CONSTRUCTING PERMUTATION ARRAYS OF KNOWN DISTANCE

by

Brian D. Malouf

APPROVED BY SUPERVISORY COMMITTEE:

Sergey Bereg, Chair

Ivan Hal Sudborough, Co-Chair

R. Chandrasekaran

Ding-Zhu Du

Benjamin Raichel

To Marian and David,

for your love and support,

for bringing me joy,

for giving me purpose.

CONSTRUCTING PERMUTATION ARRAYS OF KNOWN DISTANCE

by

BRIAN D. MALOUF, BS, MS

DISSERTATION

Presented to the Faculty of

The University of Texas at Dallas

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY IN

COMPUTER SCIENCE

THE UNIVERSITY OF TEXAS AT DALLAS

May 2023

ACKNOWLEDGMENTS

I give my sincere thanks to Dr. Linda Morales. You took my desire to learn and gave me a path to channel it. To Dr. Hal Sudborough – you have always been patient and willing to share your knowledge with someone who is eager to learn. To Dr. Sergey Bereg – your guidance and support have carried me through this process.

I thank each of you for your motivation and encouragement. When I started this journey, I did not know I would be travelling this far. Without you, I could not have.

April 2023

CONSTRUCTING PERMUTATION ARRAYS OF KNOWN DISTANCE

Brian D. Malouf, PhD
The University of Texas at Dallas, 2023

Supervising Professors: Sergey Bereg, Chair
Ivan Hal Sudborough, Co-Chair

A permutation array (PA) is a set of permutations on n symbols. A PA is said to have distance d (under some metric) if every pair of distinct permutations in the array has distance at least d. Commonly used distance metrics include Hamming distance and Chebyshev distance. PAs of a known distance can be used to construct error-correcting codes and have applications in communication over noisy channels.

Let $M(n, d)$ represent the maximum size of a permutation array on n symbols with pairwise Hamming distance d. Let $P(n, d)$ represent the maximum size of a permutation array on n symbols with pairwise Chebyshev distance d. Exact values of $M(n, d)$ and $P(n, d)$ are unknown for most values n and d with the exception of some special cases. While combinatorial upper and lower bounds exist for both $M(n, d)$ and $P(n, d)$, these can often be improved through empirical techniques. We present several such techniques to construct PAs under the Hamming and Chebyshev distance metrics, resulting in improved bounds for both $M(n, d)$ and $P(n, d)$.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

A *permutation* on a set of symbols is a linear ordering such that each symbol appears exactly once. Two permutations π and σ have *Hamming distance* d, denoted $hd(\pi, \sigma) = d$, if their symbols differ in exactly d different positions. Let $\pi(i)$ denote the symbol in position i of permutation π. Then the Hamming distance between two permutations can be calculated as,

$$hd(\pi, \sigma) = \sum_{i=1}^{n} \{1 \mid \pi(i) \neq \sigma(i)\}.$$

A *permutation array* (PA) is a set of permutations on n symbols. A PA A has Hamming distance at least d, denoted $hd(A) \geq d$, if every distinct pair of permutations in A has Hamming distance at least d. The maximum number of permutations in a PA on n symbols with $hd(A) \geq d$ is denoted $M(n, d)$.

Permutation arrays under Hamming distance have long been studied and have particular interest in applications for data transmission over noisy channels, such as power lines (Chu et al., 2004; Ferreira and Vinck, 2000; Vinck, 2000; Pavlidou et al., 2003). Rather than modulate the amplitude of a signal, power line transmissions modulate the frequency. If a set of frequencies, $f_1, f_2, \ldots, f_n$, is mapped to a set of n symbols, then the order in which the frequencies are modulated corresponds to some permutation on the n symbols.

Chebyshev distance is another interesting metric to consider between permutations. Two permutations π and σ have Chebyshev distance d, denoted $cd(\pi, \sigma) = d$, if the greatest difference between two symbols in the same position is d. That is,

$$cd(\pi, \sigma) = \max\{|\pi(i) - \sigma(i)| \mid 1 \leq i \leq n\}.$$

A PA A has Chebyshev distance at least d, denoted $cd(A) \geq d$, if every distinct pair of permutations in A has Chebyshev distance at least d. The maximum number of permutations in a PA on n symbols with $cd(A) \geq d$ is denoted $P(n, d)$.

Permutation arrays under Chebyshev distance have applications in the recharging and error correcting issues of multi-level flash memory (Jiang et al., 2009, 2008). Given a block of memory cells, $c_1, c_2, \ldots, c_n$, we consider only the relative magnitude of a cell's charge against the other cells in the block, rather than its precise value. If the cells are then ordered by rank of their relative charge, highest to lowest, we obtain a permutation on n. Such a scheme can be used to recover errors due to the drift of cell charges over time.

This dissertation is organized as follows. The rest of Chapter 1 details fundamental concepts necessary for the study of permutation arrays. It also reviews many existing techniques to construct PAs and includes known bounds for $M(n, d)$ and $P(n, d)$ obtained from these techniques.

In Chapter 2 we discuss normalization and mapping functions applicable to permutation polynomials. We show how to use these operations to reduce the search space for PPs from $O(n^{d+1})$ to $O(n^{d-3})$, and we provide an algorithm which performs this optimized search.

Chapter 3 takes the techniques used in Chapter 2 and applies them to the search of permutation rational functions. We detail how PRFs of varying degree can be combined to form PAs of a particular distance and provide several theorems which establish new lower bounds for many cases of $M(n, d)$.

Chapter 4 explores PAs under the Chebyshev distance metric. We detail several search techniques which can be used to construct PAs and introduce several theorems to improve known lower and upper bounds of $P(n, d)$. We also give exact bounds for the general cases $P(n, 2)$ and $P(n, n-2)$.

In Chapter 5 we summarize our results. We detail several possible modifications and improvements that could be applied to the search techniques we introduced. We discuss some open questions and ideas to approach them.

1.1 Groups

Groups lay the groundwork for many construction methods of permutation arrays. A group G is a set of elements, along with some binary operation $*$, such that the following three properties hold:

1. $*$ is *associative*. For any $a, b, c \in G$,

$$a * (b * c) = (a * b) * c.$$

2. There is an *identity element* $e \in G$ such that for all $a \in G$,

$$a * e = e * a = a.$$

3. For all $a \in G$, there is an *inverse element* $a^{-1} \in G$ such that,

$$a * a^{-1} = a^{-1} * a = e.$$

If the group also satisfies:

4. For all $a, b \in G$,

$$a * b = b * a,$$

then the group is known as a *commutative* or *abelian group* (Lidl and Niederreiter, 1997).

A set of permutations can form a group under the binary operation *composition*. To compose the permutation π with σ, denoted $\pi \circ \sigma$, you place the i^{th} symbol of π at the position where i occurs in σ. This is defined as,

$$\pi \circ \sigma = \{\pi(\sigma(i)) \mid 1 \leq i \leq n\}.$$

Note that the composition of permutations is not commutative.

1.1.1 Finite Fields

Many permutation groups are constructed algebraically through the use of *finite fields*. A finite field is a set of elements similar to a group, but with additional properties that must hold, sometimes referred to as *field axioms*. In order for a set to be a field, the following must be true for addition and multiplication:

1. Addition and multiplication are associative.

$$(a + b) + c = a + (b + c)$$
$$(ab)c = a(bc)$$

2. Addition and multiplication are commutative.

$$a + b = b + a$$
$$ab = ba$$

3. Multiplication distributes over addition.

$$a(b + c) = ab + ac$$

4. There exist both additive and multiplicative identities.

$$a + 0 = a$$
$$a \cdot 1 = a$$

5. Every element in the field has an additive inverse, and every nonzero element has a multiplicative inverse.

$$a + (-a) = 0$$
$$a \cdot a^{-1} = 1 \text{ if } a \neq 0$$

Table 1.1. $\mathbb{F}_8$ constructed from the primitive polynomial $x^3 + x + 1$.

x^i	Remainder	Coefficients	Coefficient Symbol	Exponent Symbol
-	0	0 0 0	0	0
x^0	1	0 0 1	1	1
x^1	x	0 1 0	2	2
x^2	x^2	1 0 0	4	3
x^3	$x + 1$	0 1 1	3	4
x^4	$x^2 + x$	1 1 0	6	5
x^5	$x^2 + x + 1$	1 1 1	7	6
x^6	$x^2 + 1$	1 0 1	5	7

If a set has a finite number of elements and observes these properties, then it is called a *finite field*, or *Galois field* (Lidl and Niederreiter, 1997).

A finite field of n elements is denoted $\mathbb{F}_n$, or also commonly $\mathbb{F}_q$, and can be constructed for any $n = p^k$ where p is prime and $k \geq 1$. Note that p is known as the *characteristic* of the field. If n itself is prime, then the field can be constructed on the symbols $\{0, 1, 2, \ldots, n-1\}$ by performing both addition and multiplication modulo n.

When $n = p^k$ is a prime power for some $k > 1$, then a *primitive polynomial* is used to generate the field elements. Primitive polynomials are irreducible, of degree k, and at least one exists for each value p^k. For each nonzero element of the field, we take some variable x^i, divide this by the primitive polynomial, then consider the remainder to identify the element of the field. We can label the element by either considering the coefficients of the remainder as a k-bit p-nary number, or simply use the symbol $i + 1$. An example construction for $\mathbb{F}_8$ showing both labeling schemes can be seen in Table 1.1.

Addition and multiplication are calculated by adding or multiplying the elements' polynomial remainders modulo the primitive polynomial. Coefficients of the resulting polynomial

are then taken modulo p. For example, if we use the exponent symbols of the field $\mathbb{F}_8$:

$$\begin{aligned} 4 + 6 &= \\ (x+1) + (x^2 + x + 1) &= \\ x^2 + 2x + 2 &= \\ x^2 &= 3. \end{aligned}$$

1.1.2 Linear Groups

The affine general linear group $AGL(1, n)$ is a permutation group that can be constructed as follows:

$$AGL(1, n) = \{ax + b \mid a, b \in \mathbb{F}_n, a \neq 0\}.$$

Since the field is constructed in $\mathbb{F}_n$, we are limited to values of n that are either prime or powers of a prime. Given that there are n choices for b, and $n - 1$ choices for a, the PA formed by $AGL(1, n)$ is of the order $n(n - 1)$. Furthermore, it is known that $AGL(1, n)$ is sharply 2-transitive (Passman, 1968).

A permutation group G is *k-transitive* if given any two ordered subsets of symbols $\{a_1, \ldots, a_k\}$ and $\{b_1, \ldots, b_k\}$, there is a permutation $\pi \in G$ that maps $a_i \mapsto b_i$ for $1 \leq i \leq k$. More plainly, pick any k symbols and any k positions, and there will be at least one permutation in G with those symbols at those positions. If the permutation in G is unique for any choice of k symbols and positions, then the group is *sharply k-transitive*.

Sharply k-transitive groups are significant for two reasons. First, they give guarantees on the Hamming distance of the permutations they contain. For example, consider $AGL(1, n)$, and assume there are two permutations in the group that agree in two positions. That would mean those two permutations map the same two symbols to the same two positions, giving us a contradiction since $AGL(1, n)$ is sharply 2-transitive, so the permutation with that

mapping must be unique. Therefore, there can be at most one agreement between any two permutations, giving us a Hamming distance of $n-1$. In general, if a group G is sharply k-transitive, then $hd(G) = n - k + 1$ (Frankl and Deza, 1977).

The second reason sharply k-transitive groups are important is that they form maximum size PAs of Hamming distance $n - k + 1$ (Frankl and Deza, 1977). This means for the values of n and d for which a sharply k-transitive group exists, we know the exact value of $M(n, d)$.

Projective groups are also constructed in some $\mathbb{F}_n$, but additionally include the symbol ∞ to generate permutations on $n+1$ symbols. Let $\mathbb{P}^1(\mathbb{F}_n) = \mathbb{F}_n \cup \{\infty\}$. The projective general linear group $PGL(2, n)$ is defined as follows:

$$PGL(2,n) = \left\{ \frac{ax+b}{cx+d} \;\middle|\; a,b,c,d \in \mathbb{F}_n, ad \neq bc, x \in \mathbb{P}^1(\mathbb{F}_n) \right\},$$

where

$$\frac{ax+b}{cx+d} = \begin{cases} \frac{ax+b}{cx+d}, & \text{if } x \in \mathbb{F}_n \text{ and } x \neq -\frac{d}{c}, \\ \infty, & \text{if } x \in \mathbb{F}_n \text{ and } x = -\frac{d}{c}, \\ \infty, & \text{if } x = \infty \text{ and } c = 0, \\ \frac{a}{c}, & \text{if } x = \infty \text{ and } c \neq 0. \end{cases}$$

$PGL(2, n)$ has order $(n^3 - n)$ and is sharply 3-transitive (Passman, 1968). Thus, when n is a prime or prime power, $M(n+1, n-1) = n^3 - n$.

1.1.3 Semilinear Groups

The affine semilinear group $A\Gamma L(1, n)$ is formed from a semidirect product of $AGL(1, n)$ and a cyclic group of order k. If $n = p^k$ for some prime p, $A\Gamma L(1, n)$ is generated iteratively by composing x^p, known as the Frobenius automorphism, with the elements of $AGL(1, n)$ (Bereg et al., 2018).

$$A\Gamma L(1,n) = \{ax^{p^i} + b \mid a, b \in \mathbb{F}_n, a \neq 0, 0 \leq i \leq k\}$$

While $A\Gamma L(1,n)$ is not sharply transitive, it is known to have $kn(n-1)$ permutations with Hamming distance given by Theorem 1.

Theorem 1. *(See Bereg et al. (2018, Theorem 1)) The Hamming distance of $A\Gamma L(1,n)$ is $n-p^{k^*}$, where $n=p^k$ and k^* is the largest proper factor of k.*

Thus, we can observe the Hamming distance of $A\Gamma L(1,n)$ is maximized if k is a prime number, since its only proper factor will be 1. For example if we consider $n=2^5=32$, Theorem 1 tells us the Hamming distance will be 30, giving us the bound $M(32,30)\geq 5\cdot 32\cdot 31=4{,}960$.

The projective semilinear group $P\Gamma L(2,n)$ is similarly constructed from a semidirect product of $PGL(2,n)$ and a cyclic group of order k generated by the Frobenius automorphism x^p.

$$P\Gamma L(2,n)=\left\{\frac{ax^{p^i}+b}{cx^{p^i}+d}\;\middle|\; a,b,c,d\in\mathbb{F}_n, ad\neq bc, x\in\mathbb{P}^1(\mathbb{F}_n), 0\leq i\leq k\right\},$$

where

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

$P\Gamma L(2,n)$ contains $k(n+1)n(n-1)$ permutations with Hamming distance given by Theorem 2.

Theorem 2. *(See Bereg et al. (2018, Theorem 2)) The Hamming distance of $P\Gamma L(2,n)$ is $n-p^{k^*}$, where $n=p^k$ and k^* is the largest proper factor of k.*

Just like $A\Gamma L(1,n)$, the Hamming distance of $P\Gamma L(2,n)$ is maximized when k is prime. If we consider the same example of $n=2^5=32$, $P\Gamma L(2,n)$ gives us the bound $M(33,30)\geq 5\cdot 33\cdot 32\cdot 31=163{,}680$.

Table 1.2. The Mathieu Groups.

Group	n	transitivity	size
M_{11}	11	sharply 4	7,920
M_{12}	12	sharply 5	95,040
M_{22}	22	3	443,520
M_{23}	23	4	10,200,960
M_{24}	24	5	244,823,040

Table 1.3. Permutation groups that form maximum size PAs.

Group	$M(n,d)$	size
$AGL(1,n)$	$M(n,n-1)^*$	$n(n-1)$
$PGL(2,n)$	$M(n+1,n-1)^*$	$(n+1)n(n-1)$
M_{11}	$M(11,8)$	7,920
M_{12}	$M(12,8)$	95,040

* n must be a prime or prime power

1.1.4 Mathieu Groups

The Mathieu groups, $M_{11}, M_{12}, M_{22}, M_{23}$, and M_{24}, are a set of five sporadic simple groups described by Emile Mathieu in 1861 and 1873. They are all k-transitive groups acting respectively on 11, 12, 22, 23, and 24 symbols (Dixon and Mortimer, 1996).

Groups M_{11} and M_{12} are especially noteworthy as they are sharply 4-transitive and sharply 5-transitive respectively. Furthermore, they are the only groups that are sharply k-transitive for $k \geq 4$.

Groups M_{22}, M_{23}, and M_{24} are 3-transitive, 4-transitive, and 5-transitive respectively. The cardinality of the Mathieu groups is noted in Table 1.2.

With the addition of M_{11} and M_{12} to the other sharply k-transitive groups discussed, Table 1.3 shows a summary of groups that can form PAs of a maximum size.

1.1.5 Cosets

Let σ and π be two permutations, and $\sigma\pi$ be defined as the composition $\pi \circ \sigma$. Let G be a permutation group. We define the *right coset* and *left coset* of G as follows:

$$\begin{aligned} \textit{right coset:} \quad & G\pi = \{g\pi \mid g \in G\}, \\ \textit{left coset:} \quad & \pi G = \{\pi g \mid g \in G\}, \end{aligned}$$

where π is known as the *representative* of the coset.

By taking advantage of the properties of cosets and groups, Bereg et al. (2018) designed an efficient algorithm for constructing large PAs known as the *coset method*. Assume you have some permutation group G and a permutation π with Hamming distance at least d from G. It can be shown that the entire coset πG has Hamming distance at least d from G.

$$\begin{aligned} hd(\pi G, G) &= \max\{hd(\pi g_1, g_2) \mid g_1, g_2 \in G\} \\ &= \max\{hd(\pi, g_2 g_1^{-1}) \mid g_1, g_2 \in G\} \\ &= \max\{hd(\pi, g) \mid g \in G\} \end{aligned}$$

This is true because $g_2 g_1^{-1} \in G$ by the properties of a group. Thus, by finding a single permutation π, we can form a new PA by taking $G \cup \pi G$, having Hamming distance $\geq d$ and cardinality $2 \cdot |G|$. Additionally, one only needs to store the coset representative π to represent this PA, as all other permutations are obtained by the predefined construction of the group G and composition with π.

While this process can be iterated on to combine multiple cosets into a larger PA, competitive bounds for $M(n, d)$ can also come from selectively choosing a single permutation π and group G. In either case, we must start with a group G that forms a good PA for $M(n, d')$ where $d' > d$. Since we know exact values of $M(n, n-1)$ and $M(n+1, n-1)$ from $AGL(1, n)$ and $PGL(2, n)$, these make excellent candidates to start with. The Mathieu

groups are also viable options, as well as the cyclic group of order n, which gives an exact value of $M(n, n)$ for all values of n, not just prime powers.

As an example, consider $G = PGL(2, 16)$, which gives us an exact value of $M(17, 15) =$ 4,080, and the permutation π given by the function $f(x) = x^2$. If we use exponent symbols for $\mathbb{F}_{16}$ and let 16 represent ∞, that gives us:

$$\begin{aligned}\pi &= f(x),\\ &= x^2,\\ &= (0\ 1\ 3\ 5\ 7\ 9\ 11\ 13\ 15\ 2\ 4\ 6\ 8\ 10\ 12\ 14\ 16).\end{aligned}$$

It is known that for $G = PGL(2, n = p^k)$, the automorphism $f(x) = x^p$ is at least distance $n - p$ from all permutations in G. Therefore, π has a Hamming distance at least 14 from G. If we then take $\pi G \cup G$, we obtain the bound $M(17, 14) \geq$ 8,160, which is competitive with other known lower bounds.

One approach to finding new permutations π to generate additional cosets is to randomly search for them, which is the approach taken in Bereg et al. (2018). While randomly searching does not seem like an ideal algorithm, the efficiency with which it is done has led to new and competitive bounds for $M(n, d)$. The algorithm proceeds as follows:

1. Select a starting permutation group G which gives a known bound on $M(n, d')$, where $d' > d$, and d is the desired Hamming distance of the constructed PA.

2. Suppose the algorithm has found k coset representative $\pi_0, \pi_1, \ldots, \pi_{k-1}$, where π_0 is the identity permutation, and $\pi_0 G$ is simply the group G. Randomly select a new permutation π_k.

3. If $hd(\pi_k, \pi_i G) \geq d$ for all $0 \leq i < k$, and $hd(\pi_k, \pi_{k-1}) = d$, add π_k to the list of coset representatives. Repeat from step 2 until the desired number of coset representatives is found.

The resulting PA will have Hamming distance at least d and cardinality $(k+1) \cdot |G|$.

In step (3), the check that $hd(\pi_k, \pi_{k-1}) = d$ is intentional, and serves to maximize the number of new coset representatives that can be found by respecting the combinatorial Gilbert-Varshimov lower bound. What we actually want to ensure is that for each π_k, $hd(\pi_k, \pi_i G) = d$ for at least some i, but the condition used in the algorithm does this more easily. If this condition were not met, that is we select some π_k such that $hd(\pi_k, \pi_i G) > d$ for all cosets $\pi_i G$, then we may greatly limit the number of remaining coset representatives that could be found.

The efficiency of this algorithm lies not only in the fact that it is only necessary to save coset representatives, rather than the entire PA, but also in the ability to more efficiently test the Hamming distance. Let P be a PA consisting of k left cosets of some permutation group G on n symbols, and let $\pi \in S_n$, where S_n is the symmetric group, that is, the group of all permutations on n symbols. By the definition of Hamming distance, $hd(\pi, P) = \min_{\sigma \in P} hd(\pi, \sigma)$. To calculate this by normal methods, the running time would be $O(n|P|) = O(nk|G|)$. However, if G is cyclic, or contains the cyclic subgroup, the Hamming distance algorithm can be improved.

Let C_n denote the cyclic subgroup, that is,

$$C_n = \{g_j \mid g_j = (j, j+1, \ldots, n-1, 0, 1, \ldots, j-1), 0 \leq j \leq n-1\}.$$

For example,

$$C_4 = \begin{bmatrix} 0123 \\ 1230 \\ 2301 \\ 3012 \end{bmatrix}.$$

All of the permutation groups we have discussed contain this subgroup, which permits the application of Theorem 3.

Theorem 3. *(See Bereg et al. (2018, Theorem 5)) If C_n is a subgroup of G, then the Hamming distance $hd(\pi, P)$ can be computed in $O(k|G|)$ time for any permutation $\pi \in S_n$.*

This improvement to the Hamming distance check, arguably the most time consuming portion of the algorithm, makes it efficient enough that even with the random guessing of new permutations, competitive results for $M(n, d)$ can be found using the *coset method* (Bereg et al., 2018).

1.2 Contraction

Contraction is a process of modifying a PA from S_n to S_{n-m} while minimally affecting the Hamming distance (Bereg et al., 2018). First, consider the case where $m = 1$, and let π be a permutation in S_n. The contraction of π, denoted π^{CT}, is a permutation in S_{n-1} defined as follows. For $0 \leq x < n - 1$,

$$\pi^{CT}(x) = \begin{cases} \pi(x), & \text{if } \pi(x) \neq n-1, \\ \pi(n-1), & \text{if } \pi(x) = n-1. \end{cases}$$

More plainly, π^{CT} is formed by changing the symbol $n-1$ to the last symbol in the permutation, $\pi(n-1)$, then deleting the symbol $n-1$ from the permutation. The contraction of a PA A, denoted A^{CT}, is defined as follows,

$$A^{CT} = \{\pi^{CT} \mid \pi \in A\}.$$

Since most of the symbols of each permutation remain unchanged, the Hamming distance of A^{CT} will not be that much less than that of A.

We can observe that the most the Hamming distance of a PA can decrease after the contraction operation for $m = 1$ is 3, which occurs if there is a 3-symbol cycle within the PA. That is, given two permutations π and σ, for some positions $i, j < n - 1$, and symbols $r, s < n - 1$, the following three things are true:

1. $\pi(i) = n-1 \quad \text{and} \quad \sigma(i) = r,$

2. $\pi(j) = s \quad \text{and} \quad \sigma(j) = n-1,$

3. $\pi(n-1) = r \quad \text{and} \quad \sigma(n-1) = s.$

For example, consider the following permutations on 6 symbols where $i = 4, j = 0, r = 0, s = 1$:

$$\pi = (1\ 2\ 3\ 4\ 5\ 0), \quad \pi^{CT} = (1\ 2\ 3\ 4\ 0),$$
$$\sigma = (5\ 3\ 4\ 2\ 0\ 1), \quad \sigma^{CT} = (1\ 3\ 4\ 2\ 0).$$

While $hd(\pi, \sigma) = 6$, after the contraction, we have $hd(\pi^{CT}, \sigma^{CT}) = 3$.

If no such 3-cycle exists, then performing the contraction operation on a PA will only reduce the Hamming distance by 2. Furthermore, the contraction operation can be applied multiple times to a PA, which leads to Theorem 4.

Theorem 4. *(See Bereg et al. (2018, Theorem 3)) Suppose a permutation array $P \subset S_n$ has Hamming distance d. Let $Q \subseteq S_{n-2}$ denote the permutation array obtained from P by applying the contraction operation two times.*

(i) The Hamming distance of Q is at least $d-6$.

(ii) Suppose, for any $\pi, \sigma \in P$, the cycle decomposition of $\pi^{-1}\sigma$ contains no 3-cycle and no 5-cycle. Then the Hamming distance of Q is at least $d-4$.

It follows that knowing whether a permutation array contains either a 3-cycle or 5-cycle is important to the application of this theorem. Fortunately, if our PA is formed from a permutation group, Lagrange's theorem can be applied to show that in order for a group to contain a k-cycle, the order of the group must be a multiple of k (Bereg et al., 2018). Since we can easily determine the order of known permutation groups, this leads to the results of Corollary 5 and Theorem 6.

Corollary 5. *(See Bereg et al. (2018, Corollary 4))*

(i) For each prime power n such that $n \equiv 2 \pmod 3$,

$$M(n-1, n-3) \geq n(n-1).$$

(ii) For each prime power n such that $n \equiv 2 \pmod 3$ and $n \not\equiv 0, 1 \pmod 5$,

$$M(n-2, n-5) \geq n(n-1).$$

Theorem 6. *(See Bereg et al. (2018, Theorem 4)) For each prime power n such that $n \equiv 2 \pmod 3$,*

$$M(n, n-3) \geq (n+1)n(n-1).$$

Corollary 5 and Theorem 6 are obtained from the application of the contraction operation to the permutations groups $AGL(1, n)$ and $PGL(2, n)$ respectively. Since the order of these groups are all based on the prime power n, you can use n itself, along with some properties of each group, to determine if a 3-cycle or 5-cycle exists in the resulting PA.

1.2.1 Contraction Graphs

When a PA is formed by a group and $n \equiv 2 \pmod 3$, it is easy to determine the Hamming distance of the resulting PA after it has been contracted either once or twice. For the case of $n \equiv 1 \pmod 3$, additional analysis must take place, which can be done through a *contraction graph* (Bereg et al., 2019).

Let π be a permutation in S_n. Define $\pi^{\triangle}$ as follows where $0 \leq x \leq n-1$:

$$\pi^{\triangle}(x) = \begin{cases} \pi(n-1), & \text{if } x = \pi^{-1}(n-1), \\ n-1, & \text{if } x = n-1, \\ \pi(x), & \text{otherwise.} \end{cases}$$

We can see that $\pi^{\triangle}$ is similar to π^{CT}, but it keeps the symbol $n-1$ at position $n-1$, thus it remains of length n. Similarly, if we have a PA A, we define $A^{\triangle}$ as:

$$A^{\triangle} = \{\pi^{\triangle} \mid \pi \in A\}.$$

Let A be a PA with $hd(A) = d$. Define the contraction graph for A, denoted $G_A^{\triangle}$, as follows:

$$V(G_A^{\triangle}) = A,$$
$$E(G_A^{\triangle}) = \{\pi\sigma \mid \pi, \sigma \in A, hd(\pi^{\triangle}, \sigma^{\triangle}) = d-3\}.$$

We can observe that the edges in $G_A^{\triangle}$ correspond to the 3-cycles in A. Furthermore, since $hd(A^{\triangle}) \geq d-3$, it would follow that an independent set I in $G_A^{\triangle}$ satisfies $hd(I^{\triangle}) \geq d-2$. Since each $\pi \in I^{\triangle}$ has the symbol $n-1$ in the position $n-1$, this symbol can simply be deleted from every permutation without affecting the Hamming distance. Thus, finding a large independent set I in $G_A^{\triangle}$ can be used to maintain a larger Hamming distance when contracting PAs which contain a 3-cycle (Bereg et al., 2019).

1.2.2 Contraction Graph for $AGL(1, n)$

Consider the group $AGL(1, n)$. Since this group has order $n(n-1)$, if $n \equiv 1 \pmod 3$, its order will be divisible by 3, and it is possible that it contains a 3-cycle. We therefore want to consider the contraction graph of $AGL(1, n)$, denoted $G^{\triangle}_{AGL(1,n)}$.

Lemma 7. *(See Bereg et al. (2019, Lemma 4)) Let π and σ be vertices of the graph $G^{\triangle}_{AGL(1,n)}$, $n \equiv 1 \pmod 3$, with $\sigma(x) = ax + r$ and $\pi(x) = bx + s$.*

(i) If $a \neq b$, then $hd(\pi, \sigma) = n-1$.

(ii) If $\pi(n-1) = n-1$, then π is an isolated point in $G^{\triangle}_{AGL(1,n)}$. There are $n-1$ points π satisfying $\pi(n-1) = n-1$.

(iii) Suppose π and σ are neighbors in $G^{\triangle}_{AGL(1,n)}$. Then

(a) $hd(\pi, \sigma) = n - 1$, and $hd(\pi^{\triangle}, \sigma^{\triangle}) = hd(\pi, \sigma) - 3$, and

(b) $\frac{a}{b}$ and $\frac{b}{a}$ are the distinct roots of the quadratic $t^2 + t + 1 = 0$ over $\mathbb{F}_n$.

Lemma 7 helps establish which vertices in $G^{\triangle}_{AGL(1,n)}$ are isolated, which are connected, and the length of the cycle each connected vertex belongs to. This then leads to Theorem 8.

Theorem 8. *(See Bereg et al. (2019, Theorem 6)) Let n be a prime power with $n \equiv 1 \pmod 3$. Then the connected components of $G^{\triangle}_{AGL(1,n)}$ are as follows.*

(i) There are $q - 1$ isolated points, these being the points π satisfying $\pi(n - 1) = n - 1$.

(ii) If n is odd, then each non-isolated point component is a cycle of length 6.

(iii) If n is even, then each non-isolated point component is a cycle of length 3.

From Theorem 8, we can construct an independent set in $G^{\triangle}_{AGL(1,n)}$ by taking all isolated points and adding 3 vertices from each cycle of 6 if n is odd, or 1 vertex from each cycle of 3 if n is even. This then leads to additional bounds for $M(n, d)$, as given in Corollary 9.

Corollary 9. *(See Bereg et al. (2019, Corollary 7)) Let n be a prime power with $n \equiv 1 \pmod 3$ and $n \geq 7$. Then*

(i) if n is odd, then $M(n - 1, n - 3) \geq (n^2 - 1)/2$, and

(ii) if n is even, then $M(n - 1, n - 3) \geq (n - 1)(n + 2)/3$.

This follows directly from Theorem 8 by applying the contraction operation a single time to a PA formed from $AGL(1, n)$.

1.2.3 Contraction Graph for $PGL(2, n)$

Since $PGL(2, n)$ consists of permutations on $n + 1$ symbols, the definition of $\pi^{\triangle}$ must be slightly adjusted. Instead, of placing the symbol $n - 1$ at position $n - 1$, we instead place the symbol ∞, sometimes represented by n, at position n. Consider this example for $n = 5$,

$$(0\ 1\ \infty\ 2\ 3\ 4) \mapsto (0\ 1\ 4\ 2\ 3\ \infty), \text{ or}$$

$$(0\ 1\ 5\ 2\ 3\ 4) \mapsto (0\ 1\ 4\ 2\ 3\ 5).$$

Since the Hamming distance of $PGL(2, n)$ is $n - 1$, then for any $\pi, \sigma \in PGL(2, n)$, we know $hd(\pi^{\triangle}, \sigma^{\triangle}) \geq n - 4$. The objective is the same as it was for $AGL(1, n)$, to construct a contraction graph for $PGL(2, n)$ and find a large independent set I such that $hd(I^{\triangle}) \geq q - 3$. However, the process is much more involved.

Rather than look at the entire contraction graph $G^{\triangle}_{PGL(2,n)}$, it becomes more prudent to only consider a proper subset $P \subset PGL(2, n)$.

Definition 10. *(See Bereg et al. (2019, Definition 8)) Fix a prime power n.*

1. *Let $k, r, i \in \mathbb{F}_n$ with $r \neq 0$. Define the function $f : \mathbb{P}^1(\mathbb{F}_n) \to \mathbb{P}^1(\mathbb{F}_n)$ by $f(x) = k + \frac{r}{x-i}$ for $x \notin \{i, \infty\}$, while $f(\infty) = k$ and $f(i) = \infty$.*

2. *Let $P = \{k + \frac{r}{x-i} \mid k, r, i \in \mathbb{F}_n, r \neq 0\}$ be the set of all functions defined in (1).*

It can be shown that $|P| = n^2(n - 1)$, and $P \subset PGL(2, n)$ such that,

$$P = \{\pi \in PGL(2, n) \mid \pi(x) = \frac{ax + b}{cx + d}, c \neq 0\}.$$

It can also be shown that for $\pi \in PGL(2, n)$, $\pi(\infty) = \infty \iff c = 0$. The $n(n - 1)$ permutations that meet this condition are actually the set of isolated points in $G^{\triangle}_{PGL(2,n)}$. Since our definition of P excludes all permutations where $c = 0$, the contraction graph $G^{\triangle}_{P}$ is actually the subgraph of $G^{\triangle}_{PGL(2,n)}$ induced by its set of edges. The proof of these points yields Corollary 11.

Corollary 11. *(See Bereg et al. (2019, Corollary 12)) Let n be an odd prime power with $n \equiv 1 \pmod 3$ and $n \geq 13$.*

(i) Let $\pi, \sigma \in P$ with $\pi(x) = a + \frac{r}{x-i}$, $\sigma(x) = b + \frac{s}{x-j}$, $r, x \neq 0$. Then $\pi\sigma \in E(G^{\triangle}_{PGL(2,n)})$ $\iff$ $r = s$ and $(b-a)(j-i) = r$.

