $\mu = 0$. By Proposition 3.1.4 (ii), as $\mu = 0$, $C_0^{e,m}$ is a subfield of GF(q).

(ii) It follows from the proof of Proposition 3.1.4 (ii) that if $C_0^{e,m} \cup \{0\}$ is a subfield, then $|C_0^{e,m}| = p^r - 1 = f$ and $e = \frac{p^m-1}{p^r-1}$ for some $r \mid m$ it follows that we can write $m = rk$ for some $k \in \mathbb{N}$. This in turn means that we can write $e = \frac{p^m-1}{p^r-1} = (p^r)^{k-1} + (p^r)^{k-2} + \ldots + (p^r) + 1 > p^r - 1 = f$. When $e < f$, we therefore get a contradiction, so $C_0^{e,m}$ is not a subfield if $e < f$.

(iii) Suppose that $e = f > 2$. By substituting $e = f$ into Equation 3.1, we obtain the expression $f - 1 = \lambda + \mu(f - 1)$. Since λ and μ are both non-negative, this means that $\mu \in \{0, 1\}$. When $\mu = 0$, this forces $\lambda = f - 1$, meaning that $C_0^{e,m}$ is a $(q, f, f - 1, 0)$-PDS. By Proposition 3.1.4, as $C_0^{e,m}$ is a $(q, f, f - 1, 0)$-PDS, this means that $C_0^{e,m}$ consists of the non-identity elements of a subfield. However, we can see from the proof of part (ii) that if $C_0^{e,m}$ is a subfield, then $e = \frac{p^m-1}{p^r-1} > p^r - 1 = f$, which is a contradiction, so $\mu \neq 0$. This leaves the case $\mu = 1$. Notice that when $\mu = 1$, this means that $\lambda = 0$ and $C_0^{e,m}$ is a $(q, f, 0, 1)$-PDS. This means that the multiset $\Delta(C_0^{e,m})$ consists of 1 copy of each cyclotomic class $C_i^{e,m}$ for $1 \leq i \leq e-1$ and no copies of $C_0^{e,m}$. Notice by Lemma 2.1.2 that we may write $\Delta(C_0^{e,m}) = \bigcup_{r=1}^{f-1} T_r$, where each transversal is a copy of the cyclotomic class C_{a_r} $(0 \leq a_r \leq e - 1)$. By Corollary 2.1.16, as $C_0^{e,m}$ is a proper PDS, this means that $q \equiv 1 \mod 2e$, it then follows by from Corollary 2.1.11 that for all $1 \leq s \neq \frac{f}{2} \leq f - 1$, $T_s = C_{a_r} = T_{f-s}$. Therefore, for any $r \neq \frac{f}{2}$, there are at least 2 copies of $C_{a_r}^{e,m}$, a contradiction unless $f = 2$. When $e = f = 2$, then $q = 5$ and $C_0^{2,1}$ is a $(5, 2, 0, 1)$-PDS. Otherwise $\mu \neq 1$, and therefore $e \neq f$. □

Notice that if $q = p^m = ef + 1$ and $e > f$, then $C_0^{e,m}$ is only a proper PDS when $m \geq 2$. When $m = 1$, this means q is prime and therefore the only subfield is the trivial subfield.

3.2 DPDF/EPDF constructions from unions of PDSs

In this Section, we use the PDS constructions identified in the previous Section to construct DPDFs in which the component sets are individually PDSs. When the DPDFs also partition larger PDSs, we are also able to obtain EPDF constructions.

Our first result in this Section follows from Theorem 3.1.5 in the last section.

Proposition 3.2.1. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^m = ef + 1$*, where* $m > 1$*. For* $r \mid m$*, let* $C_i^{e,m}$ *be the* i^{th} *cyclotomic class of order* $e = \frac{q-1}{p^r-1}$*, where* $0 \leq i \leq e-1$*. Let* S' *consist of any collection of* u *sets amongst the cyclotomic classes* $\{C_0^{e,m}, \ldots, C_{e-1}^{e,m}\}$*. Then*

(i) S' *is a* $(q, u, p^r - 1, p^r - 2, 0)$*-DPDF,*

(ii) if $u = e - 1$*,* S' *is also a* $(q, u, p^r - 1, q - 3p^r + 2, q - p^r)$*-EPDF.*

Proof. (i) By Theorem 3.1.5, the cyclotomic class $C_0^{e,m}$ is a $(q, f, f-1, 0)$-PDS: meaning that $\Delta(C_0^{e,m}) = (f-1)C_0^{e,m}$ by Definition 1.3.1. It then follows by Lemma 2.1.2(iii) that for $0 \leq j \leq e-1$, $C_j^{e,m} = \alpha^j C_0^{e,m} = \alpha^j (f-1) C_0^{e,m} = (f-1)C_j^{e,m}$, hence it follows by Definition 1.3.1 that for each $0 \leq j \leq e-1$, $C_j^{e,m}$ is a $(q, f, f-1, 0)$-PDS. It is then immediate by Theorem 1.3.20 that S' is a DPDF.

(ii) This is immediate from Theorem 1.3.21 and Theorem 1.3.20. □

Theorem 3.2.2. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^{2m} = ef + 1$*, where* $e \in \{3, 4, 6, 8\}$*. Further, let* $I \subseteq \{0, 1, \ldots, e-1\}$ *(where* $|I| = u$ *and* $2 \leq u \leq e-1$*) and* $D' = \{C_i^{e,2m}\}_{i \in I}$*. If* $C_0^{e,2m}$ *is a PDS (with parameters* $(q, \frac{q-1}{e}, \eta^2 - (e-3)\eta - 1, \eta^2 + \eta)$*) then* D' *is a* $(q, u, \frac{q-1}{e}, u\eta^2 + (u+2-e)\eta - 1, u(\eta^2 + \eta))$*-DPDF and a* $(q, u, \frac{q-1}{e}, u(u-1)\eta^2 + 2(u-1)\eta, u(u-1)\eta^2)$*-EPDF (where* $\eta = \frac{(-p)^m - 1}{e}$*).*

Proof. Observe that in each part of Theorem 3.1.3 it is demonstrated that $C_0^{e,m}$, where $e \in \{3, 4, 6, 8\}$, is a PDS precisely when $q = p^m$, where $p \equiv -1 \mod e$ and m is even. It is then immediate from Lemma 2.1.20 and Theorem 2.1.21 that each cyclotomic class $C_i^{e,2m}$ is $(q, \frac{q-1}{e}, \eta^2 - (e-3)\eta - 1, \eta^2 + \eta)$-PDS (where $0 \leq i \leq e-1$) and that D' is both a $(q, u, \frac{q-1}{e}, u\eta^2 + (u+2-e)\eta - 1, u(\eta^2 + \eta))$-DPDF and a $(q, u, \frac{q-1}{e}, u(u-1)\eta^2 + 2(u-1)\eta, u(u-1)\eta^2)$-EPDF (where $\eta = \frac{(-p)^m - 1}{e}$). □

Example 3.2.3. *Let* $q = 9$*,* $e = 4$ *and* $f = 2$*. Notice that* $q = 3^2$*, where* $3 \equiv -1 \mod 4$*, therefore for each* $0 \leq i \leq 3$*, the cyclotomic class* $C_i^{4,2}$ *is a* $(9, 2, 1, 0)$*-PDS. When* $u = 2$*,* D' *is both a* $(9, 2, 2, 1, 0)$*-DPDF and* $(9, 2, 2, 0, 2)$*-EPDF. When* $u = 3$*,* D' *is both a* $(9, 3, 2, 1, 0)$*-DPDF and* $(9, 3, 2, 2, 6)$*-EPDF. When* $u = 4$*, then* D' *is both a* $(9, 4, 2, 1)$*-DDF and a* $(9, 4, 2, 6)$*-EDF.*

3.3 DPDF/EPDF partition constructions

In this Section, we develop new DPDF and EPDF constructions by partitioning cyclotomic PDSs into collections of smaller cyclotomic classes. It is possible to identify DPDF and EPDF constructions of this type when, for a finite field GF(q), we may write $q = p^m = \epsilon\rho + 1 = ef + 1$, where $\epsilon \mid e$ we can then partition the cyclotomic class $C_0^{\epsilon,m}$ into the following set of cyclotomic classes of order e $\{C_0^{e,m}, C_\epsilon^{e,m}, \ldots, C_{e-\epsilon}^{e,m}\}$.

Similar construction techniques have been used in the literature to establish new DDF and EDF constructions (see for example Proposition 1.3.9 from the paper [14], or the papers [16] and [32]). Many of these constructions are special cases of the constructions explored in this Section. Note that all results recorded in this Section are from the paper [34].

We begin this Section by identifying all DPDFs and EPDFs that partition Difference Sets. Recall that we defined ϕ_i in Definition 2.1.7.

Theorem 3.3.1. *Let* GF(q) *be a finite field of order* $q = p^m = \epsilon\rho + 1 = ef + 1$, *where* $\epsilon \mid e$. *Let* $C_0^{\epsilon,m}$ *be a* $(q, \frac{q-1}{\epsilon}, \lambda)$*-Difference Set* ($\lambda = \frac{q-1-\epsilon}{\epsilon^2}$) *and denote by* $(C_0^{\epsilon,m})' = \{C_0^{e,m}, C_{e,m}^{e,m}, \ldots, C_{e-\epsilon}^{e,m}\}$.

(i) If $\phi_i \neq \phi_j$ *for some distinct* $i, j \in \{1, \ldots, \epsilon - 1\}$ *then* $(C_0^{\epsilon,m})'$ *is not a DPDF or an EPDF.*

(ii) Otherwise, $(C_0^{\epsilon,m})'$ *is a* $(q, \frac{e}{\epsilon}, f, \frac{f-1}{\epsilon})$*-DDF and a* $(q, \frac{e}{\epsilon}, f, \frac{(e-\epsilon)f}{\epsilon^2})$*-EDF.*

It follows that $(C_0^{\epsilon,m})'$ *is never a proper DPDF nor a proper EPDF.*

Proof. (i) By Theorem 2.1.9(iii), if $\phi_i \neq \phi_j$ for some distinct $i, j \in \{1, \ldots, \epsilon-1\}$ then $(C_0^{\epsilon,m})'$ is not a DPDF and therefore not an EPDF.

(ii) As $C_0^{\epsilon,m}$ is a Difference Set, it follows by Theorem 3.1.1 that q must be odd, ϵ must be even and ρ must be odd. It is then immediate from Corollary 2.1.16 that $(C_0^{\epsilon,m})'$ is either a DDF or not a DPDF (i.e. $(C_0^{\epsilon,m})'$ cannot be a proper DPDF). Since $\phi_0 = \phi_{\frac{\epsilon}{2}}$, this means $\phi_0 = \phi_1 = \ldots = \phi_{\epsilon-1}$, hence $(C_0^{\epsilon,m})'$ is a DDF and $C_0^{\epsilon,m}$ is a Difference Set, it follows by Lemma 1.2.4 that $(C_0^{\epsilon,m})'$ is also an EDF.

For the parameters note that $|C_0^{\epsilon,m}| = \rho = \frac{q-1}{\epsilon}$, therefore $|\Delta(C_0^{\epsilon,m})| = \frac{q-1}{\epsilon}(\frac{q-1}{\epsilon} - 1) = \frac{q-1}{\epsilon}\frac{q-1-\epsilon}{\epsilon}$. As $C_0^{\epsilon,m}$ is a Difference Set, it follows that each of the $(q-1)$ elements of $\mathrm{GF}(q)^*$ occurs an equal number of times in the multiset $\Delta(C_0^{\epsilon,m})$. It therefore follows that $\lambda = \frac{q-1-\epsilon}{\epsilon^2}$. Similarly, since there are $f-1$ diagonals of transversals in $\mathrm{Int}((C_0^{\epsilon,m})')$, and each cyclotomic class of $C_0^{\epsilon,m}$ occurs at equal frequency in $\mathrm{Int}((C_0^{\epsilon,m})')$, it follows that $\mathrm{Int}((C_0^{\epsilon,m})') = (\frac{f-1}{\epsilon})\mathrm{GF}(q)^*$. It is then immediate from Lemma 1.2.4 that $\mathrm{Ext}((C_0^{\epsilon,m})') = (\lambda - \frac{f-1}{\epsilon})\mathrm{GF}(q)^* = (\frac{q-1-\epsilon}{\epsilon^2} - \frac{f-1}{\epsilon})\mathrm{GF}(q)^* = \frac{(e-\epsilon)f}{\epsilon^2}$. □

The following two specific partition results follow as an immediate consequence of Theorem 3.3.1. The first of these results has been recorded in [32] and [62] (as well as in [34]).

Corollary 3.3.2. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^m = ef + 1 \equiv 3 \mod 4$*, where* e *is even. Let* $C_0^{2,m}$ *denote the set of squares and let* $(C_0^{2,m})' = \{C_0^{e,m}, C_2^{e,m}, \ldots, C_{e-2}^{e,m}\}$*. Then* $(C_0^{2,m})'$ *is always a* $(q, \frac{e}{2}, f, \frac{f-1}{2})$*-DDF and a* $(q, \frac{e}{2}, f, \frac{(e-2)f}{4})$*-EDF.*

Proof. Case (i) of Theorem 3.3.1 is always impossible when $\epsilon = 2$, since the only integer in the range $[1, \epsilon - 1]$ is 1. It therefore follows by Theorem 3.3.1 that $(C_0^{2,m})'$ is always a $(q, \frac{e}{2}, f, \frac{f-1}{2})$-DDF and a $(q, \frac{e}{2}, f, \frac{(e-2)f}{4})$-EDF. □

Corollary 3.3.3. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^m = ef + 1 \equiv 1 \mod 4$*, where* $4 \mid e$*, such that* $q = 1 + 4t^2$ *is the unique proper representation of* q *and* t *is odd. Let* $(C_0^{4,m})' = \{C_0^{e,m}, C_4^{e,m}, \ldots, C_{e-4}^{e,m}\}$*. If* $\phi_1 = \phi_2 = \phi_3$*, then* $(C_0^{4,m})'$ *is a* $(q, \frac{e}{4}, f, \frac{f-1}{4})$*-DDF and a* $(q, \frac{e}{4}, f, \frac{(e-4)f}{16})$*-EDF.*

Proof. By Theorem 3.1.1 when $q = 1+4t^2$ and t is odd, then $C_0^{4,m}$ is a $(q, \frac{q-1}{4}, \frac{q-5}{16})$-Difference Set. It then immediately follows from Theorem 3.3.1 that $(C_0^{4,m})'$ is a DDF. □

Example 3.3.4. *A* $(2917, 81, 9, 2)$*-DDF and* $(2917, 81, 9, 180)$*-EDF was constructed by computational checking in [16]. Since* $q = 2917 = 1+4(27)^2$*, this is an example of the construction in Corollary 3.3.3.*

In the following result, we now consider partitions of proper PDSs.

Theorem 3.3.5. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^m = \epsilon\rho + 1 = ef + 1$*, where* $\epsilon \mid e$*. Let* $C_0^{e,m}$ *be a proper* $(q, \frac{ef}{\epsilon}, \lambda, \mu)$*-PDS and denote* $(C_0^{\epsilon,m})' = \{C_0^{e,m}, C_\epsilon^{e,m}, \ldots, C_{e-\epsilon}^{e,m}\}$*.*

(i) If $\phi_i \neq \phi_j$ *for some distinct* $i, j \in \{1, \ldots, \epsilon - 1\}$*, then* $(C_0^{\epsilon,m})'$ *is neither a DPDF nor an EPDF.*

Otherwise assume that $\phi_i = \phi_j$ *for all* $i, j \in \{1, \ldots, \epsilon - 1\}$ *and let* $\kappa = \phi_1 - \phi_0$ *then*

(ii) when $\kappa = 0$*,* $(C_0^{\epsilon,m})'$ *is a* $(q, \frac{e}{\epsilon}, f, \frac{f-1}{\epsilon})$*-DDF and a* $(q, \frac{e}{\epsilon}, f, \lambda - \frac{f-1}{\epsilon}, \mu - \frac{f-1}{e})$*-EPDF.*

(iii) when $\kappa = \mu - \lambda$*,* $(C_0^{\epsilon,m})'$ *is a* $(q, \frac{e}{\epsilon}, f, \lambda - \frac{(e-\epsilon)f}{\epsilon^2}, \mu - \frac{(e-\epsilon)f}{\epsilon^2})$*-DPDF and a* $(q, \frac{e}{\epsilon}, f, \frac{(e-\epsilon)f}{\epsilon^2})$*-EDF.*

(iv) when $\kappa \notin \{0, \mu - \lambda\}$ *then* $(C_0^{\epsilon,m})'$ *is a proper* $(q, \frac{e}{\epsilon}, f, \phi_0, \phi_0 + \kappa)$*-DPDF and a proper* $(q, \frac{e}{\epsilon}, f, \lambda - \phi_0, \mu - \phi_0 - \kappa)$*-EPDF.*

Proof. By Lemma 1.2.4, since $C_0^{\epsilon,m}$ is a $(q, \frac{ef}{\epsilon}, \lambda, \mu)$-PDS, it follows that

$$\mathrm{Int}((C_0^{\epsilon,m})') + \mathrm{Ext}((C_0^{\epsilon,m})') = \lambda C_0^{\epsilon,m} \cup \mu(\mathrm{GF}(q)^* \backslash C_0^{\epsilon,m}).$$

(i) By Theorem 2.1.9, it is necessary for $\phi_i = \phi_j$ for all $i, j \in \{1, \ldots, \epsilon - 1\}$ in order for $(C_0^{\epsilon,m})'$ to be a DPDF. As this does not hold, $(C_0^{\epsilon,m})'$ is not a DPDF, and by the above, $(C_0^{\epsilon,m})'$ is also not an EPDF.

(ii) Since $\phi_1 = \phi_i$ for all $i \in \{1, \ldots, \epsilon - 1\}$, it follows by Theorem 2.1.9 that $(C_0^{\epsilon,m})'$ is a (not necessarily proper) DPDF. When $\kappa = 0$, this implies that $\phi_0 = \phi_i$ for all $1 \leq i \leq \epsilon - 1$. It therefore follows by Theorem 2.1.9 that $(C_0^{\epsilon,m})'$ is a DDF. Since there are $f - 1$ transversals in $\mathrm{Int}((C_0^{\epsilon,m})')$, ϵ cyclotomic classes of order ϵ and since $(C_0^{\epsilon,m})'$ is a DDF, each cyclotomic class must occur an equal number of times in the multiset $\mathrm{Int}((C_0^{\epsilon,m})')$ this means that $\mathrm{Int}((C_0^{\epsilon,m})') = \frac{f-1}{\epsilon}\mathrm{GF}(q)^*$. It then follows from the above that

$$\mathrm{Ext}((C_0^{\epsilon,m})')) = \left(\lambda - \frac{f-1}{\epsilon}\right)(C_0^{\epsilon,m}) \cup \left(\mu - \frac{f-1}{\epsilon}\right)(\mathrm{GF}(q)^* \backslash C_0^{\epsilon,m}).$$

(iii) When $\kappa = \mu - \lambda$, notice that this means $\phi_1 = \phi_0 + \mu - \lambda$. As above, it follows by Theorem 2.1.9 that since $\phi_1 = \phi_i$ for all $i \in \{1, \ldots, \epsilon - 1\}$, this means that $(C_0^{\epsilon,m})'$ is a DPDF. More specifically, when $\kappa = \mu - \lambda$, $(C_0^{\epsilon,m})'$ is a $(q, \frac{e}{\epsilon}, f, \phi_0, \phi_0 + \kappa)$-DPDF, where

$$\mathrm{Int}((C_0^{\epsilon,m})') = \phi_0 C_0^{\epsilon,m} \cup (\phi_0 + \kappa)(\mathrm{GF}(q)^* \backslash C_0^{\epsilon,m}).$$

It then follows that since $\kappa = \mu - \lambda$

$$\begin{aligned}\mathrm{Ext}((C_0^{\epsilon,m})') &= (\lambda - \phi_0) C_0^{\epsilon,m} \cup (\mu - \phi_0 + \kappa)(\mathrm{GF}(q)^* \backslash C_0^{\epsilon,m}) \\ &= (\lambda - \phi_0) C_0^{\epsilon,m} \cup (\mu - \phi_0 + \lambda - \mu)(\mathrm{GF}(q)^* \backslash C_0^{\epsilon,m}) \\ &= (\lambda - \phi_0)\mathrm{GF}(q)^*.\end{aligned}$$

To obtain the value for ϕ_0, note that the $\frac{ef}{\epsilon} - 1$ transversals of the multiset $\Delta(C_0^{\epsilon,m})$ are all either contained in $\mathrm{Int}((C_0^{\epsilon,m})')$ or $\mathrm{Ext}((C_0^{\epsilon,m})')$. Notice that $f - 1$ of the transversals are diagonals of transversals contained in $\mathrm{Int}((C_0^{\epsilon,m})')$ (since $C_0^{\epsilon,m}$ has cardinality f) so the remaining

$$\frac{ef}{\epsilon} - 1 - (f - 1) = \frac{ef - \epsilon f}{\epsilon} = \frac{(e - \epsilon)f}{\epsilon}$$

transversals must be contained in the multiset $\mathrm{Ext}((C_0^{\epsilon,m})')$. As $(C_0^{\epsilon,m})'$ is an EDF, each of the ϵ cyclotomic classes of order ϵ must occur equally often in the mulitset $\mathrm{Ext}((C_0^{\epsilon,m})')$ i.e. $\frac{(e-\epsilon)f}{\epsilon^2}$ times. Then since $\lambda - \phi_0 = \frac{(e-\epsilon)f}{\epsilon^2}$, this means $\phi_0 = \lambda - \frac{(e-\epsilon)f}{\epsilon^2}$ and $\phi_1 = \phi_0 + \kappa = \phi_0 + \mu - \lambda = \mu - \frac{(e-\epsilon)f}{\epsilon^2}$.

(iv) As $\phi_1 = \phi_j$ for all $2 \leq j \leq \epsilon - 1$, but $\kappa \neq 0$, it follows that $(C_0^{\epsilon,m})'$ must be a proper $(q, \frac{e}{\epsilon}, f, \phi_0, \phi_0 + \kappa)$-DPDF. It then follows that

$$\mathrm{Int}((C_0^{\epsilon,m})') = \phi_0 C_0^{\epsilon,m} \cup (\phi_0 + \kappa)(\mathrm{GF}(q)^* \backslash C_0^{\epsilon,m}).$$

By the above, this in turn implies that

$$\mathrm{Ext}((C_0^{\epsilon,m})') = (\lambda - \phi_0) C_0^{\epsilon,m} \cup (\mu - (\phi_0 + \kappa))(\mathrm{GF}(q)^* \backslash C_0^{\epsilon,m}).$$

It is then clear that since $\kappa \neq \mu - \lambda$ that $\lambda - \phi_0 \neq \mu - (\phi_0 + \kappa)$, so $(C_0^{\epsilon,m})'$ is also a proper $(q, \frac{e}{\epsilon}, f, \lambda - \phi_0, \mu - (\phi_0 + \kappa)$-EPDF. □

We can then immediately use the above result to classify all DPDFs/EPDFs partitioning the squares (the cyclotomic class $C_0^{2,m}$). Notice that the EDF result in part (ii) was noted in [16].

Corollary 3.3.6. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^m = \epsilon\rho + 1 = ef + 1 \equiv 1 \mod 4$*, where* $\epsilon = 2$ *and* e *is even. Let* $C_0^{2,m}$ *denote the set of squares, let* $(C_0^{2,m})' = \{C_0^{e,m}, C_2^{e,m}, \dots, C_{e-2}^{e,m}\}$ *and let* $\kappa = \phi_1 - \phi_0$*. Then*

(i) when $\kappa = 0$*,* $(C_0^{2,m})'$ *forms a* $(q, \frac{e}{2}, f, \frac{f-1}{2})$*-DDF and a* $(q, \frac{e}{2}, f, \frac{(e-2)f-2}{4}, \frac{(e-2)f+2}{4})$*-EPDF.*

(ii) when $\kappa = 1$*,* $(C_0^{2,m})'$ *forms a* $(q, \frac{e}{2}, f, \frac{f-2}{2}, \frac{f}{2})$*-DPDF and a* $(q, \frac{e}{2}, f, \frac{(e-2)f}{4})$*-EDF.*

(iii) when $\kappa \in \{0, 1\}$ $(C_0^{2,m})'$ *forms a proper* $(q, \frac{e}{2}, f, \phi_0, \phi_0 + \kappa)$*-DPDF and a proper* $(q, \frac{e}{2}, f, \frac{q-5}{4} - \phi_0, \frac{q-1-4\kappa}{4} - \phi_0)$*-EPDF.*

Proof. As we saw in Proposition 3.1.2, C_0^2 is a $(q, \frac{ef}{2}, \frac{q-5}{4}, \frac{q-1}{4})$-PDS when $q \equiv 1 \mod 4$. The result then follows by Theorem 3.3.5. □

Example 3.3.7. *Below are examples of cases (i)-(iii) in Corollary 3.3.6.*

(i) Let $q = 41$ *with* $e = 8$ *and* $f = 5$*. Then* $C_0^{8,1} = \{1, 10, 16, 18, 37\}$*, we can then observe that* $\Phi_0 = \{10, 37\}$ *and* $\Phi_1 = \{16, 18\}$*, therefore* $\kappa = \phi_1 - \phi_0 = 2 - 2 = 0$*, and hence* $(C_0^{2,1})'$ *is a* $(41, 4, 5, 2)$*-DDF and a* $(41, 4, 5, 7, 8)$*-EPDF.*

(ii) Let $q = 29$ *with* $e = 14$ *and* $f = 2$ *then* $\phi_0 = 0$ *and* $\phi_1 = 1$*, so* $\kappa = 1$*. It follows that* $(C_0^{2,1})'$ *is a* $(29, 7, 2, 0, 1)$*-DPDF and a* $(29, 7, 2, 6)$*-EPDF.*

(iii) When $q = 17$*,* $e = 8$ *and* $f = 2$ $\phi_0 = 1$ *and* $\phi_1 = 0$*. It then follows that* $\kappa = -1$ *and so* $(C_0^{2,1})'$ *is a* $(17, 8, 2, 1, 0)$*-DPDF and a* $(17, 8, 2, 2, 4)$*-EPDF.*

We observe that when we set $f = 4$ in Corollary 3.3.6, we obtain the EDF result in Proposition 21 of [14].

In the following result, we are able to determine conditions, purely in terms of q and f, for when a DPDF/EPDF partitioning $C_0^{2,m}$ must be proper.

Theorem 3.3.8. *Let $q = p^m = ef + 1 \equiv 1 \mod 4$, and suppose the e is even. Then, if both of the conditions in (i) or both of the conditions in (ii) hold, $(C_0^{2,m})'$ is a proper $(q, \frac{e}{2}, f, \phi_0, \phi_1)$-DPDF and a proper $(q, \frac{e}{2}, f, \frac{q-5}{5} - \phi_0, \frac{q-1}{4} - \phi_1)$-EPDF (where proper implies $\phi_0 \neq \phi_1$).*

(i) $q \equiv 1 \mod 8$ *and* $f \equiv 2 \mod 4$.

(ii) $q \equiv 1 \mod 4$ *and* $f \equiv 3 \mod 4$.

Proof. (i) Recall that $(C_0^{e,m})'$ is a proper $(q, \frac{e}{2}, f, \phi_0, \phi_1)$-DPDF if and only $\phi_0 \neq \phi_1$, and that $(C_0^{e,m})'$ is a proper EPDF if and only if $\frac{q-5}{5} - \phi_0 \neq \frac{q-1}{4} - \phi_1$. As f is even, there are precisely $\frac{f-2}{2}$ values of $0 \leq r < \frac{f}{2}$. Since $f \equiv 2 \mod 4$, it follows that $\frac{f-2}{2}$ is an even integer. As $\psi_0 + \psi_1 = \frac{f-2}{2}$ (see definition of ψ_i), it follows from this, that there are three cases for ψ_0 and ψ_1 either they are equal, they are both odd or they are both even. This means that we can establish the following relationships between ψ_0 and ψ_1: either (1) $2\psi_0 = 2\phi_1$, (2) $2\psi_1 - 2\psi_0 \geq 4$ or (3) $2\psi_1 - 2\psi_0 \leq -4$. It follows from Proposition 2.1.12, that when $q \equiv 1 \mod 8$, this means that $\phi_0 = 2\psi_0 + 1$ and $\phi_1 = 2\psi_1$: we may also write $2\psi_0 = \phi_0 - 1$. In case (1), since $2\psi_0 = 2\psi_1$, it follows that $\kappa = \phi_1 - \phi_0 = -1$. In case (2), since $2\psi_1 - 2\psi_0 \geq 4$, it follows that that $\phi_1 - (\phi_0 - 1) \geq 4$, which means $\phi_1 - \phi_0 \geq 3$. Finally, in case (3), as $2\psi_1 - 2\psi_0 \leq -4$, this means $\phi_1 - (\phi_0 - 1) \leq -4$, meaning $\phi_1 - \phi_0 \leq -5$. By Corollary 3.3.6, we know that $(C_0^{2,m})'$ is a DDF $\kappa = 0$ and an EDF if $\kappa = 1$ as $\kappa \notin \{0, 1\}$ in cases (1)-(3), it follows that $(C_0^{2,m})'$ is a proper DPDF and a proper EPDF in all cases.

(ii) The proof of this result is analogous to part (i). □

We return to the idea of using values of f to determine cyclotomic DPDF/EPDF constructions in a subsequent Section. For now, we present some further corollaries of Theorem 3.3.5. We begin by looking at partitions of the cubes.

Corollary 3.3.9. *Let* GF(q) *be a finite field of odd order, where $q = p^m = ef + 1 = \epsilon\rho + 1 =\equiv 1 \mod 3$, where $\epsilon = 3$ and $3 \mid e$. Suppose that the unique proper representation of q is given by $4q = c^2 + 27d^2$ ($c \equiv 1 \mod 3$), where $d = 0$. Let $(C_0^{3,m})' = \{C_0^{e,m}, C_3^{e,m}, \ldots, C_{e-3}^{e,m}\}$ and $\kappa = \phi_1 - \phi_0$. If $\phi_1 = \phi_2$, then* *(i) when $\kappa = 0$, $(C_0^{3,m})'$ forms a $(q, \frac{e}{3}, f, \frac{f-1}{3})$-DDF and a $(q, \frac{e}{3}, f, \frac{(e-3)f-4+c}{9}, \frac{2f(e-3)+4-c}{18})$-EPDF.*

(ii) when $\kappa = \frac{4-c}{6}$, $(C_0^{3,m})'$ forms a $(q, \frac{e}{3}, f, \frac{3f-7+c}{9}, \frac{6f-2-c}{18})$-DPDF and a $(q, \frac{e}{3}, f, \frac{(e-3)f}{9})$-EDF.

