Permutation Equivalence of Quartic 2-Rotation Symmetric Boolean Functions

by

Kelly L. Dougan

April 27, 2018

A dissertation submitted to the Faculty of the Graduate School of The University at Buffalo, State University of New York in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

Department of Mathematics
## Contents

Abstract IV

I Introduction 1
  i Definitions ............................................. 2

II Permutations Preserving 2-Rotation Symmetry 5
  i Definitions ............................................. 6
  ii Rotation Preserving Permutations ..................... 7
  iii Permutations preserving rotation symmetry for mf2 functions 13
  iv Affine Equivalence for mf2 functions .................. 16

III Number of Equivalence Classes 22
  i Definitions ............................................. 22
  ii Pólya’s Enumeration Theorem .......................... 23
  iii Number of equivalence classes of mf2 functions ...... 24

IV Counting the self-mate classes 27

V Cycle index coefficients computations 33

VI Future Work 42
  i Number of equivalence classes for mf2 functions ...... 42
  ii Application of the theory to mf1 functions .......... 42
  iii Weights of mf2 functions ............................. 43

Bibliography 44

Appendix 47
Acknowledgments

First, I would like to thank my advisor, Dr. Thomas Cusick. I appreciate all his help and advice throughout the research process, as well as our meetings which were not only insightful, but filled with humor and good conversations.

I would also like to thank my committee members, Dr. Yiqiang Li and Dr. John Ringland, for giving their time and expert opinions.

I would like to show my appreciation for all of the faculty, staff and graduate students in the Mathematics department, who have all had a part in my success.

Next, I would like to thank Matt, who patiently allowed me to talk through ideas, listened to me endlessly practice presentations and supported me no matter what.

Finally, I would like to thank my family, and in particular my parents Arden and Rodney. Their love of science and learning undoubtedly pushed me to pursue this degree.

This achievement is for all of you.
Abstract

A Boolean function is considered to be rotation symmetric if it is invariant under cyclic rotation, $\rho$, of the input variables, and is considered to be 2-rotation symmetric if it is invariant under $\rho^2$. A 2-rotation symmetric function is considered to be 2-monomial rotation symmetric (2-MRS) if the function is generated by applications of $\rho^2$ to a single monomial term. This thesis focuses on the study of mixed form 2 (mf2) quartic 2-MRS functions. These functions are generated from the monomial $x_1x_ax_bx_c$, in $2^n$ variables, denoted $2-(1,a,b,c)_{2n}$, with exactly one of $a, b$ or $c$ odd. We give a general method to determine when any two mf2 functions are equivalent by a permutation of the variables. This uses the theory of affine equivalence of quadratic MRS functions in $n$ variables, which was studied in [13]. Additionally, we show how to calculate the number of equivalence classes, and give an explicit formula in the case when the number of variables, $n = p^k, pq$ or $2^k$, where $p, q$ are odd primes.
Chapter I

Introduction

Boolean functions have been studied for their many applications in the field of Cryptography. One such example is in the design of substitution tables, or S-boxes, which are used in block ciphers such as the Data Encryption Standard (DES). An S-box is a function from $V_m \to V_n$, which can also be considered as $n$ Boolean functions over $V_m$. Kavut [12] studied rotation symmetric S-boxes and specifically $k$-rotation symmetric S-boxes, which have many desirable properties, such as high nonlinearity and low differential uniformity. This application gives motivation to further study properties of $k$-rotation symmetric Boolean functions.

Cusick and Johns [7] studied cubic 2-monomial rotation symmetric (2-MRS) Boolean functions, and were able to find conditions which would guarantee permutation equivalence among such functions. They showed that the problem of finding permutation equivalences between cubic 2-MRS functions could be reduced to finding an equivalence of corresponding cubic or quadratic 1-MRS functions.
Following the results of [7], this paper focuses on quartic mixed form 2-rotation symmetric functions as a next step toward developing a general theory. We give a method of determining the equivalence classes of such functions, based on the equivalence of corresponding quadratic 1-MRS functions. We also give a method of enumerating the equivalence classes for these functions for any degree $n$, and an explicit formula when the degree is a prime power or a product of two odd primes.

\section{Definitions}

A \textit{Boolean function} is a map from the $n$-dimensional vector space $\mathbb{V}_n$ over the field of two elements, $\mathbb{F}_2$, into $\mathbb{F}_2$. Let $f$ be a Boolean function in $n$ variables, and let $x_0 = (0, \ldots, 0), x_1 = (0, \ldots, 0, 1), \ldots, x_{2^n - 1} = (1, \ldots, 1)$ be the $2^n$ elements of $\mathbb{V}_n$, then the \textit{truth table} of $f$ is the $2^n$-tuple $(f(x_0), f(x_1), \ldots, f(x_{2^n - 1}))$.

As described in [10, p. 6], each Boolean function $f(x)$ can be written as a unique polynomial in $n$ variables over $\mathbb{F}_2$, which is called the \textit{algebraic normal form} of $f$, and can be expressed as

$$f(x_1, \ldots, x_n) = \sum_{a \in \mathbb{V}_n} c_a x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$$

where $c_a \in \mathbb{F}_2$ and $a = (a_1, a_2, \ldots, a_n)$ is a binary vector of $\mathbb{V}_n$. Let $d_i$ be the number of terms in the $i$-th monomial of the algebraic normal form of $f$, then we say that $d_i$ is the \textit{degree} of the monomial. Moreover, if $D = \{d_i\}_{i=1}^n$, the set of the degrees of all monomials in the algebraic normal form of $f$, then we say that $\max(D)$ is the \textit{degree} of $f$. 

2
Let $A$ be an $n \times n$ matrix with entries in $\mathbb{F}_2$, and $b \in \mathbb{V}_n$. If $f$, $g$ are Boolean functions in $n$ variables, then we say that $f$ and $g$ are affine equivalent if $f(Ax + b) = g(x)$ for all $x \in \mathbb{V}_n$.

Define $\rho$ to be the cyclic permutation on $n$ variables, i.e. $\rho(x_1, x_2, \ldots, x_n) = (x_2, x_3, \ldots, x_n, x_1)$. Then we say that $f$ is rotation symmetric if for all $x \in \mathbb{V}_n$, $f(\rho(x)) = f(x)$. Similarly, we say that $f$ is $k$-rotation symmetric if $k$ is the smallest integer such that $f(\rho^k(x)) = f(x)$ for all $x \in \mathbb{V}_n$. If the algebraic normal form of $f$ can be generated by cyclic (or $k$-cyclic) permutations of a monomial, we say that $f$ is monomial rotation symmetric (MRS), or analogously $k$-monomial rotation symmetric ($k$-MRS).

**Example.** Let $f$ be a quadratic MRS function in four variables, generated by the monomial $x_1x_2$. Then the algebraic normal form of $f$ is

$$f(x) = x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1.$$ 

**Example.** Let $f$ be a quartic $2$-MRS function in six variables, generated by the monomial $x_1x_2x_5x_6$. Then the algebraic normal form of $f$ is

$$f(x) = x_1x_2x_5x_6 + x_3x_4x_1x_2 + x_5x_6x_3x_4.$$ 

It follows from the definition that $k$-MRS functions are only defined in $kn$ variables.

This thesis will focus on the quartic $2$-MRS functions in $2n$ variables. Let $f$ be a $2$-MRS function in $2n$ variables, $f = x_a x_b x_c x_d + x_{a+2} x_{b+2} x_{c+2} x_{d+2} + \ldots + x_{a+2n-2} x_{b+2n-2} x_{c+2n-2} x_{d+2n-2}$. If $x_a x_b x_c x_d$ is the lexicographically
least term of \( f \), then we will refer to \( f \) as \( 2 - (a, b, c, d)_{2n} \). We will use the notation \([a, b, c, d]\) to refer to the term \( x_ax_bx cx_dx_d \) in \( f \). The terms of a quartic 2-MRS function can be written as \([a + 2i \mod 2n, b + 2i \mod 2n, c + 2i \mod 2n, d + 2i \mod 2n]\), for \( 0 \leq i \leq n \). In the case that all \( \{a, b, c, d\} \) have the same parity, there may be less than \( n \) terms, but these functions (called \textit{short functions}) are not discussed in this thesis.

We focus on the equivalence classes of 2-MRS functions, which we simplify by considering affine equivalence by a permutation matrix, or simply by permutation of the variables. These permutations which give the (permutation) equivalence classes of \( k \)-MRS functions is defined as follows.

**Definition 1.1.1.** A permutation \( \sigma \) in \( n \) variables is said to \textit{preserve \( k \)-rotation symmetry} if for any \( k \)-MRS function \( f \) in \( n \) variables, \( f \circ \sigma = g \) where \( g \) is a \( k \)-MRS function.

**Example.** Let \( f = 2 - (1, 2, 3, 4)_6 \), with algebraic normal form \( f = x_1x_2x_3x_4 + x_3x_4x_5x_6 + x_1x_2x_5x_6 \). Let \( \sigma = \left( \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 4 & 5 & 6 \end{array} \right) \), a permutation on 6 variables. Then \( f \circ \sigma = x_1x_2x_3x_4 + x_2x_4x_5x_6 + x_1x_3x_5x_6 \), which is not a 2-MRS function, therefore \( \sigma \) does not preserve 2-rotation symmetry.
Chapter II

Permutations Preserving

2-Rotation Symmetry

In this chapter, we examine the criteria for permutation equivalence for mixed form 2 (mf2) quartic 2-rotation monomial rotation symmetric functions in $2n$ variables, which we will refer to as simply mf2 functions from now on. We first find the form of all permutations on $2n$ variables which preserve 2-rotation symmetry for all quartic 2-MRS functions. We then use the form of these permutations to reduce the problem of determining whether any two given quartic 2-MRS functions in $2n$ variables are equivalent, by a permutation of the variables, to an equivalence on quadratic MRS functions in $n$ variables.
i Definitions

From the definition of the 2-MRS functions, each term of a given 2-MRS function will have the same number of even and odd variables, so we can classify a given 2-MRS function by the parity of the variables in its generating term.

Definition 2.1.1. Let \( f = 2 - (a, b, c, d)_{2n} \), then the form of \( f \) is the unordered quadruple \([a \pmod{2}, b \pmod{2}, c \pmod{2}, d \pmod{2}]\).

From the construction of the quartic 2-MRS functions, it is clear that all terms of a given function will have the same form, as the 2-MRS functions can be constructed by adding multiples of 2 to the generating monomial.

Lemma 2.1.1. Let \( f \) and \( g \) be quartic 2-MRS functions in \( 2n \) variables. If there exists a permutation \( \sigma \) which preserves 2-rotation symmetry such that \( \sigma(f) = g \), then \( f \) and \( g \) have the same form.

Proof. A proof of this can be found in [6].

