TRANSITIVITY AND HAMMING DISTANCE OF PERMUTATION ARRAYS

by

Quan Tuong Nguyen

APPROVED BY SUPERVISORY COMMITTEE:

I. Hal Sudborough, Chair

Sergey Bereg

R. Chandrasekaran

Ovidiu Daescu

This dissertation is dedicated to my parents, my beloved wife Chinh and my son Luke.

TRANSITIVITY AND HAMMING DISTANCE OF PERMUTATION ARRAYS

by

QUAN TUONG NGUYEN, BE, 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

December 2013

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

ACKNOWLEDGMENTS

I would like to thank my Supervising Professor, Dr. Hal Sudborough, for his continual and significant guidance. The routine meeting every week has kept my research going well and has provided fruitful results due to added insight and timely feedback. I learned a lot from him, in research and in the courses that he taught, both as his student and as his teaching assistant. I would like to thank him for his revisions and many invaluable comments on both the writing and the preparation of this dissertation.

I am greatly indebted to Dr. Sergey Bereg, Dr. R. Chandrasekaran and Dr. Ovidiu Daescu for spending their time serving on my dissertation committee. Their careful reading and precious comments have improved the dissertation and its exposition greatly.

I would like to send my special thanks to Dr. Linda Morales, Dr. William Fahle and Avi Levy for their great contributions to this research. I am also grateful to Dr. Saïd Bettayeb, Dr. Charles Shields and Dr. Walter Voit for their help in the early stage of this research. I appreciate the help with my paperwork from Dr. Austin Cunningham, Ms. Wanda Trotta, Ms. Amanda Aiuvalasit, Mr. Shyam Karrah, Mr. Eric Moden, Ms. Emebet Sahle and Ms. Cathy Kelley. And special thanks to all members of the Biblical Community Church.

Finally, yet importantly, I would like to express my deep appreciation to the sacrifice of my father, my mother, my sisters, my wife and my son. Thank you for always being with me, physically and spiritually, to encourage me in the completion of this dissertation.

August 2013

TRANSITIVITY AND HAMMING DISTANCE OF PERMUTATION ARRAYS

Publication No. _____

Quan Tuong Nguyen, PhD
The University of Texas at Dallas, 2013

Supervising Professor: I. Hal Sudborough

A permutation array is a set of permutations on n symbols. A permutation array is k-transitive, denoted by t-PA(n,k), if for any k-tuple of positions $\rho=(p_1,p_2,\ldots,p_k)$ and any k-tuple of symbols $\tau=(t_1,t_2,\ldots,t_k)$, there is a permutation π in t-PA(n,k) that maps ρ to τ. A code permutation array has hamming distance d, denoted by c-PA(n,d), if any two distinct permutations in this c-PA(n,d) differ in at least d positions. When there exists a sharply k-transitive group, a minimum t-PA(n,k) and a maximum c-PA(n,d) where d=n-k+1 are achieved. However, except for the trivial groups, i.e., symmetric, alternating and cyclic groups, and the Mathieu groups M_{11}, M_{12} which are sharply 4-transitive and sharply 5-transitive, respectively, the nonexistence of sharply k-transitive groups was proved for all $k > 3$ and for infinitely many values of n when $k = 2$ or $k = 3$. We consider methods to lower the size of transitive permutation arrays in those cases. We also give new techniques to increase the size of code permutation arrays for given hamming distances.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

A permutation array, denoted by PA(n,d), is a set of permutations on n symbols. Let I_n denote the set $\{1,2,\ldots,n\}$. Let S_n be the set of all permutations on I_n. A permutation array is a subset of S_n. A permutation array PA(n,d) of size m can be viewed as a two-dimensional array (i.e., a table) that has m rows and n columns, where each of its rows is a permutation on n symbols.

1.1 Transitivity

A permutation array is k-transitive, denoted by t-PA(n,k), if for any k-tuple of positions $\rho=(p_1,p_2,\ldots,p_k)$ and any k-tuple of symbols $\tau=(t_1,t_2,\ldots,t_k)$, there is a permutation π in t-PA(n,k) that maps ρ to τ. If, for all pairs ρ and τ, there is a unique permutation π in t-PA(n,k) that maps ρ to τ, the permutation array is called sharply k-transitive. If there is more than one permutation in the permutation array that maps a k-tuple of positions ρ to a k-tuple of symbols τ, that ρ-to-τ mapping is redundantly covered (or, for short, is redundant). When all ρ-to-τ mappings covered by a permutation are redundant, that permutation is also redundant because we can remove it from the permutation array without affecting the transitivity of the permutation array. A sharply k-transitive permutation array has no redundant ρ-to-τ mapping, therefore it has no redundant permutation. The objective for transitivity is to find the smallest cardinality set of permutations of length n that is k-transitive. We denote F(n,k) as the minimum size of a t-PA(n,k).

The problem of finding a k-transitive permutation array was first made known to us as the problem of finding a k-tuple cover, posed by Latifi [44]. The problem can be used to find the fault tolerance of a star network where each of the processors, or nodes, is labeled by a permutation and any two processors are connected if one can be transformed to the other by a transposition of the form (1 i), i.e., an exchange of the first and the i^{th} symbol in the permutation (Akers and Krishnamurthy [1]). A star network of size n, denoted as P_n, contains (as a sub-network) a surviving copy of a smaller star network of size n-k, denoted as P_{n-k}, if and only if there is no k-transitive set of permutations in S_n which are labels for faulty processors. For example, P_4 contains (as a subgraph) a surviving copy of P_3 if and only if there is no transitive (i.e., 1-transitive) set of permutations in S_4 which are labels for faulty processors. Other applications of transitive permutation arrays include combinatorial design of experiments (Box et al. [11]), finite projective geometry, coding theory, mutually orthogonal Latin Squares, cryptography and analytical software testing (Dalal and Mallows [20], Bein et al. [3]).

As often happens in theoretical work, two different sets of scientists research on similar problems without knowing others' work. In our case, we were originally unaware of important theorems from group theorists (Batten and Beutelspacher [2], Biggs and White [6], Bruck and Ryser [12], Cameron [13], Carmichael [15], Huppert and Blackburn [37], Kerby [40], Nagao [49], Passman [51], Wielandt [59]). For example, F(6,3) = 120 is a direct result from group theory, while we went through a lot of trouble and computations to find such a 3-tuple cover for permutations of length 6. William Fahle, via his dissertation [27], discovered the connection between the two problems, and thereby helped fill out infinitely many optimal results in the F(n,k) table. Nevertheless, as Fahle discussed, those mathematical results from group theory

stand like sharp prime-power islands in the integer sea of possible values for n and k, and are particularly sparse when k > 3. Therefore, this dissertation gives various new approaches and techniques to give good results for all values of n and k, while minimizing the computational effort.

The following results are known for transitive permutation arrays:

Proposition 1.1:

a. $(n)_k \leq F(n,k) \leq \binom{n}{k}(n)_k$ (Bein et al. [3], combinatorial bounds), where $(n)_k$ is the falling factorial and $(n)_k = n(n-1)\ldots(n-k+1)$.

b. $F(n,k-1) \leq F(n,k)$ (Bein et al. [3])

c. $F(n-1,k) \leq F(n,k)$ (Bein et al. [3], contraction operation)

d. $(n)_2 \leq F(n,2) \leq (37/25)(n)_2 = 1.48(n)_2$ (Fahle's dissertation [27])

e. $(n)_3 \leq F(n,3) \leq (217/125)(n)_3 = 1.736(n)_3$ (Fahle's dissertation [27])

f. $F(n+1,k) \leq F(n,k) + n.F(n,k-1)$ (Fahle's dissertation [27])

g. $F(n,k) \geq n.F(n-1,k-1)$ (Fahle's dissertation [27], diagonal sharpness theorem)

Transitive groups have been studied extensively (Batten and Beutelspacher [2], Biggs and White [6], Bruck and Ryser [12], Cameron [13], Carmichael [15], Huppert and Blackburn [37], Kerby [40], Nagao [49], Passman [51], Wielandt [59]). Since the group properties (closure, associativity, identity element and inverse element) are not needed in creating a permutation array, any k-transitive group is also a k-transitive permutation array. The following results are optimal and are obtained directly from group theory (Batten and Beutelspacher [2], Biggs and White [6], Bruck and Ryser [12], Cameron [13], Carmichael [15], Huppert and Blackburn [37], Kerby [40], Nagao [49], Passman [51], Wielandt [59]).

Proposition 1.2:

a. $F(n,1) = (n)_1 = n$ (Cyclic group C_n)

b. $F(n,2) = (n)_2 = n(n-1)$ (Sharply 2-transitive group AGL(1,n) when n is a power of a prime)

c. $F(n,3) = (n)_3 = n(n-1)(n-2)$ (Sharply 3-transitive group PGL(2,n-1) when n is one more than a power of a prime)

d. $F(11,4) = (11)_4 = 11*10*9*8 = 7{,}920$ (Mathieu group M_{11})

e. $F(12,5) = (12)_5 = 12*11*10*9*8 = 95{,}040$ (Mathieu group M_{12})

f. $F(n,n-2) = (n)_{n-2} = n!/2$ (Alternating group A_n)

g. $F(n,n-1) = (n)_{n-1} = n!$ (Symmetric group S_n)

Nonexistence of sharply k-transitive permutation arrays:

The existence of sharply k-transitive groups implies the existence of sharply k-transitive permutation arrays. When k = 2, the non-existence of sharply 2-transitive groups also implies the non-existence of sharply 2-transitive permutation arrays (Blake et al. [8], Kuznetsov [41-42]). In general, however, it is not known if any sharply k-transitive permutation arrays exist when the respective sharply k-transitive group does not.

Proposition 1.3:

a. There is no sharply 2-transitive permutation group of degree n (and hence, no sharply 3-transitive permutation group of degree n+1) if $n \equiv 1,2 \pmod 4$ and n is not a sum of two squares (Bruck-Ryser [12]).

b. There is no sharply 2-transitive permutation group of degree 10 (Lam et al. [43]). Consequently, there is no sharply 3-transitive permutation group of degree 11.

c. There is no sharp t-PA(n,k) if $4 \leq n-k \leq k$ (Quistorff [53]).

d. There is no sharply k-transitive permutation group for $k \geq 4$ other than the Mathieu groups M_{11} and M_{12} and alternating and symmetric groups (Kerby [40]).

e. Each invertible sharp t-PA(n,k) with $k \geq 4$ is a group (Bonisoli and Quattrocchi [10]).

Part (b) is the first example to show that the necessary condition of the Bruck-Ryser Theorem in part (a) is not sufficient. Part (a) and (b) imply that there is no sharp t-PA(n,2) when n = 10, or when $n \equiv 1,2 \pmod 4$ and n is not a sum of two squares (by Blake et al. [8], Kuznetsov [41-42]), for example when n = 6, 14, 18, 21, 22... Although we cannot conclude the non-existence of sharp t-PA(n+1,3) directly from the non-existence of the corresponding sharply 3-transitive group, the diagonal sharpness theorem showed in Fahle [27], which is part (g) of Proposition 1.1, allows us to make a stronger conclusion. For example, when n = 6, $F(6,2) \geq (6)_2 + 1 = 31$ as explained above. In fact, by an exhaustive search, we were able to prove that $F(6,2) \geq 33$. Using the diagonal sharpness theorem, we can conclude that $F(7,3) \geq 7*33 = 231$ which is better than the lower bound of $(7)_3 + 1 = 211$, $F(8,4) \geq 8*7*33 = 1848$, and so on.

Table 1.1. Published upper bounds for F(n,k) (up to Fahle's dissertation [27])

$F(n,k)$	*n=5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*
k=1	5	6	7	8	9	10	11	12
2	20	37	42	56	72	110	110	156
3	60	120	336	336	504	720	1320	1320
4	120	360	1020	3265	5911	7920	7920	22440
5		720	2520	9240	34502	86883	95040	95040
6			5040	20160	91714	389091	1257921	2303361
7				40320	181440	985306	4876216	18713347
8					362880	1814400	11667460	65305836
9						3628800	19958400	148300460
10							39916800	239500800

Table 1.1 summaries the published upper bounds of F(n,k). Most of those bounds are taken from Fahle's dissertation [27].

1.2 Hamming distance

Two permutations π and $\sigma \in S_n$ have (hamming) distance d, denoted as DIST(π,σ)=d if $\pi\sigma^{-1}$ has exactly n-d fixed points. In other words, two permutations have hamming distance d if they differ in d positions. A code permutation array, or a permutation code, has hamming distance d, denoted by c-PA(n,d), if any two distinct permutations in this c-PA(n,d) have hamming distance at least d. The objective here is to find the largest set of permutations of length n that has hamming distance d. We denote M(n,d) as the maximum size of a c-PA(n,d).

Permutation codes are of considerable interest, from block ciphers (de la Torre et al. [21]) to multilevel flash memories (Jiang et al. [39]), and primarily for communication over power-lines (Ferreira and Vinck [29], Pavlidou et al. [52], Vinck [57]). In addition to the ability of transmitting electric power, an electric power line can be used to transmit also the information by modulating its frequency to create a set of n close, but orthogonal, frequencies. These frequencies can be decoded as symbols. To avoid interference between information and power transmission, block coding, i.e., codeword of fixed length l, is used so that the power output remains as constant as possible. If each code has the same r_i occurrences of the i^{th} symbol (or i^{th} frequency) such that $\sum_{i=1}^{n} r_i = l$, then the code is a constant composition code. Especially, when $r_1=\ldots=r_n=1$ and l=n, each code is a permutation and length l is shortest possible, so the power output remains constant. Moreover, each type of noise that may arise in the information transmission will affect only a single symbol of a codeword. Therefore, the knowledge of

minimum hamming distance between any two distinct codewords in a code permutation array will help in error correction at the receiver side.

The following are known results for code permutation arrays:

Proposition 1.4: (Chu et al. [16])

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

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

c. $M(n,d) \leq n!/(d-1)! = (n)_{n-d+1}$

Proposition 1.5:

$M(n,n-1) \geq mn$ if there are m mutually orthogonal Latin squares (MOLS) of order n (Colbourn et al. [18]).

For example, $M(14,13) \geq 4*14 = 56$, because Todorov [56] has shown that there are four MOLS of order 14.

Proposition 1.6: (Frankl and Deza [30])

$M(n,d) \geq n!/V(n,d-1)$, where $V(n,r)$ is the volume of the ball in S_n of radius r centered at some permutation π, i.e., the number of permutations of distance no greater than r from π.

This lower bound is referred to as the Gilbert-Varshamov bound (Berlekamp [5]). To obtain a code permutation array of at least that many permutations, one can, in each iteration, randomly choose a permutation to put in the set and remove all permutations that are too close to it. Such permutations are in the mentioned ball of radius d-1 centered at the chosen permutation. If we consider all balls to be pairwise disjoint during the c-PA constructing process, the number of iterations, or equivalently, the size of the constructed c-PA, is at least equal to the fraction of the total number of permutations and the volume of the ball. Mathematically, the volume of a

ball of radius r is the integration of all spherical layers, each at distance exactly k away from the center, where $0 \leq k \leq r$, so $V(n,r) = \sum_{k=0}^{r} \binom{n}{k} D_k$, where D_k is the number of derangements of order k, i.e., permutations in S_k with no fixed point. Gao et al. [31] recently improved the Gilbert-Varshamov bound asymptotically by a factor of log(n), when the code length n goes to infinity.

Proposition 1.7:

Any sharp t-PA(n,k) is equivalent to a maximum c-PA(n,d), where distance d=n-k+1 (Blake et al. [8], Chu et al. [16], Frankl and Deza [30]).

Proof: For any two distinct permutations in the sharp t-PA(n,k), a hamming distance of n-k or less between them will imply that they agree in k or more positions, or in other words, these two permutations map the same k-tuple of positions to the same k-tuple of symbols. This is a violation of the sharpness property of the mentioned PA. So, the first assertion of the proposition follows. For the second assertion, a maximum c-PA(n,d) will have $(n)_{n-d+1} = (n)_k$ permutations, which is the least number of permutations to cover all k-tuple position-symbol mappings. If this c-PA(n,d) is not a sharp t-PA(n,k), then there exist two permutations in the PA that map the same k-tuple of positions to the same k-tuple of symbols. These two permutations will therefore have hamming distance n-k=d-1 or less, which is a contradiction. □

Using Propositions 1.2 and 1.7, we have the following optimal results for M(n,d):

Proposition 1.8: (Blake [7], Chu et al. [16], Frankl and Deza [30])

a. $F(n,1) = M(n,n) = (n)_1 = n$ (Cyclic group C_n)
b. $F(n,2) = M(n,n-1) = (n)_2 = n(n-1)$ (Sharply 2-transitive group AGL(1,n) when n is a power of a prime)

c. $F(n,3) = M(n,n-2) = (n)_3 = n(n-1)(n-2)$ (Sharply 3-transitive group PGL(2,n-1) when n is one more than a power of a prime)

d. $F(11,4) = M(11,8) = (11)_4 = 11*10*9*8 = 7{,}920$ (Mathieu group M_{11})

e. $F(12,5) = M(12,8) = (12)_5 = 12*11*10*9*8 = 95{,}040$ (Mathieu group M_{12})

f. $F(n,n-2) = M(n,3) = (n)_{n-2} = n!/2$ (Alternating group A_n)

g. $F(n,n-1) = M(n,2) = (n)_{n-1} = n!$ (Symmetric group S_n)

With permutation polynomials over finite fields (Chu et al. [16]), automorphism groups and with computational efforts that use greedy algorithm, maximum clique algorithms (Chu et al. [16], Smith and Montemanni [54]), or even the interest in only one particular value of M(10,9), (Janiszczak and Staszewski [38]), many entries of the M(n,d) table have been improved. Table 1.2 below summaries the published lower bounds of M(n,d).

