Maximum Codes with the Identifiable Parent Property

A Thesis
Presented to
The Academic Faculty

by

Wen Jiang

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy

School of Mathematics
Georgia Institute of Technology
December 2006

Maximum Codes with the Identifiable Parent Property

Approved by:

Dr. Xingxing Yu, Advisor
School of Mathematics
Georgia Institute of Technology

Dr. Luca Dieci
School of Mathematics
Georgia Institute of Technology

Dr. Robin Thomas
School of Mathematics
Georgia Institute of Technology

Dr. William Tom Trotter
School of Mathematics
Georgia Institute of Technology

Dr. Ye (Geoffrey) Li
School of Electrical and Computer Engineering
Georgia Institute of Technology

Date Approved: November 16, 2006

To my parents, my brothers and my husband.

ACKNOWLEDGEMENTS

There are many I would like to thank for helping me get this far. First and foremost are my family who carried the burden of supporting my study all these years. I thank them for their constant encouragement, loyal support, endless love, and for teaching me to take pride in myself. I will always be grateful for everything they have done for me.

I would like to express my special thanks to my advisor, Professor Xingxing Yu, for his great support and advice throughout my years at Georgia Tech. He has consistently provided me with freedom and encouragement whenever I needed it, and for this, I will always be indebted to him.

I owe much thanks to Professor Ye (Geoffrey) Li in the School of Electrical and Computer Engineering at Georgia Tech. Over the last five years his professional advice during our weekly meetings on Telecommunication and Signal Processing has been invaluable.

I also want to thank Professor Bolian Liu, my M.S. advisor in South China Normal University. His efforts, combined with the help of Professor Xingxing Yu, Professor Bill Green and Professor Hongjian Lai, made it possible for me to come to Georgia Tech.

All of the faculty who taught me mathematics deserve thanks. In particular I would like to thank Professors Eric Carlen, Luca Dieci, Bill Green, Evans Harrell, Chris Heil, Ted Hill, Bob Kertz, Michael Lacey, Prasad Tetali, Robin Thomas, and William Tom Trotter, all of whom I had the pleasure to work with and opportunity to learn from.

I thank Ms. Cathy Jacobson for her great help with my English. She was always available whenever I needed help. I will miss her. I thank Ms. Rena Brakebill for her great support in my teaching; she always tried to accommodate my course and schedule requests.

I thank all of my friends at Georgia Tech. Jian, Zixia, Yongfeng, Hua, Rui, Hao, Kun, Luis, Jorge, Marcio, Suleyman and many others have been very nice to me.

Finally, and most importantly, as a very special acknowledgment, I want to express my deep thankfulness to my husband, Yue. He was always there to help me when I got frustrated, and celebrate with me over accomplishments. I would never have gotten to this point without him.

TABLE OF CONTENTS

LIST OF FIGURES

SUMMARY

We study codes that have identifiable parent property. Such codes are called IPP codes. Research on IPP codes is motivated by design of schemes that protect against piracy of digital products.

Construction and decoding of maximum IPP codes have been studied in rich literature. General bounds on $F(n, q)$, the maximum size of IPP codes of length n over an alphabet with q elements, have been obtained through the use of techniques from graph theory and combinatorial design. Improved bounds on $F(3, q)$ and $F(4, q)$ are obtained. Probabilistic techniques are also used to prove the existence of certain IPP codes.

We prove a precise formula for $F(3, q)$, construct maximum IPP codes with size $F(3, q)$, and give an efficient decoding algorithm for such codes. The main techniques used in this thesis are from graph theory and nonlinear optimization. We begin by associating to each code an edge colored graph. Then a code has the IPP if and only if its associated graph has certain structural conditions. We study the underlying structure of graphs associated with IPP codes of maximum size. Using this approach, we present explicit construction of classes of graphs associated with IPP codes of length 3, which gives a lower bound on $F(3, q)$. By further investigating the structure of graphs associated with IPP codes of length 3, we show that there exist maximum IPP codes of length 3 whose associated graphs have good structural properties. Using such structural properties, we are able to convert the problem of deciding $F(3, q)$ to a nonlinear programming problem. Based on our nonlinear programming formulation, we give an algorithm which determines $F(3, q)$ numerically for each $q \geq 15$. We also describe how to construct maximum IPP codes from optimal solutions to the nonlinear programming problem, and show that such IPP codes possess good tracing capabilities. Using techniques from nonlinear programming, we prove a precise formula for $F(3, q)$ when $q \geq 15$.

Our approach may be used to improve bounds on $F(2k + 1, q)$. For example, we characterize the associated graphs of maximum IPP codes of length 5, and obtain bounds on $F(5, q)$.

CHAPTER I

INTRODUCTION

Recently, combinatorial structure and code designs have been widely used in the fields of communication, cryptography, networking and computer science. Some applications of coding theory to communication problems are described in [1]. Many practical problems where combinatorial designs have played a substantial role are discussed in some survey papers, such as those in applications of combinatorial designs in computer science [2], combinatorial designs and cryptography [3], applications of combinatorial designs to communications, cryptography, and networking [4, 5].

1.1 Fingerprinting and IPP Codes

Fingerprinting, first introduced by Wagner [6], is a technique for identifying individuals who use digital materials for unintended purposes, such as redistribution [7, 8, 9]. In order to control such misuse of digital materials, a distributor embeds a watermark (codeword) into each product through a variety of fingerprinting techniques [8, 15, 16, 17, 18, 19, 20, 21] before sending it to customers. Using different watermarks for different copies makes each copy unique. The watermark in each product can be used to identify the customer who buys that product and, thereby, redistributing the product is equivalent to exposing the customer's identity. However, a cost-effective attack against such digital fingerprints is that a group of customers can collude and create a new illegal product by combining parts of their products.

The problem of designing fingerprints that can withstand collusion and allow for the identification of colluders has been studied extensively in recent years. Several schemes for tracing colluders have been designed, see for example [9] and [10]. Frameproof codes and c-secure codes are introduced in [9] for protection against illegally copying software. Additive embedding techniques against collusion and a new class of codes, called anti-collusion codes, have been proposed in [27]. Traceability codes and schemes are studied in [10, 11, 12, 30].

IPP codes, first introduced in [31], are codes with the property that if two users create a new

image by combining parts of their images, then the new image reveals the identity of at least one of the source images. Hence, IPP codes provide traceability in the presence of a collusion attack.

1.1.1 Codes with the Identifiable Parent Property

Let Q be an alphabet and n be a positive integer. A *block code* C of length n over an alphabet Q is a set of n-tuples with components from Q. That is, $C \subseteq Q^n$, and C is called a *q-ary block code of length n*. Throughout, by a code we mean a block code. Given a code C of length n over an alphabet Q, the elements of C are called *codewords* which are of the form $(a_1, \ldots, a_n)$, where $a_i \in Q$ $(1 \leq i \leq n)$ is the ith coordinate.

Let C be a code of length n. For any two codewords $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$ in C, the *Hamming distance* between $\mathbf{a}$ and $\mathbf{b}$, denoted by $d(\mathbf{a}, \mathbf{b})$, is defined as the number of coordinates in which $\mathbf{a}$ and $\mathbf{b}$ differ. The *minimum distance* of C, denoted d_{min}, is defined as the minimum Hamming distance between all distinct pairs of codewords in C, i.e.,

$$d_{min} = \min\{d(\mathbf{a}, \mathbf{b}) : \mathbf{a}, \mathbf{b} \in C, \mathbf{a} \neq \mathbf{b}\}.$$

Let Q be an alphabet with q elements. For any code C over Q of length n and any two codewords $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$ in C, let

$$desc(\mathbf{a}, \mathbf{b}) = \{(x_1, \ldots, x_n) \in Q^n : x_i \in \{a_i, b_i\} \text{ for } 1 \leq i \leq n\}.$$

The set $desc(\mathbf{a}, \mathbf{b})$ is called the *descendant set* of $\mathbf{a}$ and $\mathbf{b}$. For any element $\mathbf{x} \in desc(\mathbf{a}, \mathbf{b})$, $\mathbf{x}$ is a *descendant* of $\mathbf{a}$ and $\mathbf{b}$, and $\mathbf{a}$ and $\mathbf{b}$ are *parents* of $\mathbf{x}$. The *descendant code* of C, denoted $desc(C)$, is defined by

$$desc(C) = \bigcup_{\mathbf{a}, \mathbf{b} \in C} desc(\mathbf{a}, \mathbf{b}).$$

For example, if C is a *binary repetition code* of length 4, i.e., $C = \{(0, 0, 0, 0), (1, 1, 1, 1)\}$, then $desc(C) = F_2^4$, where F_2 is the finite field with two elements 0 and 1. Similarly, if C is the *ternary Hamming code*, i.e.,

$$C = \left\{ \begin{array}{lll} (0,0,0,0), & (1,0,1,1), & (2,0,2,2) \\ (0,1,1,2), & (1,1,2,0), & (2,1,0,1) \\ (0,2,2,1), & (1,2,0,2), & (2,2,1,0) \end{array} \right\},$$

then $desc(C) = F_3^4$, since it is obvious that all words in a ball of radius 1 around a codeword are descendants of some pair containing that codeword.

A code C is said to have the *identifiable parent property* (IPP) if, for any $\mathbf{x} \in desc(C)$,

$$\bigcap_{\mathbf{x} \in desc(\mathbf{a},\mathbf{b})} \{\mathbf{a}, \mathbf{b}\} \neq \emptyset.$$

In other words, a code has the IPP if, whenever $\mathbf{x} \in desc(C)$, at least one of the parents of $\mathbf{x}$ can be identified. Codes with the IPP were introduced by Hollmann *et al* in [31]. A code with the IPP is also called an *IPP code*.

Trivially, any code of cardinality 2 is an IPP code, and so any repetition code $C \subseteq \{0, 1\}^n$ is an IPP code.

A less trivial example is the ternary Hamming code C. Note that for any pair of distinct codewords $\mathbf{a}, \mathbf{b} \in C$, $d(\mathbf{a}, \mathbf{b}) = 3$, so any descendant $\mathbf{x} \in desc(C)$ has distance less than or equal to 1 to exactly one of its parents in a parent pair. Hence, the unique codeword with distance at most 1 from $\mathbf{x}$ is the identifiable parent. For the other parent there are three choices if $\mathbf{c} \notin C$, and eight choices if $\mathbf{c} \in C$.

1.1.2 Motivation to Study Maximum IPP Codes and Existing Results

As mentioned earlier, IPP codes are capable of providing traceability in the presence of a collusion attack. Clearly, an IPP code with large size can mark more digital products. Hence, encoding and decoding of maximum IPP codes have been studied in rich literature.

Combinatorial properties of IPP codes and trace ability codes have been studied by several authors. Relationships of IPP codes with several other combinatorial structures and codes have been studied in [31, 32, 33]. Based on these connections several sufficient conditions on the existence of IPP codes are derived in [11, 31, 32, 34, 35]. Necessary conditions for the existence of IPP codes given in the form of an upper bound on the size of codes are obtained in [31, 33, 34, 35, 36, 37]. Probabilistic techniques are also used to prove the existence of certain IPP codes. Using the connections between IPP codes and other known combinatorial structures, several explicit constructions of IPP codes are derived in [11, 33, 36, 38, 41].

Algorithms for decoding IPP codes have also received much consideration. Various decoding algorithms including list decoding techniques have been studied in [42, 43, 44, 45, 46]. Recently,

IPP codes have been generalized for more practical applications. Generalizations of IPP codes have been studied in [35, 37, 39, 40, 47, 51, 52].

Let

$$F(n,q) = \max\{|C| : C \text{ is a } q\text{-ary code of length } n \text{ with the IPP}\}. \tag{1}$$

An IPP q-ary code of length n is said to be *maximum* if its size is $F(n,q)$.

As a trivial case, we have $F(1,q) = q$. We also have $F(2,q) = q$. It is easy to see $F(2,q) \geq q$, since we can simply construct an IPP code $C \subseteq Q^2$ with $C = \{(a_i, a_i) : a_i \in Q, 1 \leq i \leq q\}$. To prove $F(2,q) \leq q$, we consider any code $C \subseteq Q^2$. If $|C| \geq q+1$, then by the pigeon-hole principle, there exist two symbols $a_1, a_2 \in Q$ such that a_1 occurs in two different codewords as the first coordinate, and a_2 occurs in two different codewords as the second coordinate. Hence, C contains such codewords $\mathbf{a} = (a_1, x_1)$, $\mathbf{b} = (a_1, y_1)$, $\mathbf{c} = (x_2, a_2)$ and $\mathbf{d} = (y_2, a_2)$, where $x_i \neq y_i$ for $i = 1, 2$. Then the descendant $(a_1, a_2) \in desc(C)$ has no identifiable parent. Hence, $F(2,q) = q$.

$F(n,q)$ turns out to be much harder to derive when $n \geq 3$. In this thesis, we focus on explicit construction of IPP codes with maximum size $F(n,q)$. Hollmann, van Lint, Linnartz and Tolhuizen [31] obtained bounds on the maximum size of IPP codes of a given length n. They proved that $F(3,q) \leq 3q-1$ and for $n \geq 4$, there exists a constant c such that

$$c(\frac{q}{4})^{n/3} \leq F(n,q) \leq 3q^{\lceil n/3 \rceil}. \tag{2}$$

Many interesting IPP codes of length 3 are also constructed in this literature.