This Lemma implies that any 2-MRS functions which are equivalent by a permutation which preserves rotation symmetry will have the same form. Thus when considering the equivalence classes of quartic 2-MRS functions, we can separate the functions into the different forms. We give the notation for the different forms of quartic 2-MRS function in the following definition.

Definition 2.1.2. We will denote any function with form containing only 1 or only 0 as a pure function and any function with both 0 and 1 in its form as a mixed form function. Specifically, those functions with form containing
exactly three elements of 0 or 1 will be referred to as *mixed form 1* or *mf1*
and the functions with form containing two zeros and two ones as *mixed form 2* or *mf2*.

The equivalence classes of pure functions in $2n$ variables have a bijection with equivalence classes of quartic MRS functions in $n$ variables, and similarly the equivalence classes of mf1 functions have a bijection with the equivalence classes for cubic MRS functions in $n$ variables, as is shown in [6]. In this thesis, we show how to describe the equivalence classes of mf2 functions in terms of the equivalence classes of quadratic MRS functions in $n$ variables.

## Rotation Preserving Permutations

In this section, we describe how to construct permutations which preserve rotation symmetry for quartic 2-MRS functions, which we will use to find conditions on the equivalence classes of 2-MRS functions. First we examine the permutations which fix 1, showing that permutations which preserve rotation symmetry also preserve parity for the input variables.

**Lemma 2.2.1.** If $\mu$ is a permutation that preserves rotation symmetry for quartic 2-MRS functions in $2n > 4$ variables, such that $\mu(1) = 1$, then $\mu$ sends evens to evens and odds to odds.

*Proof.* First suppose $2n = 6$; assume $\mu$ is a permutation which preserves rotation symmetry and $\mu(1) = 1$ but $\mu$ sends (at least) one of $\{3, 5\}$ to an even integer, and therefore at least one of $\{2, 4, 6\}$ is sent to an odd integer.
Since $\mu$ preserves rotation symmetry, $\mu(2-(1,2,4,6)_{6}) = 2-(1,a,b,c)_{6}$, for some integers $a,b,c$. Since $\mu(x)$ is odd for some $x \in \{2,4,6\}$, we can say without loss of generality that $a$ is odd. If both $b$ and $c$ are even, then $2-(1,a,b,c)_{6}$ is an mf2 function, and thus $2-(1,2,4,6)_{6}$ and $2-(1,a,b,c)_{6}$ cannot be equivalent, as they have different forms.

Assume without loss of generality that $b$ is odd and $c$ is even. Then both $\mu(3)$ and $\mu(5)$ must be even. So the term $\mu([3,2,4,6]) = [y,a,b,c]$, where $y$ is even. This leads to a contradiction, as $c$ is assumed to be even, and thus this term has a different form than the term $[1,a,b,c]$, so $\mu$ does not preserve rotation symmetry.

Next suppose $2n > 6$; assume $\mu$ is a permutation which preserves rotation symmetry and $\mu(1) = 1$, then $\mu(2-(1,3,5,7)_{2n}) = 2-(1,a,b,c)_{2n}$, which will both be pure odd functions. If $\mu$ sends any odd integer (greater than one) to an even integer, then the form of $2-(1,a,b,c)_{2n}$ is either mf1 or mf2, which is different than the form of $2-(1,3,5,7)_{2n}$, so the two functions cannot be equivalent, which leads to a contradiction.

The previous lemma shows that the permutations which preserve rotation symmetry preserve parity of the input variables. So, when examining the affine equivalence of mf2 functions, it is natural to split the functions into the corresponding even and odd quadratic 2-MRS functions. The following lemma shows that the permutations which preserve rotation symmetry for mf2 functions also preserve rotation symmetry for the even and odd components.
Lemma 2.2.2. If $\mu$ is a permutation that preserves rotation symmetry for quartic 2-MRS function, such that $\mu(1) = 1$, then $\mu$ preserves rotation symmetry for quadratic 2-MRS functions which contain only even or only odd variables.

Proof. Let $f$ be a quadratic 2-MRS function in $2n$ variables, $f = 2 - (a, b)_{2n}$, where $a, b$ have the same parity. Let $\tilde{f} = 2 - (a, b, c, d)_{2n}$ be an mf2 function (so $c, d$ have opposite parity as $a, b$). Then if $\mu$ preserves rotation symmetry for quartic 2-MRS functions, by Lemma 2.1.1 $\mu(\tilde{f}) = 2 - (x, y, z, w)_{2n}$ is an mf2 function, and by Lemma 2.2.1, $\mu(f) = 2 - (x, y)_{2n}$, where $x, y$ have the same parity as $a, b$. 

Now that we have shown that the permutation equivalence of quadratic mf2 functions also induces an equivalence on the even and odd quadratic 2-functions, we examine how to leverage the theory of equivalence in quadratic MRS functions in $n$ variables in order to find a condition on equivalence in mf2 functions in $2n$ variables.

Lemma 2.2.3. If $\mu$ is a permutation that preserves rotation symmetry for quartic 2-MRS functions in $2n > 4$ variables, such that $\mu(1) = 1$, then $\mu(3) = 2k + 1$, where gcd($k, n$) = 1.

Proof. From Lemma 2.2.1, $\mu$ must send evens to evens and odds to odds, $\mu(3) = 2k + 1 \mod 2n$, for some integer $k$. Thus $\mu(2 - (1, 3, 2, 4)_{2n}) = 2 - (1, 2k + 1, a, b)_{2n}$, where $a, b$ are even integers. Then, by Lemma 2.2.2, $\mu(2 - (1, 3)_{2n}) = 2 - (1, 2k + 1)_{2n}$. Let $\mu^*$ denote the permutation on $n$ variables such that $\mu^*(i) = \frac{\mu(2i-1)+1}{2}$. Then $\mu^*((1, 2)_n) = (1, k + 1)_n$ and by [3, Th. 2.6], this implies gcd($1, n$) = gcd($k, n$) = 1.
We now present the following theorem, which gives the structure of all rotation preserving permutations for quartic 2-MRS functions which send 1 to 1.

**Theorem 2.2.4.** Let $\gcd(k, n) = 1$, then $\mu$ is a permutation which preserves rotation symmetry for quartic 2-MRS functions in $2n > 4$ variables such that $\mu(1) = 1$ if and only if

$$
\mu(2i - 1) = (i - 1)2k + 1
$$
$$
\mu(2i) = (i - 1)2k + \mu(2)
$$

where $\mu(2)$ is an even integer.

**Proof.** Assume that $\sigma$ preserves rotation symmetry and that $\sigma(1) = 1$, and we shall prove that $\sigma = \mu$.

First, we will show $\sigma(2i - 1) = (i - 1)2k + 1$ for some $k \in \{k : \gcd(k, n) = 1\}$ by induction on $i$. Since we assume $\sigma(1) = 1$, and Lemma 2.2.3 proves that $\sigma(3) = 2k + 1$ for some $k \in \{k : \gcd(k, n) = 1\}$, the base case is done for $i=1,2$.

For the inductive step, assume $\sigma(2i - 1) = (i - 1)2k + 1$ for some $i$. As it is mentioned in the proof of Lemma 2.2.3, $\sigma(2 - (1, 3)2n) = (1, 2k + 1)2n$. So $\sigma([2i - 1, 2i + 1]) = [(2i - 2)k + 1, (2i - 2)k + 1 + 2k]$ and thus $\sigma(2(i + 1) - 1) = ((i + 1) - 1)2k + 1$ and the induction step is proved.

Now, we will show $\sigma(2i) = (i - 1)2k + \sigma(2)$ for all $i \in \{1, 2, \ldots, n\}$ and some $k \in \{\gcd(k, n) = 1\}$ by induction on $i$. Without loss of generality, let
\(\sigma(2) = 2j,\) and \(\sigma(4) = 2j + 2k\) for some \(j, k \in \{1, 2, \ldots, n\}.\) Again since \(\sigma\) preserves rotation symmetry for pure odd or pure even quadratic 2-MRS functions, namely \(\sigma(2 - (2, 4)_{2n}) = 2 - (2j, 2j + 2k)_{2n}.\) Define \(\sigma'\) on \(n\) variables such that \(\sigma'(i) = \frac{\sigma(2i)}{2}\). Then \(\sigma'((1, 2)_n) = (j, j + k)_n = (1, k + 1)_n.\) Then by Theorem 2.6 [3], this implies \(\gcd(1, n) = \gcd(k, n) = 1.\) So the base case is done for \(i = 1, 2.\)

Assume \(\sigma(2i) = (i - 1)2k + \sigma(2)\) for some \(i.\) Again \(\sigma(2 - (2, 4)_{2n}) = 2 - (2j, 2j + 2k)_{2n},\) so \(\sigma([2i, 2i + 2]) = [(2i - 2)k + 2j, (2i - 2)k + 2j + 2k]\) and thus \(\sigma(2(i + 1)) = (2(i + 1) - 2)k + \sigma(2)\) and the induction step is proved.

Now we have shown that for some \(k, k' \in \{k : \gcd(k, n) = 1\},\)

\[
\begin{align*}
\sigma(2i - 1) &= (i - 1)2k + 1 \\
\sigma(2i) &= (i - 1)2k' + \sigma(2)
\end{align*}
\]

and we need to show \(2k \equiv 2k' \mod 2n.\)

Let \(f = 2 - (1, 2, 3, 4)_{2n}, g = 2 - (1, a, b, c)_{2n}\) such that \(\sigma(f) = g\) for some \(a = \sigma(2), b = \sigma(3), c = \sigma(4), d = \sigma(5), e = \sigma(6).\) Then in the function \(g,\) the term \([b, c, d, e] = [1 + 2k, a + 2k, b + 2k, c + 2k],\) for some \(k.\) Since \(f\) and \(g\) are assumed to be in \(2n > 4\) variables, \(k > 0.\) So \(\sigma(4) = 2k + \sigma(2) = 2k' + \sigma(2)\) from above. This implies that \(2k \equiv 2k' \mod 2n.\)

\(\square\)

Similarly, we can find the form of any rotation preserving permutation for \(mf2\) functions.
Corollary 2.2.5. Any permutation which preserves rotation symmetry for quartic 2-MRS functions in $2n$ variables must have the following form:

$$
\begin{align*}
\mu(2i-1) &= (i-1)2k + \mu(1) \\
\mu(2i) &= (i-1)2k + \mu(2)
\end{align*}
$$

where if $\mu(1)$ is odd then $\mu(2)$ is even and if $\mu(1)$ is even then $\mu(2)$ is odd, and $\gcd(k,n) = 1$.

Proof. This can be proved by repeating the argument in Theorem 2.2.4, with different conditions on $\mu(1), \mu(2)$.

Corollary 2.2.6. There are $2n^2\phi(n)$ distinct permutations which preserve rotation symmetry on quartic 2-MRS functions.

Proof. There are $2n^2$ possible ways of choosing $\mu(1)$ and $\mu(2)$ in 2.2.5, $\phi(n)$ ways of choosing $k$, where $\phi$ is the Euler totient function.

