INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.
Composition codes and designs

Narayani, Lakshmi V. R., Ph.D.

The Ohio State University, 1992
COMPOSITION CODES AND DESIGNS

DISSERTATION

Presented in Partial Fulfillment of the Requirements for
the Degree Doctor of Philosophy in the Graduate
School of The Ohio State University

By

Lakshmi Narayani, M.S.,

* * * * *

The Ohio State University

1992

Dissertation Committee:
Prof. Dijen K. Ray-Chaudhuri
Prof. Thomas A. Dowling
Prof. G. Neil Robertson

Approved by

Adviser
Department of Mathematics
ACKNOWLEDGEMENTS

I would like to thank my advisor Professor Dijen K. Ray-Chaudhuri for his help and guidance in writing this dissertation. My thanks are also due to the reading committee members Professor Thomas A. Dowling and Professor G. Neil Robertson.

Finally, I want to thank Dr. John L. Blanchard for his help with \LaTeX{} and his support throughout.
VITA

May 15, 1959 ............ Born in Pollachi, India.

1979 ..................... B.Sc., Madras University, India.

1981 ..................... M.Sc., Department of Mathematics,
                        Punjab University, Chandigarh, India.

1982-1992 ............... Graduate Teaching Associate,
                        Department of Mathematics,
                        The Ohio State University,
                        Columbus, Ohio.

1987 ..................... M.S., Graduate School,
                        Department of Mathematics,
                        The Ohio State University,
                        Columbus, Ohio.

FIELDS OF STUDY

Major Field: Mathematics
# Table of Contents

ACKNOWLEDGEMENTS .......................................................... ii

VITA ................................................................................................ iii

CHAPTER PAGE

I  Introduction ........................................................................ 1

II  A Composition of Codes .................................................... 4
   2.1 Preliminaries ................................................................. 4
   2.2 A Composition of Binary Codes ..................................... 7
      2.2.1 Cyclicity of the Composition Code ...................... 18
      2.2.2 The Dual of the Composition Code ...................... 31
      2.2.3 The Weight Enumerator of the Composition Code .... 35
      2.2.4 Iterated Composition ........................................... 37
   2.3 A Composition of Codes over an Arbitrary Finite Field ..... 40
      2.3.1 Minimum distance of the Composition ................. 45
      2.3.2 The Cyclicity of the Composition ....................... 46
      2.3.3 The Dual code of the Composition ...................... 51
      2.3.4 Complete Weight Enumerator for the Composition Code . 53
      2.3.5 Decoding and Complexity ................................. 57
   2.4 A More General Composition ....................................... 59

III Applications of Composition Codes ................................... 63
   3.1 Introduction .............................................................. 63
      3.1.1 Preliminaries ....................................................... 63
   3.2 A Generalization of Quadratic Residue Codes ............... 66
      3.2.1 The Dual and the Extended Codes of Generalized Quadratic Residue Codes ......................... 78
CHAPTER I

Introduction

Given a class of objects, a composition is a way of combining objects of that class to produce another object of the same class. This dissertation presents a composition that applies, with suitable adaptations, to the class of linear codes, the class of $t$-designs, and the class of difference families.

In Chapter 2, we define a composition of two linear codes. This composition is somewhat similar to the direct product of codes given in MacWilliams & Sloane [9] using the Kronecker product of matrices. The length, dimension, minimum distance and burst-error correction capability of a composition code are determined. Conditions for a composition code to be cyclic are given and the generator polynomial of a composition code is given in terms of the generator polynomials of the component codes. The dual of a composition is found and a sufficient condition for a composition code to be self dual is given. The weight enumerator of a composition code is shown to be a (functional) composition of the weight enumerators of the component codes in the binary case. In the general case, the complete weight enumerator of a composition is shown to be a composition of the complete weight enumerators of the component codes. For binary codes, the composition can be applied repeatedly and this composition is associative. We discuss some of the properties of these iterated
compositions. A decoding algorithm is given that has linear complexity in terms of the decoding complexity of the component codes. The burst-error capability of composition codes and burst-error decoding is considered.

In Chapter 3, we give a generalization of quadratic residue codes to prime power block length and find their dual and extended codes. These codes have properties similar to standard quadratic residue codes [9] but their minimum distances do not satisfy the square root bound. Some of the extended codes are self dual. This family of generalized quadratic residue codes is invariant under the composition of codes defined in Chapter 2 and can be obtained by iterated composition of appropriate quadratic residue codes of prime length. Consequently, all the results in Chapter 2 for composition codes can be applied to the generalized quadratic residue codes. In the binary case, these codes are a subclass of the Duadic codes given by Pless, et.al [13].

In Chapter 4, a method is presented for constructing partially balanced designs from $t$-$(v, k, \lambda)$-designs. This construction is similar in spirit to the composition of codes. When the component designs satisfy a certain compatibility condition the result is a balanced design. Using this composition, some previously unknown 2-designs and an infinite family of 3-designs are constructed. Some of the 3-designs in this family are block transitive, point imprimitive and attain the bound $v \leq \binom{k}{2}$ given by Cameron & Praeger [14] for block transitive, point imprimitive designs.

In Chapter 5, the automorphism group of a composition design is shown to be a wreath product of the automorphism groups of the component designs.
In Chapter 6, it is shown that difference families can be composed in a similar way, and some theorems analogous to those for composition designs are given for composition difference families. Some new difference families obtained using this composition are presented. Finally, the multiplier group of a composition is shown to be a semi-direct product of the multiplier groups of the component difference families.
CHAPTER II

A Composition of Codes

2.1 Preliminaries

Let $F$ be a finite field and $F^n = F \times \cdots \times F$ be the Cartesian product of $F$ with itself $n$ times. Then $F^n$ is a vector space of dimension $n$ over $F$. The Hamming distance between two vectors $\overline{x} = (x_1, \ldots, x_n)$ and $\overline{y} = (y_1, \ldots, y_n)$ of $F^n$ is the number of coordinate places where they differ and is denoted by $d(\overline{x}, \overline{y})$. That is,

$$d(\overline{x}, \overline{y}) = |\{ i : x_i \neq y_i, 1 \leq i \leq n \}|.$$

**Definition 2.1.1** Let $S$ be a subset of $F^n$. Then, the **minimum distance** of $S$, denoted by $d(S)$, is

$$\min\{ d(\overline{x}, \overline{y}) : \overline{x}, \overline{y} \in S \text{ and } \overline{x} \neq \overline{y} \}.$$ 

**Definition 2.1.2** An $[n, k, d]$ linear code $C$ over $F$ is a subspace of $F^n$ of dimension $k$ and minimum distance $d$. 

If $C$ is an $[n, k, d]$ linear code over $F$, then $n$ is called the length of $C$. For $\overline{x} = (x_1, \ldots, x_n)$, its Hamming weight, denoted by $\text{wt}(\overline{x})$, is the number of nonzero coordinates of $\overline{x}$. Then the **minimum weight** of $C$ is the minimum of the
weights of its nonzero vectors. For a linear code, its minimum weight is the same as its minimum distance.

Let $C^0$ be the set of all even weight vectors in $C$ and $C^1$ the set of all odd weight vectors in $C$. For a binary code $C$, if $C^1$ is nonempty, then we have the following result.

**Lemma 2.1.3** If a binary linear code $C$ contains both even and odd weight vectors, then the number of even weight vectors in $C$ is the same as the number of odd weight vectors in $C$.

**Proof:** Since $C$ is binary, $C^0$ which is the set of even weight vectors in $C$ is a linear subcode of $C$. $C^1$ is nonempty, so we can find a vector $x$ in $C$ of odd weight. Then the coset $C^0 + x$ of $C^0$ consists of all the odd weight vectors in $C$. So $C = C^0 \cup (C^0 + x)$. Thus

$$|C^0| = \frac{|C|}{2} = |(C^0 + x)| = |C^1|$$

which proves the lemma.

**Definition 2.1.4** Let $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ be vectors in $F^n$. Then their scalar product is

$$x \cdot y = x_1y_1 + \cdots + x_ny_n.$$

If $x \cdot y = 0$, then $x$ and $y$ are called orthogonal.

**Definition 2.1.5** Let $C$ be an $[n, k]$ linear code over $F$. Then its dual or orthogonal code $C^\perp$ is the set of vectors which are orthogonal to all the codewords of $C$:

$$C^\perp = \{ x \mid x \in F^n \text{ and } x \cdot y = 0 \text{ for all } y \in C \}.$$
Then $C^1$ is an $[n, n-k]$ linear code over $F$.

**Definition 2.1.6** Let $v = (c_0, c_1, \ldots, c_{n-1})$ be a vector in $F^n$. Then, the vector $(c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ is called the cyclic shift of $v$. A linear code $C$ over a finite field $F$ is **cyclic** if for every codeword $(c_0, c_1, \ldots, c_{n-1})$ in $C$, its cyclic shift $(c_{n-1}, c_0, c_1, \ldots, c_{n-2})$ is also in $C$.

To get an algebraic description, we can associate with the vector $\bar{v} = (c_0, c_1, \ldots, c_{n-1})$ in $F^n$, the polynomial

$$\bar{v}(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1}.$$ 

Let $R_n$ be the quotient space $F[x]/\langle (x^n - 1) \rangle$. Then $R_n$ is a principal ideal ring. And, a code $C$ of length $n$ is cyclic iff it is an ideal of $R_n$. The following theorem from [9] gives some of the properties of $C$ if it is cyclic.

**Theorem 2.1.7** Let $C$ be a cyclic code of length $n$ over $F$. Then

(i) there is unique monic polynomial $g(x)$ of minimal degree in $C$,

(ii) $C = \langle g(x) \rangle$, i.e., $g(x)$ is a generating polynomial of $C$,

(iii) $g(x)$ is a factor of $x^n - 1$,

(iv) any $c(x) \in C$ can be written uniquely as $c(x) = f(x)g(x)$ in $F[x]$, where $f(x) \in F[x]$ has degree $< n - r$, $r = \deg g(x)$. The dimension of $C$ is $n - r$.

For an $[n, k]$ linear code $C$, let $A_i$ denote the number of codewords of weight $i$ in $C$.

**Definition 2.1.8** The polynomial

$$W_C(x, y) = \sum_{i=0}^{n} A_i x^i y^{n-i}$$
is called the weight enumerator of $C$.

### 2.2 A Composition of Binary Codes

Let $C_E$ be an $[n_E,k_E,d_E]$ binary linear code and $C_I$ an $[n_I,k_I,d_I]$ binary linear code.

We call $C_E$ an exterior code and $C_I$ an interior code.

Let $C_I^n$ be a subcode of $C_I$ of codimension one and let $C^n_I = C_I \setminus C_I^n$. Then

$$C_I = C_I^n \cup C_I^1 \text{ and } C_I^n \cap C_I^1 = \emptyset.$$  

We note that, if $a \in (C_I \setminus C_I^n)$, then $C_I^n = a + C_I^n$ and so $|C_I^n| = |C_I^1|$. Since $C_I^n$ is a subcode of $C_I$ of codimension one, $C_I^n$ has dimension $k_I - 1$. Thus

$$|C_I^1| = 2^{k_I-1} = \frac{|C_I|}{2} = |C_I^n|. \quad (2.1)$$

Using $C_I^n$ and $C_I^1$, we compose $C_E$ and $C_I$ as follows: Let $\bar{y} = (y_1,\ldots,y_{n_E})$ be a vector in $C_E$. Then, since $C_E$ is binary, $y_i = 0$ or 1. Pick $\{\bar{c}_i\}_{i=1}^{n_E}$, an ordered set with $\bar{c}_i$ from $C_I$ such that

$$\bar{c}_i = (c_{i1},\ldots,c_{in_I}) \in C_I^{n_I} \text{ for } i = 1,\ldots,n_E.$$  

Here $\bar{c}_i$'s need not be distinct. Then $\bar{c}_i$ is in $C_I^n$ or $C_I^1$ depending on whether $y_i$ is 0 or 1. We call such an ordered $n_E$-set of vectors from $C_I$ a suitable set of $\bar{y}$. We note that for a given $\bar{y}$ in $C_E$ there could be many $n_E$-sets in $C_I$ suitable to $\bar{y}$.

Since $\bar{c}_i$'s are binary vectors, we can use them to define a new binary vector.
**Definition 2.2.1** If \( \bar{y} \) is a vector in \( C_E \) and \( \{\bar{r}_i\}_{i=1}^{n_E} \) a suitable set of \( \bar{y} \) from \( C_I \), then the **composition** of \( \bar{y} \) and \( \{\bar{r}_i\}_{i=1}^{n_E} \) denoted by \( \bar{y} \circ \{\bar{r}_i\}_{i=1}^{n_E} \) is defined as

\[
\bar{y} \circ \{\bar{r}_i\}_{i=1}^{n_E} = (c_{11}, \ldots, c_{n_E 1}; \ldots; c_{1n_I}, \ldots, c_{n_E n_I}).
\] (2.2)

Then, for \( 1 \leq i \leq n_E \) and \( 1 \leq j \leq n_I \), the \( ij \)th coordinate of \( \bar{y} \circ \{\bar{r}_i\}_{i=1}^{n_E} \) is equal to \( c_{ij} \), which is the \( j \)th coordinate of \( \bar{r}_i \). This way, we can compose a vector \( \bar{y} = (y_1, \ldots, y_{n_E}) \) of \( C_E \) with any of its suitable set of vectors \( \{\bar{r}_i\}_{i=1}^{n_E} \) from \( C_I \).

**Definition 2.2.2** For a fixed \( \bar{y} \) in \( C_E \), \( \bar{y} \circ (C_I^o, C_I) \) is defined to be the set of all the compositions of \( \bar{y} \) with all the suitable \( n_E \)-sets of vectors in \( C_I \).

Then

\[
\bar{y} \circ (C_I^o, C_I) = \left\{ \bar{y} \circ \{\bar{r}_i\}_{i=1}^{n_E} : \{\bar{r}_i\}_{i=1}^{n_E} \subseteq C_I \text{ and } \{\bar{r}_i\}_{i=1}^{n_E} \text{ a suitable set of } \bar{y} \right\}.
\] (2.3)

We define the composition of \( C_E \) and \( C_I \) as the union of all the \( \bar{y} \circ (C_I^o, C_I) \) as \( \bar{y} \) varies through all the elements of \( C_E \).

**Definition 2.2.3** The composition \( C_E \circ (C_I^o, C_I) \) of the codes \( C_E \) and \( C_I \) denoted by \( C \) is defined as follows:

\[
C = C_E \circ (C_I^o, C_I)
\]

\[
= \left\{ (c_{11}, \ldots, c_{n_E 1}; \ldots; c_{1n_I}, \ldots, c_{n_E n_I}) : \{\bar{r}_i\}_{i=1}^{n_E} \subseteq C_I \right\}
\]

\[
\text{is a suitable set for some } \bar{y} \in C_E \text{ and } \bar{r}_i = (c_{i1}, \ldots, c_{i n_I}) \text{ for } i = 1, \ldots, n_E \}
\] (2.4)

\[
C = \bigcup_{\bar{y} \in C_E} \bar{y} \circ (C_I^o, C_I). \] (2.5)
Clearly $\bar{y} \circ \{\bar{c}_i\}_{i=1}^{n_{E}}$ is a binary vector of length $n_{E}n_{I}$. So, $\mathcal{C} = \mathcal{C}_{E} \circ (\mathcal{C}_{i}^{\alpha}, \mathcal{C}_{i}^{\beta})$ is a set of binary vectors of length $n_{E}n_{I}$. In this chapter, we will study the properties of $\mathcal{C}$ in relation to $\mathcal{C}_{E}$ and $\mathcal{C}_{I}$.

**Lemma 2.2.4** If $\bar{c} \in \mathcal{C}_{E} \circ (\mathcal{C}_{i}^{\alpha}, \mathcal{C}_{i}^{\beta})$, then $\bar{c}$ has a unique representation of the form $\bar{y} \circ \{\bar{c}_i\}_{i=1}^{n_{E}}$ where $\bar{y} = (y_1, \ldots, y_{n_{E}}) \in \mathcal{C}_{E}$ and $\bar{c}_i \in \mathcal{C}_{i}^{y_i}$ for $i = 1, \ldots, n_{E}$.

**Proof:** Let

$$\bar{c} = (c_{11}, c_{21}, \ldots, c_{n_{E}1}; c_{12}, c_{22}, \ldots, c_{n_{E}2}; c_{1n_{I}}, c_{2n_{I}}, \ldots, c_{n_{E}n_{I}})$$

be an element of $\mathcal{C}$. Then $\bar{c} = \bar{y} \circ \{\bar{c}_i\}_{i=1}^{n_{E}}$ where $\bar{c}_i = (c_{i1}, c_{i2}, \ldots, c_{in_{I}})$ and

$$\bar{y} = (y_1, \ldots, y_{n_{E}})$$

with

$$y_i = \begin{cases} 0, & \text{if } \bar{c}_i \in \mathcal{C}_{i}^{0} \\ 1, & \text{if } \bar{c}_i \in \mathcal{C}_{i}^{1}. \end{cases}$$

Thus, for $i = 1, \ldots, n_{E}$, $\bar{c}_i$ and $y_i$ are uniquely determined for a given $\bar{c}$ in $\mathcal{C}$. From the definition of the composition $\bar{y} \in \mathcal{C}_{E}$; otherwise $\bar{c} \not\in \mathcal{C}$. Hence $\bar{c}$ has a unique representation of the form $\bar{y} \circ \{\bar{c}_i\}_{i=1}^{n_{E}}$ in $\mathcal{C}$. \qed

**Definition 2.2.5** For $\alpha, \beta \in F_2$, the sum of any two cosets $\mathcal{C}_{i}^{\alpha}, \mathcal{C}_{i}^{\beta}$ of $\mathcal{C}_{i}$ is defined as follows:

$$\mathcal{C}_{i}^{\alpha} + \mathcal{C}_{i}^{\beta} = \{ \bar{x} + \bar{y} : \bar{x} \in \mathcal{C}_{i}^{\alpha} \text{ and } \bar{y} \in \mathcal{C}_{i}^{\beta} \}.$$

**Lemma 2.2.6** Let $\alpha, \beta \in F_2$. Then

$$\mathcal{C}_{i}^{\alpha} + \mathcal{C}_{i}^{\beta} = \mathcal{C}_{i}^{\alpha+\beta}.$$
Proof: If \( \alpha = \beta = 0 \), then

\[
C_j^\alpha + C_j^\beta = C_j^\alpha + C_j^\alpha = C_j^\alpha = C_j^{\alpha + \beta}.
\]

For \( \bar{a} \notin C_i^\alpha \), \( \bar{a} + C_i^\alpha = C_i^\alpha \). So, if \( \alpha \neq \beta \), then

\[
C_i^\alpha + C_i^\beta = C_i^\alpha + C_i^\alpha = C_i^\alpha = C_i^{\alpha + \beta}.
\]

If \( \bar{a}, \bar{b} \in C_i^\alpha \), then \( C_i^\alpha = \bar{a} + C_i^\alpha = \bar{b} + C_i^\alpha \) and so \( \bar{a} + \bar{b} \in C_i^\alpha \). Thus, if \( \alpha = \beta = 1 \), then

\[
C_i^\alpha + C_i^\beta = C_i^\alpha + C_i^\alpha = C_i^\alpha = C_i^{\alpha + \beta}
\]

which proves the lemma. \( \square \)

**Theorem 2.2.7** If \( C_E \) and \( C_I \) are binary linear codes, then the composition \( C = C_E \circ (C_I, C_I) \) is also a binary linear code.

Proof: Clearly \( C \) is binary. To show that \( C = C_E \circ (C_I, C_I) \) is a linear code, let

\[
\bar{y} \circ \{\bar{c}_i\}_{i=1}^{n_E} = (c_{11}, \ldots, c_{n_E1}; \ldots; c_{1n_I}, \ldots, c_{n_En_I}) \tag{2.6}
\]

and

\[
\bar{y}' \circ \{\bar{c}'_i\}_{i=1}^{n_E} = (c'_{11}, \ldots, c'_{n_E1}; \ldots; c'_{1n_I}, \ldots, c'_{n_En_I}) \tag{2.7}
\]

be two vectors in \( C \) where \( \bar{y}, \bar{y}' \) are in \( C_E \) and \( \{\bar{c}_i\}_{i=1}^{n_E}, \{\bar{c}'_i\}_{i=1}^{n_E} \) subsets of \( C_I \) suitable to \( \bar{y}, \bar{y}' \). Let

\[
\bar{y} = (y_1, \ldots, y_{n_E}) \quad \text{and} \quad \bar{y}' = (y'_1, \ldots, y'_{n_E}).
\]
Since $C_E$, $C_I$ are linear, $\bar{y} + y'$ is in $C_E$ and $(\bar{c}_i + c'_i)_{i=1}^{n_E}$ is contained in $C_I$. We have

$$
\begin{align*}
(\bar{y} \circ \{\bar{c}_i\}_{i=1}^{n_E}) + (\bar{y}' \circ \{\bar{c}'_i\}_{i=1}^{n_E}) &= (c_{11}, \ldots, c_{n_E1}; \ldots; c_{1n_I}, \ldots, c_{n_En_I}) + (c'_{11}, \ldots, c'_{n_E1}; \ldots; c'_{1n_I}, \ldots, c'_{n_En_I}) \\
&= (c_{11} + c'_{11}, \ldots, c_{n_E1} + c'_{n_E1}; \ldots; c_{1n_I} + c'_{1n_I}, \ldots, c_{n_En_I} + c'_{n_En_I}).
\end{align*}
$$
\tag{2.8}

We claim that

$$
(\bar{y} \circ \{\bar{c}_i\}_{i=1}^{n_E}) + (\bar{y}' \circ \{\bar{c}'_i\}_{i=1}^{n_E}) = (\bar{y} + y') \circ \{\bar{c}_i + c'_i\}_{i=1}^{n_E}.
$$

To prove that, we do the following: Since $\{\bar{c}_i\}_{i=1}^{n_E}$ and $\{\bar{c}'_i\}_{i=1}^{n_E}$ are suitable sets of $\bar{y}$ and $\bar{y}'$ respectively, we have $\bar{c}_i \in C_I^{y_i}$ and $\bar{c}'_i \in C_I^{y_i'}$ for $i = 1, \ldots, n_E$. And since $c_i \in C_I$ or $C_I'$, and $c'_i \in C_I$ or $C_I'$, from Lemma 2.2.6, we get

$$
C_I^{y_i} + C_I^{y_i'} = C_I^{y_i + y_i'}.
$$

But $\bar{c}_i \in C_I^{y_i}$, $\bar{c}'_i \in C_I^{y_i'}$ and so

$$
\bar{c}_i + \bar{c}'_i \in C_I^{y_i} + C_I^{y_i'} = C_I^{y_i + y_i'}
$$

for $i = 1, \ldots, n_E$. Thus, $\{\bar{c}_i + \bar{c}'_i\}_{i=1}^{n_E}$ is a suitable set of $\bar{y} + \bar{y}' = (y_1 + y_1', \ldots, y_n + y_{n_E'})$ from $C_I$. And since $\bar{y} + \bar{y}'$ is in $C_E$, we get $(\bar{y} + \bar{y}') \circ \{\bar{c}_i + \bar{c}'_i\}_{i=1}^{n_E}$ is in $C$. Also

$$
(\bar{y} + \bar{y}') \circ \{\bar{c}_i + \bar{c}'_i\}_{i=1}^{n_E} \\
= (c_{11} + c'_{11}, \ldots, c_{n_E1} + c'_{n_E1}; \ldots; c_{1n_I} + c'_{1n_I}, \ldots, c_{n_En_I} + c'_{n_En_I}) \\
= (\bar{y} \circ \{\bar{c}_i\}_{i=1}^{n_E}) + (\bar{y}' \circ \{\bar{c}'_i\}_{i=1}^{n_E})
$$
\tag{2.9}
using (2.8), which proves our claim. Therefore \( \bar{y} \circ \{ \bar{c}_i \}_{i=1}^{n_E} + \bar{y}' \circ \{ \bar{c}'_i \}_{i=1}^{n_E} \) is in \( C \). This shows that \( C \) is closed under addition. Since \( C \) is binary and contains the zero vector, it is also closed under scalar multiplication and hence \( C \) is a binary linear code. \( \square \)

Clearly the length of \( C \) is \( n_E n_i \). Next we find the dimension of \( C = C_E \circ (C_i^o, C_i) \).

For that, we first count the number of elements in \( C \). Since \( C = \bigcup_{\bar{y} \in C_h} \bar{y} \circ (C_i^o, C_i) \), we start by counting the number of elements in \( \bar{y} \circ (C_i^o, C_i) \). Let \( |\bar{y} \circ (C_i^o, C_i)| \) stand for the number of elements in \( \bar{y} \circ (C_i^o, C_i) \).

**Lemma 2.2.8** \( |\bar{y} \circ (C_i^o, C_i)| \) is \((|C_i|/2)^{n_E}\).

**Proof:** From (2.3),

\[
\bar{y} \circ (C_i^o, C_i) = \left\{ \bar{y} \circ \{ \bar{c}_i \}_{i=1}^{n_E} : \{ \bar{c}_i \}_{i=1}^{n_E} \subseteq C_i \quad \text{and} \quad \{ \bar{c}_i \}_{i=1}^{n_E} \quad \text{a suitable set of } \bar{y} \right\}.
\]

Suppose \( \{ \bar{c}_i \}_{i=1}^{n_E} \) and \( \{ \bar{c}'_i \}_{i=1}^{n_E} \) are two distinct suitable sets of \( \bar{y} \) from \( C_i \). Then, \( \bar{c}_i \neq \bar{c}'_i \) for some \( i \) in \( \{1, \ldots, n_E\} \). Then, for some \( j \) in \( \{1, \ldots, n_i\} \), the \( j \)th coordinates \( c_{ij} \) and \( c'_{ij} \) of \( \bar{c}_i \) and \( \bar{c}'_i \) are not equal. Since \( c_{ij} \) and \( c'_{ij} \) are also the \( ij \)th coordinates of \( \bar{y} \circ \{ \bar{c}_i \}_{i=1}^{n_E} \) and \( \bar{y} \circ \{ \bar{c}'_i \}_{i=1}^{n_E} \) respectively, we get

\[
\bar{y} \circ \{ \bar{c}_i \}_{i=1}^{n_E} \neq \bar{y} \circ \{ \bar{c}'_i \}_{i=1}^{n_E}.
\]

So the size of \( \bar{y} \circ (C_i^o, C_i) \) is same as the number of suitable sets of \( \bar{y} \) contained in \( C_i \).

A set \( \{ \bar{c}_i \}_{i=1}^{n_E} \) is suitable to \( \bar{y} \) iff \( \bar{c}_i \in C_i^{y_i} \) where \( y_i = (y_1, \ldots, y_{n_E}) \). So for a fixed \( \bar{y} \), \( \bar{c}_i \) in its suitable set \( \{ \bar{c}_i \}_{i=1}^{n_E} \) has \( |C_i^{y_i}| \) choices in \( C_i \). Now

\[
C_i^{y_i} = C_i^o \quad \text{or} \quad C_i^1
\]
and from (2.1),

\[ |\mathcal{C}_j^n| = |\mathcal{C}_j^*| = \frac{|\mathcal{C}_I|}{2}. \]

So each \( \overline{c}_i \) in a suitable set \( \{\overline{c}_i\}_{i=1}^{n_E} \) of \( \overline{y} \) has \( |\mathcal{C}_I|/2 \) choices from \( \mathcal{C}_I \). Since \( \overline{c}_i \) in \( \{\overline{c}_i\}_{i=1}^{n_E} \) are chosen independent of each other, there are \( (|\mathcal{C}_I|/2)^{n_E} \) suitable sets \( \{\overline{c}_i\}_{i=1}^{n_E} \) of \( \overline{y} \).

Thus

\[ |\overline{y} \circ (\mathcal{C}_j^n, \mathcal{C}_I)| = \left( \frac{|\mathcal{C}_I|}{2} \right)^{n_E} \quad (2.10) \]

which proves the lemma. \( \square \)

We note that \( |\overline{y} \circ (\mathcal{C}_j^n, \mathcal{C}_I)| \) is independent of \( \overline{y} \).

**Lemma 2.2.9** If \( \overline{y} \neq \overline{y}' \) are two vectors of \( \mathcal{C}_E \), then \( \overline{y} \circ (\mathcal{C}_j^n, \mathcal{C}_I) \) and \( \overline{y}' \circ (\mathcal{C}_j^n, \mathcal{C}_I) \) are disjoint.

**Proof:** To prove our claim, let \( \{\overline{c}_i\}_{i=1}^{n_E} \) and \( \{\overline{c}'_i\}_{i=1}^{n_E} \) be two suitable sets of \( \overline{y} \) and \( \overline{y}' \). Since \( \overline{y} \neq \overline{y}' \), there is a \( j \) in \( \{1, \ldots, n_E\} \) such that \( y_j \neq y'_j \) where \( \overline{y} = (y_1, \ldots, y_{n_E}) \) and \( \overline{y}' = (y'_1, \ldots, y'_{n_E}) \). Say \( y_j = 0 \). Then \( y'_j = 1 \). That means, in \( \{\overline{c}_i\}_{i=1}^{n_E} \)

\[ \overline{c}_j \in \mathcal{C}_j^{n_E} = \mathcal{C}_j^n \]

and in \( \{\overline{c}'_i\}_{i=1}^{n_E} \)

\[ \overline{c}'_j \in \mathcal{C}_j^{n_E} = \mathcal{C}_j^* \]

But \( \mathcal{C}_j^n \) and \( \mathcal{C}_j^* \) are disjoint subsets of \( \mathcal{C}_I \), so \( \overline{c}_j \neq \overline{c}'_j \). This gives

\[ \overline{y} \circ \{\overline{c}_i\}_{i=1}^{n_E} \neq \overline{y}' \circ \{\overline{c}'_i\}_{i=1}^{n_E} \]

if \( \overline{y} \neq \overline{y}' \). Hence

\[ (\overline{y} \circ (\mathcal{C}_j^n, \mathcal{C}_I)) \cap (\overline{y}' \circ (\mathcal{C}_j^n, \mathcal{C}_I)) = \emptyset \]
Theorem 2.2.10  If $C_E$ is an $[n_E, k_E]$ binary linear code and $C_I$ is an $[n_I, k_I]$ binary linear code, then $C = C_E \circ (C_I^o, C_I)$ is an $[n, k]$ binary linear code where $n = n_E n_I$ and $k = (k_I - 1) n_E + k_E$.

Proof: We just need to show that the dimension of $C$ is

$$k = (k_I - 1) n_E + k_E.$$

First we show that

$$|C| = 2^{(k_I - 1) n_E + k_E}.$$

From Lemma (2.2.9), $C = \bigcup_{\tilde{y} \in C_E} \tilde{y} \circ (C_I^o, C_I)$ is a disjoint union of $\tilde{y} \circ (C_I^o, C_I)$'s.

Therefore

$$|C| = \sum_{\tilde{y} \in C_E} |\tilde{y} \circ (C_I^o, C_I)|. \quad (2.11)$$

Since $C_E$ is an $[n_E, k_E]$ binary linear code and $C_I$ is an $[n_I, k_I]$ binary linear code, $|C_E| = 2^{k_E}$ and $|C_I| = 2^{k_I}$. Using this fact and Lemma 2.2.8, we get

$$|C| = \sum_{\tilde{y} \in C_E} \left( \frac{|C_I|}{2} \right)^{n_E} = |C_E| \left( \frac{|C_I|}{2} \right)^{n_E}$$

$$= 2^{k_E} \left( \frac{2^{k_I}}{2} \right)^{n_E} = 2^{k_E + n_E (k_I - 1)} \quad (2.12)$$

Thus, we have shown that $C$ is a binary linear code containing $2^{k_E + n_E (k_I - 1)}$ vectors.

So its dimension is $k = k_E + n_E (k_I - 1)$.

If $C_E$ is the zero space, then the composition uses only the vectors in $C_I^o$. So we
have the following theorem.

In the following, \( \vec{0} \) denotes the zero vector.

**Theorem 2.2.11** \hspace{1cm} If \( C_E = \{ \vec{0} \} \), then \( C_E \circ (C_I^o, C_I) = \{ \vec{0} \} \circ (C_I^o, C_I) \).

Let \( d_E, d_I, d_I^0 \) and \( d_I^1 \) be the minimum distance of \( C_E, C_I, C_I^o \) and \( C_I \) respectively. Then \( d_I = \min\{d_I^0, d_I^1\} \). Let \( \vec{u} \in C_I^o \) and \( \vec{v} \in C_I \) be such that \( \text{wt}(\vec{u}) = d_I^0 \), \( \text{wt}(\vec{v}) = d_I^1 \).

**Theorem 2.2.12** \hspace{1cm} The minimum distance of \( C = C_E \circ (C_I^o, C_I) \) is \( d \) where

\[
d = \begin{cases} 
  d_I^0, & \text{if } d_I = d_I^0, \\
  \min\{d_I^0, d_E d_I^1\}, & \text{if } d_I = d_I^1.
\end{cases} \tag{2.13}
\]

**Proof:** Let \( \vec{y} = (y_1, \ldots, y_{n_E}) \in C_E \) and \( \{\vec{e}_i\}_{i=1}^{n_E} \) be a suitable set of \( \vec{y} \) from \( C_I \). Then \( \vec{e}_i \in C_I^o \) and \( \vec{y} \circ \{\vec{e}_i\}_{i=1}^{n_E} \) is in \( C = C_E \circ (C_I^o, C_I) \). Also

\[
\text{wt}(\vec{y} \circ \{\vec{e}_i\}_{i=1}^{n_E}) = \sum_{i=1}^{n_E} \text{wt}(\vec{e}_i). \tag{2.14}
\]

If \( \vec{y} = \vec{0} \), then \( \{\vec{w}_i\}_{i=1}^{n_E} \) with

\[
\vec{w}_1 = \vec{u} \quad \text{and} \quad \vec{w}_i = \vec{0} \quad \text{for } i \geq 2,
\]

is a suitable set of \( \vec{y} = \vec{0} \) with

\[
\text{wt}(\vec{y} \circ \{\vec{w}_i\}_{i=1}^{n_E}) = d_I^0.
\]

Then

\[
\min \text{ wt}(\vec{0} \circ (C_I^o, C_I)) = \min \text{ wt}\{\vec{0} \circ \{\vec{e}_i\}_{i=1}^{n_E} : \vec{e}_i \in C_I^o\} = \min\{\text{wt}(\vec{0} \circ \{\vec{e}_i\}_{i=1}^{n_E}) : \vec{e}_i \in C_I^o\} = \min\{\sum_{i=1}^{n_E} \text{wt}(\vec{e}_i) : \vec{e}_i \in C_I^o\} = \sum_{i=1}^{n_E} \text{wt}(\vec{w}_i) = \text{wt}(\vec{u}) = d_I^0 \quad \text{ (2.15)}
\]
since \( \text{wt } \tilde{c}_i \geq \text{wt } \tilde{w}_i \) for \( i = 1, \ldots, n_E \). If \( \tilde{y} \neq \bar{o} \), then \( \{\tilde{w}_i\}_{i=1}^{n_E} \) with \( \tilde{w}_i = \bar{o} \) if \( y_i = 0 \) and \( \tilde{w}_i = \bar{v} \) if \( y_i = 1 \), is a suitable set of \( \tilde{y} \) with

\[
\text{wt}(\tilde{y} \circ \{\tilde{w}_i\}_{i=1}^{n_E}) = d_E d_l^1.
\]

Then, for \( \tilde{y} \neq \bar{o} \),

\[
\min \text{wt}(\tilde{y} \circ (C^o_l, C_l)) = \min \{\text{wt}(\tilde{y} \circ \{\tilde{c}_i\}_{i=1}^{n_E}) : \tilde{c}_i \in C^o_l \}
\]

\[
= \min \{\text{wt}(\tilde{y} \circ \{\tilde{c}_i\}_{i=1}^{n_E}) : \tilde{c}_i \in C^o_l \}
\]

\[
= \min \left\{ \sum_{i=1}^{n_E} \text{wt}(\tilde{c}_i) : \tilde{c}_i \in C^o_l \right\}
\]

\[
= \sum_{i=1}^{n_E} \text{wt}(\tilde{w}_i) = \text{wt}(\tilde{y})\text{wt}(\bar{v})
\]

\[
= \text{wt}(\tilde{y}).d_l^1 \geq d_E d_l^1
\]

since \( \text{wt } \tilde{c}_i \geq \text{wt } \tilde{w}_i \) for \( i = 1, \ldots, n_E \). So

\[
\min \text{wt}(C) = \min \left( \bigcup_{\tilde{y} \in C^o_E} \tilde{y} \circ (C^o_l, C_l) \right)
\]

\[
= \min\{d_l^0, d_E d_l^1\}
\]

(2.16)

\[
= \begin{cases} 
  d_l^0, & \text{if } d_l = d_l^0 \\
  \min\{d_l^0, d_E d_l^1\}, & \text{if } d_l = d_l^1
\end{cases}
\]

(2.17)

(2.18)

which gives the minimum distance of \( C \). \( \square \)

**Corollary 2.2.13** The minimum distance \( d \) of \( C_l \circ (C^o_l, C_l) \) is

\[
d = \begin{cases} 
  d_l^0, & \text{if } d_l = d_l^0 \\
  \min\{d_l^0, (d_l^1)^2\}, & \text{if } d_l = d_l^1
\end{cases}
\]
Definition 2.2.14  Given a set \( X \) of size \( n \), a \( t-(v,k,\lambda) \)-design is a family \( \mathcal{D} \) of \( k \)-sets of \( X \), called blocks, with the property that each set of \( t \) points of \( X \) is in exactly \( \lambda \) blocks. A design is called simple when there are no repeated blocks.

Theorem 2.2.15  If \( n_K > 1 \), \( d_i \geq 2 \) and \( C_j^o \) contains at least one vector of weight \( d_i \), then the set of minimum weight vectors in the composition code \( C = C_E \circ (C_j^o, C_I) \) is not a 2-design.

Proof:  Let

\[
\Lambda_i = \{ \vec{v} : \vec{v} \in C_j^o \text{ and } \text{wt}(\vec{v}) = d_i \}. \tag{2.19}
\]

Then \( \Lambda_i \) consists of all the minimum weight vectors in \( C_j^o \). In the following \( \vec{o} \) stands for the zero vector of appropriate length. Let

\[
\Lambda = \left\{ \vec{o} \circ \{ \vec{v}_i \}_{i=1}^{n_E} : \vec{v}_i \in C_j^o \text{ and } \vec{v}_{i'} \in \Lambda_i \text{ for some } 1 \leq i' \leq n_E \text{ and } \vec{v}_i = \vec{o} \text{ if } i \neq i' \right\}. \tag{2.20}
\]

Then from Theorem 2.2.12, \( \Lambda \) consists of all the minimum weight vectors in \( C = C_E \circ (C_j^o, C_I) \). To show \( \lambda_e \) is not a 2-design, pick \( s \) and \( t \) with \( 1 \leq s, t \leq n_K n_I \) and \( s \neq t \).

Case 1 \( s \neq t \) (mod \( n_K \)).

In this case no vector in \( \Lambda \) will have a nonzero entry in both \( s \) and \( t \) coordinate places.

So the number of vectors in \( \Lambda \) having a nonzero entry in both \( s \) and \( t \) coordinate places is zero in this case.

Case 2 \( s \equiv t \) (mod \( n_K \)).

Since \( C_j^o \) contains at least one vector of weight \( d_i \) and \( d_i \geq 2 \), from the description of
\[ \Lambda, \text{ we note that we can find at least one vector in } \Lambda \text{ with nonzero entries in the } s \text{ and } t \text{ coordinate places for some } s \equiv t (\text{mod } n_\ell). \]

From the above two cases, we conclude that \( \Lambda \) is never a 2-design. \( \square \)

### 2.2.1 Cyclicity of the Composition Code

Like before, we let \( C_E, C_I \) be binary linear codes and \( C_i^0 \) a subcode of \( C_I \) of codimension one. In this section, we analyze how the composition \( C = C_E \circ (C_i^0, C_I) \) being cyclic is related to the components \( C_E, C_I \) and \( C_i^0 \) being cyclic.

**Lemma 2.2.16**  Let \( C \) be an \([n, k]\) binary cyclic code of odd length \( n \). If \( C \) contains a cyclic subcode \( C^0 \) of codimension one, then \( C \) must contain both even and odd weight vectors and \( C^0 \) is the subcode of \( C \) consisting of all the even weight vectors in \( C \).

**Proof:**  Let \( R[x] = \frac{F_2[x]}{(x^n - 1)} \).

Since \( C \) is cyclic, there is a polynomial \( f(x) \in R[x] \) such that \( C = \langle f(x) \rangle \). Then \( \deg f(x) = n - k \). By assumption, \( C^0 \) is a subcode of codimension one and so it is an \([n, k - 1]\) code. Since \( C^0 \) is cyclic, \( C^0 = \langle g(x) \rangle \) for some \( g(x) \in R[x] \). Then

\[
\deg g(x) = n - (k - 1) = n - k + 1.
\]

We have \( C^0 \subset C \), and so \( f(x) \) divides \( g(x) \) in \( \frac{F_2[x]}{(x^n - 1)} \). This gives

\[
g(x) = (x - a)f(x)
\]  \( \quad (2.21) \)
where \( x - a \in R[x] \). So \( a = 0 \) or \( 1 \). Since \( g(x) \) divides \( x^n - 1 \) and \( x \) does not divide \( x^n - 1 \) but \( x - 1 \) does, we get \( a = 1 \). This means, \( x - 1 \) is a divisor of \( g(x) \) in \( R[x] \). So \( g(1) = 0 \). But \( g(x) \) is the generating polynomial of \( C^0 \) and so for all the \( h(x) \in C^0 \), we get \( h(1) = 0 \). Thus 1 is a root of all the codewords in \( C^0 \), which means all the codewords in \( C^0 \) are of even weight. So \( C^0 \) is a subset of the set of even weight vectors in \( C \). Since \( n \) is odd, \( x^n - 1 \) is a separable polynomial, and since \( g(x) \) divides \( x^n - 1 \), \( g(x) \) is also separable. Using this and (2.21), we get \( x - 1 \) is not a divisor of \( f(x) \). This gives \( f(1) \neq 0 \) and hence \( f(x) \) is of odd weight. Therefore \( C \) contains both even and odd weight vectors. This allows us to apply Lemma 2.1.3 to \( C \), and consequently, the set of even weight vectors of \( C \) is a subcode of \( C \) of codimension one in this case. Therefore \( C^0 \) is exactly the set of all even weight vectors in \( C \). \( \square \)

For a vector \( \vec{u} = (u_1, \ldots, u_m) \), we denote its cyclic shift by \( x\vec{u} \) and so
\[
    x\vec{u} = (u_m, u_1, \ldots, u_{m-1}).
\]

**Theorem 2.2.17** If \( C_E \) and \( C_I \) are binary cyclic codes and \( C^0_i \) is a cyclic subcode of \( C_I \) of codimension one, then the composition \( C = C_E \circ (C^0_i, C_I) \) is also a binary cyclic code.