Table 1.2. Published lower bounds for M(n,d) (up to Smith and Montemanni [54])

$M(n,d)$	*d=4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*
n=5	20	5								
6	120	18	6							
7	349	77	42	7						
8	2688	616	336	56	8					
9	18144	3024	1512	504	72	9				
10	150480	18720	8640	720	720	49	10			
11	1742400	205920	95040	7920	7920	154	110	11		
12	20908800	2376000	190080	95040	95040	1320	1320	60	12	
13	41712480		271908			4810	906*	195	156	13
14	550368000						6552	2184	2184	52

The upper bounds of M(n,d) have also been studied (Bogaerts [9], Chu et al. [16], Deza and Vanstone [22], Dukes and Sawchuck [24], Frankl and M. Deza [30], Tarnanen [55], Yang et

al. [62]). The most complete summarization on the upper bounds of M(n,d) can be found in Smith and Montemanni [54].

1.3 Latin Square

A Latin Square of size n is a permutation array that has the same number of rows and columns, i.e., n rows and n columns, where each row or column is a permutation on I_n (McKay et al. [46], McKay and Wanless [47], Evans [26]).

Proposition 1.9: Any Latin Square of size n is equivalent to a sharp t-PA(n,1).

Proof: The first assertion is trivial because of the property of any Latin Square. For the second assertion, a sharp t-PA(n,1) is a set of n permutations, which forms a square of n rows by n columns. Because each row is a permutation already, we need to show that each column is also a permutation on I_n to complete the proof. Suppose for the sake of contradiction that there exists a column which is not a permutation on I_n, then there must exist a symbol i such that i does not appear in that column. This implies that the square is not a t-PA(n,1), which is a contradiction. □

Corollary 1.10: Any Latin Square of size n is equivalent to a maximum c-PA(n,n).

Proof: Proposition 1.7 and Proposition 1.9 give the result of Corollary 1.10. □

1.4 Problems involving permutation arrays and their complexity

Partial Latin Square Extension (PLSE) is the problem of deciding whether a partially filled Latin Square can be fully extended into a Latin Square. PLSE was proved NP-complete by C.J. Colbourn in 1984 [17]. In 2001, Easton and Parker [25] proved that completing a partially filled Latin Square with no more than three unfilled cells in any row or column remains NP-hard.

In 2007, Hajirasouliha et al. [35] proved that PLSE is APX-hard and gave a $\left(\frac{2}{3} - o(1)\right)$-approximation algorithm for the problem.

Similarly, we define Partial t-PA Extension (Pt-PAE) the problem of deciding whether a given partially filled t-PA(n,k) can be fully extended into a t-PA(n,k) and define Partial c-PA Extension (Pc-PAE) the problem of deciding whether a given partially filled c-PA(n,d) can be fully extended into a c-PA(n,d).

Proposition 1.11: Pt-PAE is NP-complete

Proof: An instance of the Pt-PAE problem is a pair of a positive integer k and a partially filled t-PA(n,k), which is a m x n grid (m rows by n columns) where each cell is either empty (0) or filled with a number in $I_n = \{1, 2, ..., n\}$ and each number (except 0) occurs at most once in every row and every column. Pt-PAE is in NP because with a completely filled grid m x n as a certificate, one can verify in polynomial time if this grid is a t-PA(n,k) and if it is an extension of the formerly given partially filled grid. Proposition 1.9 gives a polynomial time reduction from the PLSE problem to the Pt-PAE problem because the former is a special case of the latter where k=1 and m=n. Hence Pt-PAE is NP-complete. □

Proposition 1.12: Pc-PAE is NP-complete.

Proof: An instance of the Pc-PAE problem is a pair of a positive integer d and a partially filled c-PA(n,d), which is a m x n grid (m rows by n columns) where each cell is either empty (0) or filled with a number in $I_n = \{1, 2, ..., n\}$ and each number (except 0) occurs at most once in every row and every column. Pc-PAE is in NP because with a completely filled grid m x n as a certificate, one can verify in polynomial time if this grid is a c-PA(n,d) and if it is an extension of the formerly given partially filled grid. Corollary 1.10 gives a polynomial time reduction from

the PLSE problem to the Pc-PAE problem because the former is a special case of the latter where d=n and m=n. Hence Pc-PAE is NP-complete. □

The t-PA(n,k) problem is the problem of deciding, given input n, k, and m, whether there is a t-PA(n,k) of cardinality m (Bein et al. [3]). For each fixed k, the problem is in the class NP, but it is unknown whether it is NP-complete, or whether it is deterministically computable in polynomial time. Similarly, the c-PA(n,d) problem is the problem of deciding, given input n, d, and m, whether there is a c-PA(n,d) of cardinality m. For each fixed d, the problem is in the class NP, but whether it is NP-complete, or whether it is deterministically tractable is still an open question.

1.5 Isotopy/Equivalence class

We extend the isotopy class of Latin Squares (McKay et al. [46], McKay and Wanless [47]) for permutation arrays. Two permutation arrays are said to be *isotopic* if one can be obtained from the other by some number of operations that permute rows, columns or symbols (Fahle [27]). The equivalence classes of this relation are called *isotopy classes*. A permutation array is *reduced* (also called "normalized") if the first row (and optionally, the first column) is in increasing order (i.e., is I_n). Any permutation array can be reduced by sorting the rows and columns.

Theorem 1.13 (Isotopy Theorem): Any two permutation arrays in the same isotopy class have the same transitivity and same hamming distance.

Proof: The proof of this Theorem is omitted since it is straightforward and was done by Fahle in his dissertation [27].

This dissertation is organized as follows: Chapter 2 summarizes some known theorems that underlie our research and provides some preliminary improvements over those theorems. Chapter 3 contains the main results of this research where several techniques are shown to lower the size of transitive permutation arrays. The theorems are applied throughout the F(n,k) table to give infinitely many new upper bounds for every single entry of the table. Similarly, Chapter 4 gives several techniques to improve the size of code permutation arrays. It also gives a formal definition of the polymorphic hamming distance function that is used throughout the chapter and discusses the usage of frequency permutation arrays as templates to construct new code permutation arrays.

CHAPTER 2

PRELIMINARY IMPROVEMENTS

In this chapter, we show some preliminary improvements over the results found in Bein et al. [3] and in Fahle's dissertation [27]. We also give a formal definition of the contraction operation, which was first presented in Bein et al. [3]. We prove that the result of the contraction operation on an invertible permutation array is also an invertible permutation array.

2.1 Preliminary improvements

Theorem 2.1: For all $n > 2$, and $2 \leq k < n$, $F(n,k-1) < F(n,k)$.

Proof: Bein et al. [3] showed that $F(n,k-1) \leq F(n,k)$. This is straightforward because any k-transitive permutation array is also (k-1)-transitive. According to the Isotopy Theorem, any t-PA(n,k) can be transformed in order to contain the identity permutation, namely $I_n = (1, 2, \ldots, n)$. So, without loss of generality, assume that any given t-PA(n,k) S contains the identity permutation I_n. We now prove that I_n can be safely thrown away without affecting the (k-1)-transitivity of the set S. Consider any mapping from a (k-1)-tuple of positions $\rho = (p_1,p_2,\ldots,p_{k-1})$ to a (k-1)-tuple of symbols $\tau = \rho = (p_1,p_2,\ldots,p_{k-1})$ that I_n covers. Let $\rho' = (p_1,p_2,\ldots,p_{k-1},p_k)$ and let $\tau' = (p_1,p_2,\ldots,p_{k-1},t_k)$ with $p_k \neq t_k$, because S is a t-PA(n,k), there is a permutation π in S that maps ρ' to τ'. And this permutation π is not the identity permutation, because $p_k \neq t_k$. Therefore, the remaining set after the removal of I_n covers all (k-1)-ρ-to-τ mapping that I_n covers. It follows that $F(n,k-1)$ is at least one (1) less than $F(n,k)$. □

The following two theorems give tighter upper bounds for the approximation ratios of F(n,2) and F(n,3). They are in fact improvements of two corresponding theorems in (Fahle [27]). We show the intuition on how we came up with those bounds and discuss some cases where we can further improve the bounds.

Let us first restate Nagura's Theorem [50]: For any integer $n \geq 25$, there exists a prime p such that $n \leq p \leq 6n/5$.

Theorem 2.2: For all integer n, $(n)_2 \leq F(n,2) \leq (145/100)(n)_2 = 1.45(n)_2$.

Proof: The combinatorial lower bound gives us the left part of the inequality.

For any prime power $q \leq 25$, $F(q,2) = (q)_2$, and that satisfies the theorem. For any non-prime-power integer n such that $2 < n < 25$, let q be the next higher prime power. One can verify by hand that $F(n,2) \leq F(q,2) = (q)_2 \leq 1.45(n)_2$. For example, when n = 20, with the next higher prime power q = 23, $(23)_2/(20)_2 = (23*22)/(20*19) = 506/380 \leq 1.45$. The largest ratio among all $2 < n < 25$ occurs at n = 6 (q = 7), where it is $(7)_2/(6)_2 = (7*6)/(6*5) = 1.4$.

For any $n \geq 25$, by Nagura's Theorem [50], there exists a prime such that $n \leq p \leq 6n/5$.

By Proposition 1.1 (c), since $n \leq p$, $F(n,2) \leq F(p,2) = (p)_2 = p(p-1) \leq \left(\frac{6n}{5}\right)\left(\frac{6n}{5} - 1\right) \leq cn(n-1)$.

Constant c is the solution of

$$\left(\frac{6n}{5}\right)\left(\frac{6n}{5} - 1\right) \leq cn(n-1)$$

$\leftrightarrow \quad 36n^2 - 30n \leq 25cn^2 - 25cn$

$\leftrightarrow \quad (25c-30)n \leq (25c-36)n^2$

$\leftrightarrow \quad \frac{25c-30}{25c-36} \leq n$ (since $c \geq 1.4$, $25c-30 > 0$, we are just interested in $25c-36 > 0$ or $c > (6/5)^2 = 1.44$)

Since n can be as small as 25 to satisfy the condition of Nagura's Theorem [50], c can be as large as 1.45, which is the solution of $\frac{25c-30}{25c-36} = 25$.

Therefore, $(n)_2 \leq F(n,2) \leq 1.45(n)_2$. □

Note that, for c > 1.44, $\frac{25c-30}{25c-36}$ is a decreasing function. So, one can verify Theorem 2.2 up to a larger value of n to obtain a better ratio. For example, at n = 49, the solution of $\frac{25c-30}{25c-36} = 49$ gives a ratio of 1.445. One can theoretically verify Theorem 2.2 up to infinity to obtain the ratio of 1.44.

Theorem 2.3: For all integer n, $(n)_3 \leq F(n,3) \leq (134850/78000)(n)_3 \approx 1.729(n)_3$.

Proof: The combinatorial lower bound gives us the left part of the inequality.

For any prime power $q \leq 25$, $F(q+1,3) = (q+1)_3$, and that satisfies the theorem. For any non-prime-power integer n such that $2 < n < 25$, let q be the next higher prime power. One can verify by hand that $F(n+1,3) \leq F(q+1,3) = (q+1)_3 \leq 1.729(n+1)_3$. For example, when n = 14, with the next higher prime power q = 16, $(17)_3/(15)_3 = (17*16*15)/(15*14*13) = 4080/2730 \leq 1.729$. The largest ratio among all $2 < n < 25$ occurs at n = 6 (q = 7), where it is $(8)_3/(7)_3 = (8*7*6)/(7*6*5) = 1.6$.

For any $n \geq 25$, by Nagura's Theorem [50], there exists a prime such that $n \leq p \leq 6n/5$.

By Proposition 1.1 (c), since $n \leq p$, $F(n+1,3) \leq F(p+1,3) = (p+1)_3 = (p+1)p(p-1)$

$$\leq \left(\frac{6n}{5}+1\right)\left(\frac{6n}{5}\right)\left(\frac{6n}{5}-1\right) \leq c(n+1)n(n-1).$$

Constant c is the solution of

$$\left(\frac{6n}{5}+1\right)\left(\frac{6n}{5}\right)\left(\frac{6n}{5}-1\right) \leq c(n+1)n(n-1)$$

$$\leftrightarrow \quad 216n^3-150n \leq 125cn^3 - 125cn$$

$\leftrightarrow$ $(125c\text{-}150)n \leq (125c\text{-}216)n^3$

$\leftrightarrow$ $\frac{125c-150}{125c-216} \leq n^2$ (since $c \geq 1.6$, $125c\text{-}150 > 0$, we are just interested in $125c\text{-}216 > 0$ or $c > (6/5)^3 = 1.728$)

Since n can be as small as 25 to satisfy the condition of Nagura's Theorem [50], c can be as large as 1.729, which is the solution of $\frac{125c-150}{125c-216} = 25^2 = 625$.

Therefore, $(n)_3 \leq F(n,3) \leq 1.729(n)_3$. □

Similar to the note after Theorem 2.2, for $c > 1.728$, $\frac{125c-150}{125c-216}$ is also a decreasing function. So, one can verify Theorem 2.3 up to a larger value of n to obtain a better ratio. For example, at n = 49, the solution of $\frac{125c-150}{125c-216} = 49^2$ gives a ratio of 1.72822. One can theoretically verify Theorem 2.3 to infinity to obtain the ratio of 1.728.

Note that, since every prime number p is also a prime power $q = p^1$, the interval containing at least one prime power is no greater than the interval containing at least one prime number. That means if we can prove a strictly smaller interval for prime powers than the interval for prime numbers from Nagura's Theorem [50] (from n to 6n/5), we can accordingly improve, i.e., lower, the upper bounds for the approximation ratios of F(n,2) and F(n,3) as well. Obviously, an improvement of Nagura's Theorem [50] also improves our bounds.

2.2 Contraction operation

The operation was first introduced in Bein et al. [3]. It allows us to transform a set of permutations of length n into a new set of permutations of length n-1 with the same cardinality. Let A be a set of permutations of length n. For each permutation σ in A, the contraction of σ is:

$C(\sigma) = (\sigma^{-1}(n)\ n) \circ \sigma \mid_{n-1}$

where $(\sigma^{-1}(n)\ n)$ is the transposition between the position that contains symbol n in σ, i.e., $\sigma^{-1}(n)$, and position n, and $\big|_{n-1}$ denotes the projection onto the first n-1 positions of the permutation. So, (a) if the last symbol of σ(1,2,…,n) is n, delete n and put the resulting permutation on (1,2,…,n-1) in B, or (b) if the last symbol of σ(1,2,…,n) is not n, exchange n wherever it appears with the last symbol of σ(1,2,…,n), delete the last symbol (which is n after the exchange) and put the resulting permutation on (1,2,…,n-1) in B.

Theorem 2.4: The result of the contraction operation on an invertible permutation array is also an invertible permutation array.

Proof: Let A be an arbitrary invertible set of permutations of length n, i.e., A contains the identity permutation I_n and ∀σ in S_n, $\sigma \in A \Leftrightarrow \sigma^{-1} \in A$. Let B be the resulting set of applying the contraction operation on A. We prove that (1) B contains the identity permutation I_{n-1} and (2) ∀σ' in S_{n-1}, $\sigma' \in B \Leftrightarrow \sigma'^{-1} \in B$.

Indeed, $C(I_n) = I_n\big|_{n-1} = I_{n-1}$. Since $I_n \in A$, $C(I_n) = I_{n-1} \in B$.

To prove (2), we prove that ∀σ in S_n, $C(\sigma)\circ C(\sigma^{-1}) = C(\sigma^{-1})\circ C(\sigma) = I_{n-1}$.

We can simply forget about projection and prove that:

$$(\sigma^{-1}(n)\ n)\circ\sigma\circ(\sigma(n)\ n)\circ\sigma^{-1} = (\sigma(n)\ n)\circ\sigma^{-1}\circ(\sigma^{-1}(n)\ n)\circ\sigma = I_n.$$

Let $\sigma^{-1}(n) = i$ and let $\sigma(n) = a$, i.e., in permutation σ, position i contains symbol n and position n contains symbol a. We have the followings:

$$(i\ n)\circ\sigma\circ(a\ n) = \begin{pmatrix}\cdots & i & \cdots & n\\ & n & & i\end{pmatrix}\circ\begin{pmatrix}\cdots & i & \cdots & n\\ & n & & a\end{pmatrix}\circ\begin{pmatrix}\cdots & a & \cdots & n\\ & n & & a\end{pmatrix} = \begin{pmatrix}\cdots & i & \cdots & n\\ & n & & a\end{pmatrix} = \sigma$$

$$(a\ n)\circ\sigma^{-1}\circ(i\ n) = \begin{pmatrix}\cdots & a & \cdots & n\\ & n & & a\end{pmatrix}\circ\begin{pmatrix}\cdots & a & \cdots & n\\ & n & & i\end{pmatrix}\circ\begin{pmatrix}\cdots & i & \cdots & n\\ & n & & i\end{pmatrix} = \begin{pmatrix}\cdots & a & \cdots & n\\ & n & & i\end{pmatrix} = \sigma^{-1}$$

So, $(i\ n)\circ\sigma\circ(a\ n)\circ\sigma^{-1} = \sigma\circ\sigma^{-1} = I_n$ and $(a\ n)\circ\sigma^{-1}\circ(i\ n)\circ\sigma = \sigma^{-1}\circ\sigma = I_n$. □

Theorem 2.5: For all $n > 1$, and $1 \leq k < n$, $F(n-1,k) \leq F(n,k)$.

The proof can be found in Bein et al. [3]. The idea is to use the contraction operation on an arbitrary t-PA(n,k) and prove that the resulting set is a t-PA(n-1,k).

Conjecture 2.6: For all $n > 1$, and $1 \leq k < n$, $F(n-1,k) < F(n,k)$.

It is intuitive to have $F(n-1,k) < F(n,k)$ over $F(n-1,k) \leq F(n,k)$, just like $F(n,k-1) < F(n,k)$ over $F(n,k-1) \leq F(n,k)$ as we proved in Theorem 2.1. However, since we have not found a proof for $F(n-1,k) < F(n,k)$, it remains a conjecture.

