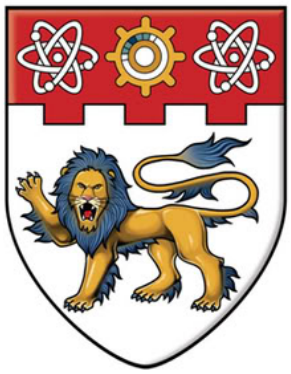

NANYANG TECHNOLOGICAL UNIVERSITY

Algebraic Constructions of Permutation Codes

Yeung Kar Wing

Supervisor: Prof Xing Chaoping

Division of Mathematical Sciences

School of Physical and Mathematical Sciences

Nanyang Technological University

4 May 2018

This Final Year Project (FYP) thesis is submitted as part of the honors requirements

Abstract

Permutation codes have received increased interest in recent years, largely due to its applications in powerline communications and flash memories. Finding good constructions of codes is one of the motivations of coding theory. In this thesis, we will look at constructions of permutation codes, in particular algebraic constructions. We will review some elementary and well-known results in the field, and cover some existing constructions as well as explore new ways of constructing permutation codes. Existing techniques mentioned in this thesis include mutually orthogonal latin squares as well as the affine and projective semilinear group. In addition, the ring of integers modulo n as well as the affine and projective general linear group were also used to provide new constructions of permutation codes.

Acknowledgement

I would like to thank my supervisor, Prof Xing Chaoping for his guidance, which without this thesis would not have been possible.

I would also like to thank my batch mates for offering their support and help when help was needed.

Contents

Chapter 1

Introduction

Permutation codes have received increased interest in recent years, largely due to its applications. One prominent use of permutation codes is in powerline communications, where the goal is to have the power output remain constant. This can be achieved by having the frequencies correspond to symbols, and by using permutation codes on those symbols, the power remains constant regardless of any codeword that is transmitted [5]. This avoids the problem of having large fluctuations in voltage that would occur with classical binary codes.

Another significant application of permutation codes can also be found in rank modulation, which is a data representation scheme used in non-volatile storage devices such as flash memories [11], [10]. In this scheme, memory cells are given ranks according to their charge levels. The ranking of the cells can be changed by increasing the charge of the cells whose rank we want to increase. As single-cell erase operations are expensive, this rank modulation scheme improves data reliability and writing speed [8].

In this thesis, we will start by stating some definitions from groups and fields as well as coding theory, then some elementary results regarding permutation codes, followed by a review of some interesting constructions that have been published, and lastly we will share some of the constructions we have explored.

1.1 Groups and fields

As we will be exploring mostly algebraic constructions in this thesis, we would like to provide the relevant definitions for the sake of completeness. In particular, we will see the affine and projective semilinear groups in Section 2.2, and the affine and projective general linear groups in Section 3.2.

Definition 1.1.1. The **general linear group** of degree n over a field F is the group of $n \times n$ invertible matrices with entries from F and matrix multiplication as the group operation. We denote it as $GL_n(F)$.

In this thesis we will only consider the field $\mathbb{F}_q$ where q is a prime power, although in general the above definition applies to any field, such as $\mathbb{R}$ or $\mathbb{C}$.

Definition 1.1.2. Let $q = p^k$, where p is prime. The **affine general linear group** of degree n over $\mathbb{F}_q$ is the group of affine linear transformations, which are maps $\gamma_{A,b} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that $\gamma_{A,b}(u) = Au + b$, for $A \in GL_n(\mathbb{F}_q), b \in \mathbb{F}_q^n$. We denote it as $AGL_n(\mathbb{F}_q)$.

The above definition follows the one in Galois Theory by David Cox [4]. However, the affine general linear group can also be defined as the semidirect product $\mathbb{F}_q^n \rtimes GL_n(\mathbb{F}_q)$, with composition as the group operation and $(C, d) \circ (A, b) = (CA, Cb+d)$. It is easy to check that this is indeed a semidirect product, as

(i) $\mathbb{F}_q^n \simeq \{\gamma_{I_n,b} \mid b \in \mathbb{F}_q^n\}$ is normal in $AGL_n(\mathbb{F}_q)$; and

(ii) $GL_n(\mathbb{F}_q) \simeq \{\gamma_{A,0} \mid A \in GL_n(\mathbb{F}_q)\}$ is a subgroup of $AGL_n(\mathbb{F}_q)$.

Alternatively, we can also think of it as a group action, where $AGL_n(\mathbb{F}_q)$ acts on the set $\mathbb{F}_q^n$. Again, one can also verify that this is indeed a "legal" group action by checking that it satisfies the conditions of a group action.

Definition 1.1.3. Let $q = p^k$, where p is prime. The **projective general linear group** of degree n over $\mathbb{F}_q$ is defined to be the quotient of the general linear group by its center, the scalar matrices. In other words, $PGL_n(\mathbb{F}_q) = GL_n(\mathbb{F}_q)/Z(GL_n(\mathbb{F}_q))$, where $Z(GL_n(\mathbb{F}_q)) = \{\lambda I_n \mid \lambda \in \mathbb{F}_q^*\}$.

While the affine general linear group acts on $\mathbb{F}_q^n$, the projective general linear group acts on the projective space $\mathbb{P}_q^{n-1}$. A definition for the projective space is given below.

Definition 1.1.4. Let $q = p^k$, where p is prime. The **projective space** of dimension $n-1$ over $\mathbb{F}_q$ is defined as $\mathbb{P}_q^{n-1} = (\mathbb{F}_q^n \setminus \{0\})/\sim$, where $\sim$ is defined by $(x_0, \cdots, x_{n-1}) \sim (y_0, \cdots, y_{n-1})$ if there exists $\lambda \in \mathbb{F}_q^*$ such that $(x_0, \cdots, x_{n-1}) = \lambda(y_0, \cdots, y_{n-1})$.

In other words, we can view the projective space of dimension $n-1$ as the set of n-dimensional lines through the origin.

Hence, we can define the action of $PGL_n(\mathbb{F}_q)$ on $\mathbb{P}_q^{n-1}$ to be

$$A : \mathbb{P}_q^{n-1} \to \mathbb{P}_q^{n-1}$$
$$u \mapsto Au$$

where $A \in PGL_n(\mathbb{F}_q)$.

We next define the Frobenius automorphism and the Galois group, which are "pre-requisites" for the affine general semilinear group and projective semilinear group.

Definition 1.1.5. Let F be a field with characteristic p. The **Frobenius automorphism** on F is the map $\phi : F \to F$ such that x is mapped to x^p for all $x \in F$.

Remark. Note that in the case of infinite fields, we have the Frobenius endomorphism instead, as the map is a homomorphism instead of an isomorphism.

Definition 1.1.6. Let $q = p^k$, where p is prime. The **Galois group of** $\mathbb{F}_q/\mathbb{F}_p$ is a cyclic group of order k generated by the Frobenius automorphism $\phi(x) = x^p$, and it is denoted by $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

In general, if $F \subset L$ is a finite extension, $\mathrm{Gal}(L/F) = \{\sigma : L \to L \mid \sigma \text{ is an automorphism and } \sigma(a) = a \ \forall a \in F\}$. In the particular case where the field is $\mathbb{F}_q/\mathbb{F}_p$, it turns out that $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p) = \langle\phi\rangle$, where ϕ is the Frobenius automorphism.

Definition 1.1.7. Let $q = p^k$, where p is prime. The **affine semilinear group** of degree n over $\mathbb{F}_q$ is the group of affine semilinear transformations, which are maps

$\gamma_{A,\sigma,b} : \mathbb{F}_q^n \to \mathbb{F}_q^n$ such that $\gamma_{A,\sigma,b}(u) = A\sigma(u) + b$, for $A \in GL_n(\mathbb{F}_q), \sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ and $b \in \mathbb{F}_q^n$. We denote this group as $A\Gamma L_n(\mathbb{F}_q)$.

In particular, we will be using $A\Gamma L_1(\mathbb{F}_q)$ for the construction in Section 2.2, and that is the set

$$A\Gamma L_1(\mathbb{F}_q) = \{ax^{p^i} + b \mid a, b \in \mathbb{F}_q, a \neq 0, 0 \leq i < n\}$$

Definition 1.1.8. Let $q = p^k$, where p is prime. The **projective semilinear group** of degree n over $\mathbb{F}_q$ is defined to be the semidirect product of the projective general linear group by the Galois group. In other words, $P\Gamma L_n(\mathbb{F}_q) = PGL_n(\mathbb{F}_q) \rtimes \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

Here, we have the natural action of $P\Gamma L_n(\mathbb{F}_q)$ on $\mathbb{P}_q^{n-1}$ to be

$$\begin{aligned}(A, \sigma) : \mathbb{P}_q^{n-1} &\to \mathbb{P}_q^{n-1} \\ u &\mapsto A\sigma(u)\end{aligned}$$

where $A \in P\Gamma L_n(\mathbb{F}_q), \sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$.