Tô and Safavi-Naini [36] obtained tighter bounds for $F(3,q)$, they proved that for $q \geq 17$,

$$3q + 6 - 6\lceil \sqrt{q+1} \rceil \leq F(3,q) \leq 3q + 6 - \lceil 6\sqrt{q+1} \rceil. \tag{3}$$

They also determined $F(3,q)$ precisely when $q \leq 48$ or when q can be expressed as $r^2 + 2r$ or $r^2 + 3r + 2$ for $r \geq 2$, and in the later case, maximum IPP codes are also constructed.

Alon, Fischer and Szegedy [34] answered an open question on $F(4,q)$ raised in [31]. They show that for any $\epsilon > 0$, if q is greater than some constant $q_0(\epsilon)$ which is related to ϵ, then

$$q^{2-\epsilon} \leq F(4,q) \leq \epsilon q^2. \tag{4}$$

1.2 Our Results

In this thesis, we primarily study structure and cardinality of maximum IPP codes of length 3 and 5, by using techniques from graph theory and nonlinear optimization. Our techniques may provide useful information on IPP codes of any odd length.

For IPP codes of length 3, we associate to each code C an *edge colored graph* as in [31], in such a way that the IPP of C is equivalent to certain structural conditions on the associated graph. We prove that there is always a maximum size IPP code of length 3 whose associated graph has a special structure (see Theorem 5.2.5). Such structural information is used to reduce the maximum size problem to a nonlinear programming problem. We then design an algorithm which determines $F(3,q)$ numerically for each $q \geq 15$. The problem for $q \leq 14$ was solved in [36]. Using the outputs of the algorithm, we describe a simple method that constructs maximum IPP codes of length 3. Designing decoding algorithm for IPP codes has been a challenging problem; however, we show that the maximum IPP codes constructed by our method allow for efficient tracing, by presenting a decoding algorithm with constant complexity. Moreover, we study the nonlinear programming problem, thereby, giving a precise formula for $F(3,q)$.

Note that for any positive integer $q \geq 0$, there exist unique integers r and k such that q can be written in the form of $q = r^2 + 2r + k$ where $0 \leq k \leq 2r+2$. Our precise formula for $F(3,q)$ is as follows. For $q \geq 15$,

$$F(3,q) = \begin{cases} 3r^2, & k = 0 \\ 3r^2 + 3k - 2, & 1 \leq k \leq 2\sqrt{r+4} - 3 \text{ and } k \text{ is odd, or} \\ & 2 \leq k \leq 2\sqrt{r+2} - 2 \text{ and } k \text{ is even} \\ 3r^2 + 3k - 3, & 2\sqrt{r+4} - 3 < k \leq r+1 \text{ and } k \text{ is odd, or} \\ & 2\sqrt{r+2} - 2 < k \leq r+1 \text{ and } k \text{ is even} \\ 3r^2 + 3k - 4, & k = r+2 \\ 3r^2 + 3k - 5, & r+3 \leq k \leq r + \sqrt{4r+21} - 2 \text{ and } k-r \text{ is odd, or} \\ & r+4 \leq k \leq r + \sqrt{4r+9} - 1 \text{ and } k-r \text{ is even} \\ 3r^2 + 3k - 6, & r + \sqrt{4r+21} - 2 < k \leq 2r+2 \; k-r \text{ is odd, or} \\ & r + \sqrt{4r+9} - 1 < k \leq 2r+2 \text{ and } k-r \text{ is even} \end{cases} \tag{5}$$

For $1 \leq q \leq 15$, see Table 1 in [36].

Using the same graph theoretic approach as for IPP codes of length 3, we obtain structural information on the associated graphs of IPP codes of length 5. We also completely characterize the

forbidden subgraphs of the associated graphs of IPP codes of length 5. These results are given in Chapter VIII.

1.3 Concepts from Coding Theory

In later Chapters, we need *extended ternary Hamming codes*, *shortened* or *extended Reed-Solomon codes* to develop our results. Hence, we include some more basic concepts from coding theory. For more information on coding theory, see e.g. [53, 54, 55, 56, 57].

Many examples we use are linear codes, and it is convenient to describe them through parity-check matrices. So we introduce basic concepts of linear codes. We use F to denote a finite field and $GF(q)$ to denote a finite field with elements $0, 1, \cdots, q-1$. The *order* of a non-zero element $\alpha \in F$ is defined as the smallest positive integer m such that $\alpha^m = 1$. An element of order $q-1$ in $GF(q)$ is called a *primitive element*. We also use the notation $GF(q)[x]$ to denote the ring of polynomials with coefficients in $GF(q)$. Denote the set of all n-tuples over F by $V_n(F)$. Then $V_n(F)$ is a *vector space* of dimension n under componentwise addition and multiplication. A *linear* (n,k)-code, or (n,k)-code for short, over F is a k-dimensional subspace of $V_n(F)$. If an (n,k)-code has minimum distance d_{min}, we also refer to this code as (n,k,d_{min})-code.

Clearly the binary repetition code $C = \{(0,0,0,0),(1,1,1,1)\} \subseteq V_4(GF(2))$ is a (4,1,4)-code. Let

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 2 \end{pmatrix}. \tag{6}$$

Define $C = \{\mathbf{c} \in V_4(GF(3)) : H\mathbf{c} = \mathbf{0}\}$. Then C is the ternary Hamming code as follows,

$$C = \left\{ \begin{array}{lll} \mathbf{c}_1 = (0,0,0,0), & \mathbf{c}_4 = (1,0,1,1), & \mathbf{c}_7 = (2,0,2,2) \\ \mathbf{c}_2 = (0,1,1,2), & \mathbf{c}_5 = (1,1,2,0), & \mathbf{c}_8 = (2,1,0,1) \\ \mathbf{c}_3 = (0,2,2,1), & \mathbf{c}_6 = (1,2,0,2), & \mathbf{c}_9 = (2,2,1,0) \end{array} \right\}. \tag{7}$$

Clearly C in (7) is a 2-dimensional subspace of $V_4(GF(3))$, and C has minimum distance 3. Hence, C is a (4,2,3)-code. The H in (6) is called the *parity check matrix* of the ternary Hamming code. A usual way to encode linear codes is to use parity check matrices.

Let C be a q-ary (n,k)-code and $\mathbf{c} = (c_0, c_1, \cdots, c_{n-2}, c_{n-1})$ be a codeword in C. The first k coordinates $c_0, c_1, \cdots, c_{k-1}$ are called the *message coordinates* of $\mathbf{c}$, and the last $n-k$ coordinates

$c_k, c_{k+1}, \cdots, c_{n-1}$ are called the *redundant coordinates* of $\mathbf{c}$. An (n,k)-code is said to be *shortened* if a message coordinate is deleted from the encoding process, and thus becomes an $(n-1, k-1)$-code. An (n,k)-code is said to be *extended* if an additional redundant coordinate is added from the encoding process, and thus becomes an $(n+1,k)$-code.

An (n,k)-code C is said to be *cyclic* if for every codeword $\mathbf{c} = (c_0, c_1, \cdots, c_{n-2}, c_{n-1}) \in C$, there is also a codeword $\mathbf{c}' = (c_{n-1}, c_0, c_1, \cdots, c_{n-2}) \in C$. Let C be a cyclic q-ary (n,k)-code and $\mathbf{c} = (c_0, c_1, \cdots, c_{n-2}, c_{n-1})$ be a codeword in C. The *code polynomial* associated with the codeword $\mathbf{c}$ is $c(x) = c_0 + c_1 x + \cdots + c_{n-2}x^{n-2} + c_{n-1}x^{n-1}$. Within the set of code polynomials associated with C, there is a unique monic polynomial $g(x)$ with minimal degree $n-k < n$, which is called the *generator polynomial* of C. Every code polynomial $c(x)$ in C can be expressed uniquely as $c(x) = m(x)g(x)$, where $g(x)$ is the generator polynomial of C and $m(x)$ is a polynomial of degree less than k in $GF(q)[x]$.

A *BCH code* over $GF(q)$ of length n and minimum distance d_{min} is a cyclic code generated by a polynomial

$$g(x) = (x-\beta^a)(x-\beta^{a+1})\cdots(x-\beta^{a+d_{min}-2})$$

in $GF(q)[x]$, where β is a primitive element in $GF(q)$ and a is some integer. A *Reed-Solomon code* is a q^m-ary BCH code of length q^{m-1}.

1.4 Thesis Outline

In Chapter II, we introduce basic terminology from graph theory and associate each code with an edge colored graph. An IPP code may be viewed as an edge colored graph with certain structural conditions.

In Chapter III, the structure of graphs associated with IPP codes of length 3 is studied. We prove two results which will be used to show that certain codes constructed in Chapter IV are IPP codes. In this chapter we also obtain further information which is crucial to the proof of (5).

In Chapter IV, we construct classes of IPP graphs associated with IPP codes of length 3, through which we obtain a lower bound on $F(3,q)$. In Chapter V, we further study the structure of graphs associated with IPP codes of length 3, and show that there exist maximum IPP codes of length 3 whose associated graphs possess very good structural properties.

In Chapter VI, we use the structure of maximum IPP graphs to convert the problem of deciding $F(3, q)$ to a nonlinear programming problem. We then derive an algorithm that determines $F(3, q)$ numerically for each $q \geq 15$ (The problem for $q \leq 14$ is done in [36]). We also describe how to construct maximum IPP codes by using optimal solutions to the nonlinear programming problem. At the end of Chapter VI, we present an algorithm, which shows that the IPP codes we construct allow for efficient tracing.

In Chapter VII, we prove (5). By using techniques from nonlinear optimization, we prove (5) for *critical values* of k at which the expression of $F(3, q)$ changes. We then complete the proof by a detailed analysis.

Finally in Chapter VIII we study IPP codes of length 5. Using the same graph theoretic approach as for IPP codes of length 3, we present structural information on the associated graphs of IPP codes of length 5.

Throughout the rest of this thesis, we fix $Q := \{\alpha_1, \alpha_2, \cdots, \alpha_q\}$, where q is some positive integer, and let $Q^n := \{(x_1, x_2, \cdots, x_n) : x_i \in Q \text{ for } i = 1, \cdots n\}$.

CHAPTER II

CODES AND ASSOCIATED GRAPHS

Several different methods have been employed to study IPP codes, including recursion techniques, number theory techniques, probabilistic methods and graph theoretic tools, see for example [31, 36, 34, 32, 38], as well as references therein. We shall use techniques from graph theory and nonlinear programming to study IPP codes.

2.1 Terminology from Graph Theory

A *graph* G consists of a vertex set $V(G)$ and an edge set $E(G)$, and each edge joins two distinct vertices of G. Typically, $V(G)$ is defined to be nonempty. For two graphs G and H, $G \cup H$ denotes the graph with vertex set $V(G) \cup V(H)$ and edge set $E(G) \cup E(H)$, $G \cap H$ denotes the graph with vertex set $V(G) \cap V(H)$ and edge set $E(G) \cap E(H)$.

Two graphs G and H are *disjoint* if $V(G) \cap V(H) = \phi$, $E(G) \cap E(H) = \phi$, and there is no edge with two ends in $V(G)$ and $V(H)$, respectively.

Two vertices u and v of G are said to be *adjacent* if $\{u, v\}$ forms an edge, where edge $\{u, v\}$ is usually written as uv or vu. If $e = uv \in E(G)$, then we say that u and v are the ends of e; and e is incident with u and v. If $e = uv \in E(G)$ with $u = v$, then e is a *loop*. We say E' is incident with V' if $E' \subseteq E(G)$ and V' is the set of ends of edges in E'.

Two or more edges that join a pair of vertices are called *multiple edges*. A *simple graph* is a graph with no loops or multiple edges. A *multigraph* is a graph which has no loops but may have multiple edges.

The *cardinality* of a set S is denoted by $|S|$. Therefore, for a graph G, $|V(G)|$ denotes the number of vertices in G, and $|E(G)|$ denotes the number of edges in G.

A graph H is a *subgraph* of a graph G if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$; if, in addition, $V(H) = V(G)$ then H is said to be *spanning*. For a subgraph H of a graph G, $G - V(H)$ denotes the subgraph of G obtained from G by deleting the vertices of H and all edges of G incident with the

vertices in $V(H)$.

A *path* in a graph is a sequence of distinct vertices $v_1v_2\cdots v_m$ such that there is an edge joining v_i and v_{i+1} for all $1 \leq i \leq m-1$; in this case, we say that the path is between v_1 and v_m and of length $m-1$. If $v_1v_2\cdots v_m$ is a path and there is an edge joining v_m and v_1, then $v_1v_2\cdots v_mv_1$ forms a *cycle* and is of length m. The *girth* of a graph is the length of the shortest cycle contained in the graph. If the graph doesn't contain any cycles, its girth is defined to be infinity.

A graph is *connected* if there is a path between every pair of distinct vertices of the graph. A *component* of a graph is a maximal connected subgraph. A vertex incident with no edges is called an *isolated* vertex. Clearly, an isolated vertex of a graph is also a component of the graph.

A graph is said to be *complete* if there is exactly one edge between every pair of distinct vertices. A complete graph with 3 vertices is also called a *triangle*.

A graph is a *bipartite graph* if the set of its vertices can be divided into two disjoint sets such that no two vertices of the same set share an edge. If a bipartite graph contains a cycle, then the length of the cycle must be even.