CHAPTER 3

TECHNIQUES TO IMPROVE T-PA

This chapter gives several techniques to obtain transitive permutation arrays of competitive size. We first describe the technique, which we call recursive construction, to construct a new t-PA from two other t-PA's (Fahle's dissertation [27]). We then discuss special cases where we can further remove redundant permutations from the constructed t-PA. New theorems allow us to improve the upper bound of infinitely many entries in the F(n,k) table with very small or even without the computational effort.

3.1 Recursive construction Theorem

The following Theorem can be found in Fahle's dissertation [27]. Due to its importance for our improved Theorems here, its proof is repeated.

Theorem 3.1: $F(n+1,k) \leq F(n,k) + n.F(n,k-1)$

Proof: Let A be a (k-1)-transitive permutation array on I_n and let B be a k-transitive permutation array on I_n. Create a new permutation array D on I_{n+1} by the following two actions:

Action 1: Let σ be a permutation in the set B. Add the symbol n+1 to the end of σ to create a new permutation σ' on I_{n+1} and add σ' into D.

Action 2: Let ϕ be a permutation in the set A. Create a permutation template ϕ' on I_{n+1} by using Action 1. Using ϕ', create a set of n new permutations $\{\phi_i\}$, where for i=1, …, n we create ϕ_i by exchanging the symbol in the i^{th} position of ϕ' with the symbol n+1 (which is in the $(n+1)^{st}$

position). All other symbols are copied without exchanges from ϕ' to the same position in ϕ_i. That is, ϕ' and ϕ_i are identical except in the i^{th} and $(n+1)^{st}$ positions. Add the permutations of $\{\phi_i\}$ into D. Note that the permutation template ϕ' will not be added into D. Figure 3.1 illustrates the recursive construction that we just described.

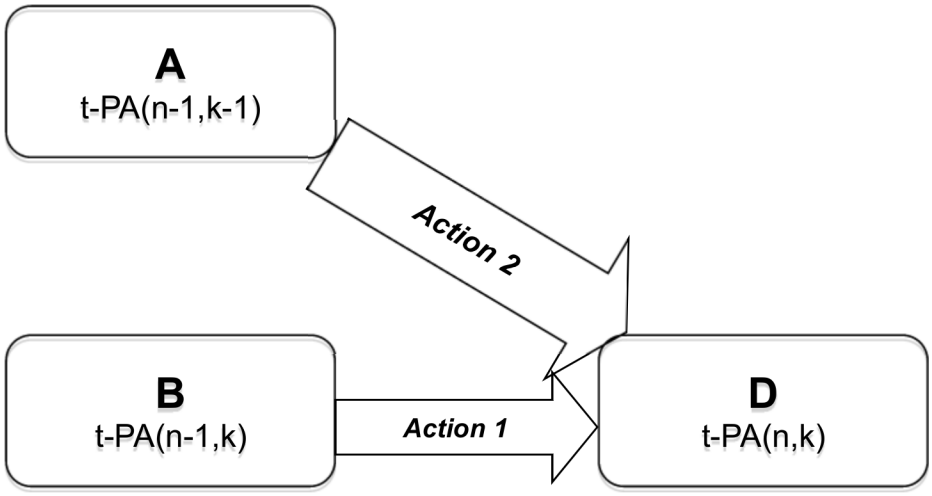

Figure 3.1. Recursive construction

We now show that D is a k-transitive permutation array on I_{n+1}, i.e., a t-PA(n+1,k). For convenience, let $\rho=(p_1,p_2,...,p_k)$ and $\tau=(t_1,t_2,...,t_k)$ be arbitrary k-tuples chosen from I_{n+1}. To show k-transitivity, we want to show that there is a permutation σ in D such that $\sigma(p_i)=t_i$ for all $1 \le i \le k$. Without loss of generality, $p_1 < p_2 < ... < p_k$ because the indices of p_i and t_i can be ordered to make this so. Note that given the passive form permutation $\sigma=(a_1, a_2, ..., a_n)$, if $\sigma(j)=t_i$ for some $j=p_i$ then $a_j=t_i$; that is, the j^{th} position of σ is t_i. There are several cases to be considered.

Case 1: n+1 is not in ρ, nor is n+1 in τ.

Since n+1 is not in either of the k-tuples ρ or τ, they contain only elements of I_n. Since B is k-transitive on I_n, there is a permutation σ in B such that $\sigma(p_i)=t_i$ for all $1 \le i \le k$. The permutation σ' in D is obtained by Action 1 of the recursive process, that is, by adding n+1 to the

end of σ. Since adding an n+1 to the end leaves the other symbols of σ in their original positions, we have $\sigma'(p_i)=t_i$ for all $1 \leq i \leq k$. Thus there is a permutation σ' in D that maps ρ to τ.

Case 2: n+1 is in ρ, but not in τ.

Since n+1 is in ρ and ρ is in order, we have $p_k=n+1$. Consider the (k-1)-tuples $\rho'=(p_1,p_2,...,p_{k-1})$ and $\tau'=(t_1,t_2,...,t_{k-1})$, obtained from ρ and τ, respectively, by deleting the k^{th} coordinate of each. Note that the two (k-1)-tuples ρ' and τ' contain only elements of I_n. Since A is (k-1)-transitive on I_n, there is a permutation ϕ in A that maps each element of ρ' to τ'. Since ϕ is a permutation on I_n, the symbol t_k must be in some position, say i, in ϕ; that is, $\phi(i)=t_k$. Now consider the permutation ϕ_i in the set D created by Action 2 of the recursive process. The permutation ϕ_i is obtained from ϕ by putting n+1 at the end of ϕ, and then exchanging it with the symbol in position i. Action 2 does not affect any other positions, so in ϕ_i, the symbol t_k is in position n+1 as desired, and all elements of ρ' are mapped to τ'. Hence, the permutation ϕ_i in D maps ρ to τ.

Case 3: n+1 is not in ρ, but n+1 is in τ.

Since n+1 is one of the t's in τ, let it be t_j, that is $t_j=n+1$ and let $i=p_j$. Consider the (k-1)-tuples $\rho'=(p_1,p_2,...,p_{j-1},p_{j+1},...,p_k)$ and $\tau'=(t_1,t_2,...,t_{j-1},t_{j+1},...,t_k)$ obtained from ρ and τ, respectively, by deleting the j^{th} coordinate of each. Note that the two (k-1)-tuples ρ' and τ' contain only elements of I_n. Since A is (k-1)-transitive on I_n, there is a permutation ϕ in A that maps each element of ρ' to τ'. Since ϕ is a permutation on I_n, the i^{th} position of ϕ must contain some symbol in I_n but not in τ. Now consider the permutation ϕ_i in the set D created by Action 2 of the recursive process. The permutation ϕ_i is obtained from ϕ by first adding n+1 to the end of ϕ, and

then exchanging it with the symbol in position i. Thus $\phi_i(i)=n+1$, and since Action 2 does not affect any other positions, all elements of ρ' are mapped to τ' in ϕ_i. That is, the permutation ϕ_i in D maps ρ to τ.

Case 4: n+1 is in both ρ and τ, but n+1 is not mapped to itself.

Since n+1 is in ρ and ρ is in order, we have $p_k=n+1$, but $t_k \neq n+1$. However there is some element of τ which is n+1, let it be t_j, and let $i=p_j$. As ρ must be mapped to τ, we must demonstrate a permutation in D that, while doing its construction, specifically has t_j in position $i=p_j$ and t_k in position $n+1=p_k$. Consider the (k-1)-tuple $\rho'=(p_1,p_2,...,p_{k-1})$ obtained by removing p_k from ρ, and the (k-1)-tuple $\tau'=(t_1,t_2,...,t_{j-1},t_k,t_{j+1},...,t_{k-1})$ obtained from τ by first replacing t_j with t_k in τ and then removing the k^{th} coordinate. These two (k-1)-tuples ρ' and τ' contain only elements of I_n. Since A is (k-1)-transitive on I_n, there is a permutation ϕ in A that maps ρ' to τ'. Due to the rearrangement of τ in τ', we have $\phi(i)=t_k$; that is, the i^{th} position of ϕ is t_k. Now consider the permutation ϕ_i in D created by Action 2 of the recursive process. The permutation ϕ_i is obtained from ϕ by first adding n+1 to the end of ϕ, and then exchanging it with the symbol in position i, so that n+1 is in position i and t_k is in position n+1 of ϕ_i. Thus $\phi_i(i)=n+1$ and $\phi_i(n+1)=t_k$, and since Action 2 does not affect any other positions, ϕ_i has the remaining k-2 symbols of τ' in their k-2 respective positions of ρ'. That is, the permutation ϕ_i in D maps ρ to τ.

Case 5: n+1 is in ρ and τ, mapped to itself.

Since n+1 is mapped to n+1, and ρ is in order, we have $p_k=t_k=n+1$. Consider the (k-1)-tuples $\rho'=(p_1,p_2,...,p_{k-1})$ and $\tau'=(t_1,t_2,...,t_{k-1})$ obtained from ρ and τ, respectively, by deleting the k^{th} coordinate of each. These two (k-1)-tuples ρ' and τ' contain only elements of I_n. Since B is k-

transitive on I_n, and hence also (k-1)-transitive, there is a permutation σ in B which maps ρ' to τ'. Now consider the permutation σ' created by Action 1 of the recursive process. The permutation σ' in D is obtained by adding n+1 to the end of σ. So, each position $p_i \in \rho'$ of σ' contains t_i, and the $n+1^{st}$ position of σ' contains n+1 as desired. Thus the permutation σ' in D maps ρ to τ.

All possible cases for the new symbol n+1 have been enumerated, so D is a k-transitive permutation array on I_{n+1}. Such a set D can be created from any t-PA(n,k) and t-PA(n,k-1), so $F(n+1,k) \leq F(n,k) + n.F(n,k-1)$. □

Theorem 3.1 helps obtaining infinitely many new upper bounds for F(n,k). However, when sets A and B have common permutations, set D will have redundant ρ-to-τ mapping, or in other words, set D has potential redundant permutations. In fact, one can modify Theorem 3.1 to obtain a slightly better result as follows:

Theorem 3.2: $F(n+1,k) \leq F(n,k) + n.F(n,k-1) - 1$

Proof: Let A be a (k-1)-transitive permutation array on I_n and let B be a k-transitive permutation array on I_n. Using the Isotopy Theorem, one can assume that A and B have the identity permutation, namely I_n=(1, 2, …, n), in common. Therefore, in the recursive construction of D from A and B, one can exclude I_n from B in performing Action 1, and obtain the result in Theorem 3.2. Looking at the proof of Theorem 3.1, we observe that there are two cases where a permutation in the set B is used in the proof that D is k-transitive, namely case 1 and case 5.

In case 1, I_n in B is not needed, because for any mapping from a k-tuple of positions $\rho=(p_1,p_2,\ldots,p_k)$ to a k-tuple of symbols $\tau=(p_1,p_2,\ldots,p_k)$ that I_n in B covers, the duplicate of I_n in A will also map ρ to τ. Furthermore, Action 2 applied on I_n in A in the recursive construction of D

makes a new permutation in D that maps ρ to τ, because the symbol n+1 is exchanged with every position, including those that are not part of the k-tuple, hence leaving the k-tuple intact.

In case 5, I_n in B is not needed, because for any mapping from a (k-1)-tuple of positions $\rho'=(p_1,p_2,\ldots,p_{k-1})$ to a (k-1)-tuple of symbols $\tau'=(p_1,p_2,\ldots,p_{k-1})$ that I_n in B covers, there is a permutation in $B\backslash\{I_n\}$ that also maps ρ' to τ'. This is true, because similar to the proof of Theorem 2.1, consider a pair of k-tuples $\rho''=(p_1,p_2,\ldots,p_{k-1},p'_k)$ and $\tau''=(p_1,p_2,\ldots,p_{k-1},t'_k)$ where $p'_k \neq t'_k$, because B is a t-PA(n,k), there is a permutation σ in B that maps ρ'' to τ''. And this permutation σ is not the identity permutation, because $p'_k \neq t'_k$. So, the permutation σ' created by applying Action 1 of the recursive process on σ will map ρ to τ as desired.

It follows that F(n+1,k) is at least one (1) less than F(n,k) + n.F(n,k-1). □

In reality, after using the recursive construction to create a new permutation array, the program of Fahle [28] is almost always able to remove a significant number of redundant permutations. For example, F(6,4)=360 (from alternating sharp group) and F(6,3)=120 (from sharply 3-transitive group). By Theorem 3.1, $F(7,4) \leq 360 + 6*120 = 1080$. Fahle's program removed 60 redundant permutations, so $F(7,4) \leq 1020$.

We can mathematically prove the following Proposition:

Proposition 3.3: $F(7,4) \leq 1020$

Proof: Let A be a sharply 3-transitive group of permutations of length 6 (F(6,3) = 120) and let B be the sharp alternating group of permutations of length 6 (F(6,4) = 360). A has 60 odd permutations and 60 even permutations. All these even permutations will also be in B, the set of all even permutations of length 6. Let S be the mentioned common set and let S_A, S_B be the copies of S in A and B, respectively. We will prove that in the recursive construction of D, a t-

PA(7,4), from A and B, one can exclude S_B from Action 1. Equivalently, we will show that all ρ-to-τ mappings covered by the resulting permutations of applying Action 1 on these 60 even permutations will be covered by other permutations in D. Let $\rho = (p_1,p_2,p_3,p_4)$ and $\tau = (t_1,t_2,t_3,t_4)$ be two arbitrary 4-tuples chosen from I_7. Similar to the proof of Theorem 3.2, we consider only case 1 and case 5 in proving 4-transitivity of D.

In case 1, we see that a permutation in S_B is not needed, because if, for any pair of 4-tuples ρ and τ, a permutation π in S_B is used to map ρ to τ, the duplicate permutation of π in S_A also maps ρ to τ. Furthermore, Action 2 applied on the copy of π in S_A in the recursive construction of D makes a new permutation in D that maps ρ to τ, because the symbol 7 is exchanged with every position, including those that are not part of the 4-tuple, hence leaving the 4-tuple intact.

In case 5, since position 7 is mapped to symbol 7, and ρ is in order, we have $p_4 = t_4 = 7$. Let $\rho'=(p_1,p_2,p_3)$ and $\tau'=(t_1,t_2,t_3)$ obtained from ρ and τ, respectively, by deleting the 4^{th} coordinate of each. Let σ be the even permutation in S_B that maps ρ' to τ'. Let σ' be a permutation obtained from σ by performing a cyclic shift of the 3 remaining positions that are not in ρ'. Because the length of the cycle is 3, an odd integer, there are 3-1=2 distinct σ' that are different than σ and both of them are even permutations. Therefore, σ' is in B. However, since σ' also maps ρ' to τ' and since A is a sharp t-PA(6,3), σ' is not in A, and hence σ' is not in S, nor is σ' in S_B. It follows that the resulting permutation of applying Action 1 on σ' in $B\backslash S_B$ will map ρ to τ as desired.

One can plug in the numbers to obtain the upper bound of $F(7,4) \leq F(6,4) + 6*F(6,3) - |S| = 360 + 6*120 - 60 = 1020$. □

The program of Fahle [28] is powerful, but its computational limitation is obvious. The largest set that we used as an input to the program was a t-PA(10,7) of size almost one million. This leads to an urge for techniques to improve the recursive construction by considering the set of duplicate permutations between set A and set B.

3.2 Recursive construction – Contraction special case

Theorem 3.4: Let C be a sharp t-PA(n,k-1). Let A be a t-PA(n-1,k-1) obtained from C by the operation of contraction, and let B be a t-PA(n-1,k). Let D be a t-PA(n,k) obtained by the recursive construction from A and B. Then $F(n+1,k) \leq F(n,k) + ((n-1)+1/n).F(n,k-1)$.

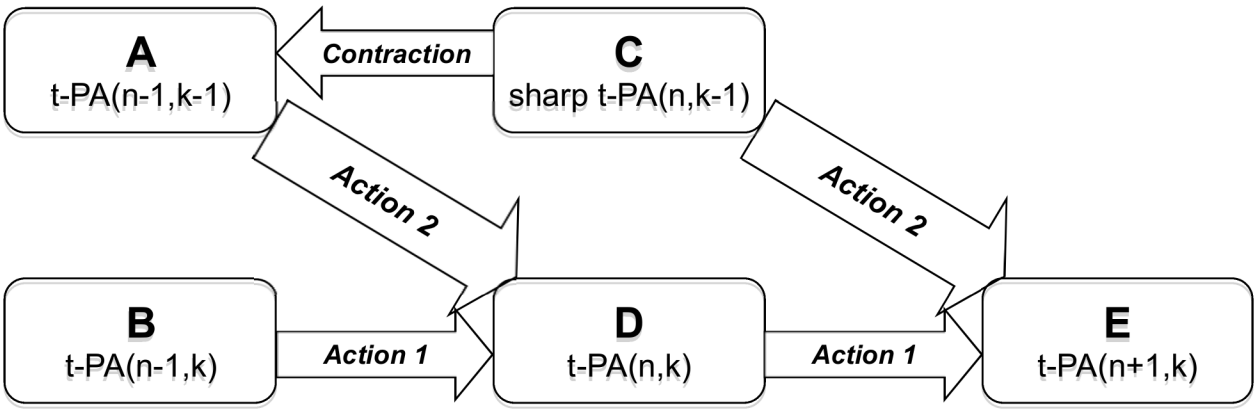

Figure 3.2. Recursive construction – Contraction special case

Proof: (See Figure 3.2) Since C is sharp, $|C|=F(n,k-1)$ and there are exactly $((n-1)/n).F(n,k-1)$ permutations π in C in which the last symbol of $\pi(1,2,\ldots,n)$ is not the symbol n. The contraction operation (defined in the proof of Theorem 2.3) changes all such permutations π by replacing the symbol n, wherever it occurs, by the last symbol of $\pi(1,2,\ldots,n)$. All of these permutations occur in A. In creating D by the recursive procedure from A and B, Action 2 (described in the proof of Theorem 2.1) does the opposite of the contraction: it adds the symbol n to the end of each

permutation ϕ in A, and then exchanges it with the symbol in each position of ϕ. Action 2, therefore, re-creates all of the permutations in C in which the last symbol is not n, and puts them into D. So, C and D have ((n-1)/n).F(n,k-1) permutations in common. Let S_C and S_D be the copies of this set of common permutations in C and D, respectively.