**Proof:** We have \( C = C^0_i \cup C_I \) by definition. Since \( C_I \) is cyclic, we get, for
\[
    \vec{c} \in C_I \implies x\vec{c} \in C_I.
\]
Also \( C^0_i \) is cyclic and \( C^0_i \cap C_I = \emptyset \), so \( C^0_i \) is also cyclic. Thus, for \( \vec{c} \in C \), both \( \vec{c} \) and \( x\vec{c} \) are in \( C^0_i \) or \( C_I \). Similarly, since \( C_E \) is cyclic, we have, for
\[
    \vec{y} = (y_1, \ldots, y_{n_E}) \in C_E \implies x\vec{y} = (y_{n_E}, y_1, \ldots, y_{n_E-1}) \in C_E.
\]
Let \( \overline{y} \circ \{ \overline{c}_i \}_{i=1}^{n_E} \) be an arbitrary element of \( C = C_E \circ (C_1^o, C_1) \), where \( \overline{y} = (y_1, \ldots, y_{n_E}) \in C_E \)
and \( \{ \overline{c}_i \}_{i=1}^{n_E} \) be a suitable set of \( \overline{y} \) from \( C_1 \) with \( \overline{c}_i = (c_{i1}, \ldots, c_{in}) \) for \( i = 1, \ldots, n_E \).
Then
\[
\overline{y} \circ \{ \overline{c}_i \}_{i=1}^{n_E} = (c_{11}, c_{21}, \ldots, c_{n_E1}; c_{12}, c_{22}, \ldots, c_{n_E2}; \ldots; c_{1n}, c_{2n}, \ldots, c_{n_E1})
\]
and \( \overline{c}_i \in C_1^o \) for \( i = 1, \ldots, n_E \). So \( x\overline{c}_i \in C_1^o \) for all those \( i \)'s. This means that \( \{ \overline{w}_i \}_{i=1}^{n_E} \), with
\[
\overline{w}_1 = x\overline{c}_{n_E}, \quad \text{and} \quad \overline{w}_i = \overline{c}_{i-1} \quad \text{for} \quad i = 2, \ldots, n_E
\]
is a suitable set of \( x\overline{y} = (y_{n_E}, y_1, \ldots, y_{n_E-1}) \). So
\[
(x\overline{y}) \circ \{ \overline{w}_i \}_{i=1}^{n_E} \in C
\]
and
\[
(x\overline{y}) \circ \{ \overline{w}_i \}_{i=1}^{n_E} = \left( c_{n_E1}, c_{11}, c_{21}, \ldots, c_{(n_E-1)1}; c_{n_E1}, c_{12}, c_{22}, \ldots, c_{(n_E-1)2}; \ldots; c_{n_E(n-1)-1}, c_{1n}, c_{2n}, \ldots, c_{(n_E-1)n} \right)
\]
\[
= x \left( \overline{y} \circ \{ \overline{c}_i \}_{i=1}^{n_E} \right)
\]
which is the cyclic shift of \( \overline{y} \circ \{ \overline{c}_i \}_{i=1}^{n_E} \). So
\[
x \left( \overline{y} \circ \{ \overline{c}_i \}_{i=1}^{n_E} \right) \in C.
\]
Hence \( C \) is cyclic. \( \square \)

**Corollary 2.2.18** If \( C_E, C_1 \) and \( C_1^o \) are cyclic and \( n_1 \) is odd, then \( C = C_E \circ (C_1^o, C_1) \) is a cyclic code with \( C_1^o \) as the set of all even weight vectors in \( C_1 \) and \( C_1^o \) as the set of all odd weight vectors in \( C_1 \).
Proof: This corollary follows from Theorem 2.2.17 and Lemma 2.2.16. \hfill \Box

**Theorem 2.2.19** Suppose \( C = C_E \circ (C_I^o, C_I) \) is cyclic, then

(i) if \( C_E = \{ \overline{0} \} \), then \( C_I^o \) is cyclic,

(ii) if \( C_E \neq \{ \overline{0} \} \) then

(a) \( C_I \) is cyclic,

(b) if \( C_I^o \) is cyclic, then \( C_I^o \) and \( C_I \) are cyclic,

(c) if \( C_I^o \) is not cyclic, then \( C_E = F_2^{n_E} \).

**Proof:** (i) Suppose \( C_E = \{ \overline{0} \} \). We want to show that \( C_I^o \) is cyclic. For that, let \( \overline{c} \in C_I^o \). Then, we need to show that \( x\overline{c} \in C_I^o \). Let \( \overline{y} = \overline{0} \) be the zero vector in \( C_E \).

Then \( \{ \overline{c}_i \}_{i=1}^{n_E} \) where \( \overline{c}_i = \overline{0} \) for \( i = 1, \ldots, n_E - 1 \) and \( \overline{c}_{n_E} = \overline{c} \) is a suitable set of \( \overline{y} \) from \( C_I^o \). Since \( C = C_E \circ (C_I^o, C_I) \) is cyclic, \( x(\overline{y} \circ \{ \overline{c}_i \}_{i=1}^{n_E}) \) is also in \( C \). But

\[
x(\overline{y} \circ \{ \overline{c}_i \}_{i=1}^{n_E}) = \overline{z} \circ \{ \overline{w}_i \}_{i=1}^{n_E}
\]

where \( \overline{w}_1 = x\overline{c}_{n_E} = x\overline{c} \) and \( \overline{w}_i = \overline{c}_{i-1} \) for \( i = 2, \ldots, n_E \), and \( \overline{z} = (z_1, \ldots, z_{n_E}) \in C_E \) such that \( \overline{w}_i \in C_I^o \). But \( C_E = \{ \overline{0} \} \) by assumption. Therefore \( \overline{z} = \overline{0} \) and so \( z_i = 0 \) for \( i = 1, \ldots, n_E \). Hence \( \overline{w}_1 \in C_I^o \) and consequently \( C_I^o \) is cyclic.

(ii) Now we assume that \( C_E \neq \{ \overline{0} \} \).

(a) We want to show that \( C_I \) is cyclic.

Since \( C_E \) is non-zero in this case, without loss of generality, we can assume that we can find a vector \( \overline{y'} = (y_1, \ldots, y_{n_E}) \) in \( C_E \) with \( y_{n_E} = 1 \). Let \( \overline{c} = (c_1, \ldots, c_{n_I}) \) be an arbitrary element of \( C_I \). Pick

\[
\overline{y} = \begin{cases} \overline{0}, & \text{if } \overline{c} \in C_I^o \\ \overline{y'}, & \text{if } \overline{c} \in C_I \end{cases} \tag{2.25}
\]
Then we can find a suitable set \( \{ \bar{c}_i \}_{i=1}^{n_E} \) of \( \bar{y} \) with \( \bar{c}_{n_E} = \bar{c} \). So \( \bar{y} \circ \{ \bar{c}_i \}_{i=1}^{n_E} \in \mathcal{C} \). Since \( \mathcal{C} \) is cyclic, \( x\left( \bar{y} \circ \{ \bar{c}_i \}_{i=1}^{n_E} \right) \in \mathcal{C} \). But
\[
x\left( \bar{y} \circ \{ \bar{c}_i \}_{i=1}^{n_E} \right) = (\bar{z}) \circ \{ \bar{w}_i \}_{i=1}^{n_E}
\]
where \( \bar{z} = (z_1, \ldots, z_{n_E}) \in \mathcal{C}_E \), and \( \bar{w}_i \in \mathcal{C}_I \) with \( \bar{w}_1 = x\bar{c}_{n_E} = x\bar{c} \) and \( \bar{w}_i = \bar{c}_{i-1} \) for \( i = 2, \ldots, n_E \) such that \( \bar{w}_i \in \mathcal{C}_I^2 \). But \( \mathcal{C}_I^2 \subset \mathcal{C}_I \) for \( i = 1, \ldots, n_E \). Therefore \( \bar{w}_1 = x\bar{c}_{n_E} = x\bar{c} \) is in \( \mathcal{C}_I \). Hence \( \mathcal{C}_I \) is cyclic.

(b) If \( \mathcal{C}_j^o \) is cyclic, then \( \mathcal{C}_j^1 \) and \( \mathcal{C}_E \) are cyclic.

- First we show that \( \mathcal{C}_j^1 \) is cyclic. For that, let \( \bar{c} \in \mathcal{C}_j^1 \). Since \( \mathcal{C}_j^1 \subset \mathcal{C}_I \) and \( \mathcal{C}_I \) is cyclic, we have \( x\bar{c} \in \mathcal{C}_I \). Also
\[
\mathcal{C}_I = \mathcal{C}_j^o \cup \mathcal{C}_j^1 \quad \text{where} \quad \mathcal{C}_j^o \cap \mathcal{C}_j^1 = \emptyset.
\]
So \( x\bar{c} \in \mathcal{C}_j^o \) or \( \mathcal{C}_j^1 \). Suppose \( x\bar{c} \notin \mathcal{C}_j^1 \). Then \( x\bar{c} \in \mathcal{C}_j^o \), and since \( \mathcal{C}_j^o \) is cyclic, all the cyclic shifts of \( x\bar{c} \) are back in \( \mathcal{C}_j^o \). In particular, \( x^{n_j} \bar{c} = \bar{c} \in \mathcal{C}_j^o \). This is a contradiction since \( \bar{c} \in \mathcal{C}_j^1 = \mathcal{C}_I \setminus \mathcal{C}_j^o \). So \( x\bar{c} \in \mathcal{C}_j^1 \) and therefore \( \mathcal{C}_j^1 \) is cyclic.

- Next we show that \( \mathcal{C}_E \) is cyclic. For that let \( \bar{y} = (y_1, \ldots, y_{n_E}) \in \mathcal{C}_E \). Then, we can find a suitable set \( \{ \bar{c}_i \}_{i=1}^{n_E} \) of \( \bar{y} \) from \( \mathcal{C}_I \) so that \( \bar{y} \circ \{ \bar{c}_i \}_{i=1}^{n_E} \in \mathcal{C} \). Since \( \mathcal{C} \) is cyclic, the cyclic shift \( x\left( \bar{y} \circ \{ \bar{c}_i \}_{i=1}^{n_E} \right) \) is also in \( \mathcal{C} \). Also, \( \mathcal{C}_j^o \) is cyclic by assumption and \( \mathcal{C}_j^1 \) is cyclic from part(a). So by using (2.24), we get
\[
x\left( \bar{y} \circ \{ \bar{c}_i \}_{i=1}^{n_E} \right) = (x\bar{y}) \circ \{ \bar{w}_i \}_{i=1}^{n_E}
\]
where \( \bar{w}_i \)'s are as in (2.22). So \( (x\bar{y}) \circ \{ \bar{w}_i \}_{i=1}^{n_E} \) is in \( \mathcal{C} \), which means \( x\bar{y} \in \mathcal{C}_E \). Therefore \( \mathcal{C}_E \) is cyclic.
(c) If \( C^o_j \) is not cyclic, then \( C_E = F_2^{n_E} \).

Since \( C^o_j \) is not cyclic, there is a code word \( \bar{u} \) in \( C^o_j \) such that its cyclic shift \( x\bar{u} \) is not in \( C^o_j \). Since \( C_I \) is cyclic from part (a), and \( C^o_j \) is a subcode of \( C_I \), \( x\bar{u} \in C_I \setminus C^o_j = C'_j \).

Let \( \bar{e}_i = (0, \ldots, 1, \ldots, 0) \in F_2^{n_E} \) be the weight one vector with one as its \( i \)th coordinate. We will show that
\[ \{ \bar{e}_i \}_{i=1}^{n_E} \subset C_E. \]
Let \( \bar{y} = \bar{0} \) be the zero vector of \( C_E \) and \( \{ \bar{e}_i \}_{i=1}^{n_E} \) be a suitable set of \( \bar{y} \) with \( \bar{e}_i = \bar{0} \) for \( i = 1, \ldots, n_E - 1 \) and \( \bar{e}_{n_E} = \bar{a} \). Then
\[ \bar{y} = \bar{y} \circ \{ \bar{e}_i \}_{i=1}^{n_E} \in C_E \circ (C^o_j, C_I). \]

Since \( C_E \circ (C^o_j, C_I) \) is cyclic, we have
\[ x\bar{y} = x(\bar{y} \circ \{ \bar{e}_i \}_{i=1}^{n_E}) \in C_E \circ (C^o_j, C_I). \]
So
\[ \bar{f} = x\bar{y} = x(\bar{y} \circ \{ \bar{e}_i \}_{i=1}^{n_E}) = \bar{z} \circ \{ \bar{w}_i \}_{i=1}^{n_E} \]
where \( \bar{z} = (z_1, \ldots, z_{n_E}) \in C_E, \bar{w}_1 = x\bar{e}_{n_E} = x\bar{a}, \bar{w}_i = \bar{e}_{i-1} = \bar{0} \) for \( i = 2, \ldots, n_E \) and \( \bar{w}_i \in C^o_j \). Because \( \bar{w}_1 = x\bar{u} \in C'_j \) and \( \bar{w}_i = \bar{0} \in C^o_j \) for \( i = 2, \ldots, n_E \), we get \( z_1 = 1 \) and \( z_i = 0 \) for \( i = 2, \ldots, n_E \). Therefore \( \bar{z} = (1, 0, \ldots, 0) = \bar{e}_1 \). Since \( \bar{z} \in C_E \), we get \( \bar{e}_1 \in C_E \). The cyclic shift \( x\bar{f} \) of \( \bar{f} \) is \( x(\bar{z} \circ \{ \bar{w}_i \}_{i=1}^{n_E}) \) and it is also in \( C = C_E \circ (C^o_j, C_I) \) since \( C \) is cyclic. It can be easily checked that
\[ x(\bar{z} \circ \{ \bar{w}_i \}_{i=1}^{n_E}) = (x\bar{z}) \circ \{ \bar{u}_i \}_{i=1}^{n_E} \]
where \( \bar{u}_i = \bar{0} \) for \( i \neq 2 \) and \( \bar{u}_2 = \bar{w}_1 = x\bar{a} \). But \( \bar{z} \in C_E \) and \( C_E \) is cyclic and so \( x\bar{z} = \bar{e}_2 \in C_E \). Proceeding in this manner, we get that for \( j = 1, \ldots, n_E \), the cyclic
shift $x^j \overline{f} = x^j \left( \overline{y} \circ \{\overline{r}_i\}_{i=1}^n \right) \in \mathcal{C}_E \circ (\mathcal{C}_i \circ \mathcal{C}_j)$ with $\overline{r}_j \in \mathcal{C}_E$ as the underlying vector. Thus

$$\{\overline{r}_j\}_{j=1}^n \subset \mathcal{C}_E$$

and so $\mathcal{C}_E = F_q^{m_E}$ in this case. \qed

Let $F_q$ be a finite field of order $q$ and $f(x) = x^n - 1$. Then $f(x) \in F_q[x]$. Let $K$ be the splitting field of $f(x)$ over $F_q$. Then the roots of $f(x)$ are called $n$th roots of unity and form a cyclic subgroup of the multiplicative group $K^*$ of $K$.

**Definition 2.2.20** An $n$th root of unity $\alpha$ is called a **primitive $n$th root of unity** if its multiplicative order $\circ(\alpha)$ is $n$.

The next lemma which gives a criterion for the existence of primitive $n$th roots of unity is a well-known result.

**Lemma 2.2.21** Let $q = p^m$, where $p$ is a prime number and $m \geq 1$. Then, if $(n,q) = 1$, then the splitting field $K$ of $f(x) = x^n - 1$ over $F_q$ contains a primitive $n$th root of unity.

**Proof:** Since $(p,n) = 1$, the derivative $f'(x) = nx^{n-1} \neq 0$ if $x \neq 0$. And $f(0) = 1$, so $(f(x), f'(x)) = 1$. Hence $f(x)$ has no multiple roots and so is a separable polynomial. Let $\Omega$ be the set of roots of $f(x)$. Then $|\Omega|$ is equal to the number of roots of $f(x)$, which in this case is $n$. So $\Omega$ is of order $n$. And since $\Omega$ is cyclic, there is an element $\alpha \in \Omega$ of order $n$. Then $\alpha$ is a primitive $n$th root of unity in $K$. \qed
In the following, we assume that \((n_E, 2) = 1\) and \((n_I, 2) = 1\).

Then from Lemma (2.2.21),

\[
x^{n_E} - 1, \ x^{n_I} - 1 \text{ and } x^{n_{E}n_{I}} - 1
\]

are separable. If \(C_I\) is a binary cyclic code, then it is an ideal of \(F_2[x]/(x^{n_I} - 1)\). Let \(f(x)\) be the generating polynomial of \(C_I\). Then

\[
C_I = \langle f(x) \rangle \text{ and } f(x) \text{ divides } (x^{n_I} - 1).
\]

Since \(x^{n_I} - 1\) is a separable polynomial, \(f(x)\) is also separable. If \(\alpha\) is a root of \(f(x)\), then it is a root of \(x^{n_I} - 1\) also, and so \(\alpha^{n_I} = 1\).

Similarly, if \(C_E\) is a nonzero cyclic code, then for some \(g(x) \neq 0\) in \(F_2[x]/(x^{n_E} - 1)\),

\[
C_E = \langle g(x) \rangle \text{ and } g(x) \text{ divides } (x^{n_E} - 1).
\]

Also, \(g(x)\) is separable and its roots are among \(n_E\) th roots of unity.

Let \(C_I\) and \(C_E\) be cyclic. Let \(C_I^0\) be a cyclic subcode of \(C_I\) of codimension one. Since \(n_I\) is odd, from Lemma 2.2.16, \(C_I^0\) is the set of all even weight vectors in \(C_I\). Then, \(C_I^0\) consists of all the odd weight vectors in \(C_I\). So the composition \(C = C_E \circ (C_I^0, C_I)\) is a cyclic code with the subcode of all even weight vectors in \(C_I\) as the only choice for \(C_I^0\).

Let \(\bar{c}(x)\) be an element of \(C\). Then, there are \(a_l\)’s in \(F_2\) such that

\[
\bar{c}(x) = \sum_{i=0}^{n_{E}n_{I}-1} a_i x^i = \sum_{i=0}^{n_{E}-1} \left( \sum_{j=0}^{n_{I}-1} a_{i+jn_E} x^{i+jn_E} \right)
\]

\[
= \sum_{i=0}^{n_{E}-1} x^i \left( \sum_{j=0}^{n_{I}-1} a_{i+jn_E} (x^{n_E})^j \right) = \sum_{i=0}^{n_{E}-1} x^i \bar{c}_i (x^{n_E})
\]

(2.29)
where
\[ \bar{c}_i(x) = \sum_{j=0}^{n_i-1} a_{i+jn_E}x^j. \] (2.30)

Using the definition of \( \mathcal{C} \),
\[ \bar{c}(x) = \bar{y}(x) \circ \{\bar{c}_i(x)\}_{i=0}^{n_E-1} \] (2.31)

where
\[ \bar{y}(x) = \sum_{i=0}^{n_E-1} x^i\bar{c}_i(1) \in \mathcal{C}_E \] (2.32)

and
\[ \bar{c}_i(x) = \sum_{j=0}^{n_i-1} a_{i+jn_E}x^j \in \mathcal{C}_I^{\bar{c}_i(1)}. \]

**Theorem 2.2.22** If \( \mathcal{C}_E = \langle g(x) \rangle \) and \( \mathcal{C}_E \) is nonzero, \( \mathcal{C}_I = \langle f(x) \rangle \), and \( \mathcal{C}_I^o \) is cyclic, then
\[ \mathcal{C} = \mathcal{C}_E \circ (\mathcal{C}_I^o, \mathcal{C}_I) = \langle g(x)f(x^{n_E}) \rangle. \]

**Proof:** First we show that \( g(x)f(x^{n_E}) \) is in \( \mathcal{C} \). For that, let
\[ g(x) = \sum_{i=0}^{n_E} g_ix^i. \]

Since \( \mathcal{C}_E \) is nonzero, there is at least one \( g_i \neq 0 \). Also, since \( \mathcal{C}_I \) contains odd weight vectors, we have \( f(1) \neq 0 \). So \( f(x) \in \mathcal{C}_I^1 \). Pick
\[ \bar{c}_i(x) = \begin{cases} \bar{o}, & \text{if } g_i = 0 \\ f(x), & \text{if } g_i = 1. \end{cases} \] (2.33)
Then \( \{ \tilde{r}_i(x) \}_{i=0}^{n_E-1} \) is a suitable set of \( g(x) \) from \( C_I \). So

\[
g(x) \circ \{ \tilde{r}_i(x) \}_{i=0}^{n_E-1} \in C.
\]

But

\[
g(x) \circ \{ \tilde{r}_i(x) \}_{i=0}^{n_E-1} = g(x)f(x^{n_E}).
\]

So \( g(x)f(x^{n_E}) \) is also in \( C \).

Let \( \bar{c}(x) \) be an arbitrary element of \( C \). We will show that \( g(x)f(x^{n_E}) \) divides \( \bar{c}(x) \).

From (2.29)

\[
(\bar{c}(x)) = \sum_{i=0}^{n_E-1} x^i \tilde{c}_i(x^{n_E})
\]

where \( \tilde{c}_i(x) \in C_I \) and

\[
\bar{v}(x) = \sum_{i=0}^{n_E-1} x^i \tilde{c}_i(1) \in C_E.
\]

Since \( \tilde{c}_i(x) \in C_I \),

\[
\tilde{c}_i(x) = h_i(x)f(x)
\]

(2.34)

where \( h_i(x) \in F_2[x]/(x^{n_I} - 1) \). But \( f(1) \neq 0 \), and so \( f(1) = 1 \). This gives

\[
\tilde{c}_i(1) = h_i(1) \quad \text{for } i = 1, \ldots, n_E-1.
\]

Thus

\[
\bar{v}(x) = \sum_{i=0}^{n_E-1} x^i \tilde{c}_i(1) = \sum_{i=0}^{n_E-1} x^i h_i(1).
\]

Using (2.34), we get

\[
\tilde{c}(x) = \sum_{i=0}^{n_E-1} x^i \tilde{c}_i(x^{n_E})
\]

\[
= \sum_{i=0}^{n_E-1} x^i \left( h_i(x^{n_E})f(x^{n_E}) \right) = f(x^{n_E}) \sum_{i=0}^{n_E-1} x^i h_i(x^{n_E}).
\]

(2.35)
We claim that \( g(x) \) divides \( \sum_{i=0}^{n_E-1} x^i h_i(x^{n_E}) \). To show this, let \( \alpha \) be a root of \( g(x) \). Then \( \alpha^{n_E} = 1 \). Putting \( x = \alpha \) in \( \sum_{i=0}^{n_E-1} x^i h_i(x^{n_E}) \), we get

\[
\sum_{i=0}^{n_E-1} \alpha^i h_i(\alpha^{n_E}) = \sum_{i=0}^{n_E-1} \alpha^i h_i(1) = \sum_{i=0}^{n_E-1} \alpha^i \bar{c}_i(1) = \bar{y}(\alpha) = 0 \quad (2.36)
\]
since \( \bar{y} \in C_E \) means \( g(x) \) divides \( \bar{y}(x) \). So the roots of \( g(x) \) are among the roots of \( \sum_{i=0}^{n_E-1} x^i h_i(x^{n_E}) \). And as we noted before, \( g(x) \) is separable. Therefore

\[
g(x) \text{ divides } \sum_{i=0}^{n_E-1} x^i h_i(x^{n_E}).
\]

So, we have

\[
\sum_{i=0}^{n_E-1} x^i h_i(x^{n_E}) = q(x)g(x)
\]

for some \( q(x) \) in \( F_2[x] \). This gives

\[
\bar{c}(x) = q(x)g(x)f(x^{n_E}).
\]

Thus, each element \( \bar{c}(x) \) of \( C \) is a multiple of \( g(x)f(x^{n_E}) \).

Hence \( C = \langle g(x)f(x^{n_E}) \rangle \). \( \square \)

Let \( n = n_\ell n_l \) and \( \beta \) be a primitive \( n \)-th root of unity over \( F_2 \). Let \( \alpha = \beta^{n_l} \) and \( \gamma = \beta^{n_E} \). Then \( \alpha \) is a primitive \( n_\ell \)-th root of unity and \( \gamma \) is a primitive \( n_l \)-th root of unity. If \( g(x) \) and \( f(x) \) are the generating polynomials of \( C_E \) and \( C_l \), then the roots of \( g(x) \) are among the powers of \( \alpha \) and the roots of \( f(x) \) are among the powers of \( \gamma \).

We let

\[
\Omega_E = \left\{ \alpha^i : g(\alpha^i) = 0, \ 0 \leq i \leq n_E - 1 \right\} \quad (2.37)
\]

\[
\Delta_E = \left\{ i : 0 \leq i \leq n_E - 1 \text{ and } g(\alpha^i) = 0 \right\} \quad (2.38)
\]
\[ \Omega_i = \{ \gamma^j : f(\gamma^j) = 0, \ 0 \leq j \leq n_i - 1 \} \]  
(2.39)

\[ \Delta_i = \{ j : 0 \leq j \leq n_i - 1 \ \text{and} \ f(\gamma^j) = 0 \}. \]  
(2.40)

Since \( f(1) \neq 0 \), we get \( 0 \notin \Delta_i \). By definition,

\[ \Delta_{E} \subseteq \mathbb{Z}_{n_E}, \ \Delta_i \subseteq \mathbb{Z}_{n_i} \setminus \{0\} \]  
(2.41)

and

\[ |\Delta_E| = \deg g(x), \ |\Delta_i| = \deg f(x). \]  
(2.42)

Let

\[ \Delta = \left\{ \bigcup_{t \in \Delta_i} \left( t + n_i \mathbb{Z}_{n_E} \right) \right\} \cup \{ln_i : l \in \Delta_E\}. \]  
(2.43)

**Lemma 2.2.23**

\[ |\Delta| = \deg f(x)n_E + \deg g(x). \]  
(2.44)

**Proof:** Let

\[ A = \bigcup_{t \in \Delta_i} \left( t + n_i \mathbb{Z}_{n_E} \right) \]  
(2.45)

and

\[ B = \{ln_i : l \in \Delta_E\}. \]  
(2.46)

We note that \( n_i \mathbb{Z}_{n_E} \) is an additive subgroup of \( \mathbb{Z}_{n_E n_i} \). If, for \( t, t' \) in \( \Delta_i \),

\[ t + n_i \mathbb{Z}_{n_E} = t' + n_i \mathbb{Z}_{n_E}, \]

then \( t - t' \in n_i \mathbb{Z}_{n_E} \). This means, \( n_i \) divides \( t - t' \). But \( 0 \leq t - t' \leq n_i - 1 \). So \( t - t' = 0 \) and thus \( t = t' \). Hence \( A \) is a disjoint union of the cosets of \( n_i \mathbb{Z}_{n_E} \) not
including \( n \mathbb{Z}_{n_E} \) since \( 0 \notin \Delta \). Clearly \( B \subseteq n \mathbb{Z}_{n_E} \). Hence \( A \cap B = \emptyset \) and so \( \Delta \) is a disjoint union of \( A \) and \( B \). This gives

\[
|\Delta| = |A| + |B| = |\Delta| n_E + |\Delta_E|
\]

\[
= \deg f(x) n_E + \deg g(x)
\]

which is the size of \( \Delta \). \( \square \)

Let

\[
\Omega = \{ \beta^s : s \in \Delta \}.
\]

(2.47)

**Theorem 2.2.24** \( \Omega \) is the set of roots of the generating polynomial

\[
P(x) = g(x)f(x^n_E)
\]

of the composition code \( C = C_E \circ (C_H, C_I) \).

**Proof:** Pick an arbitrary element \( \beta^s \) in \( \Omega \). Since \( \Omega \) is a disjoint union of \( A \) and \( B \), \( s \) is in \( A \) or is in \( B \).

**Case 1** Suppose \( s \) is in \( A \). Then \( s = t + n_I z \) for some \( t \) in \( \Delta _I \) and \( z \) in \( \mathbb{Z}_{n_E} \). Then, since \( \beta^{n_E n_I} = 1 \), putting \( x = \beta^s \) in \( f(x^n_E) \) gives

\[
f((\beta^s)^{n_E}) = f((\beta^{(t+n_I z)n_E}) = f(\beta^{n_E t}) = f(\alpha^t) = 0
\]

since \( \alpha^t \in \Omega _I \). So \( \beta^s \) is a root of \( f(x^n_E) \) and hence it is root of \( P(x) = g(x)f(x^n_E) \).

**Case 2** Suppose \( s \) is in \( B \). Then \( s = l n_I \) for some \( l \) in \( \Delta _E \). Putting \( x = \beta^s \) in \( g(x) \) gives

\[
g(\beta^s) = g(\beta^{l n_I}) = g(\gamma^l) = 0
\]

since \( \gamma^l \in \Omega _I \). So \( \beta^s \) is a root of \( g(x) \) and is therefore a root of \( P(x) = g(x)f(x^n_E) \).

Thus \( \Omega \) is among the roots of \( P(x) \). Since \( 2 \) is not a divisor of \( n_E \) or \( n_I \), \( 2 \) does not
divide $n_{E}n_{I}$. So $x^{n_{E}n_{I}} - 1$ is separable. $P(x)$ is a divisor of $x^{n_{E}n_{I}} - 1$, and so it is also separable. Thus, the number of distinct roots of $P(x)$ is the same as the degree of $P(x)$ and

$$\deg P(x) = \deg g(x) + n_{E}\deg f(x) = |\Omega|$$

using (2.2.23).

Hence $\Omega$ is the set of all the roots of $P(x) = g(x)f(x^{n_{E}})$.

\[ \square \]

### 2.2.2 The Dual of the Composition Code

Let $C_{E}$ be an $[n_{E}, k_{E}]$ binary linear code and $C_{I}$ be an $[n_{I}, k_{I}]$ binary code, and $C_{I}^{o}$ a subcode of $C_{I}$ of codimension one. In this section, we will find the dual of $\mathcal{C} = C_{E} \circ (C_{I}^{o}, C_{I})$.

We have

$$C_{I}^{o} \subset C_{I} \implies (C_{I}^{o})^\perp \supset C_{I}^\perp. \quad (2.48)$$

Also

$$\dim C_{I}^\perp = n_{I} - k_{I} \quad \text{and} \quad \dim (C_{I}^{o})^\perp = n_{I} - (k_{I} - 1) = n_{I} - k_{I} + 1. \quad (2.49)$$

From the dimensions, we notice that $C_{I}^\perp$ is a subspace of $(C_{I}^{o})^\perp$ of codimension one. Thus we can define the composition $C_{E}^\perp \circ (C_{I}^\perp, (C_{I}^{o})^\perp)$ with $C_{E}^\perp$ as the exterior code and $(C_{I}^{o})^\perp$ as the interior code with $C_{I}^\perp$ as its subcode of codimension one.

**Lemma 2.2.25** \quad Let $C_{E}$ and $C_{I}$ be $[n_{E}, k_{E}]$ and $[n_{I}, k_{I}]$ binary linear codes, then the composition $C_{E}^\perp \circ (C_{I}^\perp, (C_{I}^{o})^\perp)$ is a binary linear code of dimension

$$n_{E}(n_{I} - k_{I}) + (n_{E} - k_{E}). \quad (2.50)$$
Proof: Since \( C^\perp_E \) and \((C^n_I)^\perp \) are linear, their composition is also linear from Theorem 2.2.10. We have \( \dim(C^\perp_E) = n_E - k_E \) and \( \dim((C^n_I)^\perp) = n_I - k_I + 1 \). So using Theorem 2.2.10, we get

\[
\dim(C^\perp_E \circ (C^\perp_I, (C^n_I)^\perp)) = n_E(n_I - k_I + 1 - 1) + (n_E - k_E)
\]

\[
= n_E(n_I - k_I) + (n_E - k_E) \tag{2.51}
\]

which gives the dimension of the composition of \( C^\perp_E \) and \((C^n_I)^\perp \) using \( C^\perp_I \). \( \square \)

**Theorem 2.2.26** If \( C_E \) and \( C_I \) are binary linear codes and \( C^n_I \) a subcode of \( C_I \) of codimension one, then the dual of their composition \( C = C_E \circ (C^n_I, C_I) \), denoted by \( C^\perp \), is \( C^\perp_E \circ (C_I^\perp, (C^n_I)^\perp) \).

Proof: We first show that \( C^\perp_E \circ (C_I^\perp, (C^n_I)^\perp) \subseteq C^\perp \). For that, let

\[
\overline{y} \circ \{\overline{c}_i\}_{i=1}^{n_E} \in C \tag{2.52}
\]

where

\[
\overline{y} = (y_1, \ldots, y_{n_E}) \in C_E \quad \text{and} \quad \{\overline{c}_i\}_{i=1}^{n_E}
\]

is a suitable set of \( \overline{y} \) from \( C_I \), and

\[
\overline{w} \circ \{\overline{u}_i\}_{i=1}^{n_E} \in C^\perp_E \circ (C_I^\perp, (C^n_I)^\perp) \tag{2.53}
\]

where

\[
\overline{w} = (w_1, \ldots, w_{n_E}) \in C^\perp_E \quad \text{and} \quad \{\overline{u}_i\}_{i=1}^{n_E}
\]
is a suitable set of $\mathbf{w}$ from $(\mathcal{C}_j^o)$. Then the scalar product

$$
\left( \mathbf{y} \circ \{ \overline{c}_i \}_{i=1}^{n_E} \right) \cdot \left( \mathbf{w} \circ \{ \overline{u}_i \}_{i=1}^{n_E} \right) = \left( \sum_{i=1}^{n_E} \overline{c}_i \cdot \overline{u}_i \right) \mod 2 \tag{2.54}
$$

$$
= \left( \sum_{\overline{u}_i \in \mathcal{C}_I^f} \overline{c}_i \cdot \overline{u}_i \right) \mod 2
$$

If $\overline{u}_i \in \mathcal{C}_I^f$, then $\overline{c}_i \cdot \overline{u}_i = 0$ since $\overline{c}_i \in \mathcal{C}_I$.

If $\overline{u}_i \notin \mathcal{C}_I^f$, then $\overline{u}_i \in (\mathcal{C}_j^o)^\perp \setminus \mathcal{C}_I^f$. So, for $\overline{u}_i \notin \mathcal{C}_I^f$, $w_i = 1$. From these facts, for $\overline{u}_i \notin \mathcal{C}_I^f$, we get

$$
\overline{c}_i \cdot \overline{u}_i = \begin{cases} 
0, & \text{if } \overline{c}_i \in \mathcal{C}_I^o \\
1, & \text{if } \overline{c}_i \in \mathcal{C}_I^f
\end{cases} \tag{2.55}
$$

$$
= \begin{cases} 
0, & \text{if } w_i = 0 \\
1, & \text{if } w_i = 1
\end{cases} \tag{2.56}
$$

Thus

$$
\left( \left( \mathbf{y} \circ \{ \overline{c}_i \}_{i=1}^{n_E} \right) \cdot \left( \mathbf{w} \circ \{ \overline{u}_i \}_{i=1}^{n_E} \right) \right) = \left( 0 + \sum_{\overline{u}_i \notin \mathcal{C}_I^f} \overline{c}_i \cdot \overline{u}_i + \sum_{\overline{u}_i \in \mathcal{C}_I^f} \overline{c}_i \cdot \overline{u}_i \right) \mod 2
$$

$$
= \left( 0 + \sum_{\overline{u}_i \in \mathcal{C}_I^f} \overline{c}_i \cdot \overline{u}_i \right) \mod 2
$$

$$
= \sum_{\{w_i = 1\}} \mod 2
$$

$$
= \overline{y} \cdot \mathbf{w} = 0
$$

since $\mathbf{y} \in \mathcal{C}_E$ and $\mathbf{w} \in \mathcal{C}_I^f$. Therefore $(\mathcal{C}_E^o \circ (\mathcal{C}_j^f, (\mathcal{C}_j^o)^\perp)) \subseteq \mathcal{C}_I^\perp$. And

$$
\dim \mathcal{C}_I^\perp = \dim(\mathcal{C}_E \circ (\mathcal{C}_j^o, \mathcal{C}_I)) \perp = n_E n_I - \left( n_E (k_I - 1) + k_E \right)
$$

$$
= n_E (n_I - k_I) + (n_E - k_E) = \dim(\mathcal{C}_E^\perp \circ (\mathcal{C}_I^f, (\mathcal{C}_j^o)^\perp))
$$

using Lemma (2.2.25). Hence $\mathcal{C}_I^\perp = (\mathcal{C}_E^\perp \circ (\mathcal{C}_I^f, (\mathcal{C}_j^o)^\perp))$ and so we have the dual code of the composition $\mathcal{C}$ in terms of the duals of $\mathcal{C}_E$, $\mathcal{C}_I$ and $\mathcal{C}_j^o$. \qed
A code $C$ is called **self orthogonal** if $C \subseteq C^\perp$. The following theorem gives a sufficient condition for the composition code $C = C_E \circ (C_j^0, C_I)$ to be self orthogonal.

**Theorem 2.2.27** If $C_E$ is a binary code and $C_I$ is a binary self orthogonal code, then the composition code $C = C_E \circ (C_j^0, C_I)$ is self orthogonal.

**Proof:** Let $\overline{a}, \overline{b} \in C_I$. Then $\langle \overline{a}, \overline{b} \rangle = 0$ since $C_I$ is self orthogonal.

Let $\overline{y} \circ \{\overline{r}_i\}_{i=1}^n, \overline{w} \circ \{\overline{u}_i\}_{i=1}^n \in C$. Then

$$\langle \overline{y} \circ \{\overline{r}_i\}_{i=1}^n, \overline{w} \circ \{\overline{u}_i\}_{i=1}^n \rangle = \sum_{i=1}^n \langle \overline{r}_i, \overline{u}_i \rangle = \sum_{i=1}^n 0 = 0. \quad (2.57)$$

Thus any two elements of $C$ are orthogonal to each other and hence $C$ is self orthogonal. □

A code $C$ is called **self dual** if $C^\perp = C$. The following theorem gives a sufficient condition for the composition code $C = C_E \circ (C_j^0, C_I)$ to be self dual.

**Theorem 2.2.28** If $C_E$ and $C_I$ are binary codes such that $C_E$ is self dual and $C_I^\perp = C_j^0$, then the composition code $C = C_E \circ (C_j^0, C_I)$ is self dual.

**Proof:** Since $C_E$ is self dual, we have $C_E = C_E^\perp$. Also,

$$C_I \subseteq (C_I^\perp)^\perp = (C_I^0)^\perp \quad (2.58)$$

and $n_i - k_i = k_i - 1$ since $C_I^\perp = C_j^0$ by assumption. Therefore

$$\dim C_I = k_i = n_i - (k_i - 1) = \dim (C_I^0)^\perp.$$ 

This fact, together with (2.58) gives $C_I = (C_I^0)^\perp$. Thus

$$C = C_E \circ (C_I^0, C_I) = C_E^\perp \circ (C_I^\perp, (C_I^0)^\perp) = C^\perp$$

using Theorem 2.2.26 and hence $C$ is self dual. □
2.2.3 The Weight Enumerator of the Composition Code

Let \( W_C(x, y) \) be the weight enumerator of a code \( C \) of length \( n \). Then

\[ W_C(x, y) = \sum_{\vec{v} \in C} x^{\text{wt}(\vec{v})} y^{n - \text{wt}(\vec{v})}. \]  

(2.59)

We let \( C_E \) and \( C_I \) be two linear codes like before, and \( C_I^0 \), a subcode of \( C_I \) of codimension one. Let \( W_{C_E}(x, y) \), \( W_{C_I}(x, y) \), \( W_{C_I^0}(x, y) \) and \( W_{C_I^1}(x, y) \) be the weight enumerators of \( C_E, C_I, C_I^0 \) and \( C_I^1 \) respectively. In this section, we find an expression for the weight enumerator of \( C = C_E \circ (C_I^0, C_I) \) in terms of the weight enumerators of \( C_E, C_I^0 \) and \( C_I^1 \).

Theorem 2.2.29  
If \( W_{C_E}(x, y) \) is the weight enumerator of \( C_E \) and, \( W_{C_I^0}(x, y) \) and \( W_{C_I^1}(x, y) \) are the weight enumerators of \( C_I^0 \) and \( C_I^1 \), then the weight enumerator of the composition \( C = C_E \circ (C_I^0, C_I) \) is

\[ W_{C_E \circ (C_I^0, C_I)}(x, y) = W_{C_E \circ (C_I^0, C_I)}(x, y) = W_{C_E}(x, y) \cdot W_{C_I^0}(x, y) \cdot W_{C_I^1}(x, y). \]  

(2.60)

Proof: Let \( \bar{z} \circ \{\bar{v}_i\}_{i=1}^{u_E} \in C = C_E \circ (C_I^0, C_I) \) where \( \bar{z} = (z_1, \ldots, z_{n_E}) \in C_E \) and \( \bar{v}_i \in C_I^0 \). Then

\[ \text{wt}(\bar{z} \circ \{\bar{v}_i\}_{i=1}^{u_E}) = \sum_{i=1}^{u_E} \text{wt}(\bar{v}_i). \]

Let \( W_{\bar{z} \circ \{\bar{v}_i\}_{i=1}^{u_E}}(x, y) \) be the weight enumerator of \( \bar{z} \circ \{\bar{v}_i\}_{i=1}^{u_E} \). Then

\[ W_{\bar{z} \circ \{\bar{v}_i\}_{i=1}^{u_E}}(x, y) = x^{\text{wt}(\bar{z} \circ \{\bar{v}_i\}_{i=1}^{u_E})} y^{n_E - \text{wt}(\bar{z} \circ \{\bar{v}_i\}_{i=1}^{u_E})} = \prod_{i=1}^{u_E} \left( x^{\text{wt}(\bar{v}_i)} y^{n_I - \text{wt}(\bar{v}_i)} \right). \]  

(2.61)

Let \( W_{\bar{z} \circ (C_I^0, C_I)}(x, y) \) be the weight enumerator of \( \bar{z} \circ (C_I^0, C_I) \). Then

\[ W_{\bar{z} \circ (C_I^0, C_I)}(x, y) = \sum_{\{\bar{z} \circ \{\bar{v}_i\}_{i=1}^{u_E}\}} x^{\text{wt}(\bar{z} \circ \{\bar{v}_i\}_{i=1}^{u_E})} y^{n_E - \text{wt}(\bar{z} \circ \{\bar{v}_i\}_{i=1}^{u_E})} \]  

(2.61)
since the choice of \( \bar{c}_i \) for \( i = 1, \ldots, n_E \) are independent of each other. Thus, we have

\[
W_{\mathcal{E}_o(c_i, c_f)}(x, y) = W_{c_i}^1(x, y)W_{c_f}^2(x, y) \cdots W_{c_f}^{n_E}(x, y)
\]

\[
= \left( W_{c_i}^1(x, y) \right)^{wt(\bar{e})} \left( W_{c_f}^0(x, y) \right)^{n_E - wt(\bar{e})}
\]  \hspace{1cm} (2.62)

The weight enumerator of \( \mathcal{C}_E \) is

\[
W_{\mathcal{C}_E}(x, y) = \sum_{\bar{e} \in \mathcal{C}_E} x^{wt(\bar{e})} y^{n_E - wt(\bar{e})}.
\]  \hspace{1cm} (2.63)

Since

\[
\mathcal{C} = \mathcal{C}_E \circ (\mathcal{C}_i, \mathcal{C}_f) = \bigcup_{\bar{e} \in \mathcal{C}_E} \bar{e} \circ (\mathcal{C}_i, \mathcal{C}_f)
\]

is a disjoint union, and from (2.62), the weight enumerator of \( \mathcal{C} \) is

\[
W_{\mathcal{C}}(x, y) = \sum_{\bar{e} \in \mathcal{C}_E} W_{\mathcal{C}_o(c_i, c_f)}(x, y)
\]

\[
= \sum_{\bar{e} \in \mathcal{C}_E} \left( W_{c_i}^1(x, y) \right)^{wt(\bar{e})} \left( W_{c_f}^0(x, y) \right)^{n_E - wt(\bar{e})}
\]

\[
= W_{\mathcal{C}_E} \left( W_{c_i}^1(x, y), W_{c_f}^0(x, y) \right).
\]  \hspace{1cm} (2.64)

Thus the weight enumerator of \( \mathcal{C} \) is a composition of the weight enumerators of \( \mathcal{C}_E, \mathcal{C}_i^0 \) and \( \mathcal{C}_f^1 \).

\[ \square \]

If \( \mathcal{C}_E = \mathcal{C}_I \), then \( \mathcal{C} = \mathcal{C}_E \circ (\mathcal{C}_i^0, \mathcal{C}_I) = \mathcal{C}_I \circ (\mathcal{C}_i^0, \mathcal{C}_I) \). In this case, we write \( \mathcal{C} = \mathcal{C}_I \circ (\mathcal{C}_i^0, \mathcal{C}_I) = \mathcal{C}_I \circ \mathcal{C}_I \) for simplicity. Then, to find the weight enumerator of \( \mathcal{C} = \mathcal{C}_I \circ \mathcal{C}_I \) using the above theorem, we need only \( W_{\mathcal{C}_I}(x, y) \) and \( W_{\mathcal{C}_I}(x, y) \).
Corollary 2.2.30 The weight enumerator of \( \mathcal{C} = \mathcal{C}_1 \circ \mathcal{C}_1 \) is

\[
W_{\mathcal{C}_1 \circ \mathcal{C}_1}(x, y) = W_{\mathcal{C}_1}(W_{\mathcal{C}_1}^1(x, y), W_{\mathcal{C}_1}^0(x, y)).
\]

(2.65)

Proof: Since the weight enumerators of \( \mathcal{C}_1 \) and \( \mathcal{C}_1^0 \) are given, the weight enumerator of \( \mathcal{C}_1^1 \) is

\[
W_{\mathcal{C}_1^1}(x, y) = W_{\mathcal{C}_1}(x, y) - W_{\mathcal{C}_1}^0(x, y).
\]

Then the corollary follows from Theorem 2.2.29.

\[\square\]

2.2.4 Iterated Composition

The composition of two binary codes defined in this chapter can be used repeatedly to get a composition of more than two codes. For instance, if \( \mathcal{C}_1, \mathcal{C}_2 \) and \( \mathcal{C}_3 \) are binary codes of length \( n_1, n_2 \) and \( n_3 \) with \( \mathcal{C}_2^0, \mathcal{C}_3^0 \) as the subcodes of codimension one of \( \mathcal{C}_2 \) and \( \mathcal{C}_3 \), then the composition of \( \mathcal{C}_1, \mathcal{C}_2 \) and \( \mathcal{C}_3 \) can be defined as either

\[
\mathcal{P} = (\mathcal{C}_1 \circ (\mathcal{C}_2^0, \mathcal{C}_2)) \circ (\mathcal{C}_3^0, \mathcal{C}_3)
\]

(2.66)

or

\[
\mathcal{Q} = \mathcal{C}_1 \circ (\mathcal{C}_2^0 \circ (\mathcal{C}_3^0, \mathcal{C}_3), \mathcal{C}_2 \circ (\mathcal{C}_3^0, \mathcal{C}_3)).
\]

(2.67)

We will show, this composition is associative.