Example. In the 6 variable case, there are 36 total permutations which preserve rotation symmetry. The permutations which preserve rotation symmetry and fix 1 in 6 variables are

$$
\{\text{id}, (1\ 2\ 3\ 4\ 5\ 6), (1\ 2\ 4\ 5\ 6\ 3), (1\ 2\ 3\ 4\ 5\ 6), (1\ 2\ 3\ 4\ 5\ 6), (1\ 2\ 3\ 4\ 5\ 6)\}
$$
iii Permutations preserving rotation symmetry for mf2 functions

Now that we have a general form for the permutations which preserve rotation symmetry for quartic 2-MRS functions, we focus on equivalence classes for mf2 functions, as a thorough exposition of the equivalence classes for pure and mf1 functions is given in [6].

The mf2 functions naturally split into quadratic 2-functions by looking at the even and odd variables separately. By separating the mf2 functions in this way, and then reducing these quadratic 2-functions in $2n$ variables to corresponding 1-MRS quadratic functions in $n$ variables, we are able to obtain conditions on equivalence classes of the mf2 functions.

We give the following definitions in order to denote the quadratic 1-MRS functions which correspond to the even and odd variables in the mf2 functions.

**Definition 2.3.1.** Let $f = 2 - (1, a, b, c)_{2n}$ be an mf2 function, with $a$ odd and $b, c$ even, $b < c$. Then we define the $f_1 = 2 - (1, a)_{2n}$, be the quadratic 2-MRS containing only the odd variables of $f$, and $f_2 = 2 - (b, c)_{2n}$ be the quadratic 2-MRS containing only the even variables of $f$. We define $f_1^* = (1, \frac{a+1}{2})_n$, $f_2^* = (1, \frac{c-b}{2} + 1)_n$ to be MRS functions in $n$ variables.

The following theorem provides an equivalence between the permutations which provide equivalence between two given mf2 functions in $2n$ variables and those permutations which give equivalence of the reduced MRS functions in $n$ variables, as defined in Definition 2.3.1.
Theorem 2.3.1. Let $f, g$ be two $mf_2$ 2-MRS functions in $2n > 4$ variables.

If $\sigma$ is a permutation which preserves rotation symmetry for 2-MRS functions for which $\sigma(1) = 1$, then $\sigma(f) = g$ if and only if $\sigma_{\text{odd}}(f_1^*) = g_1^*$ and $\sigma_{\text{even}}(f_1^*) = g_2^*$, where

$$\sigma_{\text{odd}}(i) = (i - 1)k + 1$$
$$\sigma_{\text{even}}(i) = (i - 1)k + j$$

where $\gcd(k, n) = 1$ and $1 \leq j \leq n$.

Proof. Let $f = 2 - (1, a, b, c)_{2n}$ and $g = 2 - (1, q, r, s)_{2n}$, with $a, q$ odd, and $b, c, r, s$ even. Without loss of generality, let $b < c$ and $r < s$.

First assume $\sigma(f) = g$. Then, by Theorem 2.2.4,

$$\sigma(2i - 1) = (i - 1)2k + 1$$
$$\sigma(2i) = (i - 1)2k + \sigma(2).$$

Let $\sigma_{\text{odd}}$ be defined as $\sigma_{\text{odd}}(i) = \frac{i(2i - 1)k + 1}{2}$, and let $\sigma_{\text{even}}$ be defined as $\sigma_{\text{even}}(i) = \frac{i(2i - 1)}{2}$. Then

$$\sigma_{\text{odd}}(i) = (i - 1)k + 1$$
$$\sigma_{\text{even}}(i) = (i - 1)k + \sigma(2)/2.$$

Both $\sigma_{\text{odd}}$ and $\sigma_{\text{even}}$ preserve rotation symmetry for quadratic 1-MRS functions on $n$ variables, and $\sigma_{\text{odd}}([1, \frac{a+1}{2}]) = [1, \frac{q+1}{2}]$ and $\sigma_{\text{even}}([1, \frac{c-b}{2} + 1]) = [1, \frac{r-s}{2} + 1]$, by their construction, and thus $\sigma_{\text{odd}}(f_1^*) = g_1^*$ and $\sigma_{\text{even}}(f_2^*) = g_2^*$.
Now if $\sigma_{\text{odd}}(f_1^*) = g_1^*$ and $\sigma_{\text{even}}(f_2^*) = g_2^*$ as defined above, then we can define a permutation $\sigma$ on $2n$ variables such that $\sigma(2i - 1) = 2\sigma_{\text{odd}}(i) - 1$ and $\sigma(2i) = 2\sigma_{\text{even}}(i)$. Then $\sigma(f) = g$ and $\sigma$ is a permutation that preserves rotation symmetry by Theorem 2.2.4, where $\sigma(1) = 1$ and $\sigma(2) = 2j$.

Next, we show that any two mf2 functions which are equivalent by a rotation preserving permutation are in fact equivalent by a permutation which sends 1 either to 1 or 2.

**Theorem 2.3.2.** Let $\sigma$ be a permutation which preserves rotation symmetry, and let $\phi$ and $\psi$ be quartic 2-MRS functions. If $\sigma(\phi) = \psi$ then there exists a rotation symmetry preserving permutation $\sigma^*$ such that $\sigma^*(\phi) = \psi$ and either $\sigma^*(1) = 1$ or $\sigma^*(1) = 2$.

**Proof.** Assume $\sigma(\phi) = \psi$ and $\sigma$ is defined as follows:

\[
\begin{align*}
\sigma(2i - 1) & = (i - 1)2k + \sigma(1) \\
\sigma(2i) & = (i - 1)2k + \sigma(2)
\end{align*}
\]

From Lemma 2.2.1, if $\sigma(1)$ is odd, then $\sigma$ maps odds to odds and evens to evens. Define the permutation $\sigma^*$ as

\[
\begin{align*}
\sigma^*(2i - 1) & = (i - 1)2k + 1 \\
\sigma^*(2i) & = (i - 1)2k + \sigma(2) - \sigma(1) + 1.
\end{align*}
\]

Since $\sigma^*$ shifts each term of $\sigma(\phi)$ by a fixed even amount, $1 - \sigma(1) \mod 2n$,
\[ \sigma^*(\phi) = \sigma(\phi) = \psi. \]

Similarly, if \(\sigma(1)\) is even, then \(\sigma\) maps odds to evens and evens to odds. Define the permutation \(\sigma^*\) as

\[
\begin{align*}
\sigma^*(2i - 1) &= (i - 1)2k + 2 \\
\sigma^*(2i) &= (i - 1)2k + \sigma(2) - \sigma(1) + 2.
\end{align*}
\]

Since \(\sigma^*\) shifts each term of \(\sigma(\phi)\) by a fixed even amount, \(2 - \sigma(1) \mod 2n\), \(\sigma^*(\phi) = \sigma(\phi) = \psi. \)

So when finding equivalence classes for quartic 2-MRS functions, we can restrict the number of permutations to \(2n\phi(n)\), as there are \(n\) ways of choosing \(\sigma(2)\) once \(\sigma(1)\) has been determined, and \(\phi(n)\) ways to choose \(k\).

### iv  Affine Equivalence for mf2 functions

Using the explicit form for permutations which produce equivalence classes of mf2 functions, we can find conditions on the upper bound of the size of equivalence classes for mf2 functions, as well as conditions for all functions in a given equivalence class.

**Theorem 2.4.1.** Any given equivalence class of quartic 2-MRS functions in \(2n\) variables has at most \(n\phi(n)\) elements.

**Proof.** Let \(f = 2 - (1, a, b, c)_{2n}\), define \(\tilde{a} = \frac{a+1}{2}, \tilde{b} = \frac{c-b}{2} + 1\) and \(f_{\text{odd}} = (1, \tilde{a}), f_{\text{even}} = (1, \tilde{b})\), the deflated functions in \(n\) variables. Define the permutation \(\sigma_{k,j}\) on \(n\) variables to be \(\sigma_{k,j}(i) = (i - 1)k + j\). By Theorem 2.3.1,
in order to find the 2-MRS functions equivalent to \( f \), it suffices to look at the permutations \( \sigma_{k,j} \) applied to the deflated functions \( f_{\text{even}}, f_{\text{odd}} \).

If \( \gcd(k, n) = 1 \), then \( \gcd(n - k, n) = 1 \), so if \( k_1, \ldots, k_{\phi(n)} \) are the numbers coprime to \( n \), ordered from least to greatest, then \( \{ k \mid \gcd(k, n) = 1 \} = \{ k_1, \ldots, k_{\phi(n)/2}, n - k_{\phi(n)/2}, \ldots, n - k_1 \} \). The following shows that \( \sigma_{k,j} \) and \( \sigma_{n-k,j} \) generate the same quadratic MRS functions in \( n \) variables.

\[
\sigma_{k,j}((1, a)) = (j, (a - 1)k + j) \\
= (1, (a - 1)k + 1) \\
\equiv (1, n - (a - 1)k + 1)
\]

\[
\sigma_{n-k,j}((1, a)) = (j, (a - 1)(n - k) + j) \\
= (1, (a - 1)(n - k) + 1) \\
\equiv (1, n - (a - 1)k + 1)
\]

So when finding equivalence classes, we can restrict the number of permutations to \( \phi(n)/2 \). By Theorem 2.3.2, it suffices to consider only permutations for which \( \sigma(1) = 1 \) or \( \sigma(1) = 2 \). In each case, when we deflate \( \sigma_{\text{odd}} = \sigma_{k,1} \) and \( \sigma_{\text{even}} = \sigma_{k,j} \) for one of the \( \phi(n)/2 \) such \( k \) and \( j \in \{1, \ldots, n\} \), we obtain a maximum of \( n\phi(n)/2 \) possible functions which are equivalent to \( f \). Together, this gives an upper bound of \( n\phi(n) \) functions in the equivalence class of \( f \).

As we have seen in section iii, the permutations which send one mf2 function to another depend on separating a given mf2 function into its even and odd variables, then deflating these functions to half the number of vari-

17
ables. In order to give a condition on equivalence, we define $\chi$ values, which help to separate the behavior of the even and odd variables.

**Definition 2.4.1.** Let $f = 2 - (1, a, b, c)_{2n}$, where $a$ odd and $b, c$ even mod $2n$, with $b < c$. Let $\chi_1 = \frac{a - 1}{2}$, $\chi_2 = \frac{c - b}{2}$, the $\chi$ values of $f$ are $\{\chi_1, \chi_2\}$.

**Theorem 2.4.2.** If $f$ and $g$ are quartic 2-MRS functions, then $f$ and $g$ are equivalent by a permutation which preserves rotation symmetry if and only if the $\chi$ values of $g$ are $\{k\chi_1, f, k\chi_2, f\}$, $\{k\chi_1, f, n - k\chi_2, f\}$, $\{n - k\chi_1, f, k\chi_2, f\}$ or $\{n - k\chi_1, f, n - k\chi_2, g\}$, where $\gcd(k, n) = 1$, and $\{\chi_1, f, \chi_2, f\}$ are the $\chi$ values of $f$.