In particular, we will be using $P\Gamma L_2(\mathbb{F}_q)$ for the construction in Section 2.2. We will use a different (but equivalent) definition for the special case where the projective semilinear group has degree 2, and it is

$$P\Gamma L_2(\mathbb{F}_q) = \left\{ \frac{ax^{p^i} + b}{cx^{p^i} + d} \;\middle|\; a, b, c, d \in \mathbb{F}_q, ad \neq bc, 0 \leq i < n \right\}$$

.

This acts on the projective space of dimension 1, $\mathbb{P}_q^1$. However, instead of thinking it as "equivalent classes in $\mathbb{F}_q^2 - \{0\}$" as we have previously defined, to be consistent with the above definition of $P\Gamma L_2(\mathbb{F}_q)$, we can think of it as "the affine space $\mathbb{F}_q$ with its points at infinity". This is the set $\mathbb{F}_q \cup \{\infty\}$.

1.2 Coding theory

In this section, we will give a brief overview of classical binary codes, and then provide the background necessary for permutation codes.

The motivation behind coding theory is that errors arise when we transmit data over a noisy or unreliable channel. This means that we cannot transmit data "as

it is", as it is likely to be corrupted in some way at the receiving end. We would need to have a way to encode our data before sending, so that the receiver is able to detect the errors, and if possible, decode them correctly.

We first formalize the definition and some properties of the more commonly-known binary codes.

Definition 1.2.1. A **binary code** C of **length** n is a subset of $\{0,1\}^n$, and every element in C is called a **codeword**. We say that the code C has **(Hamming) distance** d if every two codewords in C differ in at least d positions, and we write the distance between two codewords as $d_H(x,y)$.

Definition 1.2.2. We say that C is l**-error-detecting** if for every codeword $c \in C$ and every $x \in \{0,1\}^n$, the statement "if $d_H(x,c) \leq l$, then $l \notin C$" holds.

Definition 1.2.3. We say that C is l**-error-correcting** if for every codeword $c \in C$ and every $x \in \{0,1\}^n$, the statement "if $d_H(x,c) \leq l$, then we decode x to c" holds.

We apply the nearest neighbour rule when we say "we decode x to c", which is decoding from a given x to some $c \in C$ such that $d_H(x,c)$ is minimized.

Example 1.2.4. $C = \{000, 011, 110, 101\}$ is 1-error-detecting, and the distance is 2. However, C is not 1-error-correcting as 111 can be decoded to 011, 110 or 101.

From this, we can see that theoretically, we can simply append any number of "error-checking" digits to the message we wish to transmit until we reach a desired error-detecting or error-correcting capability. However, it should not be difficult to see that this design is not efficient as we introduce a lot of redundancy in our pursuit of error-correction. It turns out that this is one of the main problems of coding theory, and they are:

(i) determining the maximum size of the code given the distance and the length,

(ii) constructing codes with maximum error-correction and small redundancy, and

(iii) constructing codes with efficient encoding and decoding algorithms.

Algebraic constructions of binary (and in general, q-ary) codes are well-studied, and algebraic techniques are used not only in constructions of codes, but decoding algorithms as well [16]. Similar to binary codes, we can also apply algebraic techniques to permutation codes as well.

We first provide a definition for permutation codes.

Definition 1.2.5. A **permutation code** C is a subset of S_n, and each element in C is called a **codeword**. The **length** of each codeword is n. If for every two codewords $u, v \in C$, the distance between u and v is at least d, we say that d is the **distance** of C. The **size** of the code C is usually denoted as M, and it is common to write the code C as a (n, M, d)-code.

Definition 1.2.6. Given the parameters n and d, we denote the **maximum size** of such a code as $M(n, d)$.

Much like binary codes, we are interested in investigating the distance of permutation codes. Recent studies on permutation codes have explored different metrics, such as the Chebyshev, Kendall tau, Cayley and Ulam metric due to their applications in flash memories [13], [2]. However in this thesis, we will focus on the Hamming metric, and so whenever distance is mentioned, the Hamming distance should be assumed. Although widely known, we provide a definition for the sake of completeness.

Definition 1.2.7. The **Hamming distance** between two codewords $\sigma, \tau \in S_n$ is defined as $d_H(\sigma, \tau) = |\{i \in \{1, \ldots, n\} : \sigma(i) \neq \tau(i)\}|$.

Remark. We have $d_H(\sigma, \tau) = d_H(e, \sigma\tau^{-1})$. This is clear as $\sigma(i) = \tau(i)$ if and only if $\sigma\tau^{-1}(i) = i$.

Remark. We also have $d_H(\sigma, \tau) = d_H(\gamma\sigma, \gamma\tau)$, for $\gamma \in S_n$.

Example 1.2.8. $C = \{(), (123), (132)\} \subset S_n$ is a $(3, 3, 3)$-code. We look at the image of the elements of C, and they are $\{123, 231, 312\}$. We can easily see that the distance is 3 as any two codewords do not collide in any position.

Permutation codes may sometimes be represented as an array as well. In particular, we will use the permutation array for the construction via mutually orthogonal latin squares in Section 2.1. A definition for permutation arrays is given below.

Definition 1.2.9. Let C be an (n, M, d)-code. Then a **permutation array** of size $M \times n$ is an array whose rows are the image of σ on $(1, 2, \ldots, n)$, for all σ in C. We denote the permutation array as $PA(n, d)$, and we say that it has size M.

Example 1.2.10. The Klein-4 subgroup $G = \{(), (12)(34), (13)(24), (14)(23)\}$ of S_4 is a $(4, 4, 4)$-code. The permutation array for this code is

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \\ 3 & 4 & 1 & 2 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

and we call it a $PA(4, 4)$ of size 4.

As previously mentioned, one main problem in coding theory is to find the maximum $M(n, d)$, given n and d as parameters, and this naturally applies to permutation codes as well. By finding constructions of permutation codes, we not only are able to explicitly construct codes with the given n, M and d parameters, the existence of these codes also serve as a lower bound for $M(n, d)$ as well. Lower and upper bounds are also important in coding theory, and we will explore some of them in the next section.

1.3 Elementary results

We now introduce some elementary results regarding permutation codes, which can also be found in [9] and [5].

Proposition 1.3.1. *Let $M(n, d)$ be the maximum size of a permutation code with length n and Hamming distance d. Then the following statements are true:*

(i) $M(n, 2) = n!$

(ii) $M(n, 3) = \frac{n!}{2}$

(iii) $M(n, n) = n$

(iv) $M(n, d) \geq M(n - 1, d), M(n, d + 1)$

(v) $M(n,d) \leq nM(n-1,d)$

(vi) $M(n,d) \leq \frac{n!}{(d-1)!}$

Proof. (i) This is clear as $d_H(\sigma,\tau) \geq 2$ for all $\sigma,\tau \in S_n$.

(ii) For all $\sigma,\tau \in A_n$, $\sigma\tau^{-1}$ is even, so we must have $d_H(\sigma\tau^{-1},e) \geq 3$, which then gives us $d_H(\sigma,\tau) \geq 3$. Hence $M(n,3) \geq |A_n| = \frac{n!}{2}$. On the other hand, if there exists a $(n,3)$-code Γ such that $|\Gamma| > \frac{n!}{2}$, there exists two elements in Γ belonging to $\{\sigma,(12)\sigma\}$ for some $\sigma \in A_n$ by the pigeonhole principle, which gives us a contradiction. Therefore $M(n,3) = \frac{n!}{2}$.

(iii) C_n, the cyclic group of order n, is a (n,n)-code $\Rightarrow M(n,n) \geq n$. If there exists a (n,n)-code Γ such that $|\Gamma| > n$, then $\{\sigma_1,\ldots,\sigma_{n+1}\} \subseteq \Gamma$. If we look at the first position, 2 σ_i's must overlap which gives us a contradiction. Therefore $M(n,n) = n$.

(iv) This is clear. Take a $M(n-1,d)$ code and append a fixed symbol to each codeword. Hence this code gives a lower bound for $M(n,d)$. We can also take a $M(n,d+1)$ code and replace the last digit of each codeword with a fixed symbol. This also gives us a lower bound for $M(n,d)$.