(iii) when $\kappa \notin \{0, \frac{4-c}{6}\}$, $(C_0^{3,m})'$ forms a proper $(q, \frac{e}{3}, f, \phi_0, \phi_0 + \kappa)$-DPDF and a proper $(q, \frac{e}{3}, f, \frac{q-8+c}{9} - \phi_0, \frac{2q-4-c-18\kappa}{18} - \phi_0)$-EPDF.

Proof. By Theorem 3.1.3, C_0^3 is a $(q, \frac{e}{3}, f, \frac{q-8+c}{9}, \frac{2q-4-c}{18})$-PDS when $d = 0$. The result is then immediate from Theorem 3.3.5. □

Example 3.3.10. *To see an example of case (iii) of the above corollary, let $q = 121$, $e = 60$ and $f = 2$. In $\mathrm{GF}(121)$, $C_0^{3,2}$ is a $(121, 40, 15, 12)$-PDS. Since $C_0^{60,2} = \{1, 120\}$ and $120 \in \Phi_0$, it is immediate that $(C_0^{3,2})'$ is a $(121, 20, 2, 1, 0)$-DPDF. By Corollary 3.3.9, we obtain that $(C_0^{3,2})'$ is also a $(121, 20, 2, 14, 12)$-EPDF.*

We now look at look at the case where $\epsilon = 4$. Notice that the EDF result in part (ii) below subsumes that of [16].

Corollary 3.3.11. *Let $\mathrm{GF}(q)$ be a finite field of order $q = p^m = \epsilon\rho + 1 = ef + 1$, where $\epsilon = 4$ and $4 \mid e$. Suppose that $q = s^2$ is the proper representation of q, where m is even, $p \equiv 3 \mod 4$ and $s = (-p)^{\frac{m}{2}}$. Let $(C_0^{4,m})' = \{C_0^{e,m}, C_4^{e,m}, \ldots, C_{\epsilon-4}^{e,m}\}$ and let $\kappa = \phi_1 - \phi_0$. If $\phi_1 = \phi_2 = \phi_3$, then*

(i) when $\kappa = 0$, $(C_0^{4,m})'$ is both a $(q, \frac{e}{4}, f, \frac{f-1}{4})$-DDF and a $(q, \frac{e}{4}, f, \frac{(e-4)f-6-6s}{16}, \frac{(e-4)f+2+2s}{16})$-EPDF.

(ii) when $\kappa = \frac{s+1}{2}$, $(C_0^{4,m})'$ is both a $(q, \frac{e}{4}, f, \frac{4f-10-6s}{16}, \frac{4f-2+2s}{16})$-DPDF and a $(q, \frac{e}{4}, f, \frac{(e-4)f}{16})$-EDF.

(iii) when $\kappa \notin \{0, \frac{s+1}{2}\}$, then $(C_0^{4,m})'$ is both a proper $(q, \frac{e}{4}, f, \phi_0, \phi_0 + \kappa)$-DPDF and a proper $(q, \frac{e}{4}, f, \frac{(e-4)f}{16}, \frac{q-11-6s}{16} - \phi_0, \frac{q-3+2s-16\kappa}{16} - \phi_0)$-EDF.

Proof. Notice that since $q = s^2$ is the proper representation of q, this implies that $t = 0$. By Theorem 3.1.3, when $t = 0$, this implies that $C_0^{4,m}$ is a proper $(q, \frac{ef}{4}, \frac{q-11-6s}{16}, \frac{q-3+2s}{16})$-PDS. The result then follows by Theorem 3.3.5. □

Example 3.3.12. *Let $q = 81$, $\epsilon = 4$ and $\rho = 20$. Since $4 \mid 3+1$, where $3^4 = 81$, it follows by Theorem 2.1.21 that $C_0^{4,4}$ is an $(81, 20, 1, 6)$-PDS in the finite field* GF(81)*. The only value e, where $4 \mid e$, and $\phi_1 = \phi_2 = \phi_3$ is $e = 40$. In this case $\phi_0 = 1$ and $\phi_1 = 0$. So $\kappa \notin \{0, -4\}$ and hence $(C_0^{4,4})'$ is a $(81, 20, 1, 0)$-DPDF and a $(81, 20, 0, 6)$-EPDF.*

In the final part of this Section, we demonstrate that we can apply the argument used to construct PDSs in Theorem 3.1.5 to DPDF and EPDF constructions.

Theorem 3.3.13. *Let $q = p^m = \epsilon\rho + 1 = ef + 1$, where $\epsilon \mid e$. Let $(C_0^{\epsilon,m})' = \{C_0^{e,m}, C_\epsilon^{e,m}, \dots, C_{e-\epsilon}^{e,m}\}$ be a $(q, \frac{e}{\epsilon}, f, \phi_0, \phi_1)$-DPDF.*

(i) If $\epsilon > f$, then $\phi_0 = f - 1$ and $\phi_1 = 0$, meaning that $(C_0^{\epsilon,m})'$ is a $(q, \frac{e}{\epsilon}, f, f - 1, 0)$-DPDF.

(ii) If $\epsilon > 2$ and $\epsilon = f$, then $(C_0^{\epsilon,m})'$ is a $(q, \frac{e}{\epsilon}, f, f-1, 0)$-DPDF.

(iii) In both cases (i) and (ii), if $C_0^{\epsilon,m}$ is a (q, ρ, λ, μ)-PDS, then $(C_0^{\epsilon,m})'$ is also a $(q, \frac{e}{\epsilon}, f, \lambda - f + 1, \mu)$-EPDF, which is proper unless $\mu - \lambda = f - 1$.

Proof. There are $f - 1$ diagonals of transversals in $\text{Int}((C_0^{\epsilon,m})')$, and $\epsilon - 1$ cyclotomic classes of the form $C_i^{e,m}$, where $1 \leq i \leq \epsilon - 1$. As in the proof of Theorem 3.1.5, we can derive the following expression for the diagonals of tranversals in $\text{Int}((C_0^{\epsilon,m})')$ $f - 1 = \phi_0 + \phi_1(\epsilon - 1)$. Note that f, ϵ, ϕ_0 and ϕ_1 are all non-negative integers. In part (i), it is clear that if $\epsilon > f$ then $\phi_1 = 0$, and so $(C_0^{\epsilon,m})'$ is a $(q, \frac{e}{\epsilon}, f - 1, 0)$-DPDF. In part (ii), notice that there are two cases to consider in order for $f - 1 = \phi_0 + \phi_1(\epsilon - 1)$, either (1) $\phi_0 = f - 1$ and $\phi_1 = 0$ or (2) $\phi_0 = 0$ and $\phi_1 = 1$. In both cases (1) and (2), as $\phi_0 \neq \phi_1$, it follows by Theorem 2.1.15 that this means that ϵ cannot be even while ρ is odd, since in this case we require $\phi_0 = \phi_1$ (in order for $(C_0^{e,m})'$ to be a DPDF). Therefore, in cases (1) and (2) we only need to consider the cases where ρ is even and ϵ and ρ are both odd. It follows by Theorem 2.1.15 that when $\epsilon > 2$ and ρ is even, ϕ_1 is even. Similarly, when ϵ and ρ are both odd, it follows that ϕ_1 must be even. We can therefore see that case (2) cannot hold, hence case (1) must hold. Part (iii) of this proof is immediate from Theorem 3.3.5. □

The specific case where $\epsilon = f = 2$ is explored later in this Chapter, in Theorem 3.5.1.

Example 3.3.14. *(i) In* $\mathrm{GF}(49)$*, when* $\epsilon = 8$*,* $e = 16$ *and* $f = 3$*, it follows that* $(C_0^{8,2})' = \{C_0^{16}, C_8^{16}\}$ *is a* $(49, 2, 3, 2, 0)$*-DPDF and a* $(49, 2, 3, 3, 0)$*-EPDF.*

(ii) In $\mathrm{GF}(64)$*, when* $\epsilon = 3$*,* $e = 21$ *and* $f = 3$*,* $(C_0^{3,6})' = \{C_0^{21,6}, C_3^{21,6}, C_6^{21,6}, C_9^{21,6}, C_{12}^{21,6}, C_{15}^{21,6}, C_{18}^{21,6}\}$ *is a* $(64, 7, 3, 2, 0)$*-DPDF and a* $(64, 7, 3, 6)$*-EDF.*

3.4 Explicit DPDF/EPDF constructions obtained by partitioning the squares into cyclotomic classes with small e

In this Section, we look at DPDF and EPDF results that can obtained by specifically partitioning the squares in a given finite field GF(q). All results in this Section are also recorded in my joint paper with my supervisor [34].

In our first result, we partition the squares into sets of cyclotomic classes of order 4. Notice that EDF result in part (ii) of the following Theorem corresponds to Theorem 3.2 in [32].

Theorem 3.4.1. *Let* q *be a finite field of order* $q = p^m = 4f+1$ *and let* $(C_0^{2,m})' = \{C_0^{4,m}, C_2^{4,m}\}$*. Let* s *be defined as in Theorem A.0.3. Then*

(i) when f *is even,* $(C_0^{2,m})'$ *is a* $(q, 2, \frac{q-1}{4}, \frac{q-7-2s}{8}, \frac{q-3+2s}{8})$*-DPDF and a* $(q, 2, \frac{q-1}{4}, \frac{q-3+2s}{8}, \frac{q+1-2s}{8})$ *- EPDF which are both proper, except in the case when* $s = 1$*. When* $s = 1$*,* $(C_0^{2,m})'$ *is a* $(q, 2, \frac{q-1}{4}, \frac{q-1}{8})$*-EDF.*

(ii) when f *is odd,* $(C_0^{2,m})'$ *is a* $(q, 2, \frac{q-1}{4}, \frac{q-7+2s}{8}, \frac{q-3-2s}{8})$*-DPDF and a* $(q, 2, \frac{q-1}{4}, \frac{q-3-2s}{8}, \frac{q+1+2s}{8})$*-EPDF which are both proper except when* $s = 1$*. When* $s = 1$*,* $(C_0^{2,m})'$ *is a* $(q, 2, \frac{q-1}{4}, \frac{q-5}{8})$*-DDF.*

Proof. Notice that $\mathrm{Int}((C_0^{2,m})') = \Delta(C_0^{4,m}) \cup \Delta(C_2^{4,m})$. By Lemma 2.1.2 (ii), $\Delta(C_0^{4,m}) = (0,0)_4 C_0^{4,m} \cup (1,0)_4 C_1^{4,m} \cup (2,0)_4 C_2^{4,m} \cup (3,0)_4 C_3^{4,m}$ and by Lemma 2.1.2 (iii), $\Delta(C_2^{4,m}) = (2,0)_4 C_0^{4,m} \cup (3,0)_4 C_1^{4,m} \cup (0,0)_4 C_2^{4,m} \cup (1,0)_4 C_3^{4,m}$. It then follows that $\mathrm{Int}((C_0^{2,m})') = ((0,0)_4 + (2,0)_4)(C_0^{4,m} \cup C_2^{4,m}) \cup ((1,0)_4 + (3,0)_4)(C_1^{4,m} \cup C_3^{4,m})$. By definition, $\phi_0 = (0,0)_4 + (2,0)_4$ and $\phi_1 = (1,0)_4 + (3,0)_4$.

(i) By Theorem A.0.3, when f is even, $\phi_0 = (0,0)_4 + (2,0)_4 = \frac{q-2s-7}{8}$ and $\phi_1 = (1,0)_4 + (3,0)_4 = \frac{q+2s-3}{8}$. By Corollary 3.3.6, this means that $(C_0^{2,m})'$

is a proper $(q, 2, \frac{q-1}{4}, \frac{q-2s-7}{8}, \frac{q+2s-3}{8})$-DPDF, except in the case where $\kappa = \phi_1 - \phi_0 = 0$ and a proper $(q, 2, \frac{q-1}{4}, \frac{q-3+2s}{8}, \frac{q+1-2s}{8})$-EPDF, except in the case where $\kappa = 1$. There are no values of s for which $\frac{q+2s-3}{8} - \frac{q-2s-7}{8} = 0$, but $\frac{q+2s-3}{8} - \frac{q-2s-7}{8} = 1$ when $s = 1$.

(ii) By Theorem A.0.3, when f is odd then $A = (0,0)_4 = (2,0)_4$ and $B = (1,0)_4 = (3,0)_4$. It then follows that $\phi_0 = 2A = \frac{q+2s-7}{8}$ and $\phi_1 = \frac{q-2s-3}{8}$. The result is otherwise analogous to part (i). □

We now produce similar results for $e = 6$. We first make the following interesting remark about the f odd case when $e = 6$.

Remark 3.4.2. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^m = 6f + 1$*, where* f *is odd. When* f *is odd,* $q \equiv 3 \mod 4$*. By Theorem 3.1.1, when* $q \equiv 3 \mod 4$*,* $C_0^{2,m}$ *is a Difference Set. It then follows by Theorem 3.3.1 that* $(C_0^{2,m})'$ *is a* $(q, 3, f, \frac{f-1}{2})$*-DDF and a* $(q, 3, f, f)$*-EDF.*

We now look at the case where $e = 6$ and f is even.

Theorem 3.4.3. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^m = 6f + 1$*, where* p *is an odd prime and* f *is even. Let* s *be defined as it is in Theorem A.0.4. Then* $(C_0^{2,m})'$ *is a proper* $(q, 3, \frac{q-1}{6}, \frac{q-9-4s}{12}, \frac{q-5+4s}{12})$*-DPDF and a proper* $(q, 3, \frac{q-1}{6}, \frac{q-3+2s}{6}, \frac{q+1-2s}{6})$*-EPDF, except for when* $s = 1$*. In this case,* $(C_0^{2,m})'$ *is a* $(q, 3, \frac{q-1}{6}, \frac{q-1}{6})$*-EDF.*

Proof. Note that by Theorem A.0.4, $\phi_0 = (0,0)_6 + (2,0)_6 + (4,0)_6 = \frac{q-9-4s}{12}$ and $\phi_1 = (1,0)_6 + (3,0)_6 + (5,0)_6 = \frac{q-5+4s}{12}$. The proof is otherwise analogous to the proof of Theorem 3.4.1. □

Example 3.4.4. *(i) In* $\mathrm{GF}(13)$*,* $q = 13 = 1 + 3(2)^2$*, is the proper representation of* q*, therefore* $(C_0^{2,m})'$ *is a* $(13, 3, 2, 0, 1)$*-DPDF and a* $(13, 3, 2, 2)$*-EDF.*

(ii) In the finite field $\mathrm{GF}(37)$*,* $s = -5$ *and so* $(C_0^{2,m})'$ *is a* $(37, 3, 6, 4, 1)$*-DPDF and a* $(37, 3, 6, 4, 8)$*-EPDF.*

Theorem 3.4.5. *Let $q = p^m = 8f+1$, where p is an odd prime. Let x and a be defined as in Theorem A.0.5. Then $(C_0^{2,m})'$ is always a proper $(q, 4, \frac{q-1}{8}, \frac{q-11-2x-4a}{16}, \frac{q-7+2x+4a}{16})$-DPDF and a proper $(q, 4, \frac{q-1}{8}, \frac{3q-9+2x+4a}{16}, \frac{3q+3-2x-4a}{16})$-EPDF, except in the following cases*

(i) when f is even and $x + 2a = 3$. In this case $(C_0^{2,m})'$ is a $(q, 4, \frac{q-1}{8}, \frac{3q-3}{16})$-EDF.

(ii) when f is odd and $x+2a = -1$. In this case $(C_0^{2,m})'$ is a $(q, 4, f, \frac{q-9}{16})$-DDF.

Proof. Suppose, as in Theorem A.0.5, that q is represented by $q = x^2 + 4y^2 = a^2 + 2b^2$, where $x \equiv a \equiv 1 \mod 4$. By Theorem A.0.5, it follows that

(i) when f is even, $\phi_0 = (0,0)_8 + (2,0)_8 + (4,0)_8 + (6,0)_8 = \frac{q-11-2x-4a}{16}$ and $\phi_1 = (1,0)_8 + (3,0)_8 + (5,0)_8 + (7,0)_8 = \frac{q-7+2x+4a}{16}$.

(ii) when f is odd, $A = (0,0)_8(4,0)_8$ and $N = (2,0)_8 = (6,0)_8$, meaning $\phi_0 = 2A + 2N = \frac{q-11-2x-4a}{16}$. Similarly $I = (1,0)_8 = (5,0)_8$ and $J = (3,0)_8 = (7,0)_8$ meaning $\phi_1 = 2I + 2J = \frac{q-7+2x+4a}{16}$.

The proof of this result is otherwise analogous to the proof of Theorem 3.4.1.

□

Example 3.4.6. *(i) In the finite field* GF(17)*, when $e = 8$, $f = 2$, therefore f is even. Moreover in* GF(17)*, $x = 1$ and $a = -3$, it therefore follows that $(C_0^{2,1})'$ is a $(17, 4, 2, 1, 0)$-DPDF and a $(17, 4, 2, 2, 4)$-EPDF.*

(ii) In the finite field GF(41)*, when $e = 8$, $f = 5$ is odd. In this finite field, $x = 5$ and $s = -3$, hence $(C_0^{2,1})'$ is a $(41, 4, 5, 2)$-DDF (since $x + 2a = -1$) and a $(41, 4, 5, 7, 8)$-EPDF.*

3.5 DPDF/EPDF constructions obtained by partitioning the squares into cyclotomic classes with small f

In this Section, we explore cyclotomic constructions of DPDFs and EPDF, found by partitioning the squares (the cyclotomic class $C_0^{2,1}$) in a finite field GF(q) into cyclotomic classes in which $2 \leq f \leq 6$. This gives an alternative way of using the cyclotomic framework developed in Chapter 2. All results in this subsection are recorded in the preprint [40] and have been adapted from results in [52]. Note that as all DPDFs and EPDFs in this Subsection partition the set of squares, we will consistently use the notation $(C_0^{2,s})'$ to denote the component sets of the DPDFs and EPDFs presented in this subsetion. Further, throughout this section we will use the notation D_i $(1 \leq i \leq f-1)$ to denote diagonals of transversals: for a formal definition of these objects, we refer the reader back to Definition 2.1.5.

We start by going through the $f = 2$ case. The following result is from the paper [34] and is the specific case of Theorem 3.3.13. The EDF result in part (ii) of the following Lemma was also recorded in [14] and the EDF and EPDF results from parts (i) and (ii) were also implicitly recorded in [52].

Theorem 3.5.1. *Let $q = p^s = 2\rho + 1 = ef + 1$, where $f = 2$ and $e = \frac{q-1}{2}$ is even. Let $(C_0^{2,s})' = \{C_0^{e,s}, \ldots, C_{e-2}^{e,s}\}$. Then*

(i) when $q \equiv 1 \mod 8$, $(C_0^{2,s})'$ forms a $(q, \frac{q-1}{4}, 2, 1, 0)$-DPDF and a $(q, \frac{q-1}{4}, 2, \frac{q-9}{4}, \frac{q-1}{4})$-EPDF.

(ii) when $q \equiv 5 \mod 8$, $(C_0^{2,s})'$ forms a $(q, \frac{q-1}{4}, 2, 0, 1)$-DPDF and a $(q, \frac{q-1}{4}, 2, \frac{q-3}{4})$-EDF.

Proof. By Lemma 2.1.6, when $f = 2$, $\text{Int}(C_0^{2,s})' = D_1$. Moreover, since $q \equiv 1 \mod 4$ in both cases (i) and (ii), it follows by Proposition 3.1.2 that C_0^2 is a $(q, \frac{q-1}{2}, \frac{q-5}{4}, \frac{q-1}{4})$-PDS.

(i) By Lemma's 2.1.6 and 2.1.12 when $q \equiv 1 \mod 8$, $\text{Int}((C_0^{2,s})') = D_1 = C_0^{2,s}$. By Lemma 1.2.4, this then means that

$$\begin{aligned}\text{Ext}((C_0^{2,s})') &= \left(\frac{q-5}{2} - 1\right) C_0^{2,s} \cup \left(\frac{q-1}{4}\right) (\text{GF}(q)^* \backslash C_0^{2,s}) \\ &= \left(\frac{q-9}{2}\right) C_0^{2,s} \cup \left(\frac{q-1}{4}\right) (\text{GF}(q)^* \backslash C_0^{2,s}).\end{aligned}$$

(ii) The proof of this result is analogous to the proof of part (i). □

The following results for $3 \leq f \leq 6$ are generalisations of results in [52].

Theorem 3.5.2. *Let* $\mathrm{GF}(p)$ *be a finite field of order* $p = 2\rho + 1 = 3e + 1 \equiv 1 \mod 4$*, where* p *is prime and* $e = \frac{p-1}{3}$ *is even. Let* $(C_0^{2,1})' = \{C_0^{e,1}, \ldots, C_{e-2}^{2,1}\}$*. Then* $(C_0^{2,1})'$ *is a*

(i) $(p, \frac{p-1}{6}, 3, 2, 0)$*-DPDF and* $(p, \frac{p-1}{6}, 3, \frac{p-13}{4}, \frac{p-1}{4})$*-EPDF if* $(-3)^{\frac{(p-1)}{4}} \equiv 1 \mod p$*,*

(ii) $(p, \frac{p-1}{6}, 3, 0, 2)$*-DPDF and* $(p, \frac{p-1}{6}, 3, \frac{3s-2}{2}, \frac{3s-4}{2})$*-EPDF if* $(-3)^{\frac{(p-1)}{4}} \equiv -1 \mod p$*.*

Proof. (i) By Lemma 2.1.6, when $f = 3$ it follows that $\mathrm{Int}((C_0^{2,1})') = D_1 \cup D_2$, where $D_1 = (\alpha^e - 1)C_0^{2,1}$ and $D_2 = (\alpha^{2e} - 1)C_0^{2,1}$. It was proved in [52] that $(-3)^{\frac{(p-1)}{4}} \equiv \pm 1 \mod p$. When $(-3)^{\frac{(p-1)}{4}} \equiv 1 \mod p$, $\alpha^e - 1, \alpha^{2e} - 1 \in C_0^{2,1}$ meaning $D_1 = D_2 = C_0^{2,1}$. It then follows from the first line of this proof that $\mathrm{Int}((C_0^{2,1})') = D_1 \cup D_2 = 2(C_0^{2,1})$, and so $(C_0^{2,1})'$ is a $(p, \frac{p-1}{6}, 2, 0)$-DPDF. Further, as $p \equiv 1 \mod 4$, it is immediate by Proposition 3.1.2 that $C_0^{2,1}$ is a $(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{4})$-PDS. Since $(C_0^{2,1})'$ is a partition of $C_0^{2,1}$, $(C_0^{2,1})'$ is a $(p, \frac{p-1}{6}, 3, 2, 0)$-DPDF and $C_0^{2,1}$ is a $(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{4})$-PDS, it follows by Theorem 1.3.17(i) that $(C_0^{2,1})'$ is also a $(p, \frac{p-1}{6}, 3, \frac{p-13}{4}, \frac{p-1}{4})$-EPDF.

(ii) It was proved in [52] that when $(-3)^{\frac{(p-1)}{4}} \equiv -1 \mod p$, then $\alpha^e - 1, \alpha^{2e} - 1 \in C_1^{2,1}$. Using this fact, and analogous proof strategy to the proof presented in part (i), we can prove the statement of (ii). This is left up to the reader.

□

Example 3.5.3. *(i) When* $q = 13$*,* $e = 4$ *and* $f = 3$*, observe that* $(-3)^3 = -27 \equiv -1 \mod 13$*. It therefore follows from Theorem 3.5.2(ii) that* $(C_0^{2,1})' = \{C_0^{4,1}, C_2^{4,1}\}$ *is a* $(13, 2, 3, 0, 2)$*-DPDF and a* $(13, 2, 3, 2, 1)$*-EPDF.*

(ii) Let $q = 37$*,* $e = 12$ *and* $f = 3$*, then* $(-3)^9 \equiv 1 \mod 37$*, hence Theorem 3.5.2(i) implies that* $(C_0^{2,1})' = \{C_0^{12,1}, C_2^{12,1}, C_4^{12,1}, C_6^{12,1}, C_8^{12,1}, C_{10}^{12,1}\}$ *is a* $(37, 6, 3, 2, 0)$*-DPDF and a* $(37, 6, 3, 6, 9)$*-EPDF.*

Throughout the following result, we use the notation "||" to mean "strictly divides" i.e. $a \mid b$ and $a \neq b$.

Theorem 3.5.4. *Let* $\mathrm{GF}(p)$ *be a finite field of order* $p = 2\rho + 1 = 4e + 1 \equiv 1 \mod 4$*, where* p *is prime and* $e = \frac{p-1}{4}$ *is even. Let* $(C_0^{2,1})' = \{C_0^{e,1}, \ldots, C_{e-2}^{e,1}\}$*, then* $(C_0^{2,1})'$ *is a* *(i)* $(p, \frac{p-1}{8}, 4, 3, 0)$*-DPDF and* $(p, \frac{p-1}{8}, 4, \frac{p-17}{4}, \frac{p-1}{4})$*-EPDF if* $4 \mid e$ *and* $2 \in C_0^4$ *or if* $2 \mid\mid e$ *and* $2 \in C_2^4$.

(ii) $(p, \frac{p-1}{8}, 4, 1, 2)$*-DPDF and* $(p, \frac{p-1}{8}, s, 4, 2s-2)$*-EDF if* $4 \mid e$ *and* $2 \in C_2^4$ *or if* $2 \mid\mid e$ *and* $2 \in C_0^4$.

Proof. When $f = 4$, it follows that $\mathrm{Int}((C_0^{2,s})') = D_1 \cup D_2 \cup D_3$, where $D_1 = (\alpha^e - 1)C_0^{2,1}$, $D_2 = D_{\frac{f}{2}}(2)C_0^{2,1}$ (by Corollary 2.1.11) and $D_3 = (\alpha^{3e} - 1)C_0^{2,1}$. As $e = \frac{p-1}{4}$ is even, it follows that $p \equiv 1 \mod 8$, thus it follows by Lemma 2.1.12 that $D_2 = C_0^{2,1}$ in both cases.

It was proven in [52] that when $f = 4$, $\alpha^e - 1, \alpha^{3e} - 1 \in C_0^{2,1}$ if $-2\alpha^e \in C_0^{4,1}$ and $\alpha^e - 1, \alpha^{3e} - 1 \in C_1^{2,1}$ if $-2\alpha^e \in C_2^{4,1}$. We can see that $-1 \in C_0^{4,1}$: by Lagrange's Theorem $-1 = \alpha^{e\frac{f}{2}} = \alpha^{2e}$ is a fourth power, since $f = 4$ and e is even. Therefore, $-2\alpha^e \in C_0^{4,1}$ if and only if $2\alpha^e \in C_0^{4,1}$ this happens when either $4 \mid e$ and $2 \in C_0^4$ or when $2 \mid\mid e$ and $2 \in C_2^4$. In both of these cases $D_1 = D_3 = C_0^{2,1}$, and so $\mathrm{Int}((C_0^{2,1})') = 3C_0^{2,1}$, meaning that $(C_0^{2,1})'$ is a $(p, \frac{p-1}{8}, 4, 3, 0)$-DPDF. When $2\alpha^e \in C_2^{4,1}$, it follows from the above that $D_1 = D_3 = C_1^{2,1}$ and $D_2 = C_0^{2,1}$, meaning $\mathrm{Int}((C_0^{2,1})') = C_0^{2,1} \cup 2C_1^{2,1}$: this happens when $4 \mid e$ and $2 \in C_2^4$ or when $2 \mid\mid e$ and $2 \in C_0^4$. Notice that when $\mathrm{Int}((C_0^{2,1})') = C_0^{2,1} \cup 2C_1^{2,1}$, then $(C_0^{2,1})$ is a $(p, \frac{p-1}{8}, 4, 1, 2)$-DPDF.

By Proposition 3.1.2, as $p \equiv 1 \mod 4$, it follows that $C_0^{2,1}$ is a $(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{p-1}{4})$-PDS. By Theorem 1.3.17(i), we can then see that since $(C_0^{2,1})'$ is a $(p, \frac{p-1}{8}, 4, 3, 0)$-DPDF when $4 \mid e$ and $2 \in C_0^4$ or $2 \mid\mid e$ and $2 \in C_2^4$, it follows that $(C_0^{2,1})'$ must also be an $(p, \frac{p-1}{8}, 4, \frac{p-17}{4}, \frac{p-1}{4})$-EPDF. We can then use analogous reasoning to prove that $(C_0^{2,1})'$ is a $(p, \frac{p-1}{8}, s, 4, 2s-2)$-EDF when $4 \mid e$ and $2 \in C_2^4$ or $2 \mid\mid e$ and $2 \in C_0^4$. □

Theorem 3.5.5. *Let* $\mathrm{GF}(p)$ *be a finite field of order* $p = 2\rho + 1 = 5e + 1 \equiv 1 \mod 4$*, where* p *is prime and* $e = \frac{p-1}{5}$ *is even. Let* $(C_0^{2,1})' = \{C_0^{e,1}, \ldots, C_{e-2}^{e,1}\}$*, then* $(C_0^{2,1})'$ *is a*

(i) $(p, \frac{p-1}{10}, 5, 2)$*-DDF and* $(p, \frac{p-1}{10}, 5, \frac{p-13}{4}, \frac{p-9}{4})$*-EPDF when* $5^{\frac{p-1}{4}} = -1 \mod p$.

(ii) $(p, \frac{p-1}{10}, 5, 4, 0)$*-DPDF and* $(p, \frac{p-1}{10}, 5, \frac{p-21}{4}, \frac{p-1}{4})$*-EPDF when* $5^{\frac{p-1}{4}} = 1 \mod p$ *and* $\alpha^{\frac{p-1}{5}} - 1 \in C_0^2$.

(iii) $(p, \frac{p-1}{10}, 5, 0, 4)$*-DPDF and* $(p, \frac{p-1}{10}, 5, \frac{p-5}{4}, \frac{p-17}{4})$*-EPDF when* $5^{\frac{p-1}{4}} = 1 \mod p$ *and* $\alpha^{\frac{p-1}{5}} - 1 \in C_1^2$.