Theorem 2.2.31

\[
\mathcal{P} = \mathcal{Q}.
\]

Proof: Let

\[
\overline{c} \in \mathcal{P} = (\mathcal{C}_1 \circ (\mathcal{C}_2^0, \mathcal{C}_2)) \circ (\mathcal{C}_3^0, \mathcal{C}_3).
\]
We will show that \( \tilde{c} \) is also in

\[
Q = C_1 \circ \left( C_2^0 \circ (C_3^0, C_3), C_2 \circ (C_3^0, C_3) \right).
\]

We note that \( C_2^0 \circ (C_3^0, C_3) \) is a subcode of \( Q \) of codimension one. We denote its two cosets by \( (C_2^0 \circ (C_3^0, C_3))^i \) for \( i = 1, 2 \). Then \( (C_2^0 \circ (C_3^0, C_3))^i = C_2^i \circ (C_3^i, C_3) \) where \( C_2^i \) are the two cosets of \( C_2^0 \) in \( C_2 \) for \( i = 1, 2 \) and \( C_3^i \) are the two cosets of \( C_3^0 \) in \( C_3 \) for \( i = 1, 2 \). Let

\[
\tilde{c} = (x_1, x_2, \ldots, x_{n_1})
\]

be an element of \( C_1 \), and for \( i = 1, \ldots, n_1 \),

\[
\tilde{y}_i = (y_{i1}, y_{i2}, \ldots, y_{in_2})
\]

be elements of \( C_2 \) and, for \( i = 1, \ldots, n_1 \) and \( j = 1, \ldots, n_2 \)

\[
\tilde{z}_{ij} = (z_{ij}^{1}, z_{ij}^{2}, \ldots, z_{ij}^{n_3})
\]

be elements of \( C_3 \). Then

\[
\tilde{c} = \left( \tilde{x} \circ \{ \tilde{y}_i \}_{i=1}^{n_1} \right) \circ \left\{ \{ \tilde{z}_{ij} \}_{j=1}^{n_2} \right\}_{i=1}^{n_1}
\]

\( \iff \) \( \tilde{y}_i \in C_2^{x_i} \) and \( \tilde{z}_{ij} \in C_3^{y_{ij}} \)

\( \iff \) \( \tilde{y}_i \in C_2^{x_i} \) and \( \tilde{y}_i \circ \{ \tilde{z}_{ij} \}_{j=1}^{n_2} \in C_2 \circ (C_3^0, C_3) \) for \( i = 1, \ldots, n_1 \).

\( \iff \) \( \tilde{y}_i \circ \{ \tilde{z}_{ij} \}_{j=1}^{n_2} \in \left( C_2^{x_i} \circ (C_3^0, C_3) \right) = \left( C_2 \circ (C_3^0, C_3) \right)^{x_i} \)

for \( i = 1, \ldots, n_1 \).

\( \iff \) \( \tilde{x} \circ \{ \tilde{y}_i \circ \{ \tilde{z}_{ij} \}_{j=1}^{n_2} \}_{i=1}^{n_1} \in Q \)
which gives a one to one correspondence between the elements of $\mathcal{P}$ and the elements of $\mathcal{Q}$. Also, it can be checked that both $\bar{c}$ in $\mathcal{P}$ and its corresponding element

$$\bar{c}' = \bar{x} \circ \{ \bar{y}_i \circ \{ \bar{z}_{ij} \}_{j=1}^{n_2} \}_{i=1}^{n_1}$$

in $\mathcal{Q}$ are equal to the $n_1n_2n_3$-tuple

$$\left( z_{11}^1, z_{21}^2, \ldots, z_{1n_2}^1, z_{2n_2}^2, \ldots, z_{1n_2}^{n_2}, z_{2n_2}^{n_2}, \ldots, z_{1n_2}^{n_3}, z_{2n_2}^{n_3}, \ldots, z_{1n_2}^{n_3} \right).$$

Thus $\bar{c} = \bar{c}'$ which proves that $\mathcal{P} = \mathcal{Q}$ and so the composition is associative. □

Let $\mathcal{C}_I$ be a binary code and $\mathcal{C}_I^o$ a fixed subcode of $\mathcal{C}_I$ of codimension one. In the following we write $\mathcal{C}_I \circ \mathcal{C}_I$ for $\mathcal{C}_I \circ (\mathcal{C}_I^o, \mathcal{C}_I)$ which is the composition of $\mathcal{C}_I$ with itself using $\mathcal{C}_I^o$. Let

$$\mathcal{C}_I^m = \left( \left( \left( \left( \mathcal{C}_I \circ \mathcal{C}_I \right) \circ \mathcal{C}_I \right) \circ \ldots \circ \mathcal{C}_I \right) \right)$$

where $m$ is a positive integer and the composition at each stage uses $\mathcal{C}_I^o$.

**Corollary 2.2.32** $\mathcal{C}_I^m = \mathcal{C}_I \circ \mathcal{C}_I^{m-1}$.

**Proof:** From theorem 2.2.31, the composition is associative. So

$$\mathcal{C}_I^m = \left( \left( \left( \mathcal{C}_I \circ \mathcal{C}_I \right) \circ \mathcal{C}_I \right) \circ \ldots \circ \mathcal{C}_I \right)$$

$$= \left( \mathcal{C}_I \circ \left( \left( \mathcal{C}_I \circ \mathcal{C}_I \right) \circ \ldots \circ \mathcal{C}_I \right) \right) = \mathcal{C}_I \circ \mathcal{C}_I^{m-1}$$

which proves the corollary. □
Theorem 2.2.33  

The minimum distance of $C_f^m$ is

$$d = \begin{cases} 
    d_f^0, & \text{if } d_f = d_f^0, \\
    \min\{d_f^0, (d_f^1)^m\}, & \text{if } d_f = d_f^1.
\end{cases}$$

Proof: Follows from corollary 2.2.13. □

Corollary 2.2.34  

If $d_f^0 \neq 0$ and $d_f^1 > 1$, then the minimum distance $d$ of $C_f^m$ is $d_f^0$ for all $m \geq m_0$ for some $m_0$.

Proof: Since $d_f^1 > 1$, we can find a minimum $m_0$ such that $(d_f^1)^{m_0} > d_f^0$. Then $(d_f^1)^m \geq (d_f^1)^{m_0} > d_f^0$ for $m \geq m_0$ and the corollary follows from theorem 2.2.33. □

Using Theorem 2.2.29 which gives the weight enumerator of $C_{E \oplus (C_f^0, C_f)}$ in terms of the weight enumerators of $C_E$, $C_f^0$, and $C_f$, we get the following recurrence formula for the weight enumerator of $C_f^m$.

Theorem 2.2.35

$$W_{C_f^m}(x, y) = W_{C_f}(W_{C_f^{m-1}}(x, y), W_{C_f^{m-1}}(x, y)).$$

(2.69)

Proof: Since $C_f^m = C_f \circ C_f^{m-1}$ by Corollary 2.2.32, this theorem follows from Theorem 2.2.29. □

2.3 A Composition of Codes over an Arbitrary Finite Field

In this section, we compose codes that are over an arbitrary finite field.

Let $q = p^m$ where $p$ is a prime number and $F_q$ be a field of order $q$. Let $C_f$ be an $[n_f, k_f]$ linear code over $F_q$ and $C_f^0$ be a subcode of $C_f$ of codimension 1. Then the
quotient space \( C/I_i \) has dimension one and so any nonzero element \( \bar{a} + C_i^\alpha \) in \( C/I_i \) forms a basis of \( C/I_i \). Thus

\[
\frac{C}{I_i} = \left\{ \alpha(\bar{a} + C_i^\alpha) : \bar{a} \text{ a fixed element of } C_i \setminus C_i^\alpha, \alpha \in F_q \right\}. 
\]

If we denote \( \alpha(\bar{a} + C_i^\alpha) \) by \( C_i^\alpha \), then

\[
C_i = \bigcup_{\alpha \in F_q} C_i^\alpha. 
\]

Also, we note that

\[
C_i^\alpha \cap C_i^\beta = \emptyset \text{ for } \alpha \neq \beta \in F_q. 
\]

Since both \( C/I_i \) and \( F_q \) are linear spaces of dimension one over \( F_q \) with \( \{\bar{a} + C_i^\alpha\} \) and \( \{1\} \) as their bases, there is vector space isomorphism \( \phi_{\bar{a}} : \frac{C}{I_i} \rightarrow F_q \) that sends \( \bar{a} + C_i^\alpha \) to 1. Then, for \( \alpha \in F_q \),

\[
\phi_{\bar{a}}(C_i^\alpha) = \phi_{\bar{a}}(\alpha(\bar{a} + C_i^\alpha)) = \alpha \phi_{\bar{a}}(\bar{a} + C_i^\alpha) = \alpha.1 = \alpha.
\]

Since \( C_i^\alpha \) is a subspace of \( C_i \), there is a canonical linear map \( \psi \) from \( C_i \) to \( C/I_i \) with \( C_i^\alpha \) as the kernel. Then, the composition \( \phi_{\bar{a}} \circ \psi : C_i \rightarrow F_q \) is a linear functional with \( \phi_{\bar{a}} \circ \psi(\bar{c}) = \alpha \) for all \( \bar{c} \in C_i^\alpha \) and the kernel of \( \phi_{\bar{a}} \circ \psi \) is \( C_i^\alpha \). Thus each subcode of \( C_i \) of codimension one induces a nontrivial linear functional of \( C_i \).

Conversely, the kernel of any nontrivial linear functional of \( C_i \) is a subspace of \( C_i \) of codimension one. Hence there is a correspondence between the subspaces of \( C_i \) of codimension one and the set of nontrivial linear functionals of \( C_i \). This correspondence is not necessarily one-to-one.
Let $C_E$ and $C_I$ be $[n_E, k_E]$ and $[n_I, k_I]$ linear codes over $F_q$ respectively, with $C_j^\alpha$ a subcode of $C_I$ of codimension one. Pick a vector $\alpha \in C_I \setminus C_j^\alpha$ and fix it. Then from (2.71), we get

$$C_I = \bigcup_{\alpha \in F_q} C_j^\alpha$$

where $C_j^\alpha = \alpha + C_j$ and $C_j^\alpha = \alpha(\alpha + C_j^\alpha) = \alpha\alpha + C_j^\alpha$. Also for $\alpha, \beta$ in $F_q$, we have

$$C_j^\alpha + C_j^\beta = \alpha(\alpha + C_j^\alpha) + \beta(\alpha + C_j^\beta) = (\alpha + \beta)(\alpha + C_j^\alpha)$$

$$= C_j^{\alpha + \beta} \quad (2.73)$$

and

$$\beta C_j^\alpha = \beta(\alpha + C_j^\alpha) = \beta\alpha + C_j^\alpha = C_j^{\beta\alpha}. \quad \quad (2.74)$$

We note that for $\alpha \in F_q$,

$$|C_j^\alpha| = |C_j| = q^{k_I-1}. \quad \quad (2.75)$$

The definition of the composition of $C_E$, $C_I$ using $C_j^\alpha$ is analogous to the one for the binary case.

**Definition 2.3.1** For $\bar{y} = (y_1, \ldots, y_{n_E})$ in $C_E$, a subset $\{\bar{c}_i\}_{i=1}^{n_E}$ of $C_I$ is called a suitable set of $\bar{y}$ if $\bar{c}_i \in C_j^\alpha$ for $i = 1, \ldots, n_E$.

Since $C_j^\alpha \neq \emptyset$ for any $\alpha$ in $F_q$, each $\bar{y} \in C_E$ has at least one suitable set from $C_I$; but it can have more than one.

**Definition 2.3.2** If $\bar{y}$ is a vector in $C_E$ and $\{\bar{c}_i\}_{i=1}^{n_E}$ a suitable set of $\bar{y}$ from $C_I$ where $\bar{c}_i = (c_{i1}, c_{i2}, \ldots, c_{in_I})$, then the composition of $\bar{y}$ and $\{\bar{c}_i\}_{i=1}^{n_E}$ denoted by $\bar{y} \circ \{\bar{c}_i\}_{i=1}^{n_E}$ is defined as

$$\bar{y} \circ \{\bar{c}_i\}_{i=1}^{n_E} = (c_{11}, \ldots, c_{n_E1}; \ldots; c_{n_I1}, \ldots, c_{n_E n_I}). \quad \quad (2.76)$$
Like before, for a fixed $\bar{y} \in \mathcal{C}_E$, we have

$$\bar{y} \circ (\mathcal{C}_F^n, \mathcal{C}_I) = \left\{ \bar{y} \circ \{\bar{c}_i\}_{i=1}^{n_E} : \{\bar{c}_i\}_{i=1}^{n_E} \subseteq \mathcal{C}_I \text{ and } \{\bar{c}_i\}_{i=1}^{n_E} \text{ a suitable set of } \bar{y} \right\}. \quad (2.77)$$

**Definition 2.3.3** The composition of $\mathcal{C}_E$ and $\mathcal{C}_I$ using $\mathcal{C}_F^n$ is

$$\mathcal{C} = \mathcal{C}_E \circ (\mathcal{C}_F^n, \mathcal{C}_I) = \bigcup_{\bar{y} \in \mathcal{C}_E} \bar{y} \circ (\mathcal{C}_F^n, \mathcal{C}_I).$$

Clearly $\mathcal{C} \subseteq F_q^{n_E n_I}$.

**Lemma 2.3.4** If $\bar{c} \in \mathcal{C}_E \circ (\mathcal{C}_F^n, \mathcal{C}_I)$, then $\bar{c}$ has a unique representation of the form $\bar{y} \circ \{\bar{c}_i\}_{i=1}^{n_E}$ where $\bar{y} = (y_1, \ldots, y_{n_E}) \in \mathcal{C}_E$ and $\bar{c}_i \in \mathcal{C}_i^{n_h}$ for $i = 1, \ldots, n_E$.

**Proof:** The proof of this lemma is similar to the proof of Lemma 2.2.4 in the binary case. □

**Theorem 2.3.5** If $\mathcal{C}_E$ and $\mathcal{C}_I$ are linear codes over $F_q$ and $\mathcal{C}_F^n$ is a subcode of $\mathcal{C}_I$ of codimension one, then $\mathcal{C} = \mathcal{C}_E \circ (\mathcal{C}_F^n, \mathcal{C}_I)$ is also a linear code over $F_q$.

**Proof:** The proof for showing that $\mathcal{C}$ is closed under addition is similar to the proof of the Theorem 2.2.7 in the binary case. To show $\mathcal{C}$ is closed under scalar multiplication over $F_q$, let $\bar{y} \circ \{\bar{c}_i\}_{i=1}^{n_E} \in \mathcal{C}$ and $\alpha \in F_q$ where $\bar{y} = (y_1, \ldots, y_{n_E})$. Then $\bar{c}_i \in \mathcal{C}_i^{n_h}$. So from (2.74), we get $\alpha \bar{c}_i \in \mathcal{C}_i^{n_h}$. But $\mathcal{C}_E$ and $\mathcal{C}_I$ are vector spaces and so $\alpha \bar{y} \in \mathcal{C}_E$ and $\alpha \bar{c}_i \in \mathcal{C}_I$. Therefore $\{\alpha \bar{c}_i\}_{i=1}^{n_E}$ is a suitable set of $\alpha \bar{y}$ and $(\alpha \bar{y}) \circ \{\alpha \bar{c}_i\}_{i=1}^{n_E} \in \mathcal{C}$. It can be checked that

$$\alpha \left( \bar{y} \circ \{\bar{c}_i\}_{i=1}^{n_E} \right) = (\alpha \bar{y}) \circ \{\alpha \bar{c}_i\}_{i=1}^{n_E}. \quad (2.78)$$
Thus \( \alpha(\overline{y} \circ \{c_i\}_{i=1}^{n_E}) \in \mathcal{C} \) and so \( \mathcal{C} \) is closed under scalar multiplication also. Hence \( \mathcal{C} \) is a linear code over \( F_q \). 

Next we find the dimension of \( \mathcal{C} = \mathcal{C}_E \circ (\mathcal{C}^o_i, \mathcal{C}_I) \).

**Lemma 2.3.6**  
For all \( \overline{y} \in \mathcal{C}_E \), \( |\overline{y} \circ (\mathcal{C}^o_i, \mathcal{C}_I)| = \left( |\mathcal{C}_I|/q \right)^{n_E} \).

**Proof:** Since for \( \alpha \in F_q \), by definition \( \mathcal{C}^o_i \) is a coset of \( \mathcal{C}_I \), and using (2.75), we get

\[
|\mathcal{C}^o_i| = |\mathcal{C}_I| = \frac{|\mathcal{C}_I|}{q}.
\]

Using this fact, the rest of the proof is similar to the proof of the corresponding result in the binary case.

**Lemma 2.3.7**  
If \( \overline{y} \neq \overline{y}' \) are two vectors of \( \mathcal{C}_E \), then \( \overline{y} \circ (\mathcal{C}^o_i, \mathcal{C}_I) \) and \( \overline{y}' \circ (\mathcal{C}^o_i, \mathcal{C}_I) \) are disjoint.

**Proof:** The proof of this result is similar to the proof of the Lemma 2.2.9 in the binary case.

**Theorem 2.3.8**  
If \( \mathcal{C}_E \) and \( \mathcal{C}_I \) are linear codes over \( F_q \), then the composition \( \mathcal{C} = \mathcal{C}_E \circ (\mathcal{C}^o_i, \mathcal{C}_I) \) is an \([n, k] \) linear code over \( F_q \) where \( n = n_E n_I \) and

\[
k = (k_I - 1)n_E + k_E.
\]

**Proof:** The proof of this theorem uses the Lemmas 2.3.6, 2.3.7 and the Theorem 2.3.5, and is similar to the proof of the Theorem 2.2.10 in the binary case.
2.3.1 Minimum distance of the Composition

Let $d_E, d_i, d_i^0$ and $d_i^1$ be the minimum distances of $C_E, C_i, C_i^0$ and $C_i^1$ respectively. Since for $\alpha \neq 0$ in $F_q$, we have

$$C_i^\alpha = \alpha(C_i^0 + C_i^1) = \alpha C_i^1,$$

we get

$$\min \text{ weight of } C_i^\alpha = \min \text{ weight of } C_i^1 = d_i^1.$$

So $d_i = \min\{d_i^0, d_i^1\}$. We can find $\overline{u} \in C_i^\alpha$ and $\overline{v} \in C_i^1$ with $w_t(\overline{u}) = d_i^0$ and $w_t(\overline{v}) = d_i^1$. Then $\alpha\overline{u} \in C_i^\alpha$ and $w_t(\alpha\overline{u}) = w_t(\overline{v}) = d_i^1$. The following theorem gives the relationship between the minimum distance of $C_E \circ (C_i^\alpha, C_i)$ and the minimum distances of $C_E$ and $C_i$.

**Theorem 2.3.9** The minimum distance of $C = C_E \circ (C_i^\alpha, C_i)$ is $d$ where

$$d = \begin{cases} d_i^0, & \text{if } d_i = d_i^0, \\ \min\{d_i^0, d_E d_i^1\}, & \text{if } d_i = d_i^1. \end{cases}$$ (2.79)

**Proof:** Let $\overline{y} = (y_1, \ldots, y_{n_E}) \in C_E$ and $\{\overline{c}_i\}_{i=1}^{n_E}$ be a suitable set of $\overline{y}$ from $C_i$ with at least one $\overline{c}_i \neq \overline{e}$. Then $\overline{c}_i \in C_i^{n_E}$ and $\overline{y} \circ \{\overline{c}_i\}_{i=1}^{n_E}$ is in $C = C_E \circ (C_i^\alpha, C_i)$. Also

$$w_t(\overline{y} \circ \{\overline{c}_i\}_{i=1}^{n_E}) = \sum_{i=1}^{n_E} w_t(\overline{c}_i).$$ (2.80)

If $\overline{y} = \overline{e}$, then $\{\overline{w}_i\}_{i=1}^{n_E}$ with

$$\overline{w}_1 = \overline{u} \quad \text{and} \quad \overline{w}_i = \overline{e} \quad \text{for } i \geq 2,$$

is a suitable set of $\overline{y} = \overline{e}$. Then, just like in Theorem 2.2.12, since

$$w_t(\overline{y} \circ \{\overline{c}_i\}_{i=1}^{n_E}) = \sum_{i=1}^{n_E} w_t(\overline{c}_i) \geq \sum_{i=1}^{n_E} w_t(\overline{w}_i)$$
for all nonzero \( \overline{y} \circ \{\tilde{r}_i\}_{i=1}^{n_E} \in \overline{o} \circ (C_i^o, C_I) \), we get
\[
\min \text{wt}(\overline{o} \circ (C_i^o, C_I)) = \text{wt}(\{\overline{m}_i\}_{i=1}^{n_E}) = \sum_{i=1}^{n_E} \text{wt}(\overline{m}_i) = \text{wt}(\overline{u}) = d_i^0. \tag{2.81}
\]
If \( \overline{y} \neq \overline{o} \), then \( \{\overline{m}_i\}_{i=1}^{n_E} \) with \( \overline{m}_i = \overline{o} \) if \( y_i = 0 \) and \( \overline{m}_i = y_i \overline{o} \) if \( y_i \neq 0 \), is a suitable set of \( \overline{y} \). Then, using the same reasoning as in Theorem 2.2.12 for \( \overline{y} \neq \overline{o} \), since
\[
\sum_{i=1}^{n_E} \text{wt}(\tilde{r}_i) \geq \sum_{i=1}^{n_E} \text{wt}(\overline{m}_i) \text{ for all } \overline{y} \circ \{\tilde{r}_i\}_{i=1}^{n_E} \in C_E \circ (C_i^o, C_I) \text{ in this case, we get}
\]
\[
\min \text{wt}(\overline{y} \circ (C_i^o, C_I)) = \text{wt}(\{\overline{m}_i\}_{i=1}^{n_E})
= \sum_{i=1}^{n_E} \text{wt}(\overline{m}_i) = \text{wt}(\overline{y}) \text{wt}(\overline{u}) = \text{wt}(\overline{y}) d_i^0 \geq d_E d_i^1. \tag{2.82}
\]
So
\[
\min \text{wt}(C) = \min \text{wt} \left( \bigcup_{\overline{y} \in C_E} \overline{y} \circ (C_i^o, C_I) \right)
= \min \{d_i^0, d_E d_i^1\} \tag{2.83}
= \begin{cases} d_i^0, & \text{if } d_i = d_i^0 \\ \min\{d_i^0, d_E d_i^1\}, & \text{if } d_i = d_i^1 \end{cases} \tag{2.84}
\]
which gives the minimum distance of \( C \).

\[
\square
\]

2.3.2 The Cyclicity of the Composition

In the following all codes are over an arbitrary field \( F_q \).

**Theorem 2.3.10**  
If \( C_E \) is a cyclic code and \( C_i^o \) is a subcode of \( C_I \) of codimension one such that for \( \alpha \in F_q \) all the cosets \( C_i^o \) of \( C_i^o \) are cyclic, then the composition code \( C = C_E \circ (C_i^o, C_I) \) is cyclic.

**Proof:** The proof of this theorem is similar to the proof of Theorem 2.2.17 in the binary case.  \( \square \)
Lemma 2.3.11  If $C^*_j$ is a cyclic subcode of codimension one of $C_I$ such that the coset $C^*_j$ of $C^*_I$ is cyclic, then all the cosets $C^*_I$ of $C^*_I$ are cyclic.

Proof:  Let $\bar{v} = (v_1, v_2, \ldots, v_n, 1) \in C^*_I$ where $\alpha \neq 0$. Then $\bar{v} = \alpha \bar{u}$ for some $\bar{u} = (u_1, u_2, \ldots, u_n) \in C^*_I$, and so $v_i = \alpha u_i$ for $i = 1, \ldots, n$. Thus the cyclic shift of $\bar{v}$ is given by

$$x \bar{v} = (v_n, v_1, v_2, \ldots, v_{n-1}) = (\alpha u_n, \alpha u_1, \alpha u_2, \ldots, \alpha u_{n-1})$$

$$= \alpha (u_n, u_1, u_2, \ldots, u_{n-1}) = \alpha (x \bar{u}). \quad (2.85)$$

Since $\bar{u} \in C^*_I$ and $C^*_I$ is cyclic, we get $x \bar{u} \in C^*_I$. This gives $\alpha (x \bar{u}) \in \alpha C^*_I = C^*_I$. But $\alpha (x \bar{u}) = x \bar{v}$, and so we get $x \bar{v} \in C^*_I$. Hence $C^*_I$ is cyclic. □

Corollary 2.3.12  If $C_E$ is cyclic and $C^*_j$ is a cyclic subcode of $C_I$ of codimension one with $C^*_I$ cyclic, then the composition $C = C_E \circ (C^*_I, C_I)$ is also a cyclic code.

Proof: This corollary follows from Theorem 2.3.10 and the Lemma 2.3.11. □

Corollary 2.3.13  Let $C_E$, $C_I$, and $C^*_I$ be cyclic codes. Also let $\bar{u}(x) \in C_I \setminus C^*_I$ and $C^*_I = \bar{u}(x) + C^*_I$. Then, if $(x - 1)\bar{u}(x) \in C^*_I$ then the composition $C = C_E \circ (C^*_I, C_I)$ is also cyclic.

Proof: Since $(x - 1)\bar{u}(x) \in C^*_I$, we have

$$x \bar{u}(x) + C^*_I = \bar{u}(x) + C^*_I,$$

which gives $xC^*_I = C^*_I$ by using the fact that $C^*_I$ is cyclic. Thus $C^*_I$ is cyclic and the corollary follows from Corollary 2.3.12. □
Theorem 2.3.14  Let \( \mathcal{C}_E \) and \( \mathcal{C}_I \) be cyclic codes with \( \mathcal{C}_E \) nonzero and \( \mathcal{C}_I^0 \) a cyclic subcode of \( \mathcal{C}_I \) of codimension one. Also let

\[
\mathcal{C}_E = \langle g(x) \rangle, \quad \mathcal{C}_I = \langle f(x) \rangle \quad \text{and} \quad \mathcal{C}_I^0 = \langle (x - 1)f(x) \rangle
\]

with \( f(1) \neq 0 \) and \( \mathcal{C}_I^1 = f(x) + \mathcal{C}_I^0 \). Then

\[
\mathcal{C} = \mathcal{C}_E \circ (\mathcal{C}_I^1, \mathcal{C}_I) = \langle g(x)f(x^n_E) \rangle.
\]

Proof:  We note that since \( f(1) \neq 0 \), we have \( f(x) \notin \mathcal{C}_I^0 \).

• First we show that \( g(x)f(x^n_E) \in \mathcal{C} \).

Since \( \mathcal{C}_I^1 = f(x) + \mathcal{C}_I^0 \), for any \( \alpha \in F_q \) we have,

\[
\mathcal{C}_I^0 = \alpha \mathcal{C}_I^1 = \alpha f(x) + \mathcal{C}_I^0.
\]

In particular, \( \alpha f(x) \in \mathcal{C}_I^0 \). Let \( g(x) = \sum_{i=0}^{n_E-1} g_i x^i \). Since \( \mathcal{C}_E \) is nonzero, there is at least one \( g_i \neq 0 \). For \( i = 1, \ldots, n_E \), let \( \overline{c}_i(x) = g_i f(x) \). Then \( \overline{c}_i \in \mathcal{C}_I^0 \) and so \( \{\overline{c}_i(x)\}_{i=0}^{n_E-1} \) is a suitable set of \( g(x) \). Thus \( g(x) \circ \{\overline{c}_i(x)\}_{i=0}^{n_E-1} \in \mathcal{C} \). But

\[
g(x) \circ \{\overline{c}_i(x)\}_{i=0}^{n_E-1} = g(x)f(x^n_E).
\]

Hence \( g(x)f(x^n_E) \in \mathcal{C} \).

• Next we show that \( g(x)f(x^n_E) \) generates \( \mathcal{C} = \mathcal{C}_I \circ (\mathcal{C}_I^0, \mathcal{C}_I) \).

For that, let \( \overline{v}(x) = \overline{y}(x) \circ \{\overline{c}_i(x)\}_{i=0}^{n_E-1} \in \mathcal{C} \) where \( \overline{y} = \sum_{i=0}^{n_E-1} y_i x^i \in \mathcal{C}_E \) and \( \overline{c}_i(x) \in \mathcal{C}_I^0 \). Since \( \mathcal{C}_I^h = y_i f(x) + \mathcal{C}_I^0 \) and \( \mathcal{C}_I^0 = \langle (x - 1)f(x) \rangle \), we get

\[
\overline{v}_i(x) = y_i f(x) + b_i(x)(x - 1)f(x).
\]

(2.87)
for some $b_i(x) \in F_q[x]$. So $\tilde{c}_i(x) = \left( y_i + b_i(x)(x - 1) \right) f(x)$. This gives

$$\tilde{c}_i(x^{n_E}) = \left( y_i + b_i(x^{n_E})(x^{n_E} - 1) \right) f(x^{n_E})$$

for $i = 1, \ldots, n_E$. Thus

$$\tilde{c}(x) = \overline{g}(x) \circ \{\tilde{c}_i(x)\}_{i=0}^{n_E-1} = \sum_{i=0}^{n_E-1} x^i \tilde{c}_i(x^{n_E})$$

$$= \sum_{i=0}^{n_E-1} x^i \left( y_i + b_i(x^{n_E})(x^{n_E} - 1) \right) f(x^{n_E}) = f(x^{n_E}) T(x)$$

where $T(x) = \sum_{i=0}^{n_E-1} x^i \left( y_i + b_i(x^{n_E})(x^{n_E} - 1) \right)$. We claim that $g(x)$ divides $T(x)$. For that, let $\alpha$ be a root of $g(x)$. Then $g(\alpha) = \sum_{i=0}^{n_E-1} y_i \alpha^i = 0$ and $\alpha^{n_E} = 1$. This gives

$$T(\alpha) = \sum_{i=1}^{n_E-1} \alpha^i \left( y_i + b_i(\alpha^{n_E})(\alpha^{n_E} - 1) \right)$$

$$= \sum_{i=1}^{n_E-1} \alpha^i (y_i + 0) = g(\alpha) = 0$$

Thus the roots of $g(x)$ are also roots of $T(x)$. And since $g(x)$ divides $x^{n_E} - 1$, it is separable. Hence $g(x)$ divides $T(x)$. So $T(x) = p(x)g(x)$ for some $p(x) \in F_q[x]$. Consequently $\tilde{c}(x) = p(x) \left( f(x^{n_E}) g(x) \right)$ and $C = \langle g(x) f(x^{n_E}) \rangle$. □

For $C_E$, $C_I$ and $C_I^*$ as in Theorem 2.3.14, the roots of the generating polynomial of the composition code are related to those of $C_E$ and $C_I$ as mentioned below.

Let $(n_E, q) = 1$ and $(n_I, q) = 1$. Then $(n_E n_I, q) = 1$, and so from Lemma 2.2.21, the polynomials $x^{n_E} - 1$, $x^{n_I} - 1$ and $x^{n_E n_I} - 1$ are all separable over $F_q$.

Let $n = n_E n_I$ and $\beta$ be a primitive $n$th root of unity over $F_q$. Let $\alpha = \beta^{n_I}$ and $\gamma = \beta^{n_E}$. Then $\alpha$ is a primitive $n_E$th root of unity and $\gamma$ is a primitive $n_I$th root of
unity over $F_q$. If $g(x)$ and $f(x)$ are the generating polynomials of $C_E$ and $C_I$, then the roots of $g(x)$ are among the powers of $\alpha$ and the roots of $f(x)$ are among the powers of $\gamma$. Like in the binary case, we let

\[ \Omega_E = \{ \alpha^i : g(\alpha^i) = 0, \ 0 \leq i \leq n_E - 1 \} \]  
\[ \Delta_E = \{ i : 0 \leq i \leq n_E - 1 \text{ and } g(\alpha^i) = 0 \} \]  
\[ \Omega_I = \{ \gamma^j : f(\gamma^j) = 0, \ 0 \leq j \leq n_I - 1 \} \]  
\[ \Delta_I = \{ j : 0 \leq j \leq n_I - 1 \text{ and } f(\gamma^j) = 0 \}. \]

Since $f(1) \neq 0$, $0 \not\in \Delta_I$. By definition,

\[ \Delta_E \subseteq \mathbb{Z}_{n_E}, \ \Delta_I \subseteq \mathbb{Z}_{n_I} \setminus \{0\} \]

and

\[ |\Delta_E| = \deg g(x), \ |\Delta_I| = \deg f(x). \]

Let

\[ \Delta = \left\{ \bigcup_{t \in \Delta_I} \left( t + n_I \mathbb{Z}_{n_E} \right) \right\} \cup \{ ln_I : l \in \Delta_E \}. \]

**Lemma 2.3.15**

\[ |\Delta| = \deg f(x)n_E + \deg g(x). \]

**Proof:** The proof of this lemma is similar to Lemma 2.2.23 in the binary case. □

Let

\[ \Omega = \{ \beta^s : s \in \Delta \}. \]
Theorem 2.3.16 \quad \Omega \text{ is the set of roots of the generating polynomial }

\[ P(x) = g(x)f(x^n) \text{ of the composition code } C = C_E \circ (C_I^o, C_I). \]

**Proof:** The proof of this theorem is similar to Theorem 2.2.24 in the binary case. \hfill \Box

### 2.3.3 The Dual code of the Composition

Let \( C_E \) and \( C_I \) be \([n_E, k_E]\) and \([n_I, k_I]\) linear codes over \( F_q \) respectively and \( C_I^o \) a subcode of \( C_I \) of codimension one. We will find the dual of \( C = C_E \circ (C_I^o, C_I) \).

Like in the binary case, here also we have

\[ C_I^o \subseteq C_I \implies (C_I^o)\perp \supseteq C_I^\perp, \quad (2.97) \]

\[ \dim C_I^\perp = n_I - k_I \quad \text{and} \quad \dim (C_I^o)\perp = n_I - (k_I - 1) = n_I - k_I + 1. \quad (2.98) \]

From the dimensions, we notice that \( C_I^\perp \) is a subspace of \((C_I^o)\perp\) of codimension one. Thus we can define the composition \( C_E \circ (C_I^\perp, (C_I^o)\perp) \) with \( C_E^\perp \) as the exterior code and \((C_I^o)\perp\) as the interior code with \( C_I^\perp \) as its subcode of codimension one.

**Lemma 2.3.17** \quad The composition \( C_E^\perp \circ (C_I^\perp, (C_I^o)\perp) \) is a linear code over \( F_q \) of dimension

\[ n_E(n_I - k_I) + (n_E - k_E). \quad (2.99) \]

**Proof:** This lemma follows from the Theorems 2.3.5 and 2.3.8. \hfill \Box
Theorem 2.3.18  If $C_E$ and $C_I$ are linear codes over $F_q$ and $C_I^o$ a subcode of $C_I$ of codimension one, then the dual of their composition $C = C_E \circ (C_I^o, C_I)$ denoted by $C^\perp$ is $C_E^\perp \circ (C_I^\perp, (C_I^o)^\perp)$.

Proof: We first show that $C_E^\perp \circ (C_I^\perp, (C_I^o)^\perp) \subseteq C^\perp$. For that, let
\[
\bar{y} \circ \{\bar{r}_i\}_{i=1}^{n_E} \in C
\]
where
\[
\bar{y} = (y_1, \ldots, y_{n_E}) \in C_E \quad \text{and} \quad \{\bar{r}_i\}_{i=1}^{n_E}
\]
is a suitable set of $\bar{y}$ from $C_I$, and
\[
\bar{w} \circ \{\bar{u}_i\}_{i=1}^{n_E} \in C_E^\perp \circ (C_I^\perp, (C_I^o)^\perp)
\]
where
\[
\bar{w} = (w_1, \ldots, w_{n_E}) \in C_E^\perp \quad \text{and} \quad \{\bar{u}_i\}_{i=1}^{n_E}
\]
is a suitable set of $\bar{w}$ from $(C_I^o)^\perp$. Since $\bar{r}_i \in C_I^o = y_i\bar{u} + C_I^o$ for some fixed $\bar{u} \in C_I \setminus C_I^o$, we get
\[
\bar{r}_i = y_i\bar{u} + \bar{l}_i
\]
for some $\bar{l}_i \in C_I^o$ for $i = 1, \ldots, n_E$.

Similarly, since $\bar{u}_i \in (C_I^\perp)^{w_i} = w_i\bar{b} + (C_I^\perp)$ for some fixed $\bar{b} \in (C_I^o)^\perp \setminus (C_I)^\perp$, we get
\[
\bar{u}_i = w_i\bar{b} + \bar{s}_i
\]
for some $\bar{s}_i \in C_I^\perp$ for $i = 1, \ldots, n_E$. Then the scalar product
\[
\left( \bar{y} \circ \{\bar{r}_i\}_{i=1}^{n_E} \right) \cdot \left( \bar{w} \circ \{\bar{u}_i\}_{i=1}^{n_E} \right) = \sum_{i=1}^{n_E} \bar{r}_i \cdot \bar{u}_i = \sum_{i=1}^{n_E} \left( y_i\bar{u} + \bar{l}_i \right) \cdot \left( w_i\bar{b} + \bar{s}_i \right)
\]
(2.104)
\[
= \sum_{i=1}^{n_E} \left( y_i w_i (\bar{a} \cdot \bar{b}) + y_i \bar{a} \cdot \bar{s}_i + w_i \bar{l}_i \cdot \bar{b} + \bar{l}_i \cdot \bar{s}_i \right).
\] (2.105)

Since \( \bar{a} + C_i^o \subseteq C_i \) and \( \bar{s}_i \in C_i^1 \), we get
\[
\bar{a} \cdot \bar{s}_i = 0 \quad \text{for} \quad i = 1, \ldots, n_E.
\] (2.106)

Similarly, since \( \bar{b} \in (C_i^o)^\perp \setminus C_i^1, \bar{l}_i \in C_i^o \), we get
\[
\bar{l}_i \cdot \bar{b} = 0 \quad \text{for} \quad i = 1, \ldots, n_E.
\] (2.107)

Also, because \( \bar{l}_i \in C_i^o \) and \( \bar{s}_i \in C_i^1 \subseteq (C_i^o)^\perp \), we have
\[
\bar{l}_i \cdot \bar{s}_i = 0 \quad \text{for} \quad i = 1, \ldots, n_E.
\] (2.108)

Thus from (2.105), (2.106), (2.107) and (2.108), we get
\[
\left( \bar{y} \circ \{\bar{e}_i\}_{i=1}^{n_E} \right) \cdot \left( \bar{w} \circ \{\bar{u}_i\}_{i=1}^{n_E} \right) = \sum_{i=1}^{n_E} \left( y_i w_i (\bar{a} \cdot \bar{b}) \right) = (\bar{a} \cdot \bar{b}) \left( \sum_{i=1}^{n_E} y_i w_i \right)
= (\bar{a} \cdot \bar{b}) (\bar{y} \cdot \bar{w}) = (\bar{a} \cdot \bar{b}) 0 = 0
\] (2.109)

since \( \bar{y} \cdot \bar{w} = 0 \) as \( \bar{y} \in C_E \) and \( \bar{w} \in (C_E)^\perp \). Therefore \( (C_E^r \circ (C_i^1, (C_i^o)^\perp)) \subseteq C_i^\perp \).

Also, it can be checked that \( \dim(C_E^r \circ (C_i^1, (C_i^o)^\perp)) = \dim C_i^\perp \).

Hence \( C_i^\perp = (C_E^r \circ (C_i^1, (C_i^o)^\perp)) \) and this proves the theorem. \( \square \)

2.3.4 Complete Weight Enumerator for the Composition Code

Let the elements of \( F_q \) be denoted by \( \alpha_0 = 0, \alpha_1, \ldots, \alpha_{q-1} \) in some fixed order.

The weight enumerator we are going to consider classifies codewords \( \bar{c} \) according to the number of times each field element \( \alpha_i \) occurs in \( \bar{c} \).
Definition 2.3.19 For \( \bar{c} = (c_1, c_2, \ldots, c_n) \) in \( F_q^n \) and \( \alpha \) in \( F_q \), we let

\[
 w_\alpha(\bar{c}) = |\{r_i : c_i = \alpha \text{ where } 1 \leq i \leq n\}|. \tag{2.110}
\]

Thus, we see that \( w_\alpha(\bar{c}) \) is the number of components \( c_i \) of \( \bar{c} \) that are equal to \( \alpha \).

Definition 2.3.20 Let \( C \) be an \([n, k]\) linear code over \( F_q \). Then the complete weight enumerator of \( C \) is defined to be

\[
 W_C(x_0, x_1, \ldots, x_{q-1}) = \sum_{\bar{c} \in C} x_{w_0(\bar{c})} x_{w_1(\bar{c})} \ldots x_{w_{q-1}(\bar{c})}. \tag{2.111}
\]

This definition is as in [9].

For \( \beta \in F_q \), let \( W_{C_1}^\beta(x_0, x_1, \ldots, x_{q-1}) \) be the complete weight enumerator of the coset \( C_1^\beta \) of \( C_1 \). Then for \( \beta \neq 0 \), the complete weight enumerator of \( C_1^\beta \) and that of \( C_1 \) are related as follows.