(v) Let Γ be a (n,d)-code with size $M(n,d)$. Consider a subcode Γ_k of Γ such that the first entry of each codeword is some fixed $k \in \{1,\ldots,n\}$. We have n such Γ_k's and since $|\Gamma_k| \leq |M(n-1,d)|$, we have $M(n,d) \leq nM(n-1,d)$.

(vi) This follows from (iii) and (v):

$$M(n,d) = nM(n-1,d) = n(n-1)M(n-2,d) = \cdots = \frac{n!}{(d-1)!}$$

□

In addition to the elementary results given above, we also have the well-known Gilbert-Varshamov lower bound and the sphere-packing upper bounds, which are also mentioned in [9].

Definition 1.3.2. A **derangement of order** k is a permutation of a set of k elements such that there are no fixed points.

Definition 1.3.3. Let $D(n,k)$ denote the set of all permutations in S_n which are distance k from the identity, that is $D(n,k) = \{\sigma \in S_n \mid d_H(\sigma, e) = k\}$.

We have $|D(n.k)| = \binom{n}{k} D_k$, where

$$D_k = k! \sum_{i=0}^{k} \frac{(-1)^i}{i!}, \text{ and } D_0 = 1 \text{ by convention.}$$

Proposition 1.3.4 (GV bound)**.**

$$M(n,d) \geq \frac{n!}{V(n,d-1)} = \frac{n!}{\sum_{k=0}^{d-1} |D(n,k)|}$$

Proof. The ball in S_n of radius r with center σ is the set of all permutations of distance less than or equal to r from σ. We can see that the volume of this ball is $\sum_{k=0}^{d-1} |D(n,k)|$, and hence the result follows. □

Proposition 1.3.5 (Sphere-packing upper bound)**.**

$$M(n,d) \leq \frac{n!}{\sum_{k=0}^{\lfloor \frac{d-1}{2} \rfloor} |D(n,k)|}$$

Proof. The denominator counts the number of balls B of radius $r = \lfloor \frac{d-1}{2} \rfloor$ in S_n. If $C \subseteq S_n$ is a permutation code with size $M(n,d)$, then the balls of radius r must be disjoint, and so we have $|C| \cdot |B| \leq n!$ and the result follows. □

We also have a well-known result arising from sharply k-transitive groups. We first provide definitions for transitivity and sharp k-transitivity.

Definition 1.3.6. A permutation group $G \leq S_n$ is **transitive** if for every $x, y \in \{1, \ldots, n\}$, there exists a $\sigma \in G$ such that $\sigma(x) = y$.

In other words, if G is transitive, there will always be an element in G that will take us from x to y for any x, y in the set G acts on.

Definition 1.3.7. Let x, y be k-tuples consisting of non-repeating elements from $\{1, \ldots, n\}$, that is $x = (x_1, \ldots, x_k)$ and $y = (y_1, \ldots, y_k)$, where $x_i, y_i \in \{1, \ldots, n\}$ for all $1 \leq i \leq k$ and $x_i \neq x_j, y_i \neq y_j$ for $i \neq j$. A permutation group $G \leq S_n$ is **sharply k-transitive** if for every such x, y of size k, there exists a unique $\sigma \in G$ such that $\sigma(x) = y$.

Remark. Note that if $\sigma \in G$ is not unique, we say that G is k-transitive instead of sharply k-transitive.

Example 1.3.8. S_n is sharply n and $(n-1)$-transitive. It is clear for any $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ that there exists a $\sigma \in S_n$ such that $\sigma(x) = y$. It is also similar for S_n being sharply $(n-1)$-transitive. We have $\sigma((x_1, \ldots, x_{n-1})) = (y_1, \ldots, x_{y-1})$, which gives us $(n-1)$-transitivity, and the sharpness comes from the fact that $\sigma(x_n) = y_n$ is the unique extension of σ.

Proposition 1.3.9. *If G is a sharply k-transitive group acting on a set of size n, we then have $M(n, n-k+1) = \frac{n!}{(n-k)!}$.*

Proof. Suppose G is a sharply k-transitive group acting on a set $\Omega = \{1, \ldots, n\}$. Consider $g, h \in G$. Then by the definition of sharp k-transitivity, $g(1, \ldots, k) \neq h(1, \ldots, k)$, and so $g(1, \ldots, n)$ and $h(1, \ldots, n)$ agree in at most $k-1$ positions, or in other words, the distance is at least $n-k+1$. This gives us $M(n, n-k+1) \geq |G| = \frac{n!}{(n-k)!}$. Furthermore, from Proposition 1.3.1, we get $M(n, n-k+1) \leq \frac{n!}{(n-k)!}$. The desired result then follows. □

From sharp k-transitivity, it gives us more than just a bound for $M(n, d)$; it tells us exactly what $M(n, d)$ is. However, we do not know of many sharply k-transitive groups, and thus this result cannot be extensively applied.

Example 1.3.10. The well-known Mathieu groups, M_{11} and M_{12}, are sharply 4- and 5-transitive respectively. Hence we have $M(11, 8) = 11 \cdot 10 \cdot 9 \cdot 8$ and $M(12, 8) = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$.

In addition to the results from sharply k-transitive groups, we also have results from permutation polynomials.

Definition 1.3.11. Let q be a prime power. We say that $f \in \mathbb{F}_q[x]$ is a **permutation polynomial** if the function

$$\begin{aligned} f : \mathbb{F}_q &\to \mathbb{F}_q \\ c &\mapsto f(c) \end{aligned}$$

acts as a permutation on $\mathbb{F}_q$.

Remark. It is also equivalent to say that f is a bijection.

Let $N_d(q)$ denote the number of permutation polynomials over $\mathbb{F}_q$ of a given degree d, where $1 \leq d \leq q-2$. We then have the following result.

Proposition 1.3.12. *Let q be a prime power. Then $M(q,d) \geq \sum_{i=1}^{q-d} N_i(q)$.*

Proof. Let $f, g \in \mathbb{F}_q[x]$ with degree at most $q-d$. Then clearly $f(x) - g(x) = 0$ has at most $q-d$ solutions, as $\mathbb{F}_q$ is a field. This means that f and g agree in at most $q-d$ positions, and so $d_H(f,g) \geq d$. The result then follows. □

As one can tell, this depends on whether we know $N_d(q)$ or not. It turns out that this is not a trivial problem, and a more in-depth treatment can be found in [5].

Chapter 2

Review of known constructions

In this chapter, we will look at constructions of permutation codes that have been published. Although there is increased interest in permutation codes in recent times, not much has been done on algebraic constructions in particular. Some results do arise from nice algebraic objects and properties, such as sharply k-transitive groups and permutation polynomials, which we have shown in the previous chapter. However, these results tend to be limited by the algebraic objects themselves. For example, the number of permutation polynomials given a degree d is still an open problem [12], [15], [7], and M_{11} and M_{12} are the only sharply k-transitive groups for $k > 3$, apart from those arising from S_n and A_n.

On the other hand, other constructions of permutation codes are also available, such as those that are probabilistic or computational, like the greedy algorithm or clique search. While we do not cover those techniques here, they can be found in [5]. In this section, we will review a combinatorial approach, that is mutually orthogonal latin squares, as well as a recent algebraic approach, which is based on the groups $A\Gamma L_1(\mathbb{F}_n)$ and $P\Gamma L_2(\mathbb{F}_n)$.

2.1 Mutually orthogonal latin squares

In this section, we first provide some definitions, followed by some results leading up to the main theorem. Some theorems may be weakened, as we wish to focus solely on the construction of permutation codes, without examining any additional

properties. For a complete treatment of mutually orthogonal latin squares and permutation codes, one can refer to [3].

Definition 2.1.1. Let S be a set of n symbols. A **latin square** of order n is an $n \times n$ matrix such that each symbol of S occurs exactly once in each row and each column.

Definition 2.1.2. Let L_1 and L_2 be latin squares of the same order on the sets S_1 and S_2 respectively. Then L_1 and L_2 are said to be **orthogonal** if each tuple (i, j) where $i \in S_1$, $j \in S_2$ occurs exactly once when we overlap L_1 and L_2.

Definition 2.1.3. A collection of k $n \times n$ latin squares is said to be **mutually orthogonal** if every pair of latin squares in the collection is orthogonal, and we denote this collection as MOLS(n).

Example 2.1.4. This is a set of 2 mutually orthogonal latin squares of order 3. If we overlap these 2 latin squares, we get all possible tuples (i, j) where $i, j \in \{1, 2, 3\}$.