Proof. By Lemma 2.1.6, when $f = 5$, $\text{Int}((C_0^{2,s})') = D_1 \cup D_2 \cup D_3 \cup D_4$, where $D_1 = (\alpha^e - 1)C_0^{2,1}$, $D_2 = (\alpha^{2e} - 1)C_0^{2,1}$, $D_3 = (\alpha^{3e} - 1)C_0^{2,1}$ and $D_4 = (\alpha^{4e} - 1)C_0^{2,1}$. Since ρ is even (notice that $2\rho \equiv 0 \mod 4$) it follows by Corollary 2.1.11 that $D_1 = C_i^{2,1} = D_4$ and $D_2 = C_j^{2,1} = D_3$ for some $0 \leq i, j \leq 1$.

It is demonstrated in [52], that when $(-5)^{\frac{p-1}{4}} \equiv -1 \mod p$, then exactly one of $\alpha^e - 1$ and $\alpha^{2e} - 1$ is in the cyclotomic class $C_0^{2,1}$ meaning either $D_1 = C_0^{2,1} = D_4$ and $D_2 = C_1^{2,1} = D_3$ or $D_1 = C_1^{2,1} = D_4$ and $D_2 = C_0^{2,1} = D_3$. In either case, $\text{Int}((C_0^{2,1})') = 2C_0^{2,1} \cup 2C_1^{2,1}$. It then follows by Lemma 1.2.4 and Proposition 3.1.2 that $\text{Ext}((C_0^{2,1})') = \left(\frac{p-13}{4}\right) C_0^{2,1} \cup \left(\frac{p-9}{4}\right) C_1^{2,1}$.

Further, it is proven in [52] that when $5^{\frac{p-1}{4}} = 1 \mod p$, either $\alpha^e - 1, \alpha^{2e} - 1 \in C_0^{2,1}$ or $\alpha^e - 1, \alpha^{2e} - 1 \in C_1^{2,1}$ meaning $D_1 = D_2 = D_3 = D_4$. Therefore, when $\alpha^{\frac{p-1}{5}} - 1 \in C_0^2$, $D_1 = D_2 = D_3 = D_4 = C_0^{2,1}$ meaning $\text{Int}((C_0^{2,1})') = 4C_0^{2,1}$. Since $\text{Int}((C_0^{2,1})') = 4C_0^{2,1}$ when $\alpha^{\frac{p-1}{5}} - 1 \in C_0^2$, it follows by Lemma 1.2.4 and Proposition 3.1.2, that $\text{Ext}((C_0^{2,1})') = \left(\frac{p-13}{4}\right) C_0^{2,1} \cup \left(\frac{p-9}{4}\right) C_1^2$. Analogously, when $\alpha^{\frac{p-1}{5}} - 1 \in C_0^2$, $D_1 = D_2 = D_3 = D_4 = C_1^{2,1}$ meaning $\text{Int}((C_0^{2,1})') = 4C_1^{2,1}$, and $\text{Ext}((C_0^{2,1})') = \left(\frac{p-5}{4}\right) C_0^{2,1} \cup \left(\frac{p-17}{4}\right) C_1^2$. □

Example 3.5.6. *(i) In Example 3.3.7, we saw that* $q = 41$, $e = 8$ *and* $f = 5$, $(C_0^{2,1})'$ *is a* $(41, 4, 5, 2)$*-DDF and a* $(41, 4, 5, 7, 8)$*-EDF. Observe that* $5^{10} \equiv -1 \mod 41$.

(ii) When $q = 121$, $e = 24$ *and* $f = 5$, $(C_0^{2,2})'$ *is a* $(121, 12, 5, 4, 0)$*-DPDF and a* $(121, 5, 4, 25, 30)$*-EPDF. Here* $5^{30} \equiv 1 \mod 11$ *and* $\alpha^{24} - 1 \in C_0^{2,2}$.

Theorem 3.5.7. *Let* $\text{GF}(p)$ *be a finite field of order* $p = 2\rho + 1 = 6e + 1 \equiv 1 \mod 4$, *where* p *is prime and* $e = \frac{p-1}{6}$ *is even. Let* $(C_0^{2,1})' = \{C_0^{e,1}, \ldots, C_{e-2}^{e,1}\}$, *then* $(C_0^{2,1})'$ *is a*

(i) $(p, \frac{p-1}{12}, 6, 5, 0)$*-DPDF and* $(p, \frac{p-1}{12}, 6, 3s-6, 3s)$*-EPDF if* $4 \mid e$ *and* $(-3)^{\frac{(p-1)}{4}} \equiv 1 \mod p$.

(ii) $(p, \frac{p-1}{12}, 6, 4, 1)$*-DPDF and* $(p, \frac{p-1}{12}, 6, 3s - 5, 3s - 1)$*-EPDF if* $2 \mid\mid e$ *and* $(-3)^{\frac{(p-1)}{4}} \equiv 1 \mod p$.

(iii) $(p, \frac{p-1}{12}, 6, 3, 2)$*-DPDF and* $(p, \frac{p-1}{12}, 6, 3s - 4, 3s - 2)$*-EPDF if* $4 \mid e$ *and* $(-3)^{\frac{(p-1)}{4}} \equiv -1 \mod p$.

(iv) $(p, \frac{p-1}{12}, 6, 2, 3)$*-DPDF and* $(p, \frac{p-1}{12}, 6, 3s - 3)$*-EDF if* $2 \mid\mid e$ *and* $(-3)^{\frac{(p-1)}{4}} \equiv -1 \mod p$.

Proof. When $f = 6$, it follows that $\mathrm{Int}((C_0^{2,s})') = D_1 \cup D_2 \cup D_3 \cup D_4 \cup D_5$, where $D_1 = (\alpha^e - 1)C_0^{2,1}$, $D_2 = (\alpha^{2e} - 1)C_0^{2,1}$, $D_3 = (\alpha^{3e} - 1)C_0^{2,1}$, $D_4 = (\alpha^{4e} - 1)C_0^{2,1}$ and $D_5 = (\alpha^{5e} - 1)C_0^{2,1}$.

It follows by Corollary 2.1.11 that $D_1 = D_5$, $D_2 = D_4$ and $D_3 = (2)C_0^{2,1}$. Notice that when $2 \mid\mid e$, then $p \equiv 0 \mod 12$, and hence, it follows by Lemma 2.1.12 that $2 \in C_1^{2,1}$. When $4 \mid e$, $p \equiv 0 \mod 24$, and so by Lemma 2.1.12, $2 \in C_0^{2,1}$.

$$(\alpha^e - 1)^2(\alpha^{2e} - 1)^2 = -3.$$

Further, it is also demonstrated in [52], that $(\alpha^e - 1)^2 \in C_0^{4,1}$. It therefore follows that when $-3^{\frac{p-1}{4}} \equiv 1 \mod p$, then $(\alpha^{2e}-1)^2 \in C_0^{4,1}$, and so it follows that $\alpha^e - 1, \alpha^{2e} - 1 \in C_0^{2,1}$ when $-3^{\frac{p-1}{4}} \equiv 1 \mod p$. This means that when $-3^{\frac{p-1}{4}} \equiv 1 \mod p$, $D_1 = D_2 = D_4 = D_5 = C_0^{2,1}$. The DPDF results in parts (i) and (ii) can then be obtained by combining this with the earlier D_3 result. Moreover, notice that since $(\alpha^e - 1)^2 \in C_0^{4,1}$, this means that $(\alpha^{2e} - 1)^2 \in C_2^{4,1}$ when $-3^{\frac{p-1}{4}} \equiv -1 \mod p$ hence $D_1 = D_5 = C_0^{2,1}$ and $D_2 = D_4 = C_1^{2,1}$. Again, parts (iii) and (iv) can be obtained by combining this with the earlier D_3 results. Apply Lemma 1.2.4 and Proposition 3.1.2 to obtain the relevant EPDF results. □

In the upcoming pre-print [40], I have extended these results for $7 \leq f \leq 10$, however these results have been omitted due to space constraints.

3.6 Cyclotomic DPDF construction obtained via the use of cyclotomic orbits

In this short Section, we demonstrate that cyclotomic orbits can be used to produce PDS/DPDF constructions.

Lemma 3.6.1. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^m = ef + 1$*, where* p *is an odd prime. If* e *is an odd prime and* p *is a generator of the multiplicative group* $\mathbb{Z}_e^*$*, then for all* $1 \leq i \leq e - 1$*,* $\mu = (i, i)_e = (i, 0)_e = (0, i)_e$

Proof. By Theorem 1.4.12, the following relations relations apply to the cyclotomic numbers of order e $(i, j)_e = (j, i)_e$, $(i, j)_e = (e - i, j - i)_e$ and $(i, j)_e = (ip, jp)_e$. As p is a generator of $\mathbb{Z}_e^*$, it follows that for $0 \leq i \neq j \leq e - 1$, the cyclotomic numbers $(i,i)_e$ and $(j,j)_e$ must be co-orbital, since the relation $(i,j)_e = (ip, jp)_e$ maps all cyclotomic numbers of the form $(i,i)_e$ and $(j,j)_e$ to each other. By the relation $(i,j)_e = (e-i, j-i)_e$, for each $1 \leq i \leq e-1$, the cyclotomic number $(i,i) = (e-i, 0)$, and under the relation $(i,j)_e = (e-i, j-i)_e$, the cyclotomic number $(e-i, 0)_e = (0, e-i)_e$. □

Part (i) of the following Theorem is immediate from the above. Notice that part (ii) then follows by Theorem 1.3.20(i).

Theorem 3.6.2. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^m = ef + 1$, *where* p *is an odd prime. If* e *is an odd prime and* p *is a generator of the multiplicative group* $\mathbb{Z}_e^*$, *then if* $e \mid q-1$*:*

(i) $C_0^{e,m}$ *is a* $(q, \frac{q-1}{e}, \lambda, \mu)$*-PDS in* $\mathrm{GF}(q)$*,*

(ii) any collection of s *distinct cyclotomic classes of order* e *is a* $(q, s, \frac{q-1}{e}, \lambda + (s-1)\mu, s\mu)$*-DPDF in* $\mathrm{GF}(q)$*.*

Example 3.6.3. *Notice that* $\alpha = 3$ *is a multiplicative generator of* $\mathbb{Z}_7^*$*, as* $\alpha^0 = 1$*,* $\alpha = 3$*,* $\alpha^2 = 2$*,* $\alpha^3 = 6$*,* $\alpha^4 = 4$ *and* $\alpha^5 = 6$*. As such when* $e = 7$ *and* $p = 3$*,* $(1,0)_7 = (3,0)_7 = (2,0)_7 = (6,0)_7 = (4,0)_7 = (6,0)_7$ *under the identity* $(i,j)_e = (ip, jp)_e$ *in Theorem 1.4.12, It therefore follows by Lemma 2.1.2 that in any finite field* $\mathrm{GF}(3^m)$*, where* $7 \mid 3^m - 1$*, the cyclotomic class* $C_0^{7,m}$ *is a PDS, and moreover, any collection of order* 7 *cyclotomic classes is a DPDF.*

For example, in the finite field $GF(729)$*,* $7 \mid 728$*, so* C_0^7 *is a* $(729, 104, 19, 12)$*-PDS, and any collection of* u *cyclotomic class of order* 7 *is also a* $(729, 104, 19 + (u-1)12, 12u)$*-DPDF.*

The following Remark demonstrates that this construction is a special case of uniform cyclotomy.

Remark 3.6.4. *Observe that if* p *is a multiplicative generator of* $\mathbb{Z}_e^*$*, then it follows that* $p^{\frac{e-1}{2}} = -1 \mod e$*.*

With further investigation, we hope to use this technique to prove that the external cyclotomic numbers are also identical when p is a generator of the multiplicative group $\mathbb{Z}_e^*$.

Chapter 4

A cyclotomic number algorithm and Denniston PDSs

The cyclotomic frameworks developed in Chapter 2 are a powerful tool for finding new DPDF/EPDF constructions, but can also be deployed as tool to find constructions of other difference families. This Chapter presents the work of two different projects in which I have deployed my knowledge of finite field cyclotomy in order to tackle mathematical problems outside of the remit of finding new DPDF and EPDF constructions.

Section 4.1 develops an algorithm for computing general cyclotomic numbers in large finite fields currently there are no standard methods recorded in the literature which can be used to do this directly [65]. Section 4.2 is an application of the cyclotomic techniques that we developed in Chapter 2, together with the algorithms in Section 4.1, to produce a new PDS with Denniston parameters in elementary abelian groups in which p is odd these PDS were previously thought not to exist [1].

4.1 Algorithm for computing cyclotomic numbers in large finite fields

In this Section, we connect the use of cyclotomic orbits with other standard cyclotomic techniques in order to produce an Algorithm that computes the cyclotomic numbers in large finite fields. The work in this Section is inspired by the preprint [65]. In [65], the authors develop an implicit method for computing a subset of the internal cyclotomic numbers of order 11 in the finite field GF(243). I formalise their approach into an algorithm for directly computing internal cyclotomic numbers. I then expand upon this algorithm and present an algorithm which automatically computes all internal cyclotomic orbit representatives when e and p meet the constraints presented in Theorem 2.2.33. Finally, I also present an algorithm for computing external cyclotomic numbers.

I begin this Section by stepping through the techniques used by Wen et al. in [65] to compute the internal cyclotomic numbers of order 11 in the finite field GF(243) $=$ GF(3^5). I then demonstrate how these techniques can be further developed to produce general algorithms for computing cyclotomic numbers.

4.1.1 The Wen et al. paper

In [65], the authors use the following method to compute all internal cyclotomic numbers of the form $(i,i)_{11}$ where $0 \leq i \leq 10$ in the finite field GF(243). Note that in this particular finite field $p = 3$, $m = 5$, and $|C_0^{11}| = f = 22$ when $e = 11$. Further $n_1 = 5$ and $\epsilon = 2$, in the notation of Chapter 2.

Summary of method for computing internal cyclotomic numbers:

(1) The authors begin by computing all orbits of the form $\mathrm{Orb}_{(i,j)_{11}=(3i,3j)_{11}}(i,i)_e$ for $0 \leq i \leq e-1$. They find that there are precisely three orbits of this form when $e = 11$ and $p = 3$, these are:

$\mathrm{Orb}_{(i,j)_e=(ip,jp)_e}(0,0)_{11} = \{(0,0)_{11}\}$,
$\mathrm{Orb}_{(i,j)_e=(ip,jp)_e}(1,1)_{11} = \{(1,1)_{11},(3,3)_{11},(9,9)_{11},(5,5)_{11},(4,4)_{11}\}$
$\mathrm{Orb}_{(i,j)_e=(ip,jp)_e}(2,2)_{11} = \{(2,2)_{11},(6,6)_{11},(7,7)_{11},(10,10)_{11},(8,8)_{11}\}$.

(2) The authors then use the fact that $-1 \in C_0^{11,5}$ (since $f = 22$ is even, it follows by Lemma 1.4.11 that this is true) to demonstrate that $(0,0)_{11} \geq 1$. Since $\pm 1 \in C_0^{11,5}$ and $(-1) - 1 \equiv 2 - 1 = 1 \mod 3$, it follows that there is at least one pair of elements $a, b \in C_0^{11,5}$ such that $a - b \in C_0^{11,5}$.

(3) The authors then choose an irreducible polynomial of order 6 over GF(3)$[x]$. The polynomial that they choose is the polynomial

$f(x) = x^5 + x^4 + x^3 + x^2 + 2x + 1$, which can be used to show that $x^5 = 2x^4 + 2x^3 + 2x^2 + x + 2 \in \mathrm{GF}(3)[x]$.

(4) Note that if $\{1, \theta, \theta^2, \theta^3, \theta^4\}$ is a basis of GF(243), then for every $\alpha \in \mathrm{GF}(243)$, we may write $\alpha = c_0 + c_1\theta + c_2\theta^2 + c_3\theta^3 + c_4\theta^4$, where $c_0, c_1, c_2, c_3, c_4 \in \mathrm{GF}(3)$: we can also write α in vector form $(\alpha = (c_0c_1c_2c_3c_4))$. Using the irreducible polynomial found in step 3) and primitive element $\theta = (01000)$, the authors compute the elements $\theta^0, \theta^1, \dots, \theta^{11} \in \mathrm{GF}(243)$ in vector form.

$$\begin{aligned} \theta^0 = (10000),\ \theta^1 = (01000),\ \theta^2 = (00100),\ \theta^3 = (00010),\ \theta^4 = (00001),\\ \theta^5 = (21222),\ \theta^6 = (11200),\ \theta^7 = (01120), \theta^8 = (00112), \theta^9 = (12122),\\ \theta^{10} = (10020),\ \theta^{11} = (01002). \end{aligned}$$

(5) With the element $\theta^{11} \in \mathrm{GF}(243)$ computed, the authors go on to compute the first $\frac{f}{2} = 11$ elements of the cyclotomic class C_0^{11}, we label this set D. They find that:

$$\begin{aligned} D &= \{\theta^0, \theta^{11}, \theta^{22}, \theta^{33}, \theta^{44}, \theta^{55}, \theta^{66}, \theta^{77}, \theta^{88}, \theta^{99}, \theta^{110}\}\\ &= \{(10000), (01002), (21101), (21102), (12212), (11112),\\ &\qquad (10121), (12011), (12112), (22002), (02010)\}. \end{aligned}$$

The reason why Wen et al. only compute the first 11 elements of the cyclotomic class $C_0^{11,5}$, instead all 22 elements of $C_0^{11,5}$, will become clear as we progress through their algorithm.

(6) In the paper [65], the authors use a counting argument to obtain the values of cyclotomic numbers of order 11 in GF(243). Notice that a contribution of 2 to the cyclotomic number $(11-i, 11-i)_{11}$ $(0 \leq i \leq 10 = e-1)$ can be obtained from every pair $\{\theta^{11s}, \theta^{11t}\}$, where $0 \leq s \neq t \leq 21$, satisfying $\theta^{11s} - \theta^{11t} = \theta^i$. This is because, given such a pair

$$\theta^{11s} - \theta^{11t} = \theta^i \Leftrightarrow \theta^{11(s-1)+(11-i)} - \theta^{11(t-1)+(11-i)} = 1.$$

Using Lagrange's Theorem and Theorem 1.4.12, we may obtain a second pair of powers of θ contributing to the cyclotomic number $(11-i, 11-i)_{11}$

by rearranging the above equation. Observe

$$\begin{aligned} -(-(\theta^{11(s-1)+(11-i)} - \theta^{11(t-1)+(11-i)})) = 1 \Leftrightarrow \\ -(\theta^{11(t-1)+(11-i)} - \theta^{11(s-1)+(11-i)}) = 1 \Leftrightarrow \\ \theta^{121}(\theta^{11(t-1)+(11-i)} - \theta^{11(s-1)+(11-i)}) = 1 \Leftrightarrow \\ \theta^{11(t+10)+(11-i)} - \theta^{11(s+10)+(11-i)} = 1. \end{aligned}$$

It is therefore clear that since $\theta^{11(s-1)} \neq \theta^{11(s+10)}, \theta^{11(t-1)} \neq \theta^{11(t+10)} \in C_0^{11,5}$, we can think of the above pair $\{\theta^{11s}, \theta^{11t}\}$ satisfying $\theta^{11s} - \theta^{11t} = \theta^i$, as contributing 2 to the cyclotomic number $(11-i, 11-i)_{11}$ $(0 \leq i \leq 10)$. However, notice that when running through all possible values of $0 \leq s \neq t \leq 21$ satisfying $\theta^{11(s)} - \theta^{11(t)} = \theta^i$ $(0 \leq i \leq 10)$, we double count every cyclotomic number of the form $(11-i, 11-i)_{11}$ because the pairs $\{\theta^{11s'}, \theta^{11t'}\}$ and $\{\theta^{11(s'+10)}, \theta^{11(t'+10)}\}(0 \leq s' \neq t' \leq 21)$ are both picked up as we run through all pairs $0 \leq s \neq t \leq 21$, unless we force some restrictions on s and t. (Note that as f is even, every pair $\{\theta^{11s}, \theta^{11t}\}$ satisfying $\theta^{11s} - \theta^{11t} = 1$ should be double counted, except for the pair $\{\theta^{121}, \theta^0\}$, as the expression $\theta^{121} - \theta^0$ is self-inverse. We must therefore count the pairs contributing to the cyclotomic number $(0, 0)_{11}$ in a slightly different manner to cyclotomic numbers of the form $(11-i, 11-i)_{11}$ where $1 \leq i \leq 10$.)

In the paper [65], Wen et al. enforce the restriction that $0 \leq s \neq t \leq 10$ to avoid this double counting. (Note that under this restriction, the pair $\{\alpha^{11(s+10)}, \alpha^{11(t+10)}\}$ won't be picked up independently, since $11 \leq s+10, t+10 \leq 21$ when $0 \leq s \neq t \leq 10$.) However, we see in a later example, that we cannot universally apply this restriction in an arbitrary finite field and compute all cyclotomic numbers.

Using this counting method, Wen et al. find that there is one pair $(\theta^{11s}, \theta^{11t})$ satisfying $\theta^{11s} - \theta^{11t} = \theta^4$ for $0 \leq s \neq t \leq 10$ this is the pair $(\theta^{33}, \theta^{22})$ $((21102) - (21101) = (00001))$, meaning $(7, 7)_{11} \geq 2$. Similarly, they find one pair $(\theta^{11s}, \theta^{11t})$ satisfying $\theta^{11s} - \theta^{11t} = \theta^2$ for $0 \leq s \neq t \leq 10$ this is the pair $(\theta^{88}, \theta^{44})$ $((12112) - (12212) = (00100))$, meaning $(9, 9)_{11} \geq 2$.

(7) As the authors of [65] have not run through all possible pairs $\{\theta^{11(s)}, \theta^{11(t)}\}$ satisfying $0 \leq s \neq t \leq 21$, they need to verify the cyclotomic numbers val-

ues that they have obtained in previous steps they use Theorem 1.4.12 to do this. By letting A denote the cyclotomic number contained in the cyclotomic orbit $\text{Orb}_{(i,j)_e=(ip,jp)_e}(0,0)_{11}$, B denote the value of each cyclotomic number contained in the cyclotomic orbit $\text{Orb}_{(i,j)_e=(ip,jp)_e}(1,1)_{11}$ and C denote the value of the cyclotomic number contained in $\text{Orb}_{(i,j)_e=(ip,jp)_e}(2,2)_{11}$ the authors use Theorem 1.4.12 (c)(i) to establish the equation $21 = A + 5(B+C)$. In part 2), the authors of [65] established that $A \geq 1$, and in part 6), they established that $B, C \geq 2$. By substituting these values into the formula, we obtain $21 = A + 5(B+C)$, and so $A = 1$, $B = C = 2$ are the values of the cyclotomic numbers of order 11.

4.1.2 Comments on Wen et al. algorithm

Most cyclotomic constructions of various types of difference family recorded in the literature are reliant upon uniform cyclotomy (see for example [13],[49]), the computation of cyclotomic numbers via Gauss sums (see for example [2],[67]), results on small e/f (see [34],[52]) or direct computation (as in [60]). However the methods for computing internal cyclotomic numbers of the form $(i,i)_e$ $(0 \leq i \leq e-1)$, in [65] are novel. The approach used in [65] can be viewed as an improvement upon direct computation: to compute the internal cyclotomic numbers in the finite field GF(243) directly, the elements of each cyclotomic class C_i^e, where $0 \leq i \leq e-1$, must be compared to the set $\{\alpha^{se} - 1 | \alpha^{se} \in C_0^{e,m}\}$, whereas the methods of Wen et al. only rely on the comparing the elements of the sets $\alpha^0, \alpha^1, \ldots, \alpha^{10} \in \text{GF}(243)$ to the elements of the set $D \in \text{GF}(243)$, where $D = \{\alpha^{11s} - \alpha^{11t} | 0 \leq s, t \leq 10\}$. In the first approach, 242 non-identity elements of the finite field GF(243) must be computed, whereas using the Wen et al. approach, only 21 elements of GF(243) are required to find the internal cyclotomic numbers it is therefore clear that the methods in [65] are more computationally efficient.

However, the methods of Wen et al. need to be adapted in order to be used as a standard technique for computing the internal cyclotomic numbers of the form $(i,i)_e$ $(0 \leq i \leq e-1)$ in finite fields other than GF(243). As discussed in the previous Subsection, one reason that this method cannot be universally deployed is that the authors of the Wen et al. use a counting technique that cannot be used in all finite fields. Below, I demonstrate why this counting method cannot be used in the finite field GF(729) = GF(3^6).

Example 4.1.1. *In the finite field* GF(729)*, let α be a primitive element of* GF(729)*. In this example, we are looking at the cyclotomic numbers of order* 13*. Notice that for every pair $\{\alpha^{13s}, \alpha^{13t}\}$ $(0 \leq s \neq t \leq 56)$ satisfying $\alpha^{13s} - \alpha^{13t} = \alpha^i$, for some $0 \leq i \leq 13$, we have four possibilities $0 \leq s \neq t \leq 27$, $0 \leq s \leq 27$ and $28 \leq t \leq 56$, $28 \leq s \leq 56$ and $0 \leq t \leq 27$ and $28 \leq s \neq t \leq 56$. If we apply the Wen et al. restriction (i.e. we restrict to powers of α^{13} up to $\frac{f}{2}$), we obtain all pairs $\{\alpha^{13s}, \alpha^{13t}\}$ satisfying $\alpha^{13s} - \alpha^{13t} = \alpha^i$, for some $0 \leq i \leq 13$, where either $0 \leq s \neq t \leq 27$ and $28 \leq s \neq t \leq 56$, but not any pairs in which $0 \leq s \leq 27$ and $28 \leq t \leq 56$ or $28 \leq s \leq 56$ and $0 \leq t \leq 27$.*

There is only one pair $\{\alpha^{13s}, \alpha^{13t}\}$ satisfying $\alpha^{13s} - \alpha^{13t} = \alpha^2$, for $0 \leq s \neq t \leq 27$ this is the pair $\{\alpha^{13(15)} - \alpha^{13(16)}\}$ using the Wen et al. method, this would indicate that $(9,9)_{13} \geq 2$ in the finite field GF(729)*, but infact $(9,9)_{13} = 4$. (To see this, observe that the following pairs all satisfy $\alpha^{13(s)} - \alpha^{13(t)} = \alpha^2$ for $0 \leq s \neq t \leq 56$ $\{\alpha^{13(4)}, \alpha^{13(33)}\}$, $\{\alpha^{13(5)}, \alpha^{13(32)}\}$, $\alpha^{13(15)}, \alpha^{33(16)}\}$ and $\{\alpha^{13(43)}, \alpha^{13(44)}\}$.) Therefore, we see that the counting argument used by Wen et al. is not always able to reliably count the cyclotomic number values in every finite field.*

We can, however, derive the following important result from the methods developed by Wen et al. in [65].

Theorem 4.1.2. *Let* GF(q) *be a finite field of order $q = p^m = ef + 1$, where p is prime and $m \in \mathbb{Z}$. Let $C_i^{e,m} = \alpha^i \langle \alpha^e \rangle$ $(0 \leq i \leq e-1)$ denote the i^{th} cyclotomic class of order e in* GF(q) *and let $(i,i)_e$ $(0 \leq i \leq e-1)$ be an internal cyclotomic number of order e in* GF(q)*. The number of ordered pairs (s,t), where $0 \leq s, t \leq f-1$, satisfying:*

$$\alpha^{es} - \alpha^{et} = \alpha^{e-i}$$

is precisely the cyclotomic number $(i,i)_e$.

Proof. It follows from Definition 1.4.3 that the cyclotomic number $(i,i)_e$ $(0 \leq i \leq e-1)$ is the number of pairs (s', t'), where $0 \leq s', t' \leq f-1$, satisfying:

$$\alpha^{es'+i} - \alpha^{et'+i} = 1.$$

By multiplying each term of the above equation through by α^{e-i}, we obtain:

$$\alpha^{e-i}(\alpha^{es'+i} - \alpha^{et'+i}) = \alpha^{e-i} \Leftrightarrow \alpha^{e(s'+1)} + \alpha^{e(t'+1)} = \alpha^{e-i}.$$

By letting $s \equiv s' + 1 \mod f$ and $t \equiv t' + 1 \mod f$, we see that $(i, i)_e$ $(0 \leq i \leq e - 1)$ is the number of solutions (s, t), where $0 \leq s, t \leq e - 1$, satisfying:

$$\alpha^{se} - \alpha^{te} = \alpha^{e-i}.$$

□

The rest of this Section is dedicated to using the above Theorem to develop an algorithm which computes the internal and external cyclotomic numbers of order e in a finite field GF(q).

4.1.3 Adapted Wen et al. algorithm for computing internal cyclotomic numbers

We can use the ideas presented in Theorem 4.1.2, to develop an algorithm for computing all internal cyclotomic numbers of order e. As Theorem 4.1.2 demonstrates, the cyclotomic number $(i, i)_e$ is equivalent to number of pairs of elements $(\alpha^{se}, \alpha^{te}) \in C_0^e \times C_0^e$ satisfying $\alpha^{se} - \alpha^{te} = \alpha^{e-i}$ (where $0 \leq i \leq e-1$). By developing an algorithm which counts the number of pairs $(\alpha^{se}, \alpha^{te}) \in C_0^e \times C_0^e$ satisfying the above, we can compute each cyclotomic number $(i, i)_e$ $(0 \leq i \leq e-1)$. In later Subsections, we will repeat this process for internal cyclotomic numbers in which we have additional information about the elements of each internal cyclotomic orbit, and can thus build a step into the Algorithm which computes an element of each of the internal orbits to reduce the number of computations required. We will also design a similar algorithm that computes the values of the external cyclotomic numbers.

Whilst we have not tested the computational complexity of these new algorithms (which are all based upon the same methodology) or the standard approach for computing the values of cyclotomic numbers, a dramatic difference can be seen between the two methods when computing the cyclotomic numbers using these methods. In tests that we have run, it takes around two days for the standard method for computing the cyclotomic numbers of order 13 in GF(729), whereas using the methods adapted from the Wen et al., it only takes one afternoon to compute the cyclotomic numbers of order 13 in GF(729).

We now present the first of algorithms, which is used to determine general internal cyclotomic numbers. This Algorithm is presented in pseudocode below.