Two graphs G and H are *isomorphic* if there exists a map $f : V(G) \to V(H)$ such that f is one-to-one, and for any two vertices $u, v \in V(G)$, $e = uv \in E(G)$ if and only if $e' = f(u)f(v) \in E(H)$.

It is well known that if G is a connected graph then $|E(G)| \geq |V(G)| - 1$, if $|E(G)| \geq |V(G)|$ then G contains at least one cycle.

For more information on graph theory, see for example [60].

2.2 IPP Graphs

For each code $C \subseteq Q^n$, we define a graph G such that the vertices of G represent the codewords in C, and two vertices of G are joined by an edge of color i if their corresponding codewords have the same ith coordinate. Clearly $|C| = |V(G)|$. An *IPP graph* is an edge colored graph which is associated with an IPP code.

For example, the associated graph of the binary repetition code of length n is two isolated vertices, because the code has only two codewords and they don't share any common coordinates. Figure 1 is the associated graph of the ternary Hamming code in (7), where red, blue, green and magenta represent colors 1, 2, 3, 4, respectively. In this graph, vertex v_i corresponds to codeword

$\mathbf{c}_i$, $1 \leq i \leq 9$. v_i and v_j are joined by an edge of color k if $\mathbf{c}_i$ and $\mathbf{c}_j$ share the kth coordinate where $1 \leq i \neq j \leq 9, 1 \leq k \leq 4$.

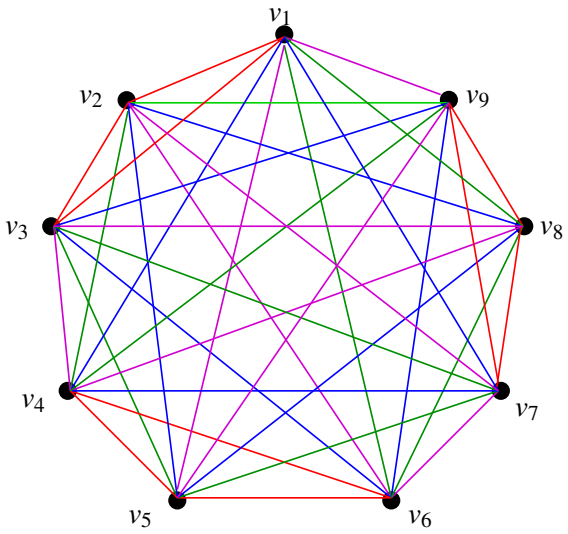


Figure 1: The associated graph of the ternary Hamming code

Let S be a component of an edge colored graph G with $|V(S)| \geq 2$. If the edges of S use only one color, then S is called a *uni-color component*; if the edges of S use exactly two colors, then S is called a *bi-color component*; if the edges of S use exactly three colors, then S is called a *tri-color component*. *Four-color components* and *five-color components* are defined similarly. In general, define *k-color components* as those components whose edges use exactly k colors for $k \geq 6$. If S is an isolated vertex, we treat S as a uni-color component using color 1 by default.

Let G be an edge colored graph using colors $\{1, \ldots, n\}$. For each $i \in \{1, \ldots, n\}$, let $G(i)$ denote the *spanning subgraph* of G whose edges are exactly those edges of G with color i. We see that the associated graph G of the ternary Hamming code in Figure 1 is a four-color component, and for each $1 \leq i \leq 4$, $G(i)$ consists of three disjoint triangles whose edges use color i.

The following result from [31] gives a necessary and sufficient condition for a code to have the IPP.

Lemma 2.2.1. *A code $C \subseteq Q^n$ has IPP iff*

(IPP1) for any three distinct codewords **a, b, c** *in C, there exists some $1 \leq i \leq n$ such that the ith coordinates of* **a, b, c** *are pairwise distinct, and*

(IPP2) For any four distinct codewords **a, b, c, d** *in C, there exists some $1 \leq i \leq n$ such that no ith*

coordinate of **a** *or* **b** *coincides with the ith coordinate of* **c** *or* **d**.

We can rephrase Lemma 2.2.1 to give a necessary and sufficient condition for an associated graph to be an IPP graph.

Lemma 2.2.2. *Let $C \subseteq Q^n$ and G be its associated graph. Then G is an IPP graph iff*
(IPP1) for any three distinct vertices u, v, w of G, there exists some color $i \in \{1, \ldots, n\}$ such that u, v, w belong to three different components of $G(i)$, and
(IPP2) for any four distinct vertices u, v, w, x of G, there exists some color $i \in \{1, \ldots, n\}$ such that any component of $G(i)$ containing u or v contains neither w nor x.

For any subgraph S of an edge colored graph G and for any color i used by G, it is easy to see that if S is a union of components of G, then each component of $S(i)$ is also a component of $G(i)$. Hence, the following result is a direct consequence of Lemma 2.2.2.

Lemma 2.2.3. Let G be an IPP graph and S be a union of components of G. Then S is an IPP graph.

It is convenient to distinguish those elements of Q that are used in different coordinate position. We shall make use of the following notation. For a code $C \subseteq Q^n$, let $Q_i(C)$ $(1 \leq i \leq n)$ denote the set of elements of Q, each of which occurs as the ith coordinate of some codeword in C. Hence, $C \subseteq \{(x_1, x_2, \cdots, x_n) : x_i \in Q_i(C)\}$. For a subgraph S of G associated with $C \subseteq Q^n$, let $Q_i(S)$ denote the set of elements of Q, each of which occurs as the ith coordinate of some codeword corresponding to a vertex of S.

CHAPTER III

ASSOCIATED GRAPHS OF IPP CODES OF LENGTH 3

3.1 Introduction

As recall this, to each code $C \subseteq Q^3$, we associate an edge colored graph G with C. The vertices of G represent the codewords in C, and two vertices of G are joined by an edge of color i if their corresponding codewords have the same ith coordinate. Hence, edges of an associated graph of an IPP code of length 3 use colors from $\{1, 2, 3\}$. In this Chapter, we aim to derive some structural information of graphs associated with IPP codes of length 3.

The following result proved in [31] gives useful structural information. It describes some forbidden edge colored subgraphs of an IPP graph associated with an IPP code of length 3.

Lemma 3.1.1. *Let $C \subseteq Q^3$ be an IPP code and G be its associated graph. Then the following statements hold:*

(i) If $|C| > |Q|$ then no two vertices of G are joined by more than one edge;

(ii) G contains no triangle whose edges use three different colors; and

(iii) G contains no path of length 3 whose edges use pairwise different colors.

As a trivial case, $F(3, 1) = 1$ and $F(3, 2) = 2$, as presented in Table 1 in this thesis. For $q \geq 3$, it has been shown that $F(3, q) \geq q + 1$ in [31]. For example, let $Q = \{\alpha_1, \alpha_2, \cdots, \alpha_q\}$, $m = \lfloor \frac{q-1}{2} \rfloor$. Let $C = \{(\alpha_1, \alpha_1, \alpha_1)\} \cup \{(\alpha_1, \alpha_i, \alpha_i) : 2 \leq i \leq m + 1\} \cup \{(\alpha_i, \alpha_1, \alpha_{i+m}) : 2 \leq i \leq m + 1\} \cup \{(\alpha_i, \alpha_i, \alpha_1) : m + 2 \leq i \leq q\}$. Then $|C| = q + m \geq q + 1$ when $q \geq 3$. In each position, every symbol α_i, $2 \leq i \leq q$, occurs in at most one codeword. So if $\mathbf{x} \in desc(C)$ and $\mathbf{x} \neq (\alpha_1, \alpha_1, \alpha_1)$, then at least one parent is identifiable. If $\mathbf{x} = (\alpha_1, \alpha_1, \alpha_1)$, then $(\alpha_1, \alpha_1, \alpha_1)$ must be an identifiable parent. Hence, C has the IPP. This implies $F(3, q) \geq q + 1$ when $q \geq 3$.

Since we are interested in maximum IPP codes of length 3 over Q, by (i) of Lemma 3.1.1, we only need to study simple graphs associated with IPP codes of length 3.

3.2 Structural Results about IPP Graphs

The next two lemmas will be used to show that certain codes constructed in the next section are IPP codes. First, by applying Lemma 2.2.2 and Lemma 2.2.3, we can establish the converse of Lemma 2.2.3.

Lemma 3.2.1. *Let $C \subseteq Q^3$ with $|C| > |Q|$, let G be the associated graph of C, and let S, T be unions of components of G such that $S \cap T = \emptyset$ and $S \cup T = G$. If S and T are IPP graphs, then so is G.*

Proof. It suffices to prove that G satisfies (IPP1) and (IPP2) of Lemma 2.2.2.

To prove that G satisfies (IPP1) of Lemma 2.2.2, let u, v, w be three distinct vertices of G. We need to show that there exists some $i \in \{1, 2, 3\}$ such that u, v, w belong to three different components of $G(i)$.

First, assume $\{u, v, w\} \subseteq V(S)$. Since S is an IPP graph, there exists some $i \in \{1, 2, 3\}$ such that u, v, w belong to three different components of $S(i)$. Since S is a union of components of G, any component of $S(i)$ is also a component of $G(i)$. Hence, u, v, w belong to three different components of $G(i)$.

So we may assume that $\{u, v, w\} \nsubseteq V(S)$. Similarly, we may assume that $\{u, v, w\} \nsubseteq V(T)$.

Then by symmetry, we may assume that $u, v \in V(S)$ and $w \in V(T)$. Since S is an IPP graph, there exists some $i \in \{1, 2, 3\}$ such that u and v belong to two different components of $S(i)$. Because $S \cap T = \emptyset$, the component of $T(i)$ containing w is disjoint from $S(i)$. Since S and T are unions of components of G, each component of $S(i)$ or $T(i)$ is also a component of $G(i)$. Hence, u, v, w belong to three different components of $G(i)$. So G satisfies (IPP1) of Lemma 2.2.2.

To prove that G satisfies (IPP2) of Lemma 2.2.2, let u, v, w, x be four distinct vertices of G. We need to show that there exists some $i \in \{1, 2, 3\}$, no component of $G(i)$ containing u or v contains w or x.

Suppose $\{u, v, w, x\} \subseteq V(S)$. Since S is an IPP graph, there exists some $i \in \{1, 2, 3\}$ such that no component of $S(i)$ containing u or v contains w or x. Since S is a union of components of G, the components of $G(i)$ containing one of $\{u, v, w, x\}$ is also a component of $S(i)$. Hence, no component of $G(i)$ containing u or v contains w or x.

Therefore, we may assume that $\{u, v, w, x\} \nsubseteq V(S)$. Similarly, we may assume that $\{u, v, w, x\} \nsubseteq$

$V(T)$.

Assume for the moment that one of S and T contains three of $\{u, v, w, x\}$, and the other contains one of $\{u, v, w, x\}$. By symmetry, we may assume that $u, v, w \in V(S)$ and $x \in V(T)$. Since S is an IPP graph, there exists some $i \in \{1, 2, 3\}$ such that u, v, w belong to three different components of $S(i)$. Because $S \cap T = \emptyset$, the component of $T(i)$ containing x is disjoint from $S(i)$. Also since S and T are unions of components of G, each component of $G(i)$ containing one of $\{u, v, w, x\}$ is also a component of $S(i)$ or $T(i)$. Therefore, no component of $G(i)$ containing u or v contains w or x.

Thus, we may assume that each of S and T contains exactly two vertices from $\{u, v, w, x\}$. We need to consider two cases.

First, one of S and T contains $\{u, v\}$ and the other contains $\{w, x\}$. By symmetry, we may assume $\{u, v\} \subseteq V(S)$ and $\{w, x\} \subseteq V(T)$. Since S is an IPP graph, there exists some $i \in \{1, 2, 3\}$ such that u, v belong to different components of $S(i)$. Note that any component of $T(i)$ containing w or x is contained in T and, hence, is disjoint from $S(i)$. As before, any component of $G(i)$ containing one of $\{u, v, w, x\}$ is a component of $S(i)$ or $T(i)$. Hence no component of $G(i)$ containing u or v contains w or x.

The remaining case to be considered is when neither S nor T contains $\{u, v\}$ or $\{w, x\}$. By symmetry, we may assume $\{u, w\} \subseteq V(S)$ and $\{v, x\} \subseteq V(T)$. Again, since S is an IPP graph, there exists some $i \in \{1, 2, 3\}$ such that u, w belong to different components of $S(i)$. Similarly, since T is an IPP graph, there exists some $j \in \{1, 2, 3\}$ such that v, x belong to different components of $T(j)$. Note that any component of $G(i)$ containing one of $\{u, v, w, x\}$ is a component of $S(i)$ or $T(i)$. If v, x belong to different components of $T(i)$, then we see that u, v, w, x belong to four different components of $G(i)$. So we may assume that v, x belong to the same component of $T(i)$. Then by (i) of Lemma 3.1.1, $i \neq j$ and, for each $\{k\} = \{1, 2, 3\} - \{i\}$, v and x belong to different components of $T(k)$. Similarly, if u, w belong to different components of $S(j)$, then u, v, w, x belong to four different components of $G(j)$. So we may assume that u, w belong to the same component of $S(j)$. Hence, by (i) of Lemma 3.1.1, u and w belong to different components of $S(k)$. Again, since S and T are unions of components of G, any component of $G(k)$ containing one of $\{u, v, w, x\}$ is a component of $S(k)$ or $T(k)$. Therefore, u, v, w, x belong to four different components of $G(k)$. Hence G satisfies (IPP2) of Lemma 2.2.2. □

Our next lemma shows a situation where a component of a graph (associated with a code) is an IPP graph.