**Proof.** Assume $f$ and $g$ are equivalent by a permutation $\sigma$ which preserves rotation symmetry, by Theorem 2.3.2,

$$
\sigma(2i - 1) = ((2i - 1) - 1)k + \sigma(1) \\
\sigma(2i) = (2i - 2)k + \sigma(2),
$$

where $\sigma(1) = 1$ or $\sigma(1) = 2$, and for some $k$ with $\gcd(k, n) = 1$. Let $\sigma(1) = 1$, and the argument when $\sigma(1) = 2$ is similar.

Let $f = 2 - (1, a, b, c)_{2n}$, then $\chi_1, f = \frac{a - 1}{2}$, and $\chi_2, f = \frac{c - b}{2}$. Since $\sigma(f) = g$, we can write $g$ as $g = 2 - (1, (a - 1)k + 1, (b - 2)k + \sigma(2), (c - 2)k + \sigma(2))_{2n}$.

So $\chi_1, g = \frac{k(a - 1)}{2} = k\chi_1, f$ and $\chi_2, g = \frac{k(c - b)}{2} = k\chi_2, f$, and thus the $\chi$ values of $g$ are $\{k\chi_1, f, k\chi_2, f\}$, and the necessary condition of the theorem is proved.

Now to prove the sufficient condition, let $g = 2 - (1, p, q, r)_{2n}$ then the $\chi$ values of $g$ are $\chi_1, g = \frac{p - 1}{2}$, $\chi_2, g = \frac{r - q}{2}$. 

18
First assume that \( \chi_{1,g} = k \chi_{1,f}, \chi_{2,g} = k \chi_{2,f} \). Then we have the following set of equivalences:

\[
\begin{align*}
\frac{p - 1}{2} & \equiv \frac{(a - 1)k}{2} \mod n \\
p - 2 & \equiv (a - 1)k \mod 2n \\
r - q & \equiv \frac{(c - b)k}{2} \mod n \\
r - q & \equiv (c - b)k \mod 2n \\
\Rightarrow r & \equiv (c - 2)k + q + (2 - b)k \mod 2n \\
\Rightarrow q & \equiv (b - 2)k + r + (2 - c)k \mod 2n
\end{align*}
\]

Then \( \sigma(f) = g \), where

\[
\begin{align*}
\sigma(2i - 1) &= ((2i - 1) - 1)k + 1 \\
\sigma(2i) &= (2i - 2)k + \sigma(2),
\end{align*}
\]

and \( \sigma(2) = q + (2 - b)k \equiv r + (2 - c)k \).

Now if \( \chi_{1,g} = n - k \chi_{1,f}, \chi_{2,g} = k \chi_{2,f} \). Then we have the following set of equivalences:

\[
\begin{align*}
\frac{p - 1}{2} & \equiv n - \frac{(a - 1)k}{2} \mod n \\
p - 1 & \equiv 2n - (a - 1)k \mod 2n \\
& \equiv \left( \frac{a + 1}{2} - 1 \right) (2n) - (a - 1)k \mod 2n \\
& \equiv (a - 1)(n - k) \mod 2n \\
r - q & \equiv \frac{(c - b)k}{2} \mod n
\end{align*}
\]
\[\equiv 2n - (b - c)k \mod 2n\]
\[\equiv (b - c)(n - k) \mod 2n\]

Then, since \(\gcd(n - k, n) = 1\), \(\sigma(f) = g\), where

\[\sigma(2i - 1) = ((2i - 1) - 1)(n - k) + 1\]
\[\sigma(2i) = (2i - 2)(n - k) + \sigma(2),\]

and \(\sigma(2) = q + (b - 2)k \equiv r + (c - 2)k\).

A similar argument shows that \(f\) and \(g\) are equivalent when \(\chi_{1,g} = k\chi_{1,f}, \chi_{2,g} = n - k\chi_{2,f}\) or \(\chi_{1,g} = n - \chi_{1,f}, \chi_{2,g} = n - k\chi_{2,f}\), as well as when the \(\chi\) values from the even values of \(f\) correspond to the odd \(\chi\) values of \(g\), and vice versa.

As shown in the proof of Theorem 2.4.1, it suffices to look at the first \(\phi(n)/2\) values of \(k\) with \(\gcd(k, n) = 1\) to find equivalence classes. And since any two functions are equivalent if their \(\chi\) values are equal up to a multiple of \(k\), we can determine an equivalence class for quartic 2-MRS functions in \(2n\) variables by grouping all \(\chi\) values if they are equal up to a multiple of one of the \(\phi(n)/2\) values of \(k\).

**Example.** Let \(f = 2 - (1, 2, 3, 4)_{10}, g = 2 - (1, 2, 5, 6)_{10}\), \(\text{mf}2\) functions in 10 variables. The \(\chi\) values of \(f\) are \(\{1, 1\}\), and the \(\chi\) values of \(g\) are \(\{2, 2\}\).

\(f\) and \(g\) are permutation equivalent because \(\{2\chi_{1,f}, 2\chi_{2,f}\} \equiv \{\chi_{1,g}, \chi_{2,g}\}\).

**Example.** Let \(f = 2 - (1, 2, 3, 4)_{10}, g = 2 - (1, 2, 5, 8)_{10}\), \(\text{mf}2\) functions in 10 variables. The \(\chi\) values of \(f\) are \(\{1, 1\}\), and the \(\chi\) values of \(g\) are \(\{2, 3\}\).
$f$ and $g$ are permutation equivalent because $\{2\chi_{1,f}, 5-2\chi_{2,f}\} \equiv \{\chi_{1,g}, \chi_{2,g}\}$.

Using this theory, the equivalence classes for mf2 functions were computed in Python, and the results for $n = 3, \ldots, 7$ are given in Tables 1-5.
Chapter III

Number of Equivalence Classes

In the previous chapter, we found a condition on affine equivalence of mf2 functions in $2n$ variables. In this chapter, we will use the $\chi$ pairs from section iv to develop the theory of counting mf2 equivalence classes in $2n$ variables. We will begin by stating some definitions.

i Definitions

We will refer to $\mathbb{Z}_n$ as the cyclic group of integers modulo $n$ under addition, and $U_n$ as the multiplicative group of units of $\mathbb{Z}_n$. For $a \in U_n$ and $z \in \mathbb{Z}_n$, define the following group action $g \cdot z = g z \mod n$. Similarly, we can extend this group action to pairs of elements of $\mathbb{Z}_n$; let $i, j \in \mathbb{Z}_n$, then define the action $a \cdot \{i, j\} = \{ai \mod n, aj \mod n\}$. 
Definition 3.1.1. Let \( \{i, j\} \) be a pair of the nonzero elements \( \mathbb{Z}_n^+ \). The equivalence class of \( \{i, j\} \) is defined as \( \{i, j\} = \{a \cdot \{i, j\} \mid a \in U_n\} \).

Definition 3.1.2. Let \( \{i, j\}, \{x, y\} \) be pairs of the nonzero elements \( \mathbb{Z}_n^+ \). Then we say \( \{i, j\} \sim \{x, y\} \) if there exists an element \( a \in U_n \) such that \( a \cdot \{i, j\} \in \{\{x, y\}\} \).

In order to count the number of \( \chi \) pairs, and therefore the number of equivalence classes of mf2 functions in \( 2^n \) variables, we will begin by examining the equivalence classes of pairs of elements in \( \mathbb{Z}_n^+ \) defined in Definition 3.1.1.

ii Pólya’s Enumeration Theorem

In order to count the equivalence classes detailed in Section i, we will need to review the Pólya theory of counting. Pólya’s theory of counting is well known in combinatorics. His fundamental theorem, which we will summarize here, gives a way to count the number of ways to color the elements of a set under certain symmetries. For a more detailed account of the theory, see [8].

Let \( G \) act on a set \( X \), with \( |X| = n \), and for each \( \sigma \) in \( G \), let \( \bar{\sigma} \) be the corresponding permutation on the set \( X \). Let \( l_i(\sigma) \) be the number of cycles of \( \bar{\sigma} \) with length \( i \). Then the cycle index polynomial of \( G \) is defined as

\[
Z_G(x_1, \ldots, x_n) = \frac{1}{|G|} \sum_{\sigma \in G} \prod_{i=1}^{n} x_i^{l_i(\sigma)}.
\]

Now let \( C \) be a set of colors for the set \( X \), i.e. there is a coloring
function \( f : X \rightarrow C \) assigning the elements of \( X \) to the colors of \( C \), and to each color \( c \in C \), we assign a weight, \( w_c \). The following theorem gives us a way to enumerate the weighted colorings of \( X \), up to permutations of the set \( X \) by the action of \( G \).

**Theorem 3.2.1** (Pólya’s Enumeration Theorem, [2]). *If \( G \) is a group which acts on a set \( X \), colored by a set \( C \), and weighted by \( w \). Then the enumeration of the weights is given by*

\[
Z_G \left( \sum_{i=1}^{m} w_{c_1}, \sum_{i=1}^{m} w_{c_2}^2, \ldots, \sum_{i=1}^{m} w_{c_l}^n \right)
\]

So given an assignment of weights on a coloring of the set \( X \), the number of ways to assign \( j_i \) weights \( w_i \), under the equivalence of permutations of \( X \) by the action of \( G \) is equal to the coefficient of \( \prod_i w_i^{j_i} \) in the cycle index polynomial from Theorem 3.2.1.

### iii Number of equivalence classes of mf2 functions

Let us now apply Pólya’s theory to find the number of equivalence classes given in Definition 3.1.1.

**Lemma 3.3.1.** *The cycle index polynomial for \( U_n \) acting on \( \mathbb{Z}_n \) is*

\[
Z_n(x_1, x_2, \ldots x_n) = \frac{1}{\phi(n)} \sum_{a \in U_n} \prod_{d|n} x_{\phi(d)/\text{ord}_d(a)}^{\phi(d)/\text{ord}_d(a)}
\]

*Proof.* See [1, Corollary 3.1].
Theorem 3.3.2. The coefficient of $y^2$ in the cycle index polynomial

$$Z_n(1 + y, 1 + y^2, \ldots, 1 + y^n)$$

gives the number of equivalence classes of pairs under $\sim$ in Definition 3.1.2.

Proof. Let $U_n$ act on $\mathbb{Z}_n$ by multiplication modulo $n$. Let $C$ be the set of colors $\{0, 1\}$ with weights $w_0 = 1, w_1 = y$. Theorem 3.2.1 gives us that the number of distinct such colorings of $\mathbb{Z}_n$ under the action of $U_n$, with exactly $i$ elements assigned the weight $y$ is the coefficient of $y^i$ in the cycle index polynomial $Z_n(1 + y, 1 + y^2, \ldots, 1 + y^n)$.