Algorithm 1 - Internal cyclotomic number algorithm

Input: To determine the cyclotomic number $(b,b)_e$ in the finite field $\mathrm{GF}(p^m)$, input the values of p , m, e and b. Input a primitive polynomial, $\alpha^m = c_0 + c_1\alpha + \ldots c_{m-1}\alpha^{m-1}$, of $\mathrm{GF}(p^m)$, in vector form $(c_0c_1 \ldots c_{m-1})$ (where $0 \leq c_a \leq p-1$ for all $0 \leq a \leq m-1$ and α^1 is a primitive element of $\mathrm{GF}(p^m)$).

Output: The value of the cyclotomic number $(b,b)_e$.

```
smallelt[1] $= \alpha$
**for** $2 \leq i \leq e$ **do**
    smallelt[$i$] $:=$ smallelt[$i-1$]$\alpha$
                                        ▷ Generates the first $e$ powers of $\alpha$ in $\mathrm{GF}(p^m)$
classelt[1] $:=$ smallelt[$e$]
**for** $2 \leq j \leq \frac{p^m-1}{e}$ **do**
    classelt[$i$] $:=$ classelt[$i-1$]smallelt[$e$]
                    ▷ Generates the elements of the cyclotomic class $C_0^{e,m} = \langle \alpha^e \rangle$
bbcount $:= 0$
**for** $1 \leq l \leq \frac{p^m-1}{e} - 1$ **do**
    **for** $l < k \leq \frac{p^m-1}{e}$ **do**
        **if** classelt[$k$] $-$ classelt[$l$] $=$ smallelt[$e-b$] **then**
            bbcount $:=$ bbcount $+ 1$
        **else if** classelt[$l$] $-$ classelt[$k$] $=$ smallelt[$e-b$] **then**
            bbcount $:=$ bbcount $+ 1$
print “(”$b$“,”$b$“)” $=$ bbcount
    ▷ This loop determines the cyclotomic number $(b,b)_e$ by calculating the number
                                of pairs of elements in $C_0^e$ with difference $\alpha^{e-b}$
```

We will now step through the design of this Algorithm. Algorithm 1 requires the computation of all f elements of the cyclotomic class $C_0^{e,m}$, as well as the first e powers of a primitive element $\alpha \in \mathrm{GF}(q)$, whereas the Algorithm used by Wen et al. only requires the computation of $\frac{f}{2} + e$ elements of $\mathrm{GF}(243)$. However, we can see that Algorithm 1 can be used to find all internal cyclotomic numbers of the form $(i,i)_e$ (where $0 \leq i \leq e-1$) in any finite field $\mathrm{GF}(q)$, while (as demonstrated in Example 4.1.1) the implicit Wen et al. algorithm won't be able to compute all cyclotomic numbers in a given finite field.

In the following example, we demonstrate how Algorithm 1, and prior knowledge about the elements contained within each of the cyclotomic orbits when $e = 11$, can be used to provide an alternative way of finding all internal cyclotomic numbers of order $e = 11$ in the finite field $\mathrm{GF}(243)$.

Example 4.1.3. *As identified in Example 2.2.31, there are precisely* $\epsilon + 1 = 3$ *internal cyclotomic orbits in the finite field* $\mathrm{GF}(243)$ *when* $e = 11$*, these are*

$$\begin{aligned}
\mathrm{Orb}_{\mathfrak{R}}(0,0)_{11} &= \{(0,0)_{11}\}\\
\mathrm{Orb}_{\mathfrak{R}}(1,1)_{11} &= \{(1,1)_{11}, (3,3)_{11}, (9,9)_{11}, (5,5)_{11}, (4,4)_{11}, (10,0)_{11}, (8,0)_{11}, (2,0)_{11},\\
&\qquad (6,0)_{11}, (7,0)_{11}, (0,10)_{11}, (0,8)_{11}, (0,2)_{11}, (0,6)_{11}, (0,7)_{11}\},\\
\mathrm{Orb}_{\mathfrak{R}}(2,2)_{11} &= \{(2,2)_{11}, (6,6)_{11}, (7,7)_{11}, (10,10)_{11}, (8,8)_{11}, (9,0)_{11}, (5,0)_{11},\\
&\qquad (4,0)_{11}, (1,0)_{11}, (3,0)_{11}, (0,9)_{11}, (0,5)_{11}, (0,4)_{11}, (0,1)_{11}, (0,3)_{11}\}.
\end{aligned}$$

We can see that the cyclotomic orbit representatives of each of these orbits are $(0,0)_{11}$*,* $(1,1)_{11}$ *and* $(2,2)_{11}$ *thus by substituting each of these cyclotomic numbers into Algorithm 1, we obtain all of the internal cyclotomic numbers of order* $e = 11$*.*

When Algorithm 1 is given $(0,0)_{11}$*, the Algorithm finds that the only pair* $(\alpha^{se}, \alpha^{te}) \in C_0^{11,5} \times C_0^{11,5}$ *satisfying* $\alpha^{se} - \alpha^{te} = 1$ *is the pair* $(\alpha^{121}, \alpha^{0})$*, hence* $(0,0)_{11} = 1$*. When Algorithm 1 is given* $(1,1)_{11}$*, it is found that the only two pairs of cyclotomic numbers* $(\alpha^{se}, \alpha^{te}) \in C_0^{11,5} \times C_0^{11,5}$ *satisfying* $\alpha^{se} - \alpha^{te} = \alpha^{11-1} = \alpha^{10}$ *are the pairs* $(\alpha^{33}, \alpha^{55})$ *and* $(\alpha^{176}, \alpha^{154})$*, therefore* $(1,1)_{11} = 2$*. Finally, the only two pairs of cyclotomic numbers* $(\alpha^{se}, \alpha^{te}) \in C_0^{11,5} \times C_0^{11,5}$ *satisfying* $\alpha^{se} - \alpha^{te} = \alpha^{11-2} = \alpha^{9}$ *are* $(\alpha^{66}, \alpha^{11})$ *and* $(\alpha^{132}, \alpha^{187})$*, so* $(2,2)_{11} = 2$*. We then know that every cyclotomic number in the same cyclotomics as the cyclotomic numbers* $(1,1)_{11}$ *and* $(2,2)_{11}$ *must also equal* 2*.*

As demonstrated in Example 4.1.3, prior knowledge of the structure of the cyclotomic orbits, simplifies the process of computing the internal cyclotomic numbers of order e. In Theorem 2.2.33, I was able to demonstrate that when $e \geq 5$, p is odd and $n_1 = \mathrm{ord}_e(p)$ is odd, the cyclotomic orbit representative of every internal cyclotomic orbit $\mathrm{Orb}_{\mathfrak{R}}(i,j)_e$ (where $\mathfrak{R} = \{(i,j)_e = (j,i)_e, (i,j)_e = (e-i, j-i)_e, (i,j)_e = (ip, jp)_e\}$) has to be the cyclotomic number $(\alpha_{j,\epsilon}, \alpha_{j,\epsilon})_e$, where $\alpha_{j,\epsilon}$ is the lexicographically smallest element contained within the cyclotomic class $C_j^{\epsilon,1} \subseteq \mathrm{GF}(e)$. I therefore decided to create an extended version of Algorithm 1, which computes the lexicographically smallest element of the cyclotomic class

$C_0^{\epsilon,1} \cong \langle p \rangle$, we can therefore build an Algorithm that directly computes the value of the cyclotomic orbit representative of each internal cyclotomic orbit when $e \geq 5$ is prime, p is odd and $n_1 = \mathrm{ord}_e(p)$ is odd. By then applying the relations $\mathfrak{R} = \{(i,j)_e = (j,i)_e, (i,j)_e = (e-i, j-i)_e, (i,j)_e = (ip, jp)_e\}$ to each of the cyclotomic orbit representative $(\alpha_{j,\epsilon}, \alpha_{j,\epsilon})_e$, we are able compute the internal cyclotomic numbers of order e more efficiently. The pseudocode on the next page (labelled Algorithm 2) describes this process in more detail. Below I demonstrate how Algorithm 2 computes the internal cyclotomic numbers using our running example where $e = 11$ in the finite field $\mathrm{GF}(243)$.

Example 4.1.4. *Algorithm 2 can also be used to identify the internal cyclotomic numbers of order $e = 11$ in the finite field $\mathrm{GF}(243)$, since $e = 11$ and $p = 3$ are both prime, and here $n_1 = \mathrm{ord}_e(p) = 5$ however, in Algorithm 2, the Algorithm computes the internal cyclotomic orbit representatives automatically. Once the values of $e = 11$, $p = 3$ and $n_1 = 5$ have been substituted into the Algorithm, the Algorithm computes the cyclotomic orbit representatives, by finding the lexicographically smallest b in each cyclotomic coset $\mathbb{C}_i = i\langle p \rangle$, where $0 \leq i \leq e-1$. In this example, the Algorithm identifies that the lexicographically smallest elements in each of the three cyclotomic cosets are the elements 0, 1 and 2.*

Once the Algorithm has identified the lexicographically smallest element $b \in \mathbb{C}_i$, it automatically computes the cyclotomic number $(b,b)_{11}$. So in this example, Algorithm 2 automatically computes the cyclotomic numbers $(0,0)_{11}$, $(1,1)_{11}$ and $(2,2)_{11}$. The actual process used to compute each of the cyclotomic numbers is analogous to the process used in Algorithm 1 to compute each cyclotomic number $(b,b)_{11}$.

Algorithm 2 - `Internal cyclotomic number algorithm: special case`

Input: For the finite field GF(p^m), specify the prime p, the integer m, a prime value of $e \geq 5$ and the value of $n_1 = \text{ord}_e(p)$. Input a primitive polynomial, $\alpha^m = c_0 + c_1\alpha + \ldots c_{m-1}\alpha^{m-1}$, of GF($p^m$), in vector form $(c_0c_1 \ldots c_{m-1})$ (where $0 \leq c_a \leq p-1$ for all $0 \leq a \leq m-1$ and α^1 is a primitive element of GF(p^m)).

Output: The value of each cyclotomic number of the form $(b,b)_e$, where $0 \leq b \leq e-1$.

```
 1: smallelt[1] := $\alpha$
 2: for $2 \leq i \leq e$ do
 3:    smallelt[$i$] := smallelt[$i-1$]$\alpha$
                                   ▷ Generates the first $e$ powers of $\alpha$ in GF($p^m$)
 4: classelt[1] := smallelt[$e$]
 5: for $2 \leq j \leq \frac{p^m-1}{e}$ do
 6:    classelt[$i$] := classelt[$i-1$]smallelt[$e$]
                      ▷ Generates the elements of the cyclotomic class $C_0^{e,m} = \langle\alpha^e\rangle$
 7: for $0 \leq b \leq e-1$ do
 8:    for $1 \leq c \leq n_1 - 1$ do
 9:       if $bp^c \mod e < b$ then
10:          next $b$
              ▷ The nested for loop in lines 7-10 is identifying the orbit representatives
                                     we skip $b$ if it is not the orbit representative
11:    bbcount := 0
12:    for $1 \leq l \leq \frac{p^m-1}{e} - 1$ do
13:       for $l < k \leq \frac{p^m-1}{e}$ do
14:          if classelt[$k$] − classelt[$l$] := smallelt[$e-b$] then
15:             bbcount := bbcount + 1
16:          else if classelt[$l$] − classelt[$k$] := smallelt[$e-b$] then
17:             bbcount := bbcount + 1
18:    print “(”$b$“,”$b$“)” = bbcount
      ▷ This loop determines the cyclotomic number $(b,b)_e$ by calculating the number
                                   of pairs of elements in $C_0^e$ with difference $\alpha^{e-b}$
```

4.1.4 Algorithm for computing external cyclotomic numbers

After determining the two previous algorithms that compute all internal cyclotomic numbers of order e in a finite field $\mathrm{GF}(q)$ we decided that it would useful to write an Algorithm that was able to compute all external cyclotomic numbers in a given finite field. As a first step in this process, I found an external analogue of Theorem 4.1.2.

Theorem 4.1.5. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^m = ef + 1$, *where* p *is prime and* $m \in \mathbb{Z}$. *Let* $C_i^{e,m} = \alpha^i\langle\alpha^e\rangle$ $(0 \leq i \leq e-1)$ *denote the* i^{th} *cyclotomic class of order* e *in* $\mathrm{GF}(q)$ *and let* $(i,j)_e$ $(1 \leq i \neq j \leq e-1)$ *be an external cyclotomic number of order* e *in* $\mathrm{GF}(q)$. *The number of ordered pairs* (s,t), *where* $0 \leq s,t \leq f-1$, *satisfying:*

$$\alpha^{es} - \alpha^{et+d} = \alpha^{e-i},$$

where $d \equiv j - i \mod e$, *is the cyclotomic number* $(i,j)_e$.

Proof. It follows from Definition 1.4.3 that the cyclotomic number $(i,j)_e$ $(1 \leq i \neq j \leq e-1)$ is the number of pairs (s',t'), where $0 \leq s',t' \leq f-1$, satisfying:

$$\alpha^{es'+i} - \alpha^{et'+j} = 1.$$

By multiplying each term of the above equation through by α^{e-i}, we obtain:

$$\alpha^{e-i}(\alpha^{es'+i} - \alpha^{et'+j}) = \alpha^{e-i} \Leftrightarrow \alpha^{e(s'+1)} + \alpha^{e(t'+1)+j-i} = \alpha^{e-i}.$$

By letting $s \equiv s'+1 \mod f$, $t \equiv t'+1 \mod f$ and $d \equiv j-i \mod e$, we see that $(i,j)_e$ $(1 \leq i \neq j \leq e-1)$ is the number of solutions (s,t), where $0 \leq s,t \leq e-1$, satisfying:

$$\alpha^{se} - \alpha^{te+d} = \alpha^{e-i}.$$

□

Using this Theorem 4.1.5, we can give the following algorithm which computes the value of any cyclotomic number of order e in a given finite field $\mathrm{GF}(q)$.

Algorithm 3 - `External cyclotomic number calculator`

Input: To calculate the value of the cyclotomic number $(i,j)_e$ in the finite field GF(p) input the values of: p, n, e, i and j. Further, input a primitive polynomial, $\alpha^n = c_0 + c_1\alpha + \ldots c_{n-1}\alpha^{n-1}$, of GF$(p^m)$, in vector form $(c_0c_1\ldots c_{n-1})$ (where $0 \leq c_a \leq p-1$ for all $0 \leq a \leq n-1$ and α is a primitive element of GF(p^m)). **Output:** The value of the cyclotomic number $(i,j)_e$.

```
smallelt[1] := $\alpha$
for $2 \leq k \leq e$ do
    smallelt[$k$] := smallelt[$k-1$]$\alpha$
                        ▷ Generates the first $e$ powers of $\alpha$ in GF$(p^m)$
classelt[1] := smallelt[$e$]
for $2 \leq l \leq \frac{p^m-1}{e}$ do
    classelt[$l$] := classelt[$l-1$]smallelt[$e$]
                        ▷ Generates the elements of the cyclotomic class $C_0^{e,n} = \langle\alpha^e\rangle$
$d := j - i$
otherclasselt[1] := smallelt[$d$]
for $2 \leq m \leq \frac{p^m-1}{e}$ do
    otherclasselt[$m$] := otherclasselt[$m-1$]smallelt[$e$]
                        ▷ Generates the elements of the cyclotomic class $C_d^{e,n} = \alpha^d\langle\alpha^e\rangle$
$z := e - i$
ijcount := 0
for $1 \leq r \leq \frac{p^m-1}{e}$ do
    for $1 \leq s \leq \frac{p^m-1}{e}$ do
        if classelt[$r$] − otherclasselt[$s$] := $\alpha^z$ then
            ijcount := ijcount + 1
print ijcount
        ▷ This loop determines the cyclotomic number $(i,j)_e$ by calculating the number
                        of pairs of elements in $C_0^e \times C_d^e$ with difference $\alpha^{e-b}$
```

Note that once we have further results about the cyclotomic orbit representatives of external cyclotomic orbits, we will be able to make this Algorithm more efficient by writing in such a way that all external orbit representatives will be automatically generated by this Algorithm. For now, this Algorithm can be used by substituting in the external cyclotomic orbit representatives. In the Example below, I demonstrate how this Algorithm can be used to determine the external cyclotomic numbers of order $e = 11$ in the finite field GF(243).

Example 4.1.6. *In the finite field* GF(243)*, when* $e = 11$*, we know from Example 2.2.31 that the external cyclotomic orbits under the relations* $\mathfrak{R} = \{(i,j)_e = (j,i)_e, (i,j)_e = (e-i, j-i)_e, (i,j)_e = (ip, jp)_e\}$ *are*

$$\begin{aligned}
\text{Orb}_{\mathfrak{R}}(1,2)_{11} = \{&(1,2)_{11},(3,6)_{11},(9,7)_{11},(5,10)_{11},(4,8)_{11},(2,1)_{11},(6,3)_{11},(7,9)_{11},\\
&(10,5)_{11},(8,4)_{11},(10,1)_{11},(8,3)_{11},(2,9)_{11},(6,5)_{11},(7,4)_{11},(1,10)_{11},\\
&(3,8)_{11},(9,2)_{11},(5,6)_{11},(4,7)_{11},(9,10)_{11},(5,8)_{11},(4,2)_{11},(1,6)_{11},\\
&(3,7)_{11},(10,9)_{11},(8,5)_{11},(2,4)_{11},(6,1)_{11},(7,3)_{11}\}\\
\text{Orb}_{\mathfrak{R}}(4,5)_{11} = \{&(1,3)_{11},(3,9)_{11},(9,5)_{11},(5,4)_{11},(4,1)_{11},(3,1)_{11},(9,3)_{11},(5,9)_{11},\\
&(4,5)_{11},(1,4)_{11},(10,2)_{11},(8,6)_{11},(2,7)_{11},(6,10)_{11},(7,8)_{11},(2,10)_{11},\\
&(6,8)_{11},(7,2)_{11},(10,6)_{11},(8,7)_{11},(8,9)_{11},(2,5)_{11},(6,4)_{11},(7,1)_{11},\\
&(10,3)_{11},(9,8)_{11},(5,2)_{11},(4,6)_{11},(1,7)_{11},(3,10)_{11}\}\\
\text{Orb}_{\mathfrak{R}}(3,4)_{11} = \{&(1,5)_{11},(3,4)_{11},(9,1)_{11},(5,3)_{11},(4,9)_{11},(5,1)_{11},(4,3)_{11},(1,9)_{11},\\
&(3,5)_{11},(9,4)_{11},(10,4)_{11},(8,1)_{11},(2,3)_{11},(6,9)_{11},(7,5)_{11},(4,10)_{11},\\
&(1,8)_{11},(3,2)_{11},(9,6)_{11},(5,7)_{11},(6,7)_{11},(7,10)_{11},(10,8)_{11},(8,2)_{11},\\
&(2,6)_{11},(7,6)_{11},(10,7)_{11},(8,10)_{11},(2,8)_{11},(6,2)_{11}\}.
\end{aligned}$$

Therefore the cyclotomic orbit representatives are the cyclotomic numbers $(1,2)_{11}$, $(4,5)_{11}$ *and* $(3,4)_{11}$*. Therefore these are the external cyclotomic numbers that we substitute into Algorithm 3 in order to determine the value of each external cyclotomic number of order* $e = 11$*.*

In each of these cases $d = |j - i| = 1$*, so the Algorithms compute all elements of the cyclotomic* $C_0^{\epsilon,1} \cong \langle p\rangle \subset \text{GF}(e)$ *and all elements of the cyclotomic class* $C_1^{\epsilon,1}$ *as well. The second stage of the Algorithm runs through all pairs* $(\alpha^{se}, \alpha^{te+1}) \in C_0^{\epsilon,1} \times C_1^{\epsilon,1}$ *to determine the value of each of the above cyclotomic numbers.*

The Algorithm finds that there is only 1 *pair of elements* $(\alpha^{se}, \alpha^{te+1}) \in C_0^{\epsilon,1} \times C_1^{\epsilon,1}$ *such that* $\alpha^{se} - \alpha^{te+1} = \alpha^{e-2} = \alpha^9$*, this is the pair* $(\alpha^{231}, \alpha^{67})$ *meaning* $(1,2)_{11} = 1$*. The Algorithm then identifies* 1 *pair of the form* $(\alpha^{se}, \alpha^{te+1}) \in C_0^{\epsilon,1} \times C_1^{\epsilon,1}$ *such that* $\alpha^{se} - \alpha^{te+1} = \alpha^{e-5} = \alpha^6$*, this is the pair* $(\alpha^{99}, \alpha^{188})$ *meaning that* $(4,5)_{11} = 1$*. Finally the Algorithm identifies that there are* 4 *pairs of the form* $(\alpha^{se}, \alpha^{te+1}) \in C_0^{\epsilon,1} \times C_1^{\epsilon,1}$ *such that* $\alpha^{se} - \alpha^{te+1} = \alpha^{e-4} = \alpha^7$*, these are the pairs* $(\alpha^{77}, \alpha^{34})$*,* $(\alpha^{55}, \alpha^{89})$*,* $(\alpha^{165}, \alpha^{166})$ *and* $(\alpha^{22}, \alpha^{210})$*. From this Algorithm we deduce that* $(3,4)_{11} = 4$*. All cyclotomic numbers in the respective orbits of* *these cyclotomic orbit representatives take the same value as their respective orbit representative.*

4.2 Denniston partial difference sets

I developed the results in this Section whilst my supervisor and I were undertaking a collaborative research project with Prof. Jim Davis and Prof. John Polhill, looking at the relationship between partial difference sets with Denniston parameters and cyclotomy. We were asked to take part in this collaborative research project with a view to establishing a cyclotomic interpretation of PDSs with Denniston parameters. My work in this Section was instrumental in giving us an understanding of the cyclotomic situation and clarified the need to develop proof techniques that combine both character theory and cyclotomy in order to further generalise Denniston's results. Our results establishing the existence of cyclotomic Denniston PDSs occur in [20]; however in this Chapter, I only present the work for which I had the key input.

4.2.1 Background

A PDS with parameters $(p^{3m}, p^r(p^m - p^{m-r} + 1)(p^m - 1), p^r(p^{m-r} - 1 + (p^m - p^{m-r} + 1)(p^r - 2)), p^r(p^m - p^{m-r} + 1)(p^r - 1))$, where p is prime, $m \geq 2$ and $1 \leq r < m$, is said to have Denniston parameters. In [23] Denniston provides a construction technique that can be used to find PDSs with parameters $(2^{3m}, 2^r(2^m - 2^{m-r} + 1)(2^m - 1), 2^r(2^{m-r} - 1 + (2^m - 2^{m-r} + 1)(2^r - 2)), 2^r(2^m - 2^{m-r} + 1)(2^r - 1))$ for every value of $1 \leq r < m$ (i.e. all PDSs with Denniston parameters that exist in the elementary abelian group $\mathbb{Z}_2^{3m}$, where $m \geq 2$). These correspond to maximal arcs in Desarguesian projective planes of even order. Since such arcs do not exist in odd characteristic, it was assumed that no Denniston PDSs would exist for odd primes [1]: as such little attention has been paid to PDSs with Denniston parameters until recently [6] and [24].

In undertaking this research project, we aimed to extend Denniston's results in [23] to the elementary abelian group $\mathbb{Z}_p^{3m}$, where $m \geq 2$ and p is an odd prime, meaning that each PDS has parameters $(p^{3m}, p^r(p^m - p^{m-r} + 1)(p^m - 1), p^r(p^{m-r} - 1 + (p^m - p^{m-r} + 1)(p^r - 2)), p^r(p^m - p^{m-r} + 1)(p^r - 1))$ for $1 \leq r < m$. Our motivation for looking at PDSs of this type arose from computational investigations undertaken by Prof. Jim Davis and Prof. John Polhill. The next two Theorems outline the main results from our paper [20]. The first of these results demonstrates that a PDS with Denniston parameters in which $r = 1$ and $m \geq 2$ exists in the elementary abelian group $\mathbb{Z}_p^{3m}$ when p is odd.

Theorem 4.2.1. *Let ω be a primitive element of* $\mathrm{GF}(p^m)$ *and let* $C_i^{\frac{p^m-1}{p-1},2m} \subseteq \mathrm{GF}(p^{2m})$*. The set*

$$\mathcal{D} := \bigcup_{i=0}^{\frac{p^m-1}{p-1}-1} (\omega^i \langle \omega^{\frac{p^m-1}{p-1}} \rangle) \times (C_i^{\frac{p^m-1}{p-1},2m} \cup \{0_{\mathrm{GF}(p^{2m})}\})$$

is a $(p^{3m}, (p^m-1)\cdot((p-1)(p^m+1)+1), p^m - p + (p^{m+1} - p^m + p)(p-2), (p^{m+1} - p^m + 1)(p-1))$*-PDS in* $\mathrm{GF}(p^m) \times \mathrm{GF}(p^{2m})$*.*

By applying Delsarte's Duality Theorem (for further information see [22]) to the parameters of $\mathcal{D}$ we were able to prove the second major result of our paper: a PDS with Denniston parameters in which $r = m - 1$ and $m \geq 2$ exists in the elementary abelian group $\mathbb{Z}_p^{3m}$ when p is odd.

Theorem 4.2.2. *Let $\mathcal{D}'$ be the dual of $\mathcal{D}$ in $\mathbb{Z}_p^{3m}$ (here we are viewing the group $\mathbb{Z}_p^{3m}$ as* $\mathrm{GF}(p^m) \times \mathrm{GF}(p^{2m})$*; for the defintion of $\mathcal{D}$ see Theorem 4.2.1). Then $\mathcal{D}'$ is a* $(p^{3m}, (p^{2m-1} - p^m + p^{m-1})(p^m - 1), p^m - p^{m-1} + (p^{2m-1} - p^m + p^{m-1})(p^{m-1} - 2), (p^{2m-1} - p^m + p^{m-1})(p^{m-1} - 1))$*-PDS.*

The proof of Theorem 4.2.1 (and thus of Theorem 4.2.2), which we ultimately presented in [20], was expressed in terms of character theory. The character theory argument can be split into three non-trivial cases: two cases in which there is a non-principal character and a principal character, and a third case in which both characters are non-prinicipal. The third case depended on demonstrating that the kernel of a certain character had a particular form: this could not be proven using a purely character theoretic approach. However, we realised that we could express the kernel cyclotomically, and used finite field cyclotomy to determine that the kernel satisfied the desired properties. Let $\mathrm{Tr}_{m/1} : \mathrm{GF}(p^m) \to \mathrm{GF}(p)$ be the trace map, given by $\mathrm{Tr}_{m/1}(x) = x + x^p + x^{p^2} + \ldots + x^{p^{m-1}}$, then proving this result boils down to using finite field cyclotomy to determine that the set:

$$D_0^{\frac{p^m-1}{p-1},2m} = \left(\bigcup_{j\in I} C_j^{\frac{p^m-1}{p-1},2m}\right) \cup \{0_{\mathrm{GF}(p^{2m})}\} \subset \mathrm{GF}(p^{2m}), \tag{4.1}$$

where $I = \{l \,|\, \mathrm{Tr}_{m/1}(\alpha^l) = 0,\ \alpha^l \in \mathrm{GF}(p^m)\}$, is a PDS in the group $\mathbb{Z}_p^{2m}$ when $m \geq 2$. Using quadratic forms and cyclotomy, we were able to prove in [20] that the set $D_0^{\frac{p^m-1}{p-1},2m}$ is indeed a regular $(p^{2m}, p^{m-1}(p^m - p + 1), p^{m-1}(p^{m-1} - p + 1), p^{m-1}(p^{m-1} - 1))$-PDS in the group $\mathbb{Z}_p^{2m}$, and were thus able to prove that $\mathcal{D}$ and $\mathcal{D}'$ are both PDSs with Denniston parameters in the group $\mathbb{Z}_p^{3m}$. Understanding of the cyclotomic structure of $\mathcal{D}$, gained from my direct computation, was instrumental in developing this approach.

In the next Subsection, I will discuss the initial approach to proving that $D_0^{\frac{p^m-1}{p-1},2m}$ is a PDS in the $\mathbb{Z}_p^{2m}$. This approach centred on direct computation in small groups to attempt to determine a general, purely cyclotomic proof that $D_0^{\frac{p^m-1}{p-1},2m}$ is a PDS in the $\mathbb{Z}_p^{2m}$. The majority of Subsection 4.2.2 is dedicated to looking at a particular example in the finite field GF(729). We will prove that for all $0 \leq i \leq \frac{p^m-1}{p-1} - 1 = 12$, the set

$$D_i^{13,6} = C_i^{13,6} \cup C_{i+4}^{13,6} \cup C_{i+10}^{13,6} \cup C_{i+12}^{13,6} \cup \{0_{\mathrm{GF}(729)}\}, \tag{4.2}$$

(where $I = \{l \mid \mathrm{Tr}_{3/1}(\alpha^l) = 0, \alpha^l \in \mathrm{GF}(3^3)\} = \{0, 4, 10, 12\}$) forms a $(729, 225, 63, 72)$-PDS in the finite field GF(729) using a purely cyclotomic argument. We will also discuss the limitations of current cyclotomic techniques in generalising this result to other finite fields.

4.2.2 Proving that a PDS with Denniston parameters in which $r = 1$ exists in $\mathbb{Z}_3^9$

As we can see from the definition of the set $D_i^{13,6} = C_i^{13,6} \cup C_{i+4}^{13,6} \cup C_{i+10}^{13,6} \cup C_{i+12}^{13,6} \cup \{0_{\mathrm{GF}(729)}\}$ (where $0 \leq i \leq 12$), the set $D_i^{13,6}$ comprises a union of cyclotomic classes in the finite field GF(729). By thinking of each set $D_i^{13,6}$ in this way, we can adapt some of the techniques that we developed in Chapter 3 to understand more about the structure of each $D_i^{13,6}$ and thus prove that each $D_i^{13,6}$ is a partial difference set.

In the Lemma below, we decompose the multiset $\Delta(D_i^{13,6})$ into a union of multisets of the form $\Delta(C_i^{13,6}, C_j^{13,6})$ (where $0 \leq i, j \leq e-1$). Note that in all following results in this Subsection, we write $0_{\mathrm{GF}(729)}$ as 0, since we are only looking at results in the finite field GF(729) in this subsection.