(ii) $\pi \in PGL(2,n)$ is an isolated point in $G^{\triangle}_{PGL(2,n)}$ $\iff$ $\pi(\infty) = \infty$.

Analysis of $G^{\triangle}_{PGL(2,n)}$ then becomes easier if we consider partitions of P defined as follows:

$$P_r = \{a + \frac{r}{x-i} \mid a, i \in \mathbb{F}_n\}.$$

By this definition we can immediately see there are $n-1$ such partitions, $|P_r| = n^2$, and $P = \cup_{r=1}^{n-1} P_r$.

By breaking down $G^{\triangle}_{PGL(2,n)}$ into subgraphs induced by some partition P_r, denoted $[P_r]$, we can see that any two $[P_r]$ are isomorphic, and each $[P_r]$ is a regular graph of degree $n-1$. With this we can fully identify the connected components of $G^{\triangle}_{PGL(2,n)}$.

Theorem 12. *(See Bereg et al. (2019, Theorem 14)) Let n be an odd prime power with $n \equiv 1 \pmod 3$ and $n \geq 13$. Then the connected components of $G^{\triangle}_{PGL(2,n)}$ are as follows.*

(i) The isolated points - these are of the form $\pi(x) = ax + b, a \neq 0$, and there are $n(n-1)$ of them.

(ii) The $(n-1)$ many connected components $[P_r]$ induced by the sets P_r.

Even though we can define the connected components of $G^{\triangle}_{PGL(2,n)}$, finding an independent set in each partition $[P_r]$ remains a challenge. The approach taken in Bereg et al. (2019) is to show that each partition is 3-colorable, thus allowing the application of Theorem 13 from Alon (1996) which sets a lower bound on the independence number of the graph, that is, the maximum number of vertices in an independent set in G, denoted $\alpha(G)$.

Theorem 13. *(See Alon (1996, Theorem 1.1)) Let $G = (V, E)$ be a graph on n vertices with average degree $t \geq 1$ in which for every vertex $v \in V$ the induced subgraph on the set of all neighbors of v is r-colorable. Then, the independence number of G is at least $\frac{c}{\log(r+1)} \frac{n}{t} \log t$, for some absolute positive constant c.*

Since we know each $[P_r]$ is 3-colorable, contains n^2 vertices, and is $(n-1)$-regular, Theorem 13 tells us,

$$\begin{aligned} \alpha([P_r]) &\geq \frac{c}{\log(4)} \frac{n^2}{n-1} \log(n-1), \\ &\geq kn \log n, \end{aligned}$$

for some constant k. If we consider this for all $n-1$ partitions P_r, and add the $n(n-1)$ independent points in $G^{\triangle}_{PGL(2,n)}$, we obtain the bounds from Corollary 14.

Corollary 14. *(See Bereg et al. (2019, Corollary 16)) Let n be an odd prime power with $n \equiv 1 \pmod 3$ and $n \geq 13$.*

(i) $\alpha(G^{\triangle}_{PGL(2,n)}) \geq kn^2 \log n$ *for some constant k.*

(ii) $M(n, n-3) \geq kn^2 \log n$ *for some constant k.*

1.2.4 Contraction of Mathieu Groups

While the five Mathieu groups, $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$, are important in group theory, the results obtained by performing the contraction operation on them are limited since they only exist for those 5 values of n, rather than infinitely many prime powers n. However, they do provide additional results for $M(n, d)$ which were given in Bereg et al. (2019). Note that $hd(M_{12}) = 8$ and $hd(M_{24}) = 16$.

Proposition 15. *(See Bereg et al. (2019, Proposition 17))*

(i) $hd(M_{12}^{CT}) \geq 6$.

(ii) $M(11, 6) \geq |M_{12}| = 95{,}040$.

(iii) $M(10, 6) \geq \frac{|M_{12}|}{11} = 8{,}640$.

Proposition 16. *(See Bereg et al. (2019, Proposition 18))*

(i) $hd(M_{24}^{CT}) \geq 14$.

(ii) $M(23, 14) \geq |M_{24}| = 244{,}823{,}040$.

(iii) $M(22, 14) \geq \frac{|M_{24}|}{23} = 10{,}644{,}480$.

(iv) $M(21, 14) \geq \frac{|M_{24}|}{23 \cdot 22} = 483{,}840$.

Proof of these propositions can be done by analyzing the cycle structure of each group, similar to the approach taken with $AGL(1, n)$, and such proofs are available in Bereg et al. (2019). However, since we are only considering the two specific groups M_{12} and M_{24}, verification can be achieved programmatically using GAP (Groups, Algorithms, Programming), a system for computational discrete algebra which emphasizes computational group theory.

1.3 Partition and Extension

Let $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. *Partition and extension* is a technique which transforms a PA on $\mathbb{Z}_n$ with Hamming distance $d-1$ into a PA on $n+1$ symbols with Hamming distance d.

Let s be a positive integer. Let $(M_1, M_2, \ldots, M_s)$ be an ordered list of pairwise disjoint PAs on $\mathbb{Z}_n$. Let $\mathcal{P} = (P_1, P_2, \ldots, P_s)$ and $\mathcal{Q} = (Q_1, Q_2, \ldots, Q_s)$ be two ordered lists of subsets of $\mathbb{Z}_n$ such that the sets in $\mathcal{P}$ and $\mathcal{Q}$ form partitions of $\mathbb{Z}_n$. For each set M_i, P_i is the set of positions, and Q_i is the set of symbols to be replaced by the new symbol n. When a permutation $\pi \in M_i$ has a symbol $q \in Q_i$ at position $p \in P_i$, π is extended, forming permutation π' on $n+1$ symbols, by placing symbol q at the end of the permutation and placing symbol n at position p (Bereg et al., 2020).

Given a permutation π on $\mathbb{Z}_n$, define the extension of π by position k, denoted $ext_k(\pi) = \pi'$ as follows:

$$\pi'(i) = \begin{cases} n, & \text{if } i = k, \\ \pi(k), & \text{if } i = n, \\ \pi(i), & \text{otherwise.} \end{cases}$$

For each i, let $covered(M_i)$ be the subset of M_i defined by:

$$covered(M_i) = \{\pi \in M_i \mid \exists p \in P_i, \pi(p) \in Q_i\}.$$

Any permutation π must be covered to be included in the set of permutations extended to $\mathbb{Z}_{n+1}$. More plainly, π must contain one of the designated symbols at one of the designated positions in order to be extended. If it so happens that π contains more than one pair of agreeing symbols and positions, you may arbitrarily choose one to cover π. It should also be clear that since not all permutations may be covered, the new PA resulting from partition and extension will likely be smaller than the original PA.

When constructing the PAs M_i for $1 \leq i \leq s$, you may also include an additional PA M_{s+1} which does not have a corresponding P_{s+1} or Q_{s+1}. The partition and extension operation extends permutations in M_{s+1} by simply appending the new symbol n to the end of them, thus every permutation in M_{s+1} is used. We can therefore define the new list $\mathcal{M} = (M_1, M_2, \ldots, M_s, M_{s+1})$, which contains the extra set M_{s+1} (Bereg et al., 2020).

Define the triple $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$ as a *distance-d partition system* for $\mathbb{Z}_n$ which satisfies the following properties:

(i) $\forall M_i \in M,\ hd(M_i) \geq d$, and

(ii) $\forall i, j\ (1 \leq i < j \leq s+1),\ hd(M_i, M_j) \geq d - 1$.

The partition and extension operation uses the sets P_i and Q_i to modify the covered permutations in M_i, for $1 \leq i \leq s$, to create a new PA on $\mathbb{Z}_{n+1}$ with distance d. Let $ext(M_i)$ be

the set of permutations on $\mathbb{Z}_{n+1}$ defined as,

$$ext(M_i) = \{ext(\pi) \mid \pi \in covered(M_i)\}.$$

Let $ext(M_{s+1})$ be the set of permutations on $\mathbb{Z}_{n+1}$ defined by appending the symbol n to the end of each permutation in M_{s+1}. Let $ext(\Pi)$ be the set of permutations on $\mathbb{Z}_{n+1}$ defined as,

$$ext(\Pi) = \bigcup_{i=1}^{s+1} ext(M_i).$$

We can observe that,

$$|ext(\Pi)| = \sum_{i=1}^{s+1} |ext(M_i)|.$$

Theorem 17. *(See Bereg et al. (2020, Theorem 1)) Let d be a positive integer. Let $\Pi = (\mathcal{M}, \mathcal{P}, \mathcal{Q})$ be a distance-d partition system for $\mathbb{Z}_n$, with $\mathcal{M} = (M_1, M_2, \ldots, M_{s+1})$ for some positive integer s. Let $ext(\Pi)$ be the PA on $\mathbb{Z}_{n+1}$ created by partition and extension. Then,*

$$hd(ext(\Pi)) \geq d.$$

Consider this example of partition and extension from Bereg et al. (2020) with permutations on $\mathbb{Z}_4$ and $d = 3$.

$$\mathcal{M} = (M_1, M_2, M_3)$$

$$\mathcal{P} = (\{0, 2\}, \{1, 3\})$$

$$\mathcal{Q} = (\{0, 1\}, \{2, 3\})$$

Initial Permutations in Π Modified Permutations in $ext(\Pi)$

$$M_1 = \begin{bmatrix} 0\,1\,2\,3 \\ 1\,0\,3\,2 \\ 2\,3\,0\,1 \\ 3\,2\,1\,0 \end{bmatrix} \qquad ext(M_1) = \begin{bmatrix} 4\,1\,2\,3\,0 \\ 4\,0\,3\,2\,1 \\ 2\,3\,4\,1\,0 \\ 3\,2\,4\,0\,1 \end{bmatrix}$$

$$M_2 = \begin{bmatrix} 0\,2\,3\,1 \\ 1\,3\,2\,0 \\ 2\,0\,1\,3 \\ 3\,1\,0\,2 \end{bmatrix} \qquad ext(M_2) = \begin{bmatrix} 0\,4\,3\,1\,2 \\ 1\,4\,2\,0\,3 \\ 2\,0\,1\,4\,3 \\ 3\,1\,0\,4\,2 \end{bmatrix}$$

$$M_3 = \begin{bmatrix} 0\,3\,1\,2 \\ 1\,2\,0\,3 \\ 2\,1\,3\,0 \\ 3\,0\,2\,1 \end{bmatrix} \qquad ext(M_3) = \begin{bmatrix} 0\,3\,1\,2\,4 \\ 1\,2\,0\,3\,4 \\ 2\,1\,3\,0\,4 \\ 3\,0\,2\,1\,4 \end{bmatrix}$$

In this example, M_1 is actually the cyclic subgroup of $AGL(1,4)$, while M_2 and M_3 are each cosets. The blue symbols are the symbols of Q_i that are in a position in P_i, while the new symbol n is marked in red. We can observe that for any i, $hd(M_i) \geq 4$, and for $i \neq j$, $hd(M_i, M_j) \geq 3$. Therefore, by Theorem 17, $hd(ext(\Pi)) \geq 4$.

This partition and extension technique has been shown in Bereg et al. (2017) to generate competitive results for $M(n,d)$ in three general situations:

1. $M(n+1,n)$ where n is a prime power,
2. $M(n+1,n)$ where n is not a prime power, and the current bound for $M(n,n-1)$ is given by mutually orthogonal Latin squares (MOLS), and

3. $M(n+1, d)$ where G is a group of permutations over $\mathbb{Z}_n$, $hd(G) = d$, and distinct cosets M_i, M_j of G have $hd(M_i, M_j) \geq d - 1$.

The previous example with permutations on $\mathbb{Z}_4$ is an example of situation (1). We know PAs formed from $AGL(1, n)$ have a Hamming distance of $n - 1$, and we can split these PAs into cyclic subgroups to form the sets M_1 to M_{s+1}, each with Hamming distance n. Performing partition and extension on such a set leads to a new PA on $n + 1$ symbols with Hamming distance n.

Situation (2) is similar in practice to situation (1), but the subsets M_1 to M_{s+1} are formed from mutually orthogonal Latin squares, which exist for any positive integer n. A Latin square is an $n \times n$ matrix on n symbols, each appearing exactly once in each row and once in each column. We can consider each row of the matrix to be a permutation, and the set of permutations given by a single Latin square has Hamming distance n. Two Latin squares are mutually orthogonal if when superimposed, the ordered pairs formed at each position are all distinct. It has been shown in Colbourn et al. (2004) that a set of k MOLS of order n can be used to form a PA of size kn with Hamming distance $n - 1$, making MOLS suitable for partition and extension.

Situation (3) is also similar to situation (1), but rather than use $AGL(1, n)$, other groups are used, for example, $PGL(2, n)$. The sets M_1 to M_{s+1} are formed from left cosets of the group, with coset representatives carefully chosen to meet the Hamming distance requirements. One result given in Bereg et al. (2017) uses $G = PGL(2, 8)$ to extend the result $M(9, 7) = 504$. The Frobenius mappings $f_1(x) = x^2$ and $f_2(x) = x^4$ are used as left cosets to form the subsets $M_1 = G, M_2 = f_1G$, and $M_3 = f_2G$. The partitions $\mathcal{P}$ and $\mathcal{Q}$ are chosen to maximize coverage of $\mathcal{M}$, leading to the new result $M(10, 7) \geq 1{,}504$. Other competitive $M(n, d)$ results from Bereg et al. (2017) obtained by using partition and extension are given in Table 1.4.

Table 1.4. $M(n, d)$ Results from Partition and Extension (Bereg et al., 2017).

New Result	Extended From
$M(10, 7) \geq 1{,}504$	$PGL(2, 8)$
$M(18, 14) \geq 12{,}240$	$PGL(2, 16)$
$M(26, 25) \geq 130$	$AGL(1, 25)$
$M(30, 29) \geq 170$	$AGL(1, 29)$
$M(33, 32) \geq 183$	$AGL(1, 32)$
$M(118, 117) \geq 936$	MOLS(117)

1.3.1 Sequential Partition and Extension

Sequential partition and extension takes the approach of splitting a PA on $\mathbb{Z}_n$ with Hamming distance d into several disjoint PAs. Partition and extension is then applied to each of these subsets individually, creating several new PAs on $n + 1$ symbols with Hamming distance d. These new PAs are then used in a second iteration of partition and extension to create a larger PA on $n + 2$ symbols with Hamming distance d (Bereg et al., 2020).

Let $M^* = \{M_1, M_2, \ldots, M_t\}$, for some t, be a collection of PAs on $\mathbb{Z}_n$ which satisfy properties (i) and (ii) of a distance-d partition system. Let $(\mathcal{M}_1, \mathcal{M}_2, \ldots, \mathcal{M}_m)$ be ordered set of subsets of M^* such that each $\mathcal{M}_i$ contains some number of PAs from M^*, and any two $\mathcal{M}_i$ and $\mathcal{M}_j$ are pairwise disjoint.

Let $\{\Pi_1, \Pi_2, \ldots, \Pi_m\}$ be a collection of distance-d partition systems on $\mathbb{Z}_n$, where for $1 \leq i \leq m$, $\Pi_i = (\mathcal{M}_i, \mathcal{P}_i, \mathcal{Q}_i)$, and $\mathcal{M}_i \subseteq M^*$. If for all $1 \leq i < j \leq m$, $\mathcal{M}_i$ and $\mathcal{M}_j$ are pairwise disjoint, then $\{\Pi_1, \Pi_2, \ldots, \Pi_m\}$ is pairwise disjoint.

Partition and extension is then performed on each Π_i to create a new PA $ext(\Pi_i)$ on $\mathbb{Z}_{n+1}$ with Hamming distance d, resulting in a set of new PAs, $\{ext(\Pi_1), ext(\Pi_2), \ldots, ext(\Pi_m)\}$. Furthermore, if the distance-d partition systems $\{\Pi_1, \Pi_2, \ldots, \Pi_m\}$ are pairwise disjoint, then the new PAs $\{ext(\Pi_1), ext(\Pi_2), \ldots, ext(\Pi_m)\}$ will also be pairwise disjoint. This leads to the results of Corollary 18.

Corollary 18. *(See Bereg et al. (2020, Corollary 4)) Let* $\Pi_1 = (\mathcal{M}_1, \mathcal{P}_1, \mathcal{Q}_1)$, $\Pi_2 = (\mathcal{M}_2, \mathcal{P}_2, \mathcal{Q}_2)$, $\ldots$, $\Pi_m = (\mathcal{M}_m, \mathcal{P}_m, \mathcal{Q}_m)$ *be a collection of pairwise disjoint distance-d partition systems, for some* $m > 1$, *where* $hd(\mathcal{M}_i, \mathcal{M}_j) \geq d - 1$, *for all* i, j $(1 \leq i < j \leq m)$. *Let* $A = ext(\Pi_1) \cup ext(\Pi_2) \cup \cdots \cup ext(\Pi_m)$. *Then*

(i) $\forall i, j$ $(1 \leq i < j \leq m)$, $hd(ext(\Pi_i), ext(\Pi_j)) \geq d - 1$,

(ii) A *is a PA on* $\mathbb{Z}_{n+1}$,

(iii) $|A| = \sum_{i=1}^{m} |ext(\Pi_i)|$, *and*

(iv) $hd(A) \geq d - 1$.

From Corollary 18 we can observe that sets $\{ext(\Pi_1), ext(\Pi_2), \ldots, ext(\Pi_m)\}$ satisfy properties (i) and (ii) of a distance-d partition system, allowing us to perform a second iteration of partition and extension. Let $\mathbb{M} = \{ext(\Pi_1), ext(\Pi_2), \ldots, ext(\Pi_m)\}$, making it a collection of PAs on $\mathbb{Z}_{n+1}$. Let $\mathbb{P}$ and $\mathbb{Q}$ be partitions of $\mathbb{Z}_{n+1}$ such that $\Psi = (\mathbb{M}, \mathbb{P}, \mathbb{Q})$ is a distance-d partition system on $\mathbb{Z}_{n+1}$. If we perform partition and extension on Ψ, by Theorem 17 we then have $ext(\Psi)$ as a PA on $\mathbb{Z}_{n+2}$ with $hd(ext(\Psi)) \geq d$. This leads to the result of Theorem 19.

Theorem 19. *(See Bereg et al. (2020, Theorem 5)) Sequential partition and extension on a collection* $\{\Pi_1, \Pi_2, \ldots, \Pi_m\}$, *of pairwise disjoint distance-d partition systems on* $\mathbb{Z}_n$, *results in a new PA on* $\mathbb{Z}_{n+2}$ *with Hamming distance* d.

1.3.2 Parallel Partition and Extension

Let r be some positive integer. *Parallel partition and extension* extends a PA on $\mathbb{Z}_n$ to one on $\mathbb{Z}_{n+r}$, but does so simultaneously rather than through sequential iterations. Let A be a PA on $\mathbb{Z}_n$ with $hd(A) \geq d - r$ for some value d. Partition A into $k = 2r$ blocks of permutations, $B_0, B_1, \ldots, B_{k-1}$ which satisfy the following properties:

(i) $\forall B_i \in A,\ hd(B_i) \geq d$, and

(ii) $\forall B_i, B_j \in A, i \neq j,\ hd(B_i, B_j) \geq d - r$.

Parallel partition and extension creates a new PA A' on $\mathbb{Z}_{n+r}$ with $hd(A') \geq d$ by inserting the symbols $\{n, n+1, \ldots, n+r-1\}$ (Bereg et al., 2020).

Define $\textsc{shift}(n, r, 0)$ as the sequence $(n, n+1, n+2, \ldots, n+r-1)$, and for each integer t, $\textsc{shift}(n, r, t)$ is the left cyclic shift of the sequence by $t \pmod r$ positions. For example, if $n = 7$ and $r = 5$, $\textsc{shift}(7, 5, 0) = (7, 8, 9, 10, 11)$, and $\textsc{shift}(7, 5, 2) = (9, 10, 11, 7, 8)$.

To create the new PA A', you first modify the blocks $B_0, B_1, \ldots, B_{r-1}$. For all B_t, $0 \leq t < r$, create a new block B'_t as follows:

(i) Replace the first r symbols of each permutation in B_t with the symbols $\textsc{shift}(n, r, t)$.

(ii) Append the r symbols that were replaced to the end of their permutation in their original order, placing them into positions $n, n+1, \ldots, n+r-1$.

Then for all B_u, $r \leq u < 2r$, create a new block B'_u by:

(iii) Append the sequence $\textsc{shift}(n, r, u)$ to the end of each permutation, placing it in positions $n, n+1, \ldots, n+r-1$.

Together, the blocks B'_t $(0 \leq t < r)$ and $B'_u (r \leq u < 2r)$ form the new PA A' on $\mathbb{Z}_{n+r}$, with $hd(A') \geq d$. Results for $M(n, d)$ from parallel partition and extension are given in Theorem 20.

Theorem 20. *(See Bereg et al. (2020, Theorem 6)) Let A be a PA on $\mathbb{Z}_n$ comprising $2r$ blocks for some r. Denote the blocks by $B_0, B_1, \ldots, B_{2r-1}$, so that $A = \cup_{i=0}^{2r-1} B_i$. If each block B_i has Hamming distance at least d, and the Hamming distance of the entire set A is at least $d - r$, then parallel partition and extension on A results in a new PA A' on $\mathbb{Z}_{n+r}$ that exhibits*

$$M(n + r, d) \geq \sum_{i=0}^{2r-1} |B_i|.$$

Table 1.1 gives an example of parallel partition and extension for PA A on $\mathbb{Z}_9$ with $hd(A) \geq 6$, extending to A' on $\mathbb{Z}_{12}$. Symbols that are repositioned are colored blue, while new symbols being introduced are in red. Each block B_i has $hd(B_i) \geq 9$, so by Theorem 20 we know $hd(A') \geq 9 - 3 = 6$.

Bereg et al. (2020) also describes an improved version of parallel partition and extension which does not limit the number of blocks to $2r$. Instead, it uses a covering system much like the basic implementation of partition and extension. The key difference is that is uses a (d, r)-*partition system* in which a permutation must have r symbols covered in order to be included in the extended block. Using this method, there is no restriction on the number of blocks you can form. However, it becomes more challenging to find a good partition system.

The authors employed several techniques to create partition systems, including a greedy algorithm, encoding the problem as an integer linear program to solve with an optimizer, and utilizing the coset properties of various groups. Results varied depending on the specific PA to be extended, but all techniques had merit. Several large tables with competitive bounds for $M(n, d)$ obtained from the various partition and extension techniques can be found in Bereg et al. (2020).

1.4 Kronecker Product

Kronecker product is a well-known matrix operation used in linear algebra, combinatorics, and several other areas of mathematics. Bereg et al. (2017) introduces a modified version of the Kronecker product operation which can be used on two PAs A and B, denoted $(A \otimes B)$. If A is a PA on l symbols and B is a PA on m symbols, then $(A \otimes B)$ is a new PA on lm symbols.

Initial Permutations in A	Modified Permutations in A'
$B_0 = \begin{bmatrix} 0&1&2&3&4&5&6&7&8 \\ 1&5&8&4&6&0&3&2&7 \\ 2&8&6&1&5&7&0&4&3 \\ 3&4&1&7&2&6&8&0&5 \\ 4&6&5&2&8&3&7&1&0 \\ 5&0&7&6&3&1&4&8&2 \\ 6&3&0&8&7&4&2&5&1 \\ 7&2&4&0&1&8&5&3&6 \\ 8&7&3&5&0&2&1&6&4 \end{bmatrix}$	$B'_0 = \begin{bmatrix} 9&10&11&3&4&5&6&7&8&0&1&2 \\ 9&10&11&4&6&0&3&2&7&1&5&8 \\ 9&10&11&1&5&7&0&4&3&2&8&6 \\ 9&10&11&7&2&6&8&0&5&3&4&1 \\ 9&10&11&2&8&3&7&1&0&4&6&5 \\ 9&10&11&6&3&1&4&8&2&5&0&7 \\ 9&10&11&8&7&4&2&5&1&6&3&0 \\ 9&10&11&0&1&8&5&3&6&7&2&4 \\ 9&10&11&5&0&2&1&6&4&8&7&3 \end{bmatrix}$
$B_1 = \begin{bmatrix} 1&3&6&7&5&8&2&4&0 \\ 5&4&3&2&0&7&8&6&1 \\ 8&1&0&4&7&3&6&5&2 \\ 4&7&8&0&6&5&1&2&3 \\ 6&2&7&1&3&0&5&8&4 \\ 0&6&4&8&1&2&7&3&5 \\ 3&8&2&5&4&1&0&7&6 \\ 2&0&5&3&8&6&4&1&7 \\ 7&5&1&6&2&4&3&0&8 \end{bmatrix}$	$B'_1 = \begin{bmatrix} 10&11&9&7&5&8&2&4&0&1&3&6 \\ 10&11&9&2&0&7&8&6&1&5&4&3 \\ 10&11&9&4&7&3&6&5&2&8&1&0 \\ 10&11&9&0&6&5&1&2&3&4&7&8 \\ 10&11&9&1&3&0&5&8&4&6&2&7 \\ 10&11&9&8&1&2&7&3&5&0&6&4 \\ 10&11&9&5&4&1&0&7&6&3&8&2 \\ 10&11&9&3&8&6&4&1&7&2&0&5 \\ 10&11&9&6&2&4&3&0&8&7&5&1 \end{bmatrix}$
$B_2 = \begin{bmatrix} 3&5&7&2&6&0&8&4&1 \\ 4&0&2&8&3&1&7&6&5 \\ 1&7&4&6&0&2&3&5&8 \\ 7&6&0&1&8&3&5&2&4 \\ 2&3&1&5&7&4&0&8&6 \\ 6&1&8&7&4&5&2&3&0 \\ 8&4&5&0&2&6&1&7&3 \\ 0&8&3&4&5&7&6&1&2 \\ 5&2&6&3&1&8&4&0&7 \end{bmatrix}$	$B'_2 = \begin{bmatrix} 11&9&10&2&6&0&8&4&1&3&5&7 \\ 11&9&10&8&3&1&7&6&5&4&0&2 \\ 11&9&10&6&0&2&3&5&8&1&7&4 \\ 11&9&10&1&8&3&5&2&4&7&6&0 \\ 11&9&10&5&7&4&0&8&6&2&3&1 \\ 11&9&10&7&4&5&2&3&0&6&1&8 \\ 11&9&10&0&2&6&1&7&3&8&4&5 \\ 11&9&10&4&5&7&6&1&2&0&8&3 \\ 11&9&10&3&1&8&4&0&7&5&2&6 \end{bmatrix}$
$B_3 = \begin{bmatrix} 4&2&7&8&0&1&3&5&6 \\ 6&8&2&7&1&5&4&0&3 \\ 5&6&4&3&2&8&1&7&0 \\ 2&1&0&5&3&4&7&6&8 \\ 8&5&1&0&4&6&2&3&7 \\ 3&7&8&2&5&0&6&1&4 \\ 7&0&5&1&6&3&8&4&2 \\ 1&4&3&6&7&2&0&8&5 \\ 0&3&6&4&8&7&5&2&1 \end{bmatrix}$	$B'_3 = \begin{bmatrix} 4&2&7&8&0&1&3&5&6&9&10&11 \\ 6&8&2&7&1&5&4&0&3&9&10&11 \\ 5&6&4&3&2&8&1&7&0&9&10&11 \\ 2&1&0&5&3&4&7&6&8&9&10&11 \\ 8&5&1&0&4&6&2&3&7&9&10&11 \\ 3&7&8&2&5&0&6&1&4&9&10&11 \\ 7&0&5&1&6&3&8&4&2&9&10&11 \\ 1&4&3&6&7&2&0&8&5&9&10&11 \\ 0&3&6&4&8&7&5&2&1&9&10&11 \end{bmatrix}$
$B_4 = \begin{bmatrix} 3&5&7&8&4&6&0&1&2 \\ 4&0&2&7&6&3&1&5&8 \\ 1&7&4&3&5&0&2&8&6 \\ 7&6&0&5&2&8&3&4&1 \\ 2&3&1&0&8&7&4&6&5 \\ 6&1&8&2&3&4&5&0&7 \\ 8&4&5&1&7&2&6&3&0 \\ 0&8&3&6&1&5&7&2&4 \\ 5&2&6&4&0&1&8&7&3 \end{bmatrix}$	$B'_4 = \begin{bmatrix} 3&5&7&8&4&6&0&1&2&10&11&9 \\ 4&0&2&7&6&3&1&5&8&10&11&9 \\ 1&7&4&3&5&0&2&8&6&10&11&9 \\ 7&6&0&5&2&8&3&4&1&10&11&9 \\ 2&3&1&0&8&7&4&6&5&10&11&9 \\ 6&1&8&2&3&4&5&0&7&10&11&9 \\ 8&4&5&1&7&2&6&3&0&10&11&9 \\ 0&8&3&6&1&5&7&2&4&10&11&9 \\ 5&2&6&4&0&1&8&7&3&10&11&9 \end{bmatrix}$
$B_5 = \begin{bmatrix} 0&4&2&5&6&1&7&3&8 \\ 1&6&8&0&3&5&2&4&7 \\ 2&5&6&7&0&8&4&1&3 \\ 3&2&1&6&8&4&0&7&5 \\ 4&8&5&3&7&6&1&2&0 \\ 5&3&7&1&4&0&8&6&2 \\ 6&7&0&4&2&3&5&8&1 \\ 7&1&4&8&5&2&3&0&6 \\ 8&0&3&2&1&7&6&5&4 \end{bmatrix}$	$B'_5 = \begin{bmatrix} 0&4&2&5&6&1&7&3&8&11&9&10 \\ 1&6&8&0&3&5&2&4&7&11&9&10 \\ 2&5&6&7&0&8&4&1&3&11&9&10 \\ 3&2&1&6&8&4&0&7&5&11&9&10 \\ 4&8&5&3&7&6&1&2&0&11&9&10 \\ 5&3&7&1&4&0&8&6&2&11&9&10 \\ 6&7&0&4&2&3&5&8&1&11&9&10 \\ 7&1&4&8&5&2&3&0&6&11&9&10 \\ 8&0&3&2&1&7&6&5&4&11&9&10 \end{bmatrix}$

Figure 1.1. Parallel partition and extension with $n = 9, d = 9, r = 3$. (Bereg et al., 2020, Table 5)

1.4.1 Block Decomposition

The Kronecker product operation is best suited for PAs that can be decomposed into a block structure, much like what is used for partition and extension. Let B be a PA on n symbols with $hd(B) \geq d$. Define the *block decomposition* of $B = B_1, B_2, \ldots, B_m$ as follows:

(i) $\forall B_i \in B,\ hd(B_i) = n,$

(ii) $\forall B_i \in B,\ |B_i| = n.$

If n is a prime power, then one can create a block decomposition of $n-1$ blocks directly from $AGL(1,n)$. Recall that $AGL(1,n)$ is defined as the set of permutations $\{ax + b \mid a, b \in \mathbb{F}_n, a \neq 0\}$. Then for any i, $(1 \leq i < n)$, define the block B_i as:

$$B_i = \{ix + b \mid b \in \mathbb{F}_n\}.$$

For example, the block decomposition of $AGL(1,5)$, using arithmetic modulo 5, gives the following 4 blocks:

$$B_1 = \begin{bmatrix} 0\,1\,2\,3\,4 \\ 1\,2\,3\,4\,0 \\ 2\,3\,4\,0\,1 \\ 3\,4\,0\,1\,2 \\ 4\,0\,1\,2\,3 \end{bmatrix} \quad B_2 = \begin{bmatrix} 0\,2\,4\,1\,3 \\ 1\,3\,0\,2\,4 \\ 2\,4\,1\,3\,0 \\ 3\,0\,2\,4\,1 \\ 4\,1\,3\,0\,2 \end{bmatrix} \quad B_3 = \begin{bmatrix} 0\,3\,1\,4\,2 \\ 1\,4\,2\,0\,3 \\ 2\,0\,3\,1\,4 \\ 3\,1\,4\,2\,0 \\ 4\,2\,0\,3\,1 \end{bmatrix} \quad B_3 = \begin{bmatrix} 0\,4\,3\,2\,1 \\ 1\,0\,4\,3\,2 \\ 2\,1\,0\,4\,3 \\ 3\,2\,1\,0\,4 \\ 4\,3\,2\,1\,0 \end{bmatrix}$$

Note that sometimes these blocks are referred to as cosets of $AGL(1,n)$. If we consider the first permutation of each block B_i, for $i > 1$, to be the coset representative of that block, π_i, then we can compose each block by taking the left coset $\pi_i B_1$. It is well known that each block constructed this way contain n permutations with Hamming distance n, thus this process will always satisfy the properties of a block decomposition (Bereg et al., 2017).

$PGL(2,n)$ can also be used to create a block decomposition. It is known that for all n, $PGL(2,n)$ contains a cyclic permutation with no trivial cycles. That is, if we consider the

cyclic notation of a permutation in which one symbol maps to the symbol which follows it, $PGL(2, n)$ contains a permutation which is an $n + 1$-cycle. For example, consider the cyclic notation of the following permutation on $\mathbb{Z}_4$,

$$(1 \mapsto 4 \mapsto 3 \mapsto 2).$$

This indicates 4 is in position 1, 3 is in position 4, 2 is in position 3, and an implied $2 \mapsto 1$ means 1 is in position 2, giving us,

$$(4\ 1\ 2\ 3).$$

Since all 4 symbols are part of the same cycle, this permutation is considered a 4-cycle. Furthermore, if we compose this permutation with 4 copies of itself, denoted $\pi^4 = \pi \circ \pi \circ \pi \circ \pi$, we will obtain the identity permutation. The *order* of a permutation is the smallest j such that π^j is the identity permutation, and a permutation which is an n-cycle on n symbols will always be order n.

We therefore take a permutation π from $PGL(2, n)$ which is an $n+1$-cycle and form block $B_1 = \{\pi^1, \pi^2, \ldots, \pi^{n+1}\}$. Then for any permutation $\sigma \in PGL(2, n) \setminus B_1$, we compose σB_1 to form the left coset $B_2 = \{\sigma\pi^1, \sigma\pi^2, \ldots, \sigma\pi^{n+1}\}$. We can repeat the process, selecting new coset representatives to form disjoint cosets $B_2, B_3, \ldots, B_{n(n-1)}$ of B_1. Each block contains $n + 1$ permutations with Hamming distance $n + 1$, satisfying the properties of a block decomposition (Bereg et al., 2017).