Theorem 2.3.21 For \( \beta \in F_q \setminus \{0\} \),

\[
 W_{C_1}^\beta(x_0, x_1, \ldots, x_{q-1}) = W_{C_1}(x_{\beta_0}, x_{\beta_1}, \ldots, x_{\beta_{q-1}}). \tag{2.112}
\]

Proof: From the definition of the complete weight enumerator of the coset \( C_1^\beta \), we have

\[
 W_{C_1}^\beta(x_0, x_1, \ldots, x_{q-1}) = \sum_{\bar{c} \in C_1} \prod_{\alpha \in F_q} x_{w_\alpha(\bar{c})} = \sum_{\bar{c} \in C_1} \prod_{\alpha \in F_q} x_{w_\alpha(\beta \bar{c})} \text{ since } C_1^\beta = \beta C_1. \\
 = \sum_{\bar{c} \in C_1} \prod_{\alpha \in F_q} x_{w_{\beta^{-1} \alpha}(\bar{c})} = \sum_{\bar{c} \in C_1} \prod_{\alpha \in F_q} x_{w_{\beta \alpha}(\bar{c})} \text{ since } \beta \alpha \in F_q \text{ iff } \alpha \in F_q. \\
 = W_{C_1}(x_{\beta_0}, x_{\beta_1}, \ldots, x_{\beta_{q-1}}). \tag{2.112}
\]
which proves the theorem.

For $\bar{y} \in F_q^{n_E}$, let the complete weight enumerator of $\bar{y}$ be

$$W_{\bar{y}}(x_{\alpha_0}, x_{\alpha_1}, \ldots, x_{\alpha_{q-1}}) = \prod_{\beta \in F_q} x_{\beta}^{w_{\beta}(\bar{y})}. \quad (2.113)$$

Let $W_{C_E}$ be the complete weight enumerator of $C_E$. Then

$$W_{C_E}(x_{\alpha_0}, x_{\alpha_1}, \ldots, x_{\alpha_{q-1}}) = \sum_{\bar{y} \in C_E} \prod_{\beta \in F_q} x_{\beta}^{w_{\beta}(\bar{y})} \quad (2.114)$$

$$= \sum_{\bar{y} \in C_E} W_{\bar{y}}(x_{\alpha_0}, x_{\alpha_1}, \ldots, x_{\alpha_{q-1}}). \quad (2.115)$$

Then the complete weight enumerator $W_C$ of the composition $C = C_E \circ (C_i^\alpha, C_I)$ can be expressed in terms of the complete weight enumerator $W_{C_E}$ and the complete weight enumerators $W_{C_{E_i}^\alpha}$ of the cosets $C_{E_i}^\alpha$ of $C_I^\alpha$ for $\alpha_i \in F_q$, as in the following theorem. In the following, we write $\bar{y} \circ C_I$ for $\bar{y} \circ (C_i^\alpha, C_I)$.

**Theorem 2.3.22** The complete weight enumerator of the composition code $C = C_E \circ (C_i^\alpha, C_I)$ is given by the following composition:

$$W_C(x_{\alpha_0}, x_{\alpha_1}, \ldots, x_{\alpha_{q-1}}) = W_{C_E}(W_{C_{E_i}^\alpha_{I_1}}, W_{C_{E_i}^\alpha_{I_2}}, \ldots, W_{C_{E_i}^\alpha_{I_{q-1}}}). \quad (2.116)$$

**Proof:** Let $\bar{y} \in C_I$. Then the complete weight enumerator of $\bar{y} \circ C_I$ is

$$W_{\bar{y} \circ C_I}(x_{\alpha_0}, x_{\alpha_1}, \ldots, x_{\alpha_{q-1}}) = \sum_{\bar{t} \in \bar{y} \circ C_I} W_{\bar{t}}(x_{\alpha_0}, x_{\alpha_1}, \ldots, x_{\alpha_{q-1}})$$

$$= \sum_{\bar{t} \in \bar{y} \circ C_I} \left( \prod_{\beta \in F_q} x_{\beta}^{w_{\beta}(\bar{t})} \right) \text{ where } \bar{t} = \bar{y} \circ \{\bar{t_i}^E\}_{i=1}^{n_E}$$

$$= \sum_{\bar{y} \circ (\bar{t_i})_{i=1}^{n_E} \in \bar{y} \circ C_I} \left( \prod_{\beta \in F_q} x_{\beta}^{w_{\beta}(\bar{y} \circ (\bar{t_i})_{i=1}^{n_E})} \right)$$
\[ W_C(x_{\alpha_0}, x_{\alpha_1}, \ldots, x_{\alpha_{q-1}}) = \sum_{\bar{y} \in \mathcal{C}_E} W_{\mathcal{C}_L}^0(x_{\alpha_0}, x_{\alpha_1}, \ldots, x_{\alpha_{q-1}}) \]
\[ = \sum_{\bar{y} \in \mathcal{C}_E} W_{\mathcal{C}_L}^0 W_{\mathcal{C}_L}^1 \cdots W_{\mathcal{C}_L}^{\alpha_{q-1}} \text{ using (2.117)} \]
\[ = W_{\mathcal{C}_E}(W_{\mathcal{C}_L}^{\alpha_0}, W_{\mathcal{C}_L}^{\alpha_1}, \ldots, W_{\mathcal{C}_L}^{\alpha_{q-1}}) \quad (2.118) \]

using (2.115). And this proves the theorem. \qed

From Theorems (2.3.21) and (2.3.22), we note that to obtain the complete weight enumerator of the composition code \( \mathcal{C} = \mathcal{C}_E \circ (\mathcal{C}_L^0, \mathcal{C}_L) \), it is sufficient to know the complete weight enumerators of \( \mathcal{C}_E, \mathcal{C}_L^0 \) and that of \( \mathcal{C}_L^1 \).
2.3.5 Decoding and Complexity

From Theorem 2.3.9, the minimum distance of $C = C_E \circ (C_i^o, C_I)$ is $d$, where

$$d = \begin{cases} d_i^0, & \text{if } d_i = d_i^0, \\ \min\{d_i^0, d_i^1\}, & \text{if } d_i = d_i^1. \end{cases}$$

(2.119)

In this section, we assume that the minimum distance $d$ of $C_E \circ (C_i^o, C_I)$ is the same as that of $C_I$. So $d = d_i$.

Let $[x]$ denote the greatest integer less than or equal to $x$.

**Theorem 2.3.23**

A code with minimum distance $d$ can correct $[\frac{1}{2}(d-1)]$ errors. If $d$ is even, the code can simultaneously correct $\frac{1}{2}(d-2)$ errors and detect $d/2$ errors.

This result is as in [9].

**Definition 2.3.24**

Let $C$ be a code of length $n$ over a finite field $F$. Then a decoding algorithm for $C$ is a function $D$ from $F^n$ into $C$.

The above definition is as in [8].

Let $C_E$ and $C_I$ be $[n_E, k_E]$ and $[n_I, k_I]$ codes over $F_q$. In the following, we describe a decoding algorithm for $C_E \circ (C_i^o, C_I)$.

**Definition 2.3.25**

Let $D_I$ be an algorithm for decoding the vectors of $F^n_{q^1}$ to $C_I$ that corrects random errors up to $[\frac{1}{2}(d - 1)]$, which is the number guaranteed by the minimum distance in Theorem 2.3.23.

**Decoding algorithm for $C_E \circ (C_i^o, C_I)$ and its Complexity:**
Let \( e = \left\lceil \frac{1}{2}(d-1) \right\rceil \) where \( d \) is the minimum distance of \( C_E \circ (C_I^o, C_I) \). As mentioned before, we assume that \( d = d_i \).

Assume that the interior code \( C_I \) has a decoding algorithm \( D_I \) as defined in (2.3.25) that can correct up to \( e \) random errors. We develop a decoding algorithm \( D \) for \( C_E \circ (C_I^o, C_I) \) using \( D_I \), that can correct up to \( e \) random errors which is the number guaranteed by the minimum distance of \( C_E \circ (C_I^o, C_I) \).

Let \( \vec{v} = (z_{11}, \ldots, z_{n_E 1}; \ldots; z_{1n_I}, \ldots, z_{n_E n_I}) \in F_q^{n_E n_I} \) be a received vector with number of errors less than or equal to \( e \). Let \( \vec{v}_i = (z_{i1}, z_{i2}, \ldots, z_{in_i}) \) for \( i = 1, \ldots, n_E \). Then \( \vec{v}_i \in F_q^{n_i} \) for \( i = 1, \ldots, n_E \) and the number of of errors in each \( \vec{v}_i \) is less than or equal to \( e \). So we can use \( D_I \) to decode \( \vec{v}_i \). Since \( D_I \) can correct all errors in a vector if the number of errors occurring is less than or equal to \( e \), \( D_I \) will decode \( \vec{v}_i \) to a unique code word in \( C_I \). For \( i = 1, 2, \ldots, n_E \), let

\[
D_I(\vec{v}_i) = \vec{c}_i
\]

(2.120)

and \( \vec{c}_i = (c_{i1}, c_{i2}, \ldots, c_{in_i}) \). Now define the decoding algorithm for \( C_E \circ (C_I^o, C_I) \) to be

\[
D(\vec{v}) = \vec{c}
\]

(2.121)

where

\[
\vec{c} = (c_{11}, c_{21}, \ldots, c_{n_E 1}; \ldots; c_{1n_I}, c_{2n_I}, \ldots, c_{n_E n_I}).
\]

(2.122)

Then

\[
\vec{c} = \vec{y} \circ \{\vec{c}_i\}_{i=1}^{n_E}
\]

(2.123)

for some \( \vec{y} \in F_q^{n_E} \). Since the number of errors in \( \vec{z} \) is less than or equal to \( e \), and from the definition of \( D \) in (2.121), \( D \) has corrected all the errors in \( \vec{z} \), and so
\( D(\bar{z}) = \bar{c} \in C_E \circ (C_1^o, C_1) \). Thus \( D \) is a decoding algorithm for \( C_E \circ (C_1^o, C_1) \) that corrects any number of errors less than or equal to \( c \).

Clearly, the complexity of the algorithm \( D \) is \( n_E \) times the complexity of \( D_1 \).

**Definition 2.3.26** If the only possible errors in a vector \( \bar{v} \) occur among \( b \) successive components, then \( \bar{v} \) is said to have a **burst** error of length \( b \).

This definition is as in [10].

**Theorem 2.3.27** If \( C_1 \) can correct burst errors of length \( b \), then the composition code \( C_E \circ (C_1^o, C_1) \) can correct burst errors of length \( n_E b \).

**Proof:** Let \( \bar{z} = (z_{11}, \ldots, z_{n_E 1}; \ldots; z_{1n_1}, \ldots, z_{n_E n_1}) \in F_q^{n_E n_1} \) be a received vector with a burst error of length \( n_E b \). Then, that burst of length \( n_E b \) in \( \bar{z} \) will overlap each of the vectors \( \bar{v}_i = (z_{i1}, z_{i2}, \ldots, z_{in_1}) \) for \( i = 1, \ldots, n_E \), in at most \( b \) consecutive coordinates. By assumption, any burst error of length \( b \) in \( C_1 \) can be corrected and so, for \( i = 1, \ldots, n_E \), all the errors in \( \bar{v}_i \) can be corrected. Consequently, all the errors in \( \bar{z} \) can be corrected. Thus the composition code has a burst error correction capability of length \( n_E b \). \( \square \)

**2.4 A More General Composition**

In our composition of codes so far, we used an interior code \( C_1 \) and a subcode \( C_1^o \) of \( C_1 \) of codimension one. In fact, we can take \( C_1^o \) to be a proper subspace of \( C_1 \) of any codimension and define a more general composition. In this section, we describe the generalization when \( C_1^o \) has codimension two in \( C_1 \). The generalization is similar if \( C_1^o \) is a subspace of \( C_1 \) of higher codimension.
Let $F_q$ be an arbitrary finite field and $C_I$ an $[n_I, k_I]$ linear code over $F_q$ and $C_I^o$ be a subcode of $C_I$ of dimension $k_I - 2$. Then, the quotient space $C_I/C_I^o$ over $F_q$ has dimension 2. Pick a basis $\{\tilde{a} + C_I, \tilde{b} + C_I^o\}$ for $C_I/C_I^o$ and fix it. Thus

$$C_I/C_I^o = \{\alpha(\tilde{a} + C_I^o) + \beta(\tilde{b} + C_I^o) : \alpha, \beta \in F_q\}.$$  \hfill (2.124)

For an ordered pair $(\alpha, \beta) \in F_q \times F_q$, let $C_I^{(\alpha, \beta)} = \alpha(\tilde{a} + C_I^o) + \beta(\tilde{b} + C_I^o)$. Then for $(\alpha, \beta) \neq (\gamma, \delta)$, $C_I^{(\alpha, \beta)} \neq C_I^{(\gamma, \delta)}$ and

$$C_I = \bigcup_{(\alpha, \beta) \in F_q \times F_q} C_I^{(\alpha, \beta)}.$$  \hfill (2.125)

From the definition of $C_I^{(\alpha, \beta)}$, we note that for $(\alpha, \beta)$ and $(\gamma, \delta) \in F_q \times F_q$, and $\nu \in F_q$, we have

$$C_I^{(\alpha, \beta)} + C_I^{(\gamma, \delta)} = C_I^{(\alpha + \gamma, \beta + \delta)} \quad \text{and} \quad \nu C_I^{(\alpha, \beta)} = C_I^{(\nu \alpha, \nu \beta)}.$$  \hfill (2.126)

Also

$$|C_I^{(\alpha, \beta)}| = |C_I^o| = q^{k_I - 2}.$$  \hfill (2.127)

Let $F_{q^2}$ be a field of size $q^2$ containing $F_q$. Then both $C_I/C_I^o$ and $F_{q^2}$ are linear spaces of dimension two over $F_q$ and so are isomorphic as vector spaces over $F_q$. Therefore we can find a linear isomorphism $\phi$ over $F_q$ between those two spaces. We pick such a $\phi$ and fix it.

Let $\psi$ be the canonical linear map from $C_I$ to $C_I/C_I^o$. Then the composition $\phi \circ \psi : C_I \longrightarrow F_{q^2}$ is a linear map over $F_q$ such that

$$\phi \circ \psi(\tilde{c}) = \alpha \phi(\tilde{a} + C_I^o) + \beta \phi(\tilde{b} + C_I^o)$$

for all $\tilde{c} \in C_I^{(\alpha, \beta)}$ where $(\alpha, \beta) \in F_q \times F_q$. 

Thus there is a one to one correspondence between the cosets of $\mathcal{C}_1^n$ in $\mathcal{C}_I$ and the elements of $F_{q^2}$.

To define the composition, we take the exterior code $\mathcal{C}_E$ to be an $[n_E, k_E]$ linear code over $F_{q^2}$ in this case.

**Definition 2.4.1** For $\overline{y} = (y_1, \ldots, y_{n_E})$ in $\mathcal{C}_E$, a subset $\{\overline{c}_i\}_{i=1}^{n_E}$ of $\mathcal{C}_I$ is called a suitable set of $\overline{y}$ if $\overline{c}_i \in \mathcal{C}_I^{(n, \beta_1)}$ where $\phi(\mathcal{C}_I^{(n, \beta_1)}) = y_i$ for $i = 1, \ldots, n_E$.

Since the cosets of $\mathcal{C}_1^n$ are nonempty, each $\overline{y}$ has at least one suitable set from $\mathcal{C}_I$.

**Definition 2.4.2** If $\overline{y}$ is a vector in $\mathcal{C}_E$ and $\{\overline{c}_i\}_{i=1}^{n_E}$ a suitable set of $\overline{y}$ from $\mathcal{C}_I$ where $\overline{c}_i = (c_{i1}, c_{i2}, \ldots, c_{i n_I})$, then the composition of $\overline{y}$ and $\{\overline{c}_i\}_{i=1}^{n_E}$ denoted by $\overline{y} \circ \{\overline{c}_i\}_{i=1}^{n_E}$ is defined as

$$
\overline{y} \circ \{\overline{c}_i\}_{i=1}^{n_E} = (c_{11}, \ldots, c_{a_{11}}, \ldots, c_{1n_I}, \ldots, c_{a_{n_{n_I}}}).
$$

(2.128)

We note that $\overline{y} \circ \{\overline{c}_i\}_{i=1}^{n_E} \in F_{q^{n_{n_I}}}$ since $\mathcal{C}_I \subseteq F_{q^{n_I}}$. Like before, for a fixed $\overline{y} \in \mathcal{C}_E$, we have

$$
\overline{y} \circ (\mathcal{C}_E, \mathcal{C}_I) = \left\{ \overline{y} \circ \{\overline{c}_i\}_{i=1}^{n_E} : \{\overline{c}_i\}_{i=1}^{n_E} \subseteq \mathcal{C}_I \text{ a suitable set of } \overline{y} \right\}.
$$

(2.129)

**Definition 2.4.3** The composition of $\mathcal{C}_E$ and $\mathcal{C}_I$ using $\mathcal{C}_1^n$ is defined as

$$
\mathcal{C} = \mathcal{C}_E \circ (\mathcal{C}_I, \mathcal{C}_I) = \bigcup_{\overline{y} \in \mathcal{C}_E} \overline{y} \circ (\mathcal{C}_I, \mathcal{C}_I).
$$

Clearly $\mathcal{C} \subseteq F_{q^{n_{n_I}}}$.

**Lemma 2.4.4** If $\overline{c} \in \mathcal{C}_E \circ (\mathcal{C}_I^n, \mathcal{C}_I)$, then $\overline{c}$ has a unique representation of the form $\overline{y} \circ \{\overline{c}_i\}_{i=1}^{n_E}$ where $\overline{y} = (y_1, \ldots, y_{n_E}) \in \mathcal{C}_E$ and $\overline{c}_i \in \mathcal{C}_I^{y_i}$ for $i = 1, \ldots, n_E$. 
Proof: The proof of this lemma is similar to that of Lemma 2.2.4. □

**Theorem 2.4.5** If $\mathbf{C}_E$ is an $[n_E, k_E]$ linear code over $F_q^2$, $\mathbf{C}_I$ a linear code over $F_q$ and $\mathbf{C}_I^\circ$ is a subcode of $\mathbf{C}_I$ of codimension two, then $\mathbf{C} = \mathbf{C}_E \circ (\mathbf{C}_I^\circ, \mathbf{C}_I)$ is an $[n_E n_I, n_E(n_I - 2) + 2k_E]$ linear code over $F_q$.

Proof: The proof of this theorem is similar to the codimension one case.

We leave the analysis of these codes to a future date.
CHAPTER III

Applications of Composition Codes

3.1 Introduction

In this chapter we present a new generalization of quadratic residue codes. This one is different from the generalization given by J.H. van Lint and F.J. MacWilliams in [7]. The family of generalized quadratic residue codes from this new definition is invariant under the composition of codes defined in Chapter 2, and it yields a subfamily of codes whose compositions give self-dual codes.

3.1.1 Preliminaries

For $q$ a positive integer which is a power of a prime and $n$ an integer relatively prime to $q$, the generator polynomial of a cyclic code of length $n$ over $F_q$ must be a factor of $x^n - 1$. We mention some facts about these factors which are used later.

Since $(q, n) = 1$, there is a smallest integer $m$ such that $n$ divides $q^m - 1$. This $m$ is called the multiplicative order of $q$ modulo $n$. Then, $n$ being a divisor of $q^m - 1$ implies $x^n - 1$ divides $x^{q^m - 1} - 1$ but does not divide $x^{q^s - 1} - 1$ for $0 < s < m$. Thus the zeros of $x^n - 1$, which are called the $n$th roots of unity, lie in the extension field $F_{q^m}$ and in no smaller field. The derivative of $x^n - 1$ is $n x^{n-1}$, which is relatively prime to $x^n - 1$, since $(n, q) = 1$. Thus $x^n - 1$ has $n$ distinct roots in $F_{q^m}$. 

63
Lemma 3.1.1  Let $q$ be a prime power and $n$ an integer with $(q,n) = 1$. Let $m$ be the smallest integer such that $q^m \equiv 1 \mod n$. Then the polynomial $f(x) = x^n - 1$ is a separable polynomial over $F_{q^m}$ and $F_{q^m}$ contains a primitive $n$th root of unity $\alpha$ such that
\[ x^n - 1 = \prod_{i=0}^{n-1} (x - \alpha^i). \]

Definition 3.1.2  The cyclotomic coset modulo $n$ over $F_q$ which contains $s$ is
\[ C_s = \{ s, sq, sq^2, \ldots, sq^{m-1} \} \]
where $sq^{m_s} \equiv s \mod n$.

Then the integers modulo $n$ are partitioned into cyclotomic cosets:
\[ \{0,1,\ldots,n-1\} = \bigcup_s C_s \]
where $s$ runs through a set of coset representatives mod $n$ and the minimal polynomial of $\alpha^s$ is
\[ M^{(s)}(x) = \prod_{i \in C_s} (x - \alpha^i). \] (3.1)

This is a monic polynomial with coefficients from $F_q$ and is the lowest degree such polynomial having $\alpha^s$ as a root. Also
\[ x^n - 1 = \prod_s M^{(s)}(x) \] (3.2)
where $s$ runs through a set of coset representatives mod $n$. This is the factorization of $x^n - 1$ into irreducible polynomials over $F_q$.

Next we introduce quadratic residues.
Definition 3.1.3 Let $p$ be an odd prime. The nonzero squares $1^2, 2^2, 3^2, \ldots$ modulo $p$ are called **quadratic residues mod $p$** or simply the residues mod $p$.

Let $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$. There are $\frac{p-1}{2}$ residues in $\mathbb{Z}_p$. The remaining $\frac{p-1}{2}$ nonzero elements in $\mathbb{Z}_p$ are called **nonresidues**. Zero is neither a residue nor a nonresidue.

Then, the product of two residues is a residue, the product of two nonresidues is a residue, and the product of a residue and a nonresidue is a nonresidue.

Let $l$ be another prime which is a quadratic residue modulo $p$. We are going to define quadratic-residue (QR) codes of prime length $p$ over $F_l$.

Let $Q$ denote the quadratic residues modulo $p$ and $N$ the set of nonresidues. Then $Q$ and $N$ are closed under multiplication by $l$. Let $\alpha$ be a primitive $p$th root of unity in some extension of $F_l$. Let

$$q(x) = \prod_{r \in Q} (x - \alpha^r) \quad \text{and} \quad n(x) = \prod_{n \in N} (x - \alpha^n).$$

(3.3)

Then, the coefficients of both $q(x)$ and $n(x)$ satisfy the equation $x^l = x$ since both $Q$ and $N$ are closed under multiplication by $l$. Therefore the coefficients of $q(x)$ and $n(x)$ are in $F_l$. Also

$$x^p - 1 = (x - 1)q(x)n(x).$$

(3.4)

Let $R$ be the ring $F_l[x]/(x^p - 1)$.

**Definition 3.1.4** The quadratic residue codes $Q, \overline{Q}, N, \overline{N}$ are cyclic codes (or ideals) of $R$ with generator polynomials

$$q(x), \quad (x - 1)q(x), \quad n(x), \quad (x - 1)n(x)$$

(3.5)

respectively.
\( \mathcal{Q} \) and \( \mathcal{N} \) are equivalent codes with parameters \([p, \frac{(n+1)}{2}]\), while \( \overline{\mathcal{Q}} \) and \( \overline{\mathcal{N}} \) are equivalent codes with parameters \([p, \frac{(n-1)}{2}]\). Also \( \mathcal{Q} \supset \overline{\mathcal{Q}} \) and \( \mathcal{N} \supset \overline{\mathcal{N}} \).

**Theorem 3.1.5** \( \text{If } d \text{ is the minimum distance of } \mathcal{Q} \text{ or } \mathcal{N}, \text{ then } d^2 \geq p. \)**

All the definitions and results in this section are as in [9].

### 3.2 A Generalization of Quadratic Residue Codes

In this section \( p \) stands for an odd prime number. Next we define quadratic residues modulo \( p^m \) where \( m \geq 1 \). Let

\[
\mathbb{Z}_{p^m} = \{0, 1, 2, \ldots, p^m - 1\},
\]

the additive group of integers modulo \( p^m \) and

\[
\mathbb{Z}_{p^m}^* = \{ a : a \in \mathbb{Z}_{p^m} \text{ and } (a, p^m) = 1 \},
\]

the multiplicative group of integers modulo \( p^m \).

**Definition 3.2.1** Let \( Q_{p^m}^+ \) be the squares in \( \mathbb{Z}_{p^m}^* \) and \( Q_{p^m}^- \) be the nonsquares. Then the elements of \( Q_{p^m}^+ \) are called **quadratic residues modulo** \( p^m \) and the elements of \( Q_{p^m}^- \) the **quadratic nonresidues modulo** \( p^m \).

From the definition of \( Q_{p^m}^+ \) and \( Q_{p^m}^- \), we have

\[
\mathbb{Z}_{p^m}^* = Q_{p^m}^+ \cup Q_{p^m}^-.
\]

Also we note that

\[
\mathbb{Z}_{p^m} = \bigcup_{s=1}^{m} p^{m-s} \mathbb{Z}_{p^s} \cup \{0\}.
\]
Lemma 3.2.2 \hspace{1cm} \textit{Let } l \text{ be a positive integer such that } (l, p) = 1 \text{ and } m \geq 1. \text{ Then } l \text{ is a quadratic residue modulo } p^m \text{ iff } l \text{ is a quadratic residue modulo } p.

\textit{Proof:} \hspace{1cm} • \text{ Suppose } l \text{ is a quadratic residue modulo } p^m.

Then, there exists an integer \( x \) such that \( p^m/(x^2 - l) \). Since \( m \geq 1 \), we get \( p/(x^2 - l) \) and so \( l \) is a quadratic residue modulo \( p \).

• Conversely, suppose \( l \) is a quadratic residue modulo \( p \).

To show that \( l \) is a residue modulo \( p^m \) for all \( m \geq 1 \), we use induction on \( m \). The result is true for \( m = 1 \) by the assumption. For \( m \geq 2 \), suppose \( l \) is a quadratic residue modulo \( p^{m-1} \). Then, there exists \( x \) such that

\[ x^2 \equiv l \pmod{p^{m-1}}. \]

So there is an integer \( k \) with

\[ x^2 - l = kp^{m-1}. \tag{3.10} \]

For \( s \) an arbitrary integer, we look at

\[ (x + sp^{m-1})^2 = x^2 + 2sxp^{m-1} + s^2p^{2m-2} = (l + kp^{m-1}) + 2sxp^{m-1} + s^2p^{2m-2} = l + (k + 2sx)p^{m-1} + s^2p^{2m-2}. \tag{3.11} \]

We note that \( 2m - 2 = m + (m - 2) \geq m \) since \( m \geq 2 \). Since \( l \) is a residue modulo \( p \), we have \( (l, p) = 1 \). This combined with (3.10) and the fact that \( p \) is odd gives \((2x, p) = 1 \). So \( 2x \) has a multiplicative inverse modulo \( p \) which we denote by \((2x)^{-1} \).

We choose \( s = -k(2x)^{-1} \mod p \). Then

\[ (k + 2sx) \equiv \left(k + (2x)(-k(2x)^{-1})\right) \pmod{p} \equiv (k - k) = 0 \pmod{p}. \]
Using this and the fact that \(2m - 2 \geq m\) in 3.11, we get

\[
(x + sp^{m-1})^2 = l + (k + 2sx)p^{m-1} + s^2 p^{2m-2} \equiv l \pmod{p^m}
\]  

(3.12)

and hence \(l\) is a quadratic residue modulo \(p^m\).

\[\square\]

**Lemma 3.2.3** If \(l\) is a quadratic residue modulo \(p^m\), then \(l\) is a quadratic residue modulo \(p^s\) for \(1 \leq s \leq m\).

**Proof:** Follows from Lemma 3.2.2. \(\square\)

The following theorem gives some properties of the residues and nonresidues modulo \(p^m\) which are analogous to the those of the residues and nonresidues modulo \(p\).

**Theorem 3.2.4** The set of quadratic residues \(Q^+_p\) and the set of quadratic nonresidues \(Q^-_p\) modulo \(p^m\) have the following properties:

(i) \(Q^+_p = Q^+_p + p^s\mathbb{Z}_{p^{m-s}}\) and \(Q^-_p = Q^-_p + p^s\mathbb{Z}_{p^{m-s}}\) for \(1 \leq s \leq m - 1\),

(ii) \(|Q^+_p| = |Q^-_p|\),

(iii) \(Q^+_p\) is a subgroup of \(\mathbb{Z}_{p^m}^*\),

(iv) Product of a residue and a nonresidue is a nonresidue,

(v) Product of a nonresidue with another nonresidue is a residue.

**Proof:** (i) First we show that \(Q^+_p = Q^+_p + p^s\mathbb{Z}_{p^{m-s}}\) for \(1 \leq s \leq m - 1\). For that, let \(a \in \mathbb{Z}_{p^m}^*\). Then \(a = tp^s + r\) for some \(t \in \mathbb{Z}_{p^{m-s}}\) and \(1 \leq r \leq p^s - 1\). From 3.2.3, \(a \in Q^+_p\) iff \(r \in Q^+_p\), and so \(t\) can be any element of \(\mathbb{Z}_{p^{m-s}}\). Thus

\[
a \in Q^+_p \text{ iff } a \in Q^+_p + p^s\mathbb{Z}_{p^{m-s}}
\]
which proves the first part of (i). Showing \( Q_{p^m}^- = Q_{p^m}^+ + p^m \mathbb{Z}_{p^m}^- \), is similar.

- (ii). From part(i), for \( s = 1 \) we have

\[
|Q_{p^m}^+| = |Q_{p^m}^+ + \mathbb{Z}_{p^m-1}| = \frac{(p - 1)}{2} p^{m-1} = \frac{|\mathbb{Z}_{p^m}^*|}{2}.
\]

Also from part(i) with \( s = 1 \), we get

\[
|Q_{p^m}^-| = \frac{(p - 1)}{2} p^{m-1} = \frac{|\mathbb{Z}_{p^m}^*|}{2}
\]

and hence \( |Q_{p^m}^+| = |Q_{p^m}^-| \).

- (iii). Let \( a \) and \( b \in Q_{p^m}^+ \). Then

\[
a \equiv x^2 \pmod{p^m} \quad \text{and} \quad b \equiv y^2 \pmod{p^m}
\]

for some \( x, y \) in \( \mathbb{Z}_{p^m}^* \). This gives

\[
a = x^2 + tp^n \quad \text{and} \quad b = y^2 + sp^n
\]

for some integers \( t \) and \( s \). From this, we get

\[
ab = x^2 y^2 + p^n(ty^2 + sx^2 + stp^n)
\]

and so \( ab \equiv (xy)^2 \pmod{p^m} \). Thus \( ab \in Q_{p^m}^+ \) and so \( Q_{p^m}^+ \) is closed under multiplication. But \( |Q_{p^m}^+| \) is finite and hence is a subgroup of \( \mathbb{Z}_{p^m}^* \).

- (iv) and (v). From part(ii) and part(iii), \( Q_{p^m}^+ \) is a subgroup of \( \mathbb{Z}_{p^m}^* \) of index two.

Since \( Q_{p^m}^+ \) and \( Q_{p^m}^- \) are disjoint subsets of \( \mathbb{Z}_{p^m}^* \) of the same size, for any \( n \in Q_{p^m}^- \), we get

\[
Q_{p^m}^- = n \cdot Q_{p^m}^+ \quad (3.13)
\]
which is the coset of $Q_{pm}^+$ other than itself. From (3.13), we obtain (iv) and (v). □

For $p$ an odd prime number and $m \geq 1$, let $l$ be another prime number which is a quadratic residue modulo $p^m$. Then from Lemma 3.1.1, there exists an element $\alpha$, a primitive $p^m$th root of unity in some extension of $F_l$. Then, for $1 \leq s \leq m$, $\alpha^{p^m - s}$ is a $p^s$th root of unity over $F_l$. For each $s$ with $1 \leq s \leq m$, we define the following pair of polynomials.

**Definition 3.2.5** We let

$$g_{p^s}(x) = \prod_{r \in Q_{p^s}^+} (x - \alpha^{p^m - s} r)$$

$$g_{p^s}^-(x) = \prod_{n \in Q_{p^s}} (x - \alpha^{p^m - s} n).$$

In the following theorem, we show that the polynomials $g_{p^s}(x)$ and $g_{p^s}^-(x)$ have coefficients from $F_l$.

**Theorem 3.2.6** The polynomials $g_{p^s}(x)$ and $g_{p^s}^-(x)$ are in $F_l[x]$.

**Proof:** First, we show that $g_{p^s}(x)$ is in $F_l[x]$. From part(iii) of Theorem 3.2.4, we know that $Q_{p^s}^+$ is a subgroup, and since $l \in Q_{p^s}^+$, we get $lQ_{p^s}^+=Q_{p^s}^+$. Thus $Q_{p^s}^+$ is a disjoint union of cyclotomic cosets modulo $p^s$ over $F_l$. So, from (3.1)

$$g_{p^s}(x) = \prod_{r \in Q_{p^s}^+} (x - \alpha^{p^m - s} r)$$

is a product of irreducible polynomials over $F_l$ and hence $g_{p^s}(x) \in F_l[x]$.

From part(iv) of Theorem 3.2.4, we have $lQ_{p^s}^- = Q_{p^s}^-$. Using this fact, the proof of showing that

$$g_{p^s}^-(x) = \prod_{n \in Q_{p^s}^-} (x - \alpha^{p^m - s} n) \in F_l[x]$$
is similar to case of showing \( g_{p^s}(x) \in F_1[x] \).

Since \( x^{p^s} - 1 \) divides \( x^{p^m} - 1 \) for \( 1 \leq s \leq m \) and \( x^{p^m} - 1 \) is separable over an extension of \( F_1 \), \( x^{p^s} - 1 \) is also a separable polynomial over that extension. And since \( g_{p^s}(x) \) and \( g_{p^s}^{-1}(x) \) are separable with their roots among the \( p^s \)th roots of unity, they both divide \( x^{p^s} - 1 \). Consequently, \( g_{p^s}^+(x) \) and \( g_{p^s}^-(x) \) divide \( x^{p^m} - 1 \) for \( s = 1, \ldots, m \).

**Lemma 3.2.7** Let

\[
M = \{ f(x) : f(x) = g_{p^s}^+(x) \text{ or } g_{p^s}^-(x) \text{ for some } s \text{ with } 1 \leq s \leq m \}.
\]

Then no two polynomials in \( M \) have a common root.

**Proof:** Clearly, the pair \( g_{p^s}^+(x) \) and \( g_{p^s}^-(x) \) have no common roots.

For \( 1 \leq s \neq s' \leq m \), \( g_{p^s}^+(x) \) has no roots in common with \( g_{p^s'}^+(x) \) or \( g_{p^s'}^-(x) \) since the roots of \( g_{p^s}^+(x) \) are of the form \( \alpha^u \) where \( u \in \mathbb{Z}_{p^s}^* \), whereas each of the other two polynomials have roots of the form \( \alpha^v \) where \( v \in \mathbb{Z}_{p^{s'}}^* \) and since \( \mathbb{Z}_{p^s}^* \) and \( \mathbb{Z}_{p^{s'}}^* \) are disjoint sets for \( s \neq s' \). For the same reason as above \( g_{p^s}^-(x) \) has no common roots with \( g_{p^s'}^+(x) \) or \( g_{p^s'}^-(x) \) and this proves the lemma.

We use the polynomials \( g_{p^s}^+(x) \)'s and \( g_{p^s}^-(x) \)'s to define the following polynomial.

Let

\[
g(x) = \prod_{s=1}^{m} q_{p^s}(x) \tag{3.14}
\]

where \( q_{p^s}(x) \) is chosen to be \( g_{p^s}^+(x) \) or \( g_{p^s}^-(x) \) for \( s = 1, \ldots, m \). Then, since each \( q_{p^s}(x) \) is a separable polynomial in \( F_1[x] \), \( g(x) \) is also in \( F_1[x] \) and is separable by
Lemma 3.2.7. And since \( q_{p^r}(x) \) divides \( x^{p^{nm}} - 1 \) and from Lemma 3.2.7 no two \( q_{p^r}(x) \) have any common root, \( g(x) \) is also a divisor of \( x^{p^{nm}} - 1 \).

We call the set of roots of \( g(x) \) as \( \Omega_{g(x)} \) and

\[
\Delta_{p^r} = \begin{cases} 
Q_{p^r}^+, & \text{if } q_{p^r}(x) = g_{p^r}^+(x) \\
Q_{p^r}^-, & \text{if } q_{p^r}(x) = g_{p^r}^-(x).
\end{cases}
\]  

(3.15)

Let

\[
\Delta_{g(x)} = \bigcup_{s=1}^{m} p^{-s} \Delta_{p^r}.
\]  

(3.16)

Then

\[
\Omega_{g(x)} = \left\{ \alpha^u : u \in \Delta_{g(x)} \right\}.
\]  

(3.17)

Let \( R \) be the ring \( F_1[x]/(x^{p^m} - 1) \).

We pick a polynomial \( g(x) \) as defined in (3.14) and for a fixed choice of \( g(x) \) we define the following cyclic code of \( R \).

**Definition 3.2.8** The generalized quadratic residue codes (or GQR codes) of length \( p^m \) over \( F_1 \) denoted by \( Q_{p^m} \) and \( \overline{Q}_{p^m} \) are cyclic codes of \( R \) with generator polynomials \( g(x) \) and \( (x-1)g(x) \) respectively, where \( g(x) \) is as defined in (3.14).

Clearly \( Q_{p^m} \supset \overline{Q}_{p^m} \) and different choices of \( g(x) \) give equivalent codes.

**Theorem 3.2.9** The GQR code \( Q_{p^m} \) is a \([p^m, \frac{1}{2}(p^m + 1)]\) code and \( \overline{Q}_{p^m} \) is a \([p^m, \frac{1}{2}(p^m - 1)]\) code.

**Proof:** Clearly the length of the GQR codes is \( p^m \). We have

\[
\text{the degree of } g(x) = \sum_{s=1}^{m} \deg q_{p^r}(x) \\
= \frac{|Z_{p^m}| - 1}{2}
\]  

(3.18)
using (3.9). Thus the degree of \( g(x) \) is \( \frac{p^m - 1}{2} \) and so the dimension of \( Q_{p^m} = \langle g(x) \rangle \) is \( p^m - \deg g(x) = \frac{1}{2} (p^m + 1) \). Similarly,

\[
\deg \left( (x - 1)g(x) \right) = \left( \deg g(x) \right) + 1 = \frac{p^m + 1}{2}.
\]

Hence the dimension of \( \overline{Q}_{p^m} \) is \( p^m - \deg \left( (x - 1)g(x) \right) = \frac{p^m - 1}{2} \). \( \square \)

Let \( \overline{1} \) be the all one vector over \( F_l \) of appropriate length.

**Theorem 3.2.10**  The generalized quadratic residue code \( Q_{p^m} \) over \( F_l \) is generated by \( \overline{Q}_{p^m} \) and \( \overline{1} \).

**Proof:** Let \( f : Q_{p^m} \rightarrow F_l \) be the linear functional such that for \( \overline{c} = (c_1, \ldots, c_{p^m}) \) in \( Q_{p^m} \),

\[
f(\overline{c}) = \sum_{i=1}^{p^m} c_i.
\]

Then \( f(\overline{c}) = \overline{c}(1) \). So \( f(\overline{c}) = 0 \) iff \( \overline{c}(1) = 0 \). But \( \overline{c}(1) = 0 \) iff \( \overline{c} \in Q_{p^m} \). Therefore \( f(\overline{c}) = 0 \) iff \( \overline{c} \in \overline{Q}_{p^m} \) and thus the kernel of the functional \( f \) is \( \overline{Q}_{p^m} \). From definition 3.2.8, we have

\[
\dim Q_{p^m} = \dim \overline{Q}_{p^m} + 1. \tag{3.19}
\]

Also, for \( \overline{1} = \sum_{i=0}^{p^m-1} x^i \), we have

\[
\overline{1}(1) = p^m.1 \neq 0
\]

in \( F_l \) since \( (p, l) = 1 \). So \( \overline{1} \notin \overline{Q}_{p^m} \). But \( \overline{1} \in Q_{p^m} \). These facts and (3.19) give

\[
Q_{p^m} = \langle \overline{Q}_{p^m}, \overline{1} \rangle
\]

which proves the theorem. \( \square \)
Let $s, t \geq 1$ be integers. We pick $l$ to be a prime number which is also a quadratic residue modulo $p$. Then by Lemma 3.2.2, $l$ is a quadratic residue modulo $p^w$ for all $w \geq 1$. In particular $l$ is a quadratic residue modulo $p^s$, $p'$ and $p^{s'}$. Let $\alpha$ be a primitive $p^{s+1}$th root of unity in an extension of $F_l$.

Then $\beta = \alpha^p$ is a primitive $p^s$th root of unity over $F_l$ and so we can use $\beta$ to define GQR codes of length $p^s$ over $F_l$. Let $\mathcal{Q}_{p^s} = \langle g(x) \rangle$ be a GQR code of length $p^s$ over $F_l$ as defined in (3.2.8). Then, from the definitions in (3.17), (3.15) and (3.16), the set of roots of $g(x)$ is
\[ \Omega_{g(x)} = \left\{ \beta^u : u \in \Delta_{g(x)} \right\} \]  
where
\[ \Delta_{g(x)} = \bigcup_{i=1}^{s} p^{s-i} \Delta_{p^i} \]  
with $\Delta_{p^i}$ equalling $Q^+_{p^i}$ or $Q^-_{p^i}$ depending on the choice of $g(x)$.

Also $\gamma = \alpha^{p'}$ is a $p'$th root of unity over $F_l$ and so we can use $\gamma$ to define GQR codes of length $p'$ over $F_l$. Let $\mathcal{Q}_{p'} = \langle h(x) \rangle$ be a GQR code of length $p'$ over $F_l$ as defined in (3.2.8). Then from the definitions (3.17), (3.15) and (3.16), the set of roots of $h(x)$ is
\[ \Omega_{h(x)} = \left\{ \beta^v : v \in \Delta_{h(x)} \right\} \]  
where
\[ \Delta_{h(x)} = \bigcup_{i=1}^{t} p^{t-i} \Delta_{p'} \]  
with $\Delta_{p'}$ equalling $Q^+_{p'}$ or $Q^-_{p'}$ depending on the choice of $h(x)$.

The following lemma gives a relationship between the exponents of the roots of $g(x)$ and those of $h(x)$. 


Lemma 3.2.11

\[ (p^{l} \Delta_{g(x)}) \cup (\Delta_{h(x)} + p^{l}Z_{p^*}) = \bigcup_{i=1}^{s+t} p^{(s+t)-i} \Delta_{p^*} \]  

where \( \Delta_{p^*} = Q_{p^*}^+ \) or \( Q_{p^*}^- \).