Lemma 4.2.3. *In the finite field* GF(729)*, let* α *be a primitive element of* GF(729)*,* $C_j^{13,6}$ *denote the* j^{th} *cyclotomic class of order* 13*,* $I = \{0, 4, 10, 12\}$ *and for* $0 \leq i \leq 12$*, let* $S_i^{13,6} = D_i^{13,6} \backslash \{0\}$*, where* $D_i^{13,6} = C_i^{13,6} \cup C_{i+4}^{13,6} \cup C_{i+10}^{13,6} \cup C_{i+12}^{13,6} \cup \{0\}$*. It then follows that*

(i) $\Delta(S_0^{13,6}) = \bigcup_{l \in I}(\Delta(C_l^{13,6}, C_0^{13,6}) \cup \alpha^4 \Delta(C_{l-4}^{13,6}, C_0^{13,6}) \cup \alpha^{10}\Delta(C_{l-10}^{13,6}, C_0^{13,6}) \cup \alpha^{12}\Delta(C_{l-12}^{13,6}, C_0^{13,6})) - 224\{0\}$,

(ii) $\Delta(S_i^{13,6}) = \alpha^i \Delta(S_0^{13,6})$.

(iii) $\Delta(D_i^{13,6}) = \Delta(S_i^{13,6}) \cup 2S_0^{13,6}$.

Proof. (i) Notice that since $\frac{729-1}{13} = 56$, for $0 \leq r \leq e-1$, each cyclotomic class $C_r^{13,6}$ has cardinality 56, meaning that as $S_0^{13,6} = C_0^{13,6} \cup C_4^{13,6} \cup C_{10}^{13,6} \cup C_{12}^{13,6}$, S_0 has cardinality 224. It then follows by Remark 1.2.2 that $\Delta(S_0^{13,6}, S_0^{13,6}) = \Delta(S_0^{13,6}) \cup 224\{0\}$. Since $S_0^{13,6} = C_0^{13,6} \cup C_4^{13,6} \cup C_{10}^{13,6} \cup C_{12}^{13,6}$, this means that we can partition the multiset $\Delta(S_0^{13,6}, S_0^{13,6})$ as follows

$$\begin{aligned}\Delta(S_0^{13,6}, S_0^{13,6}) =& \Delta(C_0^{13,6}, C_0^{13,6}) \cup \Delta(C_4^{13,6}, C_0^{13,6}) \cup \Delta(C_{10}^{13,6}, C_0^{13,6}) \cup \\ & \Delta(C_{12}^{13,6}, C_0^{13,6}) \cup \Delta(C_0^{13,6}, C_4^{13,6}) \cup \Delta(C_4^{13,6}, C_4^{13,6}) \cup \\ & \Delta(C_{10}^{13,6}, C_4^{13,6}) \cup \Delta(C_{12}^{13,6}, C_4^{13,6}) \cup \Delta(C_0^{13,6}, C_{10}^{13,6}) \cup \\ & \Delta(C_4^{13,6}, C_{10}^{13,6}) \cup \Delta(C_{10}^{13,6}, C_{10}^{13,6}) \cup \Delta(C_{12}^{13,6}, C_{10}^{13,6}) \cup \\ & \Delta(C_0^{13,6}, C_{12}^{13,6}) \cup \Delta(C_4^{13,6}, C_{12}^{13,6}) \cup \Delta(C_{10}^{13,6}, C_{12}^{13,6}) \cup \\ & \Delta(C_{12}^{13,6}, C_{12}^{13,6}) \\ =& \bigcup_{l \in I} \Delta\left(C_l^{13,6}, C_0^{13,6}\right) \cup \bigcup_{l \in I} \Delta\left(C_l^{13,6}, C_4^{13,6}\right) \cup \\ & \bigcup_{l \in I} \Delta\left(C_l^{13,6}, C_{10}^{13,6}\right) \cup \bigcup_{l \in I} \Delta\left(C_l^{13,6}, C_{12}^{13,6}\right).\end{aligned}$$

By Lemma 2.1.18(iii), we may rewrite the equation for $\Delta(S_0^{13,6}, S_0^{13,6})$ as

$$\begin{aligned}\Delta(S_0^{13,6}, S_0^{13,6}) =& \bigcup_{l\in I}\Delta\left(C_l^{13,6}, C_0^{13,6}\right) \cup \alpha^4 \bigcup_{l\in I}\Delta\left(C_{l-4}^{13,6}, C_0^{13,6}\right) \cup \\ & \alpha^{10}\bigcup_{l\in I}\Delta\left(C_{l-10}^{13,6}, C_0^{13,6}\right) \cup \alpha^{12}\bigcup_{l\in I}\Delta\left(C_{l-12}^{13,6}, C_0^{13,6}\right) \\ =& \bigcup_{l\in I}(\Delta(C_l^{13,6}, C_0^{13,6}) \cup \alpha^4\Delta\left(C_{l-4}^{13,6}, C_0^{13,6}\right) \cup \\ & \alpha^{10}\Delta\left(C_{l-10}^{13,6}, C_0^{13,6}\right) \cup \alpha^{12}\Delta\left(C_{l-12}^{13,6}, C_0^{13,6}\right)).\end{aligned}$$

As above, $\Delta(S_0^{13,6}) = \Delta(S_0^{13,6}, S_0^{13,6}) - 224\{0\}$. It then follows that

$$\begin{aligned}\Delta(S_0^{13,6}) =& \bigcup_{l\in I}(\Delta(C_l^{13,6}, C_0^{13,6}) \cup \alpha^4\Delta\left(C_{l-4}^{13,6}, C_0^{13,6}\right) \cup \alpha^{10}\Delta\left(C_{l-10}^{13,6}, C_0^{13,6}\right) \\ & \cup\ \alpha^{12}\Delta\left(C_{l-12}^{13,6}, C_0^{13,6}\right)) - 224\{0\}.\end{aligned}$$

(ii) As above

$$\begin{aligned}\Delta(S_i^{13,6}) =& \bigcup_{l\in I}(\Delta(C_{l+i}^{13,6}, C_i^{13,6}) \cup \alpha^4\Delta\left(C_{l-4+i}^{13,6}, C_i^{13,6}\right) \cup \alpha^{10}\Delta\left(C_{l-10+i}^{13,6}, C_i^{13,6}\right) \\ & \cup\ \alpha^{12}\Delta\left(C_{l-12+i}^{13,6}, C_i^{13,6}\right)) - 224\{0\} \qquad .\end{aligned}$$

By Lemma 2.1.18(iii), we may then write

$$\begin{aligned}\Delta(S_i^{13,6}) =& \bigcup_{l\in I}(\alpha^i\Delta(C_l^{13,6}, C_0^{13,6}) \cup \alpha^i\alpha^4\Delta\left(C_{l-4}^{13,6}, C_0^{13,6}\right) \\ & \cup \alpha^i\alpha^{10}\Delta\left(C_{l-10}^{13,6}, C_0^{13,6}\right) \cup\ \alpha^i\alpha^{12}\Delta\left(C_{l-12}^{13,6}, C_0^{13,6}\right)) - 224\{0\}, \\ =& \alpha^i(\bigcup_{l\in I}(\Delta(C_l^{13,6}, C_0^{13,6}) \cup \alpha^4\Delta\left(C_{l-4}^{13,6}, C_0^{13,6}\right) \cup \alpha^{10}\Delta\left(C_{l-10}^{13,6}, C_0^{13,6}\right) \\ & \cup\ \alpha^{12}\Delta\left(C_{l-12}^{13,6}, C_0^{13,6}\right)) - 224\{0\}, \\ =& \alpha^i\ \Delta(S_0^{13,6}).\end{aligned}$$

(iii) Observe that we may write $D_i^{13,6} = S_i^{13,6} \cup \{0\}$. It therefore follows that

$$\Delta(D_i^{13,6}) = \Delta(S_i^{13}, 0) \cup \Delta(0, S_i^{13,6}) \cup \Delta(S_i^{13,6}).$$

By definition, $\Delta(S_i^{13,6},0) = \{s-0 \,|\, s \in S_i^{13,6}\} = \{s \,|\, s \in S_i^{13,6}\} = S_i^{13,6}$. Similarly $\Delta(0,S_i^{13,6}) = \{-s \,|\, s \in S_i^{13,6}\}$. By definition, $S_i^{13,6}$ comprises a union of four cyclotomic class of order 13 in GF(729). Notice that for each cyclotomic class $C_r^{13,6}$ $(0 \leq r \leq 12)$, of order 13 in GF(729), $f = \frac{q-1}{e} = 56$. It then follows by Lemma 1.4.11 that for each cyclotomic class $C_r^{13,6}$, where $0 \leq r \leq 12$, the additive inverse of each element of $C_r^{13,6}$ is contained within $C_r^{13,6}$. This means that additive inverse of each element of $S_i^{13,6}$ is also contained in $S_i^{13,6}$, and so $\Delta(0,S_i^{13,6}) = S_i^{13,6}$. The result then immediately follows. □

By exploiting the known connections between cyclotomic classes and cyclotomic numbers, we can use this result to write the number of occurrences of each element of GF(q) in the multiset $\Delta(D_i^{13,6})$ in terms of a sum of cyclotomic numbers. This is demonstrated in the following result.

Lemma 4.2.4. *In the finite field* GF(729)*, let α be a primitive element of* GF(729)*, $C_j^{13,6}$ denote the j^{th} cyclotomic class of order* 13*, $I = \{0,4,10,12\}$ and for $0 \leq i \leq 12$, $S_i^{13,6} = D_i^{13,6} \backslash \{0\}$, where $D_i^{13,6} = C_i^{13,6} \cup C_{i+4}^{13,6} \cup C_{i+10}^{13,6} \cup C_{i+12}^{13,6} \cup \{0\}$. It then follows that*

(i) $\Delta(S_0^{13,6}) = \bigcup\limits_{r=0}^{12} \sum_{l\in I}((r,l)_{13} + (r-4,l-4)_{13} + (r-10,l-10)_{13} + (r-12,l-12)_{13})C_r^{13,6} - 224\{0\}$,

(ii) $\Delta(S_i^{13,6}) = \bigcup\limits_{r=0}^{12} \sum_{l\in I}((r-i,l)_{13} + (r-i-4,l-4)_{13} + (r-i-10,l-10)_{13} + (r-i-12,l-12)_{13})C_r^{13,6} - 224\{0\}$,

(iii) $\Delta(D_i^{13,6}) = \bigcup\limits_{r=0}^{12} \sum_{l\in I}((r-i,l)_{13} + (r-i-4,l-4)_{13} + (r-i-10,l-10)_{13} + (r-i-12,l-12)_{13})C_r^{13,6} \cup 2S_i^{13,6} - 224\{0\}$.

Proof. By Lemma 4.2.3

$$\Delta(S_0^{13,6}) = \bigcup_{l\in I}(\Delta(C_l^{13,6},C_0^{13,6}) \cup \alpha^4\Delta\left(C_{l-4}^{13,6},C_0^{13,6}\right) \cup \alpha^{10}\Delta\left(C_{l-10}^{13,6},C_0^{13,6}\right)$$
$$\cup\, \alpha^{12}\Delta\left(C_{l-12}^{13,6},C_0^{13,6}\right)) - 224\{0\}.$$

It then follows by Lemma 2.1.18 that:

$$\Delta(S_0^{13,6}) = \sum_{l\in I}(\bigcup_{r=0}^{12}(r,l)_{13}C_r^{13,6} \cup \alpha^4\bigcup_{r=0}^{12}(r,l-4)_{13}C_r^{13,6} \cup \alpha^{10}\bigcup_{r=0}^{12}(r,l-10)_{13}C_r^{13,6}$$

$$\cup\, \alpha^{12}\bigcup_{r=0}^{12}(r,l-12)_{13}C_r^{13,6}) - 224\{0\}.$$

$$= \bigcup_{r=0}^{12}\sum_{l\in I}((r,l)_{13}C_r^{13,6} \cup (r,l-4)_{13}C_{r+4}^{13,6} \cup (r,l-10)_{13}C_{r+10}^{13,6} \cup (r,l-12)_{13}C_{r+12}^{13,6})$$

$$-224\{0\}.$$

$$\Delta(S_0^{13,6}) = \bigcup_{r=0}^{12}\sum_{l\in I}((r,l)_{13}C_r^{13,6} \cup (r-4,l-4)_{13}C_r^{13,6} \cup (r-10,l-10)_{13}C_r^{13,6}$$

$$\cup (r-12,l-12)_{13}C_r^{13,6}) - 224\{0\}.$$

$$= \bigcup_{r=0}^{12}\sum_{l\in I}((r,l)_{13} + (r-4,l-4)_{13} + (r-10,l-10)_{13}$$

$$+(r-12,l-12)_{13})C_r^{13,6} - 224\{0\}.$$

(ii) By Lemma 4.2.3(ii) and part (i) that

$$\Delta(S_i^{13,6}) = \alpha^i(\bigcup_{r=0}^{12}\sum_{l\in I}((r,l)_{13} + (r-4,l-4)_{13} + (r-10,l-10)_{13}+$$

$$(r-12,l-12)_{13})C_r^{13,6}) - 224\{0\}$$

$$= \bigcup_{r=0}^{12}\sum_{l\in I}((r,l)_{13} + (r-4,l-4)_{13} + (r-10,l-10)_{13}+$$

$$(r-12,l-12)_{13})C_{r+i}^{13,6} - 224\{0\}.$$

It then follows by Lemma 2.1.18 that

$$\Delta(S_i^{13,6}) = \bigcup_{r=0}^{12}\sum_{l\in I}((r-i,l)_{13} + (r-i-4,l-4)_{13} + (r-i-10,l-10)_{13}+$$

$$(r-i-12,l-12)_{13})C_r^{13,6} - 224\{0\}.$$

(iii) Immediate from Lemma 4.2.3 and part (ii). □

Now that we have determined a formula for the number of times each element of GF(729) occurs in the multiset $\Delta(D_i^{13,6})$ (where $0 \leq i \leq 12$) in terms of cyclotomic numbers of order 13, we are able to prove that each set $D_i^{13,6}$ is a PDS by substituting in the values of the cyclotomic numbers of order 13. As $e = 13$ is prime $p = 3$ is odd and $n_1 = \text{ord}_{13}(3) = 3$ is odd, we are able to use Algorithm 2 to identify the values of each internal cyclotomic orbit representative. By exhaustive search, we can also identify the external cyclotomic orbit representatives, and then use Algorithm 3 to find the values of each cyclotomic orbit representative. The next few results in this Chapter are dedicated to stepping through the process of computing the internal and external cyclotomic numbers of order $e = 13$ in the finite field GF(729) in detail, as such, the internal cyclotomic number values will be listed separately from the external cyclotomic number values. To see a more accessible list of the cyclotomic numbers of order $e = 13$ in the finite field GF(729), we refer the reader to Appendix C.

We now record the values of each of the internal cyclotomic orbit representatives. These values were found by inputting $e = 13$, $p = 3$ and $n_1 = \text{ord}_{13}(3)$ into Algorithm 2.

Lemma 4.2.5. *In the finite field* GF(729)*, when* $e = 13$ *there are precisely* 5 *internal cyclotomic orbits under the relations* $\mathfrak{R} = \{(i,j)_e = (j,i)_e, (i,j)_e = (e-i, j-i)_e, (i,j)_e = (ip, jp)_e\}$*. The internal cyclotomic orbit representatives are as follows* $(0,0)_{13}$*,* $(1,1)_{13}$*,* $(2,2)_{13}$*,* $(4,4)_{13}$ *and* $(7,7)_{13}$*. The values of each of the cyclotomic orbit representatives are as follows* $(0,0)_{13} = 7$*,* $(1,1)_{13} = 4$*,* $(2,2)_{13} = 2$*,* $(4,4)_{13} = 6$ *and* $(7,7)_{13} = 4$.

Below we record the value of each of the internal cyclotomic numbers. These values have been found by then equating the value of each of the cyclotomic orbit representatives to the other elements contained within the same cyclotomic orbit.

Proposition 4.2.6. *In the finite* GF(729)*, the internal cyclotomic numbers of* 13 *are as follows*

$7 = (0,0)_{13}$

$4 = (1,1)_{13} = (3,3)_{13} = (9,9)_{13} = (12,0)_{13} = (10,0)_{13} = (4,0)_{13} = (0,12)_{13} = (0,10)_{13} = (0,4)_{13}$

$2 = (2,2)_{13} = (6,6)_{13} = (5,5)_{13} = (11,0)_{13} = (7,0)_{13} = (8,0)_{13} = (0,11)_{13} = (0,7)_{13} = (0,8)_{13}$

$6 = (4,4)_{13} = (12,12)_{13} = (10,10)_{13} = (9,0)_{13} = (1,0)_{13} = (3,0)_{13} = (0,9)_{13} = (0,1)_{13} = (0,3)_{13}$
$4 = (7,7)_{13} = (8,8)_{13} = (11,11)_{13} = (6,0)_{13} = (5,0)_{13} = (2,0)_{13} = (0,6)_{13} = (0,5)_{13} = (0,2)_{13}$.

We now compute the value of each of the external cyclotomic numbers. To do this, we use an exhaustive approach to identify that there are 4 external cyclotomic orbits of order 6 and 6 external cyclotomic orbits of order 18 under the relations $\mathfrak{R} = \{(i,j)_e = (j,i)_e, (i,j)_e = (e-i, j-i)_e, (i,j)_e = (ip, jp)_e\}$. (To see the elements contained within each of these orbits see Remark 4.2.9). We identify the values of each of the external orbit representatives in the following Lemma. Note that these values have been found by applying Algorithm 3 to each of the cyclotomic orbit representatives.

Lemma 4.2.7. *When* $e = 13$ *in finite field* GF(729)*, there are precisely* 10 *external cyclotomic orbits under the relations* $\mathfrak{R} = \{(i,j)_e = (j,i)_e, (i,j)_e = (e-i, j-i)_e, (i,j)_e = (ip, jp)_e\}$*. The orbit representatives for these external cyclotomic orbits as follows:*

(i) the orbit representative for the 4 *cyclotomic orbits of order* 6 *are* $(3,4)_{13}$*,* $(9,10)_{13}$*,* $(5,7)_{13}$ *and* $(6,8)_{13}$*,*

(ii) the orbit representatives for the 6 *cyclotomic orbits of order* 18 *are* $(1,2)_{13}$*,* $(2,3)_{13}$*,* $(4,5)_{13}$*,* $(5,6)_{13}$*,* $(6,7)_{13}$ *and* $(7,8)_{13}$*.*

The values of the orbit representatives are as follows $(3,4)_{13} = 8$*,* $(9,10)_{13} = 1$*,* $(5,7) = 6$*,* $(6,8)_{13} = 6$*,* $(1,2)_{13} = 6$*,* $(2,3)_{13} = 2$*,* $(4,5)_{13} = 4$*,* $(5,6)_{13} = 6$*,* $(6,7)_{13} = 2$*,* $(7,8)_{13} = 5$*.*

By equating each of the external cyclotomic orbit representatives to the other elements contained within the same external orbit, we can then find the value of each external cyclotomic number.

Lemma 4.2.8. *By applying Algorithm 3 to each of the external cyclotomic orbit representatives found in Remark 4.2.7 when* $\mathfrak{R} = \{(i,j)_e = (j,i)_e, (i,j)_e = (e-i, j-i)_e, (i,j)_e = (ip, jp)_e\}$ *and* $e = 13$ *in the finite field* GF(729)*, we find that* $6 = (1,2)_{13}$*,* $2 = (2,3)_{13}$*,* $8 = (3,4)_{13}$*,* $4 = (4,5)_{13}$*,* $6 = (5,6)_{13}$*,* $2 = (6,7)_{13}$ *and* $5 = (7,8)_{13}$*,* $1 = (9,10)_{13}$*,* $6 = (5,7)_{13}$ *and* $6 = (6,8)_{13}$*.*

Proposition 4.2.9. *In the finite* GF(729)*, when* $e = 13$*, the external cyclotomic numbers are take the following values*
$6 = (1,2)_{13} = (3,6)_{13} = (9,5)_{13} = (2,1)_{13} = (6,3)_{13} = (5,9)_{13} = (12,1)_{13} = (10,3)_{13} = (4,9)_{13} = (1,12)_{13} = (3,10)_{13} = (9,4)_{13} = (11,12)_{13} = (7,10)_{13} = (8,4)_{13} = (12,11)_{13} = (10,7)_{13} = (4,8)_{13}$,
$2 = (2,3)_{13} = (6,9)_{13} = (5,1)_{13} = (3,2)_{13} = (9,6)_{13} = (1,5)_{13} = (11,1)_{13} = (7,3)_{13} = (8,9)_{13} = (1,11)_{13} = (3,7)_{13} = (9,8)_{13} = (10,12)_{13} = (4,10)_{13} = (12,4)_{13} = (12,10)_{13} = (10,4)_{13} = (4,12)_{13}$,
$8 = (3,4)_{13} = (9,12)_{13} = (1,10)_{13} = (4,3)_{13} = (12,9)_{13} = (10,1)_{13}$,
$4 = (4,5)_{13} = (12,2)_{13} = (10,6)_{13} = (5,4)_{13} = (2,12)_{13} = (6,10)_{13} = (9,1)_{13} = (1,3)_{13} = (3,9)_{13} = (1,9)_{13} = (3,1)_{13} = (9,3)_{13} = (8,12)_{13} = (11,10)_{13} = (7,4)_{13} = (12,8)_{13} = (10,11)_{13} = (4,7)_{13}$,
$6 = (5,6)_{13} = (2,5)_{13} = (6,2)_{13} = (6,5)_{13} = (5,2)_{13} = (2,6)_{13} = (8,1)_{13} = (11,3)_{13} = (7,9)_{13} = (1,8)_{13} = (3,11)_{13} = (9,7)_{13} = (7,12)_{13} = (8,10)_{13} = (11,4)_{13} = (12,7)_{13} = (10,8)_{13} = (4,11)_{13}$,
$2 = (6,7)_{13} = (5,8)_{13} = (2,11)_{13} = (7,6)_{13} = (8,5)_{13} = (11,2)_{13} = (7,1)_{13} = (8,3)_{13} = (11,9)_{13} = (1,7)_{13} = (3,8)_{13} = (9,11)_{13} = (6,12)_{13} = (5,10)_{13} = (2,4)_{13} = (12,6)_{13} = (10,5)_{13} = (4,2)_{13}$,
$5 = (7,8)_{13} = (8,11)_{13} = (11,7)_{13} = (8,7)_{13} = (11,8)_{13} = (7,11)_{13} = (6,1)_{13} = (5,3)_{13} = (2,9)_{13} = (1,6)_{13} = (3,5)_{13} = (9,2)_{13} = (5,12)_{13} = (2,10)_{13} = (6,4)_{13} = (12,5)_{13} = (10,2)_{13} = (4,6)_{13}$,
$1 = (9,10)_{13} = (1,4)_{13} = (3,12)_{13} = (10,9)_{13} = (4,1)_{13} = (12,3)_{13}$,
$6 = (5,7)_{13} = (2,8)_{13} = (6,11)_{13} = (7,5)_{13} = (8,2)_{13} = (11,6)_{13}$,
$6 = (6,8)_{13} = (5,11)_{13} = (2,7)_{13} = (8,6)_{13} = (11,5)_{13} = (7,2)_{13}$.

With the internal and external cyclotomic numbers of order $e = 13$ in the finite field GF(729) calculated, we are able to prove that each $D_i^{13,6}$, where $0 \leq i \leq 12$ is a PDS in the finite field GF(729).

Theorem 4.2.10. *In the finite field* GF(729)*, let* $C_i^{13,6}$ *denote the* i^{th} *cyclotomic of order* 13 *for* $0 \leq i \leq e-1$*. Then the set*

$$D_i^{13,6} = C_i^{13,6} \cup C_{i+4}^{13,6} \cup C_{i+10}^{13,6} \cup C_{i+12}^{13,6} \cup \{0_{\mathrm{GF}(729)}\}$$

is a (729, 225, 63, 72)*-PDS.*

Proof. This result can be obtained by substituting the cyclotomic numbers, detailed in Propositions 4.2.6 and 4.2.9 into the formula

$$\Delta(D_i^{13,6}) = \bigcup_{r=0}^{12} \sum_{l \in I} ((r-i,l)_{13} + (r-i-4,l-4)_{13} + (r-i-10,l-10)_{13} + \\ (r-i-12,l-12)_{13}) C_r^{13,6} \cup 2S_i^{13,6} - 224\{0\},$$

found in Lemma 4.2.4. It is left up to the reader to satisfy themselves that this is true. A complete proof that the set $D_0^{13,6}$ is a $(729, 225, 63, 72)$-PDS is recorded in Appendix C. The reader can use Lemma 4.2.3 to obtain a formal proof that this results also holds for the set $D_i^{13,6}$ when $1 \leq i \leq 12$. □

As the reader can see from the above results, this cyclotomic result is not generalisable because the result relies upon direct computation of the cyclotomic numbers of order 13 in the finite field GF(729). To generalise this result, we would need to identify a formula or technique for determining the cyclotomic numbers of order $e = \frac{p^m-1}{p-1}$, or at least certain symmetries in the sums of these numbers, in a general finite field GF(p^{2m}) (which we can also view as the group $\mathbb{Z}_p^{2m}$). As no such results currently exist, to get around this issue in the paper [20], we relied upon quadratic forms.

Subsequent to the original submission of this Thesis, I have been involved in a collaborative project with Dr. Sophie Huczsnyska and Prof. Maura Paterson, in which we developed a technique for computing cyclotomic numbers of order $e \mid \frac{p^m-1}{p-1}$ when $m \geq 3$. For further information, see our preprint [36]. In the $m = 3$ case, our new techniques signficantly speed up the computation of cyclotomic numbers. By generalising the techniques in this paper, we hope to identify new cyclotomic number results, which will ultimately allow us to produce a purely cyclotomic proof that $D_0^{\frac{p^m-1}{p-1}}$ is a PDS in the group $\mathbb{Z}_p^{2m}$.

Chapter 5

Non-cyclotomic constructions of DPDFs and EPDFs

The previous Chapters in this Thesis are concerned with developing new cyclotomic techniques for constructing cyclotomic PDSs, DPDFs and EPDFs; however finite field cyclotomy is not the only tool that we can deploy to identify new DPDF and EPDF constructions. In this Chapter, we present a series of non-cyclotomic constructions of these objects. One particularly interesting feature of these non-cyclotomic DPDF/EDPF constructions is that unlike their cyclotomic counterparts, they rely heavily on the structure of additive subgroups/complements of subgroups. This gives wider variety to the DPDF and EPDF constructions and parameter sets in this Thesis. Another point of interest that arises from the study of non-cyclotomic DPDFs and EPDFs is that we can find examples of DPDFs that are not simultaneously EPDFs and vice versa.

We begin by covering a selection of non-cyclotomic DPDF and EPDF constructions that can be obtained via non-cyclotomic PDSs in Section 5.1. In Section 5.2, we look at some non-cyclotomic DPDF and EPDF results that can be constructed from Relative Difference Sets (we define these objects in Section 5.2). Section 5.2 includes our main result, in which we demonstrate that the "affine" RDS construction first obtained by Bose in [8] can be extended to a non-cyclotomic DPDF and EPDF construction. In the final part of the Chapter, we introduce the first examples of DPDFs that are not simultaneously EPDFs and vice versa. Note that all DPDF and EPDF constructions contained in this Chapter can be found in my joint paper with my supervisor [35].

5.1 DPDF and EPDF constructions arising from non-cyclotomic PDSs

We begin this Section by looking a result that narrows down the possibilities for DPDFs and EPDFs that partition proper PDSs.

Theorem 5.1.1. *Let $\mathbb{Z}_v$ be the cyclic group of order v. Suppose $S' = \{D_1, \ldots, D_s\}$ is a $(v, s, k, \lambda_1, \mu_1)$-DPDF and a $(v, s, k, \lambda_2, \mu_2)$-EPDF in $\mathbb{Z}_v$, which partitions a proper PDS, $S = \cup_{i=1}^{s} D_i$. Then either;*

(i) v is an odd prime and $v \equiv 1 \mod 4$, in which case S' partitions the set of non-zero quadratic residues, or the non-residues modulo v,

(ii) or v is a composite number, in which case S' partitions a proper non-trivial subgroup H of $\mathbb{Z}_v$ or its complement $\mathbb{Z}_v \backslash \mathrm{H}$.

Proof. By Definition 1.3.11, the element $0 \notin S'$ since all DPDFs partition G^*. As S' partitions S it is immediate that $0 \notin S$. Further, as S is proper, for each $s \in S$, it follows that $-s \in S$ (s and $-s$ occur the same number of times in the multiset $\Delta(S)$, so if $-s \in \mathrm{G}\backslash S$ it immediately follows from Definition 1.3.1 that S is not proper), hence we can conclude that $S = -S$. It therefore follows by Definition 1.3.1 that since $0 \in S$ and $S = -S$, S must be a regular PDS. It is stated in Corollary 5.7 of [49] that when S is a regular PDS in $\mathbb{Z}_v$, either $v \equiv 1 \mod 4$ is an odd prime and S is the set of quadratic (or non-quadratic) residues modulo v or v is a composite number, and $\mathrm{H} = S \cup \{0\}$ is either a subgroup of $\mathbb{Z}_v$ or S is the complement of a subgroup H of $\mathbb{Z}_v$. □

Below we give one example of both of the cases in Theorem 5.1.1.

Example 5.1.2. *(i) In the cyclic group $\mathbb{Z}_{17}$, $S = \{1, 2, 4, 8, 9, 13, 15, 16\}$ is the set of non-zero squares. By a result in [56] (Proposition 3.1.2 is an analogue of this result, written in cyclotomic notation) in any cyclic group of order p, where p is prime and $p \equiv 1 \mod 4$, the set of non-zero squares is a $(p, \frac{p-1}{2}, \frac{p-5}{4}, \frac{q-1}{4})$-PDS. It therefore follows that S is a $(17, 8, 3, 4)$-PDS. Notice that the following collection of sets, S' is a partition of S*

$$S' = \{\{1, 4, 13, 16\}, \{2, 8, 9, 15\}\}.$$

Moreover, observe that

$$\begin{aligned}\mathrm{Int}(S') &= \Delta(\{1,4,13,16\}) \cup \Delta(\{2,8,9,15\})\\ &= \{2,3,3,5,5,8,9,12,12,14,14,15\} \cup \{1,4,6,6,7,7,10,10,11,11,\\ &\quad 13,16\}\\ &= \{1,2,4,8,9,13,15,16\} \cup 2\{3,5,6,7,10,11,12,14\}\\ &= S \cup 2(\mathbb{Z}_{17}^{*}\backslash S).\end{aligned}$$

Hence, it naturally follows by Definition 1.3.11 that S' is a $(17,2,4,1,2)$-DPDF, and it therefore follows by Theorem 1.3.17(iii) that S' is also a $(17,2,4,2)$-EDF. Thus, S' is an example of one of the sets described in Theorem 5.1.1(i).