1.4.2 Kronecker Product of Permutation Arrays

Let $A = \{\alpha_1, \alpha_2, \ldots, \alpha_l\}$ be a PA containing l permutations on $\mathbb{Z}_l$. Let $B = \{\beta_1, \beta_2, \ldots, \beta_m\}$ be a PA containing m permutations on $\mathbb{Z}_m$. Let $\alpha_i(j)$ denote the symbol in position j of permutation α_i. Let $(\alpha_i(j), B)$ denote a modified copy of the block PA B where each symbol

of every permutation has an offset of $\alpha_i(j)m$ added to it. Define the new sub-block $(A \otimes B)_i$ as:

$$(A \otimes B)_i = [(\alpha_i(1), B), (\alpha_i(2), B), \ldots, (\alpha_i(l), B)].$$

Each sub-block $(A \otimes B)_i$ is a PA of size m on the lm symbols $\{0, 1, \ldots, lm-1\}$. Thus, we define the modified Kronecker product $(A \otimes B)$ as:

$$(A \otimes B) = \bigcup_{i=1}^{l} (A \otimes B)_i.$$

Lemma 21. *(See Bereg et al. (2017, Lemma 1)) Let A be a block of permutation on l symbols with $hd(A) = l$ and let B be a block of permutations on m symbols with $hd(B) = m$. Then,*

(i) $hd(A \otimes B) = m$, and

(ii) $|(A \otimes B)| = l|B|$.

Consider this example of $(A \otimes B)$ for $l = 2$ and $m = 3$:

$$A = \begin{bmatrix} 0\ 1 \\ 1\ 0 \end{bmatrix}, \qquad B = \begin{bmatrix} 0\ 2\ 1 \\ 2\ 1\ 0 \\ 1\ 0\ 2 \end{bmatrix},$$

$$(A \otimes B) = \begin{bmatrix} 0\ 2\ 1\ 3\ 5\ 4 \\ 2\ 1\ 0\ 5\ 4\ 3 \\ 1\ 0\ 2\ 4\ 3\ 5 \\ 3\ 5\ 4\ 0\ 2\ 1 \\ 5\ 4\ 3\ 2\ 1\ 0 \\ 4\ 3\ 5\ 1\ 0\ 2 \end{bmatrix}.$$

We can observe that $(A \otimes B)$ forms a PA on 6 symbols, with $hd(A \otimes B) = 6$, and $|(A \otimes B)| = 6$. A general construction of the PA formed by $(A \otimes B)$ can be seen in Figure 1.2.

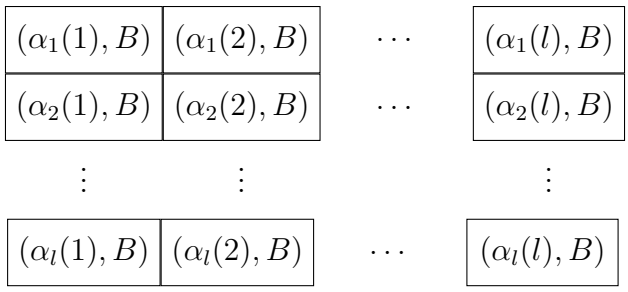

Figure 1.2. The modified Kronecker product $(A \otimes B)$ of PAs A and B. (Bereg et al., 2017, Figure 3)

Since the modified Kronecker product is defined on blocks of permutations, to take full advantage of it, we must take the Kronecker product of two PAs that can each be decomposed into multiple blocks.

Lemma 22. *(See Bereg et al. (2017, Lemma 2)) Let $A_1, A_2, \ldots, A_k$ be a block decomposition of a PA A on l symbols with $hd(A) = l - a$, and let $B_1, B_2, \ldots, B_k$ be a block decomposition of a PA B on m symbols with $hd(B) = m - b$. Then,*

(i) $hd(A \otimes B) = lm - ab$, and

(ii) $|(A \otimes B)| = kl|B|$.

Observe that each PA must contain the same number of blocks, k. In practice, if one PA contains more blocks than the other, then we simply take k as the smaller value.

Theorem 23. *(See Bereg et al. (2017, Theorem 1)) Let p and q be prime powers. Let $n = p(q+1)$ and $k = \min\{p-1, q(q-1)\}$. Then,*

$$M(n, n-2) \geq kn.$$

Theorem 23 follows directly from taking the modified Kronecker product of PA $A = AGL(1,p)$ and PA $B = PGL(2,q)$. Since $AGL(1,p)$ can be decomposed into $p-1$ blocks, and $PGL(2,q)$ can be decomposed into $q(q-1)$ blocks, then k simply becomes the minimum

of the two. As an example, consider $A = AGL(1, 31)$ and $B = PGL(2, 4)$. A therefore has a block decomposition of 30 blocks, while B has 12, giving us $k = 12$. By Lemma 22 we get the values,

$$hd(A) = 30, \qquad l = 31, \qquad a = 1,$$
$$hd(B) = 3, \qquad m = 5, \qquad b = 2.$$

This gives us $(A \otimes B)$ as a PA on $lm = 155$ symbols with,

$$hd(A \otimes B) = (31 \cdot 5) - (1 \cdot 2) = 153,$$
$$|hd(A \otimes B)| = 12 \cdot 31(5) = 1{,}860,$$
$$M(155, 153) \geq 1{,}860.$$

The modified Kronecker product sets many competitive lower bounds for $M(n, d)$, and does so for very large n that are not restricted to prime powers. Additional $M(n, d)$ results obtained from the modified Kronecker product can be seen in Bereg et al. (2017).

1.4.3 Doubling

The modified Kronecker product can be viewed as a special case of a more general operation called *tiling*. A tiling T of an array can be obtained from two sub-arrays which must have the same number of rows but may have a different number of columns. An example of tiling is illustrated in Figure 1.3.

If A is an $r \times s$ array, and B is an $r \times t$ array, then the tiled array in Figure 1.3 is a $3r \times 2t + s$ array. To ensure the resulting array is a PA, offsets must be added to B_1 and B_2 so that A, B_1, and B_2 form permutations on disjoint sets of symbols. We can therefore form B_1 by adding s to every element of B, and form B_2 by adding $s + t$ to every element of B. Since the symbols of each set are now disjoint, the resulting tiling will be a PA.

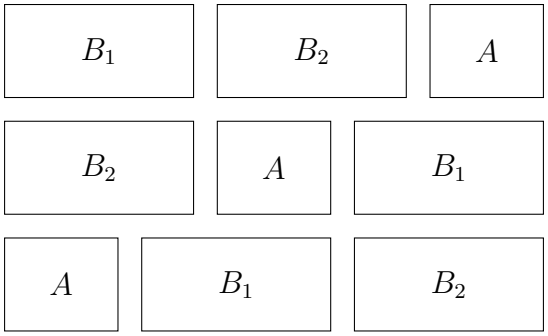

Figure 1.3. Tiling with sub-arrays A and B. (Bereg et al., 2017, Figure 4)

Doubling is a specific case of tiling in which we use four copies of an $n \times n$ array to form a $2n \times 2n$ array, as illustrated in Figure 1.4(a). To again ensure the tiling forms a PA, offsets must be added to two of the sub-arrays in opposite corners. Doubling can also be generalized to allow two different sub-arrays which have the same number of rows but a different number of columns. Generalized doubling is illustrated in Figure 1.4(b).

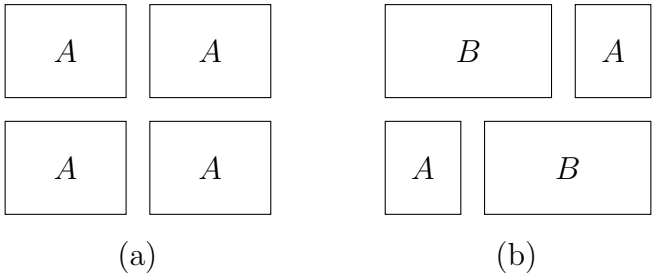

Figure 1.4. (a) Doubling of sub-array A. (b) Generalized Doubling of sub-arrays A and B. (Bereg et al., 2017, Figure 5)

To create a tiling T, consider the arrays $A = AGL(1, p)$ and $B = AGL(1, q)$ with $p \leq q$. Since tiling requires the arrays have the same number of rows, it may be necessary to remove some of the rows of B. Let $u = |B| - |A| = q(q-1) - p(p-1)$, and remove any u permutations from B. Call the resulting PA B_1. We then modify the permutations of B_1 by adding an

offset of p to each symbol, that is,

$$\pi(i) = \{\pi(i) + p \mid 0 \leq i \leq q-1, \pi \in B_1\}.$$

The permutations in A are therefore on symbols $\{0, 1, \ldots, p-1\}$, while B_1 now consists of permutations on $\{p, p+1, \ldots, q+p-1\}$. T is then formed by doubling A and B_1. By this construction, T is a PA on $p+q$ symbols containing $2p(p-1)$ permutations.

Theorem 24. *(See Bereg et al. (2017, Theorem 2)) Let p and q be primes (or prime powers), with $p \leq q$, and let $n = p + q$. Then,*

(i) if $q - 2 \leq p$, then $M(n, n-2) \geq 2p(p-1)$,

(ii) else $M(n, n-2) \geq \min\{p(p-1), \frac{1}{2}q(q-1)\}$.

Determining the Hamming distance of the resulting PA T requires some rationale. As is shown in Figure 1.4(b), there may be some overlap from the symbols in B_1 when comparing a permutation from the top half of the tiling to one in the bottom half, which would affect $hd(T)$. First consider two permutations that are either both in the top half or both in the bottom half of the tiling. Since both of our sub-arrays are formed from AGL, each sub-array may have at most one agreement between permutations. If this occurs for both sub-arrays for our two permutations in the same half, then there would be at most two agreements, giving us a Hamming distance of $q + p - 2$.

If we then consider case (i) of Theorem 24 where $q - 2 \leq p$, and compare a permutation from the top half of the tiling with one from the bottom half, then the only place an agreement could occur is in the columns of B_1 that overlap. In this case, there can be at most two overlapping columns for at most two agreements, so the Hamming distance is still $q + p - 2$.

Case (ii) has a more involved proof, but consists of constructing a bipartite graph G, partitioned by which half of the tiling contains the permutation. It can then be shown that constructing an independent set in G will contain $\min\{p(p-1), \frac{1}{2}q(q-1)\}$ permutations,

giving us the result of Theorem 24. Several competitive results for $M(n, d)$ obtained by doubling can be found in Bereg et al. (2017).

1.5 Permutation Polynomials

A polynomial f in $\mathbb{F}_q$ is a *permutation polynomial* (PP) if the function $f : x \to f(x)$ from $\mathbb{F}_q$ into itself induces a permutation. Alternatively, f is a PP of $\mathbb{F}_q$ if $f(x) = a$ has a unique solution for each $a \in \mathbb{F}_q$ (Mullen and Panario, 2013).

Permutation polynomials can be used to directly construct PAs with a known Hamming distance. Let $N_d(q)$ be the number of all PPs in $\mathbb{F}_q$ of degree d.

Theorem 25. *(See Chu et al. (2004, Theorem 2.4)) Let q be a prime power. Then*

$$M(q, q-d) \geq \sum_{i=1}^{d} N_i(q).$$

Consider two PPs $f(x)$ and $g(x)$ of degree at most d. Their corresponding permutations will agree in any position where $f(x) = g(x)$. Since this is equivalent to $f(x) - g(x) = 0$, and the polynomial formed by $f(x) - g(x)$ will also have degree at most d, there can be at most d solutions to this equation. Therefore, the permutations formed by $f(x)$ and $g(x)$ will have Hamming distance $\geq q - d$. This means that if for some q we want to form a PA with Hamming distance $q - 5$, we can use all PPs from degree 1 up to degree 5, as signified by the use of a summation in Theorem 25.

Permutation polynomials are often portrayed and discussed in *normalized form* (Lidl and Niederreiter, 1997). A PP $f(x)$ in $\mathbb{F}_q$ is in normalized form if:

1. $f(x)$ is monic. (its leading coefficient is 1)
2. $f(0) = 0$. (its constant term is 0)
3. If the degree d of $f(x)$ is not divisible by the characteristic of $\mathbb{F}_q$, the coefficient of the term x^{d-1} is 0.

If $f(x)$ is a permutation polynomial, then given $a, b, c \in \mathbb{F}_q$ with $a \neq 0$, $a \cdot f(x+b)+c$ is also a permutation polynomial. By choosing suitable a, b, and c, any PP can be transformed into its normalized form. This also means that if we consider all choices for a, b, and c, a single normalized PP is representative of $q^2(q-1)$ distinct permutations, or $q(q-1)$ permutations if condition (3) does not apply.

1.5.1 Dickson Polynomials

One sequence of polynomials which have been well studied over finite fields are the *Dickson polynomials* (Dickson, 1896). They are recursively defined as follows:

$$\begin{aligned} D_0(x,\alpha) &= 2, \\ D_1(x,\alpha) &= x, \\ D_n(x,\alpha) &= xD_{n-1}(x,\alpha) - \alpha D_{n-2}(x,\alpha). \end{aligned}$$

Observe that the Dickson polynomial $D_n(x,\alpha)$ is a polynomial of degree n.

Dickson polynomials are known to be permutation polynomials under certain conditions.

Theorem 26. *(See Lidl and Niederreiter (1997, Theorem 7.16)) The Dickson polynomial $D_n(x,\alpha)$ is a permutation polynomial of $\mathbb{F}_q$ if and only if one of the following occurs.*

1. $\alpha = 0$ *and* $\gcd(n, q-1) = 1$.

2. $\alpha \neq 0, \alpha \in \mathbb{F}_q$, *and* $\gcd(n, q^2-1) = 1$.

Given this, it is possible to form PAs on an arbitrary number of symbols, with a known Hamming distance, by simply choosing q and n which meet these conditions.

An alternative form of Dickson polynomials known as the *reversed Dickson polynomials* have also been studied for their permutational properties (Hou et al., 2009). The reversed

Dickson polynomials are constructed similarly to the Dickson polynomials, but the variables x and α are interchanged.

$$D_0(\alpha, x) = 2,$$
$$D_1(\alpha, x) = a,$$
$$D_n(\alpha, x) = \alpha D_{n-1}(\alpha, x) - xD_{n-2}(\alpha, x).$$

While the conditions for a reverse Dickson polynomial to be a PP are not as simply defined as they are for Dickson polynomials, they are still useful for creating PAs on an arbitrary number of symbols for the conditions that are known.

1.5.2 Known Classifications

Classifying all permutations polynomials of a given degree is an area of research that has long been studied. Dickson initially classified all PPs of degree ≤ 5, as shown in Table 1.5 (Dickson, 1896). However, having these classifications does not inherently give us a total count of the permutations that are represented. Not only must one extrapolate all of the normalized PPs that are represented by a given classification, the transformations $a \cdot f(x + b) + c$ must still be considered in order to obtain a total count. This was done in Chu et al. (2004), making many improvements to known bounds of $M(n, d)$.

Beyond degree 5, more recent work has included the classification of all permutation polynomials of degree 6 (Shallue and Wanless, 2013). Degree 7 PPs have also been classified for both even (Li et al., 2010) and odd (Fan, 2019) characteristics. Degree 8 PPs have been classified, but only for odd characteristics (Fan, 2020). While these classifications can be a great asset for improving the bounds of $M(n, d)$, additional work must be done to enumerate the total number of permutations represented.

Table 1.5. Classification of all PPs of degree ≤ 5.

Normalized permutation polynomial of $\mathbb{F}_q$	q
x	any q
x^2	$q \equiv 0 \pmod 2$
x^3	$q \equiv 1 \pmod 3$
$x^3 - ax$ (a not a square)	$q \equiv 0 \pmod 3$
$x^4 \pm 3x$	$q = 7$
$x^4 + a_1x^2 + a_2x$ (if its only root in $\mathbb{F}_q$ is 0)	$q \equiv 0 \pmod 2$
x^5	$q \equiv 1 \pmod 5$
$x^5 - ax$ (a not a fourth power)	$q \equiv 0 \pmod 5$
$x^5 + ax$ ($a^2 = 2$)	$q = 9$
$x^5 \pm 2x^2$	$q = 7$
$x^5 + ax^3 \pm x^2 + 3a^2x$ (a not a square)	$q = 7$
$x^5 + ax^3 + 5^{-1}a^2x$ (a arbitrary)	$q \equiv \pm 2 \pmod 5$
$x^5 + ax^3 + 3a^2x$ (a not a square)	$q = 13$
$x^5 - 2ax^3 + a^2x$ (a not a square)	$q \equiv 0 \pmod 5$

1.6 Permutation Rational Functions

Let $\mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$. Let $u(x)$ and $v(x)$ be two polynomials in $\mathbb{F}_q$ with $\gcd(u(x), v(x)) = 1$. The rational function $f(x) = u(x)/v(x)$ is a *permutation rational function* (PRF) if it induces a permutation on $\mathbb{P}^1(\mathbb{F}_q)$. PRFs have not been as rigorously studied as PPs, but they can be used very similarly for the construction of PAs (Yang et al., 2008).

1.6.1 Permutations of length $q+1$

The inclusion of ∞ as a symbol means that PRFs in $\mathbb{F}_q$ will generate permutations on $q + 1$ symbols. Let $f(x) = u(x)/v(x)$. Let $u(x)$ be of degree d_u with leading coefficient a_u. Let $v(x)$ be of degree d_v with leading coefficient a_v. Formally, we evaluate a rational function $f(x)$ at

infinity by considering the composition $f(1/x)$ evaluated at 0, but we can observe that,

$$f(\infty) = \begin{cases} \infty, & \text{if } d_u > d_v, \\ 0, & \text{if } d_u < d_v, \\ a_u/a_v, & \text{if } d_u = d_v. \end{cases}$$

Similarly, if $f(x) = a/0$ with $a \in \mathbb{F}_q, a \neq 0$, then $f(x) = \infty$. Note that the constraint $\gcd(u(x), v(x)) = 1$ prohibits the possibility of $f(x) = 0/0$.

Calculating the Hamming distance between the permutations generated from two PRFs is similar to the process for PPs. Consider the PRFs $f(x) = u(x)/v(x)$ and $g(x) = r(x)/s(x)$.

$$\begin{aligned} f(x) &= g(x) \\ u(x)/v(x) &= r(x)/s(x) \\ u(x)s(x) &= r(x)v(x) \\ u(x)s(x) - r(x)v(x) &= 0 \end{aligned}$$

If we let d_u, d_v, d_r, d_s be the degrees of their respective polynomials, then this equation is of degree at most $d_{max} = \max(d_u + d_s, d_r + d_v)$. Therefore, the resulting permutations would agree in at most d_{max} positions when evaluated over $\mathbb{F}_q$, but they may additionally agree when evaluated at ∞. We can therefore create a PA on $q+1$ symbols with Hamming distance $\geq q - d_{max}$ (Yang et al., 2008).

Constructing PAs using PRFs allows for some flexibility when selecting PRFs of a particular degree numerator and denominator, but if the goal limit the value of d_{max}, there is also some added complexity. For example, assume we want to form a PA using PRFs with $d_{max} \leq 8$. We could allow all PRFs with degree at most 4 in both the numerator and denominator, but we may find we can build a larger PA by allowing numerators up to degree 5 and denominators up to degree 3. We would have to exclusively choose one or the other, as including both types of PRFs would give $d_{max} = 9$.

1.6.2 Permutations of length q

Even though PRFs are defined as inducing permutations on $\mathbb{P}^1(\mathbb{F}_q)$, we can limit the criteria of PRFs to consider permutations only on $\mathbb{F}_q$ (Yang et al., 2008). One simple approach is as follows. If we consider some PRF $f(x) = u(x)/v(x)$, then we would want to omit PRFs where $v(a) = 0$ for some $a \in \mathbb{F}_q$. We then only evaluate $f(x)$ for $x \in \mathbb{F}_q$, resulting in a permutation without the symbol ∞.

The Hamming distance of such a PA would also be $\geq q - d_{max}$, as we eliminate both one symbol as well as the possibility of an additional agreement at $f(\infty)$. If we consider the set of PRFs that can be used to form permutations of length q as a subset of all PRFs, then they must in fact be those which have a higher degree numerator than denominator. These PRFs all evaluate $f(\infty) = \infty$, so by simply evaluating them for the values in $\mathbb{F}_q$, we obtain a permutation on $\mathbb{F}_q$.

1.6.3 Classifications of PRFs

There is limited published information on the classification of PRFs of a particular degree, but one recent paper has classified all PRFs of degree 3 (numerator or denominator) (Ferraguti and Micheli, 2020). One important result obtained is PRFs of degree 3 exist in every $\mathbb{F}_q$. Additionally, it was shown that all degree 3 PRFs are *exceptional*. This means if some rational function is a PRF in $\mathbb{F}_q$, where $q = p^k$, it is a PRF in $\mathbb{F}_{p^k}$ for infinitely many k.

In addition to classifying PRFs of degree 3, they also derived closed formulas to count how many monic PRFs of degree 3 exist, as given in Table 1.6. Since these are monic PRFs, each one is actually representative of $(q-1)$ total permutations through the transformation $a \cdot f(x)$. These counts provide many competitive $M(n, d)$ results when n is a prime power,

Table 1.6. Number of degree 3 monic PRFs by congruence class q modulo 3.

$\mathbb{F}_q$	Number of Degree 3 Monic PRFs
$q \equiv 0 \pmod 3$	$\frac{1}{2}(q^4 + q^3 + q^2 + q)$
$q \equiv 1 \pmod 3$	$\frac{1}{2}(q^4 - q^2)$
$q \equiv 2 \pmod 3$	$\frac{1}{2}(q^2 + q)^2$

given by the bounds:

$$M(n+1, n-6) \geq \frac{1}{2}(n^4 + n^3 + n^2 + n) \qquad \text{when } n \equiv 0 \pmod 3,$$
$$M(n+1, n-6) \geq \frac{1}{2}(n^4 - n^2) \qquad \text{when } n \equiv 1 \pmod 3,$$
$$M(n+1, n-6) \geq \frac{1}{2}(n^2 + n)^2 \qquad \text{when } n \equiv 2 \pmod 3.$$

1.7 Permutation Arrays under Chebyshev Distance

Though Hamming distance is the most commonly used distance metric for PAs, Chebyshev distance can be more appropriate for certain applications. Note that two permutations with a large Hamming distance could actually have a very small Chebyshev distance, and vice versa. Thus, techniques used to create or modify PAs of one type may not be applicable to the other.

1.7.1 Explicit Chebyshev PA Construction

One technique to explicitly construct a Chebyshev PA is given in Klove et al. (2010). Let $[n]$ be the set of symbols $\{1, \ldots, n\}$, and S_n be the *symmetric group* over $[n]$, that is, the set of all permutations of $[n]$. For a given n and d, construct PA C with $cd(C) \geq d$ as follows:

$$C = \big\{ \big(\pi(1), \ldots, \pi(n)\big) \in S_n \mid \pi(i) \equiv i \pmod{\ d} \text{ for all } i \in [n] \big\}.$$

This construction ensures the distance between permutations is at least d by making sure each symbol in position i of every permutation is congruent to $i \pmod d$. This means each

symbol can only appear in certain positions, but symbols in that position will have distance some multiple of d, possibly 0. Since each permutation is unique, at least one symbol in each permutation will differ from a symbol in all other permutations, giving us $cd(C) \geq d$. This construction gives the following bound for $P(n, d)$, the maximum size of a PA on n symbols with Chebyshev distance at least d.

Theorem 27. *(See Klove et al. (2010, Theorem 1)) If $n = ad + b$, where $0 \leq b < d$, then*

$$P(n, d) \geq ((a + 1)!)^b (a!)^{d-b}.$$

With Theorem 27 we can make the following observations:

$$\begin{array}{lll} \text{if } 2d > n, & \text{then } a = 1, b = n - d, & \text{and } |C| = 2^{n-d}, \\ \text{if } 2d = n, & \text{then } a = 2, b = 0, & \text{and } |C| = 2^d, \\ \text{if } 2d < n, & & \text{then } |C| \gg 2^{n-d}. \end{array}$$

One example from Klove et al. (2010) shows that for $n = 30$, $d = 2$, then $|C| \approx 1.71 \times 10^{24}$, but $2^{n-d} \approx 2.68 \times 10^8$, making $|C|$ larger by a factor of approximately 6.37×10^{15}. Thus, if d is small relative to n, this method allows for the construction of very large PAs.

1.7.2 Recursive Chebyshev PA Construction

Klove et al. (2010) also gives some recursive methods for constructing larger PAs from smaller PAs. Let C be a Chebyshev PA on n symbols with $cd(C) \geq d$ and $|C| = m$. Let $r \geq 2$ be an integer. We can construct a PA C_r on rn symbols with $cd(C_r) \geq rd$ and $|C_r| = m^r$ as follows. For each multi-set of r permutations from C,

$$\big(\pi^j(1), \ldots \pi^j(n)\big),\ 0 \leq j \leq r - 1,$$

let

$$\rho_j = \big(r\pi^j(1) - j, \ldots, r\pi^j(n) - j\big),\ 0 \leq j \leq r - 1,$$

Table 1.7. Recursive construction of C_r for $n = 3$, $d = 2$, $r = 2$.

Multi-set	ρ_0	ρ_1	C_r
123 123	246	135	246135
123 231	246	351	246351
123 312	246	513	246513
231 123	462	135	462135
231 231	462	351	462351
231 312	462	513	462513
312 123	624	135	624135
312 231	624	351	624351
312 312	624	513	624513

and include $(\rho_0|\rho_1|\ldots|\rho_{r-1})$ as a permutation in C_r.

As a simple example, consider the following PA with $n = 3$ and $d = 2$.

$$C = \begin{bmatrix} 123 \\ 231 \\ 312 \end{bmatrix}$$

Table 1.7 shows the recursive construction of C_r for $r = 2$, yielding a new PA on $n = 6$ symbols with $d = 4$ and $|C_r| = 9$. In general, this construction gives us the result in Theorem 28.

Theorem 28. *(See Klove et al. (2010, Theorem 2)) If $n > d$ and $r \geq 2$, then,*

$$P(rn, rd) \geq P(n, d)^r.$$

Klove et al. (2010) defines one additional recursive construction. Let $\pi = \big(\pi(1), \ldots, \pi(n)\big) \in S_n$, and m be an integer $1 \leq m \leq n + 1$. Define

$$\varphi_m(\pi) = \big(m, \pi'(1), \pi'(2), \ldots, \pi'(n)\big) \in S_{n+1},$$

where

$$\pi'(i) = \pi(i) \qquad \text{if } \pi(i) < m,$$
$$\pi'(i) = \pi(i) + 1 \quad \text{if } \pi(i) \geq m.$$

Table 1.8. Recursive construction of $C[s_1, s_2]$ for $n = 3$, $d = 2$, $s1 = 1$, $s2 = 3$.

π	$\varphi_{s_1}(\pi)$	$\varphi_{s_2}(\pi)$
123	1234	3124
231	1342	3241
312	1423	3412

Let C be a PA on n symbols with $cd(C) \geq d$, and let

$$1 \leq s_1 < s_2 < \cdots < s_t \leq n + 1$$

be integers. Define

$$C[s_1, s_2, \ldots, s_t] = \big\{\varphi_{s_j}(\pi) \mid 1 \leq j \leq t, \pi \in C\big\}.$$

Theorem 29. *(See Klove et al. (2010, Theorem 3)) If C is a PA on n symbols with $cd(C) \geq d$, $|C| = m$, and*

$$s_j + d \leq s_{j+1} \text{ for } 1 \leq j \leq t - 1,$$

then $C[s_1, s_2, \ldots, s_t]$ is PA on $n + 1$ symbols with distance d and size tm.

As long as all of our selected integers s_1 through s_t are separated by at least d, we can use each value to form $\varphi_{s_j}(\pi)$ for each $\pi \in C$ and add them to the new PA. If we use the same PA C on 3 symbols and $d = 2$ from the previous example and choose $s_1 = 1$, $s_2 = 3$, the resulting PA would be constructed as shown in Table 1.8. The general bound from this construction is given in Theorem 30.

Theorem 30. *(See Klove et al. (2010, Theorem 5)) If $n > d \geq 1$, then*

$$P(n + 1, d) \geq \Big(\Big\lfloor \frac{n}{d} \Big\rfloor + 1\Big) P(n, d).$$

1.7.3 Greedy Chebyshev PA Construction and Additional Bounds

A simple greedy approach to constructing PAs yields additional bounds for $P(n, d)$. Let $V(n, d)$ denote the number of permutations in S_n that are at least Chebyshev distance d away from the identity permutation, $(1, 2, \ldots, n)$.

Theorem 31. *(See Klove et al. (2010, Theorem 9)) For $n > d \geq 2$ we have*

$$P(n, d) \geq \frac{n!}{V(n, d-1)}.$$

This theorem is derived from the Gilbert-Varshamov lower bound resulting from the following greedy algorithm.

1. Start with any permutation in S_n.
2. Choose a permutation whose distance is at least d to all previously chosen permutations.
3. Repeat step (2) as long as such a permutation exists.

Similarly, this greedy algorithm can be used to show an upper Hamming bound.

Theorem 32. *(See Klove et al. (2010, Theorem 10)) If $n > d \geq 1$, then*

$$P(n, d) \leq \frac{n!}{V(n, \lfloor (d-1)/2 \rfloor)}.$$

One additional enhancement that was made to the greedy algorithm was an improvement to the greedy choice. Rather than choose the permutations at random, you start with the identity permutation, then choose the next permutation in lexicographic order with distance at least d to all previously chosen permutations. Using this improved greedy algorithm and their applicable theorems, Klove et al. produced Table 1.9 on bounds for $P(n, d)$.

Table 1.9. Bounds on $P(n, d)$. (Klove et al., 2010, Table 2)

n	$d = 2$	$d = 3$	$d = 4$	$d = 5$	$d = 6$	$d = 7$
$n = d + 1$	3	3	3	3	3	3
$n = d + 2$	6-24	10*	9-12	9-12	9-18	9-18
$n = d + 3$	29-120	20-34	28-43	28-43	28-60	28-60
$n = d + 4$	90-720	84-148	68-166	95-166	95-216	95-216
$n = d + 5$	582-5,040	401-733	283-4,077	236-714	236-850	236-850

* Table 2 in Klove et al. (2010) incorrectly shows this bound as 9

CHAPTER 2

PERMUTATION POLYNOMIALS[1]

In Section 1.5 we give several known classifications of permutation polynomials. A primary challenge to searching for PPs beyond these is that the search space for PPs in $\mathbb{F}_q$ of degree d is of the order $O(q^{d+1})$. Thus, to efficiently perform such a search requires the use of certain optimizations. In this chapter we detail functions which provide these optimizations and give an algorithm to efficiently perform an exhaustive search by reducing the search space from $O(q^{d+1})$ to $O(q^{d-3})$. These ideas were first presented in Bereg et al. (2019).

Using this search technique, we were able to classify all PPs in fields up to $\mathbb{F}_{97}$ of degree up to 10. We also calculated some cases of degrees 11 and 12. This yielded many improvements to $M(n, d)$ and laid a foundation for the searching of PRFs, which are discussed in Chapter 3.

For notation, let d denote the degree of a PP $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ over the finite field $\mathbb{F}_q$, where $q = p^k, k \geq 1$, and p is the prime characteristic. Let the $q-1$ non-zero elements of $\mathbb{F}_q$ be listed as $t^0, t^1, \ldots, t^{q-2}$, where t represents a generator of the multiplicative group of the field. We use the notation $t^0 = 1, t^1 = 2, \ldots, t^{q-2} = q-1$, which is given by Lidl and Niederreiter (1997) as a second choice of notations to denote the elements of $\mathbb{F}_q$. Note that they list the first choice as using polynomials of degree k with coefficients in $\mathbb{F}_p$.

2.1 Improved Normalization

Section 1.5 also detailed the normalization operations $a \cdot f(x + b) + c$. Using these three operations, you can convert a PP to normalized form and fix the coefficients $a_d = 1$, $a_{d-1} = 0$, and $a_0 = 0$, except in cases where d is a multiple of the characteristic p. In these cases, the

[1] ©2019. Portions used, with permission, from S. Bereg, B. Malouf, L. Morales, T. Stanley, H. Sudborough, A. Wong, "Equivalence relations for computing permutation polynomials", CoRR abs/1911.12823, November 2019.

operation $f(x+b)$ does not allow us to fix $a_{d-1}=0$ due to a property from the "Freshman's Dream" theorem (Bastida, 1984). This theorem states that in fields with prime characteristic p,

$$(\alpha+\beta)^p = \alpha^p + \beta^p. \tag{2.1}$$

Though exponents do not actually distribute over addition, in this particular case, p divides all of the intermediate binomial coefficients, making them all equal to zero. However, we have found it is possible to use $f(x+b)$ to fix an alternative coefficient at zero depending on if $p=2$, which we call *m-normalization* and *b-normalization*.

Table 2.1. Types of normalization for PPs, $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$, of degree d with field characteristic p.

Normalization	**Degree Restriction**	**Coefficient Properties**
standard	$p \nmid d$	$a_d = 1,\ a_{d-1} = 0$, and $a_0 = 0$
standard	$p \mid d$	$a_d = 1$ and $a_0 = 0$
m-normalization	$p \mid d$ and $p \neq 2$	$a_d = 1,\ a_0 = 0$, either $a_{d-1} = 0$ or $a_{d-2} = 0$
b-normalization	$p \mid d,\ p = 2$, and $2^i \leq d \leq 2^{i+1} - 3$	$a_d = 1,\ a_0 = 0$, either $a_r = 0$ or $a_{r-1} = 0$, where $r = 2^i - 1$ for some $i \geq 2$

Using these improved normalizations, we are always able fix 3 coefficients of a PP, including cases where standard normalization does not allow it. This lets us reduce the search space for PPs to $O(q^{d-2})$ even if d is a multiple of p.

2.1.1 m-normalization

If $p \neq 2$, i.e., p is odd, and d is a multiple of p, then it is possible to apply *m-normalization*. We define a PP as being in m-normalized form if $a_d = 1$, $a_0 = 0$, and either $a_{d-1} = 0$ or $a_{d-2} = 0$.

Theorem 33. *Any PP $f(x)$ where the degree d is a multiple of the field characteristic p can be transformed to an m-normalized PP $g(x)$ by the normalization operations.*

Proof. Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$, and for some $a, b, c \in \mathbb{F}_q$ with $a \neq 0$, let

$$\begin{aligned} g(x) &= a \cdot f(x+b) + c \\ &= aa_d(x+b)^d + aa_{d-1}(x+b)^{d-1} + aa_{d-2}(x+b)^{d-2} + \cdots + aa_1(x+b) + aa_0 + c \\ &= b_d x^d + b_{d-1}x^{d-1} + b_{d-2}x^{d-2} + \cdots + b_1 x + b_0, \end{aligned}$$

Observe that the degree d term of $g(x)$ has the coefficient $b_d = aa_d$. If we choose a to be the multiplicative inverse of a_d, then the degree d coefficient of $g(x)$ will be 1.