1	2	3
2	3	1
3	1	2

1	2	3
3	1	2
2	3	1

$\rightarrow$

(1,1)	(2,2)	(3,3)
(2,3)	(3,1)	(1,2)
(3,2)	(1,3)	(2,1)

To proceed with the proof of the main theorem, we will still need introduce a few more notations. Recall that a $PA(n, d)$ is a permutation array of size $M \times n$ where its rows are the image of σ on $(1, 2, \ldots, n)$, for all σ in C and any two rows in the $PA(n, d)$ differ in at least d positions. We can also see it as the two rows agreeing in at most $n - d$ positions, and thus we denote a $PA(n, d)$ of size M as $B(n, n - d; M)$. We will be using this notation in the main theorem of this section later.

Definition 2.1.5. A **generalised Room square packing (GRSP)** of size n and index λ defined on a set S with cardinality v is an $n \times n$ array A such that

- every cell of A contains a subset of S;
- every symbol of S occurs once in each row and each column of A; and
- any two distinct symbols of S occur together in at most λ cells of A.

We denote such a GRSP by $T(n, \lambda; v)$.

Before we can prove the main result, we will need to prove that $T(n, \lambda; v)$ and $B(n, \lambda; v)$ are "essentially" the same thing, but represented differently.

Theorem 2.1.6. *A $T(n, \lambda; v)$ exists if and only if a $B(n, \lambda; v)$ exists.*

Proof. We construct a $n \times n$ array as follows. The symbol k appears in the (i, j) cell of $T(n, \lambda; v)$ if and only if the (k, j) entry of $B(n, \lambda; v)$ is i. Suppose we have a $B(n, \lambda; v)$. We show the $\Leftarrow$ direction; it is clear the converse holds as well from the construction and the proof of $\Leftarrow$.

Note that we use $B(k, j)$ to denote the element in $B(n, \lambda; v)$ at the (k, j) cell and $T(i, j)$ for the element in $T(n, \lambda; v)$ at the (i, j) cell.

Claim. *Every element occurs exactly once in each row.*

Proof of Claim. Suppose not, that is k is in $T(i, j)$ and $T(i, t)$ for some $1 \leq k \leq v$, $1 \leq i, j, t \leq n$ and $j \neq t$. Then $B(k, j) = i$ and $B(k, t) = i$, but each row of $B(n, \lambda; v)$ is a permutation. Hence the assumption is false.

Claim. *Every element occurs exactly once in each column.*

Proof of Claim. Fix j. Consider $B(k, j) = i$ where $1 \leq k \leq v$ and $1 \leq i \leq n$. From the construction it is easy to see that each $k \in \{1, \ldots, v\}$ appears only once in each column of $T(n, \lambda; v)$.

Claim. *Any two distinct symbols occur together in at most λ cells.*

Proof of Claim. From the definition of $B(n, \lambda; v)$, we know that any two permutations agree in at most λ positions. Suppose we take two permutations, or rather two rows, k_1 and k_2, of $B(n, \lambda; v)$. Then $B(k_1, j) = B(k_2, j) = i$ for at most λ such i's. Hence k_1 and k_2 will coincide in at most λ such $T(i, j)$'s.

We have shown that the properties of $T(n, \lambda; v)$ are satisfied, given that we have a $B(n, \lambda; v)$. It is clear that the converse holds as well, and thus the proof is complete. □

Now that we have the above result, we can then prove the main theorem. The main theorem in the paper by Colbourn et al. [3] is a stronger version of what

we have included here, as it also proves that the permutation array is s-separable. We have chosen to omit s-separability in the proof below as it requires a few more pre-requisite theorems and lemmas. While that would give us more depth into the techniques of using MOLS to construct permutation codes, we did not want to trade the breadth of this thesis for depth in the construction via mutually orthogonal latin squares.

The modified result of the paper by Colbourn et al. is as follows.

Theorem 2.1.7. *If there exists s mutually orthogonal latin squares of order n, then there exists a $(n, n-1)$-code of size sn.*

Proof. Let $L_1, \ldots, L_s$ be a collection of latin squares of order n, where L_i is a latin square on the set of symbols $S_i = \{(i-1)n, \ldots, in-1\}$. We then construct an $n \times n$ square with the (i, j) cell containing the s symbols from the (i, j) cell in each of the s latin squares. Note that

- each latin square uses n symbols so the total number of symbols is sn;
- each row and each column contains each symbol exactly once since the s squares are latin; and
- each pair of elements occur at most once in a cell because the s squares are mutually orthogonal.

Hence, this is a $T(n, 1; sn)$. By Theorem 2.1.6, there exists a $B(n, 1; sn)$. This then gives us a $PA(n, n-1)$ of size sn. □

This then naturally begs the question of, given n, whether we can construct a set of MOLS of order n, and if so, what is the maximal size of this set. It turns out that if n is a prime power, then we can construct a maximal set of MOLS of size $n-1$. This is a well-known fact regarding MOLS and a proof can be found in [14]. In fact, we can even say the following.

Corollary 2.1.8. *For n prime power, $M(n, n-1) = n(n-1)$.*

Proof. Since n is a prime power, there exists a set of $n-1$ MOLS of order n. We can then apply Theorem 2.1.7 to get $M(n, n-1) \geq n(n-1)$. Furthermore, from

Proposition 1.3.1(vi), we also obtain $M(n, n-1) \leq n(n-1)$. The result then follows. □

2.2 $A\Gamma L_1(\mathbb{F}_n)$ and $P\Gamma L_2(\mathbb{F}_n)$

Although not much has been done on algebraic constructions of permutation codes in the last decades, some progress has been made recently in 2017 by Bereg et al. [1]. In this construction, the authors made use of the affine semilinear group of dimension 1, $A\Gamma L_1(\mathbb{F}_n)$, as well as the projective semilinear group of dimension 2, $P\Gamma L_2(\mathbb{F}_n)$, to construct permutation codes.

We first state the two main theorems, and then work our way towards the proof of the theorems via a series of lemmas.

Theorem 2.2.1. *There exists a $(n, kn(n-1), n-p^{k^*})$-code arising from $A\Gamma L_1(\mathbb{F}_n)$, where k^* is the largest proper factor of k, and $n = p^k$.*

Theorem 2.2.2. *There exists a $(n+1, kn(n+1)(n-1), n-p^{k^*})$-code arising from $P\Gamma L_2(\mathbb{F}_n)$, where k^* is the largest proper factor of k, and $n = p^k$.*

Before we prove the above two theorems, we will have to state some lemmas required for the proof.

From here onwards, we also define $d_H(G)$ to be $\min\{d_H(g_1, g_2) \mid g_1, g_2 \in G\}$, and $d_H(e, G)$ to be $\min\{d_H(e, g) \mid g \in G\}$.

Lemma 2.2.3. $d_H(G) = d_H(e, G\backslash\{e\})$.

Proof. For $g_1, g_2 \in G$, we have $d_H(g_1, g_2) = d_H(e, g_1^{-1}g_2)$. Clearly $g_1^{-1}g_2 \in G$ and $g_1^{-1}g_2 \neq e$ as $g_1 \neq g_2$. □

Remark. The above lemma allows us to find the Hamming distance of G in $O(|G|)$ time instead of $O(|G|^2)$ time.

Lemma 2.2.4. *Let G and H be subgroups of S_n such that $G = \cup_{0 \leq i \leq r} a_i H$, for some $r > 0$, where $a_0 = e$. Then $d_H(G) = \min\{d_H(e, H\backslash\{e\}), d_H(a_1, H), \ldots, d_H(a_r, H)\}$.*

Proof. Note that if $g \in aH$, then $g^{-1} \in Ha^{-1}$. This is because $g = ah$ for some $h \in H$, which gives us $g^{-1} = (ah)^{-1} = h^{-1}a^{-1} \in Ha^{-1}$. Hence we have

$$\begin{aligned} d_H(G) &= d_H(\cup_{0\leq i\leq r} a_i H) \\ &= min_{0\leq i\leq r}\{d_H(e, a_i H)\} \\ &= min_{0\leq i\leq r}\{d_H(e, Ha_i^{-1})\} \\ &= min\{d_H(e, H\backslash\{e\}), d_H(e, Ha_1^{-1}), \dots d_H(e, Ha_r^{-1})\} \\ &= min\{d_H(e, H\backslash\{e\}), d_H(a_1, H), \dots d_H(a_r, H)\} \end{aligned}$$

□

Lemma 2.2.5. *For distinct polynomials $f, g \in \mathbb{F}_n[x]$, we have $d_H(f, g) = n - r(f - g)$, where $r(f - g)$ denotes the number of roots of $f - g$ in $\mathbb{F}_n$.*

Proof. This is easy to see, as $f(x) = g(x)$ if and only if $f(x) - g(x) = 0$, for $f, g \in \mathbb{F}_n[x]$. Note that the number of $x \in \mathbb{F}_n$ such that $f(x) = g(x)$ is the number of positions where f and g collide. This means that the Hamming distance between f and g is $n - r(f - g)$, as the number of x such that $f(x) - g(x) = 0$ is precisely the number of roots of $f - g$. □

Lemma 2.2.6. *Let $a, b \in \mathbb{F}_n$ and $a \neq 0$. Then we have $r(x^{p^i} + ax + b) \leq r(x^{p^i} - x)$.*

Proof. Let $f_1(x) = x^{p^i} + ax + b$, $f_2(x) = x^{p^i} + ax$ and $f_3(x) = x^{p^i} - x$. To show that $r(f_1) \leq r(f_3)$, we show these two inequalities: $r(f_1) \leq r(f_2)$ and $r(f_2) \leq r(f_3)$.