(ii) *Let $\mathrm{G} = \mathbb{Z}_6$ and $\mathrm{H} = \{0,3\} \leq \mathrm{G}$. Since H is a subgroup of $\mathbb{Z}_6$, it follows by Theorem 1.3.19 that $S = \mathbb{Z}_6\backslash\mathrm{H} = \{1,2,4,5\}$ is a $(6,4,2,4)$-PDS.*

The following collection sets

$$S' = \{\{1,4\},\{2,5\}\}$$

is a partion of S. By computing the elements of $\mathrm{Int}(S')$ and $\mathrm{Ext}(S')$, the reader will be able to determine that S' is both a $(6,2,2,0,4)$-DPDF and a $(6,2,2,2,0)$-EPDF. Therefore, S' is an example of one of the sets described in Theorem 5.1.1 (ii).

The following result, recorded in [49], is used in subsequent results.

Lemma 5.1.3. *Let G be a group of order mn with identity e and let H be a subgroup of G of order n.*

(i) $\mathrm{H}\backslash\{e\}$ *is an $(mn, n-1, n-2, 0)$-PDS.*

(ii) $\mathrm{G}\backslash\mathrm{H}$ *is an $(mn, n(m-1), n(m-2), n(m-1))$-PDS.*

(iii) *The sets H, $\mathrm{H}\backslash\{e\}$, $\mathrm{G}\backslash\mathrm{H}$ and $\mathrm{G}\backslash\mathrm{H} \cup \{e\}$ are PDSs, with $\mathrm{H}\backslash\{e\}$ and $\mathrm{G}\backslash\mathrm{H}$ being regular.*

Proof. For part (i), it is immediate that $\Delta(\mathrm{H}\backslash\{e\}) = (n-2)\mathrm{H}$. For part (ii), notice that $\Delta(\mathrm{G}) = \Delta(\mathrm{G}\backslash\mathrm{H}) \cup \Delta(\mathrm{G}\backslash\mathrm{H},\mathrm{H}) \cup \Delta(\mathrm{H},\mathrm{G}\backslash\mathrm{H}) \cup \Delta(\mathrm{H})$; since $\Delta(\mathrm{G}) = (mn)\mathrm{G}$, $\Delta(\mathrm{H}) = n\mathrm{H}$, $\Delta(\mathrm{G}\backslash\mathrm{H},\mathrm{H}) = n(\mathrm{G}\backslash\mathrm{H})$ and $\Delta(\mathrm{H},\mathrm{G}\backslash\mathrm{H}) = n(\mathrm{G}\backslash\mathrm{H})$, we can deduce that $\Delta(\mathrm{G}\backslash\mathrm{H}) = (mn-n)\mathrm{H} \cup (mn-2n)(\mathrm{G}\backslash\mathrm{H})$. Part (iii) is an immediate consequence of part (i) and Theorem 1.3.19. □

Following on from the above Lemma, we can establish the following important result about DPDFs and EPDFs that partition subgroups with the identity removed.

Theorem 5.1.4. *Let* G *be a group of order mn and* H *be a subgroup of* G *of order n. Let $S = \mathrm{H}^*$.*

(i) If S' is an (mn, s, k, λ, μ)-DPDF (respectively EDPF) partitioning S, then $\mu = 0$, and S' is a near-complete (n, s, k, λ)-DDF (respectvely EDF) in the group H *(i.e. the component sets of S' partition H^*) .*

(ii) Each near-complete (n, s, k, λ)-DDF (respectively EDF) in the group H *corresponds to an $(mn, s, k, \lambda, 0)$-DPDF (respectively EPDF) partitioning S in every group* G*, in which $\mathrm{H} \leq \mathrm{G}$.*

Proof. (i) As H is a subgroup it follows by Lemma 5.1.3 that $\Delta(S) = (n-2)S \cup 0(\mathrm{G}^*\backslash S)$. As S' is a (mn, s, k, λ, μ)-DPDF, $\mathrm{Int}(S') = \lambda S \cup \mu(\mathrm{G}^*\backslash S)$, where $\lambda, \mu \geq 0$. As consequence of Lemma 1.2.4, $0 \leq \lambda \leq n-2$ and $\mu = 0$. Since S' partitions H^*, and hence $\mathrm{Int}(S')$ comprises λ copies of the non-identity elements of H, it naturally follows that S' is a near-complete DDF in H. We can analogously show that any EPDF partitioning H is a near-complete EDF in H.

(ii) This result naturally follows by embedding H into G. □

Example 5.1.5. *As previously noted in Example 1.3.5, the sets $\{1, 2, 4\}$ and $\{3, 5, 6\}$ form a $(7, 2, 3, 2)$-DDF in $\mathbb{Z}_7$. This DDF is near-complete as the component sets partition $\mathbb{Z}_7^*$. Notice these sets are also a $(7, 2, 3, 3)$-near-complete EDF in $\mathbb{Z}_7$.*

The group $\mathbb{Z}_{21}$ contains the subgroup $\mathrm{H} = \{0, 3, 6, 9, 12, 15, 18\}$, which is isomorphic to $\mathbb{Z}_7$ via the embedding $f : \mathbb{Z}_7 \to \mathbb{Z}_{21}$, $x \mapsto 3x$. It therefore follows that the sets $\{3, 6, 12\}$ and $\{9, 15, 18\}$ form a $(21, 2, 3, 2, 0)$-DPDF and a $(21, 2, 4, 3, 0)$-EPDF in $\mathbb{Z}_{21}$.

Note that as near-complete DDFs and EDFs have been well-studied in the literature (see for example see [14],[21]), we can find many examples of the above construction. We therefore turn our attention to DPDFs and EPDFs that partition G\H. Note that from this point in the Chapter onwards, we will be using the term **non-trivial cosets of H** to refer to the set of all cosets of H, excluding H itself.

Theorem 5.1.6. *Let* G *be a group of order* mn *and* H *be a normal subgroup of* G *of order* n*. Then the set of non-trivial cosets of* H *in* G *forms an* $(mn, m-1, n, 0, mn-n)$*-DPDF and an* $(mn, m-1, n, mn-2n, 0)$*-EPDF.*

Proof. It follows by Lemma 5.1.3 that G\H is an $(mn, mn-n, mn-2n, mn-n)$-PDS. Moreover, it is clear that non-trivial cosets of H partition G\H, and the multiset of internal differences of each non-trivial coset of H, consists of n copies of H^* and 0 copies of G\H. As there are $m-1$ non-trivial cosets of H in G, it follows that the set of non-trivial cosets of H forms a $(mn, m-1, n, 0, mn-n)$-DPDF and consequently an $(mn, m-1, n, mn-2n, 0)$-EPDF by Lemma 1.2.4. □

We finish this Section by establishing some parameter constraints for DPDFs and EPDFs that partition the complement of a subgroup, but before we get onto our main result, we require the following technical Lemma.

Lemma 5.1.7. *If* $\gcd(sk, v-1) = 1$*, then;*

(i) for every $(v, s, k, \lambda_1, \mu_1)$*-DPDF, either* $\mu_1 = 0$ *or* $\mu_1 = sk$*.*

(ii) for every $(v, s, k, \lambda_2, \mu_2)$*-EPDF, either* $\mu_2 = 0$ *or* $\mu_2 = sk$*.*

Proof. By Lemma 1.3.14 (i), $sk(k-1) = \lambda_1 sk + \mu_1(v-1-sk)$, it is therefore clear that $sk \mid \mu_1(v-1-sk)$. Since sk and $v-1$ are coprime, it therefore follows that $sk \mid \mu_1$, and as $\mu_1 \leq sk$, it follows that $\mu_1 = 0$ or $\mu_1 = sk$. Part (ii) analogously follows by Lemma 1.3.14 (ii). □

We may now state our main result of this Section.

Theorem 5.1.8. *Let* G *be a group of order* $v = mn$*. Suppose that* S' *is a* $(v, s, k, \lambda_1, \mu_1)$*-DPDF and a* $(v, s, k, \lambda_2, \mu_2)$*-EPDF that partitions* G\H*, where* H *is a subgroup of* G *order* n*. Then;*

(i) $n \mid \mu_1$ *and* $n \mid \mu_2$*.*

(ii) If $\gcd(mn-n, mn-1) = 1$*, then* S' *is one of the following:*

(a) an $(mn, s, k, k-1, 0)$*-DPDF and an* $(mn, s, k, mn-2n-k+1, mn-n)$*-EPDF,*

(b) an $(mn, s, k, k-n, mn-n)$*-DPDF and an* $(mn, s, k, mn-n-k, 0)$*-EPDF.*

(iii) If $n = 2$ *then* S' *is one of the following:*

(a) a $(2m, s, k, k-1, 0)$*-DPDF and a* $(2m, s, k, 2m-3-k, 2m-2)$*-EPDF,*

(b) a $(2m, s, k, k-2, 2m-2)$*-DPDF and a* $(2m, s, k, 2m-2-k, 0)$*-EPDF.*

Proof. In part (i), notice that since S' partitions G\H, this means that $sk = n(m-1)$. Note that there are $n-1$ elements in H$\setminus\{e\}$. It is then immediate form Lemma 1.3.14 (i) that

$$n(m-1)(k-1) = \lambda_1 n(m-1) + \mu_1(n-1).$$

Similar to the proof of Lemma 5.1.7, since $n \mid \mu_1(n-1)$ and $\gcd(n-1, n) = 1$, we have $n \mid \mu_1$. We can use a similar technique to prove that $n \mid \mu_2$. Parts (ii) and (iii) are a direct consequence of Lemma 5.1.7. Note that in part (iii), when $n = 2$, $\gcd(mn-n, mn-1) = 1$. □

5.2 DPDF and EPDF constructions arising from Relative Difference Sets

In this Section, we write G multiplicatively and we don't assume that G abelian.

Relative Difference Sets (RDSs) are combinatorial objects that were first defined by Elliot and Butson in [28], but were previously introduced implicitly by Bose in the paper [8] as an affine analogue to Singer Difference Sets. RDSs are similar objects to PDSs, in the sense that the non-identity elements of a group G occur as a pairwise difference between elements of the RDS at one of two frequencies: the distinction is that the frequency at which an element of G occurs as a pairwise difference is dependent upon membership/non-membership of a particular subgroup H. Like PDSs, RDSs have been well-studied in the literature (see [10],[15],[28],[30],[44]); for an extensive survey of RDSs see [59].

Definition 5.2.1. *Let* G *be a group of order* mn *and let* H *be normal subgroup of* G *of order* n. *We say a* k*-subset* R *of* G *is an* (m, n, k, λ)-***relative difference set*** *(or* ***RDS****) in* G *relative to* H *if the following multiset equation holds;*

$$\Delta(R) = \lambda(\mathrm{G}\backslash\mathrm{H})$$

i.e. λ *copies of each element in* G\H *and no copies of any element of* H. *If* $n = 1$, R *is a Difference Set.*

Example 5.2.2. *Let* $G = \mathbb{Z}_8$. *The set* $R = \{1, 6, 7\}$ *is a* $(4, 2, 3, 1)$*-RDS with respect to* $\mathrm{H} = \{0, 4\}$ *as the multiset* $\Delta(R)$ *consists of one copy of every element in* G\H*, and no copies of the elements of* H.

To be consistent with the original definition of an RDS, I have chosen to define RDSs as difference structures that are relative to normal subgroups in this Thesis, however it is important to note the following fact, which will be used to make a later result more general.

Remark 5.2.3. *In Definition 5.2.1, it is possible to relax the condition that* H *is a normal subgroup. In fact, in Theorem 1.1 of [15] the authors present an RDS construction in the group* A_5 *relative to a subgroup of order* 2. *Whilst this construction satisfies most requirements of an RDS, it fails to satisfy the requirement that* H *is a normal subgroup.*

We can use RDSs to identify new DPDF and EPDF constructions. In this Section, we present some theoretical results and DPDF and EPDF constructions that utilise RDSs. We begin this Section by presenting some important general results required to construct DPDFs and EPDFs from RDSs. This Section then culminates by demonstrating that Bose's original RDS construction in [8] can be extended to a construction of DPDFs.

Proposition 5.2.4. *Let* G *be a group of order* mn *and let* H *be a (not necessarily normal) subgroup of* G *of order* n. *If* $S' = \{D_1, \ldots, D_s\}$ *is a family of disjoint* k*-subsets of* G *such that;*

(i) each D_i $(1 \leq i \leq s)$ *is an* (n, m, k, λ)*-RDS in* G *relative to* H,

(ii) S' *partitions* G\H,

then S' is an $(mn, s, k, s\lambda, 0)$-DPDF and an $(mn, s, k, mn-2n-s\lambda, mn-n)$-EPDF.

Proof. As each D_i is an (n, m, k, λ)-RDS, $\Delta(D_i) = \lambda(\mathrm{G}\backslash\mathrm{H}) \cup 0(\mathrm{H})$. As $\mathrm{Int}(S') = \cup_{i=1}^{s}\Delta(D_i)$, it follows that $\mathrm{Int}(S') = s\lambda(\mathrm{G}\backslash\mathrm{H}) \cup 0(\mathrm{H})$, and so S' is an $(mn, s, k, s\lambda, 0)$-DPDF. It was demonstrated in Lemma 5.1.3 that $\mathrm{G}\backslash\mathrm{H}$ is an $(mn, mn-n, mn-2n, mn-n)$-PDS, and so it follows by Lemma 1.2.4 that S' is also an $(mn, s, k, mn-2n-s\lambda, mn-n)$-EPDF. □

One way of identifying DPDF and EPDF constructions arising from RDSs is to take a series of disjoint translates of an RDS in a group G that partitions $\mathrm{G}\backslash\mathrm{H}$. The following Lemma, based on a result of [30], highlights a property that translates of an RDS must have in order to be disjoint.

Lemma 5.2.5. *Let* G *be a group and* H *be a (not necessarily normal) subgroup of* G *and let S be an (m, n, k, λ)-RDS relative to* H*. Let $g_1 \neq g_2 \in \mathrm{G}$. Then the translates g_1S and g_2S are disjoint if and only if $g_2^{-1}g_1 \in \mathrm{H}$.*

Proof. For both directions of this proof we prove the contrapositive. In the forwards direction, suppose $g_2^{-1}g_1 \in \mathrm{G}\backslash\mathrm{H}$; notice that we may write $g_2^{-1}g_1 = y$, where $y \in \mathrm{G}\backslash\mathrm{H}$. As S is an RDS relative to H, for every element $z \in \mathrm{G}\backslash\mathrm{H}$, there are precisely $\lambda > 0$ pairs $(s_1, s_2) \in S \times S$ such that $s_2s_1^{-1} = z$ (since $s_2s_1^{-1} \in \Delta(S)$). Further, this means that there are λ pairs $(s_1, s_2) \in S \times S$ such that $s_2s_1^{-1} = y$ (where $g_2^{-1}g_1 = y$ as above). It follows from the above that when $g_2^{-1}g_1 \in \mathrm{G}\backslash\mathrm{H}$, there exist $s_1, s_2 \in S$ such that $g_2^{-1}g_1 = s_2s_1^{-1}$. We can rearrange this expression to give $g_1s_1 = g_2s_2$; this then implies $g_1S \cap g_2S \neq \emptyset$. For the reverse direction, suppose that $g_1S \cap g_2S \neq \emptyset$, meaning that there exist elements $s_1, s_2 \in S$ such that $g_1s_1 = g_2s_2$. We can rearrange this expression to give $g_2^{-1}g_1 = s_2s_1^{-1}$. As S is an RDS relative to H, this means that $s_2s_1^{-1} \in \mathrm{G}\backslash\mathrm{H}$, this implies that $g_2^{-1}g_1 \in \mathrm{G}\backslash\mathrm{H}$.

Notice that since the argument of this proof does not depend upon the subgroup H being normal, we can use Remark 5.2.3 to apply this result to RDSs relative to a subgroup H, where H is not normal. □

The following Remark about the parameters of an RDS, whose translates partition $\mathrm{G}\backslash\mathrm{H}$, is a consequence of Lemma 5.2.5.

Remark 5.2.6. *(i) Suppose S is an (n, m, k, λ)-RDS, then $k(k-1) = (mn - n)\lambda$. To see this, note that $\Delta(S) = k(k-1)$ and there are precisely $mn - m$ elements in* G\H*.*

(ii) Suppose S is an (n, m, k, λ)-RDS, whose translates partition G\H*. By Lemma 5.2.5 two translates $h_1 + S$ and $h_2 + S$ will be disjoint if and only if $h_1, h_2 \in S$. As* $|\mathrm{H}| = n$*, this means that that there are precisely n disjoint translates of S partitioning* G\H*, and since there are $nm - m$ elements in* G\H*, it follows that $nk = (nm - m)$, implying $k = m - 1$. By substituting $k = m - 1$ into the equation obtained in part (i), we find that $(m-1)(m-2) = n(m-1)\lambda$ or in other words $\lambda = \frac{m-2}{n}$.*

Henceforth, we assume that H is a normal subgroup of G.

Lemma 5.2.7. *Let* G *be a group and* H *be a normal subgroup of* G*. Suppose that S is an (m, n, k, λ)-RDS relative to* H*. Then;*

(i) $\Delta(S) = \Delta(gS)$ for any $g \in$ G*. This means that any translate gS is an (m, n, k, λ)-RDS relative to* H*.*

*(ii) S cannot contain more than one representative from any coset g*H *($g \in$* G*). In particular, $k \leq m$.*

Proof. (i) The multiset $\Delta(gS)$ consists of all elements of the form $gs_1(gs_2)^{-1} = g(s_1 s_2^{-1})g^{-1}$, where $s_1 s_2^{-1} \in \Delta(S)$. As S is an RDS, it follows that $\Delta(S)$ comprises λ copies of G\H and 0 copies of H. As H is a normal subgroup, it follows that $g\mathrm{H}g^{-1} = \mathrm{H}$ and $g\mathrm{G}g^{-1} = \mathrm{G}$, therefore we have that $g(\mathrm{G}\backslash\mathrm{H})g^{-1} = \mathrm{G}\backslash\mathrm{H}$. It then naturally follows that $\Delta(gS)$ comprises λ copies of G\H and 0 copies of H.

(ii) Suppose that S contains two elements $s_1 \neq s_2 \in g\mathrm{H}$; we write $s_1 = gh_1$ and $s_2 = gh_2$. Observe that $s_1 s_2^{-1} = gh_1(gh_2)^{-1} = g(h_1 h_2^{-1})g^{-1}$, but as we saw in part (i), as H is a normal subgroup, this means $s_1 s_2^{-1} = g(h_1 h_2^{-1})g^{-1} \in \mathrm{H}$. We must therefore have $s_1 = s_2$ which is a contradiction. □

We conclude this part of this Section with a result that ties the above results together to demonstrate that any collection of disjoint RDSs that partition G\H and meet the parameter constraints outlined in Remark 5.2.6 forms both a DPDF and an EPDF.

Theorem 5.2.8. *Let* G *be a group of order* mn *and let* H *be a normal subgroup of* G *of order* n*. Suppose there exists an* $(m, n, m-1, \frac{m-2}{n})$*-RDS* R *in* G *relative to* H*. Then there exists an* $(mn, n, m-1, m-2, 0)$*-DPDF and an* $(mn, n, m-1, (m-2)(n-1), (m-1)n)$*-EPDF which partitions* $\mathrm{G}\backslash\mathrm{H}$*.*

Proof. It is immediate from Lemma 5.2.7 that any translate gR, where $g \in \mathrm{G}$, is an $(m, n, m-1, \frac{m-2}{n})$-RDS. We also demonstrate in Lemma 5.2.7 that every RDS R contains at most one coset representative of every coset of H. Since $[\mathrm{G} : \mathrm{H}] = m$ and the cardinality of R is $m-1$, this means that R contains one representative from $m-1$ of the cosets of H and no representative from the final coset. Let $a\mathrm{H}$ be the only coset of H without a representative in R and suppose $ah \in a\mathrm{H}$. We will now prove that the translate $S := a^{-1}R$, where $a^{-1} \in \mathrm{G}$ is the multiplicative inverse of $a \in \mathrm{G}$, is an RDS comprising only of representatives of non-trivial cosets of H. Let $R' = R \cup \{ah\}$, where $ah \in a\mathrm{H}$ as above, then $a^{-1}R' = a^{-1}R \cup \{a^{-1}ah\} = a^{-1}R \cup \{h\}$. Notice that since $h \in \mathrm{H}$ and R' contains one representative of each distinct coset of H, this implies that $S = a^{-1}R$ cannot contain an element of H.

Let $S_{\mathrm{H}} = \{hS \,|\, h \in \mathrm{H}\}$, meaning that S_{H} is the set of all translates of S by elements of the multiplicative subgroup H. As S contains no elements of H, it follows that $hS \cap \mathrm{H} = \emptyset$, since if $hS \cap \mathrm{H}$ was non-empty, this would imply that there exists a $h_1 \in \mathrm{H}$ such that $h_1 = hs$ for some $s \in S$ i.e. $s = h^{-1}h_1$, which is clearly not true. By Lemma 5.2.7, the translates of S contained in S_{H} are all disjoint, so the union of the sets in S_{H} has $(m-1)n$ elements. It therefore follows that S_{H} partitions $\mathrm{G}\backslash\mathrm{H}$; thus, by Proposition 5.2.4, S_{H} is both an $(mn, n, m-1, m-2, 0)$-DPDF and an $(mn, n, m-1, (m-2)(n-1), (m-1)n)$-EPDF. □

Example 5.2.9. *Let* $\mathrm{G} = \mathbb{Z}_8$*. We saw in a previous example that the set* $S = \{1, 6, 7\}$ *is a* $(4, 2, 3, 1)$*-RDS relative to the (normal) subgroup* $\mathrm{H} = \{0, 4\}$*. By translating* S *by* 4*, we obtain the set* $\{5, 2, 3\}$*, which by Lemma 5.2.7 is also a* $(4, 2, 3, 1)$*-RDS. As the RDSs* $\{1, 6, 7\}$ *and* $\{5, 2, 3\}$ *partition* $\mathbb{Z}_8\backslash\{0, 4\}$*, it follows that* $\{1, 6, 7\}$ *and* $\{5, 2, 3\}$ *form an* $(8, 2, 3, 2, 0)$*-DPDF and an* $(8, 2, 3, 2, 6)$*-EPDF.*

5.2.1 Extension of Bose's construction to DPDFs/EPDFs

In this Subsection, we cover an elegant extension of Bose's original RDS construction in the paper [8] to constructions of DPDFs and EPDFs. This constructions fits in well with the general themes of this Thesis, as in contrast to previous results, it presents a non-cyclotomic DPDF and EDPF construction in finite fields of order q, where q is an even power of a prime. Note, while cyclotomic classes appear as multiplicative cosets in the proof below, cyclotomic techniques are not used.

Theorem 5.2.10. *Let q be a prime power and let α be a primitive element of $\mathrm{GF}(q^2)$ with primitive polynomial f over $\mathrm{GF}(q)$. For each $\alpha^i \in \mathrm{GF}(q^2)$ $(0 \le i \le q^2-2)$, there exist $a_i, b_i \in \mathrm{GF}(q)$ such that $\alpha^i = a_i + b_i\alpha$.*

(i) For each $c \in \mathrm{GF}(q)^*$, let

$$S_c := \{\alpha^i \in \mathrm{GF}(q^2) \,|\, \alpha^i = a_i + c\alpha,\ a_i \in \mathrm{GF}(q)\}.$$

Then the family $\{S_c\}_{c\in\mathrm{GF}(q)^*}$ is a multiplicative $(q^2-1, q-1, q, q-1, 0)$-DPDF and a multiplicative $(q^2-1, q-1, q, (q-1)(q-2), q^2-q)$-EPDF in $\mathrm{GF}(q^2)^*$.

(ii) For each $c \in \mathrm{GF}(q)^*$ let

$$S'_c := \{i \,|\, \alpha^i \in S_c, 0 \le i \le q^2-2\} \subseteq \mathbb{Z}_{q^2-1}.$$

Then the family $\{S'_c\}_{c\in\mathrm{GF}(q)^*}$ is an additive $(q^2-1, q-1, q, q-1, 0)$-DPDF and an additive $(q^2-1, q-1, q, (q-1)(q-2), q^2-q)$-EPDF in $\mathbb{Z}_{q^2-1}$.

Proof. Let $c \in \mathrm{GF}(q)^*$. To construct each set S_c, we first identity the elements contained in each multiplicative coset of $\mathrm{GF}(q)^*$ in $\mathrm{GF}(q^2)^*$, and we express the elements of each of the multiplicative cosets as elements of the form $a + b\alpha$ $(a, b \in \mathrm{GF}(q))$ via the primitive polynomial. There are $\frac{q^2-1}{q-1} = q+1$ cosets of $C_0 = \langle \alpha^{q+1} \rangle \cong \mathrm{GF}(q)^*$ and each of them can be written in the form $C_i = \alpha^i C_0$, where $0 \le i \le q$). The elements of each coset C_i, where $0 \le i \le q$, can be written as

$$C_i = \{t\alpha^i \,|\, t \in \mathrm{GF}(q)^*\} = \{ta_i + tb_i\alpha \,|\, t \in \mathrm{GF}(q)^*\}.$$

In each multiplicative coset C_i, there is one unique element whose coefficient of α is c; this is the element $cb_i^{-1}(a_i + b_i\alpha)$. For each $c \in \mathrm{GF}(q)^*$, observe

$$S_c = \{cb_1^{-1}(a_1 + b_1\alpha), cb_2^{-1}(a_2 + b_2\alpha), \ldots, cb_q^{-1}(a_q + b_q)\alpha\}.$$

Therefore, precisely one element of every non-trivial multiplicative coset C_i with $i \neq 0$ is contained in S_c. As c runs through $\mathrm{GF}(q)^*$, the $q-1$ sets in $\{S_c\}_{c\in\mathrm{GF}(q)^*}$ partition the elements of $\mathrm{GF}(q^2)^* \backslash C_0$. Each S_c is an example of a multiplicative $(q+1, q-1, q, 1)$-RDS in $\mathrm{GF}(q^2)^*$ with respect to the multiplicative subgroup C_0. Further, each of these RDSs is an example of the original RDSs obtained by Bose in [8]. To see that no element of C_0 arises as a multiplicative difference between a pair of elements of a particular S_c, observe that every element of S_c is in a distinct coset of C_0. It can be shown by direct computation that each element of $\mathrm{GF}(q^2)^* \backslash C_0$ arises precisely once as a difference in the multiset $\Delta(S_c)$ (the details of this are left up to the reader). As each S_c is an RDS, and $\{S_c\}_{c\in\mathrm{GF}(q)^*}$ partitions $\mathrm{GF}(q^2)^* \backslash C_0$, it follows by Theorem 5.2.8 that $\{S_c\}_{c\in\mathrm{GF}(q)^*}$ is a $(q^2-1, q-1, q, q, 0)$-DPDF and a $(q^2-1, q-1, q, (q-1)(q-2), q^2-q)$-EPDF.

Finally, we convert each S_c to a set of powers of α i.e. a set $S'_c = \{i \mid \alpha^i \in S_c, 0 \leq i \leq q^2-2\} \subseteq \mathbb{Z}_{q^2-1}$. Clearly each S'_c is an additive $(q+1, q-1, q, 1)$-RDS, hence $\{S'_c\}_{c\in\mathrm{GF}(q)^*}$ is an additive DPDF and EPDF in $\mathbb{Z}_{q^2-1}$. □

There is a natural interpretation of Theorem 5.2.10 in finite geometry; we may consider each element $\alpha^i = a_i + b_i\alpha \in \mathrm{GF}(q^2)$ to be a point (a_i, b_i) in the affine plane $AG(2, q)$. We may then view each set S_c as a line in a given parallel class, which gives us the connection to Bose's original construction in [8]; for further information see our paper [35].

Example 5.2.11. *In the finite field* $\mathrm{GF}(25)$*, let* α *be a primitive element, with primitive polynomial* x^2+x+2 *over* $\mathrm{GF}(5)$*. By computing the first* 6 *powers of* α*;* α*,* $\alpha^2 = 3+4\alpha$*,* $\alpha^3 = 2+4\alpha$*,* $\alpha^4 = 2+3\alpha$*,* $\alpha^5 = 4+4\alpha$*,* $\alpha^6 = 2$*, we can compute the non-trivial multiplicative cosets of the multiplicative subgroup* $C_0 = \{1 = \alpha^0, 2 = \alpha^6, 4 = \alpha^{12}, 3 = \alpha^{18}\} = \mathrm{GF}(5)^*$ *in* $\mathrm{GF}(25)^*$*, which are:* $C_1 = \{\alpha, 2\alpha, 4\alpha, 3\alpha\}$*,* $C_2 = \{3+4\alpha, 1+3\alpha, 2+\alpha, 4+2\alpha\}$*,* $C_3 = \{2+4\alpha, 4+3\alpha, 1+2\alpha, 3+\alpha\}$*,* $C_4 = \{2+3\alpha, 4+\alpha, 1+4\alpha, 3+2\alpha\}$*,* $C_5 = \{4+4\alpha, 3+3\alpha, 2+2\alpha, 1+\alpha\}$*.*

It follows above that $S_1 = \{\alpha^1, \alpha^{14}, \alpha^{15}, \alpha^{10}, \alpha^{17}\}$*,* $S_2 = \{\alpha^7, \alpha^{20}, \alpha^{21}, \alpha^{16}, \alpha^{23}\}$*,* $S_3 = \{\alpha^{19}, \alpha^8, \alpha^9, \alpha^4, \alpha^{11}\}$ *and* $S_4 = \{\alpha^{13}, \alpha^2, \alpha^3, \alpha^{22}, \alpha^5\}$*. Each* S_c *forms a* *multiplicative* $(6,4,5,1)$*-RDS with respect to the multiplicative subgroup* $C_0 = \{1,2,3,4\}$ *in* $\mathrm{GF}(25)^*$*, and as the subsets partition* $\mathrm{GF}(25)^* \backslash C_0$*, it is clear that they also form a* $(24,4,5,4,0)$*-DPDF and a* $(24,4,5,12,30)$*-EPDF in* $\mathrm{GF}(25)^*$*. Moreover,* $S_1' = \{1,14,15,10,17\}$*,* $S_2' = \{7,20,21,16,23\}$*,* $S_3' = \{19,8,9,4,11\}$*,* $S_4' = \{13,2,3,22,5\}$ *are individually additive* $(6,4,5,1)$*-RDSs in* $\mathbb{Z}_{24}$*, and thus form both a* $(24,4,5,4,0)$*-DPDF and* $(24,4,5,12,20)$*-EPDF in the group* $\mathbb{Z}_{24}$*.*

5.3 DPDFs that are not EPDFs and vice versa

In this short section we present a construction of a DPDF that is not also an EPDF and include some computational examples of EPDFs that are not DPDFs.