Lemma 3.2.2. *Let $C \subseteq Q^3$, let G be the associated graph of C, and let S be a component of G.*

(i) If S is a uni-color component or a bi-color component of G then S is an IPP graph.

(ii) If there exist a vertex z of S and complete subgraphs S_1, S_2, S_3 of S such that $S_1 \cup S_2 \cup S_3 = S$, $V(S_i \cap S_j) = \{z\}$ for $\{i, j\} \subseteq \{1, 2, 3\}$, and for each $i \in \{1, 2, 3\}$ all edges of S_i are colored with color i, then S is an IPP graph.

Proof. Suppose S is a uni-color or bi-color component. Let $i \in \{1, 2, 3\}$ be a color not used by edges of S. Then every component of $S(i)$ is an isolated vertex. Hence, (IPP1) and (IPP2) of Lemma 2.2.2 hold. Since G is associated with C, S is also associated with a code (whose codewords are the codewords in C corresponding to the vertices of S). So S is an IPP graph, and (i) holds.

Next, let S be given as in (ii). It suffices to show that S satisfies (IPP1) and (IPP2) of Lemma 2.2.2.

Let u, v, w be distinct vertices of S. If $\{u, v, w\} \subseteq V(S_i) \cup V(S_j)$ for some $\{i, j\} \subseteq \{1, 2, 3\}$, then u, v, w belong to three different components of $S(k)$, where $k \in \{1, 2, 3\} - \{i, j\}$. So we may assume that no S_i contains two of $\{u, v, w\}$. Then u, v, w belong to different components of $S(1)$. So S satisfies (IPP1) of Lemma 2.2.2.

Now let u, v, w, x be four distinct vertices of S. If $\{u, v, w, x\} \subseteq V(S_i \cup S_j)$ for some $\{i, j\} \subseteq \{1, 2, 3\}$, then u, v, w, x belong to four different components of $S(k)$, where $k \in \{1, 2, 3\} - \{i, j\}$. So we may assume by symmetry that S_1 contains two vertices from $\{u, v, w, x\}$ and that $S_2 - \{z\}$ and $S_3 - \{z\}$ each contain exactly one vertex from $\{u, v, w, x\}$. First, assume $\{u, v\} \subseteq V(S_1)$. Note that S_1 is a component of $S(1)$, and so, no component of $S(1)$ containing u or v contains w or x. Similarly, if $\{w, x\} \subseteq V(S_1)$, then no component of $S(1)$ containing w or x contains u or v. So by symmetry, we may assume that $\{u, w\} \subseteq V(S_1)$, $v \in V(S_2) - \{z\}$, and $x \in V(S_3) - \{z\}$. If $u = z$ then $\{u, v\} \subseteq V(S_2)$ and, as in the previous case, we can show that no component of $S(2)$ containing u or v contains w or x. Similarly, if $w = z$, then we can show that no component of $S(3)$ containing w or x contains u or v. So we may assume $u \neq z$ and $w \neq z$. Then we see that the components of $S(2)$ containing u or w or x each are an isolated vertex, and the component of $S(2)$ containing v is S_2. Hence, no component of $S(2)$ containing u or v contains w or x. This shows that S satisfies (IPP2) of Lemma 2.2.2. □

For bi-color components, we prove further information in the following, which is crucial to the nonlinear programming formulation and the proof of (5).

Lemma 3.2.3. *Let $C \subseteq Q^3$ be an IPP code with $|C| > |Q|$ and G be its associated graph. Let S be a component of G whose edges use color i and color j for some $\{i, j\} \subseteq \{1, 2, 3\}$, and let $\{k\} = \{1, 2, 3\} - \{i, j\}$. Then*

$$|Q_i(S)| + |Q_j(S)| - 1 \leq |Q_k(S)| \leq |Q_i(S)||Q_j(S)|.$$

Proof. Let $R_1, \cdots, R_{n_1}$ denote the components of $S(i)$, and let $T_1, \cdots, T_{n_2}$ be the components of $S(j)$. Then for $1 \leq i \leq n_1$ (respectively, $1 \leq t \leq n_2$), those codewords in C corresponding to vertices of R_s (respectively, T_t) have the same ith (respectively, jth) coordinate, and hence, R_s (respectively, T_t) is a complete graph. Moreover, by (i) of Lemma 3.1.1, $|V(R_s) \cap V(T_t)| \leq 1$.

Define an auxiliary graph H as follows. The vertices of H are $R_1, \cdots, R_{n_1}$ and $T_1, \cdots, T_{n_2}$. For any $1 \leq s \leq n_1$ and $1 \leq t \leq n_2$, R_s and T_t are joined with an edge in H when $|V(R_s) \cap V(T_t)| = 1$. Let m denote the number of edges in H. Since S is connected, H is connected, and hence, $m \geq n_1 + n_2 - 1$. Note that m represents the number of pairs R_s and T_t such that $|V(R_s) \cap V(T_t)| \neq 0$.

We now count $|Q_i(S)|$, $|Q_j(S)|$, and $|Q_k(S)|$. Since there is no edge of color k, and because $\cup_{s=1}^{n_1} R_s$ and $\cup_{t=1}^{n_2} T_t$ have m vertices in common, we have

$$\begin{aligned}
|Q_i(S)| &= n_1 + (\textstyle\sum_{t=1}^{n_2} |V(T_t)|) - m, \\
|Q_j(S)| &= n_2 + (\textstyle\sum_{s=1}^{n_1} |V(R_s)|) - m, \text{ and} \\
|Q_k(S)| &= (\textstyle\sum_{s=1}^{n_1} |V(R_s)|) + (\textstyle\sum_{t=1}^{n_2} |V(T_t)|) - m.
\end{aligned}$$

Hence

$$|Q_i(S)| + |Q_j(S)| = |Q_k(S)| + n_1 + n_2 - m.$$

Since $m \geq n_1 + n_2 - 1$, we have

$$|Q_k(S)| \geq |Q_i(S)| + |Q_j(S)| - 1.$$

Next, we show $|Q_k(S)| \leq |Q_i(S)||Q_j(S)|$. Suppose on the contrary $|Q_k(S)| \geq |Q_i(S)||Q_j(S)| + 1$. Then there must exist some symbol $a \in Q_i(S)$ such that a occurs as the ith coordinate of at least $|Q_j(S)| + 1$ codewords. By the pigeonhole principle, there exist two vertices of S joined by two edges, contradicting (i) of Lemma 3.1.1. □

From the conclusion of Lemma 3.2.3, we see that $|V(S)| = |Q_k(S)| \leq |Q_i(S)||Q_j(S)|$. In addition, we observe that $|Q_k(S)| = |Q_i(S)||Q_j(S)|$ only if for any $a \in Q_i(S)$ (respectively, $a \in Q_j(S)$), a occurs as the ith (respectively, jth) coordinate in exactly $|Q_j(S)|$ (respectively, $|Q_i(S)|$) codewords. Therefore, each component of $S(i)$ (respectively, $S(j)$) is a complete graph on exactly $|Q_j(S)|$ (respectively, $|Q_i(S)|$) vertices. It is easy to see that this necessary condition is also sufficient for $|Q_k(S)| = |Q_i(S)||Q_j(S)|$. This observation suggests that in order to construct a maximum IPP code, the numbers of symbols used by any two coordinate positions should be roughly equal. This observation is the foundation to our proof of main structure theorem (Theorem 5.2.5) for IPP graphs. Theorem 5.2.5 is proved in [36]. In this thesis, we provide a simple and independent proof for Theorem 5.2.5.

CHAPTER IV

LOWER BOUND

In this chapter, we use IPP graphs to derive a lower bound on $F(3, q)$, by making use of Lemma 3.2.1 and Lemma 3.2.2. We give explicit constructions of several classes of IPP codes, including some constructed in [31] and [36]. Such codes turn out to be maximum IPP codes of length 3 and can provide means for efficient tracing.

We observe that for each integer $q \geq 15$, there exist unique integers r and k such that $r \geq 3$, $0 \leq k \leq 2r + 2$, and $q = r^2 + 2r + k$.

4.1 A Partition of $\{0, 1, \cdots, 2r + 2\}$

Let $I = \{0, 1, 2, 3, \cdots, 2r+2\}$, $I_0 = \{0\}$, $I_1 = \{k : 1 \leq k \leq 2\sqrt{r+4} - 3$ when k is odd, or $2 \leq k \leq 2\sqrt{r+2} - 2$ when k is even$\}$, $I_2 = \{k : 2\sqrt{r+4} - 3 < k \leq r+1$ when k is odd, or $2\sqrt{r+2} - 2 < k \leq r+1$ when k is even$\}$, $I_3 = \{r+2\}$, $I_4 = \{k : r+3 \leq k \leq r + \sqrt{4r+21} - 2$ when $k-r$ is odd, or $r+4 \leq k \leq r + \sqrt{4r+9} - 1$ when $k - r$ is even$\}$, $I_5 = \{k : r + \sqrt{4r+21} - 2 < k \leq 2r + 2$ when $k - r$ is odd, or $r + \sqrt{4r+9} - 1 < k \leq 2r + 2$ when $k - r$ is even$\}$.

For example, if $r = 3$ then $I = \{0, 1, 2, \cdots, 8\}$, $I_0 = \{0\}$, $I_1 = \{1, 2\}$, $I_2 = \{3, 4\}$, $I_3 = \{5\}$, $I_4 = \{6\}$, $I_5 = \{7, 8\}$. If $r = 4$ then $I = \{0, 1, 2, \cdots, 10\}$, $I_0 = \{0\}$, $I_1 = \{1, 2\}$, $I_2 = \{3, 4, 5\}$, $I_3 = \{6\}$, $I_4 = \{7, 8\}$, $I_5 = \{9, 10\}$.

For any $r \geq 3$, it is easy to see that

$$\bigcup_{i=0}^{5} I_i = I \quad \text{and} \quad I_i \cap I_j = \phi \text{ for } i \neq j. \tag{8}$$

Hence, $\{I_i\}_{i=0}^{5}$ forms a partition of I. This partition is crucial for construction of certain maximum IPP codes of length 3 and derivation of the precise formula for $F(3, q)$ in (5).

4.2 Lower Bounds

For any $q \geq 15$, we first write q in the unique form of $q = r^2 + 2r + k$. According to the value of k based on the partition of I, our construction and lower bounds will be given in six cases. In each

case, we construct an edge colored graph with three bi-color components, and then construct a code associated with it. In all figures in this chapter, we use red, blue and green to represent colors 1, 2 and 3, respectively.

Lemma 4.2.1. Let $q = r^2 + 2r + k$ where $r \geq 3$ and $k \in I_0$. Let $C \subseteq Q^3$ be a maximum IPP code and G be its associated graph. Then $|V(G)| \geq 3r^2$.

Proof. It suffices to construct an IPP graph G_0 with $|V(G_0)| = 3r^2$.

For each $m \in \{1, 2, 3\}$, let $\{i, j\} = \{1, 2, 3\} - \{m\}$. We construct an edge colored graph B_m such that the edges of B_m use both color i and color j, but not color m. Take r disjoint complete graphs R_s^m with $|V(R_s^m)| = r$ $(1 \leq s \leq r)$, and label the vertices of each R_s^m by $v_{s,1}^m, v_{s,2}^m, \cdots, v_{s,r}^m$. Color all edges of each R_s^m with color i. For each $1 \leq t \leq r$, join every pair of vertices from $\{v_{1,t}^m, v_{2,t}^m, \cdots, v_{r,t}^m\}$ by edges of color j. Let B_m denote the resulting edge colored graph.

Note that $|V(B_m)| = r^2$ and the edges of B_m do not use color m. The components of $B_m(i)$ are the graphs R_s^m $(1 \leq s \leq r)$, the components of $B_m(j)$ are the complete graphs with vertex set $\{v_{1,t}^m, v_{2,t}^m, \cdots, v_{r,t}^m\}$ $(1 \leq t \leq r)$, and the components of $B_m(m)$ are the isolated vertices $v_{s,t}^m$ $(1 \leq s, t \leq r)$.