$\underline{r(f_1) \leq r(f_2)}$: If f_1 has no root in $\mathbb{F}_n$, then $r(f_1) \leq r(f_2)$ is satisfied. Suppose f_1 has at least a root, and we call it y_0. Then for any root y of f_1, we have

$$\begin{aligned} f_2(y - y_0) &= (y - y_0)^{p^i} + a(y - y_0) \\ &= y^{p^i} - y_0^{p^i} + a(y - y_0) \\ &= f_1(y) - f_1(y_0) \\ &= 0 \end{aligned} \tag{1}$$

This means that $y - y_0$ is a root of f_2. Since $y \to y - y_0$ is an injection, that is every root of f_1 corresponds to a root of f_2, we have $r(f_1) \leq r(f_2)$.

Note that (1) follows from a property of the Frobenius automorphism, which is $(x+y)^p = x^p + y^p$. This is true as we have $p \mid \binom{p}{k}$ for $0 < k < p$ and so $\binom{p}{k} = 0$ in $\mathbb{F}_n$, which then gives us

$$(x+y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} = x^p + y^p$$

$\underline{r(f_2) \leq r(f_3)}$: To show $r(f_2) \leq r(f_3)$, we first show $r(g_2) \leq r(g_3)$, where

$$g_2 = \frac{f_2}{x} = x^{p^i-1} + a, \qquad g_3 = \frac{f_3}{x} = x^{p^i-1} - 1$$

Again, if g_2 has no root in $\mathbb{F}_n$, $r(g_2) \leq r(g_3)$ holds trivially. Hence we assume that g_2 has a root.

Suppose that $a = 0$. Then we have $g_2 = x^{p^i-1}$, which means that 0 is the only root of g_2, that is $g_2(0) = 0$. We also have that 1 is a root of g_3, and so $r(g_2) = 1 \leq r(g_3)$.

Suppose that $a \neq 0$. Then 0 is not a root of g_2. Since we know that there is at least a nonzero root, we let it be z. We also let z_i range over the roots of g_2, and we map $z_i \to \frac{z_i}{z}$. We then show that $\frac{z_i}{z}$ is a root of g_3:

$$\begin{aligned} g_3(\frac{z_i}{z}) &= (\frac{z_i}{z})^{p^i-1} - 1 \\ &= (\frac{z_i^{p^i-1}}{z^{p^i-1}}) - 1 \\ &= \frac{-a}{-a} - 1 \\ &= 0 \end{aligned}$$

Since the map is injective, it follows that a root of g_2 gives us a root of g_3, and thus we have $r(g_2) \leq r(g_3) \Rightarrow r(f_2) \leq r(f_3)$.

□

We are now ready to prove Theorem 2.2.1 and Theorem 2.2.2.

Proof of Theorem 2.2.1. We know that $|A\Gamma L_1(\mathbb{F}_n)| = kn(n-1)$ and $A\Gamma L_1(\mathbb{F}_n)$ acts on $\mathbb{F}_n$ which is of size n. Hence what we really need to show is that the distance is $n - p^{k^*}$.

Let $H = AGL_1(\mathbb{F}_n) = \{ax+b \mid a, b \in \mathbb{F}_n, a \neq 0, 0 \leq i < k\}$ and $G = A\Gamma L_1(\mathbb{F}_n) = \{ax^{p^i} + b \mid a, b \in \mathbb{F}_n, a \neq 0, 0 \leq i < k\}$.

Note that:

(i) H is normal in G, as stated in Section 1.1, which then gives us $G = \bigcup_{i=0}^{k-1} x^{p^i} H$.

(ii) As H is sharply 2-transitive, we can apply Proposition 1.3.9 to get $d_H(H) = n - 1$.

Given what we have above, we can then apply Lemma 2.2.4, which means that we just need to show $d_H(x^{p^i}, H) \geq n - p^{k^*}$ for all $1 \leq i \leq k$. By Lemma 2.2.5, we would need to show $n - r(f - g) \geq n - p^{k^*} \Rightarrow r(f - g) \leq p^{k^*}$, where $f = x^{p^i}$ and $g \in H$, and so it suffices to show $x^{p^i} + ax + b \leq p^{k^*}$, for $a, b \in \mathbb{F}_n, a \neq 0$.

Fix i. Let S be the set of all roots of $f(x) = x^{p^i} - x$. S forms a finite field and is a subfield of $\mathbb{F}_n$, hence $|S| = p^j$ for some j such that $j \mid k$. Now, if we consider the extension of $f(x)$ into its splitting field, the root set of this field forms $\mathbb{F}_{p^i}$. So S is a subfield of $\mathbb{F}_{p^i}$ and hence $j \mid i$. As j divides i and k, we have $j = r(f(x)) \leq p^{\gcd(i,k)} \leq p^{k^*}$. Hence, from Lemma 2.2.6, we have $r(x^{p^i} + ax + b) \leq p^{k^*}$. The result then follows. □

For the sake of completeness, a definition for splitting field is provided below.

Definition 2.2.7. A **splitting field** of a polynomial $p(x)$ over a field K is a field extension L of K over which p factors into linear factors

$$p(x) = \prod_{i=1}^{deg(p)} (x - a_i)$$

where for each i, $x - a_i \in L[x]$.

Corollary 2.2.8. *For $n = 2^k$, k prime, we have $M(n, n-2) \geq kn(n-1)$.*

Remark. For example, we have $M(2048, 2046) = 11 \cdot 2048 \cdot 2047 = 46114816$.

We now move on to prove Thereom 2.2.2.

Proof of Theorem 2.2.2. Recall that we have

$$P\Gamma L_2(\mathbb{F}_n) = \left\{ \frac{ax^{p^i} + b}{cx^{p^i} + d} \;\middle|\; a, b, c, d \in \mathbb{F}_n, ad \neq bc, 0 \leq i < n \right\},$$

which acts on $\mathbb{F}_n \cup \{\infty\}$.

For $g \in G = P\Gamma L_2(\mathbb{F}_n)$, we have the action defined as

$$g(x) = \begin{cases} \frac{ax^{p^i}+b}{cx^{p^i}+d}, & \text{if } x \in \mathbb{F}_n \text{ and } cx^{p^i}+d \neq 0 \\ \infty, & \text{if } x \in \mathbb{F}_n, cx^{p^i}+d = 0 \text{ and } ax^{p^i}+b \neq 0 \\ \frac{a}{c}, & \text{if } x = \infty \text{ and } c \neq 0 \\ \infty, & \text{if } x = \infty, c = 0 \text{ and } a \neq 0 \end{cases}$$

where $x \in \mathbb{F}_n \cup \{\infty\}$.

We thus have the stabilizer of ∞, that is $G_\infty = \{g \in G \mid g(\infty) = \infty\}$, to be isomorphic to $A\Gamma L_1(\mathbb{F}_n)$. Note that this is true as for $g(\infty) = \infty$, we must have $c = 0$ and $a \neq 0$. We also cannot have $g(x) = \infty$ for $x \in \mathbb{F}_n$, as g is a permutation on $\mathbb{F}_n \cup \{\infty\}$, which gives us $d \neq 0$ based on the definition of the function above. Hence we have $g = \frac{ax^{p^i}+b}{d} = \frac{a}{d}x^{p^i} + \frac{b}{d} \in A\Gamma L_1(\mathbb{F}_n)$.