Proposition 5.3.1. *Let* $t > 2$*. Then in* $\mathbb{Z}_{2t+1}$*, the collection of sets*

$$S' = \{\{2,3\},\{4,5\},\ldots,\{2t-2,2t-1\}\}$$

form a $(2t+1,t-1,2,0,t-1)$*-DPDF which is not also an EPDF.*

Proof. Each $S_i \subset S'$ takes the form $\{2i, 2i+1\}$ for $(1 \leq i \leq t-1)$. It follows that for each $S_i \subset S'$, $\Delta(S_i) = \{-1,1\}$. Therefore the multiset $\mathrm{Int}(S')$ comprises $t-1$ copies of the elements of the set $\{-1,1\}$, and no copies of the other elements of $\mathbb{Z}_{2t+1}$. Since $S = \cup_{i=1}^{s} S_i$ (where $S_i \in S'$) consists of all non-zero elements of $\mathbb{Z}_{2t+1}$, except the elements ± 1, it is immediate that S' is a $(2t+1,t-1,2,0,t-1)$-DPDF.

Notice that there are $t-2$ pairs of consecutive sets in S'; for each pair of consecutive sets, we may write $S_i = \{2i, 2i+1\}$ and $S_{i+1} = \{2i+2, 2i+3\}$, where $1 \leq i \leq t-2$. Notice that for each $1 \leq i \leq t-1$, $2i+2-(2i+1) = 1 \in \Delta(S_{i+1}, S_i)$ and $2i+1-(2i+2) = -1 \in \Delta(S_i, S_{i+1})$; meaning that there are at least $t-2$ copies of the elements in the set $\{1,-1\}$ in $\mathrm{Ext}(S')$. Similarly, since $2i+2-2i, 2i+3-(2i+1) \in \Delta(S_{i+1}, S_i)$ and $2i+2-2i, 2i+3-(2i+1) = 2$, this means that there are at least $2(t-2)$ copies of 2 in $\mathrm{Ext}(S')$. We can analogously show that there are at least $2(t-2)$ copies of -2 in $\mathrm{Ext}(S')$.

As each sub-multiset $\Delta(S_i, S_j) \in \mathrm{Ext}(S')$ $(1 \leq i,j \leq t-1)$ has cardinality 4, and there are $(t-1)(t-2)$ multisets of the form $\Delta(S_i, S_j) \in \mathrm{Ext}(S')$,; this means there are $4(t-1)(t-2)$ elements in $\mathrm{Ext}(S')$. If we assume that S' is an EPDF, then each element in $\mathbb{Z}_{2t+1}^* \backslash \{1,-1\}$ must occur at the same frequency as $\{2,-2\}$, which is at least $2(t-2)$. After the removal of the copies of the elements of the set $\{\pm 1, \pm 2\}$ from the multiset $\mathrm{Ext}(S')$, we are left with at most $4(t-1)(t-2) - 6(t-2) = 2(t-2)(2t-5)$ elements in the multiset $\mathrm{Ext}(S')$. There are $2t+1-5 = 2(t-2)$ elements in $\mathbb{Z}^*_{2t+1} \backslash \{\pm 1, \pm 2\}$. This means if $\mathrm{Ext}(S')$ contains at least $t-2$ copies of $\{1, -1\}$ and at least $2(t-2)$ copies of $\{2, -2\}$; then every element of $\mathbb{Z}^*_{2t+1} \backslash \{\pm 1, \pm 2\}$ occurs with frequency at most $\frac{2(t-2)(2t-5)}{2(t-2)} = 2t-5$, and since $2t-5 < 2(t-2)$, S' is not an EDF. □

The following EPDF examples in cyclic groups (found by Prof. Chris Jefferson [41] via computation in GAP [31]) are, to date, our only examples of EPDFs that are not also DPDFs. We are yet to find an overarching construction for these results, but they have been included within this Thesis as they may be of interest to the reader.

Example 5.3.2. *(i) The sets* $\{1, 8\}, \{3, 6\}$ *form a* $(9, 2, 2, 0, 2)$*-EPDF in* $\mathbb{Z}_9$*, which is not simultaneously a DPDF.*

(ii) Similarly, the sets $\{1, 2, 11, 12\}, \{3, 5, 8, 10\}$ *form a* $(13, 2, 4, 2, 4)$*-EPDF which is not also a DPDF.*

Chapter 6

Conclusion and further work

In this Thesis, we introduced two new combinatorial objects, known as Disjoint Partial Difference Families (DPDFs) and External Partial Difference Families (EPDFs), that generalise many of the existing structures in the literature. We established two new cyclotomic frameworks which may be used to identify new cyclotomic constructions of these objects. A key strength of the cyclotomic frameworks developed in this Thesis is that they give mathematicians a novel way of using finite field cyclotomy to identify new constructions of various difference structures, without having to rely upon evaluating specific cyclotomic numbers.

We applied the cyclotomic frameworks to identify new DPDF and EPDF constructions in various finite fields. Moreover, we used the techniques from these frameworks to create a series of algorithms that compute the cyclotomic numbers of order e in large finite fields; it is useful to have algorithms that allow one to generate cyclotomic numbers in large finite fields in order to analyse patterns of cyclotomic numbers within larger finite fields and thus identify new universal cyclotomic behaviour. In this Thesis, we used this algorithm to produce the cyclotomic numbers of order 13 in the finite field GF(729), thus proving that a PDS with Denniston parameters exists in this particular finite field. Finally, we established the first non-cyclotomic constructions of DPDFs and EPDFs from collections of non-cyclotomic PDSs and RDSs.

There are many different ways in which we can expand upon the work of this Thesis. One natural direction is to look at further developing the cyclotomic frameworks that we established in Chapter 2. In the paper [51], the authors use lifting constructions to identify new constructions of cyclotomic Difference Sets.

By incorporating such techniques into our framework, we will be able to identify new cyclotomic constructions of Difference structures. Another idea that we will explore is looking at cyclotomy in Galois Domains Storer laid the foundations for this in the second half of [60], and we explored similar ideas in our Denniston project.

In terms of the cyclotomic orbit framework, there are several questions that it would helpful to answer, for example:

Question 1. *When p and $e \geq 5$ are distinct odd primes and $n_1 = \mathrm{ord}_e(p)$ in $\mathrm{GF}(e)$ is odd, can we determine the cyclotomic orbit representative of any cyclotomic orbit of order $2n_1$?*

Question 2. *When p and $e \geq 5$ are distinct odd primes and $n_1 = \mathrm{ord}_e(p)$ is odd, can we determine the cyclotomic orbit representative of any cyclotomic orbit of order $6n_1$?*

Resolving these questions will allow us to generate an algorithm which automatically computes the external cyclotomic numbers of e in a finite field $\mathrm{GF}(q)$ of order $q = p^m = ef + 1$, where p is prime, f is even, $e \geq 5$ and $n_1 = \mathrm{ord}_e(p)$ is odd, which will increase the scope of the current algorithm. Moreover, we will also continue to explore the connection between cyclotomic orbits and cyclotomic numbers more generally. In particular, we can look at cases where f is odd, e is not prime and where $n_1 = \mathrm{ord}_e(p)$ is even.

We also hope to continue to deepen our understanding of the finite field cyclotomy underlying the constructions of Denniston PDSs, in the hope that we can identify new constructions of related combinatorial structures. We note that since the original submission of this Thesis, some of the questions in open questions in our paper [20] have been answered by the paper [3]. In particular the authors of [3] have resolved the intermediate Denniston PDS cases (the cases where $2 \leq r \leq m - 2$).

Beyond cyclotomy, we plan to explore applications of DPDFs and EPDFs in experiment design and information security we have begun this process in the preprint [40].

Finally, we also wish to establish constructions for EPDFs that are not also DPDFs, and vice versa, as this has not, as of yet, been explored. The examples at the end of Chapter 5 are a first step in this process.

Bibliography

[1] S. Ball, A. Blokhuis and F. Mazzocca, Maximal arcs in Desarguesian planes of odd order do not exist, *Combinatorica*, **17** (1997), 31-41.

[2] J. Bao, L. Ji, R. Wei and Y. Zhang, New existence and nonexistence results for strong external difference families, *Discrete Math.*, **341** (2018), 1798-1805.

[3] J. Bao, Q. Xiang and M. Zhao, Partial Difference Sets with Denniston Parameters in Elementary Abelian p-Groups, preprint on ArXiV (available at arXiv: 2407.15632), (2024).

[4] L.D. Baumert, W.H. Mills and R.L. Ward, Uniform cyclotomy, *J. Number Theory*, **14** (1982), 67-82.

[5] B. Berndt, R.J. Evans and K.S. Williams, Gauss and Jacobi Sums, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, Inc., New York, 1998.

[6] J. Bierbrauer and Y. Edel, A family of 2-weight codes related to BCH-Codes, *J. Combin. Des.* **5** (1997), 391-396.

[7] R.C. Bose, On the constructions of balanced incomplete block designs, *Annuals of Eugenics*, **9(4)** (1939), 353-399.

[8] R.C. Bose. An affine analogue of Singer's theorem, *J. Indian Math. Soc. (N.S.)* **6** (1942), 1-15.

[9] M. Buratti, On simple radical difference families, *J. Comb. Des.*, **3** (1995), 161-168.

[10] M. Buratti, Recursive constructions for difference matrices and relative difference families, *J. Combin. Des.*, **6** (1998), 165-182

[11] M. Buratti, On disjoint $(v, k, k-1)$ difference families, *Des. Codes Cryptogr.*, **87** (2019), 745-755.

[12] M. Buratti and A. Pasotti, Graph decompositions with the use of difference matricies, *Bulletin of the Institute of Combinatorics and its Applications*, **47** (2006), 23-32

[13] R. Calderbank and W.M. Kantor, The geometry of two-weight codes, *Bull. Lond. Math. Soc.*, **18** (1986), 97-122.

[14] Y. Chang and C. Ding. Constructions of EDFs and DDFs, *Des. Codes Cryptogr.*, **40** (2006), 167-185.

[15] Y.Q. Chen and C.H. Li, Relative difference sets fixed by inversion and Cayley graphs, *J. Combin. Theory Ser. A.*, **111** (2005), 165-173.

[16] B. Chen, L. Lin and S. Ling, External difference families from finite fields *J. Comb. Des.*, **25** (2017), 36-48.

[17] C.J. Colbourn and J.H. Dinitz, Handbook of Combinatorial Designs, second edition, Chapman and Hall/CRC, 2007.

[18] D.A. Cox, Primes of the form $x^2 + ny^2$, John Wiley and Sons Inc., (1989), New York, xiii+354pp.

[19] R. Cramer, Y. Dodis, S. Fehr, C. Padró and D. Wichs, Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. In: N.Smith, editor, *Advances in Cryptology - EUROCRYPT*, Berlin, Heidelberg, (2008), Springer Berlin Heidelberg, 471-488.

[20] J.A. Davis, S. Huczynska, L. Johnson and J. Polhill, Partial difference sets with Denniston parameters and cyclotomy, preprint on ArXiV (available at arXiv:2311.00512), (2023).

[21] J.A. Davis, S. Huczynska and G.L. Mullen, Near-complete external difference families, *Des. Codes and Cryptogr.*, **84** (2017), 415-424.

[22] P. Delsarte, An algebraic approach to the association schemes of coding theory, *Philips Research Report*, (1973), Suppl. No. 10.

[23] R. Denniston, Some maximal arcs in finite projective planes, *J. Comb Th.*, **6** (1969), 317-319.

[24] S. de Winter, Projective two-weight sets of Denniston type, preprint on ArXiV (available at arXiv:2311.00827), (2023).

[25] L.E. Dickson, Cyclotomy, higher congruences and Waring's problem, *Am. J. Math*, **57** (1935), 391-424.

[26] J. F. Dillon, Elementary Hadamard difference sets, *Proceesings, Sixth Southeastern Conference on Combinatorics, Graph Theory and Computing, Florida Atlantic University, Boca Raton, Fla., 1975*, (1975), 237-249.

[27] C. Ding and Y. Yin, Constructions of almost difference families, *Discrete Math.*, **308** (2008), 4941-4954.

[28] J.E.H. Elliott and A.T.Butson, Relative difference sets, *Illinous J. Math.*, **10** (1966), 517-531.

[29] T. Feng, D. Horsley and X. Wang, Novak's conjecture on cyclic Steiner triple systems and its generalization, *J. Comb. Theory, Ser. A*, **184** (2021), 105515, 10 pp.

[30] M.J. Ganley and E. Spence, Relative Difference Sets and Quasiregular Collineation Groups, *J. Combin. Theory Set. A*, **19** (1975), 134-153.

[31] The GAP Group, GAP - Groups, Algorithms, and Programming, Version 4.10.2; 2019. (https://www.gap-system.org)

[32] B. Huang and D. Wu, Cyclotomic constructions of external difference families and disjoint difference families, *J. Comb. Des.*, **17** (2009), 333-341.

[33] S. Huczynska, C. Jefferson and S. Nepsinska, Strong external difference families in abelian and non-abelian groups, *Cryptogr. Commun.*, **13** (2021), 331-341.

[34] S. Huczynska and L. Johnson, Internal and external partial difference families and cyclotomy, *Discrete Math.*, **346(3)** (2023) Paper no. 113295, 24pp.

[35] S. Huczynska and L. Johnson, New constructions for disjoint partial difference families and external partial difference families, *J. Combin. Des.* **32(4)** (2024), 190-213. https://doi.org/10.1002/jcd.21930

[36] S. Huczynska, L. Johnson and M.B. Paterson, Beyond uniform cyclotomy, preprint on ArXiV (available at arXiv:2406.16805), (2024).

[37] S. Huczynska and M.B. Paterson, Weighted external difference families and R-optimal AMD codes, *Discrete Math.*, **342** (2019), 855-867.

[38] J. Jedwab and S. Li, Constructions and non-existence of strong external difference families, *J. Algebraic Comb.*, **49** (2019), 21-48.

[39] J. Jedwab and S. Li, Packings of partial difference sets, *Comb. Theory.*, **1**, (2021), Paper no. 18. 41pp.

[40] L. Johnson and S. Huczynska, Applications of partial difference families to partial designs, in preparation.

[41] C. Jefferson, personal communication.

[42] S.A. Katre and A.R. Rajwade, Resolution of the sign ambiguity in the determination of the cyclotomic numbers of order 4 and the corresponding Jacobsthal sum, *Math. Scand.*, **60** (1987), 52-62.

[43] E. Lehmer. On the number of solutions of $u^k = d + w^2 (\mod p)$, *Pac. J. Math*, **5** (1955), 103-118.

[44] P.A. Leonard, Cyclic relative difference sets, *Amer. Math. Monthly*, **93(2)** (1986), 106-111.

[45] F. Li, Q. Yue and Y. Wu, Designed distances and parameters of new LCD BCH codes over finite fields, *Cryptography and Communications*, **12** (2020), 147-163.

[46] L. Li, A note on difference families from cyclotomy, *Discrete Math.*, **340** (2017), 1784-1787.

[47] S.L. Ma, Partial difference sets, *Discrete Math.* **52** (1984), 75-89.

[48] S.L. Ma, On association schemes, Schur rings, strongly regular graphs and partial difference sets, *Ars Combin.*, **27** (1989), 211-220.

[49] S.L. Ma, A survey of partial difference sets, *Des. Codes and Cryptogr.*, **4** (1994), 221-261.

[50] W. Meidl and A. Winterhof, Some notes on the linear complexity of Sidel'nikov-Lempel-Cohn-Eastman sequences, *Des. Codes. Cryptogr.*, **38** (2006), 159-178.

[51] K. Momihara and Q. Xiang, Strongly regular Cayley graphs from partitions of subdifference sets of the Singer difference sets, *Finite Fields Appl.*, **50** (2018), 222-250.

[52] Y. Mutoh and V.D. Tonchev, Difference systems of sets and cyclotomy, *Discrete Math.*, **308** (2008), 2959-2969.

[53] S.L. Ng and M.B. Paterson, Disjoint difference families and their applications, *Des. Codes Cryptogr.*, **78** (2016), 103-127.

[54] J. Novak, A note on disjoint cyclic Steiner triples systems, in: Recent Advances in Graph theory, Proc. Symp., Prague, 1974, Academia, Praha, 1975, pp. 439-440.

[55] W. Ogata, K. Kurosawa, D.R. Stinson and H. Saido, New combinatorial designs and their applications to authentication codes and secret sharing schemes, *Discrete Math.*, **279** (2004), 383-405.

[56] R.E.A.C. Paley, On orthogonal matrices, *J. Math. Phys.* **12**, 1933, 311-320.

[57] A. Pasotti and J. H. Dinitz, A survey of Heffter arrays, preprint (2022) [accepted for publication in the Stinson 66 - New Advances in Designs, Codes and Cryptography conference proceedings, available at arXiv:2209.13879].

[58] M.B. Paterson and D.R. Stinson, Combinatorial characterizations of algebraic manipulation detection codes involving generalized difference families, *Discrete Math.*, **339(12)** (2016), 2891-2906.

[59] A. Pott, A survey in relative difference sets, in: Groups, Difference Sets, and the Monster (Columbus, OH,1993), Ohio State Univ. Math. Res. Inst. Publ., vol **4**, De Gruyter, Berlin, 1996, pp.195-232

[60] T. Storer, Cyclotomy and difference sets, in: Lectures in Advanced Mathematics, vol. **2**, Markham Publishing Co., Chicago, III, 1967, vii+134pp.

[61] E. Swartz and G. Tauscheck, Restrictions on parameters of partial difference sets in nonabelian groups, *Journal of Combinatorial Designs*, **29(1)** (2020), 38-51.

[62] V.D. Tonchev, Difference systems of sets and code synchronization, *Rend. Sem. Mat. Messine Set, II*, **9** (2003), 217-226.

[63] Z. Wang, Paley type partial difference sets in abelian groups, *Journal of Combinatorial Designs*, **28(2)** (2020), pp. 95-152.

[64] S.H. Weintraub, Galois Theory, in: Universitext (2^{nd} edition), Springer, New York, 2008, xiv+212pp.

[65] J. Wen, M. Yang and K. Feng, The (n, m, k, λ)-strong external difference family with $m \geq 5$ exists, preprint on ArXiV (available at arXiv:1612.09495), (2016).

[66] R. M. Wilson, Cyclotomy and difference families in elementary abelian groups, *Journal of Number Theory*, **4** (1972), 17-47.

[67] B. Xia, Cyclotomic difference sets in finite fields, *Mathematics of Computation*, **87(313)** (2018), 2461-2482.

Appendices

Appendix A

Cyclotomic numbers

In this Appendix, we present some results on evaluating the cyclotomic numbers of order $e \in \{3, 4, 6, 8\}$ these results are stated without proof. Before we cover the results of this Appendix, we first define the term unique proper representation, as this term is used throughout all theorems in this Section. The following definition has been taken from page 24 of [18].

Definition A.0.1. *An* ***integral binary quadratic form*** $f(x, y)$ *is a quadratic homogeneous polynomial in two variables*

$$f(x, y) = ax^2 + bxy + cy^2,$$

where $a, b, c \in \mathbb{Z}$. *An integer* n *is* ***represented*** *by* $f(x, y)$ *if there exist integers* x *and* y *such that* $n = f(x, y)$. *A representation is* ***proper*** *if* $\gcd(x, y) = 1$. *For certain values of* n*, there exists a* ***unique proper representation*** *of* n*.*

For further discussions on unique proper representations see page 56 of [60]. Note that we only give the values of internal cyclotomic numbers of the form $(i, 0)_e$ (where $0 \leq i \leq e - 1$) in many of the results of this Appendix. This is because the results in this Section are only applied in Chapter 3 of this Thesis, and in Chapter 3, we are only interested in the values of the internal cyclotomic numbers.

Our first result details the cyclotomic numbers of order $e = 3$. These results have been taken from [25] and [60].

Theorem A.0.2. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^m \equiv 1 \mod 3$*. Let*

$$4q = c^2 + 27d^2, \qquad c \equiv 1 \mod 3,$$

where,

(i) if $p \equiv 2 \mod 3$ *then* m *is even and* $d = 0$

(ii) if $p \equiv 1 \mod 3$ *then this is the unique proper representation of* $4q$ *with* $c \equiv 1 \mod 3$.

The cyclotomic number relations are as follows

$$A = (0,0)_3 = \frac{1}{9}(q - 8 + c),\ B = (2,2)_3 = (1,0)_3 = (0,1)_3 = \frac{1}{18}(2q - 4 - c - 9d),$$
$$C = (1,1)_3 = (2,0)_3 = (0,2)_3 = \frac{1}{18}(2q - 4 - c + 9d),$$
$$D = (1,2)_3 = (2,1)_3 = \frac{1}{9}(q + 1 + c).$$

Our next result details formulas for some of the cyclotomic numbers of order 4. The results quoted in this Theorem have been taken from [**?**], [42] and [60].

Theorem A.0.3. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^m \equiv 1 \mod 4$*. Let* v *be a generator of* $\mathrm{GF}(q)^*$.

(i) If $p \equiv 3 \mod 4$*, then* $s = (-p)^{\frac{m}{2}}$ *and* $t = 0$.

(ii) If $p \equiv 1 \mod 4$*, define* s *uniquely by* $q = s^2 + t^2$, $p \nmid s$, $s \equiv 1 \mod 4$*, then* t *is uniquely by* $v^{(q-1)/4} \equiv s/t \mod p$.

Then the cyclotomic numbers of the form $(i,0)_4$ *in* $\mathrm{GF}(q)$ *corresponding to* v *are determined unambiguously by the formulae:*

- *When* f *is even:* $A = (0,0)_4 = \frac{1}{16}(q - 11 - 6s)$, $B = (3,3)_4 = (1,0)_4 = (0,1)_4 = \frac{1}{16}(q - 3 + 2s + 4t)$, $C = (2,2)_4 = (2,0)_4 = (0,2)_4 = \frac{1}{16}(q - 3 + 2s)$, $D = (1,1)_4 = (3,0)_4 = (0,3)_4 = \frac{1}{16}(q - 3 + 2s - 4t)$, $E = (1,2)_4 = (1,3)_4 = (2,1)_4 = (2,3)_4 = (3,1)_4 = (3,2)_4 = \frac{1}{16}(q + 1 - 2s)$.

- *When* f *is odd* $A = (0,0)_4 = (2,0)_4 = \frac{1}{16}(q - 7 + 2s)$, $E = (1,0)_4 = (3,0)_4 = \frac{1}{16}(q - 3 - 2s)$.

The next theorem details formulas for some of the cyclotomic numbers of order $e = 6$ when f is even. These results have been taken from [25], [60] and [67] (note that whilst [67] does not explictly include the cyclotomic numbers of order 6, the cyclotomic numbers of order 6 can be derived using the results of this paper).

Theorem A.0.4. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^m \equiv 1 \mod 6$*. The cyclotomic numbers of order* 6 *are solely functions of the unique representation*

$$q = p^m = s^2 + 3t^2, \qquad s \equiv 1 \mod 4$$

determined by

(i) if $p \equiv 5 \mod 6$ *then* m *is even and* $q = (\pm p^{\frac{m}{2}})^2 + 3(0)^2$

(ii) if $p \equiv 1 \mod 6$*, then* $q = s^2 + 3t^2$ *is the unique proper representation of* q*, with* $s \equiv 1 \mod 3$ *the sign of* t *is ambiguously determined.*

Then, when f *is even, the internal cyclotomic numbers of the form* $(i, 0)_6$ *may be determined by the following formulae:*

- *when* $2 \in C_0^{6,m}$ *or* $2 \in C_3^{6,m}$*:* $A = (0,0)_6 = \frac{1}{36}(q - 17 - 20s)$*,* $B = (1,0)_6 = \frac{1}{36}(q - 5 + 4s + 18t)$*,* $C = (2,0)_6 = \frac{1}{36}(q - 5 + 4s + 6t)$*,* $D = (3,0)_6 = \frac{1}{36}(q - 5 + 4s)$*,* $E = (4,0)_6 = \frac{1}{36}(q - 5 + 4s - 6t)$*,* $F = (5,0)_6 = \frac{1}{36}(q - 5 + 4s - 18t)$*.*
- *when* $2 \in C_1^{6,m}$ *or* $2 \in C_4^{6,m}$*:* $A = (0,0)_6 = \frac{1}{36}(q - 17 - 8s + 6t)$*,* $B = (1,0)_6 = \frac{1}{36}(q - 5 + 4s + 12t)$*,* $C = (2,0)_6 = \frac{1}{36}(q - 5 + 4s - 6t)$*,* $D = (3,0)_6 = \frac{1}{36}(q - 5 + 4s - 6t)$*,* $E = (4,0)_6 = \frac{1}{36}(q - 5 - 8s)$*,* $F = (5,0)_6 = \frac{1}{36}(q - 5 + 4s - 6t)$*.*
- *when* $2 \in C_2^{6,m}$ *or* $2 \in C_5^{6,m}$*:* $A = (0,0)_6 = \frac{1}{36}(q - 17 - 8s - 6t)$*,* $B = (1,0)_6 = \frac{1}{36}(q - 5 + 4s + 6t)$*,* $C = (2,0)_6 = \frac{1}{36}(q - 5 - 8s)$*,* $D = (3,0)_6 = \frac{1}{36}(q - 5 + 4s + 6t)$*,* $E = (4,0)_6 = (q - 5 + 4s + 6t)$*,* $F = (5,0)_6 = \frac{1}{36}(q - 5 + 4s - 12t)$*.*

Our final result details formulas for the cyclotomic numbers of order $e = 8$. These results can be found in [25], [60] and [43].

Theorem A.0.5. *Let* $\mathrm{GF}(q)$ *be a finite field of order* $q = p^m \equiv 1 \mod 8$*. The cyclotomic numbers of order* 8 *are uniquely determined by* x, y, a *and* b *defined below.*

(i) $q = x^2 + 4y^2$, $x \equiv 1 \mod 4$ *is the unique proper representation of* $q = p^m$ *if* $p \equiv 1 \mod 4$ *otherwise* $x = \pm p^{\frac{m}{2}}$ *and* $y = 0$.

(ii) $q = a^2 + 2b^2$, $a \equiv 1 \mod 4$, *is the unique proper representation of* $q = p^m$ *if* $p \equiv 1 \mod 8$ *or* $p \equiv 3 \mod 8$ *otherwise* $a = \pm p^{\frac{m}{2}}$ *and* $b = 0$.

The signs of y *and* b *are ambiguously determine.*

The cyclotomic numbers of the form $(i, 0)_8$ *are then uniquely determined by the following formulae*

- *When* 2 *is a quartic residue and* f *is even:* $A = (0,0)_8 = \frac{1}{64}(q - 23 - 18x - 24a)$, $B = (1,0)_8 = \frac{1}{64}(q - 7 + 2x + 4a + 16y + 16b)$, $C = (2,0)_8 = \frac{1}{64}(q - 7 + 6x + 16y)$, $D = (3,0)_8 = \frac{1}{64}(q - 7 + 2x + 4a - 16y + 16b)$, $E = (4,0)_8 = \frac{1}{64}(q - 7 + 2x + 8a)$, $F = (5,0)_8 = \frac{1}{64}(q - 7 + 2x + 4a + 16y - 16b)$, $G = (6,0)_8 = \frac{1}{64}(q - 7 + 6x - 16y)$, $H = \frac{1}{64}(q - 7 + 2x + 4a - 16y - 16b)$.

- *When* 2 *is a quartic residue and* f *is odd:* $A = (0,0)_8 = (4,0)_8 = \frac{1}{64}(q - 15 - 2x)$, $I = (1,0)_8 = (5,0)_8 = \frac{1}{64}(q - 7 + 2x + 4a)$, $N = (2,0)_8 = (6,0)_8 = \frac{1}{64}(q - 7 - 2x - 8a)$, $J = (3,0)_8 = (7,0)_8 = \frac{1}{64}(q - 7 + 2x + 4a - 16y - 16b)$.

- *When* 2 *is not a quartic residue and* f *is even:* $A = (0,0)_8 = \frac{1}{64}(q - 23 + 6x)$, $B = (1,0)_8 = \frac{1}{64}(q - 7 + 2x + 4a)$, $C = (2,0)_8 = \frac{1}{64}(q - 7 - 2x - 8a - 16y)$, $D = (3,0)_8 = \frac{1}{64}(q - 7 + 2x + 4a)$, $E = (4,0)_8 = \frac{1}{64}(q - 7 + 10x)$, $F = (5,0)_8 = \frac{1}{64}(q - 7 + 2x + 4a)$, $G = (6,0)_8 = \frac{1}{64}(q - 7 - 2x - 8a + 16y)$, $H = \frac{1}{64}(q - 7 + 2x + 4a)$.

- *When* 2 *is not a quartic residue and* f *is odd:* $A = (0,0)_8 = (4,0)_e = \frac{1}{64}(q - 15 - 10x - 8a)$, $I = (1,0)_8 = (5,0)_8 = \frac{1}{64}(q - 7 + 2x + 4a + 16y)$, $N = (2,0)_8 = (6,0)_8 = \frac{1}{64}(q - 7 + 6x)$, $J = (3,0)_8 = (5,0)_8 = \frac{1}{64}(q - 7 + 2x + 4a - 16y)$.