If $a_{d-1} = 0$, then $b_{d-1} = 0$ and the desired property is true. So suppose that $a_{d-1} \neq 0$, and consider b_{d-2} in $g(x)$. Since d is a multiple of p, the expansion of $a_d(x+b)^d$ will derive nonzero coefficients only for terms whose degrees are multiples of p. Since $p > 2$, this means $(d-2) \nmid p$, so $a_d(x+b)^d$ will have a coefficient of 0 for the degree $d-2$ term. Hence b_{d-2} is calculated solely by the expansion of $aa_{d-1}(x+b)^{d-1} + aa_{d-2}(x+b)^{d-2}$.

The expansion of $aa_{d-1}(x+b)^{d-1}$ will produce a term of degree $d-2$ with coefficient $aa_{d-1}b'$ where $b' = \sum_1^{d-1} b$. The expansion of $aa_{d-2}(x+b)^{d-2}$ will produce a term of degree $d-2$ with coefficient $b_{d-2} = aa_{d-2}$. Therefore, the coefficient of x^{d-2} in $g(x)$ is $b_{d-2} = aa_{d-1}b' + aa_{d-2} = a(a_{d-1}b' + a_{d-2})$. And by algebra, b_{d-2} is zero if $a_{d-1}b' + a_{d-2} = 0$. Since $a_{d-1} \neq 0$ and $d-1$ is not a multiple of p, we can choose b such that b' is the additive inverse of a_{d-2}/a_{d-1}, making $b_{d-2} = 0$ in $g(x)$. So in $g(x)$, $b_d = 1$, and either $b_{d-1} = 0$ or $b_{d-2} = 0$.

If we choose c to be the additive inverse of the constant term of $a \cdot f(x+b)$, then $b_0 = 0$, and we achieve m-normalization. □

2.1.2 b-normalization

If $p = 2$ and d is a multiple of p, then it is possible to apply *b-normalization*. We define a PP as being in b-normalized form if $a_d = 1$, $a_0 = 0$, and if $2^i \leq d \leq 2^{1+1} - 3$ for some i, then either $a_r = 0$ or $a_{r-1} = 0$, where $r = 2^i - 1$. This means b-normalization can be

applied in all cases except when $d = 2^i - 2$, but in practice, the search space for $d = 6$ is small enough to not need it, and the search space for $d = 14$ is too large to currently search even if b-normalization were applicable.

We say that the integer interval $[r, s]$ has a $[t, u]$ gap if for all $d \in [r, s]$, the expansion of $(x + b)^d$ does not include any nonzero x^i terms, where $i \in [t, u]$. For example, the integer interval $[8, 13]$ has a $[6, 7]$ gap as seen by:

$$
\begin{aligned}
(x+b)^8 &= x^8 + b^8 \\
(x+b)^9 &= x^9 + bx^8 + b^8x + b^9 \\
(x+b)^{10} &= x^{10} + b^2x^8 + b^8x^2 + b^{10} \\
(x+b)^{11} &= x^{11} + bx^{10} + b^2x^9 + b^3x^8 + b^8x^3 + b^9x^2 + b^{10}x + b^{11} \\
(x+b)^{12} &= x^{12} + b^4x^8 + b^8x^4 + b^{12} \\
(x+b)^{13} &= x^{13} + bx^{12} + b^4x^9 + b^5x^8 + b^8x^5 + b^9x^4 + b^{12}x + b^{13}.
\end{aligned}
$$

That is, there are no degree 6 or 7 terms in each of these expanded polynomials.

We make use of this observation in the proofs of Lemmas 35 and 36. Lemma 35 shows that if we expand $(x + b)^d$ for $2^i \leq d \leq 2^{i+1} - 3$, the coefficients of the terms x^{2^i-2} and x^{2^i-1} are always zero. Thus, we say the interval $[2^i, 2^{i+1} - 3]$ has a $[2^i - 2, 2^i - 1]$ gap. Lemma 36 shows that in any field $\mathbb{F}_{2^k}$, and any PP $f(x)$ of even degree d, $2^i \leq d \leq 2^{i+1} - 3$, we can select some b such that the PP $f(x + b)$ will always have some designated term with a coefficient of zero. We include Lucas's Theorem, as it is also required for the proof of Lemma 35.

Theorem 34. *(Lucas's Theorem. See Cameron (1995, Theorem 3.4.1)) Let p be prime, and let $m = m_0 + m_1p + \ldots, +m_dp^d$ and $n = n_0 + n_1p + \ldots, +n_dp^d$, where $0 \leq m_i, n_i < p$ for $i = 0, 1, \ldots, d$. Then*

$$\binom{m}{n} \equiv \prod_{i=0}^{d} \binom{m_i}{n_i} \pmod{p}.$$

Lemma 35. *(Gap Lemma) In any finite field of characteristic 2, for all $i > 1$, the expansion of $(x+b)^d$, for $d \in [2^i, 2^{i+1}-3]$, has a $[2^i-2, 2^i-1]$ gap.*

Proof. Consider the expansion $(x+b)^d = \sum_{k=0}^{d} \binom{d}{k} x^{d-k} b^k$. Let $k \in \{d-(2^i-2), d-(2^i-1)\}$. Clearly, b^k is not zero, so our job is to show that the expression $\binom{d}{k}$ is zero. Let $k' = d-k$, that is $k' \in \{2^i-2, 2^i-1\}$. By a well-known identity, we have $\binom{d}{k} = \binom{d}{d-k} = \binom{d}{k'}$. Represent d and k' by their base-2 $(i+1)$-tuples $\delta = (\delta_i, \delta_{i-1}, \ldots, \delta_2, \delta_1, \delta_0)$ and $\kappa = (\kappa_i, \kappa_{i-1}, \ldots, \kappa_2, \kappa_1, \kappa_0)$, respectively, where for all i, $\delta_i, \kappa_i \in \{0,1\}$. Observe that at least one δ_j $(0 \le j \le i-2)$ must be 0 because $2^i \le d \le 2^{i+1}-3$. Observe also that $\kappa_i = 1$ for all $i > 0$. Hence there is a j such that $\delta_j = 0$ and $\kappa_j = 1$, so by Lucas' Theorem, $\binom{d}{k'} = 0 = \binom{d}{k}$. It follows that $(x+b)^d$, for $d \in [2^i, 2^{i+1}-3]$, has a $[2^i-2, 2^i-1]$ gap. □

Lemma 36. *Let $i > 1$. Let $d \in [2^i, 2^{i+1}-3]$ be even. For any PP $f(x)$ over $\mathbb{F}_{2^k}$, where $k > 2$, there is a constant b in $\mathbb{F}_{2^k}$ such that in the PP $f(x+b)$, either the x^{2^i-1} term or the x^{2^i-2} term is zero.*

Proof. By Lemma 35, the interval $[2^i, 2^{i+1}-3]$ has a $[2^i-2, 2^i-1]$ gap. Let $f(x) = a_d x^d + a_{d-1}x^{d-1} + a_{d-2}x^{d-2} + \cdots + a_1 x + a_0$, where $d \in [2^i, 2^{i+1}-3]$ is even. Adding b to the argument gives: $f(x+b) = a_d(x+b)^d + a_{d-1}(x+b)^{d-1} + a_{d-2}(x+b)^{d-2} + \cdots + a_1(x+b) + a_0$. If a_{2^i-1} is zero there is nothing to prove, so suppose a_{2^i-1} is not zero. Since $[2^i, 2^{i+1}-3]$ has a $[2^i-2, 2^i-1]$ gap, each term $(x+b)^r$, for $r \in [2^i, 2^{i+1}-3]$ has no x^t term for $t \in [2^i-2, 2^i-1]$. This means $a_{2^i-1}(x+b)^{2^i-1}$ and $a_{2^i-2}(x+b)^{2^i-2}$ are the only possible terms whose expansion has a nonzero x^{2^i-2} term. By the binomial theorem, $a_{2^i-1}(x+b)^{2^i-1} = a_{2^i-1}x^{2^i-1} + a_{2^i-1}bx^{2^i-2} + \ldots$, and $a_{2^i-2}(x+b)^{2^i-2} = a_{2^i-2}x^{2^i-2} + \ldots$, where low order terms are not shown. Summing these two expansions and isolating the x^{2^i-2} term, we solve for the value of b such that $a_{2^i-1}bx^{2^i-2} + a_{2^i-2}x^{2^i-2} = 0$. We see that when $b = -a_{2^i-1}/a_{2^i-2}$, the coefficient of the x^{2^i-2} term of $f(x+b)$ is zero. □

Consider a polynomial of degree $d = 8$. Let $f(x) = a_8x^8 + a_7x^7 + a_6x^6 + \cdots + a_1x + a_0$. Taking $f(x + b)$ gives:

$$\begin{aligned} f(x+b) &= a_8(x+b)^8 + a_7(x+b)^7 + a_6(x+b)^6 + \cdots + a_1x + a_0 \\ &= a_8(x^8 + b^8) + a_7(x^7 + bx^6 + b^2x^5 + \dots) + a_6(x^6 + b^2x^4 + \dots) + \dots \\ &= a_8x^8 + a_8b^8 + (a_7x^7 + a_7bx^6 + \dots) + (a_6x^6 + a_6b^2x^4 + \dots) + \dots \end{aligned}$$

We need to select b such that the coefficient of x^6 in $f(x + b)$ will equal zero. From this expansion, we see this coefficient is computed from the sum $a_7bx^6 + a_6x^6 = 0$. Thus, selecting $b = -a_6/a_7$ yields the desired result.

Theorem 37. *Any PP $f(x)$ over $\mathbb{F}_{2^k}$ for some $k > 2$, and $2 \mid d$ can be transformed to an b-normalized PP $g(x)$ by the normalization operations, except when $d = 2^i - 2$, for some $i \geq 2$.*

Proof. Let $f(x) = a_dx^d + a_{d-1}x^{d-1} + \cdots + a_1x + a_0$, and for some $a, b, c \in \mathbb{F}_q$ with $a \neq 0$, let

$$\begin{aligned} g(x) &= a \cdot f(x+b) + c \\ &= aa_d(x+b)^d + aa_{d-1}(x+b)^{d-1} + aa_{d-2}(x+b)^{d-2} + \cdots + aa_1(x+b) + aa_0 + c \\ &= b_dx^d + b_{d-1}x^{d-1} + b_{d-2}x^{d-2} + \cdots + b_1x + b_0, \end{aligned}$$

Observe that the degree d term of $g(x)$ has the coefficient $b_d = aa_d$. If we choose a to be the multiplicative inverse of a_d, then the degree d coefficient of $g(x)$ will be 1. If we choose c to be the additive inverse of the constant term of $a \cdot f(x + b)$, then the constant term of $g(x)$ will be 0. By Lemma 36, there is a b such that in $g(x)$, the coefficient of either the degree $2^i - 1$ term or degree $2^i - 2$ term equal to 0, except when $d = 2^i - 2$, for some $i \geq 2$. Hence $g(x)$ is b-normalized. □

2.2 Mapping Normalized PPs to Normalized PPs

In this section we describe two functions which map normalized PPs to normalized PPs, the *F-map* and the *G-map*. If the input to either function is in standard normalized form, m-normalized form, or b-normalized form, the result will be in the same. Using these two functions together, we are able to fix an additional coefficient at some value, resulting in an order of magnitude reduction in the search space for PPs.

2.2.1 The *F*-map

The F-map is a function that multiplies the degree $(d-k)$ term of $f(x)$ by t^k, for all k.

Definition 38. *Define the* ***F*-map** *by*

$$\begin{aligned} F(f(x)) &= t^0 a_d x^d + t^1 a_{d-1} x^{d-1} + \cdots + t^k a_{d-k} x^{d-k} + \cdots + t^{d-1} a_1 x + t^d a_0 \\ &= \sum_{k=0}^{d} t^k a_{d-k} x^{d-k}. \end{aligned}$$

We first show that the set of PPs is closed under the F-map.

Lemma 39. *If $f(x)$ is a PP, then $F(f(x))$ is a PP.*

Proof. We show that $F(f(x))$ is one-to-one. Observe that, for any nonzero t^i,

$$\begin{aligned} F(f(t^i)) &= t^0 a_d (t^i)^d + t^1 a_{d-1} (t^i)^{d-1} + \cdots + t^{d-1} a_1 (t^i)^1 + t^d a_0 \\ &= t^d (a_d (t^d)^{i-1} + a_{d-1} (t^{d-1})^{i-1} + \cdots + a_1 (t^1)^{i-1} + a_0) \\ &= t^d (a_d (t^{i-1})^d + a_{d-1} (t^{i-1})^{d-1} + \cdots + a_1 (t^{i-1})^1 + a_0) \\ &= t^d \cdot f(t^{i-1}) \\ &= t^d \cdot f(t^i/t). \end{aligned}$$

It follows that $F(f(x))$ is a permutation polynomial, since it is obtained from $f(x)$ by multiplying by the constant t^d and replacing the argument x by $t^{-1}x$. □

We next show that the F-map preserves any normalization.

Corollary 40. *If $f(x)$ is a PP in standard normalized form, m-normalized form, or b-normalized form, $F(f(x))$ is a PP normalized in the same form.*

Proof. By Lemma 39, we only need to show that $F(f(x))$ is normalized when $f(x)$ is normalized. Since the leading coefficient a_d is multiplied by $t^0 = 1$, the leading coefficient of $F(f(x))$ will remain unchanged. Since all other coefficients are multiplied by some nonzero constant, any coefficient of 0 will remain 0. Therefore, by the normalization definitions, all fixed coefficients in $f(x)$ will remain unchanged in $F(f(x))$, thus $F(f(x))$ will be a PP with the same normalization. □

Observe that the $q-1$ non-zero elements of $\mathbb{F}_q$ form a cyclic group, $\mathcal{G}_{q-1}$, under multiplication (Lidl and Niederreiter, 1997). Moreover, for each k, there exists an r, $(0 < r \leq q-1)$, such that the iterates, $t^k, t^{2k}, \ldots, (t^{rk \mod (q-1)} = 1)$, form a cyclic subgroup, $\mathcal{H}_{t^k}$, of $\mathcal{G}_{q-1}$. By Lagrange's theorem, the number of elements in $\mathcal{H}_{t^k}$, that is, $\text{ord}(\mathcal{H}_{t^k})$, is a divisor of $q-1$.

Consider iterations of the F-map, namely, the sequence

$$f(x), F(f(x)), F^2(f(x)), \ldots, F^i(f(x)), \ldots, \tag{2.2}$$

where $F^i(f(x)) = \sum_{k=0}^{d} t^{ik} a_{d-k} x^{d-k}$. For the degree $(d-k)$ term, iterative use of the F-map yields the sequence of coefficients

$$a_{d-k},\ t^k a_{d-k},\ t^{2k} a_{d-k},\ \ldots, (t^{rk \mod (q-1)} a_{d-k} = a_{d-k})$$

where the terms are simply the elements of $\mathcal{H}_{t^k}$ multiplied by the common factor a_{d-k}. This forms a cycle of length $r \leq q-1$ where r is smallest integer such that $t^{rk \mod (q-1)} a_{d-k} = a_{d-k}$.

Definition 41. *Let k be an integer such that $1 \leq k \leq d$. Define the $\boldsymbol{F_k}$ − map by $F_k(x) = xt^k$.*

The F_k function gives us a different way to look at the F-map, namely, for each k, the F-map computes $F_k(a_{d-k}) = t^k a_{d-k}$. In other words,

$$\begin{aligned} F(f(x)) &= a_d x^d + t^1 a_{d-1} x^{d-1} + \cdots + t^{d-1} a_1 x + t^d a_0 \\ &= a_d x^d + F_1(a_{d-1}) x^{d-1} + \cdots + F_{d-1}(a_1) x + F_d(a_0). \end{aligned}$$

Note that iterations of the F_k-map on the element 1 yields the cyclic subgroup $\mathcal{H}_{t^k}$. We call this sequence of iterations the ***F_k*-cycle**. Define the length of the F_k-cycle to be $ord(\mathcal{H}_{t^k})$. For our purposes, we are interested in those values of k for which the $(d-k)^{th}$ coefficient of a normalized PP $f(x)$ is not 0.

Observe that for any PP $f(x)$, there is an integer $s \geq 1$, such that the sequence shown in Equation (2.2) forms a cycle.

Definition 42. *The sequence of iterates of the F-map on the PP $f(x)$, namely*

$$f(x), F(f(x)), F^2(f(x)), \ldots, F^s(f(x)) = f(x)$$

is called the ***F*-cycle on $f(x)$.**

Consider the values of k for which the coefficient a_{d-k} in $f(x)$ is nonzero. For all such k, $(1 \leq k \leq d)$, let $g_k = \gcd(k, q-1)$, and let $j = \min_k\{g_k\}$. The length of the F-cycle on $f(x)$ is $s = (q-1)/j$. That is, the length of the F-cycle on $f(x)$ is the least common multiple of the orders of the subgroups $\mathcal{H}_{t^k}$ for all k such that $a_{d-k} \neq 0$.

For example, consider $\mathbb{F}_{25=5^2}$. The cyclic subgroups of $\mathcal{G}_{5^2-1}$ are $\mathcal{H}_{t^0}$, $\mathcal{H}_{t^1}$, $\mathcal{H}_{t^2}$, $\mathcal{H}_{t^3}$, $\mathcal{H}_{t^4}$, $\mathcal{H}_{t^6}$, $\mathcal{H}_{t^8}$, $\mathcal{H}_{t^{12}}$, and their orders are 1, 24, 12, 8, 6, 4, 3 and 2, respectively. To see this, observe that

$$\begin{aligned} \mathcal{H}_1 = \mathcal{H}_{t^0} &= \{t^{i*0}\} = \{1\} \text{ for all } i \\ \mathcal{H}_2 = \mathcal{H}_{t^1} &= \{t^{i*1}\} \text{ for all } i \\ &= \{t^{0*1}, t^{1*1}, t^{2*1}, t^{3*1}, \ldots\} \end{aligned}$$

$$\begin{aligned} \mathcal{H}_7 = \mathcal{H}_{t^6} &= \{t^{i*6}\} \text{ for all } i \\ &= \{t^{0*6}, t^{1*6}, t^{2*6}, t^{3*6}, t^{4*6}\} \\ &= \{t^0, t^6, t^{12}, t^{18}, t^{24} = t^0\} \end{aligned}$$

$$= \{t^0, t^1, t^2, t^3, \ldots, t^{23}, t^{24} = t^0\} \qquad = \{1, 7, 13, 19\}$$

$$= \{1, 2, 3, 4, \ldots, 24\} \qquad = \mathcal{H}_{19}$$

$$= \mathcal{H}_6 = \mathcal{H}_8 = \mathcal{H}_{12} = \mathcal{H}_{14} = \mathcal{H}_{18} = \mathcal{H}_{20} = \mathcal{H}_{24}$$

$$\mathcal{H}_3 = \mathcal{H}_{t^2} = \{t^{i*2}\} \text{ for all } i \qquad \mathcal{H}_9 = \mathcal{H}_{t^8} = \{t^{i*8}\} \text{ for all } i$$

$$= \{t^{0*2}, t^{1*2}, t^{2*2}, t^{3*2}, \ldots\} \qquad = \{t^{0*8}, t^{1*8}, t^{2*8}, t^{3*8}\}$$

$$= \{t^0, t^2, t^4, t^6, \ldots, t^{22}, t^{24} = t^0\} \qquad = \{t^0, t^8, t^{16}, t^{24} = t^0\}$$

$$= \{1, 3, 5, 7, \ldots, 23\} \qquad = \{1, 9, 17\}$$

$$= \mathcal{H}_{11} = \mathcal{H}_{15} = \mathcal{H}_{23} \qquad = \mathcal{H}_{17}$$

$$\mathcal{H}_4 = \mathcal{H}_{t^3} = \{t^{i*3}\} \text{ for all } i \qquad \mathcal{H}_{13} = \mathcal{H}_{t^{12}} = \{t^{i*12}\} \text{ for all } i$$

$$= \{t^{0*3}, t^{1*3}, t^{2*3}, t^{3*3}, \ldots\} \qquad = \{t^{0*12}, t^{1*12}, t^{2*12}\}$$

$$= \{t^0, t^3, t^6, t^9, \ldots, t^{21}, t^{24} = t^0\} \qquad = \{t^0, t^{12}, t^{24} = t^0\}$$

$$= \{1, 4, 7, 10, \ldots, 22\} \qquad = \{1, 13\}$$

$$= \mathcal{H}_{10} = \mathcal{H}_{16} = \mathcal{H}_{22}$$

$$\mathcal{H}_5 = \mathcal{H}_{t^4} = \{t^{i*4}\} \text{ for all } i$$

$$= \{t^{0*4}, t^{1*4}, t^{2*4}, t^{3*4}, t^{4*4}, t^{5*4}, t^{6*4}\}$$

$$= \{t^0, t^4, t^8, t^{12}, t^{16}, t^{20}, t^{24} = t^0\}$$

$$= \{1, 5, 9, 13, 17, 21\}$$

$$= \mathcal{H}_{21}$$

where modulo 24 arithmetic is used in the exponents.

To illustrate the computation of F-cycles, consider the normalized PP

$$f(x) = x^9 + 2x^7 + 12x^5 + 4x^3 + 17x$$

over $\mathbb{F}_{25}$. For all $k, (1 \leq k \leq d)$, the non-zero coefficients a_{d-k} are $a_7,\ a_5,\ a_3$ and a_1, which correspond to $k = 2,\ 4,\ 6$, and 8, and $g_k = \gcd(k, 24) = 2,\ 4,\ 6$, and 8 respectively. We

next compute $j = \min_k\{g_k\} = \min\{2, 4, 6, 8\} = 2$. So, the length of the F-cycle on $f(x)$ is $(q-1)/j = 24/2 = 12$. That $F^{12}(f(x)) = f(x)$ is easily verified. Note also that the length of each respective F_k-cycle is the order of the subgroup $\mathcal{H}_{t^k}$, which, referring to the list above, is $ord(\mathcal{H}_{t^2}) = 12,\ ord(\mathcal{H}_{t^4}) = 6,\ ord(\mathcal{H}_{t^6}) = 4$, and $ord(\mathcal{H}_{t^8}) = 3$, and their least common multiple is 12, which is the length of the F-cycle on $f(x)$.

In general, for larger degree normalized PPs over $\mathbb{F}_q$, there is a k such that $\gcd(k, q-1) = 1$, so the length of the F-cycle is $q-1$. This means if there is a normalized PP $a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ such that $a_{d-k} \neq 0$, then there is also one in which $a_{d-k} = 1$. This allows us to fix an additional coefficient a_{d-k} to the values in $\{0, 1\}$, thus reducing the search space for PPs to $O(q^{d-3})$.

2.2.2 The *G*-map

Though the G-map does not reduce the search space by an order of magnitude by itself, it is useful when used in conjunction with the F-map. Consider that for some k, $\gcd(k, q-1) = 1$, allowing us to fix the a_{d-k} coefficient to $\{0, 1\}$. When a_{k-d} is fixed to 0, we can actually choose a new value k' and apply the F-map to the coefficient $a_{d-k'}$. However, it may be the case that $\gcd(k', q-1) \neq 1$, giving us a larger set of values that must be searched through. In this case, the G-map can help reduce the number of values that must be checked.

The G-map is the function that raises each coefficient in $f(x)$ to the power p.

Definition 43. *Define the* ***G*-map** *by*

$$\begin{aligned} G(f(x)) &= a_d^p x^d + a_{d-1}^p x^{d-1} + \cdots + a_{d-k}^p x^{d-k} + \cdots + a_1^p x + a_0^p \\ &= \sum_{k=0}^{d} a_{d-k}^p x^{d-k}. \end{aligned}$$

We can also consider the function G to operate directly on the elements of $\mathbb{F}_q$. This follows from the definition if we consider $f(x)$ be be a polynomial of degree zero.

We show that the set of PPs is closed under the G-map.

Lemma 44. *If $f(x)$ is a PP, then $G(f(x))$ is a PP.*

Proof. Observe that for all c, d in $\mathbb{F}_q$, $(c+d)^p = c^p + d^p$, as given by Equation 2.1 from the "Freshman's Dream" theorem. So,

$$\begin{aligned}(f(x))^p &= (a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0)^p \\ &= a_d^p (x^p)^d + a_{d-1}^p (x^p)^{d-1} + \cdots + a_1^p x^p + a_0^p \\ &= G(f(x^p)).\end{aligned}$$

Also observe that if $(z_0, z_1, \ldots, z_{q-1})$ is a permutation of $\mathbb{F}_q$, then so is $(z_0^p, z_1^p, \ldots, z_{q-1}^p)$. Suppose not. That is, suppose that $z_i^p = z_j^p$. Then $(z_i^p - z_j^p) = 0$, so, $(z_i - z_j)^p = 0$. Hence, $z_i - z_j = 0$, and so, $z_i = z_j$, a contradiction.

By assumption, $f(x)$ is a PP, so $\theta = (f(0), f(1), \ldots, f(q-1))$ is a permutation. It follows that $\pi = (f(0)^p, f(1)^p, \ldots, f(q-1)^p)$ is also a permutation. Since π is the permutation generated by the polynomial $(f(x))^p$, it follows that $(f(x))^p$ is a PP. Hence, $G(f(x^p))$ is a PP, since, as shown above, $(f(x))^p = G(f(x^p))$. This means the permutation generated by $G(f(x^p))$, namely, $(G(f(0^p)), G(f(1^p)), \ldots, G(f((q-1)^p)))$ is identical to the permutation π. That is, $\pi = (f(0)^p, f(1)^p, \ldots, f(q-1)^p) = (G(f(0^p)), G(f(1^p)), \ldots, G(f((q-1)^p)))$.

Note also that $\sigma = (0^p, 1^p, \ldots, (q-1)^p)$ is a permutation. Applying $f(x)$ to σ yields the permutation $\rho = (f(0^p), f(1^p), \ldots, f((q-1)^p))$. Since ρ is a permutation, it is simply a reordering of the permutation $\theta = (f(0), f(1), \ldots, f(q-1))$. Hence the sequence $\tau = (G(f(0)), G(f(1)), \ldots, G(f(q-1)))$ is simply a reordering of the permutation $\pi = (G(f(0^p)), G(f(1^p)), \ldots, G(f((q-1)^p)))$. That is, τ is a permutation. Finally, observe that τ is the permutation generated by applying the G-map to the PP $f(x)$. So it follows that $G(f(x)) = (a_d)^p x^d + (a_{d-1})^p x^{d-1} + \cdots + (a_1)^p x + (a_0)^p$ is a PP over $\mathbb{F}_q$. □

We now show that the G-map preserves any normalization.

Corollary 45. *If $f(x)$ is a PP in standard normalized form, m-normalized form, or b-normalized form, then $G(f(x))$ is a PP normalized in the same form.*

Proof. By Lemma 44, we only need to show that $G(f(x))$ is normalized when $f(x)$ is normalized. Note that for any normalized $f(x)$, the coefficient of x^d is $a_d = 1$. Hence, by the definition of the G-map, the coefficient of x^d in $G(f(x))$ is $a_d^p = 1^p = 1$.

For any coefficient fixed at 0, that coefficient in $G(f(x))$ is $0^p = 0$. Therefore, by the normalization definitions, all fixed coefficients in $f(x)$ will remain unchanged in $G(f(x))$, thus $G(f(x))$ will be a PP with the same normalization. □

Consider iterations of the G-map, namely, the sequence

$$f(x), G(f(x)), G^2(f(x)), \ldots, G^i(f(x)), \ldots, \tag{2.3}$$

where $G^i(f(x)) = \sum_{k=0}^{d} a_{d-k}^{p^i} x^{d-k}$. Iterative use of the G-map on the $(d-k)^{th}$ coefficient yields the sequence

$$a_{d-k} = a_{d-k}^{p^0},\ a_{d-k}^{p^1},\ a_{d-k}^{p^2},\ \ldots,\ a_{d-k}^{p^m \pmod{p^m-1}} = a_{d-k}$$

where $a_{d-k}^{p^m \pmod{p^m-1}} = a_{d-k}$, because $p^m = 1 \pmod{p^m - 1}$. This forms a cycle of length m.

Let $r_{a_{d-k}} \pmod{p^m - 1}$ be the smallest integer such that $a_{d-k}^{p^{(r_{a_{d-k}})}} = a_{d-k}$. The sequence of coefficients $a_{d-k},\ a_{d-k}^{p^1},\ \ldots,\ a_{d-k}^{p^{(r_{a_{d-k}})}} = a_{d-k}$ is called the ***G*-cycle on the coefficient a_{d-k}**. Define the length of the G-cycle on the coefficient a_{d-k} to be this integer r_k.

Observe that for any PP $f(x)$, there is an integer $r \geq 1$, such that the sequence of iterates of the G-map shown in Equation 2.3 forms a cycle.

Definition 46. *The sequence of iterates of the G-map on the PP $f(x)$, namely*

$$f(x), G(f(x)), G^2(f(x)), \ldots,\ G^r(f(x)) = f(x),$$

is called the ***G*-cycle on $f(x)$**.

Consider the values of k for which the coefficient a_{d-k} in $f(x)$ is nonzero. For all such k, $(1 \leq k \leq d)$, let $r_{a_{d-k}} = \min_{1 \leq j \leq m} \{j \mid ip^j \pmod{p^m - 1} = i\}$, where $a_{d-k} = t^i$ for some i. The

length of the G-cycle on $f(x)$ is $r = \max_k\{r_{a_{d-k}}\}$. Note that for any element a in $\mathbb{F}_{q=p^m}$, the length of the G-cycle containing a is a divisor of m. Therefore, the length of the G-cycle on $f(x)$ must be the least common multiple of the lengths of the G-cycles on all nonzero coefficients of $f(x)$.

To illustrate G-cycles on coefficients, consider $\mathbb{F}_{16=2^4}$. The G-map partitions the elements of $\mathbb{F}_{16}$ into 6 disjoint subgroups, where each subgroup contains the elements of the G-cycle on the member coefficients. We label these subgroups [0], [1], [2], [4], [6], and [8] based on their smallest member.

$$
\begin{aligned}
[0] &= \{0^{2^i}\} = \{0\} \text{ for all } i \\
[1] &= [t^0] = \{(t^0)^{2^i}\} = \{1\} \text{ for all } i \\
[2] &= [t^1] = \{(t^1)^{2^i}\} \text{ for all } i \\
&= \{t^{2^0}, t^{2^1}, t^{2^2}, t^{2^3}, t^{2^4}, \dots\} \\
&= \{t^1, t^2, t^4, t^8, t^1, \dots\} \\
&= \{2, 3, 5, 9\} \\
[4] &= [t^3] = \{(t^3)^{2^i}\} \text{ for all } i \\
&= \{(t^3)^{2^0}, (t^3)^{2^1}, (t^3)^{2^2}, (t^3)^{2^3}, (t^3)^{2^4}, \dots\} \\
&= \{t^3, t^6, t^{12}, t^9, t^3, \dots\} \\
&= \{4, 7, 10, 13\}
\end{aligned}
\qquad
\begin{aligned}
[6] &= [t^5] = \{(t^5)^{2^i}\} \text{ for all } i \\
&= \{(t^5)^{2^0}, (t^5)^{2^1}, (t^5)^{2^2}, \dots\} \\
&= \{t^5, t^{10}, t^5, \dots\} \\
&= \{6, 11\} \\
[8] &= [t^7] = \{(t^7)^{2^i}\} \text{ for all } i \\
&= \{(t^7)^{2^0}, (t^7)^{2^1}, (t^7)^{2^2}, (t^7)^{2^3}, (t^7)^{2^4}, \dots\} \\
&= \{t^7, t^{14}, t^{13}, t^{11}, t^7, \dots\} \\
&= \{8, 12, 14, 15\}
\end{aligned}
$$

Note that since we are in $\mathbb{F}_{16}$, the exponents are calculated using arithmetic modulo 15. The size of each subgroup is the length of the corresponding G-cycle on the coefficient a_{d-k}. In this case, there are cycles of lengths 1, 2, and 4, as those are the divisors of $m = 4$.

To illustrate the computation of the G-cycle on $f(x)$, consider the normalized PP over $\mathbb{F}_{16}$,

$$f(x) = x^7 + x^5 + 8x^4 + 6x^2 + 4x.$$

We want to consider the values of k, $1 \leq k \leq d$, such that the coefficient a_{d-k} is nonzero. This gives us $a_5 = 1,\ a_4 = 8,\ a_2 = 6$ and $a_1 = 4$, which correspond to $k = 2$, 3, 5, and 6, respectively. As previously shown, the G-cycle of the coefficient $a_4 = 8 = t^7$, is subgroup $[8] = \{8, 12, 14, 15\}$, which gives the 4 successive coefficients of x^4 in the iterates of the G-map on $f(x)$ shown below. We compute the length of the G-cycle for each nonzero coefficient a_{d-k}, namely, $r_{a_{d-k}} = \min_{1 \leq j \leq m} \{j \mid ip^j \pmod{p^m - 1} = i\}$ resulting in $r_{a_5} = r_1 = 1$, $r_{a_4} = r_8 = 4$, $r_{a_2} = r_6 = 2$, $r_{a_1} = r_4 = 4$. By Definition 46, the length of the G-cycle on $P(x)$ is $\max_k \{r_{a_{d-k}}\} = 4$, as verified below.

$$
\begin{aligned}
f(x) &= x^7 + x^5 + 8x^4 + 6x^2 + 4x \\
G(f(x)) &= 1^2x^7 + 1^2x^5 + 8^2x^4 + 6^2x^2 + 4^2x \\
&= (t^0)^2x^7 + (t^0)^2x^5 + (t^7)^2x^4 + (t^5)^2x^2 + (t^3)^2x \\
&= (t^0)x^7 + (t^0)x^5 + (t^{14})x^4 + (t^{10})x^2 + (t^6)x \\
&= x^7 + x^5 + 15x^4 + 11x^2 + 7x \\
G^2(f(x)) &= (t^0)^2x^7 + (t^0)^2x^5 + (t^{14})^2x^4 + (t^{10})^2x^2 + (t^6)^2x \\
&= (t^0)x^7 + (t^0)x^5 + (t^{28})x^4 + (t^{20})x^2 + (t^{12})x \\
&= (t^0)x^7 + (t^0)x^5 + (t^{13})x^4 + (t^5)x^2 + (t^{12})x \\
&= x^7 + x^5 + 14x^4 + 6x^2 + 13x \\
G^3(f(x)) &= (t^0)^2x^7 + (t^0)^2x^5 + (t^{13})^2x^4 + (t^5)^2x^2 + (t^{12})^2x \\
&= (t^0)x^7 + (t^0)x^5 + (t^{26})x^4 + (t^{10})x^2 + (t^{24})x \\
&= (t^0)x^7 + (t^0)x^5 + (t^{11})x^4 + (t^{10})x^2 + (t^9)x \\
&= x^7 + x^5 + 12x^4 + 11x^2 + 10x \\
G^4(f(x)) &= (t^0)^2x^7 + (t^0)^2x^5 + (t^{11})^2x^4 + (t^{10})^2x^2 + (t^9)^2x \\
&= (t^0)x^7 + (t^0)x^5 + (t^{22})x^4 + (t^{20})x^2 + (t^{18})x \\
&= (t^0)x^7 + (t^0)x^5 + (t^7)x^4 + (t^5)x^2 + (t^3)x
\end{aligned}
$$

$$= x^7 + x^5 + 8x^4 + 6x^2 + 4x$$
$$= f(x)$$

Observe that the lengths of G-cycles on each of the nonzero coefficients $a_d - k, (1 \leq k \leq 7)$, are 1, 4, 2 and 4, respectively. Thus, the length of the G-cycle on $f(x)$ is 4, as their least common multiple is 4.