Now, consider the use of C and D in a recursive construction of a t-PA(n+1,k) called E. Looking at the proof of Theorem 3.1 we observe that there are two cases where permutations in the set D are used in the proof that E is k-transitive, namely case 1 and case 5.

In case 1, we see that S_D is not needed, because if, for any pair of k-tuples ρ and τ, a permutation π in S_D is used to map ρ to τ, the duplicate permutation of π in S_C also maps ρ to τ. Furthermore, Action 2 applied on the copy of π in C in the recursive construction of E makes a new permutation in E that maps ρ to τ, because the symbol n+1 is exchanged with every position, including those that are not part of the k-tuple, hence leaving the k-tuple intact.

In case 5, we see that S_D is not needed, because, for every pair of (k-1)-tuples ρ' and τ', where a permutation π in S_D maps ρ' to τ', there is a permutation in $D \backslash S_D$ that also maps ρ' to τ'. This is true, because each permutation in S_D is also in C, which is a sharp t-PA(n,k-1), so π is a unique permutation in C that maps ρ' to τ'. However, D is a t-PA(n,k), so for any k^{th} component added to the (k-1)-tuples ρ' and τ', to get k-tuples, ρ and τ, there must be a permutation in D that maps ρ to τ. Each of these permutations in D also maps ρ' to τ', but only one is in C. So, the removal of a permutation π in S_D from D leaves other permutations to map ρ' to τ'.

Thus, we can eliminate the set S_D when doing the recursive construction of E, and E will still be k-transitive. Since S_D has ((n-1)/n).F(n,k-1) permutations, one subtracts this number from the former bound, namely F(n,k) + n.F(n,k-1), to obtain the result. □

Table 3.1. New F(n,k) bounds

F(n, k)		*n=5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*
k=1	ALL	5	6	7	8	9	10	11	12
2	LB	20	**33**	42	56	72	91	110	132
	UB	20	**37**	42	56	72	110	110	156
	PUB	20	37	42	56	72	110	110	156
3	LB	60	120	231	336	504	720	1001	1320
	UB	60	**120**	336	336	504	720	1320	1320
	PUB	60	120	336	336	504	720	1320	1320
4	LB	120	360	841	1848	3025	5041	7920	11880
	UB	120	360	**1020**	**3251**	**5700**	7920	7920	**22438**
	PUB	120	360	1020	3265	5911	7920	7920	22440
5	LB		720	2520	6728	16632	30250	55451	95040
	UB		720	2520	**9060**	**33984**	**83938**	95040	95040
	PUB		720	2520	9240	34502	86883	95040	95040
6	LB			5040	20160	60522	166320	332750	665412
	UB			5040	20160	**88200**	**382257**	**1193589**	**2239029**
	PUB			5040	20160	91714	389091	1257921	2303361
7	LB				40320	181440	605220	1829520	3993000
	UB				40320	181440	**945885**	**4715193**	**17546353**
	PUB				40320	181440	985306	4876216	18713347
8	LB					362880	1814400	6660720	21954240
	UB					363880	1814400	**11184630**	**62488125**
	PUB					362880	1814400	11667460	65305836
9	LB						3628800	19958400	79928640
	UB						3628800	19958400	**142120815**
	PUB						3628800	19958400	148300460
10	ALL							39916800	239500800

As an example of Theorem 3.4, consider obtaining an upper bound for F(9,4). By the recursive construction, using the upper bounds for F(8,3) and F(8,4), as shown in Table 3.1, one obtains the result 5939=8*336+3251. However, as F(8,3) is sharp and the t-PA(7,3) used for

F(7,3) is obtained by contraction, Theorem 3.4 applies. In this case, we have 5766=3372+7*336+(1/8)*336. The bound of 5700 shown in Table 3.1 for F(9,4) is due to our computational effort that identified 66 redundant permutations. Also, note that we used the bound of 3372=1020+7*336 for F(8,4), although Table 3.1 gives an upper bound of 3251. This is because Theorem 3.4 requires that the t-PA(8,4) set be obtained by the recursive procedure. In a similar way, for infinitely many n, when F(n,2) and F(n,3) are optimum, due to the existence of sharply 2-transitive or 3-transitive groups, the best upper bounds for F(n-1,2) and F(n-1,3), respectively, are obtained by the contraction operation. In all of these cases, Theorem 3.4 can be used to get better upper bounds.

3.3 Recursive construction – Third diagonal special case

Theorem 3.5: (See Figure 3.3) Let A be a t-PA(n,n-3). Let B be a sharp t-PA(n,n-2), and let E be a sharp t-PA(n+1,n-1). Let S be B.(n+1), the set of all permutations formed by putting symbol (n+1) at the end of each permutation in B. Let D be a t-PA(n+1,n-2) such that S is a subset of D (such a D set can be obtained by the recursive construction from A and B). Then, $F(n+2,n-1) \leq F(n+1,n-1) + (n+1).F(n+1,n-2) – F(n,n-2) + F(n,n-3)$.

Proof: S was given to be a subset of D. S is also a subset of E because all even permutations in B followed by a fixed point of symbol n+1 in the $n+1^{st}$ position are even as well. Let S_D and S_E be the copies of subset S in D and E, respectively. We will show that, in the recursive construction of a t-PA(n+2,n-1) called F, from D and E, one can replace the subset $B.(n+1)=S_E$ with the set A.(n+1) in E.

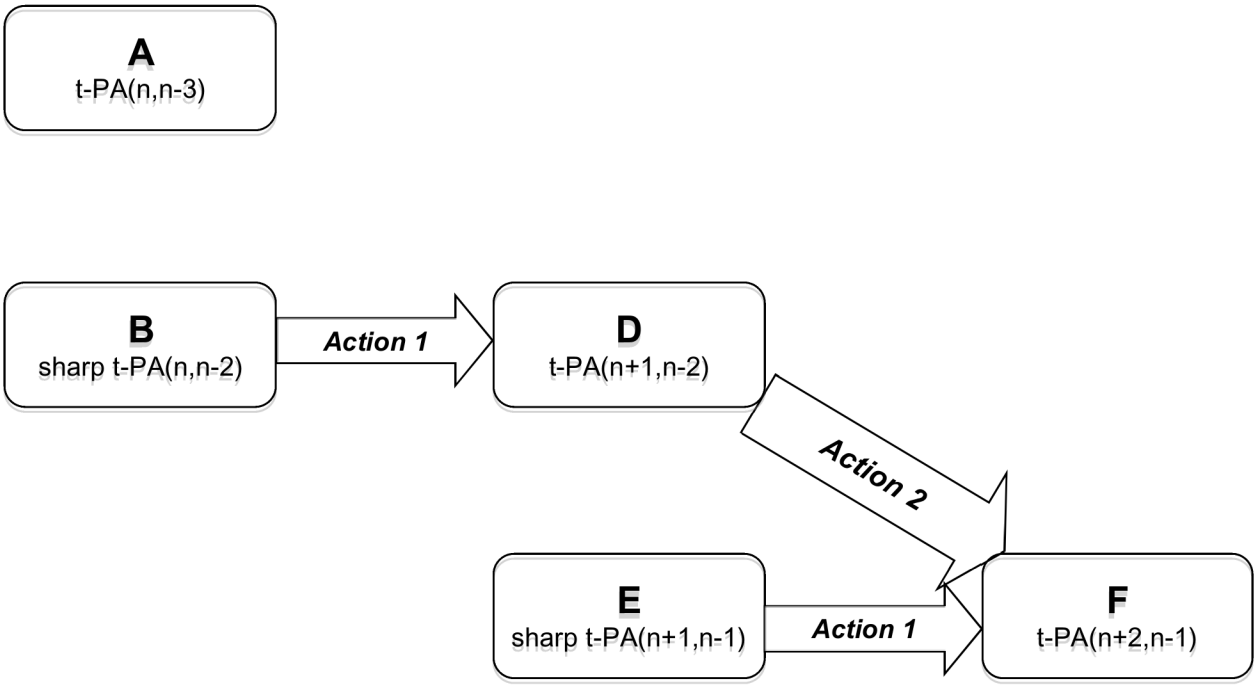

Figure 3.3. Recursive construction – Third diagonal special case

Let $\rho=(p_1, p_2, \ldots, p_{n-2}, p_{n-1})$ and $\tau = (t_1, t_2, \ldots, t_{n-2}, t_{n-1})$ be arbitrary (n-1)-tuples chosen from I_{n+2}. To show (n-1)-transitivity, we want to show that there is a permutation σ in F such that $\sigma(p_i)=t_i$ for all $1 \leq i \leq n-1$. The proof is similar to that of Theorem 3.1, except that, for the sake of brevity, here we only consider the two cases, namely case 1 and case 5, where we need a permutation in S_E for the construction of F. We will show that these two cases will instead be covered by a different permutation that is not in S_E.

Case 1: n+2 is not in ρ, nor is n+2 in τ

If there is a permutation π in S_E that maps ρ to τ, there is a duplicate in S_D that also maps ρ to τ. When applying Action 2 of the recursive process to this permutation π in S_D, there exists a position j not in ρ such that exchanging the symbol in the j^{th} position of π' with the symbol n+2

(which is in the $n+2^{nd}$ position) leaves the k-tuples ρ and τ intact, therefore $\pi_j(p_i)=t_i$ for all $1 \leq i \leq n-1$. That is, the permutation π_j in F maps ρ to τ.

Case 5: n+2 is in ρ and τ, mapped to itself

Since n+2 is mapped to n+2, and ρ is in order, we have $p_{n-1}=t_{n-1}=n+2$.

Sub case 5a: n+1 is not in ρ, nor is n+1 in τ

Consider the (n-2)-tuples $\rho' = (p_1, p_2, \ldots, p_{n-2})$ and $\tau' = (t_1, t_2, \ldots, t_{n-2})$ obtained from ρ and τ, respectively, by deleting the last coordinate of each. Because $n-2 < n$, there exists a position j not in ρ' such that $j \leq n$ (there are two of them, actually). Let $\rho'' = (p_1, p_2, \ldots, p_x = j, \ldots, p_{n-2})$ and $\tau'' = (t_1, t_2, \ldots, t_x = n+1, \ldots, t_{n-2})$ be (n-1)-tuples obtained from ρ' and τ', respectively, by adding the x^{th} coordinate to each such that the extra mapping (the x^{th} component) will be from position j to symbol n+1. Note that the two (n-1)-tuples ρ' and τ' contain only elements of I_{n+1}. Since E is a (n-1)-transitive set on I_{n+1}, there exists a permutation π in E that maps ρ'' to τ'', hence maps ρ' to τ'. This permutation is not in S_E because it doesn't have a fixed point of symbol n+1. The permutation π' in F is obtained by Action 1 of the recursive process, that is, by adding n+2 to the end of π. Since this action leaves the other symbols of π in their original positions, for each $1 \leq i \leq n-1$, we have $\pi'(p_i)=t_i$. Thus there is a permutation π' in F that maps ρ to τ.

Sub case 5b: n+1 is in ρ and τ, mapped to itself

Since n+1 is mapped to n+1, and ρ is in order, we have $p_{n-2}=t_{n-2}=n+1$. Consider the (n-3)-tuples $\rho' = (p_1, p_2, \ldots, p_{n-3})$ and $\tau' = (t_1, t_2, \ldots, t_{n-3})$ obtained from ρ and τ, respectively, by deleting the last two coordinates of each. These two (n-3)-tuples ρ' and τ' contain only elements

of I_n. Since A is (n-3)-transitive on I_n, there is a permutation π in A that maps ρ' to τ'. The permutation π' in F is obtained by applying Action 1 of the recursive process twice, that is, by adding n+1 then n+2 to the end of π. Since this action leaves the other symbols of π in their original positions, for each $1 \leq i \leq n-1$, we have $\pi'(p_i)=t_i$. Thus there is a permutation π' in F that maps ρ to τ.

Since any permutation in S_E has a fixed point of symbol n+1, we have enumerated all possible cases where we need a permutation in S_E for the construction of F. Therefore, we can replace the set S_E with the set A.(n+1) in E when doing the recursive construction of F, and F will still be (n-1)-transitive. Since S_E has F(n,n-2) and A has F(n,n-3) permutations, one plugs these numbers into the former bound, namely F(n+1,n-1) + (n+1).F(n+1,n-2), to obtain the result.

□

Application of Theorem 3.5 on the 3rd (from the bottom) diagonal: (See Figure 3.4)

After the new construction, the set F does not contain the whole subset E.(n+2) as in the original recursive construction. Instead, F will contain T = E.(n+2) \ B.(n+1).(n+2). This subset T is also a subset of G because the fixed point of symbol n+2 in the n+2nd position does not affect the evenness of those permutations. Now using the same argument to construct a n-transitive set, called H, of permutations of length (n+3) from F and G, one can replace the set of duplicates T_G in G by D.(n+2). Therefore, the contribution of G to the construction of H will be changed into:

G.(n+3) \ T.(n+3) U D.(n+2).(n+3)

= G.(n+3) \ E.(n+2).(n+3) U B.(n+1).(n+2).(n+3) U D.(n+2).(n+3)

= G.(n+3) \ E.(n+2).(n+3) U D.(n+2).(n+3) (because B.(n+1) is a subset of D)

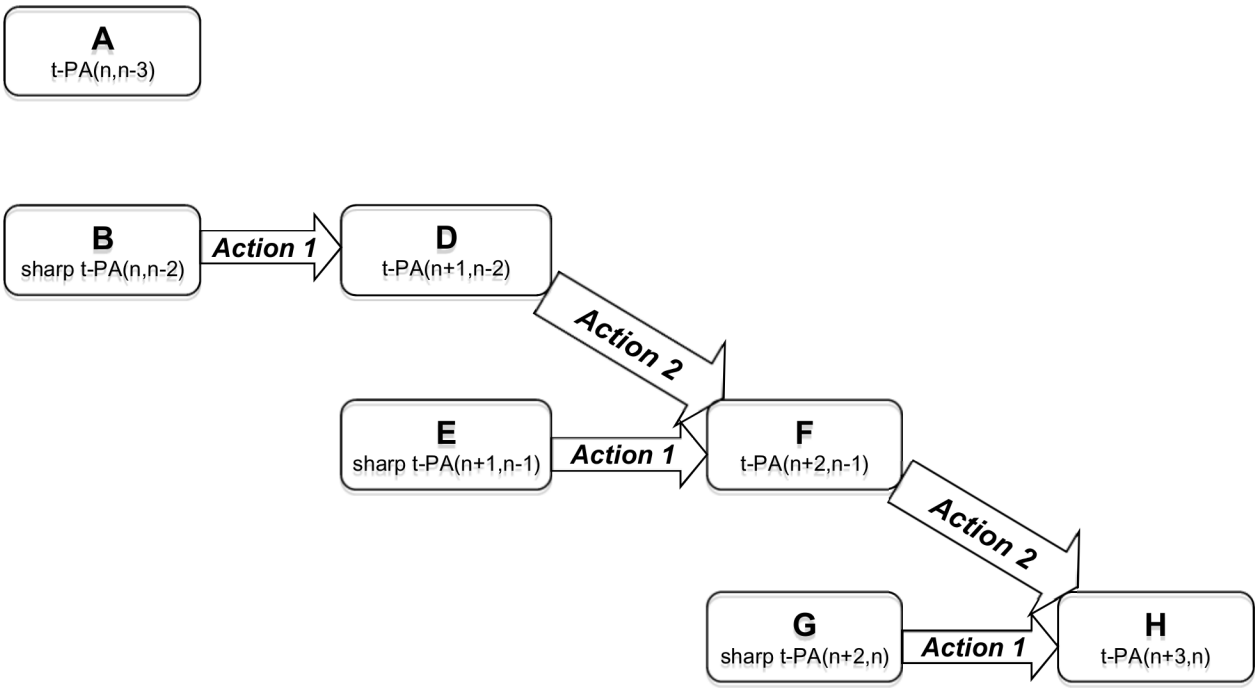

Figure 3.4. Application of Theorem 3.5 on the 3rd (from the bottom) diagonal

Therefore, $F(n+3,n) \leq F(n+2,n) + (n+2).F(n+2,n-1) - F(n+1,n-1) + F(n+1,n-2)$, which is exactly the same as applying directly Theorem 3.5. It means that Theorem 3.5 can be applied anywhere down the 3rd diagonal without having to worry that the previous permutation array has some permutations removed. The condition to use Theorem 3.5 is changed from B.(n+1) is a subset of D into (B\A).(n+1) is a subset of D. We did not take into account the intersection between A and B, that was why we needed the whole set B.(n+1) (or set S as denoted in the theorem) to be a subset of D.

Theorem 3.6 (Theorem 3.5 revised): Let A be a t-PA(n,n-3). Let B be a sharp t-PA(n,n-2), and let E be a sharp t-PA(n+1,n-1). Let S be (B\A).(n+1), the set of all permutations formed by putting symbol (n+1) at the end of each permutation in B but not in A. Let D be a t-PA(n+1,n-2) such that S is a subset of D (such a D set can be obtained by the recursive construction from A

and B, or by the construction in the proof of this theorem). Then, $F(n+2,n-1) \leq F(n+1,n-1) + (n+1).F(n+1,n-2) - F(n,n-2) + F(n,n-3)$.