Proof: We first compute \( p^{l} \Delta_{g(x)} \). We have

\[ p^{l} \Delta_{g(x)} = p^{l} \left( \bigcup_{i=1}^{s} p^{s-i} \Delta_{p^*} \right) \]

\[ = \bigcup_{i=1}^{s} p^{(s+t)-i} \Delta_{p^*}. \]  

Computing \( \Delta_{h(x)} + p^{l}Z_{p^*} \), we get

\[ \Delta_{h(x)} + p^{l}Z_{p^*} = \left( \bigcup_{j=1}^{t} p^{t-j} \Delta_{p^*} \right) + p^{l}Z_{p^*} \]

\[ = \bigcup_{j=1}^{t} \left( p^{t-j} \Delta_{p^*} + p^{l}Z_{p^*} \right) \]

\[ = \bigcup_{j=1}^{t} \left( p^{t-j} (\Delta_{p^*} + p^{l}Z_{p^*}) \right). \]  

But

\[ (\Delta_{p^*} + p^{l}Z_{p^*}) = \begin{cases} Q_{p^*}^+ + p^{l}Z_{p^*}, & \text{or} \\ Q_{p^*}^- + p^{l}Z_{p^*}, \end{cases} \]

\[ = \begin{cases} Q_{p^*+j}^+ & \text{or} \\ Q_{p^*+j}^- \end{cases} \]  

using part(i) of Theorem 3.2.4. Thus \( (\Delta_{p^*} + p^{l}Z_{p^*}) = \Delta_{p^*+j} \). Therefore

\[ \Delta_{h(x)} + p^{l}Z_{p^*} = \bigcup_{j=1}^{t} \left( p^{t-j} \Delta_{p^*+j} \right) = \bigcup_{j=s+1}^{s+t} p^{(s+t)-j} \Delta_{p^*}. \]  

From (3.26) and (3.30), we get

\[ (p^{l} \Delta_{g(x)}) \cup (\Delta_{h(x)} + p^{l}Z_{p^*}) = \bigcup_{i=1}^{s+t} p^{(s+t)-i} \Delta_{p^*}. \]
which proves the lemma. □

Let

\[ \Delta = \left( p'(\Delta_{\eta(x)}) \right) \cup \left( \Delta_{h(x)} + p'\mathbb{Z}_{p^t} \right). \]  

(3.31)

Then from Lemma 3.2.11, we get

\[
\Delta = \bigcup_{i=1}^{s+t} p^{(s+t)-i} \Delta_{p^t}, \tag{3.32}
\]

where \( \Delta_{p^t} = Q_{p^t}^+ \) or \( Q_{p^t}^- \). So \( \Delta \subset \mathbb{Z}_{p^{s+t}} \). Let

\[ p(x) = \prod_{i=1}^{s+t} q_{p^t}(x) \]  

(3.33)

where

\[ q_{p^t}(x) = \begin{cases} g_{p^t}^+(x) & \text{if } \Delta_{p^t} = Q_{p^t}^+, \\ g_{p^t}^-(x) & \text{if } \Delta_{p^t} = Q_{p^t}^- \end{cases} \]

for \( i = 1, 2, \ldots, (s+t) \) and \( \alpha \) which we chose before is the \( p^{s+t} \)th root of unity used.

From this we note that the set of roots of \( p(x) \) is

\[ \Omega_{p(x)} = \{ \alpha^\omega : \omega \in \Delta \}. \]  

(3.34)

Then from definitions (3.2.5), (3.14) and (3.2.8), we derive that the cyclic code \( \langle p(x) \rangle \)

of length \( p^{s+t} \) over \( F_1 \) is a GQR code. We call that code \( Q_{p^t}^{s+t} \). Then

\[ Q_{p^t}^{s+t} = \langle p(x) \rangle \]  

(3.35)

is a \([p^{s+t}, \frac{1}{2}(p^{s+t} + 1)]\) cyclic code over \( F_1 \) using Theorem 3.2.9.

Below we show how \( Q_{p^t}, Q_{p^t}, \) and \( Q_{p^t}^{s+t} \) are related. For that we first look at a composition of \( Q_{p^t} \) and \( Q_{p^t} \) using \( \overline{Q}_{p^t} \).
Since \( \overline{Q}_{p'} = \langle (x-1)h(x) \rangle \) and \( Q_{p'} = \langle h(x) \rangle \), we have \( \overline{Q}_{p'} \) is a subcode of \( Q_{p'} \) of codimension one and \( h(x) \not\in \overline{Q}_{p'} \). So \( h(x) + \overline{Q}_{p'} \) is a nontrivial coset of \( \overline{Q}_{p'} \). Therefore, if we let

\[
C_E = Q_{p'}, \quad C_I = Q_{p'}, \quad C_i = \overline{Q}_{p'} \quad \text{and} \quad C_j = h(x) + \overline{Q}_{p'},
\]

then the composition code \( C_E \circ (C_i, C_I) = Q_{p'} \circ (\overline{Q}_{p'}, Q_{p'}) \) is well defined over \( F_1 \).

**Theorem 3.2.12**  
The composition \( Q_{p'} \circ (\overline{Q}_{p'}, Q_{p'}) \) is a \([p^{s+t}, \frac{1}{2}(p^{s+t}+1)]\) cyclic code over \( F_1 \) with \( g(x)h(x^{p'}) \) as the generator polynomial.

**Proof:**  
Since \( Q_{p'} \) is a \([p^s, \frac{1}{2}(p^s+1)]\) cyclic code over \( F_1 \) generated by \( g(x) \) and \( Q_{p'} \) is a \([p^t, \frac{1}{2}(p^t+1)]\) cyclic code over \( F_1 \) generated by \( h(x) \) over \( F_1 \), from Theorem 2.3.8 in Chapter 2, we get the composition \( Q_{p'} \circ (\overline{Q}_{p'}, Q_{p'}) \) has length \( p^{s+t} \) and dimension

\[
p^s\left(\frac{1}{2}(p^t+1) - 1\right) + \frac{1}{2}(p^s+1) = \frac{1}{2}(p^{s+t} + 1),
\]

and from Theorem 2.3.14, the composition is a cyclic code generated by \( g(x)h(x^{p'}) \).

\[\square\]

The polynomial \( p(x) \) defined in (3.33) has the following relationship with the polynomials \( g(x) \) and \( h(x) \).

**Lemma 3.2.13**

\[
p(x) = g(x)h(x^{p'}). \tag{3.36}
\]

**Proof:**  
From Theorem 2.3.16 in Chapter 2, we get the set of roots of \( g(x)h(x^{p'}) \) to be

\[
\{ \alpha^\delta : \delta \in (p^t\Delta_{g(x)}) \cup (\Delta_{h(x)} + p^t\mathbb{Z}_{p'}) \} = \{ \alpha^\delta : \delta \in \bigcup_{i=1}^{s+t} p^{(s+t)-i}\Delta_{p'} \} \tag{3.37}
\]
where $\Delta_{p^t} = Q^+_p$ or $Q^-_p$, using Lemma 3.2.11. Therefore, using (3.32), the set of roots of $g(x)h(x^{p^t})$ is

$$\{ \alpha^\delta : \delta \in \Delta \}.$$  

From (3.34), we have that $p(x)$ also has the same set of roots. Thus $g(x)h(x^{p^t})$ and $p(x)$ are both monic separable polynomials over $F_l$ with exactly the same set of roots. Therefore $p(x) = g(x)h(x^{p^t})$. 

We have the following relationship between $Q_{p^t}$, $Q_p$, and $Q_{p'^t}$.

**Theorem 3.2.14**

$$Q_{p^t} \circ (\overline{Q}_{p'^t}, Q_p) = Q_{p'^t}.$$  

**Proof:** From Theorem 3.2.12, $Q_{p^t} \circ (\overline{Q}_{p'^t}, Q_p)$ is a $[p^{s+t}, 1, \frac{1}{2}(p^{s+t} + 1)]$ cyclic code over $F_l$ generated by $g(x)h(x^{p^t})$. Similarly, from (3.35), $Q_{p'^t}$ is a $[p^{s+t}, 1, \frac{1}{2}(p^{s+t} + 1)]$ cyclic code over $F_l$ generated by $p(x)$. From Lemma 3.2.13, $p(x) = g(x)h(x^{p^t})$ and hence the codes $Q_{p'^t}$, $Q_{p^t} \circ (\overline{Q}_{p'^t}, Q_p)$ generated by them are the same. 

Theorem 3.2.14 shows that the family of generalized quadratic residue codes is invariant under composition.

### 3.2.1 The Dual and the Extended Codes of Generalized Quadratic Residue Codes

We first give some results that are known about the quadratic residues and the dual of a cyclic code.
Lemma 3.2.15 \(-1\) is a quadratic nonresidue modulo \(p\) if and only if \(p = 4k - 1\).

Proof: Let \(\alpha\) be a primitive element of \(F_p\). Then the powers of \(\alpha\) give all the elements of \(F_p\) and in particular, \(\alpha^{p-1}/2 = -1\) since this is the element \(\neq 1\) whose square is 1. If \(p = 4k - 1\), then \(\frac{p-1}{2} = 2k - 1\) so that \(-1 = \alpha^{p-1}/2\) is an odd power of \(\alpha\) and thus not a square. If \(p = 4k + 1\), then \(\frac{p-1}{2} = 2k\) and so

\[ -1 = \alpha^{p-1}/2 = \alpha^{2k} = (\alpha^k)^2 \]

which is clearly a square. \(\square\)

The above lemma is as in [11].

Let \(\mathcal{C}\) be a cyclic code of length \(n\) with \(g(x)\) as the generator polynomial and let

\[ h(x) = \frac{(x^n - 1)}{(x - 1)g(x)}. \]  

(3.38)

Lemma 3.2.16 The dual code \(\mathcal{C}^\perp\) is cyclic with

\[ f(x) = x^{\deg h(x)}(1 - x)h(x^{-1}) \]

(3.39)

as the generator polynomial.

This result is as stated in [9].

Lemma 3.2.17 Let \(\mathcal{Q}_{pm} = \langle g(x) \rangle\) and \(\mathcal{Q}_{pm} = \langle (x - 1)g(x) \rangle\) be the GQR codes of length \(p^m\) over \(F_t\) for some choice of \(g(x)\) and let \(\mathcal{N}_{pm} = \langle h(x) \rangle\) and \(\overline{\mathcal{N}}_{pm} = \langle (x - 1)h(x) \rangle\) be cyclic codes of length \(p^m\) over \(F_t\) where

\[ h(x) = (x^{p^m} - 1)/(x - 1)g(x). \]  

(3.40)
Then the dual code of \( Q_{p^m} \) is given by:

\[
Q_{p^m}^\perp = \begin{cases} 
\overline{Q}_{p^m}, & \text{if } p = 4k - 1, \\
N_{p^m}, & \text{if } p = 4k + 1.
\end{cases}
\] (3.41)

**Proof:** Let \( \alpha \) be a \( p^m \)-th root of unity over \( F_q \). Also let \( \Omega_g(x) \) be the set of roots of \( g(x) \) and

\[
\Delta_g(x) = \{ r \in \mathbb{Z}_{p^m} : \alpha^r \in \Omega_g(x) \}.
\]

Similarly, let \( \Omega_h(x) \) be the set of roots of \( h(x) \) and

\[
\Delta_h(x) = \{ n \in \mathbb{Z}_{p^m} : \alpha^n \in \Omega_h(x) \}.
\]

Then from the definition of \( h(x) \), we get

\[
\Delta_g(x) \cup \Delta_h(x) = \mathbb{Z}_{p^m} \setminus \{0\} \quad \text{and} \quad \Delta_g(x) \cap \Delta_h(x) = \emptyset.
\] (3.42)

From the definition of \( g(x) \) in (3.14),

\[
\Delta_g(x) = s\Delta_h(x)
\] (3.43)

for any nonresidue \( s \) modulo \( p \). Using Lemma 3.2.16, the dual code \( Q_{p^m}^\perp \) is generated by

\[
f(x) = x^{\deg h(x)}(1 - x)h(x^{-1})
\] (3.44)

so that the roots of \( f(x) \) are given by

\[
\Omega_f(x) = \{1\} \cup \left\{ \alpha^{-b} : b \in \Delta_h(x) \right\}.
\] (3.45)

**Case 1** \( p = 4k - 1 \).

From Lemma 3.2.15, \(-1\) is a nonresidue modulo \( p \) in this case and thus

\[
\Delta_g(x) = (-1)\Delta_h(x)
\]
using (3.43). This fact together with (3.45) says that the set of roots of \( f(x) \) is made up of 1 and the roots of \( g(x) \). Since \( f(x) \) and \( g(x) \) are separable polynomials, we get

\[
f(x) = (x - 1)g(x)
\]

and so \( Q_{p,m}^k = \overline{Q}_{p,m} \).

**Case 2** \( p = 4k + 1 \).

In this case -1 is a residue modulo \( p \) according to Lemma 3.2.15 and so

\[
(-1)\Delta_h(x) = \Delta_h(x)
\]

using parts (iii), (iv) of Theorem 3.2.4. From this and (3.45), we get that the set of roots of \( f(x) \) in this case consists of 1 and the roots of \( h(x) \); and since \( f(x) \) and \( h(x) \) are separable polynomials, we have \( f(x) = (x - 1)h(x) \). Thus \( Q_{p,m}^k = \overline{N}_{p,m} \) in this case.

\[\square\]

**Definition 3.2.18** For \( p \) an odd prime and \( a \) an integer, let

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1, & \text{if } a \text{ is a quadratic residue mod } p, \\
-1, & \text{if } a \text{ is a nonresidue mod } p.
\end{cases}
\]

(3.46)

**Lemma 3.2.19** Gauss' quadratic reciprocity law:

If \( p, q \) are odd primes, then

\[
\left( \frac{p}{q} \right) \left( \frac{q}{p} \right) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}.
\]

(3.47)

If we know whether \( q \) is a residue or a nonresidue modulo \( p \), then the quadratic reciprocity law can sometimes be used to determine whether \( p \) is a residue modulo \( q \) or not.
Lemma 3.2.20  If $p$, $l$ are odd primes such that $l$ is a quadratic residue modulo $p$ and $p = 4k - 1$, then $-p$ is a quadratic residue modulo $l$.

Proof: From the quadratic reciprocity law in (3.47), we have

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{1}{2}(p-1)\frac{1}{2}(q-1)}. \tag{3.48}$$

Since $l$ is a quadratic residue mod $p$, we get $\left(\frac{l}{p}\right) = 1$. Using this and the assumption that $p = 4k - 1$ in (3.48) gives

$$\left(\frac{p}{l}\right) \cdot 1 = (-1)^{\frac{4k-2}{2} \cdot \frac{l-1}{2}} = (-1)^{\frac{l-1}{2}}$$

$$= \begin{cases} 
1, & \text{if } l = 4t + 1 \\
-1, & \text{if } l = 4t - 1 
\end{cases}$$

for some $t$. This means $p$ is a residue mod $l$ if $l = 4t + 1$ and it is a nonresidue mod $l$ if $l = 4t - 1$. From Lemma 3.2.15, $-1$ is a residue mod $l$ iff $l = 4t + 1$ and therefore the product $p \cdot (-1) = -p$ is always a residue mod $l$. \qed

For $l$ and $p$ prime numbers with $l$ a quadratic residue modulo $p$, the following lemma gives a criterion for $-p^m$ to be a quadratic residue modulo $l$.

Lemma 3.2.21  Let $p = 4k - 1$ be a prime and $l$ be a quadratic residue modulo $p$. Then, if (i) $l = 2$, or, (ii) $m$ is a odd integer, or, (iii) $m$ an even integer and $l = 4t + 1$ for some $t$, then $-p^m$ is a quadratic residue modulo $l$.

Proof: If $l = 2$, then $-p^m \equiv 1 \mod l$ and so is quadratic residue modulo $l$. If $l$ is odd, then from Lemma 3.2.20, $-p \equiv r^2 \mod l$ for some integer $r$. From this we get,

$$(-p)^m \equiv (r^m)^2 \mod l$$
Thus from (3.49), we have \(-p^m\) is a quadratic residue modulo \(l\) for any odd value of \(m\) and any value of \(l\). When \(m\) is even and \(l = 4t + 1\), the result follows from (3.49) and Lemma 3.2.20.

We denote the extension of a code \(C\) by \(\hat{C}\) and the extension of a code word \(\bar{c}\) in \(C\) by \(\hat{c}\).

We use the fact that \(Q_{p^m} = (Q_{p^m}, 1)\) in Theorem 3.2.10 to define an extension of the generalized quadratic residue code \(Q_{p^m}\) as follows:

**Definition 3.2.22** Let \(p = 4k - 1\) be a prime and \(l\) be a quadratic residue modulo \(p\). Then, for (i) \(l = 2\), or (ii) \(m\) an odd integer, or (iii) \(m\) an even integer and \(l = 4t + 1\) for some \(t\), we extend \(Q_{p^m}\) as follows:

For \(\bar{z} \in Q_{p^m}\), we define

\[
\hat{z} = (\bar{z}, 0). \tag{3.50}
\]

Since \(p\) and \(l\) satisfy all the conditions in Lemma 3.2.21, there is an \(r\) such that \(-p^m \equiv r^2 \mod l\). Using this fact we define an extension of the all one vector \(\bar{1} \in Q_{p^m}\) as

\[
\hat{1} = (\bar{1}, r). \tag{3.51}
\]

Let \(\bar{c} = \alpha \bar{z} + \beta \bar{1}\) be an arbitrary element of \(Q_{p^m}\) where \(\bar{z} \in Q_{p^m}\) and \(\alpha, \beta\) in \(F_l\).

We define

\[
\hat{c} = \alpha \hat{z} + \beta \hat{1} \tag{3.52}
\]
and

\[ \hat{Q}_{pm} = \{ \hat{c} : \hat{c} \in Q_{pm} \}. \tag{3.53} \]

The extended code \( \hat{Q}_{pm} \) defined above has the following properties.

**Theorem 3.2.23** Let \( p = 4k - 1 \) be a prime and \( l \) be a quadratic residue modulo \( p \). Then, for (i) \( l = 2 \), or, (ii) \( m \) an odd integer, or, (iii) \( m \) an even integer and \( l = 4t + 1 \) for some \( t \), then the extended code \( \hat{Q}_{pm} \) defined in (3.2.22) is self dual.

**Proof:** From Lemma 3.2.17, we have \( Q_{pm}^\perp = \overline{Q}_{pm} \) for \( p = 4k - 1 \). And since \( Q_{pm} \subset Q_{pm}^\perp \), we get \( \overline{Q}_{pm} \subset \overline{Q}_{pm}^\perp \). This gives, for \( \tilde{z}_1, \tilde{z}_2 \) in \( \overline{Q}_{pm}^\perp \),

\[ \langle \tilde{z}_1, \tilde{z}_2 \rangle = \langle (\tilde{z}_1, 0), (\tilde{z}_2, 0) \rangle = \langle \tilde{z}_1, \tilde{z}_2 \rangle = 0. \tag{3.54} \]

Also, since \( \tilde{1} \in Q_{pm} \) and since \( Q_{pm}^\perp = \overline{Q}_{pm} \) for \( p = 4k - 1 \) from Lemma 3.2.17, we have \( \langle \tilde{1}, \tilde{z} \rangle = 0 \) for all \( \tilde{z} \in \overline{Q}_{pm} \). Thus

\[ \langle \tilde{1}, \tilde{z} \rangle = \langle (\tilde{1}, r), (\tilde{z}, 0) \rangle = \langle \tilde{1}, \tilde{z} \rangle = 0 \tag{3.55} \]

for all \( \tilde{z} \in \overline{Q}_{pm} \). Next the inner product

\[ \langle \tilde{1}, \tilde{1} \rangle = \langle (\tilde{1}, r), (\tilde{1}, r) \rangle = p^m + r^2 = 0 \tag{3.56} \]

in \( F_1 \) by Lemma 3.2.21. Now let \( \hat{c}_1 = \alpha_1 \hat{z}_1 + \beta_1 \hat{1} \) and \( \hat{c}_2 = \alpha_2 \hat{z}_2 + \beta_2 \hat{1} \) be two arbitrary elements of \( \hat{Q}_{pm} \) where \( \hat{z}_1, \hat{z}_2 \) are in \( \hat{Q}_{pm} \). Then, their inner product

\[ \langle \hat{c}_1, \hat{c}_2 \rangle = \langle (\alpha_1 \hat{z}_1 + \beta_1 \hat{1}), (\alpha_2 \hat{z}_2 + \beta_2 \hat{1}) \rangle \tag{3.57} \]

\[ = \alpha_1 \alpha_2 \langle \hat{z}_1, \hat{z}_2 \rangle + \alpha_1 \beta_2 \langle \hat{z}_1, \hat{1} \rangle + \beta_1 \alpha_2 \langle \hat{1}, \hat{z}_2 \rangle + \beta_1 \beta_2 \langle \hat{1}, \hat{1} \rangle \tag{3.58} \]

\[ = 0 + 0 + 0 + 0 = 0 \tag{3.59} \]
using (3.54), (3.55) and (3.56). Thus

\[ \hat{Q}_{pm} \subseteq \hat{Q}_{pm}^\perp. \]  

(3.60)

But the dimension of \( \hat{Q}_{pm} \) is the same as the dimension of \( Q_{pm} \) which is \( \frac{p^m + 1}{2} \). We have the dimension of \( \hat{Q}_{pm}^\perp \) is

\[ (p^m + 1) - \frac{p^m + 1}{2} = \frac{p^m + 1}{2}. \]

Therefore \( \hat{Q}_{pm} \) and its dual have the same dimension and hence \( \hat{Q}_{pm}^\perp = \hat{Q}_{pm} \) using (3.60).

\[ \square \]

**Definition 3.2.24** For \( p = -1 \pmod{4} \) and \( m \) even, we extend \( \bar{1} \) in two different ways as follows:

\[ \hat{i}_+ = (\bar{1}, p^{m/2}) \]  

(3.61)

and

\[ \hat{i}_- = (\bar{1}, -p^{m/2}). \]  

(3.62)

Using these extensions of \( \bar{1} \), we define the following extensions of the code \( Q_{pm} \) over \( F_1 \):

\[ \hat{Q}_{pm}^+ = (\hat{Q}_{pm}, \hat{i}_+) \]  

(3.63)

and

\[ \hat{Q}_{pm}^- = (\hat{Q}_{pm}, \hat{i}_-). \]  

(3.64)

**Theorem 3.2.25** Let \( p = 4k - 1 \) be a prime and \( l \) be a quadratic residue modulo \( p \). Then, for \( l \equiv -1 \pmod{4} \) and \( m \) even, the dual \( (\hat{Q}_{pm}^+) \perp = \hat{Q}_{pm}^- \).
Proof: First of all
\[
\dim \left( \mathcal{Q}_{p,m}^+ \right) = \frac{p^m + 1}{2} = \dim \mathcal{Q}_{p,m}^-.
\] (3.65)

Let \( \hat{z}_+ = \alpha \hat{z} + \beta \hat{1}_+ \in \mathcal{Q}_{p,m}^+ \) and \( \hat{y}_- = \gamma \hat{y} + \delta \hat{1}_- \in \mathcal{Q}_{p,m}^- \) where \( z, y \in \mathcal{Q}_{p,m} \). Then
\[
\langle \hat{z}_+, \hat{y}_- \rangle = \alpha \gamma \langle \hat{z}, \hat{y} \rangle + \alpha \delta \langle \hat{z}, \hat{1}_- \rangle + \beta \gamma \langle \hat{1}_+, \hat{y} \rangle + \beta \delta \langle \hat{1}_+, \hat{1}_- \rangle
\]
\[
= 0 + 0 + 0 + 0 = 0
\]
for reasons similar to the cases in (3.54), (3.55) and because
\[
\langle \hat{1}_+, \hat{1}_- \rangle = p^m - p^m = 0.
\]
Thus \( \mathcal{Q}_{p,m}^- \subseteq \left( \mathcal{Q}_{p,m}^+ \right)^\perp \). This fact together with (3.65) gives the theorem. \( \square \)

Lemma 3.2.26 Let \( p = 4k + 1 \) and \( l \) be a quadratic residue modulo \( p \). Then
(i) if \( l = 2 \), or, \( l = 4t + 1 \) for some \( t \), then \( -p^m \) is a residue modulo \( l \),
(ii) if \( l = 4t - 1 \) for some \( t \), then \( -p^m \) is a nonresidue modulo \( l \).

Proof: If \( l = 2 \), then since \( p \) is odd, we get \( -p^m \) is a residue modulo \( l \).

For \( l \) odd, since \( l \) is a quadratic residue modulo \( p \) and \( p = 4k + 1 \), we get that \( p \) is a quadratic residue modulo \( l \) by using the quadratic reciprocity law in (3.47). And so \( p^m \) is also a residue modulo \( l \) from Lemma 3.2.15. From Lemma 3.2.15, \( -1 \) is a nonresidue modulo \( l \) iff \( l = 4k - 1 \) and thus \( -p^m \) is a residue modulo \( l \) iff \( l = 4t + 1 \).

Let \( p = 4k + 1 \) and \( l = 2 \), or, \( l = 4t + 1 \) for some \( t \). Then by Lemma 3.2.26
\( -p^m \equiv r^2 \pmod{l} \) for some \( r \) and so, for these values of \( l \), we define
\[
\hat{l} = (\overline{l}, r)
\] (3.66)
as an extension of $\overline{1}$. And, for these values of $l$, the extensions $\mathcal{Q}_{p^m}$ and $\mathcal{N}_{p^m}$ are defined similar to the one in (3.53) using $\hat{1}$.

If $l = 4t - 1$ for some $t$, then $-p^m$ is a nonresidue modulo $l$ by Lemma 3.2.26. But $-1$ is a nonresidue modulo $l$ in this case by Lemma 3.2.15 and so $p^m$ is a residue modulo $l$ which gives $p^m \equiv s^2 \pmod{l}$. We use this $s$ to define the following two extensions of $\hat{1}$:

$$\hat{1}_+ = (\overline{1}, s) \quad (3.67)$$

and

$$\hat{1}_- = (\overline{1}, -s). \quad (3.68)$$

Using these two extensions of $\overline{1}$, we define two extensions $\mathcal{Q}^+_p$, $\mathcal{Q}^-_p$ of $\mathcal{Q}_p$ and two extensions $\mathcal{N}^+_p$, $\mathcal{N}^-_p$ of $\mathcal{N}_p$ similar to the ones in the definitions (3.63) and (3.64).

These extensions are related as follows:

**Theorem 3.2.27** Let $p = 4k + 1$. Then

(i) if $l = 2$, or, $l = 4t + 1$ for some $t$, then

$$\left(\mathcal{Q}_p\right)^\perp = \mathcal{N}_p,$$

(ii) if $l = 4t - 1$ for some $t$, then

$$\left(\mathcal{Q}^+_p\right)^\perp = \mathcal{N}^-_p \quad \text{and} \quad \left(\mathcal{Q}^-_p\right)^\perp = \mathcal{N}^+_p.$$ 

**Proof:** This theorem follows from Lemmas 3.2.17 and 3.2.26. \qed
3.2.2 Some Self Dual Codes obtained through Composition

In this section we show that the composition of extended GQR codes with certain GQR codes is self dual and that one can get infinite number of self dual codes in this way.

**Theorem 3.2.28** Let $p = 4k - 1$ be a prime and $l$ be a quadratic residue modulo $p$. And, for (i) $l = 2$, or, (ii) $m$ an odd integer, or, (iii) $m$ an even integer and $l = 4t + 1$ for some $t$, let $\tilde{Q}_{pm}$ be an extended GQR code over $F_l$ defined in (3.2.22). Then the composition $\tilde{Q}_{pm} \circ (\tilde{Q}_{p^r}, Q_{p^r})$ of $\tilde{Q}_{pm}$ with any GQR code $Q_{p^r}$ of length $p^r$ over $F_l$ where $s$ is an arbitrary positive integer, is self dual.

**Proof:** By Theorem 3.2.23, $\tilde{Q}_{pm}$ is a self dual code for the values of $m$ stated in this theorem. From Lemma 3.2.17, $Q_{p^r}^\perp = \tilde{Q}_{p^r}$ for $p = 4k - 1$. Thus the exterior code $\tilde{Q}_{pm}$ and the interior code $Q_{p^r}$ satisfy the conditions of Theorem 2.2.28 in Chapter 2 and so their composition code $\tilde{Q}_{pm} \circ (\tilde{Q}_{p^r}, Q_{p^r})$ is self dual by the same theorem. □
CHAPTER IV

A Composition of Designs

4.1 Preliminaries

Definition 4.1.1 Given a set \(X\) of size \(v\), a \(t-(v, k, \lambda)\)-design is a family \(\mathcal{D}\) of \(k\)-sets of \(X\), called blocks, with the property that each set of \(t\) points of \(X\) is in exactly \(\lambda\) blocks. A design is called simple when there are no repeated blocks.

Let \(b = |\mathcal{D}|\) be the number of blocks of \(\mathcal{D}\). A simple design is called trivial when \(b\) and \(\lambda\) are maximum;

\[
    b_{\text{max}} = \binom{v}{k}
\]

and

\[
    \lambda_{\text{max}} = \binom{v-t}{k-t}.
\]

Definition 4.1.2 Taking the complements of all the blocks in \(\mathcal{D}\) gives a \(t-(v, k, \lambda_c)\) design called the Complementary Design where

\[
    \lambda_c = b \cdot \frac{\binom{v-k}{t}}{\binom{v}{t}}.
\]
For any given $v$ and $k$, there is always a $t-(v, k, \lambda_{\text{max}})$ design consisting of all the sets of size $k$. When $k \leq t$ or $v - t \leq k$, the only $t$-designs are the trivial ones. A $t$-design is an $s$-design for all $s \leq t$.

We let $r$ be the number of blocks containing any single point of $\mathcal{X}$. We will need the well-known relations [16]:

$$r = \frac{bk}{v} \quad (4.4)$$

$$\lambda = b \frac{\binom{k}{l}}{\binom{v}{l}}. \quad (4.5)$$

**Definition 4.1.3** Let $\Lambda$ be a finite set of nonnegative integers. Then a $t-(v, k, \Lambda)$ partially balanced design $\mathcal{D}$ is a set of blocks of $\mathcal{X}$ where for each set of $t$ points of $\mathcal{X}$ the number of blocks containing them is a number in $\Lambda$. When $\Lambda = \{\lambda\}$ is a singleton, then $\mathcal{D}$ is called balanced and is a usual $t-(v, k, \lambda)$-design as defined above.

### 4.2 A Composition of Designs.

Let $\mathcal{D}_e$ be a $t-(v_e, k_e, \lambda_e)$ design over the set $\mathcal{X}_e$ where $\mathcal{X}_e = \{1, 2, \ldots, v_e\}$, and $\mathcal{D}_i$, for $i=0,1$, be $t-(v_i, k_i, \lambda_i)$ designs with $v_0 = v_1$ and both over the set $\mathcal{X}_1$. Let $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_e$. Then, for any block $B_j$ in $\mathcal{D}_i$ for $i=0$ or $1$ and $j$ in $\mathcal{X}_e$, $B_j \times \{j\}$ is a subset of $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_e$ since $B_j$ is a subset of $\mathcal{X}_1$. 
Using the crossproducts $B_j \times \{j\}$ for $B_j$ in $\mathcal{D}_i$ for $i=0,1$ and $j$ in $\mathcal{X}_r$, we construct the following family of subsets of $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_r$:

Let $C$ be a block of $\mathcal{D}_r$. Then, as $j$ varies through the elements of the set $\mathcal{X}_r$, we construct $\bigcup_{j=1}^{n_r} (B_j \times \{j\})$ such that $B_j$ is chosen arbitrarily from $\mathcal{D}_1$ if $j$ is an element of $C$ and $B_j$ is an arbitrary element of $\mathcal{D}_0$ if $j$ is not an element of $C$. Since $B_j \times \{j\}$ is a subset of $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_r$ for each $j$ in $\mathcal{X}_r$, their union $\bigcup_{j=1}^{n_r} (B_j \times \{j\})$ is also a subset of $\mathcal{X}$. Because for each $j$, $B_j$ may be picked to be any element of $\mathcal{D}_0$ (or $\mathcal{D}_1$), a fixed block $C$ of $\mathcal{D}_r$ gives rise to a host of subsets of $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_r$ of the form $\bigcup_{j=1}^{n_r} (B_j \times \{j\})$. We let

$$\Delta(C) = \left\{ \left( \bigcup_{l \in C} (E_l \times \{l\}) \right) \cup \left( \bigcup_{m \in \mathcal{X}_r \setminus C} (F_m \times \{m\}) \right) : E_l \in \mathcal{D}_1 \text{ and } F_m \in \mathcal{D}_0 \right\}$$

$$= \left\{ \bigcup_{j=1}^{n_r} (B_j \times \{j\}) : B_j \in \mathcal{D}_1 \text{ when } j \in C, \right\}$$

$$\text{and } B_j \in \mathcal{D}_0 \text{ when } j \notin C \right\}. \quad (4.6)$$

$$\text{By doing this construction for each block } C \text{ of } \mathcal{D}_r, \text{ we define the composition of } \mathcal{D}_r, \mathcal{D}_0 \text{ and } \mathcal{D}_1.$$

**Definition 4.2.1**  The composition $\mathcal{D} = (\mathcal{D}_0, \mathcal{D}_1) \circ \mathcal{D}_r$ is defined as the following set of blocks over the set $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_r$:

$$\mathcal{D} = \bigcup_{C \in \mathcal{D}_r} \Delta(C). \quad (4.8)$$

$\mathcal{D}$ is a randomized Kronecker product; The elements of each block $C$ of $\mathcal{D}_r$ parametrize arbitrary blocks from $\mathcal{D}_1$ and the complement of $C$ parametrizes blocks from $\mathcal{D}_0$. 
If $\bigcup_{j=1}^{v_e}(B_j \times \{j\})$ is a block of $\mathcal{D}$, we call the subsets $B_j \times \{j\}$ the **columns** of the block. Then two blocks of $\mathcal{D}$ are equal iff the corresponding columns are the same.

**Lemma 4.2.2** $\mathcal{D}$ is simple if $\mathcal{D}_o$ and $\mathcal{D}_i$ are disjoint.

**Proof:** Let $\overline{B} = \bigcup_{j=1}^{v_e} B_j \times \{j\}$ and $\overline{B'} = \bigcup_{j=1}^{v_e} B'_j \times \{j\}$ be two blocks of $\mathcal{D}$ with $B$ and $B'$ as their underlying blocks from $\mathcal{D}_e$. We consider two cases depending on whether the underlying blocks are equal or not.

- $B = B'$: In the construction of $\mathcal{D}$, any two blocks with the same underlying block have at least one unmatching column. So $\overline{B} \neq \overline{B'}$.

- $B \neq B'$: In this case, there is a $j$ in $B$ not in $B'$. So $B_j$ is in $\mathcal{D}_i$ and $B'_j$ is in $\mathcal{D}_o$. $\mathcal{D}_i$ is disjoint from $\mathcal{D}_o$, and so $B_j \neq B'_j$. Hence $\overline{B} \neq \overline{B'}$.

Therefore $\mathcal{D}$ is simple. $\square$

**Lemma 4.2.3** The blocks of $\mathcal{D}$ are of size $k = k_{c}k_{1} + k_{0}(v_{c} - k_{c})$.

**Proof:** Let $\overline{B} = \bigcup_{j=1}^{v_e} B_j \times \{j\}$ be a block of $\mathcal{D}$ with $B$ as the underlying block from $\mathcal{D}_e$. The columns of $\overline{B}$ are disjoint from each other. So the size of a block is

$$k = |\overline{B}|$$

$$= \left| \bigcup_{j \in B} B_j \times \{j\} \right| + \left| \bigcup_{j \in \lambda_r \setminus B} B_j \times \{j\} \right|$$

$$= \sum_{j \in B} |B_j| + \sum_{j \in \lambda_r \setminus B} |B_j| \quad (4.9)$$

and since $B_j$ is in $\mathcal{D}_i$ or $\mathcal{D}_o$ depending on whether $j$ is in $B$ or not, we get

$$k = |B|k_{1} + |\lambda_{r} \setminus B|k_{0}$$

$$= k_{c}k_{1} + (v_{c} - k_{c})k_{0} \quad (4.10)$$
and this gives the size of each block in $D$.

Let $b_r, b_0$ and $b_1$ be the number of blocks of $D_r$, $D_0$ and $D_1$.

**Lemma 4.2.4** The number of blocks in $D$ is $b = b_r b_1^{k_r} b_0^{v_r - k_r}$.

**Proof:** Let $B$ be a block in $D_r$ and $\Delta(B)$ be the set of blocks in $D$ with $B$ as the underlying block. Then

$$\Delta(B) = \left\{ \bigcup_{j=1}^{v_r} B_j \times \{ j \} : B_j \in D_1 \text{ when } j \in B, \right.$$  
and $B_j \in D_o$ when $j \notin B \right\}.$ \hfill (4.11)

$B_j$ has $|D_1|$ choices for each $j$ in $B$ and $|D_o|$ choices for each $j$ not in $B$. And the choice of $B_j$ and $B_j'$ are independent of each other for $j \neq j'$. So

$$|\Delta(B)| = \left( \prod_{j \in B} |D_1| \right) \left( \prod_{j \notin B} |D_o| \right)$$  
$$= b_r^{k_r} b_0^{v_r - k_r}.$$ \hfill (4.12)

So the size of $\Delta(B)$ is independent of $B$. And since $D$ is a disjoint union of $\Delta(B)$'s as $B$ varies through $D_r$, we get:

$$b = |D| = \left| \bigcup_{B \in D_r} \Delta(B) \right|$$  
$$= \sum_{B \in D_r} |\Delta(B)| = b_r |\Delta(B)|$$  
$$= b_r b_1^{k_r} b_0^{v_r - k_r}.$$ \hfill (4.13)

and this gives the number of blocks in $D$. \hfill $\Box$
So far, we have shown that $\mathcal{D}$ is a family of $k$-sets of $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_r$ of size $b$. In general, $\mathcal{D}$ is not a $t$-design. But as we will see in the next section, it is always a partially balanced design of a special type.

4.3 Compatibility Conditions.

First, we specialize to the case of $t = 2$.

Given two points $p = (x, l)$ and $q = (y, m)$ in $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_r$, we want to count the blocks of $\mathcal{D}$ containing $p$ and $q$. Let $\overline{B} = \bigcup_{j=1}^{r^*} B_j \times \{j\}$ be a block of $\mathcal{D}$ containing both $p$ and $q$. Then, there are two possibilities:

(A) $p$ and $q$ are in the same column of $\overline{B}$.

(B) $p$ and $q$ are in separate columns of $\overline{B}$.

In the following two lemmas we count the number blocks of $\mathcal{D}$ containing both $p$ and $q$ in each of the above cases.

In what follows, the primed variables are the corresponding parameters for the complementary designs [5]: $k' = v - k$, $r' = b - r$, $\lambda' = b - 2r + \lambda$, and $\eta = r - \lambda$ is the number of blocks containing a given point and avoiding another. Also, by convention, $b = 1$ when $k = 0$.

Lemma 4.3.1 If $p$ and $q$ are in the same column of $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_r$, then the number of blocks in $\mathcal{D}$ containing them is

$$N_1 = r_r \lambda_1 b_0^{k_r} b_1^{k_r - 1} + r_r' \lambda_0 b_0^{k_r} b_1^{k_r}.$$  

(4.14)

Proof: Since $p = (x, l)$ and $q = (y, m)$ are in the same column, $l = m$. 

Let $\overline{B} = \bigcup_{j=1}^{v_c} B_j \times \{j\}$ be a block of $\mathcal{D}$ with $B$ as the underlying block from $\mathcal{D}_r$. If $\overline{B}$ contains both $p$ and $q$ then they both will be in the $B_l \times \{l\}$ column of $\overline{B}$. Consequently, $B_l$ is a block of $\mathcal{D}_o$ or $\mathcal{D}_i$ containing both $x$ and $y$. For all the other columns $B_j \times \{j\}$ of $\overline{B}$ with $j \neq l$, $B_j$ can be any of the $b_1$ blocks of $\mathcal{D}_i$ or any of the $b_0$ blocks of $\mathcal{D}_o$ depending on whether $j$ is in $B$ or not. This splits the counting into two cases as follows:

**Case 1** 
$l$ is in the underlying block $B$ of $\overline{B}$.

Since $l$ is in $B$, $B_l$ is from $\mathcal{D}_i$ and it can be picked to be any of the $\lambda_1$ blocks of $\mathcal{D}_i$ containing $x$ and $y$. $l$ being in $B$ leaves $\overline{B}$ with $(k_r - 1)$ other columns $B_j \times \{j\}$ which have $j$ in $B$ and each of those can be any of the $b_1$ blocks of $\mathcal{D}_i$. There are now $(v_c - k_r)$ columns $B_j \times \{j\}$ of $\overline{B}$ with $j$ not in $B$ and each of those $B_j$'s can be picked to be any of the $b_0$ blocks of $\mathcal{D}_o$. Since $B_j$ are chosen independent of each other for different $j$'s, this gives $\lambda_1 b_0^{v_c-k_r} b_1^{k_r-1} = \lambda_1 b_0^{k_r} b_1^{k_r-1}$ blocks of $\mathcal{D}$ containing $p$ and $q$, for each $B$ in $\mathcal{D}_c$ containing $l$.

But there are $r_c$ blocks $B$ of $\mathcal{D}_c$ containing $l$. Hence there are $r_c \lambda_1 b_0^{k_r} b_1^{k_r-1}$ blocks of $\mathcal{D}$ containing $p$ and $q$ in this case.

**Case 2** 
$l$ is not in the underlying block $B$ of $\overline{B}$.

Since $l$ is not in $B$, $B_l$ is from $\mathcal{D}_o$ and has $\lambda_0$ choices and each of the $k_r$ columns $B_j \times \{j\}$ of $\overline{B}$ with $j$ in $B$ has for $B_j$ any of the $b_1$ blocks of $\mathcal{D}_i$. For $j \neq l$, there are $(v_c - k_r - 1) = (k'_r - 1)$ columns $B_j \times \{j\}$ of $\overline{B}$ with $j$ not in $B$ and each of those $B_j$'s can be picked to be any of the $b_0$ blocks of $\mathcal{D}_o$. So for each block $B$ in $\mathcal{D}$ not containing $l$, we get $\lambda_0 b_0^{k'_r-1} b_1^{k_r}$ blocks of $\mathcal{D}$ containing $p$ and $q$. There are
$r'_r = (b_r - r_r)$ blocks of $\mathcal{D}_r$ not containing \(l\), and that gives \((b_r - r_r)\lambda_0 b_0^{k'_r - 1} b'_r\) blocks of $\mathcal{D}$ containing $p$ and $q$ in this case. Therefore, from the two cases above we get that if $p$ and $q$ are two points of $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_r$ which are in the same column, then there are

$$N_1 = v_r \lambda_1 b_0^{k'_r} b'_1^{k_r - 1} + r'_r \lambda_0 b_0^{k'_r - 1} b'_1$$

blocks of $\mathcal{D}$ containing both $p$ and $q$. \hfill \square

**Lemma 4.3.2** When $p$ and $q$ are in separate columns of $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_r$, then the number of blocks is

$$N_2 = \lambda_r v'_1 b_0^{k'_r} b'_1^{k_r - 2} + 2n_r v_r v_1 b_0^{k'_r - 1} b'_1^{k_r - 1} + \lambda'_r v'_0 b_0^{k'_r - 2} b'_1.$$

**Proof:** Let $p = (x, l)$ and $q = (y, m)$. Since $p$ and $q$ are in separate columns, $l \neq m$. If $p$ and $q$ are in a block $\overline{B} = \bigcup_{j=1}^{r_r} (B_j \times \{j\})$ of $\mathcal{D}$, then $p$ lies in the column $B_l \times \{l\}$ and $q$ in $B_m \times \{m\}$ with $x$ in $B_l$ and $y$ in $B_m$. Let $B$ be the underlying block of $\overline{B}$ in $\mathcal{B}_r$. Counting the number of blocks containing $p$ and $q$ in this case depends on whether $l, m$ are in $B$ or not. This gives the following four cases.