Let G_0 denote the edge colored graph which is the disjoint union of B_1, B_2 and B_3. Next, we show that G_0 is the associated graph of a code $C_0 \subseteq Q^3$. Let

$$C_0^3 = \{(\alpha_s, \alpha_t, \alpha_{(s-1)r+t}) : 1 \leq s, t \leq r\}.$$

Note $C_0^3 \subseteq Q^3$ and the subscript $(s-1)r + t$ ensures that all codewords in C_0^3 have distinct 3rd coordinates. It is straightforward to check that B_3 is the associated graph of C_0^3 by associating $(\alpha_s, \alpha_t, \alpha_{(s-1)r+t})$ to $v_{s,t}^3$ for all $1 \leq s, t \leq r$. Let

$$C_0^1 = \{(\alpha_{sr+t}, \alpha_{r+s}, \alpha_{r^2+t}) : 1 \leq s, t \leq r\}.$$

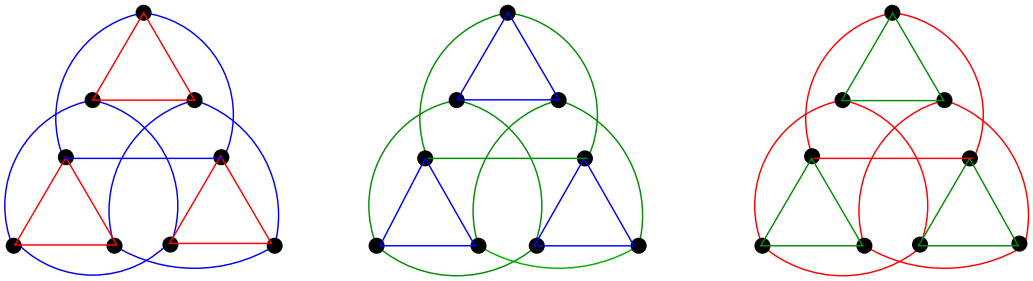
Then $C_0^1 \subseteq Q^3$ and the subscript $sr+t$ ensures that all codewords in C_0^1 have distinct 1st coordinates. It is straightforward to check that B_1 is the associated graph of C_0^1 by associating $(\alpha_{sr+t}, \alpha_{r+s}, \alpha_{r^2+t})$ to $v_{s,t}^1$ for all $1 \leq s, t \leq r$. Let

$$C_0^2 = \{(\alpha_{r^2+r+t}, \alpha_{(s+1)r+t}, \alpha_{r^2+r+s}) : 1 \leq s, t \leq r\}.$$

Then $C_0^2 \subseteq Q^3$ and the subscript $(s+1)r+t$ ensures that all codewords in C_0^2 have distinct 2nd coordinates. It is straightforward to check that B_2 is the associated graph of C_0^2 by associating $(\alpha_{r^2+r+t}, \alpha_{(s+1)r+t}, \alpha_{r^2+r+s})$ to $v_{s,t}^1$ for all $1 \leq s, t \leq r$.

Let $C_0 = C_0^1 \cup C_0^2 \cup C_0^3$. Note that C_0^1, C_0^2, C_0^3 are pairwise disjoint. Since G_0 is the disjoint union of B_1, B_2 and B_3, G_0 is the associated graph of C_0. Since B_1, B_2 and B_3 are bi-color components of G_0, by Lemma 3.2.2, B_1, B_2 and B_3 are IPP graphs. In view of Lemma 3.2.1, G_0 is an IPP graph with $|V(G_0)| = 3r^2$. □

For $r = 3$ and $k = 0$, our construction of an IPP graph G is illustrated in Figure 2. B_3 in Figure 2(a) is a bi-color component whose edges use colors 1 and 2. $B_3(1)$ consists of three pairwise disjoint red triangles, and $B_3(2)$ consists of three pairwise disjoint blue triangles. B_1 in Figure 2(b) is a bi-color component whose edges use colors 2 and 3. $B_1(2)$ consists of three pairwise disjoint blue triangles, and $B_1(3)$ consists of three green triangles. B_2 in Figure 2(c) is a bi-color component whose edges using colors 3 and 1. $B_2(3)$ consists of three pairwise disjoint green triangles, and $B_2(1)$ consists of three pairwise disjoint red triangles. G is the disjoint union of these three bi-color components. Since $|V(B_i)| = 9$ for $1 \leq i \leq 3$, $|V(G)| = 27 = 3r^2$.



(a) Bi−color component B_3 (b) Bi−color component B_1 (c) Bi−color component B_2

Figure 2: An IPP graph $G = B_1 \cup B_2 \cup B_3$ corresponding to $r = 3$, $k = 0$.

We now consider $k \in I_1$.

Lemma 4.2.2. Let $q = r^2 + 2r + k$ where $r \geq 3$, and assume $k \in I_1$. Let $C \subseteq Q^3$ be a maximum IPP code and G be its associated graph. Then $|V(G)| \geq 3r^2 + 3k - 2$.

Proof. Since $k \in I_1$, $1 \leq k \leq 2\sqrt{r+4} - 3$ when k is odd, or $2 \leq k \leq 2\sqrt{r+2} - 2$ when k is even. It suffices to construct an IPP graph G_1 with $|V(G_1)| = 3r^2 + 3k - 2$.

Case 1. k is odd and $1 \le k \le 2\sqrt{r+4} - 3$.

First, we construct a graph B_3 whose edges use color 1 and color 2. For components of $B_3(1)$, we take disjoint complete graphs R_s^3, $1 \le s \le r + 1 - \frac{k-1}{2}$, such that

$$\max\{|V(R_s^3)| : 1 \le s \le r + 1 - \frac{k-1}{2}\} = r + \frac{k-1}{2}$$

and

$$\sum_{s=1}^{r+1-\frac{k-1}{2}} |V(R_s^3)| = r^2 + k - 1 + (\frac{k-1}{2} + 1).$$

This can be done if and only if

$$(r + 1 - \frac{k-1}{2})(r + \frac{k-1}{2}) \ge r^2 + k - 1 + (\frac{k-1}{2} + 1).$$

The above inequality holds if and only if $k \le 2\sqrt{r} - 1$. Note when $r \ge 3$, $2\sqrt{r+4} - 3 \le 2\sqrt{r} - 1$. So the graphs R_s^3 can be well defined when $1 \le k \le 2\sqrt{r+4} - 3$. Now color all edges of each R_s^3 with color 1. To form components of $B_3(2)$ which are also complete graphs, we label the vertices of each R_s^3 by $v_{s,1}^3, v_{s,2}^3, \cdots, v_{s,|V(R_s^3)|}^3$. For each $1 \le t \le r + \frac{k-1}{2}$, let $J_t^3 = \{s : |V(R_s^3)| \ge t\}$ and join every pair of vertices from $\{v_{s,t}^3 : s \in J_t^3\}$ by edges of color 2. Note that $|V(B_3)| = r^2 + k + \frac{k-1}{2}$. Let

$$C_1^3 = \left\{ \begin{array}{c} (\alpha_s, \alpha_t, \alpha_{(\sum_{k=1}^{s-1} |V(R_k^3)|)+t}) : \\ 1 \le s \le r + 1 - \frac{k-1}{2}, 1 \le t \le |V(R_s^3)| \end{array} \right\}.$$

Then $C_1^3 \subseteq Q^3$ and the subscript $\sum_{k=1}^{s-1} |V(R_k^3)|) + t$ ensures that all the codewords in C_1^3 have distinct 3rd coordinates. It is straightforward to check that B_3 is the associated graph of C_1^3 by associating $(\alpha_s, \alpha_t, \alpha_{(\sum_{k=1}^{s-1} |V(R_k^3)|)+t})$ to $v_{s,t}^3$ for all $1 \le s \le r + 1 - \frac{k-1}{2}$ and $1 \le t \le |V(R_s^3)|$.

Next we construct a graph B_1 whose edges use color 2 and color 3. For components of $B_1(2)$, we take disjoint complete graphs R_s^1, $1 \le s \le r + 1 + \frac{k-1}{2}$, such that

$$\max\{|V(R_s^1)| : 1 \le s \le r + 1 + \frac{k-1}{2}\} = r - \frac{k-1}{2}$$

and

$$\sum_{s=1}^{r+1+\frac{k-1}{2}} |V(R_s^1)| = r^2 + k - 1 + \frac{k-1}{2}.$$

This can be done if and only if

$$(r + 1 + \frac{k-1}{2})(r - \frac{k-1}{2}) \ge r^2 + k - 1 + \frac{k-1}{2},$$

which holds if and only if $k \leq 2\sqrt{r+4} - 3$. Therefore, the graphs R_s^1 are well defined. Now color all edges of R_s^1 with color 2. For components of $B_1(3)$, we label the vertices of each R_s^1 by $v_{s,1}^1, v_{s,2}^1, \cdots, v_{s,|V(R_s^1)|}^1$. For each $1 \leq t \leq r - \frac{k-1}{2}$, let $J_t^1 = \{s : |V(R_s^1)| \geq t\}$. Join every pair of vertices from $\{v_{s,t}^1 : s \in J_t^1\}$ by edges of color 3. Note that $|V(B_1)| = r^2 + k - 1 + \frac{k-1}{2}$. Let

$$C_1^1 = \left\{ \begin{array}{c} (\alpha_{r+1-\frac{k-1}{2}+(\sum_{k=1}^{s-1}|V(R_k)|)+t}, \alpha_{r+\frac{k-1}{2}+s}, \alpha_{r^2+k+\frac{k-1}{2}+t}) : \\ 1 \leq s \leq r+1+\frac{k-1}{2}, 1 \leq t \leq |V(R_s^1)| \end{array} \right\}.$$

Then $C_1^1 \subseteq Q^3$ and the subscript $r + 1 - \frac{k-1}{2} + (\sum_{k=1}^{s-1} |V(R_k)|) + t$ ensures that all codewords in C_1^1 have distinct 1st coordinates. It is straightforward to check that B_1 is the associated graph of C_1^1 by associating $(\alpha_{r+1-\frac{k-1}{2}+(\sum_{k=1}^{s-1}|V(R_k)|)+t}, \alpha_{r+\frac{k-1}{2}+s}, \alpha_{r^2+k+\frac{k-1}{2}+t})$ to $v_{s,t}^1$ for all $1 \leq s \leq r + 1 + \frac{k-1}{2}$ and $1 \leq t \leq |V(R_s^1)|$.

Finally, we construct a graph B_2 whose edges use color 3 and color 1. For components of $B_2(3)$, we take r disjoint complete graphs R_s^2 with $|V(R_s)^2| = r$ $(1 \leq s \leq r)$, and assign color 3 to all edges of R_s^2. To form components of $B_2(1)$, we label the vertices of each R_s^2 by $v_{s,1}^2, v_{s,2}^2, \cdots, v_{s,r}^2$. For each $1 \leq t \leq r$, join every pair of vertices from $\{v_{1,t}^2, v_{2,t}^2, \cdots, v_{r,t}^2\}$ by edges of color 1. Note that $|V(B_1)| = r^2$. Let

$$C_1^2 = \left\{ \begin{array}{c} (\alpha_{r^2+r+k+t}, \alpha_{(s+1)r+k+t}, \alpha_{r^2+r+k+s}) : \\ 1 \leq s, t \leq r \end{array} \right\}.$$

Then $C_1^2 \subseteq Q^3$ and the subscript $(s + 1)r + k + t$ ensures that all codewords in C_1^2 have distinct 2nd coordinates. It is straightforward to check that B_2 is the associated graph of $C_1^2 \subseteq Q^3$ by associating $(\alpha_{r^2+r+k+t}, \alpha_{(s+1)r+k+t}, \alpha_{r^2+r+k+s})$ to $v_{s,t}^2$ for all $1 \leq s \leq r$ and $1 \leq t \leq r$.

Now let G_1 denote the disjoint union of B_1, B_2 and B_3, and let $C_1 = C_1^1 \cup C_1^2 \cup C_1^3$. Note that C_1^1, C_1^2, C_1^3 are pairwise disjoint. So G_1 is associated with the code C_1. Since B_1, B_2, B_3 are bi-color components of G_1, it follows from Lemma 3.2.2 that B_1, B_2, B_3 are IPP graphs. Hence, G_1 is an IPP graph by Lemma 3.2.1. Note

$$|V(G_1)| = (r^2 + k + \frac{k-1}{2}) + (r^2 + k - 1 + \frac{k-1}{2}) + r^2 = 3r^2 + 3k - 2.$$

Case 2. k is even and $2 \leq k \leq 2\sqrt{r+2} - 2$.

First, we construct a graph B_3 whose edges use color 1 and color 2. For components of $B_3(1)$,

we take disjoint complete graphs R_s^3, $1 \le s \le r+1-\frac{k}{2}$, such that

$$\max\{|V(R_s^3)| : 1 \le s \le r+1-\frac{k}{2}\} = r+\frac{k}{2}$$

and

$$\sum_{s=1}^{r+1-\frac{k}{2}} |V(R_s^3)| = r^2+k-1+\frac{k}{2}.$$

This can be done if and only if

$$(r+1-\frac{k}{2})(r+\frac{k}{2}) \ge r^2+k-1+\frac{k}{2},$$

and the inequality is true if and only if $k \le 2\sqrt{r+2}-2$. So graphs R_s^3 are well defined. Now color all edges of each R_s^3 with color 1. To form components of $B_3(2)$, we label the vertices of each R_s^3 by $v_{s,1}^3, v_{s,2}^3, \cdots, v_{s,|V(R_s^3)|}^3$. For each $1 \le t \le r+\frac{k}{2}$, let $J_t^3 = \{s : |V(R_s^3)| \ge t\}$ and join every pair of vertices from $\{v_{s,t}^3 : s \in J_t^3\}$ by edges of color 2. Note that $|V(B_3)| = r^2+k-1+\frac{k}{2}$. Let

$$C_1^3 = \left\{ \begin{array}{c} (\alpha_s, \alpha_t, \alpha_{(\sum_{k=1}^{s-1}|V(R_k^3)|)+t}) : \\ 1 \le s \le r+1-\frac{k}{2}, 1 \le t \le |V(R_s^3)| \end{array} \right\}.$$

Then $C_1^3 \subseteq Q^3$ and the subscript $|V(R_k^3)|) + t$ ensures that all codewords in C_1^3 have distinct 3rd coordinates. It is straightforward to check that B_3 is the associated graph of $C_1^3 \subseteq Q^3$ by associating $(\alpha_s, \alpha_t, \alpha_{(\sum_{k=1}^{s-1}|V(R_k^3)|)+t})$ to $v_{s,t}^3$ for all $1 \le s \le r+1-\frac{k}{2}$ and $1 \le t \le |V(R_s^3)|$.