Since G_∞ is isomrphic to $A\Gamma L_1(\mathbb{F}_n)$, we have $d_H(G_\infty) = n - p^{k^*}$ according to Theorem 2.2.1. Note that we have $P\Gamma L_2(\mathbb{F}_n) = \bigcup_{k=0}^{n-1} \pi_k G_\infty$, where $\pi_k \in P\Gamma L_2(\mathbb{F}_n)$ maps k to ∞, $\pi_0 = e$. Then by Lemma 2.2.4, we have

$$d_H(P\Gamma L_2(n)) = \min\{d_H(e, G_\infty \backslash \{e\}), d_H(\pi_1, G_\infty), \ldots, d_H(\pi_{n-1}, G_\infty)\}.$$

As we have $d_H(\pi_i, G_\infty) = d_H(G_\infty) \geq n - p^{k^*}$, $|\mathbb{F}_n \cup \{\infty\}| = n + 1$ and $|G| = kn(n+1)(n-1)$, the result follows. □

Corollary 2.2.9. *For $n = 2^k$, k prime, we have $M(n+1, n-2) \geq kn(n+1)(n-1)$.*

Remark. For example, we have $M(33, 30) = 5 \cdot 33 \cdot 32 \cdot 31 = 163680$.

Chapter 3

New constructions

In this chapter, we look at two constructions of permutation codes. The first utilizes sumsets and the ring of integers modulo n, while the second looks at the affine and projective general linear group of degree n.

A point of interest with the construction via the ring of integers modulo n is that we are able to come up with a construction that does not require n to be a prime power. While the other algebraic constructions are meaningful and interesting in their own way, they are limited to n being a prime power due to the nature of the groups involved.

3.1 Ring of integers modulo n

In this section, we will first give a definition of sumsets, and then split the construction into two cases: when n is a prime power and otherwise, where n is the length of the permutation code.

Definition 3.1.1. Let G be an abelian group, with the group operation denoted as addition. For A, $B \subseteq G$, we define the **sumset** of A and B to be $A + B := \{a + b \mid a \in A,\ b \in B\}$.

Remark. From this definition, we have $A - A = \{a - b \mid a,\ b \in A\} = A + (-A)$.

Remark. It is clear that $|A + B| \geq max\{|A|,\ |B|\}$.

3.1.1 n is a prime power

We first consider the case where n is a prime power. Suppose $n = p^r$, where p is prime and $r \geq 1$ is an integer. Recall that the Euler totient function $\phi(n)$ is the number of integers less than n that is coprime to n.

Lemma 3.1.2. *If $I \subseteq \mathbb{Z}_n$ and $|I| \geq n - \phi(n) + 1$, then $\exists\, \alpha, \beta \in I, \alpha \neq \beta$ such that $\alpha - \beta \in \mathbb{Z}_n^*$, where $\phi(n)$ is the Euler totient function.*

Proof. We make use of what we know about sumsets. Note that we have $|I - I| \geq \max\{|I|, |I|\} = |I| \geq n - \phi(n) + 1$ and $|\mathbb{Z}_n^*| = \phi(n)$. As $I, \mathbb{Z}_n^* \subseteq \mathbb{Z}_n$, we have $|(I - I) \cup \mathbb{Z}_n^*| \leq n$. We then have the following result:

$$\begin{aligned} |(I - I) \cap \mathbb{Z}_n^*| &= |I - I| + |\mathbb{Z}_n^*| - |(I - I) \cup \mathbb{Z}_n^*| \\ &\geq (n - \phi(n) + 1) + \phi(n) - n \\ &= 1 \end{aligned}$$

Hence, there exists at least an element in $|(I - I) \cap \mathbb{Z}_n^*|$. In other words, we have $\alpha, \beta \in I$ such that $\alpha - \beta \in \mathbb{Z}_n^*$. □

Theorem 3.1.3. *For a prime power $n \geq 2$, there exists a permutation code $(n, \phi(n) \cdot n,\ \phi(n))$.*

Proof. Let $n \geq 2$ be a positive integer and $\mathcal{A} = \{(a, b) \mid a \in \mathbb{Z}_n^*,\ b \in \mathbb{Z}_n\}$. Recall that the group action of $\mathcal{A}$ on $\mathbb{Z}_n$ is defined by $\sigma\alpha = a\alpha + b$, where $\alpha \in \mathbb{Z}_n$, $\sigma \in \mathcal{A}$. Note that each $\sigma \in \mathcal{A}$ gives a permutation on $\mathbb{Z}_n$.

Let $\sigma_1, \sigma_2 \in \mathcal{A}$ be two distinct permutations on $\mathbb{Z}_n$, and $d(\sigma_1, \sigma_2) = w$.

Claim. *We claim that $w \geq \phi(n)$.*

Proof of Claim. Suppose $w \leq \phi(n) - 1$. Since $d(\sigma_1, \sigma_2) = w$, there exists $I \subseteq \mathbb{Z}_n$ such that $|I| = n - w$ and $\sigma_1(\alpha) = \sigma_2(\alpha)$ for all $\alpha \in I$. Since $|I| = n - w \geq n - \phi(n) + 1$, by Lemma 3.1.2, we have $\alpha,\ \beta \in I, \alpha \neq \beta$ such that $\alpha - \beta \in \mathbb{Z}_n^*$.

Since $\sigma_1(\alpha) = \sigma_2(\alpha)$ and $\sigma_1(\beta) = \sigma_2(\beta)$, we have

$$\begin{cases} \sigma_1(\alpha) = \sigma_2(\alpha) \\ \sigma_1(\beta) = \sigma_2(\beta) \end{cases} \Rightarrow \begin{cases} a_1\alpha + b_1 = a_2\alpha + b_2 \\ a_1\beta + b_1 = a_2\beta + b_2 \end{cases} \Rightarrow a_1(\alpha - \beta) = a_2(\alpha - \beta)$$

for some $a_1, a_2 \in \mathbb{Z}_n^*$ and $b_1, b_2 \in \mathbb{Z}_n$. Since $\alpha - \beta \neq 0$, we have $a_1 = a_2 \Rightarrow b_1 = b_2 \Rightarrow \sigma_1 = \sigma_2$. Hence this is a contradiction and our claim is true.

As $|\mathcal{A}| = \phi(n) \cdot n$ and $d(\sigma_1, \sigma_2) \geq \phi(n)$, we then have a $(n, \phi(n) \cdot n, \phi(n))$ permutation code. □

Corollary 3.1.4. *For n that is prime, $(n, \phi(n) \cdot n, \phi(n))$ is an optimal code, that is the maximal size has been achieved for the given length and distance.*

Proof. Recall that from the construction via MOLS(n) we obtained Corollary 2.2.9, which said that $M(n, n-1) = n(n-1)$ for n a prime power. If we take n to be prime, we can easily see that the result follows. □

While this is not a new code, for n that is prime, we have shown an algebraic way to achieve this code without having to use mutually orthogonal latin squares.

3.1.2 n is not a prime power

We next consider the case where n is not a prime power. We first show the lemma stated below, and we will use the contrapositive in the main theorem of this subsection.

Lemma 3.1.5. *If $(n - \phi(n)) \mid n$, then n is a prime power.*

Proof. Suppose n is not a prime power, that is $n = \prod_{i=1}^{r} p_i^{e_i}$, where $p_1 < p_2 < \cdots < p_r$ are primes and $e_i \in \mathbb{Z}^+$. Since $(n - \phi(n)) \mid n$, there exists a $k > 1$ such that

$$
\begin{aligned}
& & n &= k(n - \phi(n)) \\
&\Rightarrow & n &\geq p_1(n - \phi(n)) \qquad (1) \\
&\Rightarrow & (p_1 - 1)n &\leq p_1\phi(n) \\
&\Rightarrow & (p_1 - 1)\prod_{i=1}^{r} p_i^{e_i} &\leq p_1 \prod_{i=1}^{r} (p_i - 1)p_i^{(e_i - 1)} \\
&\Rightarrow & (p_1 - 1)\prod_{i=1}^{r} p_i &\leq p_1 \prod_{i=1}^{r} (p_i - 1) \\
&\Rightarrow & \prod_{i=2}^{r} p_i &\leq \prod_{i=2}^{r} (p_i - 1)
\end{aligned}
$$

Note that (1) follows from the fact that p_1 is the smallest factor of n, and so $k \geq p_1$. As we can see, the last inequality is clearly not possible, and so n is a prime power. □

Lemma 3.1.6. *If $n \geq 6$ is not a prime power, then for any $I \subseteq \mathbb{Z}_n$ with $|I| \geq n - \phi(n)$, we have $|I - I| \geq n - \phi(n) + 1$.*

Proof. If $|I| \geq n - \phi(n) + 1$, then we have $|I - I| \geq |I| = n - \phi(n) + 1$, so we are done. Suppose that $|I| = n - \phi(n)$ and $|I - I| = n - \phi(n)$.