**Case 1** Both $l$ and $m$ are in the underlying block $B$.

In this case, both $B_l$ and $B_m$ are from $\mathcal{D}_1$. Since $x \in B_l$, $y \in B_m$ and the choice of $B_l, B_m$ are independent, both $B_l$ and $B_m$ have $r_1$ choices each in $\mathcal{D}_1$. For $j \neq l, m$, $\overline{B} = \bigcup_{j=1}^{r_r} (B_j \times \{j\})$ has $(k_r - 2)$ columns with $j$ in $B$ and each of those $(k_r - 2)$ columns can have any of the $b_1$ blocks of $\mathcal{D}_1$ as $B_j$. This leaves us with $(v_r - k_r) = k'_r$ columns of $\overline{B} = \bigcup_{j=1}^{r_r} (B_j \times \{j\})$ with their $j$’s not in $B$ and each of those columns
can have any of the $b_0$ blocks of $\mathcal{D}_o$ as $B_j$. So, for a fixed $B$ in $\mathcal{D}_e$ containing both $l$ and $m$, there are $r_1^2 b_0^{k'_e} b_1^{k_e-2}$ blocks of $\mathcal{D}$ containing $p$ and $q$. There are $\lambda_e$ blocks of $\mathcal{D}_e$ containing $l$ and $m$. Hence $\mathcal{D}$ has $\lambda_e r_1^2 b_0^{k'_e} b_1^{k_e-2}$ blocks containing $p$ and $q$ in this case.

**Case 2**  The underlying block $B$ in $\mathcal{D}_e$ contains $l$ but not $m$.

In this case, $B_l$ is a block of $\mathcal{D}_i$ containing $x$ and so has $r_1$ choices, and $B_m$ is a block of $\mathcal{D}_o$ containing $y$ and so has $r_0$ choices. For $j \neq l, m$, $B = \bigcup_{j=1}^{r_e} (B_j \times \{j\})$ has $(k_e - 1)$ columns with $j$ in $B$ and each of those columns can have any of the $b_1$ blocks of $\mathcal{D}_i$ as $B_j$, and $(v_e - k_e - 1) = (k'_e - 1)$ columns with $j$ not in $B$ and $B_j$ for each of those columns can be any of the $b_0$ blocks of $\mathcal{D}_o$. So, for a fixed $B$ in $\mathcal{D}_e$ containing $l$ and not containing $m$, there are $r_0 r_1 b_0^{k'_e - 1} b_1^{k_e - 1}$ blocks of $\mathcal{D}$ containing $p$ and $q$. There are $\eta_e = (r_e - \lambda_e)$ blocks of $\mathcal{D}_e$ containing $l$ and not containing $m$. Hence $\mathcal{D}$ has $\eta_e r_0 r_1 b_0^{k'_e - 1} b_1^{k_e - 1}$ blocks containing both $p$ and $q$.

**Case 3**  The underlying block $B$ contains $m$ but not $l$.

This case is exactly the same as the previous one with $l$ and $m$ swapped. So the number of blocks of $\mathcal{D}$ containing $p$ and $q$ in this case is the same as in the last case and is given by $\eta_e r_0 r_1 b_0^{k'_e - 1} b_1^{k_e - 1}$.

**Case 4**  Neither $l$ nor $m$ is in the underlying block $B$.

In this case, both $B_l$ and $B_m$ are in $\mathcal{D}_o$. Since $x \in B_l$, $y \in B_m$ and the choice of $B_l$, $B_m$ are independent, each of them have $r_0$ choices. For $j \neq l, m$, $B = \bigcup_{j=1}^{r_e} (B_j \times \{j\})$ has $(v_e - k_e - 2) = (k'_e - 2)$ columns with $j$ not in $B$ and each of those columns can have any of the $b_0$ blocks of $\mathcal{D}_o$ as $B_j$. $\overline{B}$ has $k_e$ remaining columns and they all
have their j’s in B. Each of those k_e columns can have any of the b_1 blocks of D as B_j. So, for each block of B in D not containing either of l, m, there are r_0^2 b_0 k_e - 2 b_1 blocks of D containing p and q. There are \lambda'_e b_e - 2r_e + \lambda_e blocks of D not containing either of l, m. Hence D has \lambda'_e r_0^2 b_0 k_e - 2 b_1 blocks of D containing both p and q in this case. Therefore, from all the four cases above, we get that when p and q are in separate columns of \mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_r, then there are

\[ N_2 = \lambda_e r_1^2 b_0^2 k_e - 2 + 2r_e r_0 b_0^2 k_e - 1 b_1 + \lambda'_e r_0^2 b_0^2 k_e - 2 b_1 \]  

(4.17)

blocks of D containing both p and q.

\[ \square \]

From Lemma (4.3.1) and Lemma (4.3.2), we derive that if p and q are any two points of \mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_r then \{p, q\} is contained in N_1 or N_2 blocks of D. N_1 and N_2 do not depend on particular p or q. Let \Lambda = \{N_1, N_2\}. Then, the above result gives the following theorem.

**Theorem 4.3.3**  
If D_e is a 2-(v_e, k_e, \lambda_e) design, and D_i, for i = 0, 1, are 2-(v_i, k_i, \lambda_i) designs, then their composition D = (D_0, D_1) o D_e is a 2-(v, k, \Lambda) partially balanced design with \(v = v_1 v_e, k = k_1 k_e + k_0 (v_e - k_e), \) and \(\Lambda\) of size at most two.

The composition is a balanced design when \(N_1 = N_2\), we equate the two quantities in (4.14) and (4.16) and obtain:

\[
r_e \lambda_1 b_0^2 b_1^{k_e - 1} + r'_e \lambda_0 b_0^{k_e - 1} b_1^{k_e - 2} = \lambda_e r_1^2 b_0^2 b_1^{k_e - 2} + 2r_e r_0 b_0^2 b_1^{k_e - 1} + \lambda'_e r_0^2 b_0^{k_e - 2} b_1^{k_e}.
\]  

(4.18)
Using the the relations (4.4) and (4.5) above for \( \lambda \)'s and \( r \)'s, the above equation becomes

\[
\frac{b_0^{k_r} b_1^{k_r} b_c}{v_r \left( \frac{v_1}{2} \right)} \left[ k_r \left( \frac{k_1}{2} \right) + k_r' \left( \frac{k_0}{2} \right) \right]
\]

\[
= \frac{b_0^{k_r} b_1^{k_r} b_c}{v_1^2 \left( \frac{v_1}{2} \right)} \left[ k_r^2 \left( \frac{k_r}{2} \right) + k_1 k_0 k_r k_r' + k_0^2 \left( \frac{k_r'}{2} \right) \right]. \tag{4.19}
\]

After eliminating the \( b \)'s and simplifying, the above equation gives the following compatibility condition for obtaining a balanced design

\[
v_1(v_c - 1) \left[ k_r \left( \frac{k_1}{2} \right) + k_r' \left( \frac{k_0}{2} \right) \right]
\]

\[
= (v_1 - 1) \left[ k_r^2 \left( \frac{k_r}{2} \right) + k_1 k_0 k_r k_r' + k_0^2 \left( \frac{k_r'}{2} \right) \right]. \tag{4.20}
\]

By symmetry and to avoid certain trivial cases we make the following restrictions:

\[
0 < k_r < v_c, \tag{4.21}
\]

\[
0 \leq k_0 < k_1 < v_1, \tag{4.22}
\]

\[
2 \leq k_1. \tag{4.23}
\]

It is easy to show that the cases excluded by these restrictions are either redundant or lead to trivial results. Subject to the above constraints, \( \mathcal{D} \) does not contain all the \( k \)-sets since each block of \( \mathcal{D} \) has at most two column sizes \( k_0 \) and \( k_1 \); and so \( \mathcal{D} \) is always nontrivial. Lemma (4.2.2) shows that in \( \mathcal{D} \) no blocks are repeated if \( \mathcal{D}_u \) and \( \mathcal{D}_1 \) are disjoint; this is true since \( k_0 < k_1 \) by (4.22). We now have the following result.
Corollary 4.3.4  If $\mathcal{D}_c$ is a 2-$(v_r,k_r,\lambda_c)$ design, and $\mathcal{D}_i$ for $i=0,1$, are 2-$(v_i,k_i,\lambda_i)$ designs satisfying (4.21), (4.22), (4.23) and the compatibility condition (4.20), then their composition $\mathcal{D} = (\mathcal{D}_o, \mathcal{D}_i) \circ \mathcal{D}_c$ is a nontrivial simple 2-$(v,k,\lambda)$ design with $v = v_1 v_r$, $k = k_1 k_r + k_0 (v_r - k_r)$, and $\lambda$ as given by (4.5) and $b$ as in Lemma (4.24).

Our aim is to find $\mathcal{D}_o$, $\mathcal{D}_i$ and $\mathcal{D}_c$ satisfying the compatibility condition (4.20) and then use them to construct $\mathcal{D}$ as we defined earlier. Surprisingly, the compatibility condition (4.20) is independent of $\lambda_c$ and the $\lambda_i$'s; as a result, trivial designs can be used to construct nontrivial designs.

In the particular case when $k_0 = 0$, we get the following result:

Theorem 4.3.5 Given $\mathcal{D}_i$ and $\mathcal{D}_o$ with $k_0 = 0$, there are an infinite number of compatible $\mathcal{D}_c$'s whose parameters satisfy the compatibility condition

$$v_1(v_r - 1) \left[ k_r \left( \frac{k_1}{2} \right) + k_r' \left( \frac{k_0}{2} \right) \right] = (v_1 - 1) \left[ k_1^2 \left( \frac{k_r}{2} \right) + k_1 k_0 k_r k_r' + k_0^2 \left( \frac{k_r'}{2} \right) \right]. \quad (4.24)$$

Proof: Putting $k_0 = 0$ in the compatibility condition 4.20, we get

$$v_1(v_r - 1) k_r \left( \frac{k_1}{2} \right) = (v_1 - 1) k_1^2 \left( \frac{k_r}{2} \right). \quad (4.25)$$

We can rewrite the above equation as

$$\frac{k_r - 1}{v_r - 1} = \frac{v_1(k_1 - 1)}{k_1(v_1 - 1)}. \quad (4.26)$$
For a given $\mathcal{D}_1$, $v_1$ and $k_1$ are known. Let

$$\frac{p}{q} = \frac{v_1(k_1 - 1)}{k_1(v_1 - 1)}$$  \hspace{1cm} (4.27)

after reduction. Then if we let $k_r = pm + 1$ and $v_r = qn + 1$ in the above equation, we get

$$\frac{k_r - 1}{v_r - 1} = \frac{pm}{qn} = \frac{p}{q} = \frac{v_1(k_1 - 1)}{k_1(v_1 - 1)}$$

for all positive integer values of $n$. So $v_r = qn + 1$ and $k_r = pm + 1$ satisfy (4.26). Since for any given $\mathcal{D}_1$, there is always the trivial design for $\mathcal{D}_e$ with parameters $v_e = qn + 1$ and $k_e = pm + 1$, and those values of $v_e$ and $k_e$ satisfy (4.26) for all positive integer values of $n$, we get an infinite number of compatible $\mathcal{D}_e$'s that make the composition $\mathcal{D}$ a balanced design. \hspace{1cm} \square

4.4 Examples

(4.4.1) The 2-(4, 2, 1) trivial design as $\mathcal{D}_1$, and the 2-(4, 0, 0) trivial design, as $\mathcal{D}_o$, are compatible with all designs with parameters 2-(3$n$ + 1, 2$n$ + 1, $\lambda_e$) for $n \geq 1$.

Composing these gives 2-(12$n$ + 4, 4$n$ + 2, $\lambda$) designs. Taking $n = 2$ gives a 2-(28, 10, 19440) design. According to the recent tables in [2], this design is new.

(4.4.2) Composing the 2-(5,2,1) design as $\mathcal{D}_r$, with the 2-(5,3,3) design as $\mathcal{D}_1$, and the 2-(5,1,0) design as $\mathcal{D}_o$, we obtain a new 2-(25,9,15000) design.

4.5 Composition of 3-Designs.

We look at the composition of 3-designs in this section.
Let $\mathcal{D}_i$ be a $3-(v_i, k_i, \mu_i)$ design for $i = 0, 1$ with $\mathcal{X}_i$ as the underlying set and $\mathcal{D}_e$ a $3-(v_e, k_e, \mu_e)$ design with $\mathcal{X}_e$ as the underlying set. Like before, $v_1 = v_0$ here also. Then $\mathcal{D}_0$, $\mathcal{D}_1$ and $\mathcal{D}_e$ are also 2-designs. In the following, $r$'s, $b$'s and $\lambda$'s are as before.

The composition $\mathcal{D}$ over $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_e$ of the 3-designs $\mathcal{D}_0$, $\mathcal{D}_1$ and $\mathcal{D}_e$ is defined the same way as the composition of 2-designs in (4.8). Then $\mathcal{D}$ has the following property.

**Theorem 4.5.1** If $\mathcal{D}_e$ is a $3-(v_e, k_e, \mu_e)$ design, and $\mathcal{D}_i$, for $i = 0, 1$, are $3-(v_i, k_i, \mu_i)$ designs, then their composition $\mathcal{D} = (\mathcal{D}_0, \mathcal{D}_1) \circ \mathcal{D}_e$ is a $3-(v, k, \Lambda)$ partially balanced design with $v = v_1 v_e$, $k = k_1 k_e + k_0(v_e - k_e)$, and $\Lambda$ of size at most three.

**Proof:** Let $\{a, b, c\}$ be three points from the underlying set $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_e$ of $\mathcal{D}$. We want to count the number blocks in $\mathcal{D}$ containing $\{a, b, c\}$. If $v_e \geq 3$, then we have the following three possibilities and in each of those three cases the number of blocks containing $a$, $b$ and $c$ is counted in a manner similar to the one in the case of the composition of 2-designs given in the last section. The possibilities are:

(A) All three points $\{a, b, c\}$ are in the same column of $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_e$.

Let $\mu_A$ be the number of blocks in $\mathcal{D}$ containing $\{a, b, c\}$ in this case. Then

$$\mu_A = (b_e - r_e) \mu_0 b_1 k_r b_0^{v_e - k_r - 1} + r_e \mu_1 b_1^{k_e - 1} b_0^{v_e - k_e}. \quad (4.28)$$

(B) Two of $\{a, b, c\}$ are in one column and the third in a separate column of $\mathcal{X}$.
In this case, let $\mu_B$ be the number of blocks of $\mathcal{D}$ containing $\{a, b, c\}$. Then

$$
\mu_B = \lambda r_1 r_1 b_1^{k_r-2} b_0^{v_r-k_r-1} + (r_c - \lambda_c) \lambda r_0 b_1^{k_r-1} b_0^{v_r-k_r-1}
+ (r_c - \lambda_c) r_1 \lambda b_0^{v_r-k_r-1} + (b_c - 2r_c + \lambda_c) \lambda r_0 b_1^{k_r} b_0^{v_r-k_r-1}. \tag{4.29}
$$

(C) All three points $\{a, b, c\}$ are in separate columns of $\mathcal{X}$.

Let $\mu_C$ be the number of blocks in $\mathcal{D}$ containing $\{a, b, c\}$ in this case. Then

$$
\mu_C = \mu_c r_1^3 b_1^{k_r-3} b_0^{v_r-k_r} + 3(\lambda_c - \mu_c) r_1^2 r_0 b_1^{k_r-2} b_0^{v_r-k_r-1}
+ (r_c - 2\lambda_c + \mu_c) r_1 r_0^2 b_1^{k_r-1} b_0^{v_r-k_r-2}
+ (b_c - 3r_c + 3\lambda_c - \mu_c) r_c^3 b_1^{k_r} b_0^{v_r-k_r-3}. \tag{4.30}
$$

If $v_c = 2$, then only the first two cases occur. So, for any three points of $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_e$, if $\mu$ is the number of blocks of $\mathcal{D}$ containing them, then $\mu$ is in

$$
\Lambda = \{\mu_A, \mu_B, \mu_C\} \text{ if } v_e \geq 3, \tag{4.31}
$$

and is in

$$
\Lambda = \{\mu_A, \mu_B\} \text{ if } v_e = 2. \tag{4.32}
$$

In any case, $\Lambda$ is at most of size three. Hence $\mathcal{D}$ is a partially balanced 3-design. \(\Box\)

The composition will be a balanced 3-design when

$$
\mu_A = \mu_B = \mu_C \text{ for } v_e \geq 3, \tag{4.33}
$$

and

$$
\mu_A = \mu_B \text{ for } v_e = 2. \tag{4.34}
$$
These equations (whichever applies) are called the compatibility conditions on the 3-designs $\mathcal{D}_o$, $\mathcal{D}_i$ and $\mathcal{D}_e$ for their composition to be balanced. These equations can be simplified to the point where they only involve the $v$'s and the $k$'s. Thus we have the analog of theorem (4.3.3) and the corollary (4.3.4).

As an example, we consider the case of only two columns, so that $v_e = 2$ and $k_e = 1$ and $\mathcal{D}_e$ is the 3-(2,1,0) trivial design. In this case we can get the parameters of all the interior designs $\mathcal{D}_o$, $\mathcal{D}_i$ that are compatible with this $\mathcal{D}_e$ and give a nontrivial composition, as shown below.

**Lemma 4.5.2**  
Let $\mathcal{D}_e$ be the 3-(2,1,0) trivial design over $\mathcal{X}_e$ and $\mathcal{D}_i$ for $i = 0, 1$, be 3-$(v_i, k_i, \mu_i)$ designs over $\mathcal{X}_i$, compatible with $\mathcal{D}_e$. Then, the composition $\mathcal{D} = (\mathcal{D}_o, \mathcal{D}_i) \circ \mathcal{D}_e$ is a 3-design if and only if it is a 2-design.

**Proof:** A 3-design is always a 2-design. So, we just need to show that if $\mathcal{D}$ is a 2-design, then it is a 3-design. For that we need to show that $\mu_A = \mu_B$ where $\mu_A$ and $\mu_B$ are as in (4.28) and (4.29). Putting $v_e = 2$, $k_e = 1$ in $\mu_A$, $\mu_B$ gives

\begin{align*}
\mu_A &= \mu_1 b_0 + \mu_0 b_1 \quad \text{and} \\
\mu_B &= \lambda_1 r_0 + \lambda_0 r_1.
\end{align*}

Suppose $\mathcal{D}$ is a 2-design. Any two points of $\mathcal{X}$ are either in the same column or in different columns of $\mathcal{X}$. Let $L$ be the number of blocks of $\mathcal{D}$ containing two given points of $\mathcal{X}$ if they are in the same column and let $l$ be the number of blocks in $\mathcal{D}$ containing two given points of $\mathcal{X}$ if they are in different columns. Then

\begin{align*}
L &= \lambda_1 b_0 + \lambda_0 b_1 \quad \text{and}
\end{align*}

(4.37)
\[ l = 2r_0r_1. \] (4.38)

Since we are assuming \( \mathcal{D} \) to be a 2-design, \( L = l \). To show that \( \mathcal{D} \) is a 3-design, we need to show that \( \mu_A = \mu_B \). The parameters of \( \mathcal{D} \) are \( v = 2v_1, k = k_1 + k_2 \). Then

\[
\mu_B = \lambda_1r_0 + \lambda_0r_1 = \frac{k_1 - 1}{v_1 - 1}r_0r_1 + \frac{k_0 - 1}{v_1 - 1}r_0r_1 \\
= \frac{k_1 + k_0 - 2}{2(v_1 - 1)}2r_0r_1 = \frac{k - 2}{v - 2}2r_0r_1 = \frac{k - 2}{v - 2}. \quad (4.39)
\]

Let

\[
\alpha = \frac{v_1 - 2}{2(v_1 - 1)} \quad \text{and} \quad \beta = \frac{v_1}{2(v_1 - 1)}. \quad (4.40)
\]

Then \( \alpha + \beta = 1 \). So

\[
\alpha\mu_A + \beta\mu_B = \frac{v_1 - 2}{2(v_1 - 1)}(\mu_A + \mu_B) + \frac{v_1}{2(v_1 - 1)}(\lambda_1r_0 + \lambda_0r_1) \\
= \frac{v_1 - 2}{2(v_1 - 1)}\left(\frac{k_1 - 2}{v_1 - 2}\lambda_1b_0 + \frac{k_0 - 2}{v_1 - 2}\lambda_0b_1\right) + \frac{v_1}{2(v_1 - 1)}(\lambda_1r_0 + \lambda_0r_1) \\
= \frac{1}{2(v_1 - 1)}((k_1 - 2)\lambda_1b_0 + (k_0 - 2)\lambda_0b_1) + \frac{v_1}{2(v_1 - 1)}\left(\frac{\lambda_1b_0k_0}{v_1} + \lambda_0\frac{b_1k_1}{v_1}\right) \\
= \frac{k - 2}{v - 2}(\lambda_1b_0 + \lambda_0b_1) = \frac{k - 2}{v - 2}L. \quad (4.41)
\]

Using the fact that \( L = l \) and (4.39), we get

\[
\alpha\mu_A + \beta\mu_B = \frac{k - 2}{v - 2}L = \frac{k - 2}{v - 2}l = \mu_B. \quad (4.42)
\]

So

\[
\alpha\mu_A = (1 - \beta)\mu_B = \alpha\mu_B
\]

since \( \alpha + \beta = 1 \). From (4.21) and (4.22), \( v_1 > 2 \). So \( \alpha \neq 0 \). Therefore \( \mu_A = \mu_B \).

Hence, if \( \mathcal{D} \) is a 2-design, then it is also a 3-design. \( \square \)
Theorem 4.5.3  
If $\mathcal{D}_i$ is the $3-(2, 1, 0)$ trivial design and $\mathcal{D}_i$ is a $3-(v_i, k_i, \mu_i)$ design for $i = 0, 1$, then the composition $\mathcal{D} = (\mathcal{D}_o, \mathcal{D}_i) \circ \mathcal{D}_r$ is a nontrivial $3-(v, k, \mu)$ design if and only if for some integer $n \geq 2$ and

$$d \text{ is a divisor of } \frac{n^2(n^2 - 1)}{4},$$

$$k_0 = \frac{n^2 - n}{2} + d, \quad k_1 = \frac{n^2 + n}{2} + d, \quad \text{and} \quad v_1 = \frac{k_0 k_1}{d}$$

with no restriction on $\mu_0$ or $\mu_1$. Then, the corresponding parameters for $\mathcal{D}$ are

$$v = \frac{1}{2d} \left((n^2 + 2d)^2 - n^2\right), \quad k = n^2 + 2d$$

(4.43)

and $\mu$ as in (4.35) or (4.36).

Proof: From Lemma (4.5.2), $\mathcal{D}$ is a 3-design iff it is a 2-design. So, it is sufficient to show that $\mathcal{D}$ is a nontrivial 2-design iff the parameters of $\mathcal{D}_o$ and $\mathcal{D}_i$ are as given above.

- First we show that if $\mathcal{D}$ is a nontrivial 2-design, then the parameters of $\mathcal{D}_o$ and $\mathcal{D}_i$ are as above. If $\mathcal{D}$ is a nontrivial 2-design, then $\mathcal{D}_r$, $\mathcal{D}_o$ and $\mathcal{D}_i$ satisfy the compatibility condition in (4.20) and the constraints in (4.22), (4.23). Putting the values $v_r = 2$, $k_r = 1$ in (4.20), we derive that $k_0$, $k_1$ and $v_1$ satisfy

$$\left(\binom{k_0}{3} + \binom{k_1}{3}\right) = \frac{k_1}{v_1} \left(\binom{k_0}{2} + \binom{k_1}{2}\right)$$

(4.44)

subject to

$$0 \leq k_0 < k_1 < v_1 \quad \text{and} \quad 2 \leq k_1.$$
If $k_0 = 0$, then (4.44) gives $k_1 = 1$, which contradicts (4.45). So, $k_0 \geq 1$ and we get

$$1 \leq k_0 < k_1 < v_1$$  \hfill (4.46)$$

which consequently gives $v_1 > 2$. Simplifying (4.44) gives

$$\begin{align*}
(k_1^2 - k_1 + k_0^2 - k_0)v_1 &= 2k_0k_1(v_1 - 1) \\
\iff (k_1 - k_0)^2v_1 &= (k_1 + k_0)v_1 - 2k_0k_1 \\
\iff ((k_1 - k_0)^2 - (k_1 + k_0))v_1 &= -2k_0k_1. \quad (4.47)
\end{align*}$$

But

$$(k_1 - k_0)^2 - (k_1 + k_0) = k_1(k_1 - 1) + k_0(k_0 - 1) - 2k_0k_1 \equiv 0 \pmod{2} \quad (4.48)$$

Using (4.48) in (4.47), we get $2v_1$ divides $2k_0k_1$. So

$$2k_0k_1 = 2dv_1 \quad (4.49)$$

for some $d$ and $d \geq 1$ from (4.46). From (4.47) and (4.49),

$$(k_1 - k_0)^2 = k_1 + k_0 - 2d. \quad (4.50)$$

Let

$$n = k_1 - k_0. \quad (4.51)$$

Then from (4.46), $n \geq 1$. If $n = 1$, then $k_1 = k_0 + 1$. Putting this in (4.44) gives $k_1 = v_1$ which contradicts (4.46). So $n \geq 2$. From (4.50) and (4.51) we get,

$$k_1 + k_0 = n^2 + 2d. \quad (4.52)$$
Solving for $k_0, k_1$ from (4.51) and (4.52), we get

$$k_0 = \frac{n^2 - n}{2} + d \quad (4.53)$$

$$k_1 = \frac{n^2 + n}{2} + d \quad (4.54)$$

and from (4.49),

$$v_1 = \frac{k_0 k_1}{d} \quad (4.55)$$

which proves the first part of the theorem.

- To prove the converse, let $n \geq 2$ be an integer and

$$d \text{ a divisor of } \frac{n^2 + n}{2} \cdot \frac{n^2 - n}{2}.$$  

Then $d \geq 1$. For this $d$, let

$$k_0 = \frac{n^2 - n}{2} + d, \quad k_1 = \frac{n^2 + n}{2} + d \quad \text{and} \quad v_1 = \frac{k_0 k_1}{d}.$$  

Since $n \geq 2$ and $d \geq 1$, we get

$$1 < k_0 < k_1 < v_1. \quad (4.56)$$

We can easily check that these values of $k_0, k_1$ and $v_1$ satisfy the compatibility condition in (4.44). So, for a given $n$ and $d$, for $\mathcal{D}_0, \mathcal{D}_1$ with the parameters $k_0, k_1$ and $v_1$ as given above, the composition $\mathcal{D} = (\mathcal{D}_0, \mathcal{D}_1) \circ \mathcal{D}_e$ is a 2-design, and it is nontrivial since (4.56) shows that $k_0, k_1$ and $v_1$ also satisfy (4.22) and (4.23), and this proves the converse. \qed

If $\mathcal{D}_e$ is the 3-(2,1,0) trivial design, then Theorem 4.5.3 gives all the solutions of the compatibility condition that result in nontrivial compositions. In this way we obtain an infinite number of 3-designs.
Definition 4.5.4 Let $\mathcal{A}$ be the automorphism group of a $t$-$(v, k, \lambda)$ design $\mathcal{D}$ over a set $\mathcal{X}$. Let $\mathcal{P} = \{P_1, P_2, \ldots, P_m\}$ be a partition of $\mathcal{X}$. Then $\mathcal{A}$ preserves $\mathcal{P}$ if for $\sigma \in \mathcal{A}$ and for each $i = 1, \ldots, m$, $\sigma(P_i) = P_j$ for some $j$ with $1 \leq j \leq m$. $\mathcal{A}$ is said to be point imprimitive on $\mathcal{X}$ if $\mathcal{A}$ preserves a nontrivial partition of $\mathcal{X}$. And, $\mathcal{A}$ is block transitive if it is transitive on the blocks of $\mathcal{D}$.

The following theorem is due to P.J.Cameron and C.E.Praeger.

Theorem 4.5.5 For a block transitive, point imprimitive $t$-$(v, k, \lambda)$ design $\mathcal{D}$,

$$v \leq \left(\frac{k}{2}\right) + 1$$

if the automorphism group $\mathcal{A}$ of $\mathcal{D}$ preserves a partition with either 2 parts or parts of size 2.

This result is stated in [14].

Theorem 4.5.6 Let $\mathcal{D}_e$ be the $3$-$(2, 1, 0)$ design. Then there are infinite number of compatible 3-designs $\mathcal{D}_o, \mathcal{D}_i$ for which the composition $\mathcal{D} = (\mathcal{D}_o, \mathcal{D}_i) \circ \mathcal{D}_e$ is a $3$-$(v, k, \mu)$ design with $v = \left(\frac{k}{2}\right) + 1$.

Proof: From Theorem 4.5.3, the parameters of $\mathcal{D}_o, \mathcal{D}_i$ are, for any $n \geq 2$ and

$$d \text{ a divisor of } \frac{n^2(n^2 - 1)}{4},$$

$$k_0 = \frac{n^2 - n}{2} + d, \quad k_1 = \frac{n^2 + n}{2} + d, \quad \text{and} \quad v_1 = \frac{k_0k_1}{d}. $$
We take \( D_0, D_1 \) to be the trivial designs with \( k_0, k_1 \) and \( v_1 \) as above. Then, the automorphism group of \( D_c \) is \( S_2 \) and the automorphism group of both \( D_0 \) and \( D_1 \) is \( S_n \), where \( S_n \) is the symmetric group over \( n \) elements. From Chapter 5, the automorphism group \( A \) of the composition \( D \) is the wreath product \( S_n \wr S_2 \). As we show in Chapter 5, since \( S_n \) and \( S_2 \) are block transitive, \( A = S_n \wr S_2 \) is also block transitive. So the automorphism group \( A \) of \( D \) is block transitive. As shown in Chapter 5, the automorphism of the composition is always point imprimitive. Since \( v_r = 2 \), the two columns of \( \lambda_1 \times \lambda_r \) give a partition of two parts and \( A = S_n \wr S_2 \) preserves that partition. Thus \( D = (D_0, D_1) \circ D_c \) satisfies all the conditions in Theorem 4.5.5. So the parameters of \( D \) satisfy \( v \leq \binom{k}{2} + 1 \). From Theorem 4.5.3, the parameters of \( D \) are

\[
v = \frac{1}{2d} \left( (n^2 + 2d)^2 - n^2 \right) \quad \text{and} \quad k = n^2 + 2d
\]

where \( n \geq 2 \) is any integer and \( d \) is as in (4.58). If we let \( d = 1 \), then

\[
v = \frac{1}{2} \left( (n^2 + 2)^2 - n^2 \right).
\]

And

\[
\binom{k}{2} + 1 = \binom{n^2 + 2d}{2} + 1 = \frac{1}{2} \left( (n^2 + 2)(n^2 + 2 - 1) + 2 \right) \\
= \frac{1}{2} \left( (n^2 + 2)^2 - (n^2 + 2) + 2 \right) = \frac{1}{2} \left( (n^2 + 2)^2 - n^2 \right) = v.
\]

So, for all \( n \geq 2 \) and \( d = 1 \), \( D \) attains the bound in Theorem 4.5.5. Thus we have proved the theorem. Also we can check that \( D \) does not attain the bound for any \( d > 1 \). \( \square \)
CHAPTER V

Automorphism Groups

5.1 Automorphism Group of the Composition Design

In this section, we assume that $t \geq 2$ and all designs are simple.

Let $\mathcal{D}_r$ be a $t\cdot(v_r, k_r, \lambda_r)$ design over the set $\mathcal{X}_r$ where $\mathcal{X}_r = \{1, 2, \ldots, v_r\}$, and $\mathcal{D}_i$, for $i=0,1$, be $t\cdot(v_i, k_i, \lambda_i)$ designs with $v_0 = v_1$ and both over the set $\mathcal{X}_1$. Let $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_r$.

The composition $\mathcal{D} = (\mathcal{D}_o, \mathcal{D}_1) \circ \mathcal{D}_r$ defined as the following set of blocks over the set $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_r$

$$
\mathcal{D} = \left\{ \bigcup_{j=1}^{v_r} (B_j \times \{j\}) : \text{for some } B \in \mathcal{D}_r, B_j \in \mathcal{D}_i \text{ when } j \in B, \right. 
\left. \text{and } B_j \in \mathcal{D}_o \text{ when } j \notin B \right\} 
$$

(5.1)

is a balanced design when $\mathcal{D}_r$, $\mathcal{D}_o$ and $\mathcal{D}_1$ satisfy the following compatibility condition

$$
v_1(v_r - 1) \left[ k_r \left( \begin{array}{c} k_1 \\ 2 \end{array} \right) + k'_r \left( \begin{array}{c} k_0 \\ 2 \end{array} \right) \right] = 
(v_1 - 1) \left[ k_1^2 \left( \begin{array}{c} k_r \\ 2 \end{array} \right) + k_1 k_0 k_r k_r' + k_0^2 \left( \begin{array}{c} k_r' \\ 2 \end{array} \right) \right].
$$

(5.2)

In this section we assume that $\mathcal{D}_r$, $\mathcal{D}_o$ and $\mathcal{D}_1$ satisfy the above compatibility condition for $\mathcal{D}$ to be a balanced design. To avoid certain trivial cases we make the
following restrictions on the parameters of \( \mathcal{D}_r, \mathcal{D}_o \) and \( \mathcal{D}_1 \):

\[
0 < k_r < v_r, \tag{5.3}
\]
\[
0 \leq k_0 < k_1 < v_1, \tag{5.4}
\]
\[
2 \leq k_1. \tag{5.5}
\]

The cases excluded by these restrictions are either redundant or lead to trivial results.

Here \( \mathcal{D}_o \) and \( \mathcal{D}_1 \) are always disjoint since \( k_0 < k_1 \) by (5.4).

Although the \( \lambda \) of a composition design is usually large, the automorphism group is often quite large also; this will be shown below.

A permutation on a set \( \mathcal{X} \) induces a permutation on the \( k \)-sets of \( \mathcal{X} \).

**Definition 5.1.1** An automorphism of a \( t-(v,k,\lambda) \)-design \( \mathcal{D} \) over the set \( \mathcal{X} \) is a permutation on \( \mathcal{X} \) that preserves the blocks of \( \mathcal{D} \).

The set of automorphisms of a \( t \)-design \( \mathcal{D} \) form a group under composition of maps and it is called the automorphism group of \( \mathcal{D} \).

Let \( \mathcal{A}_i \) be the automorphism group of \( \mathcal{D}_i \), for \( i=0,1 \), \( \mathcal{A}_r \) that of \( \mathcal{D}_r \), and \( \mathcal{A} \) that of their composition \( \mathcal{D} = (\mathcal{D}_o, \mathcal{D}_1) \circ \mathcal{D}_r \).

**Definition 5.1.2** For \( \nu = \{\nu_j\}_{j=1}^{v_r} \subseteq \mathcal{A}_o \cap \mathcal{A}_1 \), and \( \eta \in \mathcal{A}_r \) we define a map from \( \mathcal{X} \) into \( \mathcal{X} \) denoted by \( \nu \backslash \eta \), as follows: For \( a \times j \) in \( \mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_r \),

\[
(\nu \backslash \eta)(a \times j) = \nu_j(a) \times \eta(j). \tag{5.6}
\]

**Lemma 5.1.3** \( \nu \backslash \eta \) is a permutation of \( \mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_r \).
Proof: Clearly $\nu \eta$ is well-defined.

- To show that $\nu \eta$ is injective, suppose for $x \times j$ and $y \times l$ in $\mathcal{X}$,

$$
(\nu \eta)(x \times j) = (\nu \eta)(y \times l).
$$

Then

$$

\nu_j(x) \times \eta(j) = \eta(y) \times \eta(l).
$$

This means

$$
\nu_j(x) = \nu_l(y) \text{ and } \eta(j) = \eta(l).
$$

Since $\eta$ is injective on $\mathcal{X}$, $\eta(j) = \eta(l)$ implies $j = l$. Now $\nu_j(x) = \nu_l(y)$ becomes $\nu_j(x) = \nu_j(y)$. $\nu_j$ is injective on $\mathcal{X}$, so $\nu_j(x) = \nu_j(y)$ only if $x = y$. Thus

$$
(\nu \eta)(x \times j) = (\nu \eta)(y \times l) \quad \text{if and only if} \quad x = y \quad \text{and} \quad j = l.
$$

So $\nu \eta$ is injective.

- To show that $\nu \eta$ is surjective, pick an element $x \times j$ of $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_e$. Since $j$ is in $\mathcal{X}_e$ and $\eta$ surjective on $\mathcal{X}_e$, there is an element $l$ in $\mathcal{X}_e$ with $\eta(l) = j$. Similarly, since $\nu_l$ is surjective on $\mathcal{X}_1$ and $x$ is in $\mathcal{X}_1$, there is an element $y$ in $\mathcal{X}_1$ with $\nu_l(y) = x$.

Then

$$
(\nu \eta)(y \times l) = \nu_l(y) \times \eta(l) = x \times j.
$$

So $\nu \eta$ is surjective on $\mathcal{X}$.

Hence $\nu \eta$ is a permutation on $\mathcal{X}$.

The permutation of $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_e$ of the form $\nu \eta$ acts on the blocks of $\mathcal{D}$ given
in (5.1) as follows

\[(\nu \ast \eta) \left( \bigcup_{j=1}^{n_r} B_j \times \{j\} \right) = \bigcup_{j=1}^{n_r} (\nu_j(B_j) \times \{\eta(j)\}) \quad (5.7)\]

which shows that \(\eta\) permutes the columns of \(A\) and the \(\nu_j\)'s permute within the columns of \(A\).

**Definition 5.1.4** The set of permutations of \(X = X_1 \times X_r\) of the type \(\nu \ast \eta\), written as \((\mathcal{A}_n \cap \mathcal{A}_1) \ast \mathcal{A}_r\) is called a wreath product [4].

As we will see \((\mathcal{A}_n \cap \mathcal{A}_1) \ast \mathcal{A}_r\) is actually the automorphism group \(\mathcal{A}\) of \(D\).

For short, let \(\mathcal{W} = (\mathcal{A}_n \cap \mathcal{A}_1) \ast \mathcal{A}_r\).

**Lemma 5.1.5** \(\mathcal{W} = (\mathcal{A}_n \cap \mathcal{A}_1) \ast \mathcal{A}_r\) is a subgroup of \(\mathcal{A}\).

**Proof:** First we will show that \(\mathcal{W} = (\mathcal{A}_n \cap \mathcal{A}_1) \ast \mathcal{A}_r\) is a group. Let \(\sigma = \nu \ast \eta\) and \(\sigma' = \nu' \ast \eta'\) be two elements of \(\mathcal{W}\) where \(\nu = \{\nu_j\}_{j=1}^{n_r}\), \(\nu' = \{\nu'_j\}_{j=1}^{n_r}\) are subsets of \(\mathcal{A}_n \cap \mathcal{A}_1\), and \(\eta, \eta'\) are from \(\mathcal{A}_r\). We will show that \(\sigma \circ \sigma'\) is also an element of \(\mathcal{W}\). To that end, let \(x \times j\) be any element of \(\mathcal{X} = X_1 \times X_r\). Then

\[
(\sigma \circ \sigma')(x \times j) = \sigma(\sigma'(x \times j)) = \sigma\left(\nu'_j(x) \times \eta'(j)\right)
\]

\[
= (\nu_{\eta(j)}(\nu'_j(x))) \times \eta(\eta'(j)) = \left(\nu_{\eta(j)} \circ \nu'_j\right)(x) \times \left(\eta \circ \eta'(j)\right)
\]

\[
= \left[\{\nu_{\eta(j)} \circ \nu'_j\}_{j=1}^{n_r} \ast \mathcal{A}_r\right](x \times j) \quad (5.8)
\]

for every \(x \times j\) in \(\mathcal{X} = X_1 \times X_r\). So,

\[
\sigma \circ \sigma' = \nu \ast \left(\eta \circ \eta'\right)
\]
where \( \nu = \{ \nu_j(j) \circ \nu'_j \}_1^{\nu} \). Since \( \{ \nu_j(j) \}_1^{\nu} \) is just a permutation of the set \( \{ \nu_j \}_1^{\nu} \), it is also a subset of \( \mathcal{A}_o \cap \mathcal{A}_i \). So \( \nu_j(j) \) and \( \nu'_j \) are both in \( \mathcal{A}_o \cap \mathcal{A}_i \) for \( j = 1, \ldots, \nu \).

Also, since \( \mathcal{A}_o \cap \mathcal{A}_i \) is a group, we get, \( \nu_j(j) \circ \nu'_j \) is in \( \mathcal{A}_o \cap \mathcal{A}_i \) for \( j = 1, \ldots, \nu \).

Consequently, \( \nu = \{ \nu_j(j) \circ \nu'_j \}_1^{\nu} \) is contained in \( \mathcal{A}_o \cap \mathcal{A}_i \). Similarly, since \( \eta, \eta' \) are in \( \mathcal{A}_r \) and \( \mathcal{A}_r \) is group, \( \eta \circ \eta' \) is in \( \mathcal{A}_r \). Thus \( \nu \) is in \( \mathcal{A}_o \cap \mathcal{A}_i \) and \( \eta \circ \eta' \) is in \( \mathcal{A}_r \), so \( \sigma \circ \sigma' = \nu (\eta \circ \eta') \) is in \( \mathcal{W} \). Hence \( \mathcal{W} \) is closed under composition. And since \( \mathcal{W} \) is finite, it is group.

- Next we will show that \( \mathcal{W} = (\mathcal{A}_o \cap \mathcal{A}_i) \cap \mathcal{A}_r \) contained in \( \mathcal{A} \). Let \( \sigma = \nu \circ \eta \) be an element of \( (\mathcal{A}_o \cap \mathcal{A}_i) \cap \mathcal{A}_r \) where \( \nu, \eta \) are as before. We want to show that \( \sigma \) is in \( \mathcal{A} \). From (5.1.3), we know that \( \sigma \) is a permutation of \( \mathcal{X} \). To show \( \sigma \) is in \( \mathcal{A} \), we need to show that \( \sigma \) preserves the blocks of \( \mathcal{D} \). Let \( \overline{B} = \bigcup_{j=1}^{\nu} (B_j \times \{ j \}) \) be a block of \( \mathcal{D} \) with \( B \) as the underlying block in \( \mathcal{D}_r \). We claim that

\[
\sigma(\overline{B}) = \bigcup_{j=1}^{\nu} (\nu_j(B_j) \times \{ \eta(j) \})
\]

is a block of \( \mathcal{D} \) with \( \eta(B) \) as the underlying block from \( \mathcal{D}_r \). Since \( \eta \) is from \( \mathcal{A}_r \), it preserves the blocks of \( \mathcal{D}_r \). So, for \( B \) from \( \mathcal{D}_r \), \( \eta(B) \) must also be in \( \mathcal{D}_r \). Similarly, since \( \nu = \{ \nu_j \}_1^{\nu} \) is contained in \( \mathcal{A}_o \cap \mathcal{A}_i \), \( \nu_j \) preserves the blocks of both \( \mathcal{D}_o \) and \( \mathcal{D}_i \) for \( j = 1, \ldots, \nu \). Since \( B_j \) is from \( \mathcal{D}_1 \) (or \( \mathcal{D}_o \)) for \( j = 1, \ldots, \nu \), so \( \nu_j(B_j) \) is also is from \( \mathcal{D}_1 \) (or \( \mathcal{D}_o \)). From (5.4) \( k_0 < k_1 \), so \( \mathcal{D}_o \) and \( \mathcal{D}_i \) are disjoint. Thus

\[
\nu_j(B_j) \in \mathcal{D}_1 \text{ (or } \mathcal{D}_o \text{)} \iff B_j \in \mathcal{D}_1 \text{ (or } \mathcal{D}_o \text{)}.
\]

But

\[
B_j \in \mathcal{D}_1 \text{ (or } \mathcal{D}_o \text{)} \iff j \in B \text{ (or } \mathcal{X}_c \setminus B \text{)}
\]
and
\[ j \in B \; (\text{or } \mathcal{X} \setminus B) \iff \eta(j) \in \eta(B) \; (\text{or } \mathcal{X} \setminus \eta(B)). \]

Therefore
\[ \nu_j(B_j) \in \mathcal{D} \; (\text{or } \mathcal{D}_n) \iff \eta(j) \in \eta(B) \; (\text{or } \mathcal{X} \setminus \eta(B)). \]

This means
\[ \sigma(B) = \bigcup_{j=1}^{v_r} (\nu_j(B_j) \times \{\eta(j)\}) \]
is in \( \mathcal{D} \) with \( \eta(B) \) as the underlying block. Thus \( \sigma \) preserves the blocks of \( \mathcal{D} \) and so is in \( \mathcal{A} \). Therefore \((\mathcal{A}_n \cap \mathcal{A}_1) \setminus \mathcal{A}_r \) is contained in \( \mathcal{A} \). Hence it is a subgroup of \( \mathcal{A} \). \( \square \)

**Definition 5.1.6** For \( S \subseteq \mathcal{X} \) and \( \mathcal{D} \) a design over \( \mathcal{X} \), define

\[ \mathcal{D}_S = \{B \cap S : B \in \mathcal{D}\} \]

which is the set of restrictions of the blocks of \( \mathcal{D} \) to the set \( S \).