Proof: The proof for (n-1)-transitivity of the set F is exactly the same as what we showed in Theorem 3.5 because the set S in this revised theorem is just a subset of the set S in Theorem 3.5. The only difference is when we plug in the numbers. The contribution of E to the construction of F will be changed into:

$E.(n+2) \setminus (B\setminus A).(n+1).(n+2) \cup A.(n+1).(n+2)$

$= E.(n+2) \setminus B.(n+1).(n+2) \cup (B\cap A).(n+1).(n+2) \cup A.(n+1).(n+2)$

$= E.(n+2) \setminus B.(n+1).(n+2) \cup A.(n+1).(n+2)$ (because $B\cap A$ is a subset of A)

This new contribution yields the desired result. □

It is straightforward to see that the new condition in Theorem 3.6 holds if we apply the Theorem along the 3rd diagonal because in the construction of any new set F from sets D and E, we remove only the permutations that are duplicates between D and E. If we use any program (like the one of Fahle [28]) or technique to further remove some redundant permutations from the set F and if those redundant permutations are from the duplicate set of D and E, we still can apply Theorem 3.6 for the next entry of the 3rd diagonal. For example, from Proposition 3.3, $F(7,4) \leq 1020$ after removing 60 permutations, all are duplicates between t-PA(6,3) and t-PA(6,4), with 7 put at the end. So Theorem 3.6 applies and $F(8,5) \leq F(7,5)+7*F(7,4) - F(6,4)+F(6,3) \leq 2520+7*1020-360+120 = 9420$. Then, Fahle's program [28] removed 360 permutations from this t-PA(8,5) of 9420 permutations to obtain the new upper bound of $F(8,5) \leq 9060$. Because all 360 removed permutations are duplicates between t-PA(7,4) and t-PA(7,5), with 8 put at the end, we apply Theorem 3.6 again to get $F(9,6) \leq F(8,6)+8*F(8,5)-F(7,5)+F(7,4)$

≤ 20160+8*9060-2520+1020 = 91140. Now, Fahle's program [28] removed 2940 permutations to make a new upper bound of F(9,6) ≤ 88200. However, 420 of those removed permutations are in t-PA(8,6) only, not in t-PA(8,5), with 9 put at the end. So F(10,7) ≤ F(9,7)+9*F(9,6)-F(8,6)+F(8,5)+420 ≤ 181,440+9*88200-20160+9060+420 = 964,560. Here, when applying Theorem 3.6, we have to put back 420 permutations into our calculation. The current upper bound for F(10,7) is 945,885, obtained by using Theorem 3.6 combined with Fahle's program [28].

Moving to the next entry of the 3rd diagonal, F(11,8) ≤ F(10,8)+10*F(10,7)-F(9,7)+F(9,6)+4620 ≤ 1,814,400+10*945,885-181,440+88200+4620 = 11,184,630. Again, 4620 permutations are put back into our calculation because they are in t-PA(9,7) but not in t-PA(9,6) with 10 put at the end of each permutation. As discussed at the end of Section 3.1, more than 11 million permutations of a t-PA(11,8) cannot fit as an input to Fahle's program [28]. As a result, all other entries of the 3rd diagonal, starting from F(12,9), are obtained by a direct application of Theorem 3.6, namely F(12,9) ≤ F(11,9)+11*F(11,8)-F(10,8)+F(10,7) ≤ 19,958,400+11*11,184,630-1,814,400+945,885 = 142,120,815 and so on.

3.4 Two stages of the recursive construction

Theorem 3.7 (Two-stage Theorem): (See Figure 3.5) Let A be a t-PA(n,k-1), let B be a t-PA(n,k), and let C be a t-PA(n,k+1). Let S be B.(n+1), the set of all permutations formed by putting symbol (n+1) at the end of each permutation in B. Let D be a t-PA(n+1,k) such that S is a subset of D (such a D set can be obtained by the recursive construction from A and B). Let E be a t-PA(n+1,k+1) obtained by the recursive construction from B and C. Then F(n+2,k+1) ≤ F(n+1,k+1) + (n+1).F(n+1,k) – F(n,k) + F(n,k-1).

Proof:

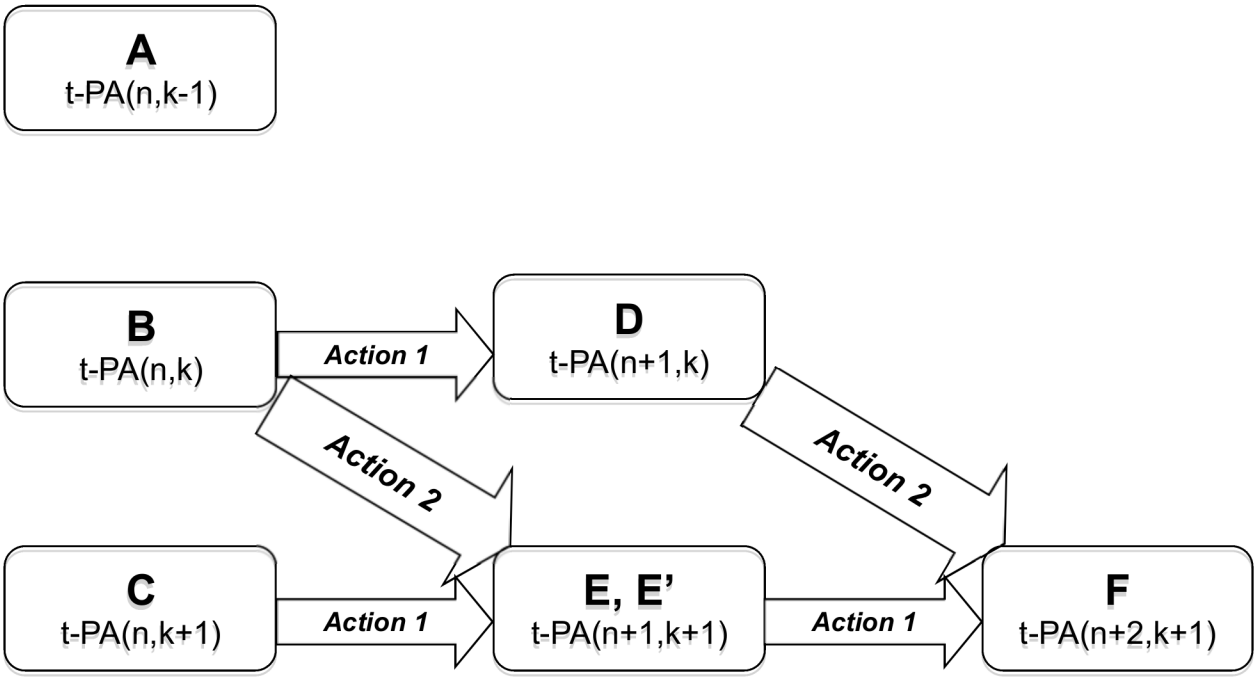

Figure 3.5. Two stages of the recursive construction

Because E is obtained by the recursive construction from B and C, E contains the subset $\{B.(n+1)\}_n$ where $\{B.(n+1)\}_n$ is obtained from B.(n+1) by exchanging the symbol in the n^{th} position with the symbol n+1 (which is in the $n+1^{st}$ position). Let E' be the set obtained by exchanging the last two positions (positions n and n+1) of all permutations in E. E' will receive B.(n+1) as a subset and since E' is in the same isotopy class with E, E' is also a t-PA(n+1,k+1).

Now we have S as a common subset of D and E'. Let S_D and $S_{E'}$ be the copies of subset S in D and E', respectively. Similarly to the Theorem 3.5, we can show that, in the recursive construction of a t-PA(n+2,k+1) called F, from D and E', one can replace the subset $B.(n+1)=S_{E'}$ with the set A.(n+1) in E', therefore obtain the result $F(n+2,k+1) \leq F(n+1,k+1) + (n+1).F(n+1,k) - F(n,k) + F(n,k-1)$. □

Application of Theorem 3.7 in the F(n,k) table: (See Figure 3.6)

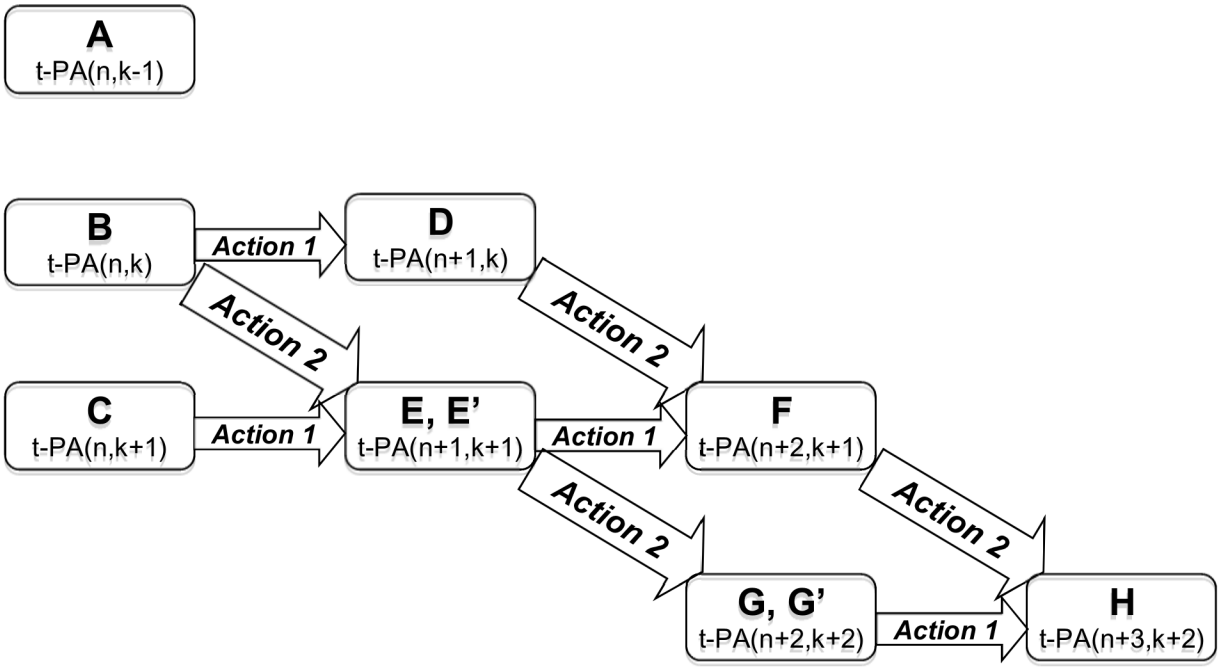

Figure 3.6. Application of Theorem 3.7 in the F(n,k) table

After the new construction, the set F does not contain the whole subset E'.(n+2) as in the original recursive construction. Instead, F will contain T = E'.(n+2) \ B.(n+1).(n+2). Let G be t-PA(n+2,k+2) obtained by the recursive construction from E' and some t-PA(n+1,k+2). Since G' is obtained from G by exchanging the last two positions, namely positions n+1 and n+2, G' contains E'.(n+2), therefore G' also contains T. Now using the same argument to construct a (k+2)-transitive set, called H, of permutations of length (n+3) from F and G', one can replace the set of duplicates $T_{G'}$ in G' by D.(n+2). Therefore, the contribution of G' to the construction of H will be changed into:

G'.(n+3) \ T.(n+3) U D.(n+2).(n+3)

= G'.(n+3) \ E'.(n+2).(n+3) U B.(n+1).(n+2).(n+3) U D.(n+2).(n+3)

= G'.(n+3) \ E'.(n+2).(n+3) U D.(n+2).(n+3) (because B.(n+1) is a subset of D)

Therefore, $F(n+3,k+2) \leq F(n+2,k+2) + (n+2).F(n+2,k+1) - F(n+1,k+1) + F(n+1,k)$, which is exactly the same as applying directly Theorem 3.7. It means that Theorem 3.7 can be applied anywhere in the F(n,k) table without having to worry that the previous permutation array has some permutations removed. The condition to use Theorem 3.7 is changed from B.(n+1) is a subset of D into (B\A).(n+1) is a subset of D. We did not take into account the intersection between A and B, that was why we needed the whole set B.(n+1) (or set S as denoted in the theorem) to be a subset of D.

Theorem 3.8 (Theorem 3.7 revised): Let A be a t-PA(n,k-1), let B be a t-PA(n,k), and let C be a t-PA(n,k+1). Let S be (B\A).(n+1), the set of all permutations formed by putting symbol (n+1) at the end of each permutation in B but not in A. Let D be a t-PA(n+1,k) such that S is a subset of D (such a D set can be obtained by the recursive construction from A and B, or by the construction in the proof of this theorem). Let E be a t-PA(n+1,k+1) obtained by the recursive construction from B and C. Then $F(n+2,k+1) \leq F(n+1,k+1) + (n+1).F(n+1,k) - F(n,k) + F(n,k-1)$.

Proof:

The proof for (k+1)-transitivity of the set F is exactly the same as what we showed in Theorem 3.7 because the set S in this revised theorem is just a subset of the set S in Theorem 3.7. The only difference is when we plug in the numbers. The contribution of E' to the construction of F will be changed into:

E'.(n+2) \ (B\A).(n+1).(n+2) U A.(n+1).(n+2)

= E'.(n+2) \ B.(n+1).(n+2) U (B∩A).(n+1).(n+2) U A.(n+1).(n+2)

= E'.(n+2) \ B.(n+1).(n+2) U A.(n+1).(n+2) (because B∩A is a subset of A)

This new contribution yields the desired result. □

Similar to the application of Theorem 3.6, if we use any program (like the one of Fahle [28]) or technique to further remove some redundant permutations from the set F that are in E' but not in D, in the recursive construction of set H from set F and G' as shown in Figure 3.6, we have to put back those permutations in our calculation. Table 3.2 shows how we used Theorem 3.8 and Fahle's program [28] to obtain new upper bounds for F(n,k), where column 5 contains the number of permutations to put back in the calculation as mentioned above and column 6 contains the number of redundant permutations that Fahle's program [28] removed after the recursive construction.

Table 3.2. Detailed calculations of some new upper bounds of F(n,k)

F(n+1,k+1)	F(n+1,k)	F(n,k)	F(n,k-1)			F(n+2,k+1)
F(7,4) ≤ 1020	F(7,3) ≤ 337	F(6,3) = 120	F(6,2) ≤ 37	0 (5)	45	F(8,4) ≤ 1020+7*337-120+37-45 = 3251
F(8,5) ≤ 9060	F(8,4) ≤ 3251	F(7,4) ≤ 1020	F(7,3) ≤ 337	0 (45)	401	F(9,5) ≤ 9060+8*3251-1020+337-401 = 33984
F(9,6) ≤ 88200	F(9,5) ≤ 33984	F(8,5) ≤ 9060	F(8,4) ≤ 3251	60 (401)	6050	F(10,6) ≤ 88200+9*33984-9060+3251+60-6050 = 382,257
F(10,7) ≤ 945885	F(10,6) ≤ 382257	F(9,6) ≤ 88200	F(9,5) ≤ 33984	954 (6050)	0	F(11,7) ≤ 945885+10*382257-88200+33984+954 = 4,715,193
F(11,8) ≤ 11184630	F(11,7) ≤ 4715193	F(10,7) ≤ 945885	F(10,6) ≤ 382257	0 (0)	0	F(12,8) ≤ 11184630+11*4715193-945885+382257 = 62,488,125
F(10,6) ≤ 382257	F(10,5) ≤ 83938	F(9,5) ≤ 33984	F(9,4) ≤ 5700	236 (1346)	0	F(11,6) ≤ 382257+10*83938-33984+5700+236 = 1,193,589

Our latest upper bounds for F(n,k) were summarized in Table 3.1 on page 29, where bold entries are new and improved bounds. Note that, in Table 3.2, we used the bound of 337 for F(7,3), although Table 3.1 shows an upper bound of 336, obtained by a contraction operation on a sharp t-PA(8,3). This is because Theorem 3.8 requires that the t-PA(7,3) be obtained by the

recursive procedure and 337 = 120+6*37-5. We used Fahle's program [28] to remove 5 redundant permutations from the constructed t-PA(7,3). All of them were from both the used t-PA(6,3) and t-PA(6,2), with 7 put at the end of each permutation.

3.5 Three stages or more of the recursive construction

As shown in the proof of Theorem 3.8, we can apply the Two-stage Theorem anywhere in the F(n,k) table without having to worry that the permutations which were removed by the previous construction may affect the later construction. This ability can be considered as a three-stage, or more-than-three-stage construction as shown in Figure 3.6, or in its generalized version, respectively. Theorem 3.8 also showed that, as long as the condition of the Theorem is satisfied, we can use the Theorem with the best known upper bounds of all four quantities on the right hand side. This is very important, especially with the second quantity of F(n+1,k) that comes with an asymptotic factor of O(n). A possible three-or-more stage recursive construction must take this ability into account in order to yield competitive results.

CHAPTER 4

TECHNIQUES TO IMPROVE C-PA

In this chapter, we first give a formal definition of the polymorphic hamming distance function and prove some basic properties of the function. We then prove that the result of the contraction operation on a c-PA(n,d) is a c-PA(n-1,d-3). We also discuss cases when a c-PA(n-1,d-2) is obtained instead. We prove some theorems that allow us to use groups and their cosets to construct a c-PA(n,d). A random algorithm to search for cosets of a group to construct competitive code permutation arrays is described. Finally, we consider frequency permutation arrays and discuss their usage as templates to construct new code permutation arrays.

4.1 The polymorphic hamming distance function

Two permutations π and $\sigma \in S_n$ have (hamming) distance d, denoted as DIST(π,σ)=d if $\pi\sigma^{-1}$ has exactly n-d fixed points. In other words, two permutations have hamming distance d if they differ in d positions. We define our polymorphic hamming distance function as follows:

$$\text{DIST}(\pi,\sigma) = \text{count}\{1 \le i \le n \mid \pi(i) \ne \sigma(i)\}$$

$$\text{DIST}(A) = \min\{\text{DIST}(\pi,\sigma) \mid \pi \in A, \sigma \in A, \pi \ne \sigma\}$$

$$\text{DIST}(A,\sigma) = \min\{\text{DIST}(\pi,\sigma) \mid \pi \in A\}$$

$$\text{DIST}(A,B) = \min\{\text{DIST}(\pi,\sigma) \mid \pi \in A, \sigma \in B\}$$

where π and σ are permutations and A and B are sets of permutations. So a set A of permutations of length n is a c-PA(n,d) if and only if DIST(A) $\ge$ d.