Let $\tilde{X}$ be the set of all ordered pairs $\{i, j\}$, with $i, j \in \mathbb{Z}_n^+$. We will give a bijection between the colorings of $\mathbb{Z}_n$ under the action of $U_n$ with exactly two elements assigned to $y$, and the number of equivalence classes under $\sim$ of the set $\tilde{X}$. For all $i \in \mathbb{Z}_n^+$, we assign $x_i$ the weight 1 if $i$ does not appear in a given pair, and we assign $x_i$ the weight $y$ if $i$ appears in the pair. We assign the element 0 the weight 1 if the pair contains two distinct elements, and we assign 0 the weight $y$ if the pair contains a duplicate. Under this coloring, the coefficient of $y^2$ gives us the number of equivalence classes under the action $\sim$. \hfill \Box

This gives us a way to count the number of equivalence classes of pairs of elements in $\mathbb{Z}_n^+$, but in order to count the number of $\chi$ pairs under $\sim$, and therefore the number of equivalence classes for $\text{mf}2$ functions, we need to ensure that $\{i, j\} \sim \{i, n - j\}$, for all $i, j \in \mathbb{Z}_n^+$. In order to do so, we introduce the following definition.
Definition 3.3.1. An equivalence class \([i,j]\) under Definition 3.1.2 is self-mate if \(\{i, n - j\} \in \{i, j\}\).

Theorem 3.3.3. Let \(b_n\) be the number of equivalence classes given in Definition 3.1.2 and let \(s_n\) be the number of self-mate equivalence classes, both over \(\mathbb{Z}_n^+\) (and we will simply refer to these as \(b\) and \(s\) if the number of variables \(n\) is understood). Then the number of equivalence classes of \(mf_2\) functions in \(2n\) variables is \(b + s\).

Proof. As shown in Theorem 2.4.2, two \(mf_2\) functions \(f, g\) in \(2n\) variables are equivalent if and only if \(\{\chi_{1,f}, \chi_{2,f}\} \sim \{\chi_{1,g}, \pm \chi_{2,g}\}\). The number of equivalence classes of such pairs \(b\) counts the number of pairs which are equivalent under \(\sim\), but does not identify pairs \(\{i, j\}\) such that \(\{i, j\} \not\sim \{i, -j\}\). Thus the number of equivalence classes of \(\chi\) pairs, is equal to \(\frac{b + s}{2}\) because \(b + s\) double counts each pair, whether or not the pair is self-mate, thus we divide by 2 to obtain the number of equivalence classes. 

Now that we have a method of counting the equivalence classes of \(mf_2\) functions, we can divide the problem into counting the number of self-mate classes and the number of equivalence classes of pairs, given by the coefficients of the cycle index polynomials.
Chapter IV

Counting the self-mate classes

In this chapter, we give a general formula for the number of self-mate classes. In order to obtain this formula, we provide the following lemmas which simplify the problem of finding representatives of self-mate classes.

Lemma 4.0.1. Let $\gcd(n, i) = q$, $\gcd(n, j) = r$. If $q \neq r$, then the equivalence class \{i, j\} is self-mate if and only if $\gcd(nq, nr) \in \{1, 2\}$.

If $q = r$, then \{i, j\} is self-mate if and only if there exists a quadratic residue of $-1 \pmod{nq}$.

Proof. Let $i = aq, j = br$, where $a, b \in U_n$. Then \{i, j\} $\in$ \{q, xr\} where $x \equiv a^{-1}b \pmod{n}$. The equivalence class \{\{i, j\}\} is self-mate if and only if there exists $y \in U_n$ such that $y\{q, xr\} \equiv \{q, -xr\}$.

If $y\{q, xr\} \equiv \{q, -xr\}$, then there are two cases to consider. The first case is when $yq \equiv q \pmod{n}$ and $yxr \equiv -xr \pmod{n}$, and so $y \equiv 1$.
and \( y \equiv -1 \pmod{n} \). Then by an application of the Chinese Remainder Theorem, this is only possible if \( 1 = -1 \pmod{\gcd(n, r)} \). This equivalence only occur when \( \gcd(n, q) \in \{1, 2\} \). When \( q = r \), then this is occurs when \( \frac{n}{q} \in \{1, 2\} \). Since \( i, j \) are assumed to be elements of \( \mathbb{Z}_n \), thus \( 1 \leq i, j < n \), which implies that \( q < n \), and therefore \( \frac{n}{q} \neq 1 \). Thus the equivalence in this case occurs only when \( \frac{n}{q} = 2 \), and -1 is a quadratic residue \( \pmod{2} \).

The second case is when \( yq \equiv -xr \pmod{n} \) and \( yxq \equiv r \pmod{n} \). If we assume that \( q \neq r \), then since \( x, y \in U_n \), this would imply that \( \gcd(n, q) = \gcd(n, r) \), which leads to contradiction, as \( q, r \) are factors of \( n \). When \( q = r \), the above equivalences imply that \( (y^2 + 1)q \equiv 0 \pmod{n} \), or \( y^2 \equiv -1 \pmod{\frac{n}{q}} \).

Now we have conditions on when a given equivalence class representative will be self-mate, depending on the greatest common factor between \( n \) and the representative elements. We will use this condition to count the number of self-mate classes. First, we show that any pair which have the same pair of greatest common factors with \( n \) are in the same self-mate equivalence class.

**Lemma 4.0.2.** Let \( q, r \) be factors of \( n \) such that \( \gcd(n, q) \in \{1, 2\} \). For all \( x \in U_n, \{q, r\} \sim \{q, xr\} \).

**Proof.** It follows from Definition 3.1.1 that \( \{q, r\} \sim \{q, xr\} \) if and only if there exists \( a \in U_n \) such that either \( aq \equiv q \pmod{n} \) and \( ar \equiv xr \pmod{n} \) or \( aq \equiv xr \pmod{n} \) and \( ar \equiv q \pmod{n} \). The latter case will only hold when
$q = r$, since $q$ and $r$ are factors of $n$. When $q = r$, then for any $x \in U_n$, \{q, xq\} \sim \{q, q\} by letting $a = x^{-1}$.

The former case occurs if and only if $a \equiv 1 \pmod{\frac{n}{q}}$ and $a \equiv x \pmod{\frac{n}{r}}$. As a result of the Chinese Remainder Theorem, this is true if and only if $x \equiv 1 \pmod{\gcd(\frac{n}{q}, \frac{n}{r})}$. If $\gcd(\frac{n}{q}, \frac{n}{r}) = 1$, then this is clearly true, and if $\gcd(\frac{n}{q}, \frac{n}{r}) = 2$, then $x \equiv 1 \pmod{2}$ because $x \in U_n$ and in this case $2 | n$. □

It is clear from Lemma 4.0.1 that in counting the self-mate classes it will be important to know the number of quadratic residues of $-1$ for each factor of $n$. The following lemma provides a way of counting the number of self-mate classes from the second case of Lemma 4.0.1, based on the number of quadratic residues of $-1$.

**Lemma 4.0.3.** If $q | n$, $r = \frac{n}{q}$ and there exist $k$ quadratic residues of $-1 \pmod{q}$, then there are $\frac{k}{2}$ self-mate classes of the form \{r, xr\}, where $x^2 \equiv -1 \pmod{q}$.

**Proof.** If there are $k$ quadratic residues of $-1 \pmod{q}$, then \{r, xr\} \sim \{r, -xr\} for each $x \in \{x : x^2 \equiv -1 \pmod{m}\}$. And if $x, y$ are quadratic residues mod $m$, then it is simple to check that \{r, xr\} \equiv \{r, yr\} if and only if $x \equiv y$, leaving $\frac{k}{2}$ self-mate equivalence classes of this form. □

With the previous lemmas, the number of self-mate equivalence classes is equal to the number of pairs of factors $q, r$ of $n$ such that $\gcd(q, r) \in \{1, 2\}$ plus the number of factors $m$ of $n$ where $-1$ is a quadratic residue mod $m$, times half the number of such quadratic residues. We compute and prove these formulas for even and odd $n$ separately in the following theorems.
Theorem 4.0.4. For $n = \prod_{i=1}^{k} p_i^{e_i}$, where each $p_i$ is an odd prime, and $p_i \neq p_j$, the number of self-mate equivalence classes is

$$\sum_{i=2}^{k} \sum_{S \subseteq \mathcal{P}} \prod_{s \in S} s \cdot (2^{i-1} - 1) + \sum_{i=1}^{m} \sum_{S \subseteq \mathcal{M}} \prod_{s \in S} s \cdot 2^{i-1},$$

where $m$ is the number of prime factors $p_i \equiv 1 \pmod{4}$, $\mathcal{P} = \{e_i\}_{i=1}^{k}$, and $\mathcal{M} = \{e_i : p_i \equiv 1 \pmod{4}\}$.

Proof. By Lemmas 4.0.2 and 4.0.1, since $n$ is odd, counting the self-mate equivalence classes is equivalent to counting all pairs of factors $\{i, j\}$ such that $gcd(i, j) = 1$ and counting all factors $P$ of $n$ where $-1$ is a quadratic residue $\pmod{P}$, multiplying by $\frac{q}{2}$, where $q$ is the number of quadratic residues of $-1 \pmod{P}$, by Lemma 4.0.3.

First, to count all pairs of factors $\{i, j\}$ such that $gcd(i, j) = 1$, we should look at the number of ways to split any combination of $i$ prime power factors of $n$ into pairs. Given any $i$ prime power factors $\{p_{j_1}^{e_{j_1}}, p_{j_2}^{e_{j_2}}, \ldots, p_{j_i}^{e_{j_i}}\}$, there will be $e_1 e_2 \cdots e_i$ ways of combining $i$ factors $\{p_{j_1}^{f_{j_1}}, p_{j_2}^{f_{j_2}}, \ldots, p_{j_i}^{f_{j_i}}\}$, where $f_{j_l} \leq e_{j_l}$ for all $l = 1, \ldots i$. For each combination of the factors, there is $2^{i-1} - 1$ ways of splitting the combination into pairs. So if $\mathcal{P} = \{e_i\}_{i=1}^{k}$, the number of pairs of factors $\{i, j\}$ such that $gcd(i, j) = 1$ is

$$\sum_{i=2}^{k} \sum_{S \subseteq \mathcal{P}} \prod_{s \in S} s \cdot (2^{i-1} - 1).$$

Now, if $m$ is the number of prime factors $p_i$ of $n$ such that $p_i \equiv 1 \pmod{4}$, then for any combination of $i$ prime power factors of $n$, $\{p_{j_1}^{e_{j_1}}, p_{j_2}^{e_{j_2}}, \ldots, p_{j_i}^{e_{j_i}}\}$, where $i \leq m$, there will be $e_1 e_2 \cdots e_i$ ways of combining $i$ factors $\{p_{j_1}^{f_{j_1}}, p_{j_2}^{f_{j_2}}, \ldots, p_{j_i}^{f_{j_i}}\}$, where $f_{j_l} \leq e_{j_l}$ for all $l = 1, \ldots i$. For each of these factors, there are
2^i quadratic residues of \(-1 \mod p_{j_1}^{f_{j_1}} \cdot p_{j_2}^{f_{j_2}} \cdots p_{j_i}^{f_{j_i}}\). Then by Lemma 3, there is a total of \(\sum_{i=1}^{m} \sum_{S \subseteq M} \prod_{s \in S} s \cdot 2^{i-1}\) self-mate classes of the form \(\{\prod_{i=1}^{i} p_{j_i}^{f_{j_i}}, a \prod_{i=1}^{i} p_{j_i}^{f_{j_i}}\}\).