Like before, \( b = |\mathcal{D}| \), is the number of blocks of \( \mathcal{D} \), and \( r \) is the number of blocks containing any single point of \( \mathcal{X} \). Then

\[ r = \frac{bk}{v} \quad (5.9) \]

and

\[ \lambda = b \frac{\binom{k}{t}}{\binom{v}{t}}. \quad (5.10) \]
Lemma 5.1.7  If $\mathcal{D}$ is a $2-(v,k,\lambda)$ design over the set $\mathcal{X}$ with $0 < k < v$, and $S$ is a subset of $\mathcal{X}$ of size $s$ with $0 < s < v$, then the blocks of $\mathcal{D}_S$ do not have the same size.

Proof:  First we consider the following three trivial cases.

Case 1  $k = 1$.
Then $\mathcal{D}$ is a trivial design containing all blocks of size one. Since $v \geq 2$, $\mathcal{D}$ contains at least two blocks in this case. But $1 \leq s < v$, and so we can find a block of $\mathcal{D}$ that intersects with $S$ nontrivially and a block of $\mathcal{D}$ that does not intersect with $S$. Thus $\mathcal{D}_S$ has blocks of size zero as well as one. Hence the lemma is true in this case.

Case 2  $k = v - 1$.
In this case, the complementary design $\mathcal{D}^\circ$ has blocks of size one. Then, from Case 1, $(\mathcal{D}^\circ)_S$ does not have blocks of the same size. Since the blocks in $\mathcal{D}$ and $\mathcal{D}^\circ$ are complements, $\mathcal{D}_S$ does not have constant block size either.

Case 3  $s = 1$.
Since $0 < k < v$, we have $1 \leq r < b$ for $\mathcal{D}$ where $b$ is the number of blocks in $\mathcal{D}$ and $r$ is the number of blocks in $\mathcal{D}$ containing a given point in $\mathcal{X}$. So, in this case, we can find a block of $\mathcal{D}$ containing $S$ and a block of $\mathcal{D}$ not containing $S$. Then $\mathcal{D}_S$ has blocks of size both zero and one and so the lemma is true in this case.

In the remaining cases, we have $1 < k \leq v - 2$ and $s > 1$.

In the following cases, suppose the blocks of $\mathcal{D}_S$ have constant block size $w$. Then, since $k \geq 2$ and $s \geq 2$, we get $w \geq 2$ and so $\mathcal{D}_S$ is a $2-(s,w,\lambda^{(s)})$ design over the set $S$ (though not simple) with $b^{(s)} = b$, $r^{(s)} = r$ and $\lambda^{(s)} = \lambda$ since for any subset $T$ of
two points of $S$, $T$ is in $S \cap B$ for some block $B$ in $\mathcal{D}$ iff $T \subseteq B$ and there are $\lambda$ blocks of $\mathcal{D}$ containing any two points of $\mathcal{X}$. Using (5.9) and (5.10) in $r^{(s)} = r$ and $\lambda^{(s)} = \lambda$ for 2-designs, we get

\[ \frac{s}{w} = \frac{v}{k} \quad (5.11) \]

and

\[ \frac{\binom{s}{2}}{\binom{w}{2}} = \frac{\binom{v}{2}}{\binom{k}{2}}. \quad (5.12) \]

Since $w, k \geq 2$, we can divide the above equations to get

\[ s - w = v - k. \quad (5.13) \]

Since $s \geq 2$ and $w > 0$, we have

\[ s - w < s. \]

Depending on whether $k$ and $s$ are less than or equal to $v/2$ or not, we get the following four cases.

**Case 4** $2 \leq k \leq v/2$ and $2 \leq s \leq v/2$.

Then $v - k \geq v/2$. Since $s - w < s$, we have

\[ v/2 \leq v - k = s - w < s \leq v/2 \]

which gives $v/2 < v/2$. This contradiction proves the lemma in this case.

**Case 5** $2 \leq k \leq v/2$ and $2 \geq s > v/2$.

• $s < v - 1$.

In this case, we use $S^c = \mathcal{X} \setminus S$ instead of $S$. Let $s' = |S^c|$. Then $s' = v - s$. Then $\mathcal{D}_{S^c}$,
which is the restriction of \( D \) to \( S' \), will have constant block size \( w' = k - w \geq 2 \), since \( D_S \) has constant block size \( w \). So \( D_{S'} \) is a \( 2-(v - s, w', \lambda^{(s')}) \) design with \( b^{(s')} = b \), \( r^{(s')} = r \) and \( \lambda^{(s')} = \lambda \). Like before, relating the last two equations and using (5.9) and (5.10), we get

\[
v - k = s' - w'.
\]

Putting the values of \( s' \) and \( w' \) in gives

\[
v - k = (v - s) - (k - w).
\]

After simplification, the last equation becomes

\[
0 = -s + w \quad \text{or} \quad s = w.
\]

Using this relation together with the assumptions in this case, we have

\[
v/2 < s = w \leq k \leq v/2
\]

which gives \( v/2 < v/2 \). This contradiction proves the lemma in this subcase.

- \( s = v - 1 \).

Then \( S^c = \mathcal{X} \setminus S \) has size one. So, \( D_{S^c} \) does not have constant block size and hence \( D_S \) does not have constant block size either.

**Case 6** \( v - 2 \geq k > v/2 \) and \( 2 \leq s \leq v/2 \).

In this case we use the complementary design of \( D \) as in (4.1.2). We denote this complementary design by \( D^c \). Then \( D^c \) is a \( 2-(v, v - k, \lambda_c) \) design where

\[
\lambda_c = b \frac{\binom{v - k}{2}}{\binom{v}{2}}
\]
from (4.3). Let $b_r$, $r_e$ be the $b$ and $r$ of $\mathcal{D}_r$. Then $b_r = b$ and $r_e = (v - k)/v$. $(\mathcal{D}_r)_S$, which is the restriction of $\mathcal{D}_r$ to $S$ has constant block size $w' = s - w \geq 2$ since $v - k \geq 2$, $s \geq 2$ and $\mathcal{D}_S$ has constant block size $w$. So $(\mathcal{D}_r)_S$ is a $2-(s, w', \lambda(s))$ design with $b^{(s)} = b$, $r^{(s)} = r_e$ and $\lambda^{(s)} = \lambda_r$. Relating the last two equations and using (5.9) and (5.10), we have

$$v - (v - k) = s - w'.$$

After putting $w' = s - w$ and simplifying, the last equation gives $k = w$. Using this relation together with the assumptions in this case, we get

$$v/2 < k = w \leq s \leq v/2$$

which gives $v/2 < v/2$. This contradiction proves the lemma in this subcase.

**Case 7** \(v - 2 \geq k > v/2 \) and \(v > s > v/2\).

• $s < v - 1$.

Like in the last case, we use $\mathcal{D}_r$ in this case also. But instead of $S$, we use $S^c = \mathcal{X} \setminus S$ like in Case 2. Then $2 < s' = |S^c| = v - s < v/2$ since $s > v/2$ in this case. $(\mathcal{D}_r)_{S^c}$, the restriction of $\mathcal{D}_r$ to $S^c$ has constant block size $w' = (v - k) - (s - w) \geq 2$, since $v - k \geq 2$, $|S^c| \geq 2$ and $\mathcal{D}_S$ has constant block size $w$. So $(\mathcal{D}_r)_{S^c}$ is a $2-(v - k, w', \lambda(s^c))$ design with $b^{(s^c)} = b$, $r^{(s^c)} = r_e$ and $\lambda^{(s^c)} = \lambda_e$. Relating the last two equations and using (5.9), (5.10), we have

$$v - (v - k) = s' - w'.$$

After putting in $s' = v - s$, $w' = (v - k) - (s - w)$ and simplifying, we have

$$k = k - w. \ So, \ w = 0$$
which is a contradiction since \( w \geq 2 \). So the lemma is proved in this subcase.

\* \( s = v - 1 \).

Since \(|S| = v - 1 \) and \( k < v - 1 \), we get \( D_S \) has blocks of size both \( k \) and \( k - 1 \), and so the lemma is true in this subcase also.

Thus, for all possible values of \( s \) and \( k \), the lemma is true. Therefore, for \( 0 < k < v \) and \( 0 < s < v \), the blocks of \( D_S \) do not have constant block size. \( \square \)

**Lemma 5.1.8**  
*If the composition design \( D \) is nontrivial, then the automorphisms of \( D \) send columns of \( \mathcal{X} \) to columns of \( \mathcal{X} \).*

**Proof:** Suppose \( D \) had an automorphism \( \sigma \) which does not send columns of \( \mathcal{X} \) to columns of \( \mathcal{X} \). Then there would be two or more columns of \( \mathcal{X} \) parts of which go to the same column in the image under \( \sigma \). Let us say, parts of first and second columns of \( \mathcal{X} \) go to the \( r \)th column of the image \( \sigma(\mathcal{X}) \). Let

\[
P = \{ (x, 1) : \sigma(x, 1) = (y, r) \text{ for some } x, y \in \mathcal{X}_1 \},
\]

\[
Q = \{ (u, 2) : \sigma(u, 2) = (v, r) \text{ for some } u, v \in \mathcal{X}_1 \}.
\]

Then \( 0 < |P|, |Q| < v_1 \), and \( \sigma P, \sigma Q \subset \mathcal{X}_1 \times \{ r \} \) which is the \( r \)th column of \( \sigma(\mathcal{X}) \).

Then, in the first two columns nothing else other than \( P \) and \( Q \) gets mapped into the \( r \)th column of the image by \( \sigma \).

Since \( D \) is nontrivial, the parameters of \( D_o \), \( D_i \) and \( D_e \) satisfy (5.3), (5.4) and (5.5) and so we have the following cases.

**Case 1**  
\( D_i \) is nontrivial (ie, \( 0 < k_1 < v_1 \) and \( k_r \geq 2 \).
In this case, \( k_r \geq 2 \) and so we can find a block \( B \) in \( \mathcal{D}_r \) which contains \( \{1, 2\} \). Then, any block of \( \mathcal{D} \) with \( B \) as the underlying block must have its first two columns from \( \mathcal{D}_1 \). Let
\[
B = \{1, 2, \theta_1, \theta_2, \ldots, \theta_{k_r-2}\}
\]
for some \( \theta_1, \ldots, \theta_{k_r-2} \) in \( \mathcal{X}_r \). Pick \( A_{\theta_1}, A_{\theta_2}, \ldots, A_{\theta_{k_r-2}} \) to be some blocks from \( \mathcal{D}_1 \) and for \( j \in \mathcal{X}_r \setminus B \), pick \( A_j \)'s to be some blocks from \( \mathcal{D}_n \), and fix all of them. We define \( \mathcal{R}_B \) to be the following subset of blocks of \( \mathcal{D} \) with \( B \) as the underlying block from \( \mathcal{D}_r \).
\[
\mathcal{R}_B = \left\{ \left( A_1 \times \{1\} \right) \cup \left( A_2 \times \{2\} \right) \cup \left( \bigcup_{i=1}^{k_r-2} \left( A_{\theta_i} \times \{\theta_i\} \right) \right) \cup \left( \bigcup_{j \in \mathcal{X}_r \setminus B} A_j \times \{j\} \right) : A_1, A_2 \in \mathcal{D}_1 \right\}. \tag{5.14}
\]
Then, all the blocks in \( \mathcal{R}_B \) have the same \( j \)th column for \( 3 \leq j \leq v_r \). Let
\[
\mathcal{R}_B \cap P = \left\{ \overline{B} \cap P : \overline{B} \in \mathcal{R}_B \right\}.
\]
Since \( P \subset \mathcal{X}_1 \times \{1\} \) and by definition, \( \mathcal{R}_B \) has at least one block with any given block of \( \mathcal{D}_1 \) in its first column, we have
\[
\mathcal{R}_B \cap P = \left\{ (A \times \{1\}) \cap P : (A \times \{1\}) \subset \overline{B} \text{ for some } \overline{B} \in \mathcal{R}_B \right\}
= \left\{ (A \times \{1\}) \cap P : A \in \mathcal{D}_1 \right\}
\]
which is the restriction of \( \mathcal{D}_1 \) to \( P \), denoted by \( (\mathcal{D}_1)_P \). Since \( 0 < k_1 < v_1 \) in this case and \( 0 < |P| < v_1 \) by assumption, from Lemma 5.1.7, \( (\mathcal{D}_1)_P \) does not have constant block size. So \( (\mathcal{D}_1)_P \) has at least two different block sizes. For exactly the same
reasons as above, $\mathcal{R}_H \cap Q$ contains $(\mathcal{D}_i)_Q$ and $(\mathcal{D}_i)_Q$ has at least two different block sizes.

Let $\overline{B} = \bigcup_{j=1}^{v_r} (B_j \times \{j\})$ be a block in $\mathcal{R}_H$. Then

$$
\sigma(\overline{B}) = \bigcup_{j=1}^{v_r} \sigma(B_j \times \{j\})
$$

for some $C = \bigcup_{j=1}^{v_r} (C_j \times \{j\})$ in $\mathcal{D}$. Let $(\sigma \overline{B})_r$ denote the $r$th column of $\sigma \overline{B}$. Then $(\sigma \overline{B})_r = C_r \times \{r\}$. And since $\sigma P, \sigma Q \subseteq X_1 \times \{r\}$ in $\sigma X$, we have

$$
(\sigma \overline{B})_r = \left( (\sigma \overline{B})_r \cap \sigma P \right) \cup \left( (\sigma \overline{B})_r \cap \sigma Q \right) \cup \left( (\sigma \overline{B})_r \setminus (\sigma P \cup \sigma Q) \right).
$$

Since nothing else other than $P$ and $Q$ from the first and second columns of $X$ gets mapped into the $r$th column of $\sigma X$, the preimage of $\left( (\sigma \overline{B})_r \setminus (\sigma P \cup \sigma Q) \right)$ does not contain any element from the first and second columns of $\overline{B}$. So the preimage $\sigma^{-1}\left( (\sigma \overline{B})_r \setminus (\sigma P \cup \sigma Q) \right)$ is completely from the columns $3$ to $v_r$ of $\overline{B}$. Since by definition (5.14), all the blocks in $\mathcal{R}_H$ have the same $j$th column for each $j = 3, \ldots, v_r$, the preimage $\sigma^{-1}\left( (\sigma \overline{B})_r \setminus (\sigma P \cup \sigma Q) \right)$ is the same for all $\overline{B}$ in $\mathcal{R}_H$.

So $|\sigma^{-1}\left( (\sigma \overline{B})_r \setminus (\sigma P \cup \sigma Q) \right)|$ is a constant $c$, say, as $\overline{B}$ varies through $\mathcal{R}_H$. Thus

$$
| (\sigma \overline{B})_r | = | (\sigma \overline{B})_r \cap \sigma P | + | (\sigma \overline{B})_r \cap \sigma Q | + | (\sigma \overline{B})_r \setminus (\sigma P \cup \sigma Q) |
$$

$$
= | (\sigma \overline{B})_r \cap \sigma P | + | (\sigma \overline{B})_r \cap \sigma Q | + c.
$$

This gives

$$
| (\sigma \overline{B})_r \cap \sigma P | + | (\sigma \overline{B})_r \cap \sigma Q | = | (\sigma \overline{B})_r | - c
$$
for all \( \overline{B} \) in \( \mathcal{R}_B \). Since the \( r \)th column \( (\sigma \overline{B})_r = C_r \times \{ r \} \) of \( \sigma \overline{B} \) has \( C_r \) either from \( \mathcal{D}_a \) or \( \mathcal{D}_1 \),

\[
| (\sigma \overline{B})_r | = | C_r | = k_0 \text{ or } k_1 \tag{5.21}
\]

for all \( \overline{B} \) in \( \mathcal{R}_B \). Using (5.20) and (5.21), we have

\[
| (\sigma \overline{B})_r \cap \sigma P | + | (\sigma \overline{B})_r \cap \sigma Q | = k_0 - c \text{ or } k_1 - c \tag{5.22}
\]

for all \( \overline{B} \) in \( \mathcal{R}_B \). So as \( \overline{B} \) varies through \( \mathcal{R}_B \), the sum

\[
| (\sigma \overline{B})_r \cap \sigma P | + | (\sigma \overline{B})_r \cap \sigma Q |
\]

has at most two possible values. For \( \overline{B} = \bigcup_{j=1}^{v_1} (B_j \times \{ j \}) \),

\[
| (\sigma \overline{B})_r \cap \sigma P | = | \sigma^{-1} \left( (\sigma \overline{B})_r \cap \sigma P \right) | = | \overline{B} \cap P | = | B_1 \cap P |. \tag{5.23}
\]

As \( \overline{B} \) varies through \( \mathcal{R}_B \), \( B_1 \) varies through all the blocks of \( \mathcal{D}_1 \). So

\[
\{ | (\sigma \overline{B})_r \cap \sigma P | : \overline{B} \in \mathcal{R}_B \} = \{ | B_1 \cap P | : B_1 \in \mathcal{D}_1 \} = \text{ Set of block sizes of } (\mathcal{D}_1)_P. \tag{5.24}
\]

Since \( (\mathcal{D}_1)_P \) has at least two block sizes,

\[
| \{ | (\sigma \overline{B})_r \cap \sigma P | : \overline{B} \in \mathcal{R}_B \} | \geq 2. \tag{5.25}
\]

Also, \( 0 < k_1 < v_1 \) and \( | \mathcal{D}_1 | \geq 2 \). So, there are two blocks \( \overline{L}, \overline{L} \) in \( \mathcal{R}_B \) with \( L_1, L_1' \) from \( \mathcal{D}_1 \) in their first columns such that

\[
| (\sigma \overline{L})_r \cap \sigma P | = | L_1 \cap P | = p_1 \tag{5.26}
\]

and

\[
| (\sigma \overline{L}')_r \cap \sigma P | = | L_1' \cap P | = p_2 \tag{5.27}
\]
for some $p_1, p_2$ with $p_1 < p_2$. For exactly the same reasons as above, there are two blocks $\overline{M}, \overline{M'}$ of $\mathcal{R}_H$ with $M_2, M_2'$ from $\mathcal{D}$, in their second columns and

$$|(\sigma \overline{M})_r \cap \sigma Q| = |M_1 \cap Q| = q_1$$  \hspace{1cm} (5.28)

and

$$|(\sigma \overline{M'})_r \cap \sigma Q| = |M'_1 \cap Q| = q_2$$  \hspace{1cm} (5.29)

for some $q_1, q_2$ with $q_1 < q_2$. Then

$$p_1 + q_1 < p_1 + q_2 < p_2 + q_2.$$  \hspace{1cm} (5.30)

Since the blocks in $\mathcal{R}_B$ can have any element of $\mathcal{D}$, in the first two columns, $\mathcal{R}_H$ has three different blocks $\overline{X}, \overline{Y}, \overline{Z}$ such that $\overline{X}$ has $L_1, M_1$ as the first two columns, $\overline{Y}$ has $L_1, M'_1$ as the first two columns and $\overline{Z}$ has $L'_1, M'_1$ as the first two columns. Then

$$|(\sigma \overline{X})_r \cap \sigma P| + |(\sigma \overline{X})_r \cap \sigma Q| = |L_1 \cap P| + |M_1 \cap Q| = p_1 + q_1$$  \hspace{1cm} (5.31)

$$|(\sigma \overline{Y})_r \cap \sigma P| + |(\sigma \overline{Y})_r \cap \sigma Q| = |L_1 \cap P| + |M'_1 \cap Q| = p_1 + q_2$$  \hspace{1cm} (5.32)

$$|(\sigma \overline{Z})_r \cap \sigma P| + |(\sigma \overline{Z})_r \cap \sigma Q| = |L'_1 \cap P| + |M'_1 \cap Q| = p_2 + q_2.$$  \hspace{1cm} (5.33)

From (5.31), (5.32) and (5.33), we get that

$$\{ |(\sigma \overline{B})_r \cap \sigma P| + |(\sigma \overline{B})_r \cap \sigma Q| : \overline{B} \in \mathcal{R}_B \}$$  \hspace{1cm} (5.34)

has at least three values. But from (5.22), the sum has at most two values. This contradiction proves that our assumption that $\sigma$ sends parts of two different columns of $\mathcal{X}$ to the same column in $\sigma \mathcal{X}$ is wrong. Thus, in this case, the automorphisms of $\mathcal{D}$ send columns of $\mathcal{X}$ to columns of $\mathcal{X}$.

**Case 2**  \hspace{1cm} $\mathcal{D}_o$ is nontrivial (i.e., $0 < k_0 < v_1$) and $k_r \leq v_r - 2$. 

This case is exactly the same as Case 1 but with $\mathcal{D}_o$ in the first two columns of $\mathcal{R}_H$ where $B$ in this case is a block of $\mathcal{D}_r$ not containing the set $\{1, 2\}$. Proceeding in the same manner as in the previous case, we arrive at a similar contradiction. So in this case also, our assumption is wrong and the automorphisms of $\mathcal{D}$ must send columns of $\mathcal{X}$ to columns of $\mathcal{Y}$.

**Case 3** Both $\mathcal{D}_o$, $\mathcal{D}_i$ are nontrivial (ie, $0 < k_0 < v_1$, $0 < k_1 < v_1$).

Since by (5.9), $0 < k_r < v_r$, we have $v_r \geq 2$. Also $1 \leq k_r < v_r$, so we can find a block $B$ of $\mathcal{D}_r$ which contains $\{1\}$ but not $\{2\}$. With this $B$ as the underlying block, we proceed like in Case 1 with the blocks of $\mathcal{R}_B$ having their second column from $\mathcal{D}_o$ instead of $\mathcal{D}_i$. Making the same arguments as in Case 1 leads to a similar contradiction. So in this case also the automorphisms of $\mathcal{D}$ must send columns of $\mathcal{X}$ to columns of $\mathcal{Y}$.

**Case 4** $\mathcal{D}_i$ is nontrivial (ie, $0 < k_1 < v_1$), $k_r = 1$ and $k_0 = 0$.

Putting $k_r = 1$ and $k_0 = 0$ in the compatibility condition in (5.2), we get

$$\left(\begin{array}{c} k_1 \\ k_2 \end{array}\right)(v_r - 1)v_1 = 0.$$

Since $v_r \geq 2$, $k_1 > 0$ and $v_1 > 1$, we have $k_1 = 1$. That means the blocks of $\mathcal{D}$ are of size one and so $\mathcal{D}$ is a trivial design in this case. But, we want the composition $\mathcal{D}$ to be nontrivial. So this case does not occur.

Hence in all the cases when $\mathcal{D}$ is nontrivial, the automorphisms of $\mathcal{D}$ send columns of $\mathcal{X}$ to columns of $\mathcal{Y}$.

Lemma 5.1.9  The permutation of the columns of $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_r$ induced by an
automorphism of $\mathcal{D}$ is an automorphism of $\mathcal{D}_r$.

Proof: Let $\sigma$ be an automorphism of $\mathcal{D}$. Then by Lemma 5.1.8, $\sigma$ sends columns of $\mathcal{X}$ to columns of $\mathcal{X}$. So, for $j$ in $\mathcal{X}_r$

$$\sigma(\mathcal{X}_1 \times \{j\}) = \mathcal{X}_1 \times \{l\}$$

(5.35)

for some $l$ in $\mathcal{X}_r$. Let $\eta$ be the permutation of the columns of $\mathcal{X}$ induced by $\sigma$. Then $\eta$ is a permutation of $\mathcal{X}_r$ such that, for $j$ in $\mathcal{X}_r$, $\eta(j) = l$ where $j$ and $l$ are related by $\sigma$ as in (5.35). Then

$$\sigma(\mathcal{X}_1 \times \{j\}) = \mathcal{X}_1 \times \{\eta(j)\}.$$  \hspace{1cm} (5.36)

We want to show that $\eta$ is an automorphism of $\mathcal{D}_r$.

- For that, we need to show that $\eta$ preserves the blocks of $\mathcal{D}_r$. Let $B$ be a block of $\mathcal{D}_r$. We want $\eta(B)$ also in $\mathcal{D}_r$. Let $\overline{B} = \bigcup_{j=1}^{v_r}(B_j \times \{j\})$ be a block of $\mathcal{D}$ with $B$ as the underlying block from $\mathcal{D}_r$. $\sigma$ is in $\mathcal{A}$, so $\sigma(\overline{B}) = \bigcup_{j=1}^{v_r}(C_j \times \{j\})$ is also in $\mathcal{D}$. Therefore $C_j$ is from $\mathcal{D}_o$ or $\mathcal{D}_i$ for each $j$ in $\mathcal{X}_r$. Then from (5.35)

$$\sigma(B_j \times \{j\}) = C_{\eta(j)} \times \{\eta(j)\}$$

and

$$\sigma(\overline{B}) = \bigcup_{j=1}^{v_r} \sigma(B_j \times \{j\})$$

$$= \bigcup_{j=1}^{v_r} C_{\eta(j)} \times \{\eta(j)\}.$$  \hspace{1cm} (5.37)

Thus

$$|B_j| = |B_j \times \{j\}| = |\sigma(B_j \times \{j\})| = |C_{\eta(j)} \times \{\eta(j)\}| = |C_{\eta(j)}|.$$
Also \( k_0 < k_1 \), so \( |C_{\eta(j)}| = k_1 \) (or \( k_0 \)) iff \( |B_j| = k_1 \) (or \( k_0 \)). That is, \( C_{\eta(j)} \) is from \( D_i \) (or \( D_o \)) iff \( B_j \) is from \( D_i \) (or \( D_o \)). Thus \( \overline{B} = \bigcup_{j=1}^{m} (B_j \times \{j\}) \) has its \( j \)th column from \( D_i \) (or \( D_o \)) iff \( \eta(B) \) has its \( \eta(j) \)th column from \( D_i \) (or \( D_o \)). Therefore the underlying block of \( \eta(B) \) is

\[
\{ \eta(j) : B_j \in D_i \} = \{ \eta(j) : j \in B \} = \eta(B).
\]

(5.38)

Since \( \eta(B) \) is in \( D \), its underlying block \( \eta(B) \) is in \( D_r \). Thus \( \eta \) preserves the blocks of \( D_r \), and so it is an automorphism of \( D_r \).

Hence \( \eta \) is in \( A_r \). \( \square \)

**Lemma 5.1.10** \( \) The permutation induced by an automorphism of \( D \) within each column of \( X = X_1 \times X_r \) is an automorphism of both \( D_o \) and \( D_i \).

*Proof:* Let \( j \) be an element of \( X_r \). Then from (5.36), the image of the \( j \)th column \( X_1 \times \{j\} \) of \( X \) under \( \sigma \) is

\[
\sigma(X_1 \times \{j\}) = X_1 \times \eta(j)
\]

where \( \eta \) is the permutation of the columns induced by \( \sigma \). Let \( \nu_j \) be the permutation induced by the restriction of \( \sigma \) to \( X_1 \times \{j\} \) on \( X_1 \). Then, for \( x, y \) in \( X_1 \),

\[
\nu_j(x) = y \quad \text{if and only if} \quad \sigma(x \times j) = (y \times \eta(j)).
\]

(5.39)

So

\[
\sigma(x \times j) = (\nu_j(x) \times \eta(j))
\]

(5.40)
for all $x \times j$ in $\mathcal{V}$. Let $\overline{B} = \bigcup_{j=1}^{v_x} (B_j \times \{j\})$ be a block of $\mathcal{D}$ with $B$ as the underlying block from $\mathcal{D}_c$. Then $\sigma \overline{B}$ is in $\mathcal{D}$ with $\eta(B)$ as the underlying block from $\mathcal{D}_e$.

- We claim that

$$\sigma \overline{B} = \bigcup_{j=1}^{v_x} (\nu_j(B_j) \times \eta(j)).$$

From Lemma 5.1.9, we have

$$\sigma \overline{B} = \bigcup_{j=1}^{v_x} \sigma(B_j \times \{j\}) = \bigcup_{j=1}^{v_x} (C_{\eta(j)} \times \eta(j))$$

where $C_{\eta(j)}$ is from $\mathcal{D}_i$ (or $\mathcal{D}_o$) iff $B_j$ is from $\mathcal{D}_i$ (or $\mathcal{D}_o$). Then

$$C_{\eta(j)} = \{ y : y \times \eta(j) \in \sigma(B_j \times \{j\}) \}$$

$$= \{ y : y \times \eta(j) = \sigma(x \times j) \text{ for some } x \text{ in } B_j \}$$

$$= \{ y : y \times \eta(j) = \nu_j(x) \times \eta(j) \text{ for some } x \text{ in } B_j \}$$

$$= \{ \nu_j(x) : x \in B_j \} = \nu_j(B_j).$$

This proves our claim.

- Now we will show that $\nu_j$ is an automorphism of $\mathcal{D}_i$. For that, let $E^1$ be a block of $\mathcal{D}_i$ and $B$ be a block of $\mathcal{D}_c$ containing $j$. Then, by definition, $\mathcal{D}$ has a block $\overline{B} = \bigcup_{l=1}^{v_x} (B_l \times \{l\})$ with $B_j$ in $\mathcal{D}_i$ and $B_j = E^1$. Pick such a $\overline{B}$ and fix it. From (5.41),

$$\sigma \overline{B} = \bigcup_{l=1}^{v_x} (\nu_l(B_l) \times \eta(l)).$$

And $\sigma \overline{B}$ has $\eta(B)$ as the underlying block. So,

$$\nu_l(B_l) \in \mathcal{D}_i \text{ iff } B_l \in \mathcal{D}_i.$$
For $l = j$, $B_j = E^1$, and $E^1$ is in $D_1$. So $\nu_j(E^1) = \nu_j(B_j)$ in $D_1$. Thus $\nu_j$ preserves the blocks of $D_1$ and is therefore in $A_1$.

Now we will show that $\nu_j$ is an automorphism of $D_o$. Let $F^0$ be a block of $D_o$. Since $k_r < v_r$, we can find a block $B$ of $D_e$ such that $j$ is not in $B$. Then, all the blocks of $D$ with $B$ as the underlying block have their $j$th column from $D_o$. Let $\overline{B} = \bigcup_{l=1}^{v_r} B_l \times \{l\}$ be a block of $D$ with $B$ as the underlying block and $B_j = F^0$. Pick such a $\overline{B}$ and fix it. From (5.41),

$$\sigma \overline{B} = \bigcup_{l=1}^{v_r} \left( \nu_l(B_l) \times \eta(l) \right).$$

And $\sigma \overline{B}$ has $\eta(B)$ as the underlying block. So,

$$\nu_l(B_l) \in D_o \text{ iff } B_l \in D_o.$$

For $l = j$, $B_j = F^0$, and $F^0$ is in $D_o$. So $\nu_j(F^0) = \nu_j(B_j)$ in $D_o$. Thus $\nu_j$ preserves the blocks of $D_o$ and is therefore in $A_o$.

Hence $\nu_j$ is in $A_o \cap A_i$ for all $j$ in $X_e$. \(\square\)

**Theorem 5.1.11**  
Let $D_0$, $D_1$ and $D_e$ be designs satisfying (5.3), (5.4), (5.5) and the compatibility condition (5.2) so that the composition $D$ is a nontrivial balanced design. Then the automorphism group of $D$ is $A = (A_o \cap A_i) \cup A_e$. If any of these conditions is not satisfied, then $D$ is trivial and the automorphism group $A$ is the full symmetric group on $X$.

**Proof:** Suppose the composition $D$ is a nontrivial balanced design. Then from Lemma 5.1.5, $(A_o \cap A_i) \cup A_e \subset A$. To show $A \subset (A_o \cap A_i) \cup A_e$, let $\sigma$ be in $A$. Then from
where $\nu_j$ is the permutation induced by $\sigma$ within the $j$th column of $\mathcal{X}$ and $\eta$ is the permutation of the columns of $\mathcal{X}$ induced by $\sigma$. From Lemma 5.1.10, $\nu_j$ is in $\mathcal{A}_o \cap \mathcal{A}_i$ for all $j$ in $\mathcal{X}_r$, and from Lemma 5.1.9, $\eta$ is in $\mathcal{A}_r$. Let $\nu = \{\nu_j\}_{j=1}^{m_e}$. Then $\nu \subset (\mathcal{A}_o \cap \mathcal{A}_i)$. So by definition 5.6, $\nu \permutation \eta$ is in $(\mathcal{A}_o \cap \mathcal{A}_i) \permutation \mathcal{A}_r$. For $x \times j$ in $\mathcal{X}$, we now have

$$(\nu \permutation \eta)(x \times j) = \nu_j(x) \times \eta(j) = \sigma(x \times j).$$

So $\nu \permutation \eta = \sigma$. But $\nu \permutation \eta$ is in $(\mathcal{A}_o \cap \mathcal{A}_i) \permutation \mathcal{A}_r$, and thus $\sigma$ is also in $(\mathcal{A}_o \cap \mathcal{A}_i) \permutation \mathcal{A}_r$. Hence $\mathcal{A} \subset (\mathcal{A}_o \cap \mathcal{A}_i) \permutation \mathcal{A}_r$. Therefore $\mathcal{A} = (\mathcal{A}_o \cap \mathcal{A}_i) \permutation \mathcal{A}_r$. 

Next we study the point imprimitivity and the block transitivity properties of the automorphism group of the composition design.

**Definition 5.1.12** Let $\mathcal{A}$ be the automorphism group of a $t$-$(v, k, \lambda)$ design $\mathcal{D}$ over a set $\mathcal{X}$. Let $\mathcal{P} = \{P_1, P_2, \ldots, P_m\}$ be a partition of $\mathcal{X}$. Then $\mathcal{A}$ preserves $\mathcal{P}$ if for $\sigma \in \mathcal{A}$ and for each $i = 1, \ldots, m$, $\sigma(P_i) = P_j$ for some $j$ with $1 \leq j \leq m$. $\mathcal{A}$ is said to be point imprimitive on $\mathcal{X}$ if $\mathcal{A}$ preserves a nontrivial partition of $\mathcal{X}$. And, $\mathcal{A}$ is block transitive if it is transitive on the blocks of $\mathcal{D}$.

**Theorem 5.1.13** Let $\mathcal{D}_o$, $\mathcal{D}_i$, and $\mathcal{D}_r$ be designs satisfying (5.3), (5.4), (5.5) and the compatibility condition (5.2) so that the composition $\mathcal{D}$ is a nontrivial balanced design. Then the automorphism group $\mathcal{A} = (\mathcal{A}_o \cap \mathcal{A}_i) \permutation \mathcal{A}_r$ of $\mathcal{D}$ has the following properties:
(i) \( \mathcal{A} \) is point-imprimitive,

(ii) \( \mathcal{A} \) is never 2-transitive,

(iii) If \( \mathcal{A}_s \cap \mathcal{A}_i \) and \( \mathcal{A}_r \) are block transitive, then \( \mathcal{A} \) is also block transitive.

Proof: (i) Let

\[ \mathcal{P} = \{ \mathcal{Y}_1 \times \{ j \} : j \in \mathcal{Y}_r \} \]

be the set of columns of \( \mathcal{Y} = \mathcal{Y}_1 \times \mathcal{Y}_r \). Then, since \( n_r \geq 2 \) by (5.3), \( \mathcal{P} \) is a nontrivial partition of \( \mathcal{Y} \). From Lemma (5.1.8), the elements of \( \mathcal{A} \) preserve the columns of \( \mathcal{Y} \) and so they preserve the nontrivial partition \( \mathcal{P} \). Hence \( \mathcal{A} \) is point imprimitive.

(ii) From (5.3), we get \( n_r \geq 2 \). Using (5.4) and (5.5), and the fact that \( n_r \geq 2 \), we can pick two points \( (x, 1) \) and \( (y, 1) \) from the first column of \( \mathcal{Y} \) with \( x \neq y \) where \( x, y \) are in \( \mathcal{Y}_1 \). Similarly, we can pick two points \( (u, l) \) and \( (v, m) \) in \( \mathcal{Y} \) with \( l \neq m \). Then \( (u, l) \) and \( (v, m) \) are from two different columns of \( \mathcal{Y} \). If there is an automorphism \( \sigma \) of \( \mathcal{D} \) with

\[ \sigma(x, 1) = (u, l) \quad \text{and} \quad \sigma(y, 1) = (v, m), \]

then from Lemma (5.1.8), \( l = m \). This contradicts our assumption that \( l \neq m \) and therefore \( \mathcal{A} \) is not 2-transitive.

(iii) Let \( \overline{B} = \bigcup_{j=1}^{n_r} (B_j \times \{ j \}) \) and \( \overline{C} = \bigcup_{j=1}^{n_r} (C_j \times \{ j \}) \) be two blocks of \( \mathcal{D} \) with \( B, C \) as the underlying blocks from \( \mathcal{D}_e \). We will find an automorphism of \( \mathcal{D} \) that sends \( \overline{B} \) to \( \overline{C} \). Since the automorphism group \( \mathcal{A}_r \) of \( \mathcal{D}_r \) is block transitive, we can find \( \eta \) in \( \mathcal{A}_r \) with \( \eta(B) = C \). Pick such an \( \eta \in \mathcal{A}_r \) and fix it. Then for \( j \in \mathcal{Y}_r \), we have \( j \in B \) iff \( \eta(j) \in C \). From the definition of \( \overline{B}, \overline{C} \) and \( \eta \), we get

\[ B_j \in \mathcal{D}_i (\text{or } \mathcal{D}_o) \iff j \in B \text{ (or } j \notin B) \]
\[ \iff \eta(j) \in \eta(B) = C \text{ (or } \eta(j) \notin C) \]
\[ \iff C_{\eta(j)} \in \mathcal{D}, \text{ (or } \mathcal{D}_a). \]

Thus, for \( j \in \mathcal{X} \) we have both \( B_j \) and \( C_{\eta(j)} \) are in \( \mathcal{D} \) or \( \mathcal{D}_a \). And since \( \mathcal{A}_n \cap \mathcal{A}_n \) is block transitive by assumption, for each \( j \in \mathcal{X} \), we can find \( \nu_j \in (\mathcal{A}_n \cap \mathcal{A}_n) \) such that

\[ \nu_j(B_j) = C_{\eta(j)}. \]

Let \( \nu = \{\nu_j\}_{1}^{n} \) and \( \sigma = \nu \circ \eta \). Then, by the definition of \((\nu \circ \eta)\) in (5.1.2), for \((x \times j) \in \mathcal{X}\),

\[ \sigma(x \times j) = (\nu \circ \eta)(x \times j) = \nu_j(x) \times \eta(j). \]

From Lemma 5.1.5, we have \( \sigma \in \mathcal{A} \). And

\[ \sigma(\overline{B}) = \sigma\left(\bigcup_{j=1}^{n} (B_j \times \{j\})\right) = \bigcup_{j=1}^{n} \sigma(B_j \times \{j\}) \]
\[ = \bigcup_{j=1}^{n} \left(\nu_j(B_j) \times \{\eta(j)\}\right) = \bigcup_{j=1}^{n} \left(C_{\eta(j)} \times \{\eta(j)\}\right) = \overline{C}. \]

Therefore, we have found an automorphism of \( \mathcal{D} \) that sends \( \overline{B} \) to \( \overline{C} \). But \( \overline{B} \) and \( \overline{C} \) are arbitrary blocks of \( \mathcal{D} \), hence \( \mathcal{A} \) is block transitive. \( \square \)
CHAPTER VI

A Composition of Difference Families

6.1 Difference Families

Definition 6.1.1 Given an abelian group $G$ of size $v$, a $(v, k, \lambda)$ difference family $\mathcal{F}$ is a family of subsets

$\left( B_1, \ldots, B_s \right)$

of $G$ called base blocks each of size $k$ such that for each nonzero $d \in G$, there are $\lambda$ ordered triples $(j, g_1, g_2)$ with the properties that $j \in \{1, 2, \ldots, s\}$, $g_1, g_2 \in B_j$ and $g_1 - g_2 = d$. That is, there are exactly $\lambda$ ways of expressing each nonzero element $d$ in $G$ in the form $d = g_1 - g_2$ where $g_1, g_2 \in B_j$ for some $j$ with $1 \leq j \leq s$.

Here, the blocks of $\mathcal{F}$ need not be distinct. This definition of a group difference family is more general than the one by Beth [1], which assumes that the stabilizers of the blocks of $\mathcal{F}$ are trivial.

Let $\text{dev} \mathcal{F}$, called the development of $\mathcal{F}$, be the family of translates of the elements of $\mathcal{F}$ with any multiplicities counted. That is

$\text{dev} \mathcal{F} = \mathcal{F} + G$

$= \left( B + g : B \in \mathcal{F}, g \in G, \text{ multiple blocks counted as distinct blocks } \right)$. 

134
That is, if two translates of a block of $\mathcal{F}$ are equal, they are treated as distinct blocks and are counted twice.

**Definition 6.1.2** The action of a group $\mathcal{G}$ on a set $\mathcal{X}$ is said to be **regular** if for any two elements of $\mathcal{X}$, there is exactly one element of $\mathcal{G}$ sending one to the other.

**Lemma 6.1.3** If $\mathcal{F}$ is a $(v, k, \lambda)$ difference family, then $\text{dev}\mathcal{F}$ is a $2-(v, k, \lambda)$-design, not necessarily simple, with the action of $\mathcal{G}$ on itself being regular and $\text{dev}\mathcal{F}$ invariant under that action.

**Proof:** Let $a, b$ be two distinct points of $\mathcal{G}$. We claim that there are exactly $\lambda$ blocks of $\text{dev}\mathcal{F}$ containing both $a$ and $b$. Let $d = a - b$. Then $d \neq 0$ since $a \neq b$. For $l = 1, \ldots, s$, let $\lambda_l(d)$ be the number of pairs $\{g_l, g'_l\} \subseteq B_l$ with $d = g_l - g'_l$. Since $\mathcal{F}$ is a $(v, k, \lambda)$-difference family,

$$\lambda = \sum_{l=1}^{s} \lambda_l(d) \quad (6.2)$$

for all $d$ in $\mathcal{G}$. Let $B_l$ be a fixed block of $\mathcal{F}$. Then there are $\lambda_l(d)$ pairs $\{g_l, g'_l\}$ in $B_l$ with $d = g_l - g'_l$. So for $i = 1, \ldots, \lambda_l(d)$ there are pairs $\{g_i, g'_i\}$ in $B_l$ for which we have,

$$a - b = d = g_i - g'_i$$

$$\iff a - g_i = b - g'_i = u_i \quad \text{(say)}$$

$$\iff a = u_i + g_i, \ b = u_i + g'_i$$

iff $a$ and $b$ are in $u_i + B_l$. So the number of translates of $B_l$ in $\text{dev}\mathcal{F}$ containing both $a$ and $b$ is $\lambda_l(d) = \lambda_l(a - b)$. Thus, the number of blocks of $\text{dev}\mathcal{F}$ containing $a$ and $b$.
\[
\left| \left\{ g + B : a, b \in g + B, \ g \in \mathcal{G} \text{ and } B \in \mathcal{F}, \text{ multiplicities counted} \right\} \right| \\
= \sum_{i=1}^{s} \left| \left\{ g + B_i : a, b \in g + B_i, \ g \in \mathcal{G}, \text{ multiplicities counted} \right\} \right| \\
= \sum_{i=1}^{s} \lambda_i (a - b) = \lambda.
\]

So any two elements of \( \mathcal{G} \) is contained in exactly \( \lambda \) blocks of \( \text{dev}\mathcal{F} \). This shows \( \text{dev}\mathcal{F} \) is a 2-\((v, k, \lambda)\)-design. Each element of \( \mathcal{G} \) induces a permutation of \( \Lambda = \mathcal{G} \) by pointwise translation. This action of \( \mathcal{G} \) on \( \Lambda \) is regular, since for any two points of \( \Lambda \) there is exactly one element of \( \mathcal{G} \) sending one to the other. Also, since \( \mathcal{D} = \mathcal{F} + \mathcal{G} \), \( \mathcal{D} \) is obviously invariant under the action of \( \mathcal{G} \).