Next we construct a graph B_1 whose edges use color 2 and color 3. For components of $B_1(2)$, we take disjoint complete graphs R_s^1, $1 \le s \le r+\frac{k}{2}$, such that

$$\max\{|V(R_s^1)| : 1 \le s \le r+\frac{k}{2}\} = r+1-\frac{k}{2}$$

and

$$\sum_{s=1}^{r+\frac{k}{2}} |V(R_s^1)| = r^2+k-1+\frac{k}{2}.$$

This can be done if and only if

$$(r+\frac{k}{2})(r+1-\frac{k}{2}) \ge r^2+k-1+\frac{k}{2},$$

which holds if and only if $k \le 2\sqrt{r+2}-2$. So graphs R_s^1 are well defined. Now color all edges of R_s^1 with color 2. To form components of $B_1(3)$, we label the vertices of each R_s^1 by

$v^1_{s,1}, v^1_{s,2}, \cdots, v^1_{s,|V(R^1_s)|}$. For each $1 \le t \le r+1-\frac{k}{2}$, let $J^1_t = \{s : |V(R^1_s)| \ge t\}$. Join every pair of vertices from $\{v^1_{s,t} : s \in J^1_t\}$ by edges of color 3. Note that $|V(B_1)| = r^2 + k - 1 + \frac{k}{2}$. Let

$$C^1_1 = \left\{ \begin{array}{c} (\alpha_{r+1-\frac{k}{2}+(\sum_{k=1}^{s-1}|V(R_k)|)+t}, \alpha_{r+\frac{k}{2}+s}, \alpha_{r^2+k-1+\frac{k}{2}+t}) : \\ 1 \le s \le r+\frac{k}{2}, 1 \le t \le |V(R^1_s)| \end{array} \right\}.$$

Then $C^1_1 \subseteq Q^3$ and the subscript $r+1-\frac{k}{2}+(\sum_{k=1}^{s-1}|V(R_k)|)+t$ ensures that all codewords in C^1_1 have distinct 1st coordinates. It is straightforward to check that B_1 is the associated graph of $C^1_1 \subseteq Q^3$ by associating $(\alpha_{r+1-\frac{k}{2}+(\sum_{k=1}^{s-1}|V(R_k)|)+t}, \alpha_{r+\frac{k}{2}+s}, \alpha_{r^2+k-1+\frac{k}{2}+t})$ to $v^1_{s,t}$ for all $1 \le s \le r+\frac{k}{2}$ and $1 \le t \le |V(R^1_s)|$.

Finally we construct B_2 and the codewords C^2_1 associated to the vertices of B_2 as in Case 1.

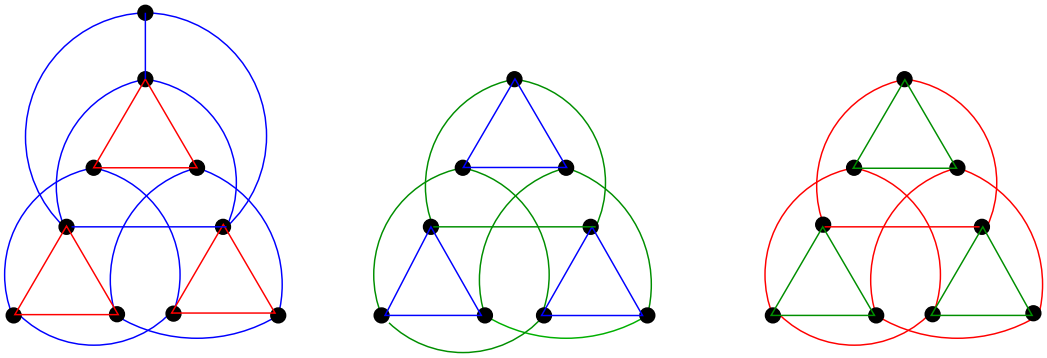
Now let G_1 denote the disjoint union of B_1, B_2 and B_3, and let $C_1 = C^1_1 \cup C^2_1 \cup C^3_1$. Note that C^1_1, C^2_1, C^3_1 are pairwise disjoint. So G_1 is the associated graph of the code C_1. Since B_1, B_2, B_3 are bi-color components of G_1, it follows from Lemma 3.2.2 that B_1, B_2, B_3 are IPP graphs. Hence, G_1 is an IPP graph by Lemma 3.2.1. Note

$$|V(G_1)| = (r^2 + k - 1 + \frac{k}{2}) + (r^2 + k - 1 + \frac{k}{2}) + r^2 = 3r^2 + 3k - 2.$$

□

Corresponding to $r = 3$ and $k = 1$, we describe an example to construct an IPP graph in Figure 3. B_3 in Figure 3(a) is a bi-color component whose edges use colors 1 and 2. $B_3(1)$ consists of three pairwise disjoint red triangles and an isolated vertex, and $B_3(2)$ consists of three pairwise disjoint blue complete graphs with order 3, 3, 4, respectively. B_1 in Figure 3(b) is a bi-color component whose edges use colors 2 and 3, and B_2 in Figure 3(c) is a bi-color component whose edges use colors 3 and 1. B_1 and B_2 are constructed in the same way as in Figure 2(b) and Figure 2(c). G is the disjoint union of these three bi-color components. Since $|V(B_3)| = 10$ and $|V(B_i)| = 9$ for $1 \le i \le 2$, $|V(G)| = 28 = 3r^2 + 3k - 2$.

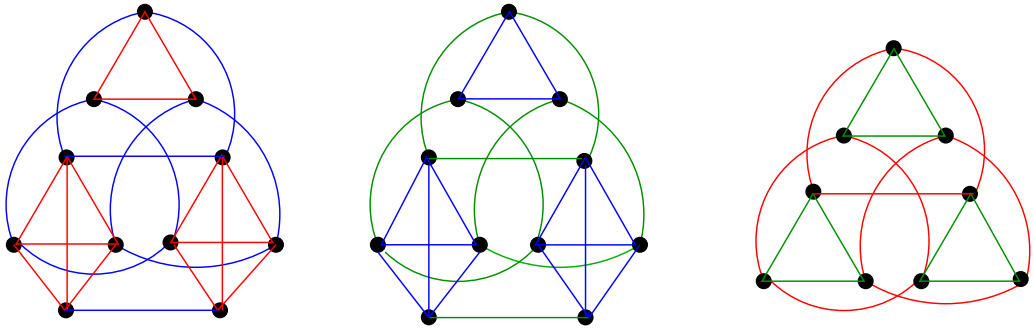
For $r = 3$ and $k = 2$, we describe an example to construct an IPP graph in Figure 4. B_3 in Figure 4(a) is a bi-color component whose edges use colors 1 and 2. $B_3(1)$ consists of three pairwise disjoint red complete graphs with order 3, 4, 4, respectively. $B_3(2)$ consists of four pairwise disjoint blue complete graphs with order 2, 3, 3, 3, respectively. B_1 in Figure 4(b) is a bi-color component whose edges use colors 2 and 3. $B_1(2)$ consists of three pairwise disjoint blue complete graphs with order 3, 4, 4, respectively, and $B_1(3)$ consists of four pairwise disjoint green complete graphs with



(a) Bi–color component B_3 (b) Bi–color component B_1 (c) Bi–color component B_2

Figure 3: An IPP graph $G = B_1 \cup B_2 \cup B_3$ corresponding to $r = 3$, $k = 1$.

order 2, 3, 3, 3, respectively. B_2 in Figure 4(c) is a bi-color component whose edges use colors 3 and 1. $B_2(3)$ consists of three pairwise disjoint green triangles, and $B_2(1)$ consists of three pairwise disjoint red triangles. G is the disjoint union of these three bi-color components. Since $|V(B_2)| = 9$ and $|V(B_1)| = |V(B_3)| = 11$, $|V(G)| = 31 = 3r^2 + 3k - 2$.



(a) Bi–color component B_3 (b) Bi–color component B_1 (c) Bi–color component B_2

Figure 4: An IPP graph $G = B_1 \cup B_2 \cup B_3$ corresponding to $r = 3$, $k = 2$.

We now consider $k \in I_2$.

Lemma 4.2.3. Let $q = r^2 + 2r + k$ with $r \geq 3$, and assume $k \in I_2$. Let $C \subseteq Q^3$ be a maximum IPP code and G be its associated graph. Then $|V(G)| \geq 3r^2 + 3k - 3$.

Proof. Since $k \in I_2$, $2\sqrt{r+4} - 3 < k \leq r + 1$ when k is odd, and $2\sqrt{r+2} - 2 < k \leq r + 1$ when k is even. It suffices to construct an IPP graph G_2 with $|V(G_2)| = 3r^2 + 3k - 3$.

For each $1 \le m \le 3$, let $\{i, j\} = \{1, 2, 3\} - \{m\}$, and let B_1, B_2, B_3 be obtained as in the proof of Lemma 4.2.1. Let B'_m be obtained from B_m by adding $k-1$ vertices $v^m_{s,r+1}$ $(1 \le s \le k-1)$, joining $v^m_{s,r+1}$ to each of $\{v^m_{s,1}, v^m_{s,2}, \cdots, v^m_{s,r}\}$ by an edge of color i for all $1 \le s \le k-1$, and joining every pair of vertices from $\{v^m_{1,r+1}, v^m_{2,r+1}, \cdots, v^m_{k-1,r+1}\}$ by an edge of color j.

Let G_2 denote the disjoint union of B'_1, B'_2, B'_3. Let X_m, $1 \le m \le 3$, denote the set of codewords corresponding to the $k-1$ vertices added to B_m, where

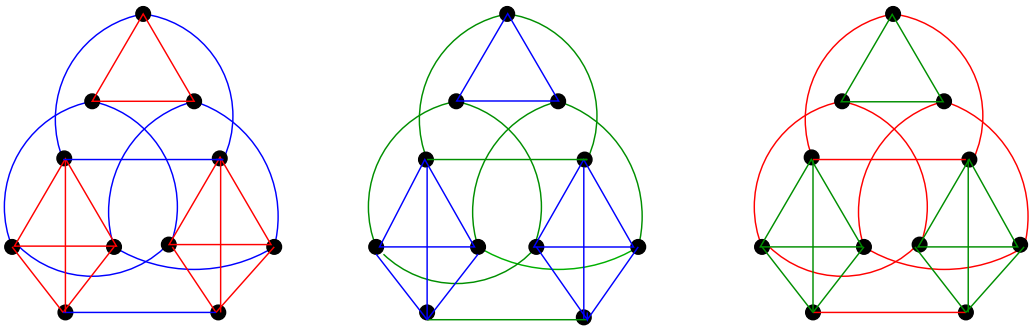
$$X_3 = \{(\alpha_s, \alpha_{r^2+2r+1}, \alpha_{r^2+2r+s}), 1 \le s \le k-1\},$$
$$X_1 = \{(\alpha_{r^2+2r+s}, \alpha_{r+s}, \alpha_{r^2+2r+k}), 1 \le s \le k-1\},$$
$$X_2 = \{(\alpha_{r^2+2r+k}, \alpha_{r^2+2r+1+s}, \alpha_{r^2+r+s}), 1 \le s \le k-1\}.$$

One can check that C_0, X_1, X_2, X_3 are pairwise disjoint, and G_2 is associated with the code $C_2 := C_0 \cup X_3 \cup X_1 \cup X_2$. Since B'_1, B'_2, B'_3 are bi-color components of G_2, B'_1, B'_2, B'_3 are IPP graphs by Lemma 3.2.2. Hence G_2 is an IPP graph by Lemma 3.2.1. Note

$$|V(G_2)| = 3r^2 + 3(k-1) = 3r^2 + 3k - 3.$$

□

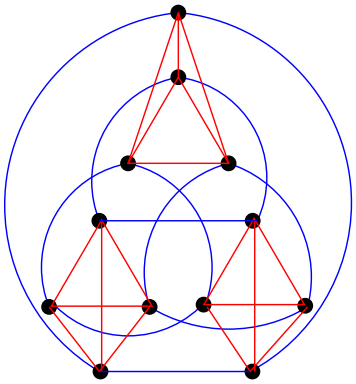
For $r = 3$ and $k = 3$, we describe our construction of an IPP graph in Figure 5. B_3 in Figure 5(a) is a bi-color component whose edges use colors 1 and 2 and B_1 in Figure 5(b) is a bi-color component whose edges use colors 2 and 3. B_3 and B_1 are constructed in the same way as in Figure 4(a) and Figure 4(b). B_2 has the same structure as B_3 except using different colors. Let G be the disjoint union of the three bi-color components. Since $|V(B_i)| = 11$ for $1 \le i \le 3$, $|V(G)| = 3r^2 + 3k - 3$.