**Theorem 4.0.5.** For \(n = 2^a \prod_{i=1}^{k} p_i^{e_i}\), where each \(p_i\) is a distinct odd prime, the number of self-mate equivalence classes is

\[
\sum_{i=2}^{k+1} \sum_{S \subseteq \mathcal{P}} \prod_{s \in S} s \cdot (2^{i-1} - 1) + (2a - 1) \sum_{i=1}^{k} \sum_{S \subseteq \mathcal{P}_2} \prod_{s \in S} s \cdot 2^{i-1} + \sum_{i=1}^{m} \sum_{S \subseteq \mathcal{M}} \prod_{s \in S} s \cdot 2^i + a,
\]

where \(m\) is the number of prime factors \(p_i \equiv 1 \mod 4\), \(\mathcal{P}\) is the set of all powers of prime factors of \(n\), \(\mathcal{P}_2 = \{e_i\}_{i=1}^{k}\), and \(\mathcal{M} = \{e : p_i \equiv 1 \mod 4\}\).

**Proof.** Following the proof of Theorem 4.0.4, we need to first count the number of pairs \(\{i, j\}\), \(i, j\) both factors of \(n\), with \(gcd(i, j) = 1\). Since there are \(k - 1\) prime factors, there will be \(\sum_{i=2}^{k+1} \sum_{S \subseteq \mathcal{P}} \prod_{s \in S} s \cdot (2^{i-1} - 1)\) total pairs of this type.

Now, we will count the number of pairs \(\{i, j\}\) with \(gcd(i, j) = 2\). For any combination of \(i\) odd prime power factors of \(n\), there are \(2^{i-1} - 1\) ways of splitting the \(i\) factors into unordered pairs, and one way to make an unordered pair of the form \(\{1, P\}\), where \(P\) is the product of the \(i\) factors. The total number of such pairs is \(\sum_{i=1}^{k} \sum_{S \subseteq \mathcal{P}_2} \prod_{s \in S} s \cdot 2^{i-1}\). To count the number of all pairs with \(gcd(i, j) = 2\), we need to multiply this by \(2a - 1\), for there are \(2a - 1\) distinct pairs of the form \(\{2, 2^i\}\) or \(\{2^i, 2\}\), as each pair \(\{i, j\}\) with \(gcd(i, j) = 2\) will be of the form \(\{2P, 2^iQ\}\), where \(1 \leq i \leq a\) and \(P, Q\) are odd factors of \(n\), with \(gcd(P, Q) = 1\). Then, to finish this count, there are also \(a\) pairs of the form \(\{2^i\}\).
To count all factors with a quadratic residue of -1, we can follow the proof of Theorem 4.0.4, and we obtain \( \sum_{i=1}^{m} \sum_{S \subseteq \mathcal{M}} \prod_{s \in S} s \cdot 2^{i-1} \) pairs of the form \( \{P, aP\} \), where \( P \) is an odd factor of \( n \), multiplied by 2, for each pair of the form \( \{2P, 2aP\} \).

**Example.** Let \( n = 15 \), then \( k = 2, \mathcal{P} = \{1, 1\}, m = 1, \) and \( \mathcal{M} = \{1\} \). So the number of self mate equivalence classes of \( \mathbb{Z}_{15} \) is equal to

\[
\sum_{i=2}^{2} \sum_{|S|=i} \prod_{s \in S} s \cdot (2^{i-1} - 1) + \sum_{i=1}^{1} \sum_{|S|=i} \prod_{s \in S} s \cdot 2^{i-1}
= 1(2 - 1) \cdot 1(2 - 1) + 1(2^0) = 2.
\]

The representatives of the self-mate equivalence classes of \( \mathbb{Z}_{15} \) are \( \{3, 5\} \) and \( \{3, 6\} \), which was calculated by a program in Python.
Chapter V

Cycle index coefficients computations

In this chapter, we offer a collection of formulas for the number of equivalence classes of pairs of elements of $\mathbb{Z}_n^+$, or the value of $b$ in Theorem 3.3.3 for certain values of $n$. For $n = pq$ and $n = p^k$, this is done by first computing the cycle index polynomial from Lemma 3.3.1 and then computing the coefficient of $y^2$, which gives the number of equivalence classes by Theorem 3.2.1. In the case of $n = 2^k$, we compute the coefficient of $y^2$ directly, without first finding the cycle index polynomial.

**Theorem 5.0.1.** Let $p$ be an odd prime. The cycle index polynomial, $Z_{p^k}(x_1, x_2, \ldots, x_{p^k})$, of $U_{p^k}$ acting on $\mathbb{Z}_{p^k}$ is equal to

$$
\frac{1}{p^k - p^{k-1}} \sum_{d|p-1} \phi(dp^j) \prod_{i=0}^{k-j} x_{d \phi(p^i) \text{ mod } \phi(p^i)} \prod_{m=k-j+1}^k x_{dp^m - (k-j)}
$$
Proof. As $U_{p^k}$ is a cyclic group of order $\phi(p^k)$, and for each divisor $d$ of $\phi(p^k)$, there are $\phi(d)$ elements of order $d \mod p^k$. Then, by Lemma 3.3.1, there will be $\phi(d)$ terms with a factor of $x^{\phi(p^k)/d}$. The rest of the factors of each term are of the form $x^{\phi(p^i)/\text{ord}_{p^i}a}$, where $a \in U_{p^i}$.

Since $d \mid \phi(p^k) = p^k - 1$, $d = bp^j$, where $b \mid p - 1, j \leq k - 1$. If $a$ has order $d$, then $a = x^{\phi(p^k)/d} = x^{\frac{p^k - 1}{p^j}}$ where $x$ is a generator of $U_{p^k}$. If $i \leq k - j$, then $\text{ord}_{p^i}a \equiv b \mod \phi(p^j)$, and if $i > k - j$, then $\text{ord}_{p^i}a \equiv bp^j(k - j) \mod \phi(p^j)$.

**Corollary 5.0.2.** Let $p$ be an odd prime. The coefficient of $y^2$ in the polynomial $Z_{p^k}(1 + y, 1 + y^2, \ldots, 1 + y^k)$ is

$$\frac{1}{\phi(p^k)} \sum_{j=0}^{k-1} \frac{\phi(p^j)(p^{2(k-j)} - 1)}{2}$$

Proof. In order to determine the coefficient of $y^2$, we need to find all terms with a factor of $x_1$ or $x_2$ in $Z_{p^k}(x_1, \ldots, x_{p^k})$. From the formula for $Z_{p^k}$ in Theorem 5.0.1, the terms with a factor of $x_1$ occur when $d = 1$ and $i \leq k - j$.

So each such term contributes $k - j$ factors of $x_1$,

$$\frac{\phi(p^j)}{\phi(p^k)} \prod_{i=0}^{k-j} x_1^{p^i - p^{i-1}} = \frac{\phi(p^j)}{\phi(p^k)} x_1^{\prod_{i=1}^{k-j} \phi(p^j)x_1^{p^i - p^{i-1}}} = \frac{\phi(p^j)}{\phi(p^k)} x_1^{p^{k-j}}.$$ 

If we substitute $1 + y$ for $x_1$, then the coefficient of $y^2$ is $\frac{\phi(p^j)}{\phi(p^k)} (p^{k-j})$.

Similarly, the terms with a factor of $x_2$ occur when $d = 2$ and $i \leq k - j$. 

34
Each term contributes \( k - j - 1 \) factors of \( x_2 \),

\[
\phi(2p^j) \prod_{i=1}^{k-j} x_2^{(p^{i-j}-1)/2} = \phi(p^j)x_2^{(k-j-1)/2}.
\]

If we substitute \( 1 + y^2 \) for \( x_2 \), then the coefficient of \( y^2 \) is \( \frac{\phi(p^j)}{\phi(p^k)} \left( \frac{p^{k-j} - 1}{1} \right) \).

Combining the coefficients coming from \( x_1 \) and \( x_2 \), ranging over \( j \), we obtain

\[
\sum_{j=1}^{k-1} \frac{\phi(p^j)}{\phi(p^k)} \left( \binom{p^{k-j}}{2} + \binom{p^{k-j-1}}{1} \right)
\]

\[
= \sum_{j=1}^{k-1} \frac{\phi(p^j)}{\phi(p^k)} \left( \frac{p^{k-j}(p^{k-j} - 1)}{2} + \frac{p^{k-j} - 1}{2} \right)
\]

\[
= \sum_{j=1}^{k-1} \frac{\phi(p^j)}{\phi(p^k)} \left( \frac{(p^{k-j} + 1)(p^{k-j} - 1)}{2} \right)
\]

\[
= \sum_{j=1}^{k-1} \frac{\phi(p^j)}{\phi(p^k)} \left( \frac{(p^{2(k-j)} - 1)}{2} \right).
\]

\( \square \)

**Theorem 5.0.3.** Let \( p, q \) be odd primes. The cycle index polynomial, \( Z_{pq}(x_1, \ldots, x_{pq}) \), for \( U_{pq} \) acting on \( \mathbb{Z}_{pq} \) is

\[
\frac{1}{\phi(pq)} x_1 \sum_{d_1|\phi(p)} \phi(d_1) \phi(d_2) x_1^{\phi(p)/d_1} x_2^{\phi(q)/d_2} x_{\text{lcm}(d_1,d_2)}^{\phi(pq)/\text{lcm}(d_1,d_2)}.
\]

**Proof.** Using the formula in Lemma 3.3.1, we obtain

\[
Z_{pq}(x_1, \ldots, x_{pq}) = \frac{1}{\phi(pq)} \sum_{a \in U_{pq}} \prod_{d \in \{1, p, q, pq\}} x_1^{\phi(d)/\text{ord}_{a}}.
\]

35
For any $a \in U_{pq}$, if $\text{ord}_p a = \alpha_1$ and $\text{ord}_q a = \alpha_2$, then $\text{ord}_{pq} a = \text{lcm}(\alpha_1, \alpha_2)$.