Let $I = \{a_1, \cdots, a_{n-\phi(n)}\}$. Since $|I - I| = n - \phi(n)$, for all $1 \leq i,\ j \leq n - \phi(n)$, $a_i - a_1, \cdots, a_i - a_{n-\phi(n)}$ is a permutation of $a_j - a_1, \cdots, a_j - a_{n-\phi(n)}$. This implies that

$$\begin{aligned} & \sum_{k=1}^{n-\phi(n)} (a_i - a_k) = \sum_{k=1}^{n-\phi(n)} (a_j - a_k) \\ \Rightarrow \quad & (n - \phi(n))a_i - \sum_{k=1}^{n-\phi(n)} a_k = (n - \phi(n))a_j - \sum_{k=1}^{n-\phi(n)} a_k \\ \Rightarrow \quad & (n - \phi(n))(a_i - a_j) = 0 \end{aligned}$$

which means that $(n - \phi(n))x \equiv 0 \bmod n$ has at least $n - \phi(n)$ solutions, by fixing a_i and varying a_j. However, $(n - \phi(n))x \equiv 0 \bmod n$ has $gcd(n - \phi(n), n)$ solutions, which means that $gcd(n - \phi(n), n) \geq n - \phi(n)$.

On the other hand, since n is not a prime power, from Lemma 3.1.5, we have $(n - \phi(n)) \nmid n$, which gives us $gcd(n - \phi(n), n) < n - \phi(n)$. Hence this is a contradiction and $|I - I| = n - \phi(n)$ is false, which means that $|I - I| \geq n - \phi(n) + 1$. □

Theorem 3.1.7. *If $n \geq 6$ is not a prime power, there exists a $(n,\ \phi(n) \cdot n,\ \phi(n) + 1)$ permutation code.*

Proof. This proof is similar to the case where n is a prime power, so we will keep it brief. Let $n \geq 2$ be a positive integer and $\mathcal{A} = \{(a, b) \mid a \in \mathbb{Z}_n^*,\ b \in \mathbb{Z}_n\}$. Let σ_1, $\sigma_2 \in \mathcal{A}$ be two distinct permutations on $\mathbb{Z}_n$, and $d(\sigma_1,\ \sigma_2) = w$.

Claim. *We claim that $w \geq \phi(n) + 1$.*

Proof of Claim. Suppose $w \leq \phi(n)$. Since $d(\sigma_1,\ \sigma_2) = w$, there exists $I \subseteq \mathbb{Z}_n$ such that $|I| = n - w$ and $\sigma_1(\alpha) = \sigma_2(\alpha)$ for all $\alpha \in I$. Since $|I| = n - w \geq n - \phi(n)$, we

apply Lemma 3.1.6 to get $|I - I| \geq n - \phi(n) + 1$. This then gives us

$$\begin{aligned} |(I-I) \cap \mathbb{Z}_n^*| &= |I-I| + |\mathbb{Z}_n^*| - |(I-I) \cup \mathbb{Z}_n^*| \\ &\geq (n - \phi(n) + 1) + \phi(n) - n \\ &= 1, \end{aligned}$$

that is there exists $\alpha, \beta \in I, \alpha \neq \beta$ such that $\alpha - \beta \in \mathbb{Z}_n^*$.

Since $\sigma_1(\alpha) = \sigma_2(\alpha)$ and $\sigma_1(\beta) = \sigma_2(\beta)$, we have

$$\begin{cases} \sigma_1(\alpha) = \sigma_2(\alpha) \\ \sigma_1(\beta) = \sigma_2(\beta) \end{cases} \Rightarrow \begin{cases} a_1\alpha + b_1 = a_2\alpha + b_2 \\ a_1\beta + b_1 = a_2\beta + b_2 \end{cases} \Rightarrow a_1(\alpha - \beta) = a_2(\alpha - \beta)$$

for some $a_1, a_2 \in \mathbb{Z}_n^*$ and $b_1, b_2 \in \mathbb{Z}_n$. Since $\alpha - \beta \neq 0$, we have $a_1 = a_2 \Rightarrow b_1 = b_2 \Rightarrow \sigma_1 = \sigma_2$. Hence this is a contradiction and our claim is true.

As $|\mathcal{A}| = \phi(n) \cdot n$ and $d(\sigma_1, \sigma_2) \geq \phi(n) + 1$, we then have a $(n, \phi(n) \cdot n, \phi(n) + 1)$ permutation code. □

3.2 $AGL_n(\mathbb{F}_q)$ and $PGL_n(\mathbb{F}_q)$

We can also construct permutation codes using the affine general linear group $AGL_n(\mathbb{F}_q)$ and the projective general linear group $PGL_n(\mathbb{F}_q)$. That can be achieved with the help of the following lemma, which is a general property of permutation codes arising from groups acting on a set.

Lemma 3.2.1. *Suppose a group G acts on a finite set Ω, where $|\Omega| = n$. Let $\Omega^g := \{\omega \in \Omega \mid g\omega = \omega\}$. If $|\Omega^g| \leq t$ for all $g \in G, g \neq 1$, then there exists a $(n, |G|, n - t)$-code.*

Proof. This is clear. $|\Omega^g| \leq t$ means that $g \in G, g \neq 1$ fixes at most t elements, and so the Hamming distance is at least $n - t$. □

3.2.1 $AGL_n(\mathbb{F}_q)$

Recall that the affine general linear group as mentioned in Section 1.1, $AGL_n(\mathbb{F}_q) = \mathbb{F}_q^n \rtimes GL_n(\mathbb{F}_q)$, acts on $\mathbb{F}_q$ in the following manner:

$$\begin{aligned}(A,b) : \mathbb{F}_q^n &\to \mathbb{F}_q^n \\ u &\mapsto Au + b\end{aligned}$$

where $(A, b) \in AGL_n(\mathbb{F}_q)$.

Theorem 3.2.2. *Let $n \geq 1$ be an integer and q be a prime power. Then there exists a $\left(q^n, q^n \prod_{i=0}^{n-1}(q^n - q^i), q^n - q^{n-1}\right)$-code.*

Proof. To apply Lemma 3.2.1, we consider $|\{u \in \mathbb{F}_q^n \mid Au + b = u\}|$ for $(A, b) \in AGL_n(\mathbb{F}_q), (A, b) \neq (I, 0)$. Given such (A, b), we want to find the number of u's that will satisfy $(A - I)u = -b$. Since $A \neq I$, we must have $\text{rank}(A - I) \geq 1$, and thus $\text{nullity}(A - I) \leq n - 1$, which then gives us $|\{u \in \mathbb{F}_q^n \mid Au + b = u\}| \leq q^{n-1}$. Since $|\mathbb{F}_q^n| = q^n$ and $|AGL_n(\mathbb{F}_q)| = q^n \prod_{i=0}^{n-1}(q^n - q^i)$, we can then apply Lemma 3.2.1 to get a $\left(q^n, q^n \prod_{i=0}^{n-1}(q^n - q^i), q^n - q^{n-1}\right)$-code. □

3.2.2 $PGL_n(\mathbb{F}_q)$

Recall that we have defined the projective general linear group in Section 1.1, and it is $PGL_n(\mathbb{F}_q) = GL_n(\mathbb{F}_q)/Z(GL_n(\mathbb{F}_q))$, where $Z(GL_n(\mathbb{F}_q)) = \{\lambda I_n \mid \lambda \in \mathbb{F}_q^*\}$. The projective general linear group acts on $\mathbb{P}_q^{n-1}$ in the following manner

$$\begin{aligned}A : \mathbb{P}_q^{n-1} &\to \mathbb{P}_q^{n-1} \\ u &\mapsto Au\end{aligned}$$

where $A \in PGL_n(\mathbb{F}_q)$.