2.2.3 Iterating the F-map and the G-map

We have introduced two functions, the F-map and G-map, that transform normalized PPs into other normalized PPs. These functions can be applied sequentially. For example, we can represent the application of the F and G maps alternately two times on the PP $f(x)$ by the sequence $(G \circ F \circ G \circ F)(f(x))$, meaning one first applies the F-map, then the G-map, the F-map, and finally the G-map again. By using the F-map and G-map together, a single normalized PP can represent a subgroup of normalized PPs, computed through these F-map and G-map iterations.

It is interesting to note that two different sequences of compositions can represent the same transformation. In the following we show that we can replace any sequence of compositions by an equivalent sequence in which all of the G-maps are applied first, followed by some number of F-maps. The number of F-maps is related to the field characteristic p. Our result is illustrated by the following diagram, which indicates that $(G \circ F)(f(x))$ is the same as $(F^p \circ G)(f(x))$, for all PPs $f(x)$.

$$\begin{array}{ccc} f(x) & \xrightarrow{\quad G \quad} & G(f(x)) \\ {\scriptstyle F}\downarrow & & \downarrow{\scriptstyle F^p} \\ F(f(x)) & \xrightarrow[\quad G \quad]{} & (F^p \circ G)(f(x)) \end{array}$$

In Lemma 47, we show that any sequence of F-maps and G-maps is equivalent to a sequence F^i, G^j, for some i $(0 \leq i \leq r)$ and some j $(0 \leq j \leq s)$, where r is the length of the F-cycle and s is the length of the G-cycle.

Lemma 47. *For any PP $f(x)$, $(G \circ F)(f(x)) = (F^p \circ G)(f(x))$.*

Proof. Let $f(x) = \sum_{k=0}^{d} a_{d-k} x^{d-k}$. If $a_{d-k} = 0$ then the coefficients of x^{d-k} in $(G \circ F)(f(x))$ and $(F^p \circ G)(f(x))$ are both 0. Suppose that $a_{d-k} \neq 0$. Then $a_{d-k} = t^j$, for some j, $0 \leq j \leq q-2$. Then the x^{d-k}-th term in $F(f(x))$, $G(f(x))$, $(G \circ F)(f(x))$, and $(F^p \circ G)(f(x))$, respectively, are:

$$
\begin{aligned}
F(f(x)) &= \cdots + t^{j+k} x^{d-k} + \ldots \\
G(f(x)) &= \cdots + t^{pj} x^{d-k} + \ldots \\
(G \circ F)(f(x)) &= \cdots + t^{(j+k)^p} x^{d-k} + \cdots = \cdots + t^{p(j+k)} x^{d-k} + \ldots \\
(F^p \circ G)(f(x)) &= \cdots + t^{pj+pk} x^{d-k} + \cdots = \cdots + t^{p(j+k)} x^{d-k} + \ldots
\end{aligned}
$$

Hence, the coefficients of x^{d-k}, $0 \leq k \leq d$ in $(G \circ F)(f(x))$ and $(F^p \circ G)(f(x))$ are equal and the lemma follows. □

For example, let $f(x)$ be an PP over $\mathbb{F}_{32=2^5}$. Consider $(G \circ F \circ G \circ F)(f(x))$. Since $p = 2$, by Lemma 47 $(G \circ F)(f(x)) = (F^2 \circ G)(f(x))$. So, $(G \circ F \circ G \circ F)(f(x)) = (G \circ F \circ F^2 \circ G)(f(x)) = (G \circ F^3 \circ G)(f(x))$. Then by an iterative use of Lemma 47, we get $(G \circ F^3 \circ G)(f(x)) = (F^6 \circ G \circ G)(f(x)) = (F^6 \circ G^2)(f(x))$.

For the purpose of our PP search, we are interested in the set of PPs that can be reached through some iteration of the F-map and G-map on a given PP. Specifically, Lemma 47 lets us know this set can be obtained by calculating the F-cycle on each PP of the G-cycle on $f(x)$.

Definition 48. *Let f(x) and g(x) be PPs of degree d in $\mathbb{F}_q$. If f(x) can be converted into g(x) by some sequence consisting of F-map and G-map operations, then f(x) and g(x) are* ***FG*-related**.

We are also interested in observing the iteration of the F-map and G-map on a single coefficient of a PP.

Definition 49. *Let a_k be the coefficient of the x^k term of the PP $f(x)$. Let a'_k be the coefficient of the x^k term of any PP FG-related to $f(x)$. We define the union of all possible values of a'_k the* ***FG*-cycle of the coefficient**.

Coefficients with larger FG-cycles are better candidates when considering which coefficient to fix. Specifically, we want to select a coefficient that requires the fewest representatives such that the union of their FG-cycles cover all nonzero elements of $\mathbb{F}_q$.

2.3 Optimized Search Algorithm

Algorithm 1 computes the set $\mathcal{S}$ of all normalized PPs in $\mathbb{F}_q$ of degree d, and utilizes improved normalization, the F-map, and the G-map to reduce the search space from $O(n^{d+1})$ to $O(n^{d-3})$. Our improved normalization allows us to fix the leading coefficient at 1, the constant term at 0, and a designated third coefficient at 0, even for cases when $p \mid d$. The F-map and G-map are then used together to fix a fourth coefficient. Even though m or b-normalization may be used in the search, the returned set of PPs are in standard normalized form, as it is the general convention.

To designate which coefficients are currently locked, the algorithm uses *masks*. Define a mask as a Boolean array associated with a polynomial's coefficients. False, or 0, designates that the corresponding coefficient should not change, as it is fixed at a particular value. True, or 1, designates the coefficient can change as the polynomial is updated, and it will always have a nonzero value. The purpose of using masks is to maximize our usage of the F-map and G-map functions. Since both the F-map and G-map take the symbol 0 to itself, masks allow us to consider only nonzero elements when selecting a coefficient to fix.

For example, consider the search for PPs of degree 5 over $\mathbb{F}_{25}$. Since $p \mid d$ and $p > 2$, the masks must correspond to m-normalization, that is, to PPs in the form $a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ where $a_5 = 1,\ a_0 = 0$, and either $a_4 = 0$ or $a_3 = 0$. Since a_5 is always fixed at

Algorithm 1: Optimized PP Search

```
1  if p ∤ d then Create the set M of all possible masks corresponding to standard
     normalization
2  else if p = 2 then Create the set M of all possible masks corresponding to
     b-normalization
3  else Create the set M of all possible masks corresponding to m-normalization
4  S = ∅
5  foreach mask m ∈ M do
6      Of the unfixed coefficients in m, select the one which requires the fewest
         representatives whose FG-cycles cover F_q. Fix this coefficient to only iterate
         through these representatives.
7      currentPolynomial = its default value where each fixed coefficient is assigned its
         designated value, and each unfixed coefficient is assigned 1
8      do
9          if currentPolynomial is a PP and currentPolynomial ∉ S then
10             T = the set of all PPs that are FG-related to currentPolynomial
11             if p | d then
12                 foreach PP f ∈ T and b ∈ F_q do
13                     T = T ∪ f(x + b)
14             S = S ∪ T
15         increment currentPolynomial
16     while currentPolynomial is not maximized
17 return S
```

1, and a_0 is always fixed at 0, we can first consider all cases where a_4 is fixed at 0. Algorithm 1 generates $2^3 = 8$ masks in the form $[a_5, a_4, a_3, a_2, a_1, a_0]$ to account for all combinations where a_3, a_2, and a_1 are either fixed at 0 or are unfixed and nonzero. The eight masks are,

$$[0,0,0,0,0,0], \quad [0,0,0,0,1,0], \quad [0,0,0,1,0,0], \quad [0,0,0,1,1,0],$$
$$[0,0,1,0,0,0], \quad [0,0,1,0,1,0], \quad [0,0,1,1,0,0], \quad [0,0,1,1,1,0].$$

The algorithm also creates an additional 4 masks for the cases where a_3 is fixed at 0, and a_4 is unfixed, namely,

$$[0,1,0,0,0,0], \quad [0,1,0,0,1,0], \quad [0,1,0,1,0,0], \quad [0,1,0,1,1,0].$$

Each of these masks has 3 coefficients fixed from normalization, but a fourth coefficient to fix must still be selected. This is done by comparing the FG-cycles of the unfixed coefficients.

Table 2.2. FG-cycles for the mask $[0, 1, 0, 1, 0, 0]$ in $\mathbb{F}_{25}$ degree 5.

$\boldsymbol{FG}$-Cycles for $\boldsymbol{a_4}$	$\boldsymbol{FG}$-Cycles for $\boldsymbol{a_2}$
$\{0\}$	$\{0\}$
$\{1, 2, 3, \ldots, 24\}$	$\{1, 4, 7, 10, 13, 16, 19, 22\}$
	$\{2, 3, 5, 6, 8, 9, 11, 12, 14, 15, 17, 18, 20, 21, 23, 24\ \}$

Consider the mask $[0, 1, 0, 1, 0, 0]$ where the FG-cycles for coefficients a_4 and a_2 are shown in Table 2.2. Ignoring the cycle $\{0\}$ since we are only concerned about nonzero values, we see that a_4 has a single cycle of length 24, while a_2 has two cycles of lengths 8 and 16. Fixing the coefficient a_2 would require checking two values, one representative from each cycle, but fixing a_4 only requires a single value, making it the better option.

Once the last fixed coefficient is decided, *currentPolynomial* is initialized to its starting value, where fixed coefficients are given their assigned values, and unfixed coefficients are assigned 1. For our example mask $[0, 1, 0, 1, 0, 0]$, this would correspond to the polynomial $x^5 + x^4 + x^2$. *currentPolynomial* is then checked to determine if it is a PP, which can be done by evaluating it for all $x \in \mathbb{F}_q$ to see if it is bijective. If *currentPolynomial* is a PP, we add all its FG-related permutations to the set $\mathcal{S}$. If it is the case that $p \mid d$, then we also apply the transformation $f(x + b)$ to each of these FG-related permutations, for all $b \in \mathbb{F}_q$. This is so the final result contains all standard normalized PPs.

Once *currentPolynomial* has been checked, it is incremented as a $d + 1$-tuple and adds 1 to the lowest degree, unfixed coefficient. If that coefficient were to exceed its maximum value, it is instead set to 1, and the next highest coefficient is incremented. Note that if the coefficient fixed by the F-map and G-map does not reduce to a single value, we can include it in our increment function, but it only increments through the minimum necessary values as determined by its FG-cycles.

If incrementing *currentPolynomial* would cause the highest degree unfixed coefficient to exceed its maximum value, then we say it is maximized, and the algorithm can proceed with

the next mask. Once all masks have been iterated, the algorithm terminates, and $\mathcal{S}$ will contain the set of all standard normalized PPs in $\mathbb{F}_q$ of degree d.

2.4 Implementation and Results

The first consideration to an implementation of Algorithm 1 is the need to use finite field arithmetic. Most math-focused programming language, such as MATLAB or Magma, will support finite field operations, but these are typically interpreted languages, which would limit execution speed. Considering this, we selected Java to implement the algorithm.

In order to use Java, we first needed to write a class to handle the finite field operations, as they are not natively supported. The class finds a primitive polynomial to generate the elements of the field, then creates tables to store the result of all possible addition, multiplication, and exponent operations. These tables are implemented as 2D integer arrays which allow the main program to perform any operation in $O(1)$ time. For example, to multiply any two values $a, b \in \mathbb{F}_q$, we simply access the value stored in the array $mult[a][b]$.

Using this optimized search algorithm, we were able to classify all PPs in all fields up to $\mathbb{F}_{97}$ of degree at most 10. Many of the searches completed within minutes or hours. Some of the larger searches took several weeks to well over a month when performed on an Intel Core i7 processor. Additional searches were completed for fields up to $\mathbb{F}_{37}$ for degree 11, but the search time quickly becomes prohibitive as the size of the field increases.

While these searches initially provided several improvements for $M(n, d)$, the results are subsumed by the search for permutation rational functions. However, the number of PPs are still needed for calculating $M(n, d)$ results for PRFs. Degree 11 results can be seen in Table 2.3. Results for degrees 6 through 10 can be found in the appendix.

Table 2.3. Number of PPs for degree 11 polynomials over $\mathbb{F}_q$.

q	**Total PPs**	**Normalized PPs**
16	4,751,093,760	1,237,264
17	4,001,494,000	865,375
19	2,431,915,488	374,256
23	0	0
25	6,509,295,000	433,953
27	2,826,989,100	149,150
29	1,014,518,484	43,083
31	385,053,480	13,356
32	190,940,160	6,015
37	446,266,620	9,055

CHAPTER 3

PERMUTATION RATIONAL FUNCTIONS[1]

Section 1.6 details some of the initial work done to classify PRFs of degree 3. In this chapter we extend our search techniques for PPs to search for PRFs of higher degree. We define several notations and formulas to provide counts of PRFs of a given degree. We then introduce several theorems which apply these formulas to combine sets of PRFs of varying degree and give improved bounds for numerous cases of $M(n, d)$. These ideas were first presented in Bereg et al. (2020) and Bereg et al. (2022).

For notation, let $f(x) = \frac{u(x)}{v(x)}$ and $g(x) = \frac{r(x)}{s(x)}$ be PRFs formed by polynomials of degree u, v, r, and s, with coefficients a_i, b_i, c_i, and d_i respectively. That is, $u(x) = \sum_{i=0}^{u} a_i x^i$, $v(x) = \sum_{i=0}^{v} b_i x^i$, $r(x) = \sum_{i=0}^{r} c_i x^i$, and $s(x) = \sum_{i=0}^{s} d_i x^i$. Also recall that $\mathbb{P}^1(\mathbb{F}_q) = \mathbb{F}_q \cup \{\infty\}$.

3.1 Optimized Search for PRFs

Let $f(x) = u(x)/v(x)$ be a PRF where the degree of $u(x)$ is u and the degree of $v(x)$ is v. A complete search for all PRFs in $\mathbb{F}_q$ would have a search space of $O(q^{u+v+2})$. While normalization is not formally defined for PRFs, we can use the same operations $a \cdot f(x+b)+c$ to reduce the search space, as we did for PPs.

First consider $a \cdot f(x) = \frac{a \cdot u(x)}{v(x)}$. If we fix the leading coefficients of both $u(x)$ and $v(x)$ at 1, this transformation will yield $q-1$ PRFs just as it would a PP. Such a PRF is also called *monic*. It is beneficial to fix both coefficients at 1 in order to avoid duplicates in the search, as $f(x) = \frac{u(x)}{v(x)} = \frac{2u(x)}{2v(x)} = \frac{3u(x)}{3v(x)}$, etc.

Let us next consider $f(x) + c$, and assume that $u > v$. We make this assumption because if $\frac{u(x)}{v(x)}$ is a PRF, then so is $\frac{v(x)}{u(x)}$, so it is only necessary to search one of the cases. Later we

[1]

will also show in Theorem 52 we can obtain all PRFs where $u = v$ by transforming the results where $u > v$, so we can omit this case as well. This gives us

$$\begin{aligned} f(x) + c &= \frac{u(x)}{v(x)} + c \\ &= \frac{u(x)}{v(x)} + \frac{c \cdot v(x)}{v(x)} \\ &= \frac{u(x) + c \cdot v(x)}{v(x)}. \end{aligned}$$

Since $u > v$, the polynomial $u(x) + c \cdot v(x)$ will also be of degree u, so $f(x) + c$ yields a new PRF of degree u over degree v. To take advantage of this transformation, we can fix the constant term of $u(x)$ at 0 and only allow the nonzero constant terms for $v(x)$. Note that we always want nonzero constant terms for $v(x)$, otherwise we would have both $f(0) = \infty$ and $f(\infty) = \infty$, so it would not generate a permutation. Any PRF we find in this manner would then represent q total PRFs by considering all $c \in \mathbb{F}_q$.

Lastly, we consider $f(x + b)$. For some value b, we could fix the second coefficient of either $u(x)$ or $v(x)$ at 0, but not necessarily both. For this transformation to not interfere with the transformation $f(x) + c$, we must explicitly choose the denominator $v(x)$. If for example $u = 4$ and $v = 3$ and we tried to fix the second coefficient of $u(x)$, that is the x^3 term, then the operation $u(x) + c \cdot v(x)$ would add some value to that coefficient, changing it from our fixed value of 0. This means we must also consider if $p \mid v$. If $p \nmid v$, we simply fix the second coefficient of $v(x)$ at 0 like standard normalization of a PP. If instead $p \mid v$, we can still choose a new coefficient to fix by utilizing either m or b-normalization.

Using these three normalization operations allows us to fix 4 coefficients of a PRF, but we can still fix one additional coefficient by utilizing the F-map and G-map. With a total of 5 fixed coefficients, the search space is reduced from $O(q^{u+v+2})$ to $O(q^{u+v-3})$.

3.2 Counting PRFs

Let $N_d(q)$ be the number of permutation polynomials of degree d over $\mathbb{F}_q$. We generalize this notation by defining $N_{u,v}(q)$, $N^m_{u,v}(q)$, and other useful concepts for PRFs.

Definition 50. *Let $P_{u,v}(q) = \{u(x)/v(x) \mid u(x)$ has degree u, $v(x)$ has degree v, and $u(x)/v(x)$ is a PRF $\}$. Let $\Pi_{u,v}(q)$ be the set of permutations on $\mathbb{P}^1(\mathbb{F}_q)$ defined by the PRFs in $P_{u,v}(q)$.*

Let $P^m_{u,v}(q)$ denote the corresponding set for monic PRFs, and let $\Pi^m_{u,v}(q)$ be the related set of permutations. Also, let $N_{u,v}(q) = |P_{u,v}(q)|$ and $N^m_{u,v}(q) = |P^m_{u,v}(q)|$.

Let $\mathcal{G}_u(q) = N_{u,u}(q) + 2\sum_{v<u} N_{u,v}(q)$ be the number of degree u PRFs.

In order to obtain lower bounds for $M(n,d)$ we need to know the number of degree u PRFs of the form $u(x)/v(x)$, where $u(x)$ is of degree u and $v(x)$ is of degree $v \leq u$, for a given u. That is, we need $N_{u,v}(q)$ for u and v as described. For example, for all q, we need to know $N_{4,3}(q)$ and such specific values are not immediately evident from Ding and Zieve (2020), Hou (2020) or Hou and Sze (2020).

To begin, we show in Theorem 52 that for any $u > 1$, $N_{u,u}(q) = (q-1)\sum_{v<u} N_{u,v}(q)$. $N_{u,u}(q)$ and $N_{u,v}(q)$ are used in the computation of $\mathcal{S}_k(q)$ and $\mathcal{T}_k(q)$, which are defined below. These are used in our lower bound theorems for $M(q,d)$ and $M(q+1,d)$. In Theorem 53, we provide a simpler formula for $\mathcal{G}_u(q)$ which we use in several additional proofs.

Lemma 51. *If $u(x)/v(x)$ is a PRF of degree u over degree v and $u > v$, then $v(x)/u(x) + c$ for any $c \neq 0$, is a PRF of degree u over degree u.*

Proof. Assume $u(x)/v(x)$ is a PRF of degree u over degree v and $u > v$. Then $v(x)/u(x)$ is also a PRF. We can express the addition of any constant c to $v(x)/u(x)$ as a new PRF $\frac{v(x)+c\cdot u(x)}{u(x)}$. If c is nonzero, then the coefficient of the x^u term of $c \cdot u(x)$ will also be nonzero. Since $u > v$, the resulting PRF must be degree u over degree u. □

Theorem 52. *For all q and for any $u > 1$, $N_{u,u}(q) = (q-1)\sum_{v<u} N_{u,v}(q)$.*

Proof. Let u be arbitrary, and let $v < u$. There are $N_{u,v}(q)$ PRFs of degree u over degree v for any specific v. By Lemma 51, each gives rise to a PRF of degree u over degree u of the form $\frac{v(x)+c\cdot u(x)}{u(x)}$. Since there are $q-1$ nonzero options for $c \in \mathbb{F}_q$, there are $(q-1)N_{u,v}(q)$ PRFs of degree u over degree u. Thus, $N_{u,u}(q) = (q-1)\sum_{v<u} N_{u,v}(q)$.

To show each of these PRFs is unique, assume we have two PRFs $\frac{u(x)}{v(x)}$ and $\frac{r(x)}{s(x)}$ where $u > v$, $r > s$, $u = r$, and $\frac{v(x)}{u(x)} + c = \frac{s(x)}{r(x)} + d$ for some constants c and d. We have

$$\frac{v(x)}{u(x)} = \frac{s(x)}{r(x)} + c', \text{ where } c' = d - c$$
$$\frac{v(x)}{u(x)} = \frac{s(x) + c' \cdot r(x)}{r(x)}$$
$$v(x)r(x) = s(x)u(x) + c' \cdot r(x)u(x)$$

Note that the polynomial $v(x)r(x)$ has degree $v+r$ and the polynomial $s(x)u(x)+c'\cdot r(x)u(x)$ has degree $r+u > v+r$ since $v < u = r$. Thus, the equality holds only when $c' = 0$, meaning $c = d$. Therefore, the PRFs in the summation are unique.

To show that all PRFs of degree u over degree u are accounted for, we show that any such PRF can be transformed to a PRF where the degree of the numerator is greater than the degree of the denominator by performing the operations in reverse order. Consider an arbitrary PRF $\frac{v(x)}{u(x)}$ such that $v = u$. Adding a constant c gives us $\frac{v(x)+c\cdot u(x)}{u(x)}$. If we choose $c = \frac{-b_v}{a_u}$, the leading coefficient of the numerator becomes $b_v + ca_u = 0$, and the resulting PRF $\frac{v'(x)}{u(x)}$ will have $v' < u$. Note that depending on the values of the other coefficients, it is possible that more than just the leading coefficient is zeroed out. If we then take the inverse PRF $\frac{u(x)}{v'(x)}$, we will have a PRF where the degree of the numerator is greater than the degree of the denominator. Thus, $\frac{v(x)}{u(x)}$ can be found through Lemma 51. □

Theorem 53. *For q and for all $u > 1$, $\mathcal{G}_u(q) = (q+1)\sum_{v<u} N_{u,v}(q)$.*

Proof. Recall that $\mathcal{G}_u(q) = N_{u,u}(q) + 2\sum_{v<u} N_{u,v}(q)$. Using Theorem 52 to substitute for $N_{u,u}(q)$ gives $\mathcal{G}_u(q) = (q-1)\sum_{v<u} N_{u,v}(q) + 2\sum_{v<u} N_{u,v}(q) = (q+1)\sum_{v<u} N_{u,v}(q)$. □

We make the following straightforward observations, which are used in many of our proofs.

Observation 1: $N_{d,0}(q) = N_d(q)$.

Of specific interest are the formulas for $N_{2,0}(q),\ N_{3,0}(q),\ N_{4,0}(q)$, and $N_{5,0}(q)$, the number of permutation polynomials of degree 2, 3, 4 and 5, respectively. Formulas for these values can be found in Chu et al. (2004), but we reproduce them as equations 3.2 through 3.5 below.

Observation 2: $N_{v,u}(q) = N_{u,v}(q)$.

To see why, note that $\frac{u(x)}{v(x)}$ is a PRF if and only if $\frac{v(x)}{u(x)}$ is also a PRF. That is, if $(\pi_0, \pi_1, \ldots, \pi_q)$ is a permutation of $\mathbb{P}^1(\mathbb{F}_q)$, then $(\pi_0^{-1}, \pi_1^{-1}, \ldots, \pi_q^{-1})$ is also a permutation of $\mathbb{P}^1(\mathbb{F}_q)$.

Observation 3: $N_{u,v}^m(q) \geq \frac{1}{q-1} N_{u,v}(q)$.

To see why, note that $\frac{u(x)}{v(x)} = \sum_{i=0}^{u} a_i x^i / v(x) = a_u x^u / v(x) + \sum_{i=0}^{u-1} a_i x^i / v(x)$. There are $q-1$ nonzero values for the high-order coefficient $a_u \in \mathbb{F}_q$, so by the Pigeonhole Principle, there are at least $\frac{1}{q-1} N_{u,v}(q)$ monic PRFs of degree u over degree v.

Observation 4: $N_{u,1}(q) = 0 = N_{1,u}(q),\ \textit{for all } u > 1$.

To see why, consider any rational function $\frac{u(x)}{v(x)}$ such that $v = 1$. Note that $v(x)$ has one root, say a, that is, $v(a) = 0$. Then $\frac{u(a)}{v(a)} = \frac{u(a)}{0} = \infty$. Also, since $u > v$, $\frac{u(\infty)}{v(\infty)} = \infty$. Thus, ∞ appears in two positions, so $\frac{u(x)}{v(x)}$ is not a PRF. Hence, $N_{u,1}(q) = 0$, and so $N_{1,u}(q) = 0$ as well.

We summarize known results for degree 1, 2, 3, 4 and degree 5 PRFs. First, from Chu et al. (2004) we have,

$$N_{1,0}(q) = q(q-1) \qquad \text{for all } q, \tag{3.1}$$

$$N_{2,0}(q) = \begin{cases} q(q-1), & \text{when } q = 2^m, \\ 0, & \text{otherwise.} \end{cases} \tag{3.2}$$

$$N_{3,0}(q) = \begin{cases} \frac{1}{2}q(q-1)^2 + q(q-1), & \text{when } q \equiv 0 \pmod 3, \\ 0, & \text{when } q \equiv 1 \pmod 3, \\ q^2(q-1), & \text{when } q \equiv 2 \pmod 3. \end{cases} \tag{3.3}$$

$$N_{4,0}(q) = \begin{cases} 0, & \text{for odd } q > 7, \\ \frac{1}{3}q(q-1)(q^2+2), & \text{for even } q > 7. \end{cases} \tag{3.4}$$

$$N_{5,0}(q) = \begin{cases} \frac{1}{2}q^2(q-1)^2 + \frac{3}{4}q(q-1)^2 + q(q-1), & \text{when } q \equiv 0 \pmod 5, \\ 0, & \text{when } q \equiv 1 \pmod 5, \\ q^3(q-1), & \text{when } q \equiv 2, 3 \pmod 5, \\ q^2(q-1), & \text{when } q \equiv 4 \pmod 5. \end{cases} \tag{3.5}$$

For degree 3 PRFs, the following results are known (Ferraguti and Micheli, 2020):

$$N_{3,2}(q) = \tfrac{1}{2}q^2(q-1)^2, \qquad \text{for all } q, \tag{3.6}$$

$$N_{3,3}(q) = \begin{cases} \frac{1}{2}(q^5 - 2q^4 + 2q^3 - 2q^2 + q), & \text{when } q \equiv 0 \pmod 3, \\ \frac{1}{2}q^2(q-1)^3, & \text{when } q \equiv 1 \pmod 3, \\ \frac{1}{2}q^2(q-1)^2(q+1), & \text{when } q \equiv 2 \pmod 3. \end{cases} \tag{3.7}$$

For degree 4 PRFs, it is known that (Hou and Sze, 2020)

$$N_{4,2}(q) = 0, \text{ for all } q > 7. \tag{3.8}$$

As observed earlier, $N_{u,v}(q) = N_{v,u}(q)$, so $N_{2,4}(q) = 0$ as well. Recall that $\mathcal{G}_u(q)$ is the number of PRFs of degree u. The number of degree 4 PRFs is (Ding and Zieve, 2020; Hou, 2020)

$$\mathcal{G}_4(q) = \begin{cases} \frac{1}{3}(q^3 - q)^2, & \text{when } q \text{ is odd and } q > 7, \\ \frac{1}{3}q(q-1)(q+2)(q^3+1), & \text{when } q \text{ is even and } q > 7. \end{cases} \tag{3.9}$$

We now use Theorem 53, Observation 4 and equations 3.1 through 3.7 to derive expressions for $\mathcal{G}_1(q)$, $\mathcal{G}_2(q)$ and $\mathcal{G}_3(q)$ which are used in several theorems in Section 3.3.

$$\mathcal{G}_1(q) = (q+1)N_{1,0}(q) = (q+1)q(q-1) = |PGL(2,q)|. \tag{3.10}$$

$$\mathcal{G}_2(q) = (q+1)N_{2,0}(q) = \begin{cases} (q+1)q(q-1), & \text{when } q = 2^m, \\ 0, & \text{otherwise.} \end{cases} \tag{3.11}$$

$$\begin{aligned} \mathcal{G}_3(q) &= (q+1)(N_{3,2}(q) + N_{3,0}(q)) \\ &= \begin{cases} (q+1)(\frac{1}{2}q^2(q-1)^2 + \frac{1}{2}q(q-1)^2 + q(q-1)), & \text{when } q \equiv 0 \pmod 3, \\ (q+1)(\frac{1}{2}q^2(q-1)^2), & \text{when } q \equiv 1 \pmod 3, \\ (q+1)(\frac{1}{2}q^2(q-1)^2 + q^2(q-1)), & \text{when } q \equiv 2 \pmod 3. \end{cases} \end{aligned} \tag{3.12}$$

In Theorem 54, we derive a closed formula for $N_{4,3}(q)$ for all prime powers $q > 7$.

Theorem 54. *For all prime powers $q > 7$, $N_{4,3}(q) = \frac{1}{3}(q+1)q^2(q-1)^2$.*

Proof. By Theorem 53 and using Observation 4 and equation 3.8 to eliminate terms, the number of degree 4 PRFs for $q > 7$ is

$$\mathcal{G}_4(q) = (q+1)(N_{4,3}(q) + N_{4,0}(q)).$$

Solving for $N_{4,3}(q)$, we get

$$N_{4,3}(q) = \tfrac{1}{q+1}\mathcal{G}_4(q) - N_{4,0}(q).$$

For odd values of $q > 7$, Ding and Zieve (2020) proved that there are $\mathcal{G}_4(q) = \frac{1}{3}(q^3-q)^2 = \frac{1}{3}(q+1)^2q^2(q-1)^2$ degree 4 PRFs. By equation 3.4 we know that $N_{4,0}(q) = 0$ for odd q. Hence

$$\begin{aligned} N_{4,3}(q) &= \tfrac{1}{q+1}\mathcal{G}_4(q) \\ &= \tfrac{1}{3}(q+1)q^2(q-1)^2 \end{aligned}$$

Now consider even values of $q > 7$. Ding and Zieve (2020) proved that there are $\mathcal{G}_4(q) = \frac{1}{3}q(q-1)(q+2)(q^3+1)$ degree 4 PRFs. By equation 3.4, $N_{4,0}(q) = \frac{1}{3}q(q-1)(q^2+2)$ when $q > 7$ is even. Hence,

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

□

We define two new quantities, $\mathcal{T}_k(q)$ and $\mathcal{S}_k(q)$, which are used to construct lower bounds for $M(q+1, q-k)$ and $M(q, q-k)$. Furthermore, by adding the term $N^m_{\frac{k+3}{2},\frac{k+1}{2}}(q)$ to $\mathcal{T}_k(q)$ and to $\mathcal{S}_k(q)$, we obtain new lower bounds for $M(q+1, q-k-1)$ and $M(q, q-k-1)$. The choices for u and v in the definitions are specifically tailored to meet certain degree requirements for the PRFs, as will be explained in Sections 3.3 and 3.4.

Definition 55. *For odd integers k, let $\mathcal{T}_k(q) = |\bigcup_{u,v} \Pi_{u,v}(q)| = \sum_{u,v} N_{u,v}(q)$, for all $u, v \leq (k+1)/2$. Recursively, we have*

$$\mathcal{T}_k(q) = \begin{cases} \mathcal{G}_1(q) = N_{1,1}(q) + N_{1,0}(q) + N_{0,1}(q) = |PGL(2,q)|, & \text{when } k = 1, \\ \mathcal{T}_{k-2}(q) + \mathcal{G}_{\frac{k+1}{2}}(q), & \text{when } k \geq 3. \end{cases} \tag{3.13}$$

where $|PGL(2,q)| = (q+1)q(q-1)$.

For example,

$$\mathcal{T}_3(q) = \begin{cases} 2(q+1)q(q-1) = 2q^3 - 2q, & \text{when } q = 2^m, \\ (q+1)q(q-1) = q^3 - q, & \text{otherwise.} \end{cases} \tag{3.14}$$

Definition 56. *For odd integers k, let $\mathcal{S}_k(q) = \sum_{u,v} N_{u,v}(q)$, where u and v are evaluated as*

$$u, v \leq \begin{cases} (k+1)/2, & \text{when } u > v, \\ (k-3)/2, & \text{when } u \leq v. \end{cases}$$

Recursively, we have

$$\mathcal{S}_k(q) = \begin{cases} N_{1,0}(q) = |AGL(1,q)|, & \text{when } k = 1, \\ \mathcal{S}_{k-2}(q) + \sum_{v<j} N_{j,v}(q) + \sum_{u \le j-2} N_{u,j-2}(q), & \text{when } k \ge 3,\ j = \frac{k+1}{2}. \end{cases} \tag{3.15}$$

where $|AGL(1,q)| = q(q-1)$.