Since $p, q$ are odd primes, $U_p$ and $U_q$ are cyclic, which implies there are $\phi(\alpha_1), \phi(\alpha_2)$ elements in $\mathbb{Z}_p, \mathbb{Z}_q$ with orders $\alpha_1, \alpha_2$, respectively. Then by the Chinese Remainder Theorem, these elements correspond to $\phi(\alpha_1) \phi(\alpha_2)$ unique elements of order $\text{lcm}(\alpha_1, \alpha_2)$ in $\mathbb{Z}_{pq}$.

**Corollary 5.0.4.** Let $p, q$ be odd primes. The coefficient of $y^2$ in the cycle index polynomial $Z_{pq}(1 + y, \ldots, 1 + y^{pq})$ is

$$\frac{1}{\phi(pq)} \left( \left( \phi(p) + \phi(q) + \phi(pq) + 1 \right) + \left( \sum_{d|\phi(q)} \phi(d) \right) - 1 \right) \left( \frac{p}{2} \right)$$

$$+ \left( \sum_{d|\phi(p)} \phi(d) \right) - 1 \left( \frac{q}{2} \right) + \phi(p) + \phi(q) + \frac{3\phi(pq)}{2}$$

$$+ \left( \sum_{d|\phi(q)} \phi(d) \right) - 2 \frac{\phi(p)}{2} + \left( \sum_{d|\phi(p)} \phi(d) \right) - 2 \frac{\phi(q)}{2}$$

**Proof.** In order to determine the coefficient of $y^2$ in the cycle index polynomial $Z_{pq}$, we should find all terms with factors of $x_1$ and $x_2$. This occurs when $d_1$ or $d_2$ in Corollary 3 are equal to 1 or 2. When $d_1 = d_2 = 1$, the term in $Z_{pq}$ is $\frac{1}{\phi(pq)} x_1^{\phi(p)} x_1^{\phi(q)} = \frac{1}{\phi(pq)} x_1^{1+\phi(p)+\phi(q)+\phi(pq)}$. When $1 + y$ is substituted for $x_1$, this contributes $\frac{1}{\phi(pq)} \left( \frac{1}{2} (1+\phi(p)+\phi(q)+\phi(pq)) \right)$ to the coefficient of $y^2$.

When $d_1 = 1, d_2 > 1$, the resulting terms are:

$$\frac{1}{\phi(pq)} x_1 \sum_{d_2>1} d_2 | \phi(q) \phi(d_2) x_1^{\phi(p)/d_2} x_1^{\phi(q)/d_2} x_1^{\phi(pq)/d_2} = \frac{1}{\phi(pq)} \sum_{d_2>1} d_2 | \phi(q) \phi(d_2) x_1 x_2^{\phi(q)/d_2} x_2^{\phi(pq)/d_2}.$$
Substituting $1 + y^i$ for $x_i$, the contributing part of the coefficient of $y^2$,
is\[
\frac{1}{\phi(pq)} \sum_{d_2 \geq 1} d_2 \phi(q) \left( \frac{d}{2} \right) = \left( \sum_{d_1 \phi(q)} \phi(d) \right) - 1 \left( \frac{d}{2} \right).
\]
Similarly when $d_1 > 1, d_2 = 1$, the contributing part of the coefficient of $y^2$
is\[
\frac{1}{\phi(pq)} \left( \sum_{d_1 \phi(q)} \phi(d) \right) - 1 \left( \frac{d}{2} \right).
\]
When $d_1 = d_2 = 2$, the term is \[
\frac{1}{\phi(pq)} x_1 \phi(2) \phi(2) x_2 \phi(2)/2 x_2 \phi(2)/2 \phi(pq)/2
\]
which contributes \[
\frac{1}{\phi(pq)} \left( \frac{\phi(2) + \phi(2)}{2} \right) = \frac{\phi(p) + \phi(q) + \phi(pq)}{2},
\]
when $1 + y^i$ is substituted for $x_i$. When $d_1 = 2, d_2 \neq 2$, the terms of the polynomial are\[
\frac{1}{\phi(pq)} x_1 \sum_{d_2 \neq 2} d_2 \phi(q) \phi(2) \phi(d_2) x_2 \phi(d_2)/2 x_2 \phi(d_2)/2 x_{\text{lcm}(2,d_2)}
\]
which splits into two parts. When $d_1 = 1$, the term is \[
\frac{1}{\phi(pq)} x_1 x_2 \phi(2)/2 x_1 \phi(q)/2 x_2 \phi(pq)/2.
\]
Since we have already counted the coefficient coming from the $x_1$ part, substituting $1 + y^2$ for $x_2$, the term contributes \[
\frac{1}{\phi(pq)} \frac{\phi(p) + \phi(pq)}{2}
\]
to the coefficient of $y^2$. The contributing part from the rest of the terms where $d_2 > 2$ is\[
\frac{1}{\phi(pq)} \left( \sum_{d_1 \phi(q)} \phi(d) \right) - 2 \frac{\phi(p)}{2}.
\]
Similarly, when $d_1 \neq 2, d_2 = 2$, the contributing part of the coefficient of $y^2$
is\[
\frac{1}{\phi(pq)} \left( \frac{\phi(p) + \phi(pq)}{2} \right) + \left( \sum_{d_1 \phi(q)} \phi(d) \right) - 2 \frac{\phi(q)}{2}.
\]

Theorem 5.0.5. The coefficient of $y^2$ in the cycle index polynomial $Z_{2^n}(1 + y, \ldots, 1 + y^{2^n})$ is $3 \cdot 2^{n-1} + n - 4$, where $n \geq 3$.

Proof. By Lemma 3.3.1, the cycle index polynomial for $U_{2^n}$ acting on $Z_{2^n}$ is\[
Z_{2^n}(x_1, x_2, \ldots, x_{2^n}) = \frac{1}{2^{n-1}} \sum_{a \in U_{2^n}} \prod_{i=0}^{n} x_{\text{ord}_{2^i} a}^{2^i/\text{ord}_{2^i} a}
\]
\[
= \frac{1}{2^{n-1}} \sum_{a \in U_{2^n}} x_1^2 \prod_{i=2}^{n} x_{\text{ord}_{2^i} a}^{2^i-1/\text{ord}_{2^i} a}
\]

37
In order to find the coefficient of $y^2$ in $Z(1 + y, 1 + y^2, \ldots, 1 + y^{2^n})$, we first need to find the coefficients of $x_1$ and $x_2$ in the cycle index polynomial.

From the form of the cycle index polynomial, it suffices to find when a given $a \in U_{2^n}$ has order 1 or 2 mod $2^i$, for all $2 \leq i \leq n$.

Let $a \in U_{2^n}$, then $a = 2b - 1$ for some $b \in 1, 2, \ldots, 2^{n-1}$. Clearly $ord_{2i}a = 1$ when $a \equiv 1 \mod 2^i$, or equivalently, when $b \equiv 1 \mod 2^{i-1}$.

Now let’s examine the conditions under which $ord_{2i}a = 2$. This occurs when

\[
\begin{align*}
a^2 &\equiv 1 \mod 2^i \\
(2b - 1)^2 &\equiv 1 \mod 2^i \\
4b^2 - 4b + 1 &\equiv 1 \mod 2^i \\
4(b^2 - b) &\equiv 0 \mod 2^i \\
b(b - 1) &\equiv 0 \mod 2^{i-2}
\end{align*}
\]

Thus, if $ord_{2i}a = 2$, then $b \equiv 0 \mod 2^{i-2}$ or $b \equiv 1 \mod 2^{i-2}$. If $b \equiv 0 \mod 2^{i-2}$, and $b \not\equiv 0 \mod 2^k$, for $k > i - 2$, then $ord_{2j}a = 2$ for $i \geq 2$. If $b \equiv 1 \mod 2^{i-2}$ and $b \not\equiv 1 \mod 2^k$, for $k > i - 2$, then $ord_{2j}a = 2$ when $j = i$ and $ord_{2j}a = 1$ when $j < i$.

We now have conditions on when $ord_{2i}a = 1$ or 2, for each $i$. If $b \equiv 0 \mod 2^i$, and $b \not\equiv 0 \mod 2^j$, where $j > i$, then $b = 2^i x$, where $x \in U_{2^{n-i-1}}$, and therefore there are $2^n - i - 2$ such $b$. Similarly, if $b \equiv 1 \mod 2^i$, and $b \not\equiv 1 \mod 2^j$, where $j > i$, then $b = 2^i x + 1$, where $x \in U_{2^{n-i-1}}$, and therefore there are $2^n - i - 2$ such $b$.  

38
So now we know the order of each \( a \in U_{2n} \), and the number of units which share order 1 or 2 under the same moduli. Let us break apart the computation of the coefficients of \( y^2 \) into four cases.

Case 1: \( a = 1 \). Then the contributing terms for the coefficient of \( x_1 \) and \( x_2 \) are:

\[
\frac{1}{2^{n-1}} x_1^2 \prod_{i=1}^{n} x_1^{2^{i-1}} = \frac{1}{2^{n-1}} x_1^2 \sum_{i=2}^{n} 2^{i-1} x_1^{2^{i-1}} = \frac{1}{2^{n-1}} x_1^2 \sum_{i=0}^{n-2} 2^{i+1} x_1^{2^{i+1}} = \frac{1}{2^{n-1}} x_1^2 2^{(n-1)-1} = \frac{1}{2^{n-1}} x_1^2 x_1^{2^{n-2}} = \frac{1}{2^{n-1}} x_1^2.
\]

Thus this term then contributes \( \frac{1}{2^{n-1}} \left( \begin{array}{c} n \\ 2 \end{array} \right) \) to the coefficient of \( y^2 \).