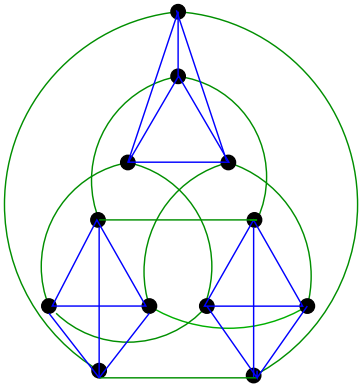
(a) Bi−color component B_3 (b) Bi−color component B_1 (c) Bi−color component B_2

Figure 5: An IPP graph $G = B_1 \cup B_2 \cup B_3$ corresponding to $r = 3$, $k = 3$.

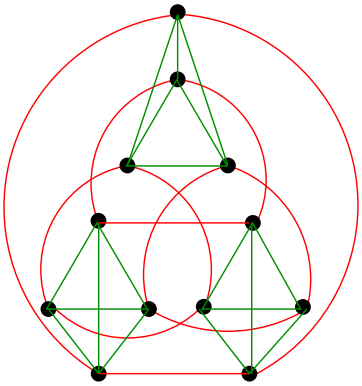
For $r = 3$ and $k = 4$, we describe an example to construct an IPP graph in Figure 6. B_3 in Figure 6(a) is a bi-color component whose edges use colors 1 and 2. $B_3(1)$ consists of three pairwise disjoint red complete graphs with order 4, 4, 4, respectively, and $B_3(2)$ consists of four pairwise disjoint blue triangles. B_1 in Figure 6(b) is a bi-color component whose edges use colors 2 and 3, and B_2 in Figure 6(c) is a bi-color component whose edges use colors 3 and 1. B_1 and B_2 have the same structure as B_3 except using different colors. Let G be the disjoint union of B_1, B_2, B_3. Since $|V(B_i)| = 12$ for $1 \leq i \leq 3$, $|V(G)| = 3r^2 + 3k - 3$.



(a) Bi−color component B_3



(b) Bi−color component B_1



(c) Bi−color component B_2

Figure 6: An IPP graph $G = B_1 \cup B_2 \cup B_3$ corresponding to $r = 3$, $k = 4$.

Now we consider $k \in I_3 = \{r + 2\}$.

Lemma 4.2.4. Let $q = r^2 + 2r + k$ with $r \geq 3$, and $k \in I_3$. Let $C \subseteq Q^3$ be a maximum IPP code and G be its associated graph. Then $|V(G)| \geq 3r^2 + 3k - 4$.

Proof. Since $k \in I_3$, $k = r + 2$. It suffices to construct an IPP graph G_3 with $|V(G_3)| = 3r^2 + 3k - 4$.

First, we construct a graph B_3 whose edges use color 1 and color 2. For components of $B_3(1)$, we take disjoint complete graphs R_s^3, $1 \le s \le r + 1$, such that

$$\max\{|V(R_s^3)| : 1 \le s \le r + 1\} = r + 1$$

and

$$\sum_{s=1}^{r+1} |V(R_s^3)| = r^2 + r + 2.$$

This can be done because $(r + 1)(r + 1) \ge r^2 + r + 2$ when $r \ge 1$. Now assign color 1 to all edges of each R_s. To form components of $B_3(2)$, we label the vertices of each R_s^3 by $v_{s,1}^3, v_{s,2}^3, \cdots, v_{s,|V(R_s^3)|}^3$. For each $1 \le t \le r + 1$, let $J_t^3 = \{s : |V(R_s^3)| \ge t\}$ and join every pair of vertices from $\{v_{s,t}^3 : s \in J_t^3\}$ by edges of color 2. Note that $|V(B_3)| = r^2 + r + 2$. Let

$$C_3^3 = \left\{ \begin{array}{c} (\alpha_s, \alpha_t, \alpha_{(\sum_{k=1}^{s-1} |V(R_k^3)|)+t}) : \\ 1 \le s \le r + 1, 1 \le t \le |V(R_s^3)| \end{array} \right\}.$$

Then $C_3^3 \subseteq Q^3$ and the subscript $|V(R_k^3)|) + t$ ensures that all codewords in C_3^3 have distinct 3rd coordinates. It is straightforward to check that B_3 is the associated graph of C_3^3 by associating $(\alpha_s, \alpha_t, \alpha_{(\sum_{k=1}^{s-1} |V(R_k^3)|)+t})$ to $v_{s,t}^3$ for all $1 \le s \le r + 1$ and $1 \le t \le |V(R_s^3)|$.

Next we construct a graph B_1 whose edges use color 2 and color 3. For components of $B_1(2)$, we take disjoint complete graphs R_s^1, $1 \le s \le r + 1$, such that $|V(R_s^1)| = r$, and color all edges of R_s^1 with color 2. To form components of $B_1(3)$, we label the vertices of each R_s^1 by $v_{s,1}^1, v_{s,2}^1, \cdots, v_{s,r}^1$. Join every pair of vertices from $\{v_{s,t}^1 : 1 \le t \le r\}$ by edges of color 3. Note that $|V(B_1)| = r^2 + r$. Let

$$C_3^1 = \left\{ \begin{array}{c} (\alpha_{(r+1)t+s}, \alpha_{r+1+s}, \alpha_{r^2+r+2+t}) : \\ 1 \le s \le r + 1, 1 \le t \le r \end{array} \right\}.$$

Then $C_3^1 \subseteq Q^3$ and the subscript $(r + 1)t + s$ ensures that all codewords in C_3^1 have distinct 1st coordinates. It is straightforward to check that B_1 is the associated graph of C_3^1 by associating $(\alpha_{(r+1)t+s}, \alpha_{r+1+s}, \alpha_{r^2+r+2+t})$ to $v_{s,t}^1$ for all $1 \le s \le r + 1$ and $1 \le t \le r$.

Finally, we construct a graph B_2 whose edges use color 3 and color 1. To form components $B_2(3)$, take disjoint complete graphs R_s^2, $1 \le s \le r$, such that $V(R_s^2)| = r+1$, and color all edges of R_s^2 with color 3. To form components of $B_2(1)$, we label the vertices of each R_s^2 by $v_{s,1}^2, v_{s,2}^2, \cdots, v_{s,r+1}^2$.

Join every pair of vertices from $\{v^2_{s,t} : 1 \le t \le r+1\}$ by edges of color 1. Note that $|V(B_2)| = r^2 + r$. Let

$$C_3^2 = \left\{ \begin{array}{c} (\alpha_{r^2+2r+1+t}, \alpha_{2r+2+(s-1)(r+1)+t}, \alpha_{r^2+2r+2+s}) : \\ 1 \le s \le r, 1 \le t \le r+1 \end{array} \right\}.$$

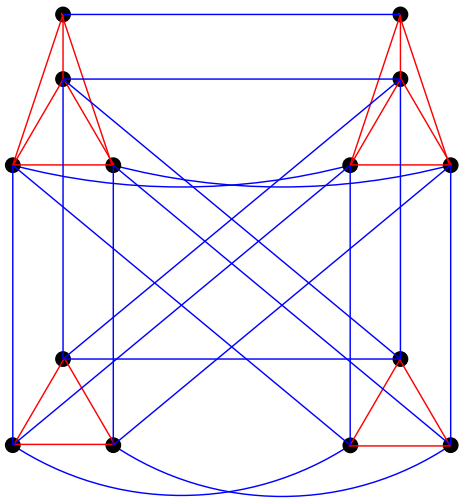
Then $C_3^2 \subseteq Q^3$ and the subscript $2r + 2 + (s-1)(r+1) + t$ ensures that all codewords in C_3^2 have distinct 2nd coordinates. It is straightforward to check that B_2 is the associated graph of C_3^2 by associating $(\alpha_{r^2+2r+1+t}, \alpha_{2r+2+(s-1)(r+1)+t}, \alpha_{r^2+2r+2+s})$ to $v^2_{s,t}$ for all $1 \le s \le r+1$ and $1 \le t \le r$.

Now let G_3 denote the disjoint union of B_1, B_2 and B_3, and let $C_3 = C_3^1 \cup C_3^2 \cup C_3^3$. Note that C_3^1, C_3^2, C_3^3 are pairwise disjoint. So G_3 is associated with the code C_3. Since B_1, B_2, B_3 are bi-color components of G_3, it follows from Lemma 3.2.2 that B_1, B_2, B_3 are IPP graphs. Hence, G_3 is an IPP graph by Lemma 3.2.1. Note

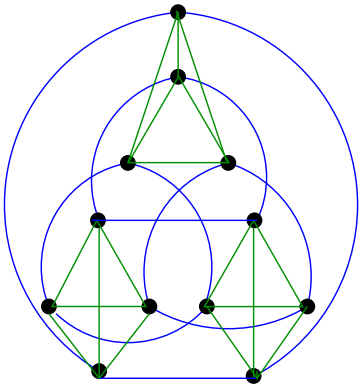
$$|V(G_3)| = (r^2 + r + 2) + (r^2 + r) + (r^2 + r) = 3r^2 + 3k - 4.$$

□

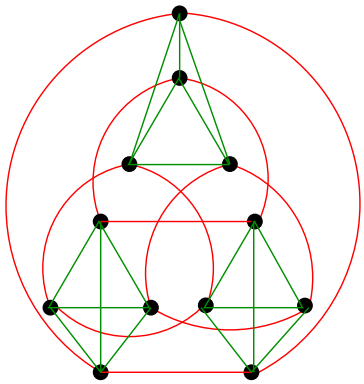
For $r = 3$ and $k = 5$, we describe an example to construct an IPP graph in Figure 7. B_3 in Figure 7(a) is a bi-color component whose edges use colors 1 and 2. $B_3(1)$ consists of four pairwise disjoint red complete graphs with order 3, 3, 4, 4, respectively, and $B_3(2)$ consists of four pairwise disjoint blue complete graphs with order 2, 4, 4, 4, respectively. B_1 in Figure 7(b) is a bi-color component whose edges use colors 2 and 3, and B_2 in Figure 7(c) is a bi-color component whose edges use colors 3 and 1. B_1 and B_2 are identical to Figure 6(b) and Figure 6(c), respectively. Let G be the disjoint union of B_1, B_2, B_3. Since $|V(B_3)| = 14$ and $|V(B_1)| = |V(B_2)| = 12$, $|V(G)| = 3r^2 + 3k - 4$.



(a) Bi−color component B_3



(b) Bi−color component B_1



(c) Bi−color component B_2

Figure 7: An IPP graph $G = B_1 \cup B_2 \cup B_3$ corresponding to $r = 3$, $k = 5$.

We now consider $k \in I_4$.

Lemma 4.2.5. Let $q = r^2 + 2r + k$ with $r \geq 3$, and assume $k \in I_4$. Let $C \subseteq Q^3$ be a maximum IPP code and G be its associated graph. Then $|V(G)| \geq 3r^2 + 3k - 5$.

Proof. Since $k \in I_4$, $r+3 \leq k \leq r + \sqrt{4r+21} - 2$ when $k - r$ is odd, and $r+4 \leq k \leq r + \sqrt{4r+9} - 1$ when $k - r$ is even. It suffices to construct an IPP graph G_4 with $|V(G_4)| = 3r^2 + 3k - 5$.

Case 1. $k - r$ is odd and $r + 3 \leq k \leq r + \sqrt{4r+21} - 2$.

First we construct B_3 whose edges use color 1 and color 2. To form components $B_3(1)$, we take

disjoint complete graphs R_s^3, $1 \le s \le r+2-\frac{k-r-1}{2}$, such that

$$\max\{|V(R_s^3)| : 1 \le s \le r+2-\frac{k-r-1}{2}\} = r+\frac{k-r-1}{2}$$

and

$$\sum_{s=1}^{r+2-\frac{k-r-1}{2}} |V(R_s^3)| = r^2+k-2+(\frac{k-r-1}{2}+1).$$

This can be done if and only if

$$(r+2-\frac{k-r-1}{2})(r+\frac{k-r-1}{2}) \ge r^2+k-2+(\frac{k-r-1}{2}+1),$$

which holds if and only if $k \le r+\sqrt{4r+1}$. In particular, the inequality holds when $r+3 \le k \le r+\sqrt{4r+21}-2$. Hence, R_s^3 are well defined. Now color all edges of each R_s^3 with color 1. To form components of $B_3(2)$, we label the vertices of each R_s^3 by $v_{s,1}^3, v_{s,2}^3, \cdots, v_{s,|V(R_s^3)|}^3$. For each $1 \le t \le r+\frac{k-r-1}{2}$, let $J_t^3 = \{s : |V(R_s^3)| \ge t\}$ and join every pair of vertices from $\{v_{s,t}^3 : s \in J_t^3\}$ by edges of color 2. Note that $|V(B_3)| = r^2+k+\frac{k-r-1}{2}-1$. Let

$$C_4^3 = \left\{ \begin{array}{c} (\alpha_s, \alpha_t, \alpha_{(\sum_{k=1}^{s-1}|V(R_k^3)|)+t}) : \\ 1 \le s \le r+2-\frac{k-r-1}{2}, 1 \le t \le |V(R_s^3)| \end{array} \right\}.$$

Then $C_4^3 \subseteq Q^3$ and the subscript $(\sum_{k=1}^{s-1}|V(R_k^3)|)+t$ ensures that all codewords in C_4^3 have distinct 3rd coordinates. It is straightforward to check that B_3 is the associated graph of C_4^3 by associating $(\alpha_s, \alpha_t, \alpha_{(\sum_{k=1}^{s-1}|V(R_k^3)|)+t})$ to $v_{s,t}^3$ for all $1 \le s \le r+2-\frac{k-r-1}{2}$ and $1 \le t \le |V(R_s^3)|$.