Lemma 3.2.3. *Suppose $r = \min\{\text{rank}(\lambda A - I) \mid \lambda \in \mathbb{F}_q^*\} = \text{rank}(\lambda_0 A - I)$ for some λ_0, where $A, I \in GL_n(\mathbb{F}_q)$ and $A \neq kI$, for $k \in \mathbb{F}_q^*$. Then $\forall \lambda \neq \lambda_0$, we have that $\text{rank}(\lambda A - I) \geq n - r$.*

Proof. Recall that from linear algebra, we have $\text{rank}(A-B) \leq \text{rank}(A)+\text{rank}(-B) =$

$\text{rank}(A) + \text{rank}(B)$. Thus we have the following result:

$$\begin{aligned}
\text{rank}(\lambda_0 A - I - (\lambda A - I)) &\leq \text{rank}(\lambda_0 A - I) + \text{rank}(\lambda A - I) \\
\text{rank}(\lambda_0 A - \lambda A) &\leq \text{rank}(\lambda_0 A - I) + \text{rank}(\lambda A - I) \\
n &\leq r + \text{rank}(\lambda A - I) \\
\text{rank}(\lambda A - I) &\geq n - r
\end{aligned}$$

□

Theorem 3.2.4. *Let $n \geq 1$ be an integer and q be a prime power. Then there exists a $\left(\frac{q^n-1}{q-1}, \frac{1}{q-1}\prod_{i=0}^{n-1}(q^n - q^i), q^{n-1} - q + 2\right)$-code.*

Proof. To apply Lemma 3.2.1, we want to find a t such that $|\mathbb{P}_q^{n-1\,A}| = |\{u \in \mathbb{P}_q^{n-1} \mid Au = u\}| \leq t$ for all $A \in PGL_n(\mathbb{F}_q)$ that is not the identity. To find u that satisfies $Au = u$, we consider $\lambda A'u = u$, with $A' \in GL_n(\mathbb{F}_q)$ corresponding to $A \in PGL_n(\mathbb{F}_q)$, and $\lambda \in \mathbb{F}_q^*$.

We let $r = \min\{\text{rank}(\lambda A' - I) \mid \lambda \in \mathbb{F}_q^*\} = \text{rank}(\lambda_0 A' - I)$ for some λ_0, where $A', I \in GL_n(\mathbb{F}_q)$ and $A' \neq kI$ for $k \in \mathbb{F}_q^*$. Then from Lemma 3.2.3, $\forall \lambda \neq \lambda_0$, $\text{rank}(\lambda A' - I) \geq n - r$, and thus $\text{nullity}(\lambda_0 A' - I) \leq n - r$ and $\text{nullity}(\lambda A' - I) \leq r$. Hence, the number of u that satisfies $\lambda A'u = u$ is at most $(q^{n-r} - 1) + (q-2)(q^r - 1)$, and consequently, the number of u that satisfies $Au = u$ is at most $\frac{(q^{n-r}-1)}{q-1} + \frac{(q-2)(q^r-1)}{q-1} \leq \frac{q^{n-1}-1}{q-1} + q - 2$.

From Lemma 3.2.1, we know that the length of the code is $|\mathbb{P}_q^{n-1}| = \frac{q^n-1}{q-1}$ and the size is $|PGL_n(\mathbb{F}_q)| = \frac{1}{q-1}\prod_{i=0}^{n-1}(q^n - q^i)$. Furthermore, the distance is $\frac{q^n-1}{q-1} - (\frac{q^{n-1}-1}{q-1} + q - 2) = q^{n-1} - q + 2$.

Hence, we obtain a $\left(\frac{q^n-1}{q-1}, \frac{1}{q-1}\prod_{i=0}^{n-1}(q^n - q^i), q^{n-1} - q + 2\right)$-code. □

Chapter 4

Conclusion and further study

In this thesis, we have covered as much as possible, the elementary results of permutation codes, as well as some (hopefully interesting) algebraic constructions, alongside a combinatorial one. We briefly summarize the results below.

From the known constructions, for n prime power, we have these results:

(i) $M(n, n-1) = n(n-1)$ from MOLS(n),

(ii) $M(n, n-p^{k^*}) \geq kn(n-1)$ from $A\Gamma L_1(\mathbb{F}_n)$, and

(iii) $M(n+1, n-p^{k^*}) \geq k(n+1)n(n-1)$ from $P\Gamma L_2(\mathbb{F}_n)$.

From the new constructions, we have these results:

(i) $M(n, \phi(n)) \geq \phi(n) \cdot n$ for n prime power,

(ii) $M(n, \phi(n)+1) \geq \phi(n) \cdot n$ for n not prime power,

(iii) $M(q^n, q^n - q^{n-1}) \geq q^n \prod_{i=0}^{n-1}(q^n - q^i)$, and

(iv) $M(\frac{q^n-1}{q-1}, q^{n-1} - q + 2) \geq \frac{1}{q-1} \prod_{i=0}^{n-1}(q^n - q^i)$ where q is prime power.

As the area of permutation codes is still relatively new compared to classical binary codes, the existing literature of the former is not as rich as the latter. Hence, there are gaps to fill and areas to work on, and its applications serve as a motivation for research in this direction.

Regarding possible topics for future research, one can work on finding better constructions of codes, in particular algebraic ones, as the algebraic constructions

available are limited. As one may have observed, the algebraic constructions in this paper tend to have the restriction of n to be a prime power, as that is necessary to have a finite field. Hence we can either improve on these results, or work on finding results for n that is not a prime power.

Moving away from the direction we have taken in this thesis, one can also try to apply algebraic constructions to other metrics, such as the Kendall tau or Ulam metric. Another area of interest is constant composition codes, which are codes where each symbol can be repeated more than once in each codeword, but they have to appear the same number of times for every codeword. Permutation codes are a special case of constant composition codes, where each symbol occurs only once. A good introduction to constant composition codes can be found in [6].

Bibliography

[1] S. Bereg, A. Levy, I. H. Sudborough, "Constructing permutation arrays from groups," *Design, Codes and Cryptography* pp. 1-17, 2017.

[2] Y. M. Chee and V. K. Vu, "Breakpoint analysis and permutation codes in generalized Kendall tau and Cayley metrics," *IEEE International Symposium on Information Theory*, pp. 2959-2963, 2014.

[3] C. J. Colbourn, T. Klove and A. C. H. Ling, "Permutation arrays for powerline communication and mutually orthogonal latin squares," *IEEE Transactions on Information Theory*, vol. 50, no. 6, pp. 1289-1291, Jun. 2004.

[4] D. A. Cox, "Galois Theory", *Wiley's Pure and Applied Mathematics*, 2004.

[5] W. Chu, C. J. Colbourn, and P. Dukes. "Constructions for permutation codes in powerline communications," *Designs, Codes and Cryptography*, vol. 32, pp. 51–64, 2004.

[6] W. Chu, C. J. Colbourn, and P. Dukes. "On constant composition codes," *Discrete Applied Mathematics*, vol. 154, no. 6, pp. 912-929, 2006.

[7] P. Das, "The number of permutation polynomials of a given degree over a finite field," *Finite Fields and Their Applications*, vol. 8, no. 4, pp. 478-490, 2002.

[8] E. En Gad, E. Yaakobi, A. A. Jiang and J. Bruck, "Rank-modulation rewrite coding for flash memories," in *IEEE Transactions on Information Theory*, vol. 61, no. 8, pp. 4209-4226, Aug. 2015.

[9] F. Gao, Y. Yang and G. Ge, "An improvement on the Gilbert–Varshamov bound for permutation codes," in *IEEE Transactions on Information Theory*, vol. 59, no. 5, pp. 3059-3063, May 2013.

[10] A. Jiang, R. Mateescu, M. Schwartz, and J. Bruck, "Rank modulation for flash memories," *IEEE Transactions on Information Theory*, vol. 55, no. 6, pp. 2659–2673, Jun. 2009.

[11] A. Jiang, M. Schwartz, J. Bruck, "Error-correcting codes for rank modulation," in *IEEE International Symposium on Information Theory*, pp. 1736-1740, 2008.

[12] K. Y. Kim, R. Kim and J. S. Kim, "On the number of permutation polynomials over a finite field," *International Journal of Number Theory 2016*, vol. 12, no. 6, pp. 1519-1528, 2016.

[13] T. Klove, T. T. Lin, S. C. Tsai and W. G. Tzeng, "Permutation arrays under the chebyshev distance," in *IEEE Transactions on Information Theory*, vol. 56, no. 6, pp. 2611-2617, Jun. 2010.

[14] C. F. Laywine, and G. L. Mullen, "Discrete Mathematics Using Latin Squares", *Wiley-Interscience Series in Discrete Mathematics and Optimization*, no. 49, 1998.

[15] R. Lidl, G. L. Mullen, "When does a polynomial over a finite field permute the elements of the field?," *Amer. Math. Monthly*, vol. 95, no. 3, pp. 243-246, Mar 1988.

[16] S. Ling, C. Xing, "Coding Theory: A First Course", *Cambridge University Press*, 2004.