Case 2: \( b = 2^k x, 1 \leq k \leq n - 2 \). Then the contributing terms for the coefficient of \( x_1 \) and \( x_2 \) are:

\[
\frac{1}{2^{n-1}} \sum_{k=1}^{n-2} 2^{n-k-2} x_1^2 \prod_{i=2}^{k+2} x_2^{2^{i-1}/2} = \frac{1}{2^{n-1}} \sum_{k=1}^{n-2} 2^{n-k-2} x_1^2 \sum_{i=2}^{k+2} 2^{i-2} x_2^{2^{i-2}} = \frac{1}{2^{n-1}} \sum_{k=1}^{n-2} 2^{n-k-2} x_1^2 \sum_{i=0}^{k} 2^i x_2^{2^i} = \frac{1}{2^{n-1}} \sum_{k=1}^{n-2} 2^{n-k-2} x_1^2 x_2^{k+1} - 1
\]
Thus these terms contribute the following to $y^2$:

$$\frac{1}{2^{n-1}} \sum_{k=1}^{n-2} 2^{n-k-2} \left( \binom{2}{k} + \binom{2k+1}{1} \right)$$

$$= \frac{1}{2^{n-1}} \sum_{k=1}^{n-2} 2^{n-k-2} \left( 1 + 2^{k+1} - 1 \right)$$

$$= \frac{1}{2^{n-1}} \sum_{k=1}^{n-2} 2^{n-1}$$

$$= \frac{1}{2^{n-1}} (n - 2) 2^{n-1}$$

$$= n - 2$$

Case 3: $b = 2^k x + 1, 1 \leq k \leq n - 2$. Then the contributing terms for the coefficient of $x_1$ and $x_2$ are:

$$\frac{1}{2^{n-1}} \sum_{k=1}^{n-2} 2^{n-k-2} x_1 \prod_{i=0}^{k-1} x_1^{2i} x_2^{2^{i-1} + 1}$$

$$= \frac{1}{2^{n-1}} \sum_{k=1}^{n-2} 2^{n-k-2} x_1 x_2^{2^k - 1}$$

$$= \frac{1}{2^{n-1}} \sum_{k=1}^{n-2} 2^{n-k-2} x_1^{2k+1} x_2^k$$

$$= \frac{1}{2^{n-1}} \sum_{k=1}^{n-2} 2^{n-k-2} x_1^{2k+1} x_2^k$$

Thus these terms contribute the following to $y^2$:

$$\frac{1}{2^{n-1}} \sum_{k=1}^{n-2} 2^{n-k-2} \left( \binom{2k+1}{2} + \binom{2^k}{1} \right)$$
\[
= \frac{1}{2n-1} \sum_{k=1}^{n-2} 2^{n-k-2}(2^k(2^{k+1} - 1) + 2^k)
= \frac{1}{2n-1} \sum_{k=1}^{n-2} 2^{n-k-2}2^{2k+1}
= \frac{1}{2n-1} \sum_{k=1}^{n-2} 2^{n+k+1}
= \frac{1}{2n-1} 2^n(2^{n-2} - 1)
= 2(2^{n-2} - 1)
\]

Case 4: \(a = 2^n - 1, (b = 2^{n-1})\). Then the contributing term for the coefficient of \(x_1\) and \(x_2\) are:

\[
\frac{1}{2n-1} x_1^2 \prod_{i=2}^{n} x_2^{2^{i-1/2}} = \frac{1}{2n-1} x_1^2 \sum_{i=2}^{n} 2^{i-2}
= \frac{1}{2n-1} x_1^2 2^{n-1}-1
\]

Thus the terms which contribute to \(y^2\) are \(\frac{1}{2^{n-1}} \left( \binom{2}{2} + \binom{2^{n-1}-1}{1} \right) = \frac{1}{2^{n-1}} 2^{n-1} = 1\).

So in total the coefficient of \(y^2\) is \(2^n - 1 + n - 2 + 2(2^{n-2} - 1) + 1 = 3 \cdot 2^{n-1} + n - 4\).

Table 6 gives the number of equivalence classes of mf2 functions in \(2n\) variables, for all \(3 \leq n \leq 25\). This was computed by a program written in Python.
Chapter VI

Future Work

i  Number of equivalence classes for $mf_2$ functions

In this thesis we compute the number of equivalence classes of $mf_2$ functions by separating the $\chi$ pairs into the number self-mate equivalence classes, and the number of equivalence classes obtained from Definition 3.1.1, which we call $s_n$ and $b_n$, respectively, as in Theorem 3.2.1. General formulas have only been found for $s_n$, and a general theory for $b_n$ has yet to be developed. It is possible that the use of representation theory could be applied to find a general formula.

ii  Application of the theory to $mf_1$ functions

This thesis does not address the equivalence classes of $mf_1$ functions, as it is shown in [6] that there is a correspondence between the $mf_1$ functions in $2n$ variables and the cubic MRS functions in $n$ variables. In particular,
it is shown that the number of mf1 equivalence classes in $2n$ variables is equal to the number of cubic MRS functions in $n$ variables. Although this has already been established, one should be able to apply the Pólya theory to find a proof of the number of equivalence classes for the mf1 functions. Applying this method might give some insight on a general theory for the number of equivalence classes for $k$-MRS functions.

iii Weights of mf2 functions

The weight of a Boolean function $f$ is the number of ones in the truth table of $f$. This thesis was mainly concerned with developing the theory of equivalence classes of mf2 functions, but as weight is an affine invariant, it is a natural next step to determine the weight of mf2 functions. This question has been investigated for MRS functions of varying degrees, as can be found in [9], [13], and even for the mf1 functions in [6]. As the equivalence of mf2 functions depends heavily on the equivalence of the quadratic MRS functions, it is possible that the weight of mf2 functions depends on the weights of these reduced functions as well.
Bibliography


Appendix

Table 1: Equivalence classes of mf2 2-MRS functions in $2n = 6$ variables

<table>
<thead>
<tr>
<th>Class</th>
<th>Size</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 1</td>
<td>3</td>
<td>[1, 2, 3, 4] [1, 2, 3, 6] [1, 2, 4, 5]</td>
</tr>
</tbody>
</table>

Table 2: Equivalence classes of mf2 2-MRS functions in $2n = 8$ variables

<table>
<thead>
<tr>
<th>Class</th>
<th>Size</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 1</td>
<td>4</td>
<td>[1, 2, 3, 4] [1, 2, 3, 8] [1, 2, 4, 7] [1, 3, 6, 8]</td>
</tr>
<tr>
<td>Class 2</td>
<td>4</td>
<td>[1, 2, 3, 6] [1, 2, 4, 5] [1, 2, 5, 8] [1, 2, 6, 7]</td>
</tr>
<tr>
<td>Class 3</td>
<td>2</td>
<td>[1, 2, 5, 6] [1, 4, 5, 8]</td>
</tr>
</tbody>
</table>

Table 3: Equivalence classes of mf2 2-MRS functions in $2n = 10$ variables

<table>
<thead>
<tr>
<th>Class</th>
<th>Size</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 1</td>
<td>10</td>
<td>[1, 2, 3, 4] [1, 2, 3, 10] [1, 2, 4, 9] [1, 2, 5, 6] [1, 2, 5, 8]  [1, 2, 6, 7] [1, 3, 6, 8] [1, 4, 5, 8] [1, 4, 5, 10]</td>
</tr>
<tr>
<td>Class 2</td>
<td>10</td>
<td>[1, 2, 3, 6] [1, 2, 3, 8] [1, 2, 4, 5] [1, 2, 4, 7] [1, 2, 5, 10] [1, 2, 6, 9] [1, 2, 7, 10] [1, 2, 8, 9] [1, 3, 6, 10] [1, 4, 6, 7]</td>
</tr>
</tbody>
</table>
### Table 4: Equivalence classes of mf2 2-MRS functions in $2n = 12$ variables

<table>
<thead>
<tr>
<th>Class</th>
<th>Size</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 1</td>
<td>6</td>
<td>[1, 2, 3, 4], [1, 2, 3, 10, 12], [1, 2, 10, 11]</td>
</tr>
<tr>
<td>Class 2</td>
<td>12</td>
<td>[1, 2, 3, 6], [1, 2, 3, 10, 12], [1, 2, 10, 11]</td>
</tr>
<tr>
<td>Class 3</td>
<td>6</td>
<td>[1, 2, 3, 8], [1, 2, 4, 7], [1, 2, 7, 12]</td>
</tr>
<tr>
<td>Class 4</td>
<td>6</td>
<td>[1, 2, 5, 6], [1, 2, 5, 14], [1, 2, 6, 7]</td>
</tr>
<tr>
<td>Class 5</td>
<td>6</td>
<td>[1, 2, 5, 8], [1, 2, 6, 7], [1, 2, 7, 12]</td>
</tr>
<tr>
<td>Class 6</td>
<td>3</td>
<td>[1, 2, 7, 8], [1, 4, 7, 10]</td>
</tr>
</tbody>
</table>

### Table 5: Equivalence classes of mf2 2-MRS functions in $2n = 14$ variables

<table>
<thead>
<tr>
<th>Class</th>
<th>Size</th>
<th>Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 1</td>
<td>21</td>
<td>[1, 2, 3, 4], [1, 2, 6, 11], [1, 2, 3, 14]</td>
</tr>
<tr>
<td>Class 2</td>
<td>42</td>
<td>[1, 2, 3, 6], [1, 2, 4, 7], [1, 2, 5, 14]</td>
</tr>
<tr>
<td>Class 3</td>
<td>6</td>
<td>[1, 2, 3, 8], [1, 2, 4, 7], [1, 2, 6, 11]</td>
</tr>
<tr>
<td>Class 4</td>
<td>6</td>
<td>[1, 2, 5, 6], [1, 2, 5, 14], [1, 2, 6, 7]</td>
</tr>
<tr>
<td>Class 5</td>
<td>6</td>
<td>[1, 2, 5, 8], [1, 2, 6, 7], [1, 2, 7, 12]</td>
</tr>
<tr>
<td>Class 6</td>
<td>3</td>
<td>[1, 2, 7, 8], [1, 4, 7, 10]</td>
</tr>
</tbody>
</table>
Table 6: Number of mf2 2-MRS equivalence classes in $2n$ variables

<table>
<thead>
<tr>
<th>Degree$(2n)$</th>
<th>Number of classes</th>
<th>$s_n$</th>
<th>$b_n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>8</td>
<td>3</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>12</td>
<td>6</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>14</td>
<td>2</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>16</td>
<td>7</td>
<td>3</td>
<td>11</td>
</tr>
<tr>
<td>18</td>
<td>4</td>
<td>0</td>
<td>8</td>
</tr>
<tr>
<td>20</td>
<td>9</td>
<td>5</td>
<td>13</td>
</tr>
<tr>
<td>22</td>
<td>3</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>24</td>
<td>16</td>
<td>7</td>
<td>25</td>
</tr>
<tr>
<td>26</td>
<td>4</td>
<td>1</td>
<td>7</td>
</tr>
<tr>
<td>28</td>
<td>10</td>
<td>3</td>
<td>17</td>
</tr>
<tr>
<td>30</td>
<td>10</td>
<td>2</td>
<td>18</td>
</tr>
<tr>
<td>32</td>
<td>14</td>
<td>4</td>
<td>24</td>
</tr>
<tr>
<td>34</td>
<td>5</td>
<td>1</td>
<td>9</td>
</tr>
<tr>
<td>36</td>
<td>19</td>
<td>5</td>
<td>33</td>
</tr>
<tr>
<td>38</td>
<td>5</td>
<td>0</td>
<td>10</td>
</tr>
<tr>
<td>40</td>
<td>22</td>
<td>9</td>
<td>35</td>
</tr>
<tr>
<td>42</td>
<td>12</td>
<td>1</td>
<td>23</td>
</tr>
<tr>
<td>44</td>
<td>14</td>
<td>3</td>
<td>25</td>
</tr>
<tr>
<td>46</td>
<td>6</td>
<td>0</td>
<td>12</td>
</tr>
<tr>
<td>48</td>
<td>35</td>
<td>11</td>
<td>59</td>
</tr>
<tr>
<td>50</td>
<td>10</td>
<td>2</td>
<td>18</td>
</tr>
</tbody>
</table>