For example,

$$\mathcal{S}_3(q) = \begin{cases} 2q(q-1) = 2q^2 - 2q, & \text{when } q = 2^m, \\ q(q-1) = q^2 - q, & \text{otherwise.} \end{cases} \tag{3.16}$$

3.3 New Lower Bounds for $M(q+1,\ d)$

We now discuss properties of PRFs that are useful for improving lower bounds for $M(q+1, d)$ for various d. Some similar ideas were given in Yang et al. (2008).

Recall that by definition, $\gcd(u(x), v(x)) = 1$ for any PRF, as this property is implicit in our counting arguments. For the proofs in this section, we consider the PRFs $f(x) = \frac{u(x)}{v(x)}$ and $g(x) = \frac{r(x)}{s(x)}$ that permute the elements of $\mathbb{P}^1(\mathbb{F}_q)$, and such that $u(x)s(x) - v(x)r(x)$ is not a constant. The degrees of the PRFs $f(x)$ and $g(x)$ need not be the same.

Note that the number of values $a \in \mathbb{F}_q$ such that $f(a) = g(a)$ is given by the number of roots for the polynomial $u(x)s(x) - v(x)r(x)$. That is, the number of agreements between the permutations generated by the PRFs $f(x)$ and $g(x)$ is given by the degree of the polynomial, which is $\max\{u + s, v + r\}$.

Definition 57.

$$\delta_1 = \deg(u(x)s(x) - v(x)r(x)) \le \max\{u + s, v + r\}, \text{ and}$$

$$\delta_2 = \begin{cases} 1, & \text{when } f(\infty) = g(\infty), \\ 0, & \text{otherwise.} \end{cases}$$

Lemma 58. *Let π and σ be the permutations of $\mathbb{P}^1(\mathbb{F}_q)$ generated by $f(x)$ and $g(x)$ respectively. Then for all q, $hd(\pi, \sigma) \geq q + 1 - (\delta_1 + \delta_2)$.*

Proof. It suffices to show that π and σ agree in at most $\delta_1 + \delta_2$ positions. If $a \in \mathbb{F}_q$ and $f(a) = g(a)$, then $u(a)s(a) - v(a)r(a) = 0$, that is, a is a root. There are at most δ_1 roots of $u(x)s(x) - v(x)r(x)$. Finally, π and σ agree at ∞ if and only if $\delta_2 = 1$. □

It follows that permutations corresponding to different PRFs are different since the permutations have non-trivial Hamming distance.

Recall that $\Pi_{u,v}(q)$ is the set of permutations over $\mathbb{P}^1(\mathbb{F}_q)$ defined by PRFs of the form $f(x) = \frac{u(x)}{v(x)}$. In Lemma 59, we prove that the set of permutations $\bigcup_{u,v} \Pi_{u,v}(q)$, for $u, v \leq (k+1)/2$, has Hamming distance at least $q - k$. We use this in Theorem 60 to show that $M(q + 1, q - k) \geq \mathcal{T}_k(q)$.

Lemma 59. *For $q > 7$ and for odd $k \geq 3$, let $u, v \leq (k+1)/2$. Then $hd(\bigcup_{u,v} \Pi_{u,v}(q)) \geq q-k$.*

Proof. Let π and σ be distinct permutations in $\bigcup_{u,v} \Pi_{u,v}(q)$, for $u, v \leq (k + 1)/2$. Let $f(x) = \frac{u(x)}{v(x)}$ and $g(x) = \frac{r(x)}{s(x)}$ be the PRFs that generate π and σ, respectively. By Lemma 58, it suffices to show that $\delta_1 + \delta_2 \leq k+1$. Note that $\delta_1 = \deg(u(x)s(x) - v(x)r(x)) \leq k+1$. The lemma follows immediately if $\delta_2 = 0$, so suppose instead that $\delta_2 = 1$, that is $f(\infty) = g(\infty)$. It suffices to show that in this case, $\delta_1 \leq k$.

Case 1. $f(\infty) = g(\infty) = \infty$.

For this to occur, we must have $u > v$ and $r > s$. So by Definition 57, $\delta_1 \leq \max\{(\frac{k+1}{2} + \frac{k-1}{2}), (\frac{k-1}{2} + \frac{k+1}{2})\} = k$.

Case 2. $f(\infty) = g(\infty) = 0$.

In this case we must have $u < v$ and $r < s$, so $\delta_1 \leq k$.

Case 3. $f(\infty) = g(\infty) \notin \{0, \infty\}$.

In this case, $u = v, r = s$ and $a_u/b_v = c_r/d_s$. Thus, the degree of the $u + s = v + r$ term in the polynomial $u(x)s(x) - v(x)r(x)$, namely $(a_u d_s - b_v c_r)x^{u+s}$, has a coefficient equal to

zero, ensuring that the degree of the polynomial is less than $u+s$. So $\delta_1 < u+s \leq k+1$, that is $\delta_1 \leq k$. □

Theorem 60. *For odd $k \geq 3$ and $q \geq k+2$, $M(q+1, q-k) \geq \mathcal{T}_k(q)$.*

Proof. This follows from Lemma 59, because by definition, $\mathcal{T}_k(q) = |\bigcup_{u,v} \Pi_{u,v}(q)|$ for $u, v \leq (k+1)/2$. □

By taking $q = 47$ and $k = 7$ Theorem 60 gives an improved lower bound of $M(48, 40) \geq$ 3,781,770,400. The previous lower bound of 9,655,492 came from permutation polynomials for $q = 47$ and extending the length of each permutation by appending a new symbol to the end.

In order to obtain additional results, we can relax the Hamming distance constraint and utilize the set of monic PRFs, $P^m_{r,s}(q)$. Recall that the size of this set is $N^m_{r,s}(q)$. By including monic PRFs in our set, we are able to obtain results for $M(q+1, q-k-1)$.

Let $u, v, s \leq \frac{k+1}{2}$ and $r = \frac{k+3}{2}$. Lemma 61 shows that $\Pi^m_{r,s}(q)$, the set of permutations generated by the monic PRFs has Hamming distance $q-k-1$. Lemma 62 shows that permutations in the union of the two sets $\bigcup_{u,v} \Pi_{u,v}(q)$ and $\Pi^m_{r,s}(q)$ have pairwise Hamming distance at least $q-k-1$. Theorem 63 uses these results to give the new lower bound $M(q+1, q-k-1) \geq \mathcal{T}_k(q) + N^m_{\frac{k+3}{2}, \frac{k+1}{2}}(q)$, for $q > 7$ and for $k \geq 3$. A special case is presented by $k = 3$, and in Theorem 65 we show that $M(q+1, q-4)$ has a better lower bound than Theorem 63 would suggest.

Lemma 61. *For odd $k \geq 3$ and for $q \geq k+3$, let $r = (k+3)/2$ and $s = (k+1)/2$. Then $hd(\Pi^m_{r,s}(q)) \geq q-k-1$.*

Proof. Let $f(x) = \frac{u(x)}{v(x)}$ and $g(x) = \frac{r(x)}{s(x)}$ be distinct PRFs in $P^m_{r,s}(q)$. By Lemma 58, it suffices to show that $\delta_1 + \delta_2 \leq k+2$. Note that $\delta_1 = \deg(u(x)s(x) - v(x)r(x)) \leq k+2$. However, since the PRFs in $P^m_{r,s}(q)$ are monic, the high order term of the polynomial

$(u(x)s(x) - v(x)r(x))$ is zero, so in fact, $\delta_1 = \deg(u(x)s(x) - v(x)r(x)) \leq k+1$. Note also that since $r > s$, $f(\infty) = g(\infty) = \infty$. Thus, $\delta_2 = 1$, and the lemma follows. □

Lemma 62. *For odd $k \geq 3$ and for $q \geq k+3$, let $u, v, s \leq (k+1)/2$, and let $r \leq (k+3)/2$. Then $hd(\bigcup_{u,v} \Pi_{u,v}(q), \Pi^m_{r,s}(q)) \geq q-k-1$.*

Proof. Let $\pi \in \bigcup_{u,v} \Pi_{u,v}(q)$ and $\sigma \in \Pi^m_{r,s}(q)$. Let $f(x) = \frac{u(x)}{v(x)}$ and $g(x) = \frac{r(x)}{s(x)}$ be the PRFs that generate π and σ, respectively. We show that $hd(\pi, \sigma) \geq q-k-1$. By Lemma 58 it suffices to show that $\delta_1 + \delta_2 \leq k+2$. Note that $\delta_1 \leq k+2$. The theorem follows immediately if $\delta_2 = 0$. So suppose $\delta_2 = 1$, that is, $f(\infty) = g(\infty)$. We show that $\delta_1 \leq k+1$.

Case 1. $f(\infty) = g(\infty) = \infty$.

In this case, $u > v$ and $r > s$, so $\delta_1 \leq \frac{k+3}{2} + \frac{k-1}{2} = k+1$.

Case 2. $f(\infty) = g(\infty) = 0$.

Then $u < v$ and $r < s$, so $\delta_1 \leq \frac{k+1}{2} + \frac{k-1}{2} = k < k+1$.

Case 3. $f(\infty) = g(\infty) \notin \{0, \infty\}$.

In this case, $u = v, r = s$ and $a_u/b_v = c_r/d_s$, so $\delta_1 \leq \frac{k+1}{2} + \frac{k+1}{2} = k+1$. □

Theorem 63. *For $q > 7$ and odd $k \geq 5$, $M(q+1, q-k-1) \geq \mathcal{T}_k(q) + N^m_{\frac{k+3}{2}, \frac{k+1}{2}}(q)$.*

Proof. This follows from Lemmas 59, 61 and 62, since $\mathcal{T}_k(q) = |\bigcup_{u,v} \Pi_{u,v}(q)|$, and $N^m_{r,s}(q) = |\Pi^m_{r,s}(q)|$, for $u, v, s \leq (k+1)/2$, and $r \leq (k+3)/2$. □

Note that when $k = 3$, $u, v, s \leq \frac{k+1}{2} = 2$ and $r \leq \frac{k+3}{2} = 3$.

Lemma 64. *Let $u, v \leq 2$. Then for all q, $hd(\bigcup_{u,v} \Pi_{u,v}(q), \Pi_{3,0}(q)) \geq q-4$.*

Proof. We use the fact that $hd(\Pi_{3,0}(q)) \geq q-3$ (Chu et al., 2004) . Let $\pi \in \bigcup_{u,v} \Pi_{u,v}(q)$ and $\sigma \in \Pi_{3,0}(q)$. Let $f(x) = \frac{u(x)}{v(x)}$ and $g(x) = \frac{r(x)}{s(x)}$ be the PRFs that generate π, σ, respectively. We show that $hd(\pi, \sigma) \geq q-4$. By Lemma 58 it suffices to show that $\delta_1 + \delta_2 \leq 5$. First note that $\delta_1 \leq \max\{u+s, v+r\} = \max\{2+0, 2+3\} \leq 5$. The theorem follows immediately if

$\delta_2 = 0$. So suppose $\delta_2 = 1$, that is, $f(\infty) = g(\infty)$. Since $r = 3$ and $s = 0$, r is always greater than s, so $g(\infty) = \infty$. Hence $f(\infty) = g(\infty) = \infty$ implies that $u > v$. This means that $v \leq 1$, so $\delta_1 = \max\{2 + 0, 1 + 3\} \leq 4$. The lemma follows. □

Theorem 65. *For* $q > 7$, $M(q+1, q-4) \geq \mathcal{T}_3(q) + \max\{N^m_{3,2}(q), N_{3,0}(q)\}$.

Proof. We use Lemmas 62 and 64. First we note that by Lemma 62, $hd(\bigcup_{u,v\leq 2} \Pi_{u,v}(q), \Pi^m_{3,2}(q)) \geq q - 4$. To obtain the largest set of permutations on $q + 1$ symbols with Hamming distance $q - 4$, we add to $\mathcal{T}_3(q)$ either $N_{3,0}(q)$ or $N^m_{3,2}(q)$, whichever is larger. For $k = 3$, we use equation 3.6 and Observation 3 to obtain $N^m_{\frac{k+3}{2},\frac{k+1}{2}}(q) = N^m_{3,2}(q) \leq (\frac{1}{q-1})N_{3,2}(q) = \frac{1}{2}q^2(q-1)$.

When $q \equiv 1 \pmod 3$, $N_{3,0}(q) = 0$, so clearly in this case, $N^m_{3,2}(q) > N_{3,0}(q)$. However, when $q \equiv 0, 2 \pmod 3$, a better result can be achieved by using $N_{3,0}(q)$ instead of $N^m_{3,2}(q)$. In particular, from equation 3.3 when $q \equiv 0 \pmod 3$, $N_{3,0}(q) = \frac{1}{2}q(q-1)^2 + q(q-1)$, and when $q \equiv 2 \pmod 3$, $N_{3,0}(q) = q^2(q-1)$. Thus in both cases, $N^m_{3,2}(q) < N_{3,0}(q)$.

The theorem follows from Lemma 62, and Lemma 64 since $\mathcal{T}_3(q) = |\bigcup_{u,v} \Pi_{u,v}(q)|$ for $u, v \leq 2$, $N^m_{3,2}(q) = |\Pi^m_{3,2}(q)|$, and $N_{3,0}(q) = |\Pi_{3,0}(q)|$. □

For example, by taking $q = 47$ and $k = 5$, Theorem 63 gives a lower bound of $M(48, 41) \geq$ 118,788,928. Also for $q = 47$, Theorem 65 gives a lower bound of $M(48, 43) \geq$ 208,390.

Using these results, we derive explicit formulas for $M(q + 1, q - k)$ for $k \in \{4, 5, 6, 7\}$, which are listed in Table 3.1. For $M(q+1, q-5)$ and $M(q+1, q-7)$, the formulas are derived from Theorem 60 and the definitions of $\mathcal{T}_5(q)$ and $\mathcal{T}_7(q)$, respectively. For $M(q + 1, q - 4)$ the formulas are derived from Theorem 65, equations 3.3 and 3.6, and Observation 3. For $M(q + 1, q - 6)$ the formulas are derived from Theorems 63 and 54 and Observation 3. Note that empty congruence classes are not included.

3.4 New Lower Bounds for $M(q, d)$

Recall in Section 1.6.2 we gave one simple approach to form permutations of length q from a subset of PRFs. A less restrictive approach is to use the contraction operation discussed in

Table 3.1. Explicit formulas for lower bounds on $M(q+1, q-k)$ for $q > 9$ and $k \in \{4, 5, 6, 7\}$.

$\boldsymbol{M(q+1, q-k)}$	**Size**	**Condition**
$M(q+1, q-4) \geq$	$\frac{3}{2}(q^3 - q)$	$q \equiv 0 \pmod 3$
	$\frac{1}{2}(3q^3 - q^2 - 2q)$	odd $q \equiv 1 \pmod 3$
	$\frac{1}{2}(5q^3 - q^2 - 4q)$	even $q \equiv 1 \pmod 3$
	$2q^3 - q^2 - q$	odd $q \equiv 2 \pmod 3$
	$3q^3 - q^2 - 2q$	even $q \equiv 2 \pmod 3$
$M(q+1, q-5) \geq$	$\frac{1}{2}(q^5 + 2q^3 - 3q)$	$q \equiv 0 \pmod 3$
	$\frac{1}{2}(q^5 - q^4 + q^3 + q^2 - 2q)$	odd $q \equiv 1 \pmod 3$
	$\frac{1}{2}(q^5 - q^4 + 3q^3 + q^2 - 4q)$	even $q \equiv 1 \pmod 3$
	$\frac{1}{2}(q^5 + q^4 + q^3 - q^2 - 2q)$	odd $q \equiv 2 \pmod 3$
	$\frac{1}{2}(q^5 + q^4 + 3q^3 - q^2 - 4q)$	even $q \equiv 2 \pmod 3$
$M(q+1, q-6) \geq$	$\frac{1}{6}(3q^5 + 2q^4 + 6q^3 - 2q^2 - 9q)$	$q \equiv 0 \pmod 3$
	$\frac{1}{6}(3q^5 - q^4 + 3q^3 + q^2 - 6q)$	odd $q \equiv 1 \pmod 3$
	$\frac{1}{6}(3q^5 - q^4 + 9q^3 + q^2 - 12q)$	even $q \equiv 1 \pmod 3$
	$\frac{1}{6}(3q^5 + 5q^4 + 3q^3 - 5q^2 - 6q)$	odd $q \equiv 2 \pmod 3$
	$\frac{1}{6}(3q^5 + 5q^4 + 9q^3 - 5q^2 - 12q)$	even $q \equiv 2 \pmod 3$
$M(q+1, q-7) \geq$	$\frac{1}{6}(2q^6 + 3q^5 - 4q^4 + 6q^3 + 2q^2 - 9q)$	$q \equiv 0 \pmod 3$
	$\frac{1}{6}(2q^6 + 3q^5 - 7q^4 + 3q^3 + 5q^2 - 6q)$	odd $q \equiv 1 \pmod 3$
	$\frac{1}{6}(2q^6 + 5q^5 - 7q^4 + 11q^3 + 5q^2 - 16q)$	even $q \equiv 1 \pmod 3$
	$\frac{1}{6}(2q^6 + 3q^5 - q^4 + 3q^3 - q^2 - 6q)$	odd $q \equiv 2 \pmod 3$
	$\frac{1}{6}(2q^6 + 5q^5 - q^4 + 11q^3 - q^2 - 16q)$	even $q \equiv 2 \pmod 3$

Section 1.2 to remove the symbol ∞ from each permutation. Using contraction allows us to consider all permutations in the PA, rather than only considering a subset. For convenience we give an updated definition of contraction as it applies to our usage with PRFs.

For this section, let π and σ be permutations on $\mathbb{P}^1(\mathbb{F}_q)$ generated by the PRFs $f(x) = \frac{u(x)}{v(x)}$ and $g(x) = \frac{r(x)}{s(x)}$, respectively. Let π' and σ' denote the permutations on $\mathbb{F}_q$ generated by the operation of contraction on π and σ, and let $\bigcup_{u,v} \Pi'_{u,v}(q)$ and $\Pi'^{m}_{u,v}(q)$ denote the PAs on $\mathbb{F}_q$ generated by the operation of contraction on the PAs $\bigcup_{u,v} \Pi_{u,v}(q)$ and $\Pi^m_{u,v}(q)$, respectively.

Definition 66. *Let π be any permutation on $\mathbb{P}^1(\mathbb{F}_q)$. The contraction operation converts π to a new permutation π' on $\mathbb{F}_q$ by the following rules:*

1. *If $\pi(\infty) = \infty$, then simply eliminate the symbol ∞ creating a permutation π' on $\mathbb{F}_q$.*

2. *If $\pi(\infty) = a$, with $a \in \mathbb{F}_q$, then exchange the symbol ∞ wherever it occurs in π with the symbol a. This moves the symbol ∞ to the last position in the permutation, so it can be eliminated, creating a permutation π' on $\mathbb{F}_q$.*

Define δ_3 to be the number of new agreements created by the operation of contraction on two permutations π and σ on $\mathbb{P}^1(\mathbb{F}_q)$.

Lemma 67.

$$\delta_3 \leq \begin{cases} 0, & \text{when } \pi(\infty) = \sigma(\infty) = \infty, \\ 1, & \text{when } \pi(\infty) = \infty, \text{ and } \sigma(\infty) = a \text{ for some } a \in \mathbb{F}_q, \\ 2, & \text{when } \pi(\infty) = b \text{ for some } b, \in \mathbb{F}_q \text{ and } \sigma(\infty) = a \text{ for some } a \in \mathbb{F}_q. \end{cases} .$$

Proof. Let π' and σ' be two permutations on $\mathbb{F}_q$, created by the contraction two distinct permutations π and σ on $\mathbb{P}^1(\mathbb{F}_q)$. We consider the number of new agreements created by contraction.

Case 1. If π' and σ' are both created by Rule 1 of Definition 66, then no new agreements are created, so $\delta_3 = 0$.

Case 2. Suppose that π' is created by Rule 1 and σ' is created by Rule 2 (or vice-versa). Suppose also that $\sigma(x) = \infty$ for some $x \in \mathbb{F}_q$. By Rule 2, $\sigma'(x) = a$ which would result in one new agreement if and only if $\pi(x) = a$. Thus, in this case, $\delta_3 \leq 1$.

Case 3. If π' and σ' are both created by Rule 2, then at most two new agreements could result. This worst case happens if and only if $\sigma(x) = \infty$, $\sigma(y) = b$, $\sigma(\infty) = a$, $\pi(y) = \infty$, $\pi(x) = a$ and $\pi(\infty) = b$ for some $x, y, a, b \in \mathbb{F}_q,\ x \neq y$. So in this case, $\delta_3 \leq 2$. □

Lemma 68. $hd(\pi', \sigma') \geq q - (\delta_1 + \delta_3)$.

Proof. It suffices to show that π' and σ' agree in at most $\delta_1 + \delta_3$ positions. If $x \in \mathbb{F}_q$ and $f(x) = g(x)$ then $u(x)s(x) - v(x)r(x) = 0$, that is, x is a root. There are at most δ_1 roots of $u(x)s(x) - v(x)r(x)$, that is, there are at most δ_1 positions where π and σ agree (before contraction). Finally, by Lemma 67, contraction creates at most δ_3 new agreements. □

In Lemma 69, we prove that the set of permutations $\bigcup_{u,v} \Pi'_{u,v}(q)$ for u, v as given, has Hamming distance at least $q-k$. We use this in Theorem 70 to show that $M(q, q-k) \geq \mathcal{S}_k(q)$.

Lemma 69. *For odd $k \geq 3$, let u and v be defined by*

$$u, v \leq \begin{cases} (k+1)/2, & \text{when } u > v, \\ (k-3)/2, & \text{when } u \leq v. \end{cases}$$

Then $hd(\bigcup_{u,v} \Pi'_{u,v}(q)) \geq q - k$.

Proof. Let $f(x) = \frac{u(x)}{v(x)}$ and $g(x) = \frac{r(x)}{s(x)}$ be distinct PRFs which generate permutations in $\bigcup_{u,v} \Pi_{u,v}(q)$. By Lemma 68, it suffices to show that $\delta_1 + \delta_3 \leq k$. We do a proof by cases based on the value of δ_3. Recall the rules for evaluating $f(\infty)$ detailed in Section 1.6.1.

Case 1. $\delta_3 = 0$.

By Lemma 67, this case occurs when $f(\infty) = g(\infty) = \infty$, that is, when $u > v$ and $r > s$. In particular, for this condition, $\delta_1 = k$ exactly when $u = r = (k+1)/2$ and $v = s = (k-1)/2$, and $\delta_1 < k$ otherwise. Thus, $\delta_1 + \delta_3 \leq k$.

Case 2. $\delta_3 = 1$.

By Lemma 67, this case occurs either when $f(\infty) = \infty$ and $g(\infty) = a \in \mathbb{F}_q$, that is, $u > v$ and $r \leq s$, or similarly, when $g(\infty) = \infty$ and $f(\infty) = a \in \mathbb{F}_q$, that is, $r > s$ and $u \leq v$. Either way, $\delta_1 \leq k - 1$, so $\delta_1 + \delta_3 \leq k$.

Case 3. $\delta_3 = 2$.

By Lemma 67, this case occurs when $f(\infty) = a$ for some $a \in \mathbb{F}_q$ and $g(\infty) = b$ for some $b \in \mathbb{F}_q$, that is, when $u \leq v$ and $r \leq s$. This means that $\delta_1 \leq (k-3)/2 + (k-3)/2$, so $\delta_1 + \delta_3 \leq k$. □

Theorem 70. *For odd $k \geq 3$ and $q \geq k+2$, $M(q, q-k) \geq \mathcal{S}_k(q)$.*

Proof. This follows from Lemma 69, because by definition, $\mathcal{S}_k(q) = |\bigcup_{u,v} \Pi'_{u,v}(q)|$, for u and v as specified in Definition 56 and in Lemma 69. □

For example, by taking $q = 59$, $k = 5$, and using the formulas from Section 3.2 to calculate $\mathcal{S}_5(59)$, Theorem 70 gives a lower bound of $M(59, 54) \geq 6{,}262{,}260$.

As we did in Section 3.3, we can relax the Hamming distance constraint and utilize monic PRFs to obtain results for $M(q, q-k-1)$, which we give in Theorem 73.

Lemma 71. *For odd $k \geq 3$, let $r = (k+3)/2$ and $s = (k+1)/2$. Let $\Pi'^m_{r,s}(q)$ be the set of permutations generated by the operation of contraction on $\Pi^m_{r,s}(q)$. Then $hd(\Pi'^m_{r,s}(q)) \geq q-k-1$.*

Proof. By Lemma 68, it suffices to show that $\delta_1 + \delta_3 \leq k+1$. Note that $\delta_1 = \deg(u(x)s(x) - v(x)r(x)) \leq k+2$. However, since the PRFs $P^m_{r,s}(q)$ are monic, the high order term of the polynomial $(u(x)s(x) - v(x)r(x))$ disappears under subtraction, so in fact, $\delta_1 = \deg(u(x)s(x) - v(x)r(x)) \leq k+1$. Note also that since $r > s$, $f(\infty) = g(\infty) = \infty$. Thus, $\delta_3 = 0$, and $\delta_1 + \delta_3 \leq k+1$. □

Lemma 72. *For odd $k \geq 3$, let $r = (k+3)/2$ and $s = (k+1)/2$. Let u and v be defined by*

$$u, v \leq \begin{cases} (k+1)/2, & \text{when } u > v, \\ (k-3)/2, & \text{when } u \leq v, \end{cases}$$

Then $hd(\bigcup_{u,v} \Pi'_{u,v}(q), \Pi'^m_{r,s}(q)) \geq q-k-1$.

Proof. Let $\pi \in \bigcup_{u,v} \Pi_{u,v}(q)$ and $\sigma \in \Pi^m(u,v)(q)$. Let $f(x) = \frac{u(x)}{v(x)}$ and $g(x) = \frac{r(x)}{s(x)}$ be the PRFs that generate π and σ, respectively. Note that r and s are fixed at $r = (k+3)/2$ and $s = (k+1)/2$. We show that $hd(\pi', \sigma') \geq q - k - 1$. By Lemma 68, it suffices to show that $\delta_1 + \delta_3 \leq k + 1$. We do a proof by cases based on the value of δ_3.

Case 1. $\delta_3 = 0$.

By Lemma 67, this case occurs when $f(\infty) = g(\infty) = \infty$, that is, when $u > v$ and $r > s$. In particular, $\delta_1 = k + 1$ exactly when u, v, r and s achieve their maximum values, that is, $u = (k+1)/2$, $v = (k-1)/2$, $r = (k+3)/2$ and $s = (k+1)/2$. Otherwise, $\delta_1 < k + 1$. Thus, $\delta_1 + \delta_3 \leq k + 1$.

Case 2. $\delta_3 = 1$.

By Lemma 67, this case occurs when $r > s$ and $u \leq v$, that is, when $g(\infty) = \infty$ and $f(\infty) = a \in \mathbb{F}_q$. So $\delta_1 = \max((k-3)/2 + (k+1)/2, (k-3)/2 + (k+3)/2) = k$. Thus, $\delta_1 + \delta_3 \leq k + 1$.

Case 3. $\delta_3 = 2$.

By Lemma 67, this case occurs when $f(\infty) = a$ for some $a \in \mathbb{F}_q$ and $g(\infty) = b$ for some $b \in \mathbb{F}_q$ (that is, when $u \leq v$ and $r \leq s$). This means that $\delta_1 \leq ((k-3)/2 + (k+1)/2, (k+1)/2 + (k-1)/2) = k - 1$, so $\delta_1 + \delta_3 \leq k + 1$. □

Theorem 73. *For odd $k \geq 3$ and $q \geq k + 2$, $M(q, q-k-1) \geq \mathcal{S}_k(q) + N^m_{\frac{k+3}{2}, \frac{k+1}{2}}(q)$*

Proof. This follows from Theorems 69, 71 and 72, since $\mathcal{S}_k(q) = |\bigcup_{u,v} \Pi'_{u,v}(q)|$, and $N'^m_{r,s}(q) = |\Pi^m_{r,s}(q)|$, for u, v, r and s as given. □

Using these results, we derive explicit formulas for $M(q, q-k)$ for $k \in \{5, 6, 7\}$, which are listed in Table 3.2. For $M(q, q-5)$ and $M(q, q-7)$, the formulas are derived from Theorem 70 and the definitions of $\mathcal{S}_5(q)$ and $\mathcal{S}_7(q)$, respectively. For $M(q, q-6)$, the formulas are derived from Theorems 73 and 54, the definition of $\mathcal{S}_5(q)$, and Observation 3. Note that empty congruence classes are not listed.

Table 3.2. Explicit formulas for lower bounds on $M(q, q-k)$ for $q > 9$ and $k \in \{5, 6, 7\}$.

$\boldsymbol{M(q, q-k)}$	**Size**	**Condition**
$M(q, q-5) \geq$	$\frac{1}{2}(q^4 + q^3 + q^2 - 3q)$	$q \equiv 0 \pmod 3$
	$\frac{1}{2}(q^4 + q^2 - 2q)$	odd $q \equiv 1 \pmod 3$
	$\frac{1}{2}(q^4 + 3q^2 - 4q)$	even $q \equiv 1 \pmod 3$
	$\frac{1}{2}(q^4 + 2q^3 - q^2 - 2q)$	odd $q \equiv 2 \pmod 3$
	$\frac{1}{2}(q^4 + 2q^3 + q^2 - 4q)$	even $q \equiv 2 \pmod 3$
$M(q, q-6) \geq$	$\frac{1}{6}(5q^4 + 3q^3 + q^2 - 9q)$	$q \equiv 0 \pmod 3$
	$\frac{1}{6}(5q^4 + q^2 - 6q)$	odd $q \equiv 1 \pmod 3$
	$\frac{1}{6}(5q^4 + 7q^2 - 12q)$	even $q \equiv 1 \pmod 3$
	$\frac{1}{6}(5q^4 + 6q^3 - 5q^2 - 6q)$	odd $q \equiv 2 \pmod 3$
	$\frac{1}{6}(5q^4 + 6q^3 + q^2 - 12q)$	even $q \equiv 2 \pmod 3$
$M(q, q-7) \geq$	$\frac{1}{6}(2q^5 + q^4 + q^3 + 5q^2 - 9q)$	$q \equiv 0 \pmod 3$
	$\frac{1}{6}(2q^5 + q^4 - 2q^3 + 5q^2 - 6q)$	odd $q \equiv 1 \pmod 3$
	$\frac{1}{6}(2q^5 + 3q^4 + 2q^3 + 9q^2 - 16q)$	even $q \equiv 1 \pmod 3$
	$\frac{1}{6}(2q^5 + q^4 + 4q^3 - q^2 - 6q)$	odd $q \equiv 2 \pmod 3$
	$\frac{1}{6}(2q^5 + 3q^4 + 8q^3 + 3q^2 - 16q)$	even $q \equiv 2 \pmod 3$

3.5 Computational Results

Using the optimizations detailed in Section 3.1, we were able to obtain additional results for restricted values of q by running a modified version of Algorithm 1 to search through PRFs rather than PPs. For instance, we have computed $N_{5,4}(q)$ for all values $32 \leq q \leq 127$, which we use as a basis for Theorem 74.

Theorem 74. *For* $32 \leq q \leq 127$*,*

$$N_{5,4}(q) = \begin{cases} \frac{1}{2}(q^6 - 2q^4 + 62q^3 - 61q^2), & \text{when } q \equiv 0 \pmod 5, \\ \frac{1}{2}(q^6 - q^4 - 2q^3 + 2q^2), & \text{when } q \equiv 1, 4 \pmod 5, \\ \frac{1}{2}(q^6 - 2q^4 + q^2), & \text{when } q \equiv 2, 3 \pmod 5. \end{cases}$$

□

To compute $N_{5,5}(q)$, we use Theorem 52 and Theorem 74 as follows. First, Observation 4 gives $N_{5,1}(q) = 0$. In addition, we observe experimentally that $N_{5,2}(q) = 0$ and $N_{5,3}(q) = 0$, for all $32 \leq q \leq 127$. So by Theorem 52, $N_{5,5}(q) = (q-1)(N_{5,4}(q) + N_{5,0}(q))$ for q within this range. Using the formulas for $N_{5,0}(q)$ given by Equation 3.5, we obtain the explicit formulas for $N_{5,5}(q)$ in Theorem 75.

Theorem 75. *For* $32 \leq q \leq 127$*,*

$$N_{5,5}(q) = \begin{cases} \frac{1}{4}(2q^7 - 2q^6 - 2q^5 + 125q^4 - 245q^3 + 121q^2 + q), & \text{when } q \equiv 0 \pmod 5, \\ \frac{1}{2}(q^7 - q^6 - q^5 - q^4 + 4q^3 - 2q^3 - 2q^2), & \text{when } q \equiv 1 \pmod 5, \\ \frac{1}{2}(q^7 - q^6 - 2q^4 + 3q^3 - q^2), & \text{when } q \equiv 2, 3 \pmod 5, \\ \frac{1}{2}(q^7 - q^6 - q^5 + q^4), & \text{when } q \equiv 4 \pmod 5. \end{cases}$$

□

We conjecture that some of the formulas from Theorems 74 and 75 may be true for all $q \geq 128$.

Explicit formulas for lower bounds on $M(q+1, q-8)$ and $M(q, q-8)$ for $32 \leq q \leq 127$ based on the mod 5 congruence classes of q are shown in Tables 3.3 and 3.4. For $M(q+1, q-8)$, we use Theorem 63, the definition of $\mathcal{T}_7(q)$, appropriate formulas from Section 3.2, Theorem 74, and computational results. For $M(q, q-8)$, we use Theorem 73, the definition of $\mathcal{S}_7(q)$, appropriate formulas from Section 3.2, Theorem 74,and computational results. Note that empty congruence classes are not listed.

Explicit formulas for lower bounds on $M(q+1, q-9)$ and $M(q, q-9)$ for $32 \leq q \leq 127$ based on the mod 5 congruence classes of q are shown in Tables 3.5 and 3.6. For $M(q+1, q-9)$, we use Theorem 60, the definition of $\mathcal{T}_9(q)$, appropriate formulas from Section 3.2, Theorems 74, 75, and computational results. For $M(q, q-9)$, we use Theorem 70, the definition of $\mathcal{S}_9(q)$, appropriate formulas from Section 3.2, Theorem 74, and computational results. Note that empty congruence classes are not listed.