Proposition 4.1:

a. $DIST(\mu\circ\pi,\mu\circ\sigma) = DIST(\pi\circ\mu,\sigma\circ\mu) = DIST(\pi,\sigma)$

b. $DIST(\mu\circ A) = DIST(A\circ\mu) = DIST(A)$

c. $DIST(\mu\circ A,\mu\circ B) = DIST(A\circ\mu,B\circ\mu) = DIST(A,B)$

d. $DIST(A \cup B) = \min\{DIST(A), DIST(B), DIST(A,B)\}$

e. $DIST(\bigcup_{i=1}^{k} A_i) = \min\{\min\{DIST(A_i) \mid 1 \le i \le k\}, \min\{DIST(A_i,A_j) \mid 1 \le i < j \le k\}\}$

where $\mu\circ A$ is the set formed by the composition of the permutation μ and each element of set A and $A\circ\mu$ is the set formed by the composition of each element of set A and the permutation μ.

Proof: For part (a), $DIST(\mu\circ\pi,\mu\circ\sigma) = count\{1 \le i \le n \mid \mu(\pi(i)) \ne \mu(\sigma(i))\}$. Since μ is a permutation, $\mu(\pi(i)) \ne \mu(\sigma(i)) \Leftrightarrow \pi(i) \ne \sigma(i)\ \forall i \in I_n$. It follows that $DIST(\mu\circ\pi,\mu\circ\sigma) = DIST(\pi,\sigma)$. Similarly, $DIST(\pi\circ\mu,\sigma\circ\mu) = count\{1 \le i \le n \mid \pi(\mu(i)) \ne \sigma(\mu(i))\} = count\{1 \le j \le n \mid \pi(j) \ne \sigma(j)\} = DIST(\pi,\sigma)$. Parts (b) and (c) follow directly from part (a). Part (d) follows from definition and part (e) is the generalization of part (d) which can be proved by an induction on part (d). □

In fact, parts (d) and (e) can be used to compute the hamming distance of a large set where it is divided into many smaller disjoint subsets. One can compute the hamming distance of each subset, the "cross distances" between distinct subsets, and finally obtain the hamming distance of the original set by taking the minimum of those distances.

4.2 Effect of contraction operation on hamming distance

In Chapter 2, we have shown that the result of the contraction operation on a t-PA(n,k) keeps the k-transitivity of the set. We now consider the effect of the contraction operation on the hamming distance of a c-PA(n,d).

Theorem 4.2: For all positive integers n, d > 3, M(n-1,d-3) ≥ M(n,d).

Proof: Let A be a c-PA(n,d). We construct B, a c-PA(n-1,d-3), by the contraction operation. Recall that the contraction operation works as follows: for each permutation σ' in A, (a) if the last symbol of σ'(1,2,…,n) is n, delete n and put the resulting permutation on (1,2,…,n-1) in B, or (b) if the last symbol of σ'(1,2,…,n) is not n, exchange n wherever it appears with the last symbol of σ'(1,2,…,n), delete the last symbol (which is n after the exchange) and put the resulting permutation on (1,2,…,n-1) in B. We now show that any two permutations in B have distance at least d-3. Let π and σ be distinct permutations in B that were created by distinct permutations π' and σ', respectively, in A. If both π and σ were created by (a), the pair (π,σ) in B has the same number of disagreements as the pair (π',σ') in A does, which is at least d because A is a c-PA(n,d). If either π or σ was created by (b), we consider the maximum number of positions where π(1,2,…,n-1) and σ(1,2,…,n-1) agree. Since π' and σ' are in A, which is a c-PA(n,d), they can agree in at most n-d positions. Suppose the last symbol of π'(1,2,…,n) is x and the last symbol of σ'(1,2,…,n) is y. If x is exchanged with n in the i^{th} position of π'(1,2,…,n) and σ'(1,2,…,n) has the symbol x in its i^{th} position, then the resulting permutations π(1,2,…,n-1) and σ(1,2,…,n-1) agree also in the new position i. Likewise, if y is exchanged with n in the j^{th} position of σ'(1,2,…,n) and π'(1,2,…,n) has the symbol y in its j^{th} position, then the resulting permutations π(1,2,…,n-1) and σ(1,2,…,n-1) agree also in the new position j. This scenario is shown in Figure 4.1. So, π(1,2,…,n-1) and σ(1,2,…,n-1) agree in at most n-d+2 positions. That is, the distance between π and σ is at least (n-1)-(n-d+2)=d-3. So, B is a c-PA(n-1,d-3) with the same number of permutations as there are in A. □

Note: A similar proof can be found in an unpublished paper of Yang et al. [61].

Position	i	j	n
π' = (…	n …	y …	x)
σ' = (…	x …	n …	y)

Figure 4.1. Two new agreements after contraction

Sometimes, the contraction operation produces a permutation array with distance d-2 rather than d-3. Avi Levy [45] called these two cases 2-contraction and 3-contraction, respectively, and proved that, for any sharply k-transitive group G that is both a sharp t-PA(n,k) and a maximum c-PA(n,d) where d=n-k+1 as shown in Section 1.2, G contracts to a c-PA(n-1,d-3) when d is divisible by 3 and G contracts to a c-PA(n-1,d-2) when d is not divisible by 3. Some applications of the contraction operation to compute values of M(n,d) are as follows, where resulting distances of d-2 are marked with *.

* M(17,14) ≥ 4896 (from M(18,16) = F(18,3) = 4896)

M(15,9) ≥ 40320 (from M(16,12) ≥ 40320, as given in Smith and Montemanni [54])

* M(16,14) ≥ 272 (from M(17,16) = F(17,2) = 272)

M(19,15) ≥ 6840 (from M(20,18) = F(20,3) = 6840)

* M(23,20) ≥ 12144 (from M(24,22) = F(24,3) = 12144)

* M(21,15) ≥ 12144 (from M(23,20) by double contractions)

M(21,16) ≥ 11955 (from M(21,15) by Morales' program [48] to remove 189 permutations)

* M(32,29) ≥ 32736 (from M(33,31) = F(33,3) = 32736)

* M(31,27) ≥ 32736 (from M(32,29))

M(30,24) ≥ 32736 (from M(31,27))

M(30,25) ≥ 32331 (from M(30,24) by Morales' program [48] to remove 405 permutations)

4.3 The coset technique

Theorem 4.3: Let G be a group of permutations such that G is a c-PA(n,d), i.e., DIST(G) ≥ d. If one can find a permutation μ, which we call a magic permutation, such that DIST(G,μ) ≥ d, then $G_1 = G \cup \mu \circ G$ is also a c-PA(n,d).

Proof: Proposition 4.1 gives us DIST(G ∪ μ∘G) = min{DIST(G), DIST(μ∘G), DIST(G,μ∘G)} and DIST(μ∘G) = DIST(G) ≥ d.

DIST(G,μ∘G) = min{DIST(π,μ∘σ) | π ∈ G, σ ∈ G} (by definition)

= min{DIST($\pi \circ \sigma^{-1}$,μ) | π ∈ G, σ ∈ G} (by Proposition 4.1 (a))

= min{DIST(σ',μ) | σ' ∈ G} (since G is a group, π ∈ G ∧ σ ∈ G ⇒ $\pi \circ \sigma^{-1}$ ∈ G)

= DIST(G,μ) (by definition)

≥ d (by hypothesis)

Therefore, DIST(G ∪ μ∘G) ≥ d.

Since G ∪ μ∘G is a set of permutations of length n, it follows that G ∪ μ∘G is a c-PA(n,d). □

Corollary 4.4: Let G be a group of permutations of length n such that DIST(G) ≥ d. If one can find a magic permutation μ such that DIST(G,μ) ≥ d, then M(n,d) ≥ 2|G|.

Proof: By Theorem 4.3, G ∪ μ∘G is a c-PA(n,d). So M(n,d) ≥ | G ∪ μ∘G| = |G| + |G| = 2|G|. □

Theorem 4.5: Let G be a group of permutations such that G is a c-PA(n,d), i.e., DIST(G) ≥ d. If one can find a sequence of permutations μ_0=e, μ_1, μ_2, …, μ_k, which we call a sequence of magic permutations, such that DIST($\mu_i \circ G, \mu_j$) ≥ d, for all 0 ≤ i < j ≤ k, then $G_k = \bigcup_{i=0}^{k} \mu_i \circ G$ is also a c-PA(n,d).

Proof: Proposition 4.1 gives us

$\mathrm{DIST}(\bigcup_{i=0}^{k} \mu_i \circ G) = \min\{\min\{\mathrm{DIST}(\mu_i \circ G) \mid 0 \le i \le k\}, \min\{\mathrm{DIST}(\mu_i \circ G, \mu_j \circ G) \mid 0 \le i < j \le k\}\}$

and $\min\{DIST(\mu_i \circ G) \mid 0 \leq i \leq k\} = DIST(G) \geq d$.

Similarly to the proof of Theorem 4.3, for all $0 \leq i < j \leq k$,

$DIST(\mu_i \circ G, \mu_j \circ G) = \min\{DIST(\mu_i \circ \pi, \mu_j \circ \sigma) \mid \pi \in G, \sigma \in G\}$ (by definition)

$= \min\{DIST(\mu_i \circ \pi \circ \sigma^{-1}, \mu_j) \mid \pi \in G, \sigma \in G\}$ (by Proposition 4.1 (a))

$= \min\{DIST(\mu_i \circ \sigma', \mu_j) \mid \sigma' \in G\}$ (since G is a group)

$= DIST(\mu_i \circ G, \mu_j)$ (by definition)

$\geq d$ (by hypothesis)

Therefore, $DIST(\bigcup_{i=0}^{k} \mu_i \circ G) \geq d$.

Since $\bigcup_{i=0}^{k} \mu_i \circ G$ is a set of permutations of length n, it follows that $\bigcup_{i=0}^{k} \mu_i \circ G$ is a c-PA(n,d). □

Corollary 4.6: Let G be a group of permutations of length n such that $DIST(G) \geq d$. If one can find a sequence of magic permutations $\mu_0=e, \mu_1, \mu_2, \ldots, \mu_k$, such that $DIST(\mu_i \circ G, \mu_j) \geq d$, for all $0 \leq i < j \leq k$, then $M(n,d) \geq (k+1)|G|$.

Proof: By Theorem 4.5, $\bigcup_{i=0}^{k} \mu_i \circ G$ is a c-PA(n,d). So $M(n,d) \geq |\bigcup_{i=0}^{k} \mu_i \circ G| = (k+1)|G|$. □

4.4 A random search algorithm

Some constructions for code permutation arrays have been developed (Chu et al. [16], Colbourn et al. [18], Ding et al. [23], Yang et al. [60]). Theorem 4.5 allows us to construct new code permutation arrays with competitive size. Starting with a sharply k-transitive group G, since G is also a maximum c-PA(n,d) where d = n-k+1 (by Proposition 1.7), there is no magic permutation μ such that $DIST(G,\mu) \geq d$. However, since every c-PA(n,d) is also a c-PA(n,d'), where $d' < d$, reducing the distance from d to d' of the group G gives us a possibility of finding a magic permutation μ such that $DIST(G,\mu) \geq d'$. As defined in Cameron and Wanless [14] and in

Wanless and Zhang [58], the covering radius of a set $S \subset S_n$, denoted by cr(S), is the smallest radius r such that all permutations in S_n are at distance no greater than r away from one of the permutations in S. In other words, S_n is covered by the balls of radius r centered at all permutations in S. So, when cr(G) > d', a magic permutation μ such that DIST(G,μ) $\geq$ d' is guaranteed to be found, because at covering radius d', G will not cover the whole set S_n. Similarly, when cr(G) < d', a magic permutation μ such that DIST(G,μ) $\geq$ d' cannot be found, because all permutations in S_n are at distance strictly less than d' away from a permutation in S. However, since the number of permutations in S_n increases exponentially by n, computing cr(G) quickly becomes infeasible. For example, at n = 18, the total number of permutations of length 18 is $18! > 6.4*10^{15}$.

Therefore, we used an algorithm that, at a particular distance d', randomly searches for a sequence of magic permutations, one after another, and adds their corresponding cosets into the group G to make a larger c-PA(n,d'). After a threshold of time without finding any more magic permutation, we decrease d' and repeat the process. Our algorithm is greedy in the sense that it will try to find the longest sequence of magic permutations before reducing the distance for a new search. There are several benefits of Theorem 4.5 in implementing this algorithm. When a magic permutation candidate μ_k is randomly generated, if DIST(G_{k-1},μ_k) $\geq$ d', we have $G_k = G_{k-1} \cup \mu_k \circ G$ as a new c-PA(n,d') without having to recheck that DIST(G_k) $\geq$ d'. Checking the condition of DIST(G_{k-1},μ_k) $\geq$ d' is also easy with less space complexity because instead of storing the big set G_{k-1}, one can store only G and the sequence of magic permutations obtained so far, namely μ_1 to μ_{k-1} (Bereg [4], Morales[48]). Moreover, as pointed out by Avi Levy [45], one can check the hamming distance of a group structure by considering only its conjugacy classes,

instead of dealing with every single permutation in the group. The set of conjugacy classes of a group is normally very small in comparison to the group itself. GAP [32] provides an easy way to play with these conjugacy classes.

In creating a program to remove redundancy of a t-PA(n,k), Fahle [28] noticed that the order used to remove permutations affects the ultimate number of redundant permutations that are removed. We observe a similar effect in our random search algorithm where the set of previously added magic permutations affects the chance of finding the next magic permutation, and consequently, affects the ultimate number of cosets to union with the original group, for a particular distance d'. To yield competitive results, we took the best one among many runs for small n and d' and also created different versions of the random search algorithm. A version of such a program created by Linda Morales [48] yields many new lower bounds for the M(n,d) table. Experimental results also lead us to the following conjecture:

Conjecture 4.7: For any sharply k-transitive group that is also a maximum c-PA(n,d) where d = n-k+1, one can find a permutation μ such that $DIST(G,\mu) \geq d-2$.

Conjecture 4.7 was verified for all sharply k-transitive groups of degree $n \leq 20$. Namely, we have the following results that are either as good as or better than (marked with *) results in Chu et al. [16] and Smith and Montemanni [54]:

M(8,4)	$\geq$ 8*M(8,6)	=	2688
M(9,6)	$\geq$ 3*M(9,7)	=	1512
M(11,6)	$\geq$ 12*M(11,8)	=	95,040
M(12,6)	$\geq$ 2*M(12,8)	=	190,080
M(14,10)	$\geq$ 3*M(14,12)	=	6552

* M(17,13) $\geq$ 3*M(17,15) = 12,240

* M(18,14) $\geq$ 2*M(18,16) = 9792

* M(20,16) $\geq$ 2*M(20,18) = 13,680

When considering good groups for the random search algorithm, we encountered, when q is a power of a prime, i.e., $q = p^r$, the affine general semilinear group AΓL(1,q) and the projective general semilinear group PΓL(2,q), which are formed by adding the Frobenius Automorphism of the Galois Field GF(q) into the AGL(1,q) and PGL(2,q), respectively (Groupprops [33], Gruenberg and Weir [34]). These semilinear groups are r times larger than their linear counterparts and were proved by Avi Levy [45] to have hamming distance of $q-p^{r*}$, where r* is the largest proper factor of r. So when p and r are primes and $q = p^r$, the AΓL(1,q) of size rq(q-1) is a c-PA(q,q-p) and the PΓL(2,q) of size r(q+1)q(q-1) is a c-PA(q+1,q-p). This gives infinitely many theoretical results that computational efforts can presumably not match, even with small values of n and d. Here are some examples:

M(9,6) $\geq$ 3*M(9,7) = 1512

* M(26,20) $\geq$ 2*M(26,24) = 31,200 (we found 6 more magic permutations that gives a set of 7*31,200 = 218,400 permutations without reducing the distance)

* M(28,24) $\geq$ 3*M(28,26) = 58,968

* M(33,30) $\geq$ 5*M(33,31) = 163,680

* M(126,120) $\geq$ 3*M(126,124) = 5,859,000

* M(129,126) $\geq$ 7*M(129,127) = 14,679,168

Levy [45] also proved that the distance between the Frobenius permutation and the AGL(1,q) and PGL(2,q) groups is q-p. Therefore, Conjecture 4.7 was partially proved for all

sharply 2- and 3-transitive groups AGL(1,2^r), AGL(1,3^r), PGL(2,2^r) and PGL(2,3^r), with the Frobenius Automorphism as the magic permutation. In general, we have, for any prime power q = p^r, M(q,q-p) ≥ 2M(q,q-1) = 2q(q-1) and M(q+1,q-p) ≥ 2M(q+1,q-1) = 2(q+1)q(q-1). In particular, the following lower bounds are more of interest, where q = 2^r or q = 3^r:

$M(2^r,2^r-2) \geq 2*M(2^r,2^r-1) = 2*2^r(2^r-1) = 2^{r+1}(2^r-1)$

$M(2^r+1,2^r-2) \geq 2*M(2^r+1,2^r-1) = 2*(2^r+1)2^r(2^r-1) = 2^{r+1}(2^{2r}-1)$

$M(3^r,3^r-3) \geq 2*M(3^r,3^r-1) = 2*3^r(3^r-1)$

$M(3^r+1,3^r-3) \geq 2*M(3^r+1,3^r-1) = 2*(3^r+1)3^r(3^r-1)$

For example:

M(16,14) ≥ 2*M(16,15) = 480

M(17,14) ≥ 2*M(17,15) = 8160

M(64,62) ≥ 2*M(64,63) = 8064

M(65,62) ≥ 2*M(65,63) = 524,160

M(81,78) ≥ 2*M(81,80) = 12,960 (not as good as a 2-contraction from a c-PA(82,80) which gives a set of 531,360 permutations)

M(82,78) ≥ 2*M(82,80) = 1,062,720

In an unpublished paper, Yang et al. [61] proved that M(n-1,d-2) ≥ $\left(\frac{2}{n}\right)$M(n,d) for n ≥ d > 2. One corollary of this theorem, which gives M(q,q-3) ≥ $\left(\frac{2}{q+1}\right)$M(q+1,q-1) = $\frac{2(q+1)q(q-1)}{q+1}$ = 2q(q-1) = 2M(q,q-1), where q is a power of a prime, is an additional evidence to support the correctness of Conjecture 4.7.