This Lemma shows that every \((v, k, \lambda)\) difference family \( \mathcal{F} \) over a group \( \mathcal{G} \) can be associated with the 2-\((v, k, \lambda)\)-design \((\mathcal{G}, \text{dev}\mathcal{F})\) with a regular group of automorphisms induced by the the action of \( \mathcal{G} \) on itself. Let \( b \) be the number of blocks in \( \text{dev}\mathcal{F} \). Then the parameters of \( \text{dev}\mathcal{F} \) satisfy the two following relations

\[
b = sv \\
\lambda = b \left( \begin{array}{c}
k \\
2 \end{array} \right) \\
\left( \begin{array}{c}
v \\
2 \end{array} \right).
\]

Conversely, a 2-\((v, k, \lambda)\)-design satisfying certain conditions is the development of a \((v, k, \lambda)\) difference family.

**Lemma 6.1.4** If \( \mathcal{D} \) is a 2-\((v, k, \lambda)\) design over \( \mathcal{G} \), not necessarily simple, such that \( \mathcal{D} \) is invariant under the action of \( \mathcal{G} \) and if there is a subset \( \mathcal{F} \) of \( \mathcal{D} \) with
\( \mathcal{D} = \mathcal{F} + \mathcal{G} \) counting all multiplicities, then \( \mathcal{F} \) is a \((v, k, \lambda)\)-difference family over the group \( \mathcal{G} \).

**Proof:** Let \( g \neq 0 \) be an element of \( \mathcal{G} \). Since \( \mathcal{D} \) is a \( 2-(v, k, \lambda) \)-design over \( \mathcal{G} \), \( \mathcal{D} \) has \( \lambda \) blocks \( x_i + B_i \) containing 0 and \( g \), with \( x_i \) in \( \mathcal{G} \), \( B_i \) in \( \mathcal{F} \) and \( 1 \leq i \leq \lambda \). Then

\[
g = x_i + \alpha_i \quad \text{and} \quad 0 = x_i + \beta_i
\]

for some \( \alpha_i, \beta_i \) in \( B_i \). So

\[
g - 0 = \alpha_i - \beta_i \quad \text{with} \quad 1 \leq i \leq \lambda \quad \text{and} \quad \{ \alpha_i, \beta_i \} \subseteq B_i
\]

where \( B_i \) is in \( \mathcal{F} \). Therefore, for each nonzero element \( g \) of \( \mathcal{G} \) there are at least \( \lambda \) pairs \( \{ \alpha_i, \beta_i \} \) from the blocks of \( \mathcal{F} \) with \( g = \alpha_i - \beta_i \). Let \( m \) be the average number of times \( g \) occurs as the difference of two distinct elements in the blocks of \( \mathcal{F} \) as \( g \) ranges over \( \mathcal{G} \). Then \( m \geq \lambda \). If a nonzero \( g_0 \) in \( \mathcal{G} \) is expressible as a difference for more than \( \lambda \) pairs in \( \mathcal{F} \), then the average \( m > \lambda \). But the average can be computed as follows:

\[
m = \frac{\left| \mathcal{F} \right|k(k-1)}{(v-1)} = \frac{(\left| \mathcal{F} \right|v)k(k-1)}{v(v-1)}
\]

\[
= \frac{\left| \mathcal{D} \right|k(k-1)}{v(v-1)} \quad \text{since} \quad \mathcal{D} = \mathcal{F} + \mathcal{G}
\]

\[
= \frac{k \binom{2}{2}}{v \binom{2}{2}} = \frac{k}{v} = \lambda.
\]

Hence each nonzero element of \( \mathcal{G} \) is expressible as a difference exactly \( \lambda \) times in \( \mathcal{F} \) and therefore \( \mathcal{F} \) is a \((v, k, \lambda)\)-difference family in \( \mathcal{G} \). \( \square \)
Lemmas (6.1.3) and (6.1.4) give an association between difference families and 2-designs. Using this association and the composition of designs given in Chapter 4, a composition of difference families can be defined.

Let $\mathcal{F}_i$, for $i=0,1$, and $\mathcal{F}_r$ be $(v_i, k_i, \lambda_i)$ and $(v_r, k_r, \lambda_r)$-difference families respectively, with $\mathcal{G}_o = \mathcal{G}_1$ and assume their parameters satisfy the compatibility condition in equation (4.20)

$$v_1(v_r - 1) \left[ k_r \left( \begin{array}{c} k_1 \\ 2 \end{array} \right) + k_r' \left( \begin{array}{c} k_0 \\ 2 \end{array} \right) \right] = (v_1 - 1) \left[ k_1^2 \left( \begin{array}{c} k_r' \\ 2 \end{array} \right) + k_1 k_0 k_r k_r' + k_0^2 \left( \begin{array}{c} k_r' \\ 2 \end{array} \right) \right]. \quad (6.5)$$

For $i = 0, 1$, let

$$\mathcal{D}_i = \text{dev} \mathcal{F}_i, \quad \mathcal{D}_r = \text{dev} \mathcal{F}_r$$

be the associated designs. Then $\mathcal{D}_o, \mathcal{D}_1$ and $\mathcal{D}_r$ are 2-designs and they satisfy the compatibility condition. It follows that the composition $\mathcal{D} = (\mathcal{D}_o, \mathcal{D}_1) \circ \mathcal{D}_r$ is a 2-$(v, k, \lambda)$-design with $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_r$ as the underlying point set and

$$v = v_1 v_r, \quad k = k_1 k_r + k_0(v_r - k_r),$$

$$b = b_i b_0^{(v_r - k_r)} b_1^{k_r}, \quad \lambda = b \left( \begin{array}{c} k \\ 2 \end{array} \right) \left( \begin{array}{c} v \\ 2 \end{array} \right). \quad (6.6)$$

Now we will show that the composition $\mathcal{D}$ is induced by a difference family. Let $\mathcal{G}_r = \{ e_1, e_2, \ldots, e_{v_r} \}$, with $e_1 = 0$ the zero element of $\mathcal{G}_r$. Take a block

$$\overline{C} = \bigcup_{j=1}^{v_r} (B_j \times \{ e_j \})$$

of $\mathcal{D}$ with $B$ as the underlying block from $\mathcal{D}_r$. We denote this as

$$\overline{C} = \left( \bigcup_{j=1}^{v_r} (B_j \times \{ e_j \}) \right)_H.$$
with $B_j$ from $\mathcal{D}_o$ or $\mathcal{D}_i$, and $B_j$ is from $\mathcal{D}_i$ if and only if $e_j$ is in $B$.

**Lemma 6.1.5**  \( D \) is invariant under the action of $G = G_i \times G_e$.

**Proof:** We have, $D = (F_0 + G_i, F_1 + G_i) \circ (F_r + G_e)$ and this action of $G$ is regular.

An arbitrary block of $D$ can be written as

$$C = \left( \bigcup_{j=1}^{n_e} (B_j + g_j) \times \{e_j\} \right)_{B+e_r}. \quad (6.7)$$

where $B$ is a base block in $F_r$, and $B_j$ in $F_0$ or $F_1$ with $B_j$ in $F_i$ iff $e_j$ is in $B + e_i$. Let an element $(g, c)$ of $G = G_i \times G_e$ act on it. That action sends $C$ to

$$C + (g, c) = \left( \bigcup_{j=1}^{n_e} (B_j + g_j + g) \times \{e_j + e\} \right)_{(B+e_r)+e}. \quad (6.8)$$

We want to show that $C + (g, c)$ is also in $D$. Since $B$ is in $F_1$, $e_i + e$ is in $G_e$ and $D_e = F_e + G_e$, so $(B + e_i) + e$ is in $D_e$. For the same reason, $B_j + g_j + g$ is in $D_o$ (or $D_i$) since $B_j + g_j$ is in $D_o$ (or $D_i$). $C$ is in $D$, so

$$B_j + g_j \in D_i \iff e_j \in B + e_i.$$

This means

$$B_j + g_j + g \in D_i \iff e_j \in B + e_i.$$ 

But

$$e_j \in B + e_i \iff e_j + e \in B + e_i + e.$$ 

So

$$B_j + g_j + g \in D_i \iff e_j + e \in B + e_i + e. \quad (6.9)$$
Thus, in $\overline{C} + (g, c)$, $B_j + g_j + g$ is in $D_o$ or $D_i$ with $B_j + g_j + g$ in $D_i$ iff $c_j + c$ is in $B + c + c$. So $\overline{C} + (g, c)$ is back in $D$ with $(B + c + c)$ as the underlying block from $D_c$. Hence $D$ is invariant under the action of $G$. □

Define the following subset of blocks from $D$

$$F = \left( \left( \bigcup_{j=1}^{v_e} (B_j + g_j) \times \{e_j\} \right) \right)_{B \in F_o, g_j \in G_i,}
B_j \in F_o \text{ if } e_j \notin B \text{ and } B_j \in F_i \text{ if } e_j \in B \right) \quad (6.10)$$

with appropriate multiplicities. $F$ is called the composition of the difference families $F_o$, $F_i$, and $F_r$ and is written as

$$F = (F_o, F_i) \circ F_r. \quad (6.11)$$

The next theorem shows that $F$ is a difference family.

**Theorem 6.1.6** Let $F_i$, for $i=0,1$, be $(v_i, k_i, \lambda_i)$ difference families over the groups $G_o \simeq G_i$, and $F_r$ a $(v_r, k_r, \lambda_r)$ difference family over $G_r$. If the compatibility condition (6.5) is satisfied, then their composition $F = (F_o, F_i) \circ F_r$ in (6.10) is a $(v, k, \lambda)$ difference family over the group $G = G_i \times G_r$ with $v = v_i v_r$, $k = k_1 k_r + k_0 (v_r - k_r)$, and $\lambda$ and $b$ given by (6.6) above.

**Proof:** From Lemma (6.1.5), $D$ is invariant under the action of $G$. So, if we show that $D = F + G$, then from Lemma (6.1.4), $F$ will be a $(v, k, \lambda)$ difference family. To show $D = F + G$, let

$$\overline{C} = \left( \bigcup_{j=1}^{v_e} (B_i + g_i) \times \{e_j\} \right)_{B+r}$$
be a block of $\mathcal{D}$. Then

$$
\overline{C} = \left( \bigcup_{j=1}^{v_r} (B_j + g_j - g_1) \times \{ e_j - e \} \right)_{B} + (g_1, e) \quad (6.12)
$$

$$
= \overline{B} + (g_1, e)
$$

where

$$
\overline{B} = \left( \bigcup_{j=1}^{v_r} (B_i + g_i - g_1) \times \{ e_j - e \} \right)_{B}.
$$

(6.13)

$\overline{B}$ is in $\mathcal{F}$ since its first column is $(B_1 + g_1 - g_1) = B_1$ and the other columns are from $\mathcal{D}_o$ or $\mathcal{D}_i$ and $B \in \mathcal{F}_o$ is its underlying block. So for each $\overline{C}$ in $\mathcal{D}$, $\overline{C} = \overline{B} + g$ where $\overline{B}$ is some block in $\mathcal{F}$ and $g$ is an element of $\mathcal{G}$. Hence $\mathcal{D} = \mathcal{F} + \mathcal{G}$ and so from Lemma (6.1.4), $\mathcal{F}$ is a $(v, k, \lambda)$ difference family. □

6.2 Multiplier Group of the Composition Difference family

Let $\mathcal{G}$ be a group and $\mathcal{F}$ be a $(v, k, \lambda)$ difference family over $\mathcal{G}$ and $\mathcal{D} = \mathcal{F} + \mathcal{G}$ be the associated design.

**Definition 6.2.1** A group automorphism of $\mathcal{G}$ is called a multiplier of the difference family $\mathcal{F}$ if it preserves the blocks of $\text{dev}\mathcal{F}$.

So multipliers are design automorphisms that are also group automorphisms. This definition is as in Beth [1]. The multipliers of $\mathcal{F}$ form a group under the composition of maps. We will denote the set of multipliers of $\mathcal{D}$ by $\mathcal{M}$.

Having defined the composition of difference families, we will show that the multiplier group of the composition can be expressed in terms of the multiplier groups of the component families.
Let $\mathcal{M}_0$, $\mathcal{M}_1$ and $\mathcal{M}_e$ be the multiplier groups of $\mathcal{F}_0$, $\mathcal{F}_1$ and $\mathcal{F}_e$ over the groups $\mathcal{G}_0$, $\mathcal{G}_1$ and $\mathcal{G}_e$ with $\mathcal{G}_0 \cong \mathcal{G}_1$. Let $\mathcal{M}$ be the multiplier group of the composition difference family $\mathcal{F} = (\mathcal{F}_0, \mathcal{F}_1) \circ \mathcal{F}_e$ over the group $\mathcal{G} = \mathcal{G}_1 \times \mathcal{G}_e$.

Let $\mathcal{K} = \text{Hom}(\mathcal{G}_e, \mathcal{G}_1)$ be the group of homomorphisms from $\mathcal{G}_e$ to $\mathcal{G}_1$ where the group operation is the pointwise addition defined as follows:

For $f$, $g$ in $\mathcal{K}$ and $\alpha$ in $\mathcal{G}_e$, we have

$$(f + g)(\alpha) = f(\alpha) + g(\alpha).$$

Let $\mathcal{Q} = (\mathcal{M}_0 \cap \mathcal{M}_1) \times \mathcal{M}_e$ be the group under coordinatewise multiplication.

In this section, we show that $\mathcal{M}$ is a certain semidirect product of $\mathcal{K}$ and $\mathcal{Q}$.

Let $\mathcal{A}_0$, $\mathcal{A}_1$, $\mathcal{A}_e$ and $\mathcal{A}$ be the design automorphism groups of $\mathcal{D}_0$, $\mathcal{D}_1$, $\mathcal{D}_e$ and $\mathcal{D}$ as in Chapter 5. From Theorem (5.1.11)\n
$\mathcal{A} = (\mathcal{A}_0 \cap \mathcal{A}_1) \mathcal{A}_e.$ \hspace{1cm} (6.14)

Since a multiplier of a difference family $\mathcal{F}$ over $\mathcal{G}$ is a design automorphism of $\text{dev} \mathcal{F}$, the group of multipliers of $\mathcal{F}$ is a subgroup of the group of automorphisms of $\text{dev} \mathcal{F}$. So $\mathcal{M}_i \subseteq \mathcal{A}_i$ for $i = 0, 1$, $\mathcal{M}_e \subseteq \mathcal{A}_e$ and $\mathcal{M} \subseteq \mathcal{A}$.

Let

$\mathcal{G}_e = \{e_1, e_2, \ldots, e_{v_e}\}$

with $e_1$ the identity and

$\mathcal{G}_i = \{g_1, g_2, \ldots, g_{v_i}\}$
Let $\sigma$ be a multiplier of $\mathcal{F} = (\mathcal{F}_o, \mathcal{F}_i) \circ \mathcal{F}_r$. Then $\sigma$ is an automorphism of $\mathcal{D} = \text{dev}\mathcal{F}$ and so is in $\mathcal{A}$. Since $\mathcal{A}$ is a wreath product as in (6.14),

$$\sigma = \{\nu_j\}_{j=1}^{v_r} \uparrow \eta$$

(6.15)

where $\nu_j$ for $j = 1, \ldots, v_r$ are in $\mathcal{A}_o \cap \mathcal{A}_i$ and $\eta$ is in $\mathcal{A}_r$ such that for $(g, e_j)$ in $\mathcal{G}$

$$\sigma(g, e_j) = \nu_j(g) \times \{\eta(e_j)\}.$$  

(6.16)

When $\sigma$ is in the multiplier group $\mathcal{M}$ of $\mathcal{F}$, then the $\nu_j$'s and $\eta$ have the properties described in the following Lemma.

**Lemma 6.2.2**  
If $\sigma = \{\nu_j\}_{j=1}^{v_r} \uparrow \eta$ is a multiplier of $\mathcal{F}$ then

(i) $\eta$ is a multiplier of $\mathcal{F}_r$,

(ii) $\sigma$ fixes the first column of $\mathcal{G} = \mathcal{G}_o \times \mathcal{G}_r$,

(iii) $\nu_1$ is a multiplier of both $\mathcal{F}_o$ and $\mathcal{F}_i$, and

(iv) For $j = 1, \ldots, v_r$, $\nu_j = \nu_1 + f(e_j)$ for some $f$ in $\mathcal{K} = \text{Hom}(\mathcal{G}_r, \mathcal{G}_i)$.

**Proof:** From (6.15), $\eta$ is an automorphism of $\text{dev}\mathcal{F}_r$. So to show that $\eta$ is in $\mathcal{M}_r$, we need to just prove that $\eta$ is an automorphism of $\mathcal{G}_r$. To that end, let $e_l, e_m$ be two elements of $\mathcal{G}_r$ and $e_l + e_m = e_n$. Then, $(0, e_l), (0, e_m)$ are elements of $\mathcal{G} = \mathcal{G}_i \times \mathcal{G}_r$ and

$$(0, e_n) = (0, e_l) + (0, e_m).$$

(6.17)

Since $\sigma$ is a multiplier of $\mathcal{F}$,

$$\sigma(0, e_n) = \sigma(0, e_l) + \sigma(0, e_m).$$

(6.18)
Using (6.15), this gives
\[
\left( \nu_n(0), \eta(e_n) \right) = \left( \nu_l(0), \eta(e_l) \right) + \left( \nu_m(0), \eta(e_m) \right).
\]
Simplifying the right side of the above equation gives
\[
\left( \nu_n(0), \eta(e_l + e_m) \right) = \left( \nu_l(0) + \nu_m(0), \eta(e_l) + \eta(e_m) \right). \tag{6.19}
\]
Equating the second coordinates from both sides, we get
\[
\eta(e_l + e_m) = \eta(e_l) + \eta(e_m)
\]
which shows that \( \eta \) is a homomorphism of \( \mathcal{G}_r \), and hence is a multiplier of \( \mathcal{F}_r \) and so is in \( \mathcal{M}_r \).

- We want to show that \( \sigma \) fixes the first column \( \mathcal{G}_i \times \{0\} \) of \( \mathcal{G} = \mathcal{G}_i \times \mathcal{G}_r \). For that purpose, let \( (g_j, 0) \) be an element of the first column of \( \mathcal{G} \). Then
\[
\sigma(g_j, 0) = \left( \nu_1(g_j), \eta(0) \right) = \left( \nu_1(g_j), 0 \right)
\]
since \( \eta \) is in \( \mathcal{M}_r \), \( \eta(0) = 0 \). So the image under \( \sigma \) of the first column of \( \mathcal{G} \) is back in its first column of \( \mathcal{G} \). So \( \sigma \) fixes the first column of \( \mathcal{G} \).

- From (6.15), \( \nu_1 \) is in \( \mathcal{A}_o \cap \mathcal{A}_i \). So to show that \( \nu_1 \) is a multiplier of both \( \mathcal{F}_o \) and \( \mathcal{F}_i \), we just need to show that \( \nu_1 \) is a homomorphism of \( \mathcal{G}_i \). To that end, let \( g_j, g_{j'} \) be two elements of \( \mathcal{G}_i \). Then \( (g_j, 0), (g_{j'}, 0) \) are in \( \mathcal{G} \). Since \( (g_j, 0) + (g_{j'}, 0) = (g_j + g_{j'}, 0) \) and \( \sigma \) is in \( \mathcal{M} \),
\[
\sigma(g_j + g_{j'}, 0) = \sigma(g_j, 0) + \sigma(g_{j'}, 0)
\]
\[
\implies \left( \nu_1(g_j + g_{j'}, 0), \eta(0) \right) = \left( \nu_1(g_j), \eta(0) \right) + \left( \nu_1(g_{j'}), \eta(0) \right)
\]
\[
\implies \left( \nu_1(g_j + g_{j'}), 0 \right) = \left( \nu_1(g_j) + \nu_1(g_{j'}), 0 \right) \tag{6.22}
\]
which is obtained by using the fact that $\eta(0) = 0$ and simplifying the right side. Equating the first coordinates from both sides of the last equation, we get

$$\nu_1(g_j + g_j') = \nu_1(g_j) + \nu_1(g_j')$$  \hspace{1cm} (6.23)

which shows that $\nu_1$ is a homomorphism of $G$ and so is in $M \cap M_1$.

- We want to show that for $j = 1, \ldots, n$, $\nu_j = \nu_1 + f(e_j)$ for some $f$ in $K = \text{Hom}(G, G)$. To do that, let $(g, e_i)$ be a point of $G = G \times G$. Then

$$(g, e_i) = (g, 0) + (0, e_i),$$

where 0 in the first coordinate is the zero element of $G$, and the 0 in the second coordinate is the zero element of $G$. Since $\sigma$ is in $M$,

$$\sigma(g, c_i) = \sigma(g, 0) + \sigma(0, c_i). \hspace{1cm} (6.24)$$

$$\Rightarrow (\nu_1(g), \eta(e_i)) = (\nu_1(g), \eta(0)) + (\nu_1(0), \eta(e_i)) \hspace{1cm} (6.25)$$

$$= (\nu_1(g) + \nu_1(0), \eta(0) + \eta(e_i)). \hspace{1cm} (6.26)$$

Equating the first coordinates from both sides gives

$$\nu_1(g) = \nu_1(g) + \nu_1(0). \hspace{1cm} (6.27)$$

For a given $\sigma$ in $M$, define a map $f$ from $G$ to $G_1$ such that for $e_i$ in $G$, $f(e_i) = \nu_i(0)$. Since equating the first coordinates from both sides of (6.19) gives

$$\nu_n(0) = \nu_1(0) + \nu_1(0) \hspace{1cm} (6.28)$$

where $n$ is such that $e_n = e_l + e_m$, we get

$$f(e_l + e_m) = f(e_l) + f(e_m) \hspace{1cm} (6.29)$$
for any two $c_i, c_m$ in $\mathcal{G}_c$. Thus $f$ is a homomorphism and so is in $\mathcal{K}$. Using this $f$ in (6.27) gives

$$\nu_i(g) = \nu_i(g) + f(v_i)$$

which proves our claim. □

Lemma (6.2.2) shows that $\sigma$ is completely determined by $\nu_1, \eta, f$ for some $\nu_1$ in $\mathcal{M}_o \cap \mathcal{M}_1$, $\eta$ in $\mathcal{M}_c$ and $f$ in $\mathcal{K} = \text{Hom}(\mathcal{G}_c, \mathcal{G}_c)$. The converse that each such triple $\nu_1, \eta, f$ produces a multiplier of $\mathcal{F}$ is also true as shown below. Let

$$\mathcal{T} = \mathcal{K} \times (\mathcal{M}_o \cap \mathcal{M}_1) \times \mathcal{M}_c.$$  \hfill (6.30)

Then

$$\mathcal{T} = \{(f, \nu, \eta) : \text{ where } f \in \mathcal{K}, \nu \in \mathcal{M}_o \cap \mathcal{M}_1 \text{ and } \eta \in \mathcal{M}_c\}. \hfill (6.31)$$

**Lemma 6.2.3**  \hfill There is a one to one correspondence between the elements of $\mathcal{M}$ and the set of triples in $\mathcal{T}$.

**Proof:** we define a map $\Phi$ from the set of triples $\mathcal{T}$ to $\mathcal{M}$ as follows:

For $(f, \nu, \eta)$ in $\mathcal{T}$, let

$$\Phi(f, \nu, \eta) = \sigma \hfill (6.32)$$

where

$$\sigma(g, e) = (\nu(g) + f(e), \eta(e)) \hfill (6.33)$$

for $(g, e)$ in $\mathcal{G}$. 

We show that $\Phi$ is a bijection between $\mathcal{T}$ and $\mathcal{M}$. For that, first we show that

$$\Phi(f, \nu, \eta) = \sigma$$

is in $\mathcal{M}$.

- Clearly $\sigma$ is a map from $\mathcal{G}$ to $\mathcal{G}$. We here show that it is injective. Suppose for $(g, c), (g', c')$ in $\mathcal{G}$,

$$\sigma(g, c) = \sigma(g', c').$$

Then

$$(\nu(g) + f(c), \eta(c)) = (\nu(g') + f(c'), \eta(c')).$$

This is true only if

$$\nu(g) + f(c) = \nu(g') + f(c') \text{ and } \eta(c) = \eta(c').$$

But $\eta$ is in $\mathcal{M}_e$ and so $\eta(c) = \eta(c')$ means $c = c'$. So $f(c) = f(c')$. Using this fact in (6.36), we get $\nu(g) = \nu(g')$ which gives $g = g'$ since $\nu$ is in $\mathcal{M}_o \cap \mathcal{M}_e$. Thus $\sigma(g, c) = \sigma(g', c')$ iff $(g, c) = (g', c')$ and so $\Phi(f, \nu, \eta) = \sigma$ is injective.

For $(g, c)$ in $\mathcal{G}$, we can find $g'$ in $\mathcal{G}_i$ and $e'$ in $\mathcal{G}_e$ such that $\nu(g') = g - f(c)$ and $\eta(c') = e$ since $\nu$ and $\eta$ are surjective. Then $(g', c')$ is in $\mathcal{G}$ and

$$\sigma(g', c') = (\nu(g') + f(c), \eta(c')) = (g, c).$$

So $\Phi(f, \nu, \eta) = \sigma$ is surjective.

To show $\sigma$ is an automorphism of $\mathcal{G}$, let $(g, c), (g', c')$ be two elements of $\mathcal{G}$. Then

$$(g, c) + (g', c') = (g + g', c + c')$$

and

$$\sigma((g, c) + (g', c')) = \sigma(g + g', c + c') = (\nu(g + g') + f(c + c'), \eta(c + c'))$$

would show that $\sigma$ is an automorphism.
and so $\sigma$ is an automorphism of $\mathcal{G}_r$.

Let $\nu_i = \nu + f(c_i)$. Then since $\nu$ is in $\mathcal{M}_o \cap \mathcal{M}_i$ and $\text{dev} \mathcal{F}_o = \mathcal{F}_o + \mathcal{G}_1$, $\text{dev} \mathcal{F}_i = \mathcal{F}_i + \mathcal{G}_1$, $\nu_i + f(c_i)$ preserves the blocks of both $\text{dev} \mathcal{F}_o$ and $\text{dev} \mathcal{F}_i$ for $i = 1, \ldots, v_r$. And we note that $\sigma = \{\nu_i\}_{i=1}^{v_r} \eta$ with $\nu_i$ in $\mathcal{M}_o \cap \mathcal{M}_i$ and $\eta$ in $\mathcal{M}_r$.

Then by Theorem (5.1.11), $\sigma$ is an automorphism of $\text{dev} \mathcal{F}$ and hence $\Phi(f, \nu, \eta) = \sigma$ is a multiplier of $\mathcal{F}$ and so is in $\mathcal{M}$. So $\Phi$ is a map from $\mathcal{T}$ to $\mathcal{M}$. Next we show that it is actually bijective.

- To show $\Phi$ is injective, suppose for $(f, \nu, \eta)$ and $(f', \nu', \eta')$ in $\mathcal{T}$, we have

$$\Phi(f, \nu, \eta) = \Phi(f', \nu', \eta').$$

(6.39)

Let $\sigma = \Phi(f, \nu, \eta)$ and $\sigma' = \Phi(f', \nu', \eta')$. Then from (6.39), for all $(g, \epsilon)$ in $\mathcal{G}$,

$$\sigma(g, \epsilon) = \sigma'(g, \epsilon).$$

(6.40)

From the definition of $\Phi$, this gives

$$\left(\nu(g) + f(\epsilon), \eta(\epsilon)\right) = \left(\nu'(g) + f'(\epsilon), \eta'(\epsilon)\right).$$

(6.41)

Equating the corresponding coordinates, we get

$$\nu(g) + f(\epsilon) = \nu'(g) + f'(\epsilon) \quad \text{and} \quad \eta(\epsilon) = \eta'(\epsilon).$$

(6.42)
From (6.42), we get \( \eta = \eta' \). Since \( f(0) = f'(0) = 0 \), putting \( \epsilon = 0 \) in (6.42) gives \( \nu(g) = \nu'(g) \) for all \( g \) in \( \mathcal{G}_1 \). So \( \nu = \nu' \). Using this in (6.42) gives \( f = f' \). Thus

\[
\Phi(f, \nu, \eta) = \Phi(f', \nu', \eta') \iff (f, \nu, \eta) = (f', \nu', \eta').
\]

So \( \Phi \) is injective.

- From Lemma (6.2.2), \( \Phi \) is surjective.

Therefore \( \Phi \) is a bijection between \( \mathcal{T} \) and \( \mathcal{M} \).

We can easily check that for \((f, \nu, \eta)\) and \((f', \nu', \eta')\) in \( \mathcal{T} \),

\[
\Phi \left( (f, \nu, \eta) \circ (f', \nu', \eta') \right) = \Phi \left( (f'f + f\eta'), \nu\nu', \eta\eta' \right).
\]

(6.43)

Let \( \mathcal{Q} = (\mathcal{M}_\alpha \cap \mathcal{M}_\beta) \times \mathcal{M}_\gamma \). Our aim is to show that \( \mathcal{M} \) is actually the semidirect product of \( \mathcal{K} = \text{Hom} (\mathcal{G}_\lambda, \mathcal{G}_\omega) \) and \( \mathcal{Q} \). We recall the definition of semidirect product from [15].

**Definition 6.2.4** A group \( \mathcal{G} \) is a semidirect product of \( \mathcal{K} \) by \( \mathcal{Q} \), denoted by \( \mathcal{G} = \mathcal{K} \ltimes \mathcal{Q} \), if \( \mathcal{G} \) contains subgroups \( \mathcal{K} \) and \( \mathcal{Q} \) such that

\[
\mathcal{K} \triangleleft \mathcal{G}, \quad \mathcal{K}\mathcal{Q} = \mathcal{G} \text{ and } \mathcal{K} \cap \mathcal{Q} = \{1\}.
\]

The following Lemma from [15] gives a criterion for the crossproduct of two groups to be a semidirect product. Let \( \mathcal{K}, \mathcal{Q} \) be two groups and let \( \text{Aut}\mathcal{K} \) be the group of automorphisms of \( \mathcal{K} \), and \( \Theta \) a map from \( \mathcal{Q} \) to the \( \text{Aut}\mathcal{K} \). Let \( \mathcal{K} \ltimes_\Theta \mathcal{Q} \) be the set of all ordered pairs \((k, x)\) in \( \mathcal{K} \times \mathcal{Q} \) under the binary operation

\[
(k, x) \ltimes_\Theta (k_1, y) = (k\Theta_x(k_1), xy)
\]

(6.44)

where \( \Theta_x \) is the image of \( x \) under the mapping \( \Theta \). This gives the following Lemma.
Lemma 6.2.5 \( \mathcal{K} \times_{\Theta} \mathcal{Q} \) is a semidirect product of \( \mathcal{K} \) by \( \mathcal{Q} \), if \( \Theta \) is a homomorphism.

Let \( \mathcal{K} = \text{Hom}(\mathcal{G}_r, \mathcal{G}_i), \mathcal{Q} = (\mathcal{M}_n \cap \mathcal{M}_i) \times \mathcal{M}_r \). We define \( \Theta : \mathcal{Q} \to \text{Aut} \mathcal{K} \) such that for \((\nu, \eta)\) in \( \mathcal{Q} \),

\[
\Theta_{(\nu,\eta)}(f) = \nu f \eta^{-1}
\]
for \( f \) in \( \mathcal{K} \). Here \( \Theta_{(\nu,\eta)} \) denotes the image of \((\nu, \eta)\) under \( \Theta \).

Lemma 6.2.6 \( \Theta \) is a homomorphism.

Proof: First we show that \( \Theta_{(\nu,\eta)} \) is in \( \text{Aut} \mathcal{K} \) for each \((\nu, \eta)\) in \( \mathcal{Q} \). Since \( \nu, f \) and \( \eta \) are homomorphisms, their composition \( \nu f \eta^{-1} \) is a homomorphism from \( \mathcal{G}_r \) to \( \mathcal{G}_i \) for all \( f \) in \( \mathcal{K} \). So \( \Theta_{(\nu,\eta)} \) induces a map from \( \mathcal{K} \) into \( \mathcal{K} \). To show \( \Theta_{(\nu,\eta)} \) is a homomorphism, let \( f, f' \) be two elements of \( \mathcal{K} \). Then for \( c \) in \( \mathcal{G}_r \),

\[
\left( \Theta_{(\nu,\eta)} \right)(f + f')(c) = \nu (f + f')(\eta^{-1})(c) \\
= \nu \left( f \eta^{-1}(c) + f' \eta^{-1}(c) \right) = \nu f \eta^{-1}(c) + \nu f' \eta^{-1}(c) \\
= \left( \nu f \eta^{-1} + \nu f' \eta^{-1} \right)(c) \\
= \left( \Theta_{(\nu,\eta)}(f) + \Theta_{(\nu,\eta)}(f') \right)(c). \tag{6.46}
\]

So

\[
\Theta_{(\nu,\eta)}(f + f') = \Theta_{(\nu,\eta)}(f) + \Theta_{(\nu,\eta)}(f')
\]

which proves that \( \Theta_{(\nu,\eta)} \) is a homomorphism. To show \( \Theta_{(\nu,\eta)} \) is injective, suppose for \( f, f' \) in \( \mathcal{K} \),

\[
\Theta_{(\nu,\eta)}(f) = \Theta_{(\nu,\eta)}(f').
\]
Then for all $c$ in $\mathcal{G}_c$,
\[ \nu \eta^{-1}(c) = \nu f \eta^{-1}(c). \tag{6.47} \]
Since $\nu$ is injective, we get
\[ f \eta^{-1}(c) = f' \eta^{-1}(c). \tag{6.48} \]
Then, since as $c$ varies through $\mathcal{G}_c$, $\eta^{-1}(c)$ gives all of $\mathcal{G}_c$, we get $f = f'$. Hence $\Theta_{(\nu, \eta)}$ is injective. For $f$ in $\mathcal{K}$, $\nu^{-1} f \eta$ is also in $\mathcal{K}$, and
\[ \Theta_{(\nu, \eta)}(\nu^{-1} f \eta) = \nu \nu^{-1} f \eta \eta^{-1} = f \]
which shows that $\Theta_{(\nu, \eta)}$ is surjective. Hence $\Theta_{(\nu, \eta)}$ is in Aut$\mathcal{K}$.

To show $\Theta$ is a homomorphism, let $(\nu, \eta), (\nu', \eta')$ be two elements of
\[ Q = (\mathcal{M}_0 \cap \mathcal{M}_1) \times \mathcal{M}_c. \]
Then $(\nu, \eta)(\nu', \eta') = (\nu \nu', \eta \eta')$ and for $f$ in $\mathcal{K}$,
\[ \Theta(\nu \nu', \eta \eta')(f) = \nu \nu' f(\eta')^{-1} \eta^{-1} = \nu \left( \Theta_{(\nu', \eta')}(f) \right) \eta \]
\[ = \left( \Theta_{(\nu, \eta)} \Theta_{(\nu', \eta')} \right)(f). \tag{6.49} \]
So,
\[ \Theta(\nu \nu', \eta \eta') = \Theta_{(\nu, \eta)} \Theta_{(\nu', \eta')} \tag{6.50} \]
Therefore $\Theta$ is a homomorphism from $Q$ to Aut$\mathcal{K}$.

**Lemma 6.2.7** For $\mathcal{K} = \text{Hom}(\mathcal{G}_c, \mathcal{G}_c)$, $Q = (\mathcal{M}_0 \cap \mathcal{M}_1) \times \mathcal{M}_c$, $\mathcal{K} \rtimes Q$ is a semidirect product of $\mathcal{K}$ by $Q$ where $\Theta$ is defined in (6.45).

**Proof:** $\Theta$ defined in (6.45) is a homomorphism from Lemma (6.2.6). So by Lemma (6.2.5), $\mathcal{K} \rtimes Q$ with the binary operation in (6.44) is a semidirect product of $\mathcal{K}$ and $Q$. □
Theorem 6.2.8  The multiplier group $\mathcal{M}$ of the composition difference family $\mathcal{F}$ is equal to the semidirect product $\mathcal{K} \rtimes \Theta \mathcal{Q}$.

Proof: We define a map $\Psi : \mathcal{K} \rtimes \Theta \mathcal{Q} \to \mathcal{M}$ such that for $(f, (\nu, \eta))$ in $\mathcal{K} \rtimes \Theta \mathcal{Q}$

$$
\Psi(f, (\nu, \eta))(g, e) = (\nu(g) + f\eta(e), \eta(e))
$$

for $(g, e)$ in $\mathcal{G} = \mathcal{G}_i \times \mathcal{G}_r$. We show that $\Psi$ is an isomorphism. By Lemma (6.2.3), $\Psi(f, (\nu, \eta))$ is a bijection between $\mathcal{K} \rtimes \Theta \mathcal{Q}$ and $\mathcal{M}$. To show that $\Psi$ is a homomorphism, let $(f, (\nu, \eta)), (f', (\nu', \eta'))$ be two elements of $\mathcal{K} \rtimes \Theta \mathcal{Q}$. Then for $(g, e)$ in $\mathcal{G}$,

$$
\Psi(f, (\nu, \eta))\Psi(f', (\nu', \eta'))(g, e) = \Psi(f, (\nu, \eta))(\nu'(g) + f'\eta'(e), \eta'(e))
$$

$$
= (\nu(\nu'(g) + f'\eta'(e)) + f\eta\eta'(e), \eta\eta'(e))
$$

$$
= (\nu\nu'(g) + \nu f'\eta'(e) + f\eta\eta'(e), \eta\eta'(e))
$$

$$
= (\nu\nu'(g) + (\nu f'\eta^{-1} + f)(\eta\eta'(e)), \eta\eta'(e))
$$

$$
= \Psi((\nu f'\eta^{-1} + f), (\nu\nu', \eta\eta'))(g, e) \quad (6.52)
$$

$$
= \Psi((f, (\nu, \eta))\rtimes \Theta (f', (\nu', \eta')))(g, e) \quad (6.53)
$$

So $\Psi$ is an isomorphism and $\mathcal{M} = \mathcal{K} \rtimes \Theta \mathcal{Q}$. $\square$

6.3  Examples

(6.3.1) Let $\mathcal{G}_e = \mathbb{Z}_3$ and $\mathcal{G}_i = \mathbb{Z}_7$. Let $\mathcal{F}_e = \{\{1\}\}$. Then $\mathcal{F}_e$ is a $(3,1,0)$ difference family over $\mathcal{G}_e$ and $\mathcal{D}_e = \text{dev}\mathcal{F}_e$ is a $2$-$(3,1,0)$ design. Let $\mathcal{F}_o = \{\{1\}\}$, then $\mathcal{F}_o$ is a $(7,1,0)$ difference family over $\mathcal{G}_i$ and $\mathcal{D}_o = \text{dev}\mathcal{F}_o$ is a $2$-$(7,1,0)$ design. Let

$$
\mathcal{F}_1^1 = \{\{0,1,3\}\}, \quad \mathcal{F}_1^2 = \{\{0,1,3\}, \{0,1,5\}\},
$$
\[ F_1^3 = \{\{0, 1, 2\}, \{0, 1, 4\}, \{0, 2, 4\}\}, \]
\[ F_1^4 = \{\{0, 1, 2\}, \{0, 1, 4\}, \{0, 2, 4\}, \{0, 1, 5\}\} \]
\[ F_1^5 = \{\{0, 1, 3\}, \{0, 1, 2\}, \{0, 1, 4\}, \{0, 1, 5\}, \{0, 2, 4\}\}. \]

Then, for \( s = 1, \ldots, 5 \), \( F_1^s \) is a \((7, 3, s)\) difference family over \( G \), and gives \( D_1 = \text{dev} F_1^s \) is a \(2-(7,3,s)\) design. We can check that the parameters of \( F_r \), \( F_o \), and \( F_i \) satisfy the compatibility condition (6.5). Thus the composition \( F \) of \( F_o \), \( F_i \) and \( F_r \) as in (6.10) is a difference family over \( G = G_e \times G_i \) and it generates the composition \( D = (D_o, D_i) \circ D_r \) which is a \(2-(21,5,49s)\) design with \( s = 1, \ldots, 5 \).

These are all new designs for \( s = 2, 3, 4, 5 \).

(6.3.2) Let \( G_e = I_3 \) and \( G_i = I_5 \). Then \( F_r = \{\{0, 1\}\} \) is a \((3,2,1)\) difference family over \( G_e \) and so \( D_r = \text{dev} F_r \) is a \(2-(3,2,1)\) design. Let \( F_o = \{\{1\}\} \), then it is a \((5,1,0)\) difference family over \( G_i \) and so \( D_o = \text{dev} F_o \) is a \(2-(5,1,0)\) design. Let \( F_i = \{\{0, 1, 3\}, \{0, 1, 2\}\} \), then \( F_i \) is a \((5,3,3)\)-difference family and so \( D_i = \text{dev} F_i \) is a \(2-(5,3,3)\) design. We can check that the parameters of \( F_r \), \( F_o \) and \( F_i \) satisfy the compatibility condition (6.5). Thus the composition \( F \) of \( F_o \), \( F_i \) and \( F_r \) as in (6.10) is a difference family over \( G = G_e \times G_i \) and it generates the composition \( D = (D_o, D_i) \circ D_r \) which is a \(2-(15,7,300)\) design. This is also a new design.

(6.3.3) Let \( G_e \), \( G_i \) be \( I_4 \) or \( K_4 \) where \( K_4 \) denotes the Klein's four group. Let \( F_r = \{\{a\}\} \) where \( a \) is an element of \( G_e \). Then \( F_r \) is a \((4,1,0)\) difference family over \( G_e \) and so \( D_r = \text{dev} F_r \) is a \(2-(4,1,0)\) design. Let \( F_o = \{\{g\}\} \) where \( g \) is an element of \( G_i \). Then \( F_i \) is a \((4,1,0)\)-difference family and so \( D_o = \text{dev} F_o \) is a \(2-(4,1,0)\) design.
Let $\mathcal{F}_i = \{e, g, h\}$ where $e, g$ and $h$ are elements of $\mathcal{G}_i$ with $e$ as the identity. Then $\mathcal{F}_i$ is a $(4,3,2)$-difference family and so $\mathcal{D}_i = \text{dev}\mathcal{F}_i$ is a $2-(4,3,2)$ design. We can check that the parameters of $\mathcal{F}_e, \mathcal{F}_o$ and $\mathcal{F}_i$ satisfy the compatibility condition (6.5). Thus the composition $\mathcal{F}$ of $\mathcal{F}_o, \mathcal{F}_i$ and $\mathcal{F}_e$ as in (6.10) is a difference family over $\mathcal{G} = \mathcal{G}_e \times \mathcal{G}_i$ and it generates the composition $\mathcal{D} = (\mathcal{D}_o, \mathcal{D}_i) \circ \mathcal{D}_e$ which is a $2-(16,6,128)$ design.
Bibliography