Table 3.3. Explicit formulas for lower bounds on $M(q+1, q-8)$ for $32 \leq q \leq 127$.

q (mod 3)	q (mod 5)	Size
odd $q \equiv 0 \pmod 3$	$q \equiv 1, 4 \pmod 5$	$\frac{1}{6}(2q^6 + 6q^5 - q^4 + 6q^3 - 4q^2 - 9q)$
	$q \equiv 2, 3 \pmod 5$	$\frac{1}{6}(2q^6 + 6q^5 - q^4 + 3q^3 - q^2 - 9q)$
odd $q \equiv 1 \pmod 3$	$q \equiv 0 \pmod 5$	$\frac{1}{3}(q^6 + 3q^5 - 2q^4 + 94q^2 - 3q)$
	$q \equiv 1, 4 \pmod 5$	$\frac{1}{6}(2q^6 + 6q^5 - 4q^4 + 3q^3 - q^2 - 6q)$
	$q \equiv 2, 3 \pmod 5$	$\frac{1}{3}(q^6 + 3q^5 - 2q^4 + q^2 - 3q)$
odd $q \equiv 2 \pmod 3$	$q \equiv 0 \pmod 5$	$\frac{1}{3}(q^6 + 3q^5 + q^4 + 91q^2 - 3q)$
	$q \equiv 1, 4 \pmod 5$	$\frac{1}{6}(2q^6 + 6q^5 + 2q^4 + 6q^3 - 7q^2 - 6q)$
	$q \equiv 2, 3 \pmod 5$	$\frac{1}{3}(q^6 + 3q^5 + q^4 - 2q^2 - 3q)$
even $q \equiv 1 \pmod 3$	$q \equiv 1, 4 \pmod 5$	$\frac{1}{6}(2q^6 + 8q^5 - 4q^4 + 11q^3 - q^2 - 16q)$
even $q \equiv 2 \pmod 3$	$q \equiv 2, 3 \pmod 5$	$\frac{1}{3}(q^6 + 4q^5 + q^4 + 4q^3 - 2q^2 - 8q)$

Table 3.4. Explicit formulas for lower bounds on $M(q, q-8)$ for $32 \leq q \leq 127$.

q (mod 3)	q (mod 5)	Size
odd $q \equiv 0 \pmod 3$	$q \equiv 1, 4 \pmod 5$	$\frac{1}{6}(5q^5 + 4q^4 + q^3 - q^2 - 9q)$
	$q \equiv 2, 3 \pmod 5$	$\frac{1}{6}(5q^5 + 4q^4 - 2q^3 + 2q^2 - 9q)$
odd $q \equiv 1 \pmod 3$	$q \equiv 0 \pmod 5$	$\frac{1}{6}(5q^5 + 4q^4 - 5q^3 + 188q^2 - 6q)$
	$q \equiv 1, 4 \pmod 5$	$\frac{1}{6}(5q^5 + 4q^4 - 2q^3 - q^2 - 6q)$
	$q \equiv 2, 3 \pmod 5$	$\frac{1}{6}(5q^5 + 4q^4 - 5q^3 + 2q^2 - 6q)$
odd $q \equiv 2 \pmod 3$	$q \equiv 0 \pmod 5$	$\frac{1}{12}(5q^5 + 4q^4 + q^3 + 182q^2 - 6q)$
	$q \equiv 1, 4 \pmod 5$	$\frac{1}{6}(5q^5 + 4q^4 + 4q^3 - 7q^2 - 6q)$
	$q \equiv 2, 3 \pmod 5$	$\frac{1}{6}(5q^5 + 4q^4 + q^3 - 4q^2 - 6q)$
even $q \equiv 1 \pmod 3$	$q \equiv 1, 4 \pmod 5$	$\frac{1}{6}(5q^5 + 6q^4 + 2q^3 + 3q^2 - 16q)$
even $q \equiv 2 \pmod 3$	$q \equiv 2, 3 \pmod 5$	$\frac{1}{6}(5q^5 + 6q^4 + 5q^3 - 16q)$

Table 3.5. Explicit formulas for lower bounds on $M(q+1, q-9)$ for $32 \leq q \leq 127$.

q (mod 3)	q (mod 5)	Size
odd $q \equiv 0 \pmod 3$	$q \equiv 1 \pmod 5$	$\frac{1}{6}(3q^7 + 5q^6 - 13q^4 + 6q^3 + 8q^2 - 9q)$
	$q \equiv 2, 3 \pmod 5$	$\frac{1}{6}(3q^7 + 5q^6 + 3q^5 - 10q^4 + 3q^3 + 5q^2 - 9q)$
	$q \equiv 4 \pmod 5$	$\frac{1}{6}(3q^7 + 5q^6 - 7q^4 + 6q^3 + 2q^2 - 9q)$
odd $q \equiv 1 \pmod 3$	$q \equiv 0 \pmod 5$	$\frac{1}{12}(6q^7 + 10q^6 + 349q^4 + 9q^3 - 359q^2 - 15q)$
	$q \equiv 1 \pmod 5$	$\frac{1}{6}(3q^7 + 5q^6 - 16q^4 + 3q^3 + 11q^2 - 6q)$
	$q \equiv 2, 3 \pmod 5$	$\frac{1}{6}(3q^7 + 5q^6 + 3q^5 - 13q^4 + 8q^2 - 6q)$
	$q \equiv 4 \pmod 5$	$\frac{1}{6}(3q^7 + 5q^6 - 10q^4 + 3q^3 + 5q^2 - 6q)$
odd $q \equiv 2 \pmod 3$	$q \equiv 0 \pmod 5$	$\frac{1}{12}(6q^7 + 10q^6 + 361q^4 + 9q^3 - 371q^2 - 15q)$
	$q \equiv 1 \pmod 5$	$\frac{1}{6}(3q^7 + 5q^6 - 10q^4 + 3q^3 + 5q^2 - 6q)$
	$q \equiv 2, 3 \pmod 5$	$\frac{1}{6}(3q^7 + 5q^6 + 3q^5 - 7q^4 + 2q^2 - 6q)$
	$q \equiv 4 \pmod 5$	$\frac{1}{6}(3q^7 + 5q^6 - 4q^4 + 3q^3 - q^2 - 6q)$
even $q \equiv 1 \pmod 3$	$q \equiv 1, 4 \pmod 5$	$\frac{1}{6}(3q^7 + 5q^6 + 2q^5 - 10q^4 + 11q^3 + 5q^2 - 16q)$
even $q \equiv 2 \pmod 3$	$q \equiv 2, 3 \pmod 5$	$\frac{1}{6}(3q^7 + 5q^6 + 5q^5 - 7q^4 + 8q^3 + 2q^2 - 16q)$

Table 3.6. Explicit formulas for lower bounds on $M(q, q-9)$ for $32 \leq q \leq 127$.

q (mod 3)	q (mod 5)	Size
odd $q \equiv 0 \pmod 3$	$q \equiv 1 \pmod 5$	$\frac{1}{6}(3q^6 + 5q^5 - 5q^4 - 2q^3 + 8q^2 - 9q)$
	$q \equiv 2, 3 \pmod 5$	$\frac{1}{6}(3q^6 + 5q^5 - 2q^4 + q^3 - q^2 - 6q)$
	$q \equiv 4 \pmod 5$	$\frac{1}{6}(3q^6 + 5q^5 - 8q^4 + 13q^3 - 7q^2 - 6q)$
odd $q \equiv 1 \pmod 3$	$q \equiv 1 \pmod 5$	$\frac{1}{6}(3q^6 + 5q^5 - 8q^4 - 5q^3 + 11q^2 - 6q)$
	$q \equiv 2, 3 \pmod 5$	$\frac{1}{6}(3q^6 + 5q^5 - 5q^4 - 5q^3 + 8q^2 - 6q)$
	$q \equiv 4 \pmod 5$	$\frac{1}{6}(3q^6 + 5q^5 - 8q^4 + q^3 + 5q^2 - 6q)$
odd $q \equiv 2 \pmod 3$	$q \equiv 0 \pmod 5$	$\frac{1}{12}(6q^6 + 10q^5 - 4q^4 + 371q^3 - 368q^2 - 15q)$
	$q \equiv 1 \pmod 5$	$\frac{1}{6}(3q^6 + 5q^5 - 2q^4 - 5q^3 + 5q^2 - 6q)$
	$q \equiv 2, 3 \pmod 5$	$\frac{1}{6}(3q^6 + 5q^5 + q^4 - 5q^3 + 2q^2 - 6q)$
	$q \equiv 4 \pmod 5$	$\frac{1}{6}(3q^6 + 5q^5 - 2q^4 + q^3 - q^2 - 6q)$
even $q \equiv 1 \pmod 3$	$q \equiv 1 \pmod 5$	$\frac{1}{6}(3q^6 + 5q^5 - 6q^4 - q^3 + 15q^2 - 16q)$
	$q \equiv 4 \pmod 5$	$\frac{1}{6}(3q^6 + 5q^5 - 6q^4 + 5q^3 + 9q^2 - 16q)$
even $q \equiv 2 \pmod 3$	$q \equiv 2, 3 \pmod 5$	$\frac{1}{6}(3q^6 + 5q^5 + 3q^4 - q^3 + 6q^2 - 16q)$

CHAPTER 4

CHEBYSHEV DISTANCE

In this chapter we discuss methods used to construct PAs under the Chebyshev distance metric. We first detail several search techniques to form PAs and provide bounds for $P(n, d)$. We introduce several theorems which establish general upper and lower bounds on $P(n, d)$, including exact bounds for $P(n, 2)$ and $P(n, n-2)$. These ideas were first presented in Bereg et al. (2022).

For notation, let an array A of permutations on $[1 \dots n]$ with Chebyshev distance d be called an (n, d) PA. We generalize $P(n, d)$ to $P_d(\Sigma)$. Let $P_d(\Sigma)$ be the maximum size of a PA over the alphabet $\Sigma \subseteq [1 \dots n]$ with pairwise Chebyshev distance d. For example, $P_2(\{1, 3, 5, 7\}) = 4! = 24$, whereas $P(4, 2) = 6$. Let $P(n, m, d)$ be the maximum size of a PA with permutations of length m, $m \leq n$, over the alphabet $[1 \dots n]$ with pairwise Chebyshev distance d.

4.1 Search Techniques

Unlike a search for PPs or PRFs, using a search algorithm to form PAs under Chebyshev distance must search permutations directly. This means there are no normalization operations to reduce the search space from $O(n!)$. Additionally, any time a new permutation is considered, its Chebyshev distance must be checked against every permutation already in the set. This was unnecessary when searching for PPs or PRFs as the Hamming distance was ensured algebraically. To work around these challenges, we devised several approaches.

4.1.1 Clique Search

Consider a graph where every permutation is represented by a vertex. Connect two vertices with an edge if their Chebyshev distance is at least d. Thus, any clique in this graph would

correspond to a set of permutations with pairwise distance d, and a maximum clique would give an exact bound for $P(n, d)$.

Since running an NP-complete algorithm on a graph of $n!$ vertices is computationally demanding, this approach is only viable for small values of n. Even so, there is one optimization we can make. Any maximum clique found in the graph which does not contain the identity permutation $(1\ 2\ \ldots\ n)$ would be isomorphic to some other clique which does. We can therefore prune any vertices which are not at least distance d from the identity permutation.

To utilize this method, we created a Java application that constructs a textual representation of a graph for the chosen n and d. We then used the Parallel Maximum Clique (PMC) Library (Rossi et al., 2012) to search the graph. PMC can utilize a multi-core processor to perform the search in parallel, but we were still limited to values of $n \leq 7$ due to the size of the graphs.

4.1.2 Random/Greedy Search

Consider two permutations $\pi = (1\ 2\ 3)$ and $\sigma = (3\ 2\ 1)$. Note that while $d(\pi, \sigma) = 2$, they satisfy this distance agreement in two positions, the first and the last. Forming a distance agreement in more positions than necessary can be detrimental when constructing a PA, as it limits the positions that a new permutation could use to form its own distance agreements. In this particular example, there is no third permutation that has distance of 2 with both π and σ.

Instead, consider the permutations $\pi = (1\ 2\ 3)$ and $\sigma = (2\ 3\ 1)$. We still have $d(\pi, \sigma) = 2$, but they now only form an agreement in the last position. Because of this, we can add a new permutation $\rho = (3\ 1\ 2)$, and all three permutations have pairwise distance 2. This highlights the greedy choice we want our algorithm to make; add the next permutation to the PA that minimizes extraneous distance agreements.

Implementing this specific greedy choice would require a lot of additional computation, but we find that considering permutations in lexicographic order gives us a good approximation.

When considering the lexicographic successor of a permutation, it often only differs from the current permutation in a small number of positions. This lets us often find permutations for the PA that differ from the previous permutations in only enough positions to form the necessary distance agreements. Finding the lexicographic successor of a permutation can also be done efficiently using Knuth's algorithm to generate permutations in lexicographic order (Knuth, 2005).

To add variance to the search, we implement a random element as well. The search algorithm is as follows:

1. Generate random permutations until there are k total with pairwise distance d.

2. Iterate through all permutations in lexicographic order, adding any permutation which preserves the distance of the PA.

In practice, we obtain our best with results for small values of k, typically for $1 \leq k \leq 20$ depending on the size of n. Because we must iterate through all permutations, we are still very limited by the size of n. Searches for $n = 11$ terminate relatively quickly, but there is noticeable slowdown for $n \geq 12$.

4.1.3 Maximum Weighted Clique

Maximum Weight Clique is a search technique that forms a PA by combining a set of *prefix* permutations with their respective sets of *suffix* permutations. Consider combining prefixes of length m with suffixes of length n to form permutations over the alphabet $[1 \ldots (n+m)]$.

Any suffix must use the complement of the alphabet used in the prefix, so if π is a prefix, let π^C denote the complement in $[1 \ldots (n+m)]$ of the set of symbols used in π. Let $Q((n+m), m, d)$ denote the collection of all sets A of permutations on an m symbol subset of $[1 \ldots (n+m)]$ with $d(A) \geq d$. We want to select the set A which maximizes the total number

of permutations when each prefix in A is combined with its set of suffixes. More precisely, we want to find $\max_{A \in Q((n+m),m,d)} \sum_{\pi \in A} P_d(\pi^C)$.

For any prefix π, assume we have already calculated the number of suffix permutations that can be formed using the complement alphabet, that is, $P_d(\pi^C)$. We still need a method to decide which permutations belong in A. For example, suppose we want to compute a bound for $P(12, 4)$ by using prefixes of length 5 and suffixes of length 7, and consider the following prefixes:

$$\pi = (6\ 2\ 5\ 12\ 9), \quad P_4(\pi^C) \geq 105$$
$$\sigma = (3\ 5\ 7\ 11\ 8), \quad P_4(\sigma^C) \geq 140$$

Since $d(\pi, \sigma) = 3$, only one of these permutations can be included in A. We could make the greedy choice of choosing σ since $P_4(\sigma^C)$ is larger, but there is no guarantee this choice is optimal. Our maximum weighted clique approach solves this problem as follows:

1. Let each prefix of m symbols taken from $[1 \ldots (n+m)]$ be a vertex.
2. Give each vertex weight equal to the number of suffixes with pairwise distance d that can be formed using the complement alphabet.
3. Connect two vertices with an edge if their Chebyshev distance is at least d.
4. Search the resulting graph for a maximum weighted clique.

This requires us to have already calculated each $P_d(\pi^C)$, which can be done using either a standard clique search, or the random/greedy search, depending on the length of the suffix. We can also use isomorphism to limit the number of searches that need to be conducted. For example, consider the alphabets $\{1, 2, 3, 5, 7, 9\}$ and $\{1, 3, 5, 7, 8, 9\}$. If you form a graph for each alphabet where two symbols are connected by an edge if their distance is at least d, the resulting graphs will be isomorphic.

The advantage of this approach is it lets us consider larger n than are otherwise feasible using the clique or random/greedy searches. Our implementation using the Python package NetworkX (Hagberg et al., 2008) was able to find maximum weighted cliques in graphs up to $n + m = 14$.

4.2 Lower Bounds

Recall the recursive constructions from Section 1.7.2 given by Klove et al. (2010). We improve each of these constructions by generalizing them, often leading to improved lower bounds.

We first consider Theorem 29. This construction adds a single symbol prefix to the front of some (n, d) PA, such that each prefix is at least distance d from the others. This creates a new PA over $n + 1$ symbols, and gives us the following bound from Theorem 30,

$$P(n+1, d) \geq \Big(\Big\lfloor \frac{n}{d} \Big\rfloor + 1\Big) P(n, d).$$

Rather than insert each prefix into the same (n, d) PA, we can often compute a larger PA over the corresponding suffix alphabet, giving us the result from Theorem 76.

Theorem 76. *Let A be a subset of $[1 \ldots (n+1)]$ such that $d(A) \geq d$. If $n > d \geq 1$, then*

$$P(n+1, d) \geq \sum_{i \in A} P_d([1 \ldots (n+1)] - \{i\}).$$

Proof. Let $A = \{a_1, a_2, \ldots, a_k\}$ be a subset of $[1 \ldots (n+1)]$ such that $d(A) \geq d$. For $a_i \neq a_j$, and permutations π and σ in $[1 \ldots (n+1)] - \{a_i\}$ and $[1 \ldots (n+1)] - \{a_j\}$, respectively, $a_i\pi$ and $a_j\sigma$ are permutations on $[1 \ldots (\mathrm{n}{+}1)]$ such that $d(a_i\pi, a_j\sigma) \geq d$. It follows that $\bigcup_{a_i \in A} a_i B$, with B a set of permutations over $[1 \ldots (n+1)] - \{a_i\}$ with Chebyshev distance $\geq d$, is a set of permutations on $[1 \ldots (n+1)]$ with Chebyshev distance $\geq d$. □

For example, the best known bound for $P(10, 3)$ is 9,033. Applying Theorem 30 gives us $P(11, 3) \geq 4 \cdot 9{,}033 = 36{,}132$. We instead choose our set of prefixes $A = \{3, 6, 9\}$ and

calculate the following bounds over each suffix alphabet:

$$P_3([1\ldots11]-\{3\}) = P_3([1\ldots11]-\{9\}) \geq 17{,}573,$$
$$P_3([1\ldots11]-\{6\}) \geq 18{,}403.$$

This gives us a result from Theorem 76 of $P(11,3) \geq 53{,}549$.

We now consider the recursive construction which took the Cartesian product of some (n,d) PA, r times, giving us the following bound from Theorem 28,

$$P(rn,rd) \geq P(n,d)^r.$$

We generalize this in Theorem 77 which allows us to take the product of two PAs with differing values n and d.

Theorem 77. *$P(n,d) \geq \max\{P(n_1,d_1)\cdot P(n_2,d_2) \mid d_1+d_2=d$ and $n_1+n_2=n$ and, for some constant a, $n_1 = ad_1+r_1$ and $n_2=ad_2+r_2$, with $0 \leq r_1 \leq d_1$ and with $0 \leq r_2 \leq d_2\}$, where the maximum is taken over all possible values of n_1,n_2,d_1,d_2.*

Proof. Let $n=n_1+n_2$ and $d=d_1+d_2$. Let A be a PA on the n_1 symbols in $\Sigma_1=[1\ldots n_1]$ with Hamming distance d_1 and let B be a PA on the n_2 symbols in $\Sigma_2=[1\ldots n_2]$ with Hamming distance d_2. Let $\Sigma=[1\ldots n=n_1+n_2]$. Define the function F_1 mapping Σ_1 into Σ by:

$$F_1(x) = \begin{cases} x, & \text{if } 1 \leq x \leq r_1, \\ x+sd_2, & \text{if } (s-1)d_1+r_1+1 \leq x \leq sd_1+r_1, \text{ for some } 1 \leq s \leq a. \end{cases}$$

Define the function F_2 mapping Σ_2 into Σ by:

$$F_2(x) = \begin{cases} x+(t-1)d_1+r_1, & \text{if } (t-1)d_2 < x \leq td_2, \text{ for some } 1 \leq t \leq a, \\ x+n_1, & \text{if } ad_2 < x \leq ad_2+r_2. \end{cases}$$

Construct the PA $C = \{ F_1(\pi)F_2(\sigma) \mid \pi \in A \text{ and } \sigma \in B \}$.

C is a set of $|A| \cdot |B|$ permutations on the alphabet Σ of n symbols. We show that the Chebyshev distance between permutations in C is at least $d = d_1 + d_2$. Consider two different permutations $\rho_1 = F_1(\pi_1)F_2(\sigma_1)$ and $\rho_2 = F_1(\pi_2)F_2(\sigma_2)$ in C, where $\pi_1, \pi_2 \in A$ and $\sigma_1, \sigma_2 \in B$. Since $\rho_1 \neq \rho_2$, either $\pi_1 \neq \pi_2$ or $\sigma_1 \neq \sigma_2$.

Due to the similarity of the argument we only explicitly examine the case when $\pi_1 \neq \pi_2$. So, the Chebyshev distance between π_1 and π_2 is at least d_1. That is, there is a position i $(1 \leq i \leq n_1)$ such that $|\pi_1(i) - \pi_2(i)| \geq d_1$. Assume, without loss of generality, that $\pi_1(i) > \pi_2(i)$. In other words, $\pi_1(i)$ and $\pi_2(i)$ are in different intervals of d_1 symbols in Σ_1, i.e., $\pi_2(i)$ is in the interval $[(s-1)d_1 + r_1 \ldots sd_1 + r_1]$, for some s, and $\pi_1(i)$ is in the interval $[(s'-1)d_1 + r_1 \ldots s'd_1 + r_1]$, for some $s' > s$. Hence, F_1 maps $\pi_1(i)$ to $\pi_1(i) + s'd_2$ and maps $\pi_2(i)$ to $\pi_2(i) + sd_2$. So,

$$\begin{aligned} |(\pi_1(i) + s'd_2) \ - (\pi_2(i) + sd_2)| = \\ |\pi_1(i) - \pi_2(i) + s'd_2 - sd_2| = \\ |\pi_1(i) - \pi_2(i)| + |s'd_2 - sd_2| \geq d_1 + d_2. \end{aligned}$$

□

For example, we can use Theorem 77 to show $P(16, 9) \geq P(9, 5) \cdot P(7, 4) \geq 3{,}399$. If we take $a = 1$, $r_1 = 4$, and $r_2 = 3$, we get,

$$F_1(x) = \begin{cases} x, & \text{if } 1 \leq x \leq 4, \\ x + 4, & \text{if } 5 \ \leq x \leq 9, \end{cases} \qquad F_2(x) = \begin{cases} x + 4, & \text{if } 1 \leq x \leq 4, \\ x + 9, & \text{if } 5 \ \leq x \leq 7. \end{cases}$$

Consider the permutations,

$$\pi = (1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ 9), \qquad \sigma = (6\ 1\ 4\ 3\ 2\ 5\ 8\ 9\ 7), \qquad \rho = (1\ 2\ 3\ 4\ 5\ 6\ 7).$$

Observe that $d(\pi, \sigma) = 5$. This gives us,

$$F_1(\pi) = (1\ 2\ 3\ 4\ 9\ 10\ 11\ 12\ 13), \qquad F_1(\sigma) = (10\ 1\ 4\ 3\ 2\ 9\ 12\ 13\ 11),$$

and

$$F_1(\pi)F_2(\rho) = (1\ 2\ 3\ 4\ 9\ 10\ 11\ 12\ 13\ 5\ 6\ 7\ 8\ 14\ 15\ 16),$$
$$F_1(\sigma)F_2(\rho) = (10\ 1\ 4\ 3\ 2\ 9\ 12\ 13\ 11\ 5\ 6\ 7\ 8\ 14\ 15\ 16),$$

which are permutations on $[1 \ldots 16]$ with Chebyshev distance 9.

Theorem 78 is derived from our Maximum Weighted Clique technique. Recall that $Q((n+m), m, d)$ denotes the collection of all sets A of permutations on an m symbol subset of $[1 \ldots (n+m)]$ with $d(A) \geq d$.

Theorem 78. *For any $n \geq d \geq 1$, $m \geq 1$,*

$$P(n+m, d) \geq \max_{A \in Q((n+m), m, d)} \sum_{\pi \in A} P_d(\pi^C).$$

Proof. Let A be a PA of *prefixes* of length m over the alphabet $[1 \ldots (n+m)]$ with $d(A) \geq d$. For each *prefix* $\pi \in A$, let B_{π^C} be a PA of *suffixes* of length n over the alphabet π^C with $d(B_{\pi^C}) \geq d$. Let $C = \{\pi\sigma \mid \pi \in A, \sigma \in B_{\pi^C}\}$. Since C is formed by prefixes and suffixes using complementary alphabets, each permutation in C is over the alphabet $[1 \ldots (n+m)]$.

We show that $d(C) \geq d$. Consider two arbitrary permutations from C, say ρ and τ. If ρ and τ share the same prefix π, then their respective suffixes both come from B_{π^C}, and $d(\rho, \tau) \geq d$ since $d(B_{\pi^C}) \geq d$. If ρ and τ have different prefixes from A, then $d(\rho, \tau) \geq d$ since $d(A) \geq d$. The theorem follows. □

Theorem 79 shows that improvements over the iterative use of Theorem 30 are possible, even when restrictions due to large numbers prevent computational results. The idea is instead of iteratively using Theorem 30 d times, we can combinatorically form a set of prefixes of length and distance d which yields a larger PA.

Theorem 79. *For any $d \geq 3$ and $k \geq 1$,*

$$P(dk+d-1,d) \geq \left((k+1)^d - \binom{k+d-1}{d-1}\right) P(dk-1,d).$$

Proof. Let $\Phi(a_1, a_2, \ldots, a_s)$ denote the alphabet $[1 \ldots (dk+d-1)] - \{a_1, a_2, \ldots, a_s\}$ for $a_1, a_2, \ldots, a_s \in [1 \ldots (dk+d-1)]$. By Theorem 76, $P(dk+d-1,d) \geq \sum_{a_1 \in A_1} P_d(\Phi(a_1))$ where $A_1 = \{d-1, 2d-1, \ldots, kd+d-1\}$. Note that $|\Phi(a_1)| = dk+d-2$. Similarly, for each $\Phi(a_1)$, by Theorem 76, $P_d(\Phi(a_1)) \geq \sum_{a_2 \in A_2} P_d(\Phi(a_1, a_2))$ where $A_2 = \{d-2, 2d-2, \ldots, kd+d-2\}$. Note that $|\Phi(a_1, a_2)| = dk+d-3$. By applying Theorem 76 $d-1$ times, $P_d(\Phi(a_1, a_2, \ldots, a_{d-2})) \geq \sum_{a_{d-1} \in A_{d-1}} P_d(\Phi(a_1, a_2, \ldots, a_{d-1}))$, where $A_{d-1} = \{1, d+1, \ldots, kd+1\}$. Note that $|\Phi(a_1, a_2, \ldots, a_{d-1})| = dk$.

$$P(dk+d-1,d) \geq \sum_{a_1 \in A_1} \sum_{a_2 \in A_2} \cdots \sum_{a_{d-1} \in A_{d-1}} P_d(\Phi(a_1, a_2, \ldots, a_{d-1})).$$

Note that there are $k+1$ choices for each of the symbols a_i, $1 \leq i \leq d-1$, with the property that any two choices are at distance at least d. Consider a sequence $\alpha = (a_1, a_2, \ldots, a_{d-1})$ with $a_i \in A_i$, $i = 1, 2, \ldots, d-1$. We call sequence $a_1, a_2, \ldots, a_{d-1}$ *monotone* if $a_1 > a_2 > \cdots > a_{d-1}$; otherwise, the sequence is *mixed*. So far, we have sequences, such as α, of length $d-1$. We now consider sequences of length d obtained by adding an extra symbol to the end of α. Since $|\Phi(a_1, a_2, \ldots, a_{d-1})| = dk$, by Theorem 30,

$$P_d(\Phi(a_1, a_2, \ldots, a_{d-1})) \geq kP(dk-1,d).$$

That is, the proof of Theorem 30 shows there are always k symbols one can add to the end of such sequences α and preserve distance d. We show that $P_d(\Phi(a_1, a_2, \ldots, a_{d-1})) \geq (k+1)P(dk-1,d)$ if the sequence $a_1, a_2, \ldots, a_{d-1}$ is mixed. That is, there are always $k+1$ symbols at pairwise distance d to add to the end of α, if α is mixed. Note that for symbols x and y, such that $d(x,y) \geq d$, $d(\alpha x, \alpha y) \geq d$.

Assume $a_1, a_2, \ldots, a_{d-1}$ is mixed. We construct a sequence $S = s_1, s_2, \ldots s_{k+1}$ of elements in $P_d(\Phi(a_1, a_2, \ldots, a_{d-1}))$ with $d(s_i, s_{i+1}) \geq d$, for all i. Using S, we get $k+1$ sequences,

Table 4.1. An example of a mixed sequence (in bold), for $d = 6$ and $k = 5$. The sequence 17, 22, 15, 8, 1 is shown right-to-left.

1	2	3	4	5
7	**8**	9	10	11
13	14	**15**	16	**17**
19	20	21	**22**	23
25	26	27	28	29
31	32	33	34	35

say $T_1, T_2, \ldots, T_{k+1}$, where T_i consists of $a_1, a_2, \ldots, a_{d-1}$ followed by s_i. It follows that $P_d(\Phi(T_i)) \geq (k+1)P(dk-1, d)$.

Consider a table T with $d-1$ columns and $k+1$ rows, where row i of T contains the i^{th} element of A_j, and column j of T, $1 \leq j \leq d-1$ contains the elements of A_{d-j} in sorted order. In particular, row i and column j of T contains the element $(i-1)d+j$. See Table 4.1 for an example when $d = 6$ and $k = 5$.

The desired sequence $S = s_1, s_2, \ldots, s_{k+1}$ is obtained from the table T by choosing one element from each row with the property that the element chosen from row $i+1$ must come from a column whose index is at least as large as the index of the column chosen for row i. This is to ensure distance at least d. Also, an element must be chosen from each row in order to get a sequence of length $k+1$. In addition, one cannot choose the elements in the sequence $a_1, a_2, \ldots, a_{d-1}$, which are numbers deleted from the alphabet and include one and only one element from each column. For example, consider the mixed sequence 17, 22, 15, 8, 1, shown in bold in Table 4.1, represented in the table in right-to-left order. In this example, a desired sequence S can be chosen to be 4, 10, 16, 23, 29, 35. In the mixed sequence 17, 22, 15, 8, 1 we have $a_1 = 17 < a_2 = 22$.

In every mixed sequence $a_1, a_2, \ldots, a_{d-1}$ there must be a j such that $a_j \leq a_{j+1}$. The desired sequence S can be chosen by taking elements in order in column $d-j-1$ until, but not including, a_{j+1}, followed by elements in column $d-j$ beginning with the element in the

same row as a_{j+1} and continuing through all remaining rows. This always works as (1) each column has one and only one deleted element, and (2) the condition $a_j \leq a_{j+1}$ ensures that the deleted element in column $d-j$ occurs in a row with index smaller than i.

Observe that if $a_1, a_2, \ldots, a_{d-1}$ is monotone, there is no j such that $a_j < a_{j+1}$. Consequently, there is no way to construct the desired sequence S by moving to a higher index column when a deleted symbol is encountered. That is, the higher index column always has a different deleted symbol in the given row or a latter row.

Let M be the set of all sequences $m_j = a_1, a_2, \ldots, a_{d-1}$ with $a_i \in \{d-i, 2d-i, \ldots, kd+d-i\}$, for all $i, 1 \leq i \leq d-1$, with the property that, for $j \neq k$, $d(m_j, m_k) \geq d$. Map each sequence $a_1, a_2, \ldots, a_{d-1}$ to $x \in [0 \ldots k]^{d-1}$ using,

$$x = \left(\left\lfloor \frac{a_1}{d} \right\rfloor, \left\lfloor \frac{a_2}{d} \right\rfloor, \left\lfloor \frac{a_3}{d} \right\rfloor, \ldots, \left\lfloor \frac{a_{d-1}}{d} \right\rfloor \right).$$

A sequence $a_1, a_2, \ldots, a_{d-1}$ is monotone if and only if $x_1 \geq x_2 \geq \cdots \geq x_{d-1}$. The number of such vectors x is $\binom{k+d-1}{d-1}$, which is the number of ways of choosing a set of $d-1$ elements from $k+1$ sets of $d-1$ indistinguishable items. So, the number of monotone sequences $a_1, a_2, \ldots, a_{d-1}$ is $n_{mon} = \binom{k+d-1}{d-1}$. The number of mixed sequences $a_1, a_2, \ldots, a_{d-1}$ is $n_{mix} = (k+1)^{d-1} - \binom{k+d-1}{d-1}$. That is, the number of choices for $a_1 \in A_1, a_2 \in A_2, ..., a_{d-1} \in A_{d-1}$ is $(k+1)^{d-1}$, and

$$\begin{aligned} P(dk+d-1, d) &\geq \sum_{a_1 \in A_1} \sum_{a_2 \in A_2} \cdots \sum_{a_{d-1} \in A_{d-1}} P_d(\Phi(a_1, a_2, \ldots, a_{d-1})) \\ &\geq (kn_{mon} + (k+1)n_{mix}) P(dk-1, d) \\ &\geq \left((k+1)^d - \binom{k+d-1}{d-1} \right) P(dk-1, d). \end{aligned}$$

The theorem follows. □

As an example of the improvement shown by Theorem 79, consider the case when $k = 3$ and $d = 3$. The theorem states that $P(11, 3) \geq 54 \cdot P(8, 3) = 54 \cdot 430 = 23{,}220$, whereas the three-fold iterative use of Theorem 30 only gives $P(11, 3) \geq (\lfloor \frac{10}{3} \rfloor + 1) \cdot (\lfloor \frac{9}{3} \rfloor + 1) \cdot (\lfloor \frac{8}{3} \rfloor + 1) \cdot P(8, 3) =$

$48 \cdot P(8,3) = 48 \cdot 430 = 20{,}640$. By computational methods, we know that $P(11,3,3) \geq 59$ and hence, by Theorem 78, we have $P(11,3) \geq 59 \cdot P(8,3) = 59 \cdot 430 = 25{,}370$. However, as was shown in the example from Theorem 76, we actually know $P(11,3) \geq 53,549$.

Table 4.2 shows many lower bounds for $P(n,d)$. Bounds that are known to be exact are in bold. Many results were computed using the clique search, random/greedy search, and maximum weighted clique techniques. Additional bounds were derived from Theorems 76, 77, 78, and 88.