Now construct B_1. To form components of $B_1(2)$, we take disjoint complete graphs R_s^1, $1 \le s \le r+1+\frac{k-r-1}{2}$, such that

$$\max\{|V(R_s^1)| : 1 \le s \le r+1+\frac{k-r-1}{2}\} = r+1-\frac{k-r-1}{2}$$

and

$$\sum_{s=1}^{r+1+\frac{k-r-1}{2}} |V(R_s^1)| = r^2+k-2+(\frac{k-r-1}{2}-1).$$

This can be done if and only if

$$(r+1+\frac{k-r-1}{2})(r+1-\frac{k-r-1}{2}) \ge r^2+k-2+(\frac{k-r-1}{2}-1),$$

which, in turn, holds if and only if $k \le r+\sqrt{4r+21}-2$. Now color all edges of R_s^1 with color 2. To form the components of $B_1(3)$, we label the vertices of each R_s^1 by $v_{s,1}^1, v_{s,2}^1, \cdots, v_{s,|V(R_s^1)|}^1$. For each

$1 \le t \le r+1-\frac{k-r-1}{2}$, let $J_t^1 = \{s : |V(R_s^1)| \ge t\}$. Join every pair of vertices from $\{v_{s,t}^1 : s \in J_t^1\}$ by edges of color 3. Note that $|V(B_1)| = r^2 + k + \frac{k-r-1}{2} - 3$. Let

$$C_4^1 = \left\{ \begin{array}{c} (\alpha_{r+2-\frac{k-r-1}{2}+(\sum_{k=1}^{s-1}|V(R_k)|)+t}, \alpha_{r+\frac{k-r-1}{2}+s}, \alpha_{r^2+k+\frac{k-r-1}{2}-3+t}) : \\ 1 \le s \le r+1+\frac{k-r-1}{2}, 1 \le t \le |V(R_s^1)| \end{array} \right\}.$$

Then $C_4^1 \subseteq Q^3$ and the subscript $r+2-\frac{k-r-1}{2}+(\sum_{k=1}^{s-1}|V(R_k)|)+t$ ensures that all codewords in C_4^1 have distinct 1st coordinates. It is straightforward to check that B_1 is the associated graph of C_4^1 by associating $(\alpha_{r+2-\frac{k-r-1}{2}+(\sum_{k=1}^{s-1}|V(R_k)|)+t}, \alpha_{r+\frac{k-r-1}{2}+s}, \alpha_{r^2+k+\frac{k-r-1}{2}-3+t})$ to $v_{s,t}^1$ for all $1 \le s \le r+1+\frac{k-r-1}{2}$ and $1 \le t \le |V(R_s^1)|$.

Finally, we construct a graph B_2 whose edges use color 1 and color 3. To form components of $B_2(3)$, we take disjoint complete graphs R_s^2, $1 \le s \le r+1$, such that $|V(R_s^1)| = r$. Color all edges of R_s^1 with color 3. To form components of $B_2(1)$, we label the vertices of each R_s^3 by $v_{s,1}^1, v_{s,2}^1, \cdots, v_{s,r}^3$. Join every pair of vertices from $\{v_{s,t}^1 : 1 \le t \le r\}$ by edges of color 1. Note that $|V(B_2)| = r^2 + r$. Let

$$C_4^2 = \left\{ \begin{array}{c} (\alpha_{r^2+r+k+t}, \alpha_{r+k+(s-1)r+t}, \alpha_{r^2+r+k-1+s}) : \\ 1 \le s \le r+1, 1 \le t \le r \end{array} \right\}.$$

Then $C_4^2 \subseteq Q^3$ and the subscript $r+k+(s-1)r+t$ ensures that all codewords in C_4^2 have distinct 2nd coordinates. It is straightforward to check that B_2 is the associated graph of C_4^2 by associating $(\alpha_{r^2+r+k+t}, \alpha_{r+k+(s-1)r+t}, \alpha_{r^2+r+k-1+s})$ to $v_{s,t}^2$ for all $1 \le s \le r+1$ and $1 \le t \le r$.

Now let G_4 denote the disjoint union of B_1, B_2 and B_3, and let $C_4 = C_4^1 \cup C_4^2 \cup C_4^3$. Note that C_4^1, C_4^2, C_4^3 are pairwise disjoint. So G_4 is associated with the code C_4. Since B_1, B_2, B_3 are bi-color components of G_4, it follows from Lemma 3.2.2 that B_1, B_2, B_3 are IPP graphs. Hence, G_4 is an IPP graph by Lemma 3.2.1. Note

$$|V(G_4)| = (r^2 + k + \frac{k-r-1}{2} - 1) + (r^2 + k + \frac{k-r-1}{2} - 3) + (r^2 + r) = 3r^2 + 3k - 5.$$

Case 2. $k - r$ is even and $r + 4 \le k \le r + \sqrt{4r+9} - 1$.

Construction of B_3 whose edges use color 1 and color 2. To form components of $B_3(1)$, we take disjoint complete graphs R_s^3, $1 \le s \le r+1-\frac{k-r-2}{2}$ such that

$$\max\{|V(R_s^3)| : 1 \le s \le r+1-\frac{k-r-2}{2}\} = r+1+\frac{k-r-2}{2}$$

and

$$\sum_{s=1}^{r+1-\frac{k-r-2}{2}} |V(R_s^3)| = r^2 + k - 2 + (\frac{k-r-2}{2} + 1).$$

This can be done if and only if

$$(r + 1 - \frac{k-r-2}{2})(r + 1 + \frac{k-r-2}{2}) \geq r^2 + k - 2 + (\frac{k-r-2}{2} + 1),$$

which, in turn, holds if and only if $k \leq r + \sqrt{4r+9} - 1$. Now color all edges of each R_s with color 1. To form components of $B_3(2)$, we label the vertices of each R_s^3 by $v_{s,1}^3, v_{s,2}^3, \cdots, v_{s,|V(R_s^3)|}^3$. For each $1 \leq t \leq r + 1 + \frac{k-r-2}{2}$, let $J_t^3 = \{s : |V(R_s^3)| \geq t\}$ and join every pair of vertices from $\{v_{s,t}^3 : s \in J_t^3\}$ by edges of color 2. Note that $|V(B_3)| = r^2 + k + \frac{k-r-2}{2} - 1$. Let

$$C_4^3 = \left\{ \begin{array}{c} (\alpha_s, \alpha_t, \alpha_{(\sum_{k=1}^{s-1} |V(R_k^3)|)+t}) : \\ 1 \leq s \leq r + 1 - \frac{k-r-2}{2}, 1 \leq t \leq |V(R_s^3)| \end{array} \right\}.$$

Then $C_4^3 \subseteq Q^3$ and the subscript $(\sum_{k=1}^{s-1} |V(R_k^3)|) + t$ shows that all codewords in C_4^3 have distinct 3rd coordinates. It is straightforward to check that B_3 is the associated graph of C_4^3 by associating $(\alpha_s, \alpha_t, \alpha_{(\sum_{k=1}^{s-1} |V(R_k^3)|)+t})$ to $v_{s,t}^3$ for all $1 \leq s \leq r + 1 - \frac{k-r-2}{2}$ and $1 \leq t \leq |V(R_s^3)|$.

Construction of B_1 whose edges use color 2 and color 3. To form components of $B_1(2)$, we take disjoint complete graphs R_s^1, $1 \leq s \leq r + 1 + \frac{k-r-2}{2}$, such that

$$\max\{|V(R_s^1)| : 1 \leq s \leq r + 2 + h\} = r + 1 - \frac{k-r-2}{2}$$

and

$$\sum_{s=1}^{r+2+h} |V(R_s^1)| = r^2 + k - 2 + \frac{k-r-2}{2}.$$

This can be done if and only if

$$(r + 1 + \frac{k-r-2}{2})(r + 1 - \frac{k-r-2}{2}) \geq r^2 + k - 2 + \frac{k-r-2}{2},$$

which holds if and only $k \leq r + \sqrt{4r+13} - 1$. In particular, it holds with $k \leq r + \sqrt{4r+9} - 1$. So R_s^1 are well defined. Now color all edges of R_s^1 with color 2. To form components of $B_1(3)$, we label the vertices of each R_s^1 by $v_{s,1}^1, v_{s,2}^1, \cdots, v_{s,|V(R_s^1)|}^1$. For each $1 \leq t \leq r+1-\frac{k-r-2}{2}$, let $J_t^1 = \{s : |V(R_s^1)| \geq t\}$. Join every pair of vertices from $\{v_{s,t}^1 : s \in J_t^1\}$ by edges of color 3. Let B_1 denote the resulting edge colored graph. Note that $|V(B_1)| = r^2 + k - 2 + \frac{k-r-2}{2}$. Let

$$C_4^1 = \left\{ \begin{array}{c} (\alpha_{r+1-\frac{k-r-2}{2}+(\sum_{k=1}^{s-1} |V(R_k)|)+t}, \alpha_{r+1+\frac{k-r-2}{2}+s}, \alpha_{r^2+k+\frac{k-r-2}{2}-1+t}) : \\ 1 \leq s \leq r + 1 + \frac{k-r-2}{2}, 1 \leq t \leq |V(R_s^1)| \end{array} \right\}.$$

Then $C_4^1 \subseteq Q^3$ and the subscript $r+1-\frac{k-r-2}{2}+(\sum_{k=1}^{s-1}|V(R_k)|)+t$ shows that all codewords in C_4^1 have distinct 1st coordinates. It is straightforward to check that B_1 is the associated graph of C_4^1 by associating $(\alpha_{r+1-\frac{k-r-2}{2}+(\sum_{k=1}^{s-1}|V(R_k)|)+t}, \alpha_{r+1+\frac{k-r-2}{2}+s}, \alpha_{r^2+k+\frac{k-r-2}{2}-1+t})$ to $v_{s,t}^1$ for all $1 \leq s \leq r+1+\frac{k-r-2}{2}$ and $1 \leq t \leq |V(R_s^1)|$.

Let B_2 and C_4^2 be obtained as in the proof of Case 1.

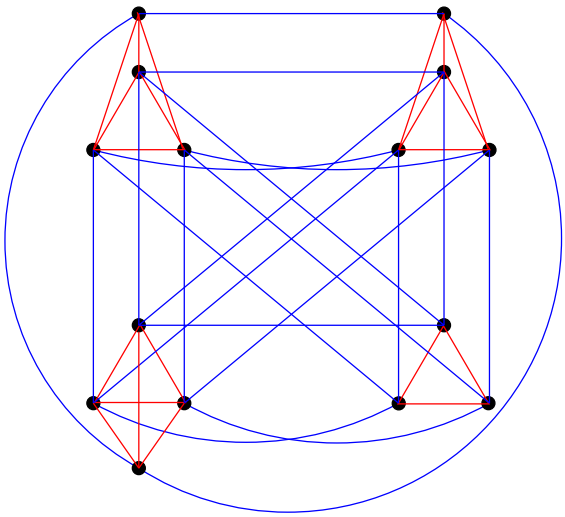
Now let G_4 denote the disjoint union of B_1, B_2 and B_3, and let $C_4 = C_4^1 \cup C_4^2 \cup C_4^3$. Note that C_4^1, C_4^2, C_4^3 are pairwise disjoint. So G_4 is associated with the code C_4. Since B_1, B_2, B_3 are bi-color components of G_4, it follows from Lemma 3.2.2 that B_1, B_2, B_3 are IPP graphs. Hence, G_4 is an IPP graph by Lemma 3.2.1. Note

$$|V(G_4)| = (r^2 + k + \frac{k-r-2}{2} - 1) + (r^2 + k - 2 + \frac{k-r-2}{2}) + (r^2 + r) = 3r^2 + 3k - 5.$$

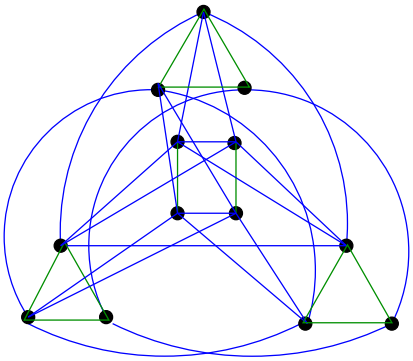
□

Corresponding to $r = 3$ and $k = 6$, we describe how to construct an IPP graph in Figure 8. B_3 in Figure 8(a) is a bi-color component whose edges use colors 1 and 2. $B_3(1)$ consists of four pairwise disjoint red complete graphs with order 3, 4, 4, 4, respectively, and $B_3(2)$ consists of four pairwise disjoint blue complete graphs with order 3, 4, 4, 4, respectively. B_1 in Figure 8(b) is a bi-color component whose edges use colors 2 and 3. $B_1(3)$ consists of five pairwise disjoint blue complete graphs with order 2, 2, 3, 3, 3, respectively, and $B_1(2)$ consists of three pairwise disjoint blue complete graphs with order 4, 4, 3, respectively. B_2 in Figure 8(c) is a bi-color component whose edges use colors 3 and 1, and B_2 is identical to Figure 7(c). Let G be the disjoint union of B_1, B_2, B_3. Since $|V(B_3)| = 14$, $|V(B_1)| = 13$ and $|V(B_2)| = 12$, $|V(G)| = 3r^2 + 3k - 5$.