In another unpublished paper, Yang et al. [60] proved that the three Mathieu groups M_{22}, M_{23} and M_{24} have hamming distance 16 and claimed new lower bounds for M(22,16), M(23,16)

and M(24,16), respectively. However, these bounds were already published in a paper by Blake et al. [8] in 1979 and cited there as Jordan's results. They are all big groups (M_{24} has nearly 245 million permutations) and, therefore, promise to give really good results with our random search algorithm.

As mentioned in Chapter 1, $M(n,d) \leq M(n+1,d)$. This is because for an arbitrary c-PA(n,d), one can put the symbol n+1 at the end of each permutation to form a c-PA(n+1,d) with the same cardinality. Doing this on a sharply k-transitive group G gives G.(n+1) as denoted in Chapter 3. One can easily prove that G.(n+1) is also a group by verifying group properties, and that G.(n+1) is no longer a maximum c-PA(n,d) where d = n-k+1. This again gives us a possibility of finding a magic permutation μ such that $DIST(G.(n+1),\mu) \geq d$, or $DIST(G.(n+1).(n+2),\mu) \geq d$, and so on. Instead of running our random algorithm on these groups and distance d to search for a magic permutation (or a sequence of them), the following theorem allows us to reuse the magic permutation(s) that we found when reducing distance d to d'.

Theorem 4.8: Let G be a group of permutations such that G is a c-PA(n,d), i.e., $DIST(G) \geq d$, if one can find a sequence of magic permutations $\mu_0=e, \mu_1, \mu_2, \ldots, \mu_k$, such that $DIST(\mu_i \circ G,\mu_j) \geq d-\delta$, for all $0 \leq i < j \leq k$, then $M(n+t,d-\delta+t) \geq \min\{2t,k+1\} * M(n,d)$ for all $1 \leq t \leq \delta$.

Proof: By Proposition 4.1, each coset formed by the composition of a magic permutation in the sequence and the group is a c-PA(n,d). If we put symbols from (n+1) to (n+t) to t places, consistently among all permutations of the coset, we form a c-PA(n+t,d). We can vary the way we put symbols from (n+1) to (n+t) for up to 2t different cosets to obtain the desired hamming distance as follows:

Collection 1 of cosets

$\mu_0 \circ G$ (n+1) (n+2) … (n+t-1) (n+t)

$\mu_1 \circ G$ (n+2) (n+3) … (n+t) (n+1)

…

$\mu_{t-1} \circ G$ (n+t) (n+1) … (n+t-2) (n+t-1)

Collection 2 of cosets:

(n+1) (n+2) … (n+t-1) (n+t) $\mu_t \circ G$

(n+2) (n+3) … (n+t) (n+1) $\mu_{t+1} \circ G$

…

(n+t) (n+1) … (n+t-2) (n+t-1) $\mu_{2t-1} \circ G$

The “cross distance” between any two cosets in the same collection is at least d-δ+t because the cyclic shift of symbols from (n+1) to (n+t) adds t extra disagreements to the original distance of at least d-δ. The “cross distance” between a coset in collection 1 and a coset in collection 2 is also at least d-δ+t because an “old symbol” from 1 to n will mismatch with a “new symbol” from n+1 to n+t, and consequently, at least t extra disagreements are added to the original distance of at least d-δ.

Since each modified (by putting symbols from (n+1) to (n+t) into appropriate columns) coset is a c-PA(n+t,d) and the “cross distance” between any two modified cosets is at least d-δ+t, the union of those modified cosets are a c-PA(n+t,d-δ+t). So, it follows that $M(n+t,d-\delta+t) \geq \min\{2t,k+1\} * M(n,d)$ for all $1 \leq t \leq \delta$. □

Note that we cannot make other collection of cosets with a cyclic shift of symbols from (n+1) to (n+t) for columns, say from t+1 to 2t. This is because the swaps for those positions will

potentially give agreements in other columns with other coset and we will not have at least t extra disagreements as desired.

Corollary 4.9: For any prime power $q = p^r$, $M(q+p-1,q-1) \geq 2M(q,q-1) = 2q(q-1)$ and $M(q+p,q-1) \geq 2M(q+1,q-1) = 2(q+1)q(q-1)$.

Proof: As mentioned above in the discussion on Conjecture 4.7, the Frobenius Automorphism is a magic permutation when reducing the distance from q-1 to q-p of the AGL(1,q) and PGL(2,q) groups (Levy [45]). Using Theorem 4.8, we obtain the desired results. □

Again, the following lower bounds are more of interest, where $q = 2^r$ or $q = 3^r$:

$M(2^r+1,2^r-1) \geq 2*M(2^r,2^r-1) = 2*2^r(2^r-1) = 2^{r+1}(2^r-1)$

$M(2^r+2,2^r-1) \geq 2*M(2^r+1,2^r-1) = 2*(2^r+1)2^r(2^r-1) = 2^{r+1}(2^{2r}-1)$

$M(3^r+2,3^r-1) \geq 2*M(3^r,3^r-1) = 2*3^r(3^r-1)$

$M(3^r+3,3^r-1) \geq 2*M(3^r+1,3^r-1) = 2*(3^r+1)3^r(3^r-1)$

For example:

$M(18,15) \geq 2*M(17,15) = 8160$

$M(65,63) \geq 2*M(64,63) = 8064$ (not as good as a random search that found 4031 magic permutations for the cyclic group C_{65} that gives a set of 4032*65 = 262,080 permutations)

$M(66,63) \geq 2*M(65,63) = 524,160$

$M(84,80) \geq 2*M(82,80) = 1,062,720$

<u>Application of Theorem 4.8 in the M(n,d) table</u>:

Some examples of how we apply Theorem 4.8 to come up with new lower bounds for M(n,d) are as follows:

$M(9,6) \geq 3*M(9,7) = 1512 \Rightarrow M(10,7) \geq 2*M(9,7) = 1008$ (where $k+1 = 3$, $\delta = 1$)

$M(12,6) \geq 2*M(12,8) = 190,080 \Rightarrow M(13,7) \geq 2*M(12,8) = 190,080$ (t = 1)

and $M(14,8) \geq 2*M(12,8) = 190,080$ (where k+1 = 2, δ = 2)

$M(17,13) \geq 3*M(17,15) = 12,240 \Rightarrow M(19,15) \geq 3*M(17,15) = 12,240$ (where k+1 = 3, δ = 2)

$M(18,14) \geq 2*M(18,16) = 9792 \Rightarrow M(20,16) \geq 2*M(18,16) = 9792$ (where k+1 = 2, δ = 2)

$M(20,16) \geq 2*M(20,18) = 13,680 \Rightarrow M(21,17) \geq 2*M(20,18) = 13,680$ (t = 1)

and $M(22,18) \geq 2*M(20,18) = 13,680$ (where k+1 = 2, δ = 2)

Table 4.1. New M(n,d) lower bounds for $5 \leq d \leq 9$

n\d	5	6	7	8	9
10	18,720	8640	1008 = 2*504 (NB) 720	720	49
11	205,920	95,040	7920	7920	154
12	2,376,000	190,080	95,040	95,040	1320
13	6,592,404 = 42,259*156 (NB) 2,147,724	959,556 = 6151*156 (NB) 271,908	190,080 = 2*95,040 (NB) ---	95,040	4810
14	58,227,624 = 26,661*2184 (NB) 22,767,826	9,247,056 = 4234*2184 (NB) ---	1,644,552 = 753*2184 (NB) ---	209,664 = 96*2184 (NB) ---	26,208 = 12*2184 (NB)
15	---	---	---	1,022,910 = 68,194*15 (NB) ---	162,750 = 10,850*15 (NB)
16	---	---	---	---	1,320,960 = 5504*240 (NB) ---

The lower bound of 1008 for M(10,7) is a big improvement from 720, which is due to the sharply 3-transitive group of degree 10 ($M(10,7) \geq M(10,8) = 720$). This is the best current lower bound to our knowledge for M(10,7). Also note that some bounds above are outperformed by a

random search algorithm applied in other places. For example, currently we have the following lower bounds:

$M(14,8) \geq 96*M(14,12) = 96*2184 = 209,664$

$M(20,16) \geq 2*M(20,18) = 2*6840 = 13,680$

Table 4.2. New M(n,d) lower bounds for $10 \leq d \leq 14$

n\d	10	11	12	13	14
14	6552 = 3*2184	2184	2184	56	14
15	21,615 = 1441*15 (NB) ---	6076	2520	243	60
16	158,880 = 662*240 (NB)	40320	40320	1266	480 = 2*240 (NB)
17	1,240,320 = 304*4080 (NB) ---	187,680 = 46*4080 (NB) ---	83504	12,240 = 3*4080 (NB)	8160 = 2*4080 (NB)
18	---	1,228,896 = 251*4896 (NB) ---	176,256 = 36*4896 (NB) ---	24,480 = 5*4896 (NB) ---	9792 = 2*4896 (NB)
19	---	---	1,221,624 = 3572*342 (NB) ---	163,476 = 478*342 (NB) ---	65322
20	---	---	10,745,640 = 1571*6840 (NB) ---	1,477,440 = 216*6840 (NB) ---	150,480 = 22*6840 (NB) ---
21	---	---	---	---	1,120,266 = 53,346*21(NB)
22	---	---	$244,823,040_2$ (NB)	---	$10,200,960_2$ (NB)
23	---	---	---	---	$244,823,040_2$ (NB)

Tables from 4.1 through 4.4 give new lower bounds for M(n,d) where the first column gives n, the first row gives d, and the entries are current lower bounds, with (NB) representing a new lower bound, and "---" representing that previously only the Gilbert-Varshamov, i.e.,

"combinatorial", lower bounds or bounds by Proposition 1.4 (a) ($M(n,d) \geq M(n-1,d), M(n,d+1)$) are known. Subscripts 2 and 3 are for results from a 2- and 3-contraction, respectively. Entry $M(27,22) = 23{,}919_{2(3x)} = 24360\text{-}441$ in Table 4.4 denotes a combination of several techniques, namely, first we applied 3 times of contractions from the maximum c-PA(30,28), then we used a program (Morales [48]) to remove 441 permutations to form a c-PA(27,22).

Table 4.3. New M(n,d) lower bounds for $15 \leq d \leq 19$

n\d	15	16	17	18	19
18	8160 = 2*4080 (NB) ---	4896	70	18	
19	12,240 = 3*4080 (NB) ---	4896	343	342	19
20	20,520 = 3*6840 (NB) ---	13,680 = 2*6840 (NB) ---	---	6840	80
21	164,325 = 7825*21 (NB) ---	24864 = 1184*21 (NB) ---	13,680 = 2*6840 (NB) ---	---	210 = 10*21 (NB) ---
22	1,425,600 = 64,800*22 (NB) ---	443,520 (M_{22})	28,270 = 1285*22 (NB) ---	13,680 = 2*6840 (NB) ---	1100 = 10*110 (NB) ---
23	---	10,200,960 (M_{23})	---	279,818 = 553*506 (NB) ---	---
24	---	244,823,040 (M_{24})	1,335,840 = 110*12,144 (NB) ---	---	36,432 = 3*12,144 (NB) ---
25	---	---	---	---	---
26	---	---	---	9,313,200 = 597*15,600 (NB) ---	1,232,400 = 79*15,600 (NB) ---

Table 4.4. New M(n,d) lower bounds for $20 \leq d \leq 24$

n\d	20	21	22	23	24
22	1012 = 46*22 (NB) ---	66	22		
23	$12{,}144_2$ (NB) ---	---	506	23	
24	23,782 (NB) ---	---	12,144	144	24
25	---	$15{,}600_3$ (NB) ---	---	---	600
26	218,400 = 7*31,200 (NB) ---	31,200 = 2*15,600 (NB) ---	---	---	15,600
27	---	---	$23{,}919_{2(3x)}$ = 24360-441 (NB) ---	---	$19{,}656_2$ (NB) ---
28	---	1,316,952 = 67*19,656 (NB) ---	235,872 = 12*19,656 (NB) ---	---	58969 = 3*19,656 (NB) ---
29	---	---	---	---	---
30	---	---	---	1,291,080 = 53*24,360 (NB) ---	170,520 = 7*24,360 (NB) ---

4.5 Frequency permutation array

A frequency permutation array (FPA) of length $n = m\lambda$ and distance d, denoted by $FPA_\lambda(n,d)$, is a set of multipermutations on a multiset of m symbols, each repeated with frequency λ (Huczynska and Mullen [36]). Let $M_\lambda(n,d)$ be the maximum size of a $FPA_\lambda(n,d)$. When $\lambda=1$, $FPA_1(n,d)$ is simply a c-PA(n,d) and $M_1(n,d) = M(n,d)$.

Using a random search algorithm to add more frequency permutations into a FPA, we obtained the following results:

$M_{12}(36,24) \geq 34$

$M_{9}(36,28) \geq 17$

$M_{12}(36,30) \geq 4$

$M_{10}(40,32) \geq 11$

$M_{11}(44,32) \geq 46$

$M_{12}(48,40) \geq 7$

$M_{16}(64,48) \geq 28$

We were more interested in FPA's on only two symbols 0 and 1. One of the questions that was raised among our research group was how much one can improve $M_n(2n,d)$. For example, we found a $FPA_{12}(24,16)$ of size 4 and were asking whether it can be improved further. The following theorem is sometimes useful for answering this question.

Theorem 4.10: $M_{n-1}(2n-2,d-2) \geq M_n(2n,d)$

Proof: Let A be a $FPA_n(2n,d)$, we construct B, a $FPA_{n-1}(2n-2,d-2)$ of the same cardinality as A, by the contraction operation. Note that $FPA_n(2n,d)$ and $FPA_{n-1}(2n-2,d-2)$ are sets of strings of 0's and 1's. The contraction operation applied on $FPA_n(2n,d)$ is as follows: For each string of n 0's and n 1's in A, if the pair of symbols in positions n and 2n is (0,1) or (1,0), do nothing, but if this pair is (0,0) or (1,1), let i (j, respectively) be the largest position (nearest to the end of the string) that contains symbol 1 (symbol 0, respectively). Exchange the symbol 1 in the i^{th} position (symbol 0 in the j^{th} position, respectively) with the symbol 0 (symbol 1, respectively) in the $(2n)^{th}$ position. Then delete positions n and 2n from the string and add the resulting string into the set B. Clearly, set A and set B have the same cardinality. Also note that, because we delete

one symbol 0 and one symbol 1 from each string, the string structure holds, namely each string in B will have (n-1) 0's and (n-1) 1's.

We now show that all strings in the new set B have pairwise hamming distance at least d-2, or equivalently, have at most a=(2n-2)-(d-2)=2n-d agreements. Let π and σ be distinct strings in B that were created by distinct strings π' and σ', respectively, in A. Because A is a $FPA_n(2n,d)$, π' and σ' have hamming distance at least d, or equivalently, have at most 2n-d=a agreements. Let A_1, A_2, A_3 and A_4 be disjoint subsets of A such that strings in these subsets contain (0,1), (1,0), (0,0), and (1,1), respectively in positions n and 2n, as shown below:

	n	n+1	i	j	2n	
…	0				1	(A_1)
…	1				0	(A_2)
…	0		1	…0	…0	(A_3)
…	1			0	…1	(A_4)

If π' and σ' were in the same subset A_1 (or A_2), since we deleted 2 agreements between π' and σ', π and σ have at most a-2 agreements. If π' and σ' were in the same subset A_3 (or A_4), each of the two exchanges of symbols (one exchange occurring in π' and the other occurring in σ') potentially gives a new agreement. After that, we still delete 2 agreements between π' and σ', therefore, the maximum number of agreements between π and σ can be a+2-2=a.

If π' was in A_1 and σ' was in A_2, since we deleted 2 disagreements between π' and σ', π and σ have at most a agreements.

If π' was in A_1 or A_2 and σ' was in A_3 or A_4, π' and σ' agree in either position n or position 2n, but not both, and this position will be deleted. Since the exchange of symbols

occurring in σ' potentially gives a new agreement, the maximum number of agreements between π and σ can be a-1+1=a. For example, if π' was in A_2 and σ' was in A_3, π' and σ' agree in position 2n. The exchange of symbols occurring in σ' first creates a new disagreement in position 2n, and then it may create a new agreement of symbol 0 in the i^{th} position.

If π' was in A_3 and σ' was in A_4, by the pigeon-hole principle, $n < i < 2n$ and $n < j < 2n$, otherwise, π' and σ' don't have n 0's and n 1's. If i = j, $\pi'(i) = 1 \neq \sigma'(j) = 0$ and after the contraction, $\pi(i) = 0 \neq \sigma(j) = 1$, so π and σ have the same number of agreements as π' and σ' do, namely at most a agreements. If i < j, because i is the largest position in π' that contains symbol 1, $\pi'(k) = 0$ for all k > i. It follows that, after the contraction, the exchange of symbols occurring in σ' gives $\pi(j) = 0 \neq \sigma(j) = 1$ which is a new disagreement. The exchange of symbols occurring in π' may create a new agreement of symbol 0 in position i, so the maximum number of agreements between π and σ can be a-1+1=a. The case where i > j is symmetric to the case where i < j.

All possible cases of choosing a pair of distinct permutations (π,σ) in B have been enumerated, so B is a $FPA_{n-1}(2n-2,d-2)$. □

As an example of Theorem 4.10, we have $M_5(10,2) \geq M_6(12,4) \geq M_7(14,6) \geq M_8(16,8) \geq M_9(18,10) \geq M_{10}(20,12) \geq M_{11}(22,14) \geq M_{12}(24,16)$. Since $M_5(10,2) = 252$, as we have a maximum $FPA_5(10,2)$ of size 252, $M_{12}(24,16)$ cannot be improved to greater than 252, or in general, there is a limitation on how much $M_n(2n,d)$ can be improved. Our search program shows that $M_8(16,8) \geq 30$ and $M_6(12,4) \geq 68$. And we were finally able to prove that $M_{12}(24,16) = 4$ by using mathematical arguments, so $M_n(2n,2n-8) \leq 4$ for all n > 12.