4.3 Upper Bounds

Theorem 80 provides a general upper bound which offers significant improvement over published Hamming upper bounds that were shown in Theorem 32. Note that the best results from Theorem 80 typically come from choosing $k = d$.

Theorem 80. *For* $1 \leq k \leq d < n$,

$$P(n,d) \leq P(n-k,d) \cdot \binom{n}{k}.$$

Proof. Consider any PA on n symbols with distance d. Partition the PA into subsets determined by the positions of the highest k symbols, $\{n-k+1, n-k+2, \ldots, n\}$. Two permutations are in the same subset if their highest k symbols occur in the same subset of k positions, though not necessarily with the same symbol in the same position. For example if $n = 5, d = 2$, and $k = 2$, then the permutations 54321 and 45132 would be in the same subset since the symbols 4 and 5 both occur in positions 1 and 2. Observe that there can be at most $\binom{n}{k}$ subsets since that is the number of ways to choose k positions.

Since any two permutations must have distance at least d, and there is no way for any pair of the highest $k \leq d$ symbols to satisfy this distance, within a single subset the Chebyshev distance must be satisfied by the remaining $n-k$ symbols, $\{1, 2, \ldots, n-k\}$. Assume each of

Table 4.2. Lower Bounds for $P(n, d)$.

n/d	2	3	4	5	6	7	8	9	10
2	1	1	1	1	1	1	1	1	1
3	**3**	1	1	1	1	1	1	1	1
4	**6**	**3**	1	1	1	1	1	1	1
5	**30**	**10**	**3**	1	1	1	1	1	1
6	**90**	**20**	**10**	**3**	1	1	1	1	1
7	**630**	100	33	**10**	**3**	1	1	1	1
8	**2,520**	430	**70**	33	**10**	**3**	1	1	1
9	**22,680**	1,654	295	103	33	**10**	**3**	1	1
10	**113,400**	9,033	1,336	247	103	33	**10**	**3**	1
11	see Thm 88	53,549	6,397	998	326	103	33	**10**	**3**
12	see Thm 88	317,728	26,678	4,355	842	330	103	33	**10**
13	see Thm 88	1,642,473	114,720	17,049	3,294	978	330	103	33
14	see Thm 88	11,081,916	647,420	81,888	10,709	2,805	1,089	330	103
15	see Thm 88	55,409,580	3,887,796	392,033	50,283	8,604	3,144	1,089	330
16	see Thm 88	332,457,480	15,551,184	1,898,103	250,867	37,017	9,379	3,399	1,089
17	see Thm 88	1,994,744,880	77,755,920	7,592,412	1,261,267	174,655	30,106	10,374	3,399
18	see Thm 88	11,968,469,280	514,382,400	33,735,870	3,783,801	862,566	129,756	31,779	10,758

the $\binom{n}{k}$ subsets contains $P(n-k,d)$ permutations. If we add one additional permutation to the PA, it will belong to exactly one of these subsets. If we take that subset and delete the highest k symbols from each permutation, we are left with a contracted PA on $n-k$ symbols and distance d, however it now contains more than $P(n-k,d)$ permutations, giving us a contradiction. Therefore, we can have no more than $P(n-k,d) \cdot \binom{n}{k}$ permutations in the original PA. □

As an example, Theorem 80 gives $P(11,6) \leq P(5,6)\binom{11}{6}$. Since $P(5,6) = 1$, this means $P(11,6) \leq \binom{11}{6} = 462$. By comparison, the Hamming upper bound given in Klove et al. (2010) is $P(11,6) \leq 2{,}603$.

Klove et al. (2010) give the following theorem which shows that for a fixed r, where $n = d + r$, at some point, increasing n and d uniformly no longer increases the maximum size of the PA.

Theorem 81. *(See Klove et al. (2010, Theorem 7)) For fixed r, there exist constants c_r and d_r such that $P(d+r,d) = c_r$ for $d \geq d_r$. Moreover,*

$$c_r \leq 2^{2r}(2r)!$$

and

$$d_r \leq 1 + (2r-1)c_r - r.$$

The proof of Theorem 81 uses the concept of *potent symbols*. An integer i is potent for Chebyshev distance d if there is another integer j in the given alphabet such that $|i-j| \geq d$. That is, the symbol can be used in permutations to achieve distance d. For example, in the alphabet $[1 \ldots 7]$ for $d = 5$, the potent symbols are 1, 2, 6, and 7. In general, for permutations over $n = d + r$, the symbols $\{1, 2, \ldots, r\}$ and $\{d+1, d+2, \ldots, d+r\}$ are potent.

While Theorem 81 does provide bounds for c_r and d_r, the authors' primary intent was simply to show the existence of such bounds, noting that the given bounds were generally

weak. The following theorem gives improved upper bounds for c_r and d_r. The idea is that for all $n > n_0$, a PA is limited by the number of ways to form distance agreements using potent symbols, rather than being limited by the number of available positions.

Theorem 82. *Suppose that* $P(n_0, n_0 - k) \leq m$ *such that*

$$2k(m+1) < (n_0+1)(1 + \lfloor n_0/(2k-1) \rfloor). \tag{4.1}$$

Then for all $n \geq n_0$*,*

$$P(n, n-k) \leq m.$$

Proof. Suppose to the contrary that $P(n, n-k) \geq m+1$, for some $n > n_0$. Suppose that n is the smallest such number, we will find a contradiction. Let $A = \{\pi_1, \pi_2, \ldots, \pi_{m+1}\}$ be a PA on n symbols with distance $n-k$. Let k_i denote the number of potent symbols in position i, taken over all permutations in A. Let $z = 1 + \lfloor n_0/(2k-1) \rfloor$. We show that $k_i \geq z$, for all i. Suppose, by symmetry of argument, that $k_1 \leq z-1$ and (by rearranging permutation order) only $\pi_i,\ 1 \leq i \leq k_1$, have potent symbols in the first position. Observe that each permutation has $2k$ potent symbols and that, by our assumption, all of the first k_1 permutations, and only the first k_1 permutations, have a potent symbol in position 1. So, if there are $z-1$ permutations, each adding $2k-1$ potent symbols to some position $j > 1$, the total number of potent symbols (other than the one in position 1) is $(2k-1)(z-1)$. Since the number of positions, namely, $n > n_0$ is greater than $(2k-1)(z-1)$, by the pigeonhole principle, there is a position $j > 1$ where all $\pi_i,\ 1 \leq i \leq k_1$, do not have potent symbols. Merge columns 1 and j and decrease n. That is, do the following:

- For each permutation π_i, $1 \leq i \leq k_1$, exchange the potent symbol in position 1 with the symbol in position j.

- Delete the symbol in position 1 in all permutations (they are no longer potent) and appropriately modify the symbols in each permutation so that they are consecutive integers (deletions may have created gaps).

The result is a PA of $m+1$ permutations on $n-1$ symbols with Chebyshev distance $n-k$. This contradicts our choice of n being smallest.

Note that the total number of potent symbols in the PA A is $2k(m+1)$. Since $k_i \geq z$, for all $1 \leq i \leq n$, $2k(m+1) \geq nz \geq (n_0+1)(1+\lfloor n_0/(2k-1) \rfloor)$ which contradicts Inequality 4.1. □

For $r=2$, Theorem 81 gives the bounds $c_2 \leq 384$ and $d_2 \leq 1{,}151$. We use Theorem 82 to show the exact values are $c_2 = 10$ and $d_2 = 3$, which we prove in Corollary 84. We first give Theorem 83 from Klove et al. (2010) which is necessary for our proof of Corollary 84.

Theorem 83. *(See Klove et al. (2010, Theorem 6)) If $d < n \leq 2d$, then*

$$P(n+1, d+1) \geq P(n, d).$$

Corollary 84.

$$P(n, n-2) = 10, \text{ for all } n \geq 5.$$

Proof. $P(n, n-2) = 10$, for all $5 \leq n \leq 11$, by the clique approach. In Theorem 82, set $n_0 = 11, k = 2$, and $m = 10$. Then $z = 1 + \lfloor n_0/(2k-1) \rfloor = 4$ and $2k(m+1) = 44 < 48 = (n_0+1)z$. So, $P(n, n-2) \leq 10$, for all $n \geq 11$, follows by Theorem 82. By Theorem 83, $P(n, n-2) \geq 10$, for all $n \geq 5$. Therefore, $P(n, n-2) = 10$, for all $n \geq 5$. □

Table 4.3 shows several upper bounds for $P(n, d)$.

Table 4.3. Upper Bounds for $P(n, d)$.

n/d	2	3	4	5	6	7	8	9	10
2	1	1	1	1	1	1	1	1	1
3	3	1	1	1	1	1	1	1	1
4	6	3	1	1	1	1	1	1	1
5	30	10	3	1	1	1	1	1	1
6	90	20	10	3	1	1	1	1	1
7	630	105	35	10	3	1	1	1	1
8	2,520	560	70	56	10	3	1	1	1
9	22,680	1,680	378	126	84	10	3	1	1
10	113,400	12,600	2,100	256	210	100	10	3	1
11	1,247,400	92,400	11,550	1,386	462	330	110	10	3
12	7,484,400	369,600	34,650	7,920	924	792	495	120	10
13	97,297,200	3,603,600	270,270	72,072	5,148	1,716	1,287	715	130
14	681,080,400	33,633,600	2,102,100	252,252	30,030	3,432	3,003	2,002	910
15	10,216,206,000	360,360,000	15,765,750	768,768	420,420	95,925	31,975	5,005	3,003

4.4 $P(n, 2)$

We now consider a bound for the general case $P(n, 2)$. Theorem 85 shows an iterative construction that extends any $(n, 2)$ PA by 2 additional symbols.

Theorem 85. *For all $n \geq 3$,*

$$P(n, 2) \geq P(n-2, 2)\binom{n}{2}.$$

Proof. Let A be a PA on the $n-2$ symbols $\{1, ..., n-2\}$ with Chebyshev distance 2. Take new symbols $a = n-1$, $b = n$, and insert them into each permutation of A in each of the possible $\binom{n}{2}$ positions such that a precedes b. If in the resulting permutation, the symbols appear in the order $a, n-2, b$, possibly separated by other symbols, then swap the positions of a and b. Let the resulting PA be B. Clearly, B has $\binom{n}{2}$ times as many permutations as A. We show that B has Chebyshev distance 2.

For a proof by contradiction, assume $\pi, \sigma \in B$ have $d(\pi, \sigma) \leq 1$. If π and σ are such that $\pi(i), \sigma(i) \in \{a, b\}$ and $\pi(j), \sigma(j) \in \{a, b\}$, for some i, j, then $d(\pi, \sigma) \geq 2$, because removing symbols a, b gives a permutation in A, and all permutations in A have distance at least 2. It follows that two permutations π, σ have at most one position, say i, such that $\pi(i), \sigma(i) \in \{a, b\}$. If there is no position i such that $\pi(i), \sigma(i) \in \{a, b\}$, then $d(\pi, \sigma) \geq 2$, as the symbol b is at distance at least 2 with all symbols except a and itself. Similarly, it follows that there cannot be a position i such that $\pi(i) = \sigma(i) = a$, or $\pi(i) = a$ and $\sigma(i) = b$, as this means $\pi(j) = b$, for some j, and $\sigma(j) \notin \{a, b\}$, *i.e.* $|\pi(j) - \sigma(j)| \geq 2$.

There is one remaining case, namely, $\pi(i) = \sigma(i) = b$, for some i, then, for some $j \neq k$, $\pi(j) = a$ and $\sigma(k) = a$. As we are assuming $d(\pi, \sigma) \leq 1$, we must have $\sigma(j) = n-2$ and $\pi(k) = n-2$. Now consider the order of the positions i, j, and k. If both j and k are less than i, say in the order $j < k < i$, then the permutation π has symbols in the order $a, n-2, b$, which contradicts the requirement that the symbols a and b are swapped. If both j and k

are greater than i, say in the order $i < j < k$, then the permutation π has the symbols in the order b, a, $n-2$, which contradicts the requirement that the symbols a and b not be swapped. Lastly, if we have the order, say $j < i < k$, then the permutation π has the symbols in the order $n-2$, b, a, which contradicts the requirement that the symbols a and b not be swapped. □

To show an example of the construction described in Theorem 85, consider the following $(3, 2)$ PA containing 3 permutations.

123
231
312

We then insert the symbols 4 and 5 into each of the $\binom{5}{2} = 10$ possible combinations of positions.

45123	41523	41253	41235	14523	14253	14235	12453	12435	12345
45231	42531	42351	42315	24531	24351	24315	23451	23415	23145
45312	43512	43152	43125	34512	34152	34125	31452	31425	31245

Observe that all permutations whose symbols appear in the order 4, 3, 5 are marked in red. We must then swap the positions of the symbols 4 and 5.

45123	41523	41253	51234	14523	14253	15234	12453	12534	12345
45231	42531	52341	52314	24531	25341	25314	23451	23415	23145
45312	53412	53142	53124	34512	34152	34125	31452	31425	31245

The result is a $(5, 2)$ PA of size $3 \cdot \binom{5}{2} = 30$. We have derived a formula for the size of this lower bound, given in Corollary 86.

Corollary 86. $P(n, 2) \geq \frac{n!}{2^{\lfloor n/2 \rfloor}}$.

Proof. This is shown by induction on n. First observe that $P(1,2) = P(2,2) = 1$. For the inductive step, assume $P(n,2) \geq \frac{n!}{2^{\lfloor n/2 \rfloor}}$. By Theorem 85, $P(n+2,2) \geq P(n,2)\binom{n+2}{2}$. By the inductive hypothesis, we obtain $P(n+2,2) \geq \frac{n!}{2^{\lfloor n/2 \rfloor}} \cdot \frac{(n+2)(n+1)}{2} = \frac{(n+2)!}{2^{\lfloor (n+2)/2 \rfloor}}$ □

We take a similar approach for an upper bound by applying Theorem 80 for $k = 2$, given in Corollary 87.

Corollary 87. $P(n,2) \leq \frac{n!}{2^{\lfloor n/2 \rfloor}}$.

Proof. This is shown by induction on n. First observe that $P(1,2) = P(2,2) = 1$. For the inductive step, assume $P(n,2) \leq \frac{n!}{2^{\lfloor n/2 \rfloor}}$. By Theorem 80, $P(n+2,2) \leq P(n,2)\binom{n+2}{2}$. By the inductive hypothesis, we obtain $P(n+2,2) \leq \frac{n!}{2^{\lfloor n/2 \rfloor}} \cdot \frac{(n+2)(n+1)}{2} = \frac{(n+2)!}{2^{\lfloor (n+2)/2 \rfloor}}$ □

As these corollaries show an agreement, we provide the following exact bound on $P(n,2)$.

Theorem 88.

$$P(n,2) = \frac{n!}{2^{\lfloor n/2 \rfloor}}.$$

Proof. Follows directly from Corollaries 86 and 87. □

CHAPTER 5

CONCLUSION AND FUTURE WORK

In Chapter 2 we described several normalization and mapping operations which helped us more efficiently search for permutation polynomials. Using Algorithm 1 we were able to identify all PPs of degree at most 10 in finite fields up to $\mathbb{F}_{97}$. This gave us improved bounds for many cases of $M(n, d)$, and also provided exact counts of what can be considered PRFs with a denominator of degree 0.

One initial observation is this algorithm is well suited to be adapted for multi-threaded or parallel processing. If we were conducting a search on permutations directly, each time a new permutation is considered, its distance must be checked against every permutation already in the set, which would cause synchronization issues. However, as we are searching for PPs, the distance is determined by the degree of the polynomial, so any PP found is valid. As Algorithm 1 already partitions the search space through its use of *masks*, this would be a natural way to divide the search into several threads.

Further normalization could also be achieved in certain cases by the use of Hermite's Criterion, which sates if $f(x)$ is a PP over $\mathbb{F}_q$, then for each k, $1 \leq k \leq q-2$, in $f(x)^k$, the sum of the coefficients of $x^{(q-1)i} = 0$ over all positive integers i (Lidl and Niederreiter, 1997). As an example, consider some normalized degree 11 PP $f(x) = x^{11} + a_9x^9 + \cdots + a_0$ over F_{43}. If we consider $f(x)^4$, then the sum of the coefficients of the $x^{(q-1)i}$ terms must equal 0. Since there is only one such coefficient in $f(x)^4$, of the term x^{42}, and its value is $4 \cdot a_9$, this implies a_9 must equal 0, giving us another fixed coefficient.

Since PPs have applications far beyond lower bounds of $M(n, d)$, sometimes an exhaustive search is unnecessary. Simply knowing of the existence of PPs of a large degree over some large F_q can be worth investigation. In these cases, we could alter the algorithm to limit the number of nonzero coefficients to some small value k, thus greatly reducing the search space.

While a failed search would not imply the nonexistence of PPs of that degree, it would allow partial searching of spaces otherwise infeasible.

In Chapter 3 we extended our normalization and mapping operations to the search of PRFs. We combined our findings with previous results in order to provide several new theorems which establish many new lower bounds for $M(n, d)$. As with PPs, we again observe that our computational results become limited for larger degree PRFs in larger $\mathbb{F}_q$.

Define the set of Möbius transformations $\mathcal{M} = \left\{ \frac{ax+b}{cx+d} \mid ad - bc \neq 0 \right\}$ as a subset of the rational functions over $\mathbb{F}_q$. Let $f(x) = \frac{u(x)}{v(x)}$ and $g(x) = \frac{r(x)}{s(x)}$ be PRFs. In Ferraguti and Micheli (2020), they define two PRFs as equivalent if their exist $m_1, m_2 \in \mathcal{M}$ such that $m_1 \circ f(x) \circ m_2 = g(x)$. Using this equivalence relation, they were able to represent all degree 3 PRFs with two representatives when $q \equiv 2 \pmod 6$, and with a single representative otherwise. Thus, we observe that the equivalence relation defined by composing on the left and right with Möbius transformations is much larger than what can be represented with our normalization and mapping operations.

The challenge is this transformation does not directly correspond to fixing coefficients, which is the primary approach of our search technique. To incorporate improvements from the composition of Möbius transformations, we would first need to find some kind of pattern or subset of $\mathcal{M}$ which would fix a designated coefficient at some value.

The other option would be to take a new search approach more directed by these Möbius compositions. The search could begin with a degree d PP, since there are many well-known classes of PPs, and a PP can still be considered a PRF. We could then iterate through the Möbius compositions to build a set of PRFs of the same degree. Since the composition of different transformations can result in the same PRF, it would be possible to reduce the search space for Möbius compositions.

For example, consider degree 3 PRFs over $\mathbb{F}_{11}$. Each of the Möbius transformations has 4 variables, giving us $11^8 = 214{,}358{,}881$ possible compositions. Factoring in the condition that

for each transformation $ad \neq bc$, this reduces the number to 5,336,100 compositions. Of these, there are only 87,120 distinct degree 3 PRFs over $\mathbb{F}_{11}$. Being able to identify beforehand which compositions would yield a duplicate result could make the search space very feasible, even for large $\mathbb{F}_q$.

In Chapter 4 we introduce multiple search techniques to construct PAs under Chebyshev distance. We make general improvements to existing theorems, and provide new theorems which establish improved lower and upper bounds for $P(n, d)$. We also give exact bounds for the general cases $P(n, 2)$ and $P(n, n-2)$.

For our Random/Greedy search, we make the greedy choice of choosing the next permutation in lexicographic order, but there are other heuristics that could be considered. We experimented with choosing the next permutation which invalidates the fewest remaining permutations, but this is computationally expensive and feasible for only small n. It slightly outperformed lexicographic order when no random permutations were used, but with random permutations, there was little to no benefit. Additionally, utilizing randomness generally improved the results. Still, there are other greedy choices or heuristics that could be applied to this search to yield improvements.

Our iterative construction for PAs of distance 2 is rather simple, yet it produces to the exact bound of $P(n, 2)$. So far, efforts to apply this technique to other distances has been unsuccessful, but it may still be possible. For distances 3 and greater, it may be necessary to add less than d symbols per iteration, or even to swap additional symbols than just the newly added symbols.

Bounds of the form $P(n, n-k)$ are an interesting problem, including finding the values n_0 and m such that $P(n, n-k) = m$ for all $n \geq n_0$. While Theorem 82 makes improvements on finding these values, for the case of $P(n, n-2)$, it can only be applied when $n_0 \geq 11$, and we know the actual value of $n_0 = 5$. This required us to prove the bound from $5 \leq n < 11$ by other methods. New approaches to this problem could yield additional bounds for larger values k.

APPENDIX

PP RESULTS

Table A.1. Number of normalized PPs (NPPs) and Total PPs for $q \leq 97$ and degree d, $6 \leq d \leq 10$.

q	6	7	8	9	10
11					
NPPs	24	225	2,754	29,985	
Total	29,949	272,250	3,332,340	36,281,850	
13					
NPPs	0	115	1,380	16,740	218,020
Total	0	233,220	2,798,640	33,948,720	442,144,560
16					
NPPs	840	216	14,816	4,200	1,417,600
Total	201,600	829,440	3,555,840	16,128,000	340,224,000
17					
NPPs	0	209	0	3,023	50,608
Total	0	966,416	0	13,978,352	234,011,392
19					
NPPs	0	112	864	0	19,544
Total	0	727,776	5,614,272	0	126,996,912
23					
NPPs	0	89	154	3,092	50,402
Total	0	1,035,782	1,792,252	35,984,696	586,578,476
25					
NPPs	0	45	0	1,038	401,280
Total	0	675,000	0	15,570,000	240,768,000
27					
NPPs	702	14	364	29,550	7,098
Total	492,804	265,356	6,899,256	20,744,100	134,535,492
29					
NPPs	0	0	32	1,751	1,568
Total	0	0	753,536	41,232,548	36,923,264
31					
NPPs	0	106	30	630	0
Total	0	3,055,980	864,900	18,162,900	0

Table A.1 continued

q	6	7	8	9	10
32					
NPPs	1,024	32	19,624	311	410,720
Total	1,015,808	1,015,808	19,467,008	9,872,384	407,434,240
37					
NPPs	0	37	0	0	216
Total	0	1,823,508	0	0	10,645,344
41					
NPPs	0	1	0	331	0
Total	0	67,240	0	22,256,440	0
43					
NPPs	0	0	0	42	98
Total	0	0	0	3,261,636	7,610,484
47					
NPPs	0	47	0	116	0
Total	0	4,775,858	0	11,787,224	0
49					
NPPs	0	3,961	0	96	16
Total	0	9,316,272	0	11,063,808	1,843,968
53					
NPPs	0	53	0	53	0
Total	0	7,741,604	0	7,741,604	0
59					
NPPs	0	59	0	117	0
Total	0	11,911,982	0	23,622,066	0
61					
Total	0	13,618,860	0	0	0
NPPs	0	61	0	0	0
64					
NPPs	0	0	80,968	0	21,120
Total	0	0	326,462,976	0	85,155,840
67					
NPPs	0	67	0	0	0
Total	0	19,850,358	0	0	0
71					
NPPs	0	0	0	71	0
Total	0	0	0	25,053,770	0

Table A.1 continued

q	6	7	8	9	10
73					
NPPs	0	73	0	0	0
Total	0	28,009,224	0	0	0
79					
NPPs	0	79	0	0	0
Total	0	38,457,042	0	0	0
81					
NPPs	0	81	0	471,891	0
Total	0	42,515,280	0	3,057,853,680	0
83					
NPPs	0	1	0	83	0
Total	0	564,898	0	46,886,534	0
89					
NPPs	0	89	0	89	
Total	0	62,037,272	0	62,037,272	
97					
NPPs	0	1	0	0	
Total	0	903,264	0	0	

REFERENCES

Alon, N. (1996). Independence numbers of locally sparse graphs and a ramsey type problem. *Random Structures & Algorithms 9*(3), 271–278.

Bastida, J. R. (1984). *Field extensions and Galois theory*. Number 22 in Encyclopedia of Mathematics and its Applications. Cambridge University Press.

Bereg, S., M. Haghpanah, B. Malouf, and I. H. Sudborough (2022). Improved bounds on permutation arrays for chebyshev metric. JCDCG3.

Bereg, S., A. Levy, and I. H. Sudborough (2018). Constructing permutation arrays from groups. *Designs, Codes and Cryptography 86*(5), 1095–1111.

Bereg, S., B. Malouf, L. Morales, T. Stanley, and I. H. Sudborough (2020). Improved lower bounds for permutation arrays using permutation rational functions. In J. Bajard and A. Topuzoglu (Eds.), *8th International Workshop on the Arithmetic of Finite Fields (WAIFI 2020)*, Volume 12542 of *Lecture Notes in Computer Science*, pp. 234–252. Springer. `https://doi.org/10.1007/978-3-030-68869-1_14`.

Bereg, S., B. Malouf, L. Morales, T. Stanley, and I. H. Sudborough (2022). Using permutation rational functions to obtain permutation arrays with large hamming distance. *Designs, Codes and Cryptography 90*(7), 1659–1677.

Bereg, S., B. Malouf, L. Morales, T. Stanley, I. H. Sudborough, and A. Wong (2019). Equivalence relations for computing permutation polynomials. *CoRR abs/1911.12823*, 1–39.

Bereg, S., Z. Miller, L. G. Mojica, L. Morales, and I. H. Sudborough (2019). New lower bounds for permutation arrays using contraction. *Designs, Codes and Cryptography 87*(9), 2105–2128.

Bereg, S., L. G. Mojica, L. Morales, and H. Sudborough (2017). Kronecker product and tiling of permutation arrays for hamming distances. In *2017 IEEE International Symposium on Information Theory (ISIT)*, pp. 2198–2202. IEEE.

Bereg, S., L. G. Mojica, L. Morales, and H. Sudborough (2020). Constructing permutation arrays using partition and extension. *Designs, Codes and Cryptography 88*(2), 311–339.

Bereg, S., L. Morales, and I. H. Sudborough (2017). Extending permutation arrays: improving mols bounds. *Designs, Codes and Cryptography 83*(3), 661–683.

Cameron, P. J. (1995). *Combinatorics: Topics, Techniques and Algorithms*. Cambridge University Press.

Chu, W., C. J. Colbourn, and P. Dukes (2004). Constructions for permutation codes in powerline communications. *Designs, Codes and Cryptography 32*(1), 51–64.

Colbourn, C. J., T. Klove, and A. C. Ling (2004). Permutation arrays for powerline communication and mutually orthogonal latin squares. *IEEE Transactions on Information Theory 50*(6), 1289–1291.

Dickson, L. E. (1896). The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *The Annals of Mathematics 11*(1/6), 65–120.

Ding, Z. and M. E. Zieve (2020). Low-degree permutation rational functions over finite fields. *arXiv e-prints 2010.15657*, 1–25. `https://arxiv.org/pdf/2010.15657.pdf`.

Dixon, J. D. and B. Mortimer (1996). *Permutation groups*, Volume 163. Springer Science & Business Media.

Fan, X. (2019). A classification of permutation polynomials of degree 7 over finite fields. *Finite Fields and Their Applications 59*, 1–21.

Fan, X. (2020). Permutation polynomials of degree 8 over finite fields of odd characteristic. *Bulletin of the Australian Mathematical Society 101*(1), 40–55.

Ferraguti, A. and G. Micheli (2020). Full classification of permutation rational functions and complete rational functions of degree three over finite fields. *Designs, Codes and Cryptography 88*(5), 867–886.

Ferreira, H. C. and A. H. Vinck (2000). Interference cancellation with permutation trellis codes. In *Vehicular Technology Conference Fall 2000. IEEE VTS Fall VTC2000. 52nd Vehicular Technology Conference (Cat. No. 00CH37152)*, Volume 5, pp. 2401–2407. IEEE.

Frankl, P. and M. Deza (1977). On the maximum number of permutations with given maximal or minimal distance. *Journal of Combinatorial Theory, Series A 22*(3), 352–360.

Hagberg, A. A., D. A. Schult, and P. J. Swart (2008). Exploring network structure, dynamics, and function using networkx. In G. Varoquaux, T. Vaught, and J. Millman (Eds.), *Proceedings of the 7th Python in Science Conference*, Pasadena, CA USA, pp. 11 – 15.

Hou, X. and C. Sze (2020). On a type of permutation rational functions over finite fields. *Finite Fields Their Appl. 68*, 101758.

Hou, X.-D. (2020). Rational functions of degree four that permute the projective line over a finite field. *arXiv e-prints 2005.07213v2*, 1–12. `https://arxiv.org/pdf/2005.07213v2.pdf`.

Hou, X.-d., G. L. Mullen, J. A. Sellers, and J. L. Yucas (2009). Reversed dickson polynomials over finite fields. *Finite Fields and Their Applications 15*(6), 748–773.

Jiang, A., R. Mateescu, M. Schwartz, and J. Bruck (2009). Rank modulation for flash memories. *IEEE Transactions on Information Theory 55*(6), 2659–2673.

Jiang, A., M. Schwartz, and J. Bruck (2008). Error-correcting codes for rank modulation. In *2008 IEEE International Symposium on Information Theory*, pp. 1736–1740. IEEE.

Klove, T., T.-T. Lin, S.-C. Tsai, and W.-G. Tzeng (2010). Permutation arrays under the chebyshev distance. *IEEE Transactions on Information Theory 56*(6), 2611–2617.

Knuth, D. E. (2005). *The Art of Computer Programming, Volume 4, Fascicle 2: Generating All Tuples and Permutations (Art of Computer Programming)*. Addison-Wesley Professional.

Li, J., D. B. Chandler, and Q. Xiang (2010). Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2. *Finite Fields and Their Applications 16*(6), 406–419.

Lidl, R. and H. Niederreiter (1997). *Finite fields*. Number 20 in Encyclopedia of Mathematics and its Applications. Cambridge university press.

Mullen, G. L. and D. Panario (2013). *Handbook of finite fields*, Volume 17. CRC Press Boca Raton.

Passman, D. (1968). *Permutation groups*. New York, New York: W.A. Benjamin, Inc.

Pavlidou, N., A. H. Vinck, J. Yazdani, and B. Honary (2003). Power line communications: state of the art and future trends. *IEEE Communications magazine 41*(4), 34–40.

Rossi, R. A., D. F. Gleich, A. H. Gebremedhin, and M. M. A. Patwary (2012). A fast parallel maximum clique algorithm for large sparse graphs and temporal strong components. In *ArXiv-preprint*, pp. 1–9.

Shallue, C. J. and I. M. Wanless (2013). Permutation polynomials and orthomorphism polynomials of degree six. *Finite Fields and Their Applications 20*, 84–92.

Vinck, A. H. (2000). Coded modulation for powerline communications. *AEU Int. J. Electron. Commun. 54*, 45–49.

Yang, L., K. Chen, and L. Yuan (2008). New constructions of permutation arrays. *arXiv preprint arXiv:0801.3987*, 1–11.

BIOGRAPHICAL SKETCH

After a long career in technical sales, and a fifteen year absence from school, Brian Malouf returned to academia full time to resume his education. He earned his BS in Computer Science in 2019 from The University of Texas at Dallas, graduating Summa Cum Laude. Though he initially planned to rejoin the workforce, he was eventually persuaded to continue his studies.

In 2021 he completed his MS in Computer Science from The University of Texas at Dallas, following the Intelligent Systems Track. He continued with his research focused on permutation arrays, completing his PhD in Computer Science in 2023.

CURRICULUM VITAE

Brian Malouf

Email: brian.malouf@utdallas.edu

Education

2020-2023 **PhD in Computer Science**, The University of Texas at Dallas, May 2023
Research Supervised by Prof. Sergey Bereg, Prof. Hal Sudborough
Thesis: Constructing Permutation Arrays of Known Distance

2020-2021 **MS in Computer Science**, The University of Texas at Dallas, May 2021
Intelligent Systems Track, GPA 4.0

2017-2019 **BS in Computer Science**, The University of Texas at Dallas, Dec 2019
Summa Cum Laude, GPA 4.0

Experience

2020-2023 **Teaching Assistant**, The University of Texas at Dallas
Assisted with teaching and grading for the following courses:
- CS 3345 Data Structures and Intro to Algorithmic Analysis
- CS 3354 Software Engineering
- CS 4341 Digital Logic and Computer Design
- CS 6319 Computational Geometry
- CS 6363 Design and Analysis of Computer Algorithms

2020-2022 **Lab Instructor**, The University of Texas at Dallas
Instructed students and ran lab for CS 4141 Digital Systems Laboratory.

Summer 2019 **Software Development Intern**, HCL America, Inc.
Developed several software solutions for clients using IBM Sterling OMS.

2007-2015 **Enterprise Solution Specialist**, MarketStar/Hewlett-Packard
Worked as a specialist for HP's Imaging and Printing Group with various responsibilities: technical consulting, client training, marketing support, account management.

Awards and Honors

Spring 2022 **Best Teaching Assistant**, Erik Jonsson School of Engineering and Computer Science, The University of Texas at Dallas.

Spring 2021 **Doctor Family Prize**, Department of Computer Science, The University of Texas at Dallas. Awarded to graduate student with best academic performance graduating in current semester.

Fall 2019 **Senior Project - First Place Award**, Department of Computer Science, The University of Texas at Dallas.

Publications

Journal Papers

Using permutation rational functions to obtain permutation arrays with large Hamming distance. Joint with Sergey Bereg, Linda Morales, Thomas Stanley, and Hal Sudborough. *Designs, Codes, and Cryptography*, 90(7):1659-1677, 2022.

Conference Papers

Improved lower bounds for permutation arrays using permutation rational functions. Joint with Sergey Bereg, Linda Morales, Thomas Stanley, and Hal Sudborough. *Proceedings of the 8th International Workshop on the Arithmetic of Finite Fields* (WAIFI), 234-252, 2020.

Conference Presentations

Improved bounds on permutation arrays for Chebyshev metric. Joint with Sergey Bereg, Mohammadreza Haghpanah, and Hal Sudborough. *Japan Conference on Discrete and Computational Geometry, Graphs, and Games* (JCDCG^3), 2022.

Improved permutation arrays for Kendall tau metric. Joint with Sergey Bereg, William Bumpass, Mohammadreza Haghpanah, and Hal Sudborough. *Japan Conference on Discrete and Computational Geometry, Graphs, and Games* (JCDCG^3), 2022.

Manuscripts

Equivalence relations for computing permutation polynomials. Joint with Sergey Bereg, Linda Morales, Thomas Stanley, Hal Sudborough, and Alexander Wong. *CoRR*, abs/1911.12823, 2019.

Research Interests

Coding theory; algorithms and data structures; computational geometry; artificial intelligence; multi-agent systems; graph algorithms.