Appendix B

All cyclotomic DPDFs and EPDFs

This Appendix contains a series of tables which list all known DPDF and EPDF constructions in finite fields of order $q \leq 121$ and $\epsilon \in \{2,3,4,6,8\}$.

q	ϵ	ρ	PDS Parameters	e	f	DPDF Parameters	EPDF Parameters
9	2	4	$(9,4,1,2)$-PDS	4	2	$(9,2,2,1,0)$-DPDF	$(9,2,2,0,2)$-EPDF
13	2	6	$(13,6,2,3)$-PDS	4	3	$(13,2,3,0,2)$-DPDF	$(13,2,3,2,1)$-EPDF
13	2	6	$(13,6,2,3)$-PDS	6	2	$(13,2,3,0,1)$-DPDF	$(13,2,3,2)$-EPDF
17	2	8	$(17,8,3,4)$-PDS	4	4	$(17,2,4,1,2)$-DPDF	$(17,2,4,2)$-(S)EDF
17	2	8	$(17,8,3,4)$-PDS	8	2	$(17,4,2,1,0)$-DPDF	$(17,4,2,2,4)$-EPDF
25	2	12	$(25,12,5,6)$-PDS	4	6	$(25,2,6,3,2)$-DPDF	$(25,2,6,2,4)$-EPDF
25	2	12	$(25,12,5,6)$-PDS	6	4	$(25,3,4,3,0)$-DPDF	$(25,3,4,2,6)$-DPDF
25	2	12	$(25,12,5,6)$-PDS	8	3	$(25,4,3,0,2)$-DPDF	$(25,4,3,5,4)$-EPDF
25	2	12	$(25,12,5,6)$-PDS	12	2	$(25,6,2,1,0)$-DPDF	$(25,6,2,4,6)$-EPDF
25	3	8	$(25,8,3,2)$-PDS	6	4	$(25,2,4,3,0)$-DPDF	$(25,2,4,0,2)$-EPDF
25	3	8	$(25,8,3,2)$-PDS	12	2	$(25,4,2,1,0)$-DPDF	$(25,4,2,2)$-EDF
25	6	4	$(25,4,3,0)$-PDS	12	2	$(25,2,2,1,0)$-DPDF	$25,2,2,2,0)$-EPDF
29	2	14	$(29,14,6,7)$-PDS	4	7	$(29,2,7,4,2)$-DPDF	$(29,2,7,2,5)$-EPDF
29	2	14	$(29,14,6,7)$-PDS	14	2	$(29,7,2,0,1)$-DPDF	$(29,7,2,6)$-EDF
37	2	18	$(37,18,8,9)$-PDS	4	9	$(37,2,9,4)$-DDF	$(37,2,9,4,5)$-EPDF
37	2	18	$(37,18,8,9)$-PDS	6	6	$(37,3,6,4,1)$-DPDF	$(37,3,6,4,8)$-EPDF
37	2	18	$(37,18,8,9)$-PDS	12	3	$(37,6,3,2,0)$-DPDF	$(37,6,3,6,9)$-EPDF
37	2	18	$(37,18,8,9)$-PDS	18	2	$(37,9,2,0,1)$-DPDF	$(37,9,2,8)$-EDF

q	ϵ	ρ	PDS Parameters	e	f	DPDF Parameters	EPDF Parameters
41	2	20	$(41,20,9,10)$-PDS	4	10	$(41,2,10,3,6)$-DPDF	$(41,2,10,6,4)$-EPDF
41	2	20	$(41,20,9,10)$-PDS	8	5	$(41,4,5,2)$-DDF	$(41,4,5,7,8)$-EPDF
41	2	20	$(41,20,9,10)$-PDS	10	4	$(41,5,4,3,0)$-DPDF	$(41,5,4,6,10)$-EPDF
41	2	20	$(41,20,9,10)$-PDS	20	2	$(41,10,2,1,0)$-DPDF	$(41,10,2,8,10)$-EPDF
49	2	24	$(49,24,11,12)$-PDS	4	12	$(49,2,12,5,6)$-DPDF	$(49,2,12,6)$-EDF
49	2	24	$(49,24,11,12)$-PDS	6	8	$(49,3,8,3,4)$-DPDF	$(49,3,8,8)$-EDF
49	2	24	$(49,24,11,12)$-PDS	8	6	$(49,4,6,5,0)$-DPDF	$(49,4,6,6,12)$-EPDF
49	2	24	$(49,24,11,12)$-PDS	12	4	$(49,6,4,3,0)$-DPDF	$(49,2,8,12)$-EPDF
49	2	24	$(49,24,11,12)$-PDS	16	3	$(49,8,3,2,0)$-DPDF	$(49,8,3,9,12)$-EPDF
49	2	24	$(49,24,11,12)$-PDS	24	2	$(49,12,2,1,0)$-DPDF	$(49,12,2,10,12)$-EPDF
49	4	12	$(49,12,5,2)$-PDS	8	6	$(49,2,6,5,0)$-DPDF	$(49,2,6,0,2)$-EPDF
49	4	12	$(49,12,5,2)$-PDS	16	3	$(49,4,3,2,0)$-DPDF	$(49,4,3,3,2)$-EPDF
49	4	12	$(49,12,5,2)$-PDS	24	2	$(49,6,2,1,0)$-DPDF	$(49,6,2,4,2)$-EPDF
49	8	6	$(49,8,5,0)$-PDS	16	3	$(49,2,3,2,0)$-DPDF	$(49,2,3,3,0)$-EPDF
49	8	6	$(49,8,5,0)$-PDS	24	2	$(49,3,2,1,0)$-DPDF	$(49,3,2,4,0)$-EPDF
53	2	26	$(53,26,12,13)$-PDS	4	13	$(53,2,13,4,8)$-DPDF	$(53,2,13,8,5)$-EPDF
53	2	26	$(53,26,12,13)$-PDS	26	2	$(53,13,2,0,1)$-DPDF	$(53,2,13,12)$-EDF
61	2	30	$(61,30,14,15)$-PDS	4	15	$(61,2,15,8,6)$-DPDF	$(61,2,15,6,9)$-EPDF
61	2	30	$(61,30,14,15)$-PDS	6	10	$(61,3,10,2,7)$-DPDF	$(61,3,10,12,8)$-EPDF
61	2	30	$(61,30,14,15)$-PDS	10	6	$(61,5,6,4,1)$-DPDF	$(61,5,6,10,14)$-EPDF
61	2	30	$(61,30,14,15)$-PDS	12	5	$(61,6,5,2)$-DDF	$(61,6,5,12,13)$-EPDF
61	2	30	$(61,30,14,15)$-PDS	20	3	$(61,10,3,2,0)$-DPDF	$(61,6,5,12,15)$-EPDF
61	2	30	$(61,30,14,15)$-PDS	30	2	$(61,15,2,0,1)$-DPDF	$(61,15,2,14)$-EDF
64	3	21	$(64,21,8,6)$-PDS	9	7	$(64,3,7,6,0)$-DPDF	$(64,3,7,2,6)$-EPDF
64	3	21	$(64,21,8,6)$-PDS	21	3	$(64,7,3,2,0)$-DPDF	$(64,7,3,6)$-EDF
73	2	36	$(73,36,17,18)$-PDS	4	18	$(73,2,18,9,8)$-DPDF	$(73,2,18,8,10)$-EPDF
73	2	36	$(73,36,17,18)$-PDS	6	12	$(73,3,18,7,4)$-DPDF	$(73,3,12,10,14)$-EPDF
73	2	36	$(73,36,17,18)$-PDS	8	9	$(73,4,9,4)$-DDF	$(73,4,9,13,14)$-EPDF
73	2	36	$(73,36,17,18)$-PDS	12	6	$(73,6,6,3,2)$-DPDF	$(73,6,6,14,16)$-EPDF
73	2	36	$(73,36,17,18)$-PDS	18	4	$(73,9,4,1,2)$-DPDF	$(73,9,4,16)$-EDF
73	2	36	$(73,36,17,18)$-PDS	24	3	$(73,12,3,0,2)$-DPDF	$(73,12,3,17,16)$-EPDF
73	2	36	$(73,36,17,18)$-PDS	36	2	$(73,18,2,1,0)$-DPDF	$(73,18,2,16,18)$-EPDF
81	2	40	$(81,40,19,20)$-PDS	4	20	$(81,2,20,7,12)$-DPDF	$(81,2,20,12,8)$-EPDF
81	2	40	$(81,40,19,20)$-PDS	8	10	$(81,4,10,5,4)$-DPDF	$(81,4,10,14,16)$-EPDF

q	ϵ	ρ	PDS Parameters	e	f	DPDF Parameters	EPDF Parameters
81	2	40	$(81, 40, 19, 20)$-PDS	10	8	$(81, 5, 8, 7, 0)$-DPDF	$(81, 5, 8, 12, 20)$-EPDF
81	2	40	$(81, 40, 19, 20)$-PDS	16	5	$(81, 8, 5, 0, 4)$-DPDF	$(81, 8, 5, 19, 16)$-EPDF
81	2	40	$(81, 40, 19, 20)$-PDS	20	4	$(81, 10, 4, 3, 0)$-DPDF	$(81, 10, 4, 16, 20)$-EPDF
81	2	40	$(81, 40, 19, 20)$-PDS	40	2	$(81, 20, 2, 1, 0)$-DPDF	$(81, 10, 4, 18, 20)$-EPDF
81	4	20	$(81, 20, 1, 6)$-PDS	40	2	$(81, 10, 2, 1, 0)$-DPDF	$(81, 10, 2, 0, 6)$-EPDF
89	2	44	$(89, 44, 21, 22)$-PDS	4	22	$(89, 2, 22, 9, 12)$-DPDF	$(89, 2, 22, 12, 10)$-EPDF
89	2	44	$(89, 44, 21, 22)$-PDS	8	11	$(89, 4, 11, 2, 8)$-DPDF	$(89, 4, 11, 19, 14)$-EPDF
89	2	44	$(89, 44, 21, 22)$-PDS	22	4	$(89, 11, 4, 1, 2)$-DPDF	$(89, 11, 4, 20)$-EDF
89	2	44	$(89, 44, 21, 22)$-PDS	44	2	$(89, 11, 4, 1, 0)$-DPDF	$(89, 11, 20, 22)$-EPDF
97	2	48	$(97, 48, 23, 24)$-PDS	4	24	$(97, 2, 24, 9, 14)$-DPDF	$(97, 2, 24, 14, 10)$-EPDF
97	2	48	$(97, 48, 23, 24)$-PDS	6	16	$(97, 3, 16, 5, 10)$-DPDF	$(97, 3, 16, 18, 14)$-EPDF
97	2	48	$(97, 48, 23, 24)$-PDS	8	12	$(97, 4, 12, 3, 8)$-DPDF	$(97, 4, 12, 20, 16)$-EPDF
97	2	48	$(97, 48, 23, 24)$-PDS	12	8	$(97, 6, 8, 3, 4)$-DPDF	$(97, 6, 8, 20)$-EDF
97	2	48	$(97, 48, 23, 24)$-PDS	16	6	$(97, 8, 6, 3, 2)$-DPDF	$(97, 8, 6, 20, 22)$-EPDF
97	2	48	$(97, 48, 23, 24)$-PDS	24	4	$(97, 12, 4, 1, 2)$-DPDF	$(97, 12, 4, 22)$-EDF
97	2	48	$(97, 48, 23, 24)$-PDS	32	3	$(97, 16, 3, 0, 2)$-DPDF	$(97, 16, 3, 23, 22)$-EPDF
97	2	48	$(97, 48, 23, 24)$-PDS	48	2	$(97, 24, 2, 1, 0)$-DPDF	$(97, 24, 2, 22, 24)$-EPDF
101	2	50	$(101, 50, 24, 25)$-PDS	4	25	$(101, 2, 25, 12)$-DDF	$(101, 2, 25, 12, 13)$-EPDF
101	2	50	$(101, 50, 24, 25)$-PDS	10	10	$(101, 5, 10, 4, 5)$-DPDF	$(101, 5, 10, 20)$-EDF
101	2	50	$(101, 50, 24, 25)$-PDS	20	5	$(101, 10, 5, 0, 4)$-DPDF	$(101, 10, 5, 24, 21)$-EPDF
101	2	50	$(101, 50, 24, 25)$-PDS	50	2	$(101, 25, 2, 0, 1)$-DPDF	$(101, 25, 2, 24)$-EDF
109	2	54	$(109, 54, 26, 27)$-PDS	4	27	$(109, 2, 27, 12, 14)$-DPDF	$(109, 2, 27, 14, 13)$-EPDF
109	2	54	$(109, 54, 26, 27)$-PDS	6	18	$(109, 3, 18, 8, 9)$-DPDF	$(109, 3, 18, 18)$-EDF
109	2	54	$(109, 54, 26, 27)$-PDS	12	9	$(109, 6, 9, 4)$-DDF	$(109, 6, 9, 22, 23)$-EPDF
109	2	54	$(109, 54, 26, 27)$-PDS	18	6	$(109, 9, 6, 2, 3)$-DPDF	$(109, 6, 9, 24)$-EDF
109	2	54	$(109, 54, 26, 27)$-PDS	36	3	$(109, 18, 3, 0, 2)$-DPDF	$(109, 18, 3, 26, 25)$-EPDF
109	2	54	$(109, 54, 26, 27)$-PDS	54	2	$(109, 27, 2, 0, 1)$-DPDF	$(109, 27, 2, 26)$-EDF
113	2	56	$(113, 56, 27, 28)$-PDS	4	28	$(113, 2, 28, 15, 12)$-DPDF	$(113, 2, 28, 12, 16)$-EPDF
113	2	56	$(113, 56, 27, 28)$-PDS	8	14	$(113, 4, 14, 5, 8)$-DPDF	$(113, 2, 28, 22, 20)$-EPDF
113	2	56	$(113, 56, 27, 28)$-PDS	14	8	$(113, 7, 8, 3, 4)$-DPDF	$(113, 7, 8, 24)$-EDF
113	2	56	$(113, 56, 27, 28)$-PDS	16	7	$(113, 8, 7, 2, 4)$-DPDF	$(113, 8, 7, 25, 24)$-EPDF
113	2	56	$(113, 56, 27, 28)$-PDS	28	4	$(113, 14, 4, 3, 0)$-DPDF	$(113, 14, 4, 24, 28)$-EPDF
113	2	56	$(113, 56, 27, 28)$-PDS	56	2	$(113, 28, 2, 1, 0)$-DPDF	$(113, 28, 2, 26, 28)$-EPDF
121	2	60	$(121, 60, 29, 30)$-PDS	4	30	$(121, 2, 30, 17, 12)$-DPDF	$(121, 2, 30, 12, 18)$-EPDF

q	ϵ	ρ	PDS Parameters	e	f	DPDF Parameters	EPDF Parameters
121	2	60	$(121, 60, 29, 30)$-PDS	6	20	$(121, 3, 20, 13, 6)$-DPDF	$(121, 3, 20, 16, 24)$-EPDF
121	2	60	$(121, 60, 29, 30)$-PDS	8	15	$(121, 4, 15, 10, 4)$-DPDF	$(121, 4, 15, 19, 26)$-EPDF
121	2	60	$(121, 60, 29, 30)$-PDS	10	12	$(121, 5, 12, 5, 6)$-DPDF	$(121, 5, 12, 24)$-EDF
121	2	60	$(121, 60, 29, 30)$-PDS	12	10	$(121, 6, 10, 9, 0)$-DPDF	$(121, 6, 10, 20, 30)$-EPDF
121	2	60	$(121, 60, 29, 30)$-PDS	20	6	$(121, 10, 6, 5, 0)$-DPDF	$(121, 10, 6, 24, 30)$-EPDF
121	2	60	$(121, 60, 29, 30)$-PDS	24	5	$(121, 12, 5, 4, 0)$-DPDF	$(121, 12, 5, 25, 30)$-EPDF
121	2	60	$(121, 60, 29, 30)$-PDS	30	4	$(121, 15, 4, 1, 2)$-DPDF	$(121, 15, 4, 28)$-EDF
121	2	60	$(121, 60, 29, 30)$-PDS	40	3	$(121, 20, 3, 2, 0)$-DPDF	$(121, 20, 3, 27, 30)$-EPDF
121	2	60	$(121, 60, 29, 30)$-PDS	60	2	$(121, 30, 2, 1, 0)$-DPDF	$(121, 30, 2, 28, 30)$-EPDF
121	3	40	$(121, 40, 15, 12)$-PDS	6	20	$(121, 2, 20, 11, 4)$-DPDF	$(121, 2, 20, 4, 8)$-EPDF
121	3	40	$(121, 40, 15, 12)$-PDS	12	10	$(121, 4, 10, 9, 0)$-DPDF	$(121, 4, 10, 6, 12)$-EPDF
121	3	40	$(121, 40, 15, 12)$-PDS	15	8	$(121, 5, 8, 3, 2)$-DPDF	$(121, 5, 8, 12, 10)$-EPDF
121	3	40	$(121, 40, 15, 12)$-PDS	24	5	$(121, 8, 5, 4, 0)$-DPDF	$(121, 8, 5, 11, 12)$-EPDF
121	3	40	$(121, 40, 15, 12)$-PDS	30	4	$(121, 10, 4, 3, 0)$-DPDF	$(121, 10, 4, 12)$-EDF
121	3	40	$(121, 40, 15, 12)$-PDS	60	2	$(121, 20, 2, 1, 0)$-DPDF	$(121, 20, 2, 14, 12)$-EPDF
121	4	30	$(121, 30, 11, 6)$-PDS	12	10	$(121, 3, 10, 9, 0)$-DPDF	$(121, 3, 10, 2, 6)$-EPDF
121	4	30	$(121, 30, 11, 6)$-PDS	24	5	$(121, 3, 10, 4, 0)$-DPDF	$(121, 3, 10, 7, 6)$-EPDF
121	4	30	$(121, 30, 11, 6)$-PDS	60	2	$(121, 15, 2, 1, 0)$-DPDF	$(121, 15, 2, 10, 6)$-EPDF
121	6	20	$(121, 20, 9, 2)$-PDS	12	10	$(121, 2, 10, 9, 0)$-DPDF	$(121, 2, 10, 0, 2)$-EPDF
121	6	20	$(121, 20, 9, 2)$-PDS	24	5	$(121, 4, 5, 4, 0)$-DPDF	$(121, 4, 5, 5, 2)$-EPDF
121	6	20	$(121, 20, 9, 2)$-PDS	60	2	$(121, 10, 2, 1, 0)$-DPDF	$(121, 10, 2, 8, 2)$-EPDF

Appendix C

Cyclotomic numbers of order 13 in the finite field GF(729)

In this Appendix, we have a table that presents the cyclotomic numbers of order 13 in the finite field GF(729). The purpose of this Appendix is to present these cyclotomic numbers in a more readable format. Note that for a particular cyclotomic number $(i, j)_e$, the number indexing the row of the table denotes the value of i and the number indexing the column of the table denotes the value of j.

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	7	6	4	6	4	4	4	2	2	6	4	2	4
1	6	4	6	4	1	2	5	2	6	4	8	2	6
2	4	6	2	2	2	6	6	6	6	5	5	2	4
3	6	4	2	4	8	5	6	2	2	4	6	6	1
4	4	1	2	8	6	4	5	4	6	6	2	6	2
5	4	2	6	5	4	2	6	6	2	6	2	6	5
6	4	5	6	6	5	6	2	2	6	2	4	6	2
7	2	2	6	2	4	6	2	4	5	6	2	6	5
8	2	6	6	2	6	2	6	5	4	2	6	5	4
9	6	4	5	4	6	6	2	6	2	4	1	2	8
10	4	8	5	6	2	2	4	2	6	1	6	4	2
11	2	2	2	6	6	6	6	6	5	2	4	4	6
12	4	6	4	1	2	5	2	5	4	8	2	6	6

Appendix D

Cyclotomic number calculations in GF(729)

In this Appendix, we run through the full proof that $D_0^{13,6} = C_0^{13,6} \cup C_4^{13,6} \cup C_{10}^{13,6} \cup C_{12}^{13,6} \subseteq \mathrm{GF}(729)$ is a $(729, 225, 63, 72)$-PDS.

In Lemma 4.2.3, we determined the following expression for the multiset $\Delta(D_0^{13,6})$

$$\begin{aligned}\Delta(D_0^{13,6}) = \bigcup_{r=0}^{12} \sum_{l \in I} ((r,l)_{13} + (r-4, l-4)_{13} + (r-10, l-10)_{13} +\\ (r-12, l-12)_{13}) C_r^{13,6} \cup 2(S_0^{13,6}) - 224\{0\}.\end{aligned}$$

We may write this as

$$\begin{aligned}\Delta(D_0^{13,6}) = \bigcup_{r=0}^{12} ((r,0)_{13} + (r-4,9)_{13} + (r-10,3)_{13} + (r-12,1)_{13}\\ +(r,4)_{13} + (r-4,0)_{13} + (r-10,7)_{13} + (r-12,5)_{13}\\ +(r,10)_{13} + (r-4,6)_{13} + (r-10,0)_{13} + (r-12,11)_{13}\\ +(r,12)_{13} + (r-4,8)_{13} + (r-10,2)_{13} + (r-12,0)_{13}) C_r^{13,6}\\ +2(C_0^{13,6} \cup C_4^{13,6} \cup C_{10}^{13,6} \cup C_{12}^{13,6}) - 224\{0\}.\end{aligned}$$

We now write this expression out in full.

$$\begin{aligned}
\Delta(D_0^{13,6}) = {} & ((0,0)_{13} + (9,9)_{13} + (3,3)_{13} + (1,1)_{13} + (0,4)_{13} + (9,0)_{13} \\
& +(3,7)_{13} + (1,5)_{13} + (0,10)_{13} + (9,6)_{13} + (3,0)_{13} + (1,11)_{13} \\
& +(0,12)_{13} + (9,8)_{13} + (3,2)_{13} + (1,0)_{13} + 2)C_0^{13,6} \\
& \cup((1,0)_{13} + (10,9)_{13} + (4,3)_{13} + (2,1)_{13} + (1,4)_{13} + (10,0)_{13} \\
& +(4,7)_{13} + (2,5)_{13} + (1,10)_{13} + (10,6)_{13} + (4,0)_{13} + (2,11)_{13} \\
& +(1,12)_{13} + (10,8)_{13} + (4,2)_{13} + (2,0)_{13})C_1^{13,6} \\
& \cup((2,0)_{13} + (11,9)_{13} + (5,3)_{13} + (3,1)_{13} + (2,4)_{13} + (11,0)_{13} \\
& +(5,7)_{13} + (3,5)_{13} + (2,10)_{13} + (11,6)_{13} + (5,0)_{13} + (3,11)_{13} \\
& +(2,12)_{13} + (11,8)_{13} + (5,2)_{13} + (3,0)_{13})C_2^{13,6} \\
& \cup((3,0)_{13} + (12,9)_{13} + (6,3)_{13} + (4,1)_{13} + (3,4)_{13} + (12,0)_{13} \\
& +(6,7)_{13} + (4,5)_{13} + (3,10)_{13} + (12,6)_{13} + (6,0)_{13} + (4,11)_{13} \\
& +(3,12)_{13} + (12,8)_{13} + (6,2)_{13} + (4,0)_{13})C_3^{13,6} \\
& \cup((4,0)_{13} + (0,9)_{13} + (7,3)_{13} + (5,1)_{13} + (4,4)_{13} + (0,0)_{13} \\
& +(7,7)_{13} + (5,5)_{13} + (4,10)_{13} + (0,6)_{13} + (7,0)_{13} + (5,11)_{13} \\
& +(4,12)_{13} + (0,8)_{13} + (7,2)_{13} + (5,0)_{13} + 2)C_4^{13,6} \\
& \cup((5,0)_{13} + (1,9)_{13} + (8,3)_{13} + (6,1)_{13} + (5,4)_{13} + (1,0)_{13} \\
& +(8,7)_{13} + (6,5)_{13} + (5,10)_{13} + (1,6)_{13} + (8,0)_{13} + (6,11)_{13} \\
& +(5,12)_{13} + (1,8)_{13} + (8,2)_{13} + (6,0)_{13})C_5^{13,6} \\
& \cup((6,0)_{13} + (2,9)_{13} + (9,3)_{13} + (7,1)_{13} + (6,4)_{13} + (2,0)_{13} \\
& +(9,7)_{13} + (7,5)_{13} + (6,10)_{13} + (2,6)_{13} + (9,0)_{13} + (7,11)_{13} \\
& +(6,12)_{13} + (2,8)_{13} + (9,2)_{13} + (7,0)_{13})C_6^{13,6} \\
& \cup((7,0)_{13} + (3,9)_{13} + (10,3)_{13} + (8,1)_{13} + (7,4)_{13} + (3,0)_{13} \\
& +(10,7)_{13} + (8,5)_{13} + (7,10)_{13} + (3,6)_{13} + (10,0)_{13} + (8,11)_{13} \\
& +(7,12)_{13} + (3,8)_{13} + (10,2)_{13} + (8,0)_{13})C_7^{13,6} \\
& \cup((8,0)_{13} + (4,9)_{13} + (11,3)_{13} + (9,1)_{13} + (8,4)_{13} + (4,0)_{13} \\
& +(11,7)_{13} + (9,5)_{13} + (8,10)_{13} + (4,6)_{13} + (11,0)_{13} + (9,11)_{13} \\
& +(8,12)_{13} + (4,8)_{13} + (11,2)_{13} + (9,0)_{13})C_8^{13,6}
\end{aligned}$$

$$\begin{aligned}
&\cup((9,0)_{13}+(5,9)_{13}+(12,3)_{13}+(10,1)_{13}+(9,4)_{13}+(5,0)_{13}\\
&+(12,7)_{13}+(10,5)_{13}+(9,10)_{13}+(5,6)_{13}+(12,0)_{13}+(10,11)_{13}\\
&+(9,12)_{13}+(5,8)_{13}+(12,2)_{13}+(10,0)_{13})C_{9}^{13,6}\\
&\cup((10,0)_{13}+(6,9)_{13}+(0,3)_{13}+(11,1)_{13}+(10,4)_{13}+(6,0)_{13}\\
&+(0,7)_{13}+(11,5)_{13}+(10,10)_{13}+(6,6)_{13}+(0,0)_{13}+(11,11)_{13}\\
&+(10,12)_{13}+(6,8)_{13}+(0,2)_{13}+(11,0)_{13}+2)C_{10}^{13,6}\\
&\cup((11,0)_{13}+(7,9)_{13}+(1,3)_{13}+(12,1)_{13}+(11,4)_{13}+(7,0)_{13}\\
&+(1,7)_{13}+(12,5)_{13}+(11,10)_{13}+(7,6)_{13}+(1,0)_{13}+(12,11)_{13}\\
&+(11,12)_{13}+(7,8)_{13}+(1,2)_{13}+(12,0)_{13})C_{11}^{13,6}\\
&\cup((12,0)_{13}+(8,9)_{13}+(2,3)_{13}+(0,1)_{13}+(12,4)_{13}+(8,0)_{13}\\
&+(2,7)_{13}+(0,5)_{13}+(12,10)_{13}+(8,6)_{13}+(2,0)_{13}+(0,11)_{13}\\
&+(12,12)_{13}+(8,8)_{13}+(2,2)_{13}+(0,0)_{13}+2)C_{12}^{13,6}-224\{0\}.
\end{aligned}$$

By then substituting in the individual cyclotomic number values obtained in Propositions 4.2.6 and 4.2.9, we see that

$$\begin{aligned}
\Delta(D_0^{13,6}) &= 63(C_0^{13,6})\cup 72(C_1^{13,6})\cup 72(C_2^{13,6})\cup 72(C_3^{13,6})\cup 63(C_4^{13,6})\cup 72(C_5^{13,6})\\
&\cup 72(C_6^{13,6})\cup 72(C_7^{13,6})\cup 72(C_8^{13,6})\cup 72(C_9^{13,6})\cup 63(C_{10}^{13,6})\cup\ 72(C_{11}^{13,6})\cup 63(C_{12}^{13,6})\\
&-224\{0\}.
\end{aligned}$$

And so $D_0^{13,6}$ is a $(729,225,63,72)$-PDS. What is particular interesting about this result is that, while all elements of $D_0^{13,6}$ occur 63 times in the multiset $\Delta(D_0^{13,6})$, and all elements in $\mathrm{GF}(729)^*\backslash D_0^{13,6}$ occur 72 times, there seem to be no obvious relations between the cyclotomic number expressions for the different cyclotomic classes contained in $D_0^{13,6}$. For example, it is clear from the above calculations that there are

$$\begin{aligned}
&(0,0)_{13}+(9,9)_{13}+(3,3)_{13}+(1,1)_{13}+(0,4)_{13}+(9,0)_{13}+(3,7)_{13}+(1,5)_{13}+(0,10)_{13}\\
&+(9,6)_{13}+(3,0)_{13}+(1,11)_{13}+(0,12)_{13}+(9,8)_{13}+(3,2)_{13}+(1,0)_{13}+2=63
\end{aligned}$$

copies of each element of $C_0^{13,6}$ in the multiset $\Delta(D_0^{13,6})$. Notice that in this expression for the number of copies of $C_0^{13,6}$ there is 1 element from $\mathrm{Orb}_{\mathfrak{R}}(0,0)_{13}$, there are 6 elements from $\mathrm{Orb}_{\mathfrak{R}}(1,1)_{13}$, there 3 elements from $\mathrm{Orb}_{\mathfrak{R}}(4,4)_{13}$ and 6 elements from the orbit $\mathrm{Orb}_{\mathfrak{R}}(2,3)_{13}$.

If we repeat this same process for $C_4^{13,6}$, it follows from the above calculations that there are

$$(4,0)_{13}+(0,9)_{13}+(7,3)_{13}+(5,1)_{13}+(4,4)_{13}+(0,0)_{13}+(7,7)_{13}+(5,5)_{13}+(4,10)_{13}$$
$$+(0,6)_{13}+(7,0)_{13}+(5,11)_{13}+(4,12)_{13}+(0,8)_{13}+(7,2)_{13}+(5,0)_{13}+2=63$$

copies of each element of $C_4^{13,6}$ in the multiset $\Delta(D_0^{13,6})$. Notice that in this expression for the number of copies of $C_4^{13,6}$ there is 1 element from $\mathrm{Orb}_{\mathfrak{R}}(0,0)_{13}$, there is 1 element from $\mathrm{Orb}_{\mathfrak{R}}(4,4)_{13}$, there are 2 elements from $\mathrm{Orb}_{\mathfrak{R}}(4,4)_{13}$, there are 3 elements from $\mathrm{Orb}_{\mathfrak{R}}(2,2)_{13}$, there are 3 elements from $\mathrm{Orb}_{\mathfrak{R}}(7,7)_{13}$, there are 2 elements from $\mathrm{Orb}_{\mathfrak{R}}(6,8)_{13}$ and there are 4 elements from $\mathrm{Orb}_{\mathfrak{R}}(2,3)_{13}$.

As these cyclotomic number expressions contain elements from distinct orbits, there is no obvious mapping from the expression for the number of copies of $C_0^{13,6}$ in $\Delta(D_0)^{13,6}$ and the number of copies of $C_4^{13,6}$ in $\Delta(D_0)^{13,6}$. Therefore cyclotomy does not give us the full picture of the underlying behaviour.