Theorem 4.11: $M_\lambda(n,d) \geq n/\lambda = m$

Proof: The following is a $FPA_\lambda(n,n)$:

0…0	1…1	…	(m-2)…(m-2)	(m-1)…(m-1)
1…1	2…2	…	(m-1)…(m-1)	0…0
…				
(m-1)…(m-1)	0…0	…	(m-3)…(m-3)	(m-2)…(m-2)

Since any $FPA_\lambda(n,d)$ is also a $FPA_\lambda(n,d-1)$, the desired result follows.

Templates for code permutation arrays:

A frequency permutation of length n on m symbols can be used as a template to create a new permutation of length n from a given permutation of length $\lambda = n/m$. First we create m copies of the given permutation, where the next copy is formed by adding the length λ of the permutation to each symbol in the previous copy. So we obtained a permutation on I_n. Second, we rearrange the positions accordingly to the template.

For example, let us be given 0,1,2,2,0,1,0,0,2,1,1,2 as a frequency permutation of length 12 on 3 symbols 0, 1 and 2, each symbol appears exactly 4 times. Let us also be given 2,4,3,1 as a permutation of length 12/3 = 4. After the first step we have (2,4,3,1), (6,8,7,5), (10,12,11,9) which is a permutation on I_{12}. Here we group the symbols for better visualization. The first copy corresponds to all the zeros in the template, the second copy to all the ones and the third copy to all the twos. Rearrange the positions, we get 2,6,10,12,4,8,3,1,11,7,5,9. A frequency permutation can be considered as a template because following the same rules as described above, its application on different permutations produces different results. The following theorem shows a

construction of a new code permutation array from a frequency permutation array and another code permutation array.

Theorem 4.12: Let F be a $FPA_\lambda(n,d)$ and let A be a c-PA(λ,λd/n), then the set of all permutations formed by applying each frequency permutation in F as a template on each permutation in A is a c-PA(n,d).

Proof: The application of a template on a set is similar to making a coset from a magic permutation and a group. Consider one such subset. The step of rearranging the positions does not affect the hamming distance of the subset because each permutation in the subset receives the same rearrangement from the same template. The hamming distance between any two distinct permutations in the subset after step 1 is at least (λd/n)*m = d (because λ = n/m), so the hamming distance of the whole subset is at least d. Consider two different subsets, the distance of at least d between the two templates that created these two subsets guarantees the "cross distance" of at least d between them. □

Corollary 4.13: $M(n,d) \geq M_\lambda(n,d)*M(\lambda,\lambda d/n)$

Proof: Theorem 4.12 gives a construction of a c-PA(n,d) whose size is at least as large as $M_\lambda(n,d)*M(\lambda,\lambda d/n)$. □

Corollary 4.14: For all prime power q, $M(2q,2q-2) \geq 2q(q-1)$ and $M(2q+2,2q-2) \geq 2(q+1)q(q-1)$.

Proof: Using Corollary 4.13 with $M_q(2q,2q-2) \geq 2q/q = 2$ and $M_{q+1}(2q+2,2q-2) \geq (2q+2)/(q+1) = 2$ from Theorem 4.11 and M(q,q-1) = q(q-1) and M(q+1,q-1) = (q+1)q(q-1) from Proposition 1.8 gives the desired result.

Some examples of using Theorems 4.11-12 and Corollaries 4.13-14:

$M(22,20) \geq M_{11}(22,20)*M(11,10) \geq 2*11*10 = 220$ (not as good as a random search that found 45 magic permutations for the cyclic group C_{22} that gives a set of 46*22 = 1012 permutations)

$M(34,32) \geq M_{17}(34,32)*M(17,16) \geq 2*17*16 = 544$

$M(46,44) \geq M_{23}(46,44)*M(23,22) \geq 2*23*22 = 1012$

$M(58,56) \geq M_{29}(58,56)*M(29,28) \geq 2*29*28 = 1624$ (not as good as a 2-contraction from a maximum c-PA(59,58) which gives a set of 3422 permutations)

CHAPTER 5

CONCLUSIONS AND FUTURE WORK

Many techniques have been developed to improve the size of permutation arrays. For transitivity, our new recursive theorems help remove duplicate permutations between two permutation arrays in the creation of a new one. Experiments have shown that the resulting transitive permutation arrays require less effort from redundancy removal programs, like that of Fahle [28], and their sizes are competitive even without redundancy removal. For code permutation arrays, the coset technique combined with a random search algorithm yields many new lower bounds for M(n,d). Frequency permutation arrays can also be used as templates to construct new code permutation arrays. However, places where this method could give competitive results are very sparse.

Future work in this area is very promising. One can look into non-sharply transitive groups or "pseudogroups", like the M_{13} extension mentioned in Conway et al. [19]. Group structure is very beneficial, especially for hamming distance calculation and coset searching, as shown in Chapter 4. Finding good groups and improving the random search algorithm for cosets of those groups will potentially improve the lower bounds of M(n,d). Some examples of good groups are the three Mathieu groups M_{22}, M_{23} and M_{24} where the "giant" M_{24} has nearly 245 million permutations. Special handling of those groups is needed and tools like GAP [32] are very handy, especially in dealing with conjugacy classes of the group for hamming distance calculation. A three-or-more stage recursive construction is also an interesting direction to explore. And, further computational effort is needed, for example, in improving redundancy

removal, and in computing better bounds for F(6,2), F(7,3), F(7,4), F(8,4), F(9,4), F(12,2), M(7,4), M(7,5), M(8,5), M(9,6), M(10,7), M(10,9)…

REFERENCES

[1] S. B. Akers and B. Krishnamurthy, "A Group-Theoretic Model for Symmetric Interconnection Networks," *IEEE Trans. on Computer*, vol. 38, no. 4, pp. 555-566, 1989.

[2] L. M. Batten and A. Beutelspacher, "The Theory of Finite Linear Spaces," Cambridge Univ. Press, 2010, Online ISBN: 9780511666919.

[3] W. Bein, S. Latifi, L. Morales, and I. H. Sudborough, "Bounding the Size of k-Tuple Covers," *Proc. 42nd Hawaii International Conf. on System Sciences*, pp. 1-8, 2009.

[4] S. Bereg, "A communication on Permutation Arrays," The University of Texas at Dallas, email 2012.

[5] E. R. Berlekamp, "Algebraic Coding Theory," McGraw-Hill, New York, 1968.

[6] N. L. Biggs and A. T. White, "Permutation Groups and Combinatorial Structures," *London Math Soc. Lecture Note Series*, vol. 33, Cambridge Univ. Press, 1979, ISBN: 0521222877.

[7] I. F. Blake, "Permutation Codes for Discrete Channels," *IEEE Trans. on Inform. Theory*, vol. 20, pp. 138-140, 1974.

[8] I. F. Blake, G. Cohen and M. Deza, "Coding with Permutations," *Information and Control*, vol. 43, pp. 1-19, 1979.

[9] M. Bogaerts, "New Upper Bounds for the Size of Permutation Codes via Linear Programming," *Electronic Journal of Combinatorics*, vol. 17, #R135, 2010.

[10] A. Bonisoli and P. Quattrocchi, "Each Invertible Sharply d-Transitive Finite Permutation Set with $d \geq 4$ is a Group," *J. Algebraic Combinatorics*, vol. 12, no. 3, pp. 241-250, 2000.

[11] G. E. P. Box, J. S. Hunter and W. G. Hunter, "Statistics for Experimenters: Design, Innovation, and Discovery," 2nd Edition, Wiley, 2005, ISBN: 0471718130.

[12] R. H. Bruck and H. J. Ryser, "The nonexistence of certain finite projective planes," *Canadian J. Math*, vol. 1, pp. 88-93, 1949.

[13] P. J. Cameron, "Permutation Groups," *London Math Soc. Student Texts*, vol. 45, Cambridge Univ. Press, 1999, ISBN: 0521653789.

[14] P. J. Cameron and I. M. Wanless, "Covering radius for sets of permutations," *Discrete Math*, vol. 293, pp. 91-109, 2005.

[15] R. D. Carmichael, "Introduction to the Theory of Groups of Finite Order," Dover, New York, 1956, ISBN: 0486603008.

[16] W. Chu, C.J. Colbourn and P. Dukes, "Constructions for Permutation Codes in Powerline Communications," *Designs, Codes and Cryptography*, vol. 32, pp. 51-64, 2004.

[17] C. J. Colbourn, "The complexity of completing partial Latin squares," *Discrete Applied Math*, vol. 8, pp. 25-30, 1984.

[18] C. J. Colbourn, T. Kløve and A. C. H. Ling, "Permutation Arrays for Powerline Communication and Mutually Orthogonal Latin Squares," *IEEE Trans. on Inform. Theory*, vol. 50, no. 6, pp. 1289-1291, 2004.

[19] J. H. Conway, N. D. Elkies and J. L. Martin, "The Mathieu group M_{12} and its pseudogroup extension M_{13}," *Experimental Mathematics*, vol. 15, no. 2, pp. 223-236, 2006.

[20] S. R. Dalal and C. L. Mallows, "Factor-Covering Designs for Testing Software," *Technometrics*, vol. 40, no. 3, pp. 234-243, 1998.

[21] D. R. de la Torre, C. J. Colbourn and A. C. H. Ling, "An Application of Permutation Arrays to Block Ciphers," *Proc. 31st Southeastern International Conf. on Combinatorics, Graph Theory and Computing*, vol. 145, pp. 5-7, 2000.

[22] M. Deza and S. A. Vanstone, "Bounds for permutation arrays," *J. Statistical Planning and Inference*, vol. 2, no.2, pp. 197-209, 1978.

[23] C. Ding, F. Fu, T. Kløve and V. K. Wei, "Constructions of Permutation Arrays," *IEEE Trans. on Inform. Theory*, vol. 48, no. 4, pp. 977-980, 2002.

[24] P. Dukes and N. Sawchuck, "Bounds on permutation codes of distance four," *J. Algebraic Combinatorics*, vol. 31, pp. 143-158, 2010.

[25] T. Easton and R. G. Parker, "On completing latin squares," *Discrete Applied Math*, vol. 113, pp. 167-181, 2001.

[26] A. B. Evans, "Latin squares without orthogonal mates," *Designs, Codes and Cryptography*, vol. 40, pp. 121-130, 2006.

[27] W. A. Fahle, "Multiply Transitive Permutation Sets," Ph.D. Dissertation, The University of Texas at Dallas, 2012.

[28] W. A. Fahle, A program to remove redundancy in transitive permutation arrays, 2012.

[29] H. C. Ferreira and A. J. H. Vinck, "Interference Cancellation with Permutation Trellis Codes," *Proc. IEEE Vehicular Technology Conf.*, vol. 5, pp. 2401-2407, 2000.

[30] P. Frankl and M. Deza, "On the Maximum Number of Permutations with Given Maximal or Minimal Distance," *J. Combinatorial Theory*, vol. 22, pp. 352-360, 1977.

[31] F. Gao, Y. Yang and G. Ge, "An Improvement on the Gilbert–Varshamov Bound for Permutation Codes," *IEEE Trans. on Inform. Theory*, vol. 59, no. 5, pp. 3059-3063, 2013.

[32] The GAP Group, GAP – Groups, Algorithms, and Programming, Current Version 4.6.5 (July 2013), since 2008. *http://www.gap-system.org*.

[33] Groupprops – The Group Properties Wiki, "Projective semilinear group," *http://groupprops.subwiki.org/wiki/Projective_semilinear_group*, retrieved on August 18, 2013.

[34] K. W. Gruenberg and A. J. Weir, "Linear Geometry," 2nd Edition, Springer-Verlag, 2010. ISBN: 1441928065.

[35] I. Hajirasouliha, H. Jowhari, R. Kumar and R. Sundaram, "On Completing Latin Squares," *Proc. 24th Annual Symp. on Theoretical Aspects of Computer Science*, pp. 524-535, 2007.

[36] S. Huczynska and G. L. Mullen, "Frequency Permutation Arrays," *J. Combinatorial Designs*, vol. 14, no. 6, pp. 463-478, 2006.

[37] B. Huppert and N. Blackburn, "Finite Groups II & III," Springer-Verlag, 1982.

[38] I. Janiszczak and R. Staszewski, "An improved bound for permutation arrays of length 10," *http://www.iem.uni-due.de/preprints/IJRS.pdf*, retrieved on July 16, 2013.

[39] A. Jiang, R. Mateescu, M. Schwartz and J. Bruck, "Rank Modulation for Flash Memories," *Proc. IEEE International Symp. on Information Theory*, pp. 1731–1735, 2008.

[40] W. Kerby, "On infinite sharply multiply transitive groups," Vandenhoeck and Ruprecht, Göttingen, 1974, ISBN: 3525403070.

[41] E. A. Kuznetsov, "About of one class of ternary systems," *Kvazigruppi*, Kishinev, "Shtiintsa", vyp. 95, pp. 71-85, 1987.

[42] E. A. Kuznetsov, “Sharply k-transitive sets of permutations and loop transversals in S_n,” *Quasigroups and related systems*, vol.1, no. 1, pp 43-50, 1994.

[43] C. W. H. Lam, L. Thiel, and S. Swiercz, “The Non-existence of Finite Projective Planes of Order 10,” *Canadian J. Math*, vol. 41, pp. 1117-1123, 1989.

[44] S. Latifi, “A study of fault tolerance in star graph,” *Information Processing Letters*, vol. 102, no. 5, pp. 196-200, 2007.

[45] A. Levy, “A communication on Permutation Arrays and Permutation Groups,” working paper, The University of Texas at Dallas, 2012.

[46] B. D. McKay, A. Meynert and W. Myrvold, “Small Latin Squares, Quasigroups and Loops,” *J. Combinatorial Designs*, vol. 15, no. 2, pp. 98-119, 2007.

[47] B. D. McKay and I. M. Wanless, “On the number of Latin squares,” *Ann. Combin.*, vol. 9, pp. 335-344, 2005.

[48] L. Morales, “A communication on transitive and code Permutation Arrays,” The University of Texas at Dallas, email 2012.

[49] H. Nagao, “Multiply Transitive Groups,” Mathematics Department, California Institute of Technology, Pasadena, California, 1967.

[50] J. Nagura, “On The Interval Containing At Least One Prime Number,” *Proc. Japan Academy*, vol. 28, no. 4, pp. 177-181, 1952.

[51] D. S. Passman, “Permutation Groups,” Dover Publications, 2012, ISBN: 0486485927.

[52] N. Pavlidou, A.J. H. Vinck, J. Yazdani and B. Honary, “Power Line Communications: State of the Art and Future Trends,” *IEEE Communications Magazine*, vol. 41, no. 4, pp. 34-40, 2003.

[53] J. Quistorff, “A new nonexistence result for sharply multiply transitive permutation sets,” *Discrete Math*, vol. 288, pp. 185-186, 2004.

[54] D. H. Smith and R. Montemanni, “A new table of permutation codes,” *Designs, Codes and Cryptography*, vol. 63, pp. 241-253, 2012.

[55] H. Tarnanen, “Upper bounds on permutation codes via linear programming,” *European Journal of Combinatorics*, vol. 20, pp. 101-114, 1999.

[56] D.T. Todorov, “Four Mutually Orthogonal Latin Squares of Order 14,” *J. Combinatorial Designs*, vol. 20, no. 8, pp. 363-367, 2012.

[57] A. J. H. Vinck, “Coded Modulation for Power Line Communications,” *AEÜ International Journal of Electronics and Communications*, vol. 54, pp. 45-49, 2000.

[58] I. M. Wanless and X. Zhang, “Transversals of Latin squares and covering radius of set of permutations,” *European Journal of Combinatorics*, vol. 34, pp. 1130-1143, 2013.

[59] H. Wielandt, “Finite Permutation Groups,” Academic Press, 1964, ISBN: 0127496505.

[60] L. Yang, K. Chen and L. Yuan, “New Constructions of Permutation Arrays,” CoRR, abs/0801.3987, 2008. *http://arxiv.org/abs/0801.3987*.

[61] L. Yang, K. Chen and L. Yuan, “New Lower Bounds on Sizes of Permutation Arrays,” CoRR, abs/0801.3986, 2008. *http://arxiv.org/abs/0801.3986*.

[62] L. Yang, L. Dong and K. Chen, “New Upper Bounds on Sizes of Permutation Arrays,” CoRR, abs/0801.3983, 2008. *http://arxiv.org/abs/0801.3983*.

VITA

Quan Tuong Nguyen received his B.Eng. in Aeronautical Engineering from Ho Chi Minh City University of Technology, Vietnam, in 2005. He has served in academia since then. He taught GED Mathematics and Informatics at the Vietnamese American Private School for 2 years. He taught 2 sections of Microcomputer and Applications in Fall 2007, at the Center for International Education, Vietnam National University in Ho Chi Minh City. In Spring 2008, he became a Teaching Assistant and Research Fellow at the University of Houston-Clear Lake while earning a M.S. degree in Computer Science. His main research area was in graph theory, especially on the genus of the interconnection network. He was also interested in Data Analysis and Data Mining. His work in a Financial Data Mining course was honorably mentioned in the *Houston Chronicle* (http://www.chron.com/default/article/Some-take-the-tech-route-to-stock-market-success-1728897.php). He joined The University of Texas at Dallas in Fall 2009 to earn a Ph.D. degree in Computer Science, and continued serving as a Teaching Assistant and Research Fellow. He has been a TA for many courses, mainly for algorithms, theory of computation and automata theory. His research at UT Dallas was on combinatorial problems such as Topswops (also called the deterministic pancake problem) and permutation arrays. He is co-author of a paper on transitive permutation arrays, which has been submitted for publication, and has published in the Online Encyclopedia of Integer Sequences (oeis.org) a new exact number for topswops when n=17.

Quan Nguyen is also an enthusiast in computer repair and system correction. Since 2000, he has dedicated most of his free time to assembling, fixing, upgrading several desktops and laptops, and to trouble-shooting their problems at both hardware and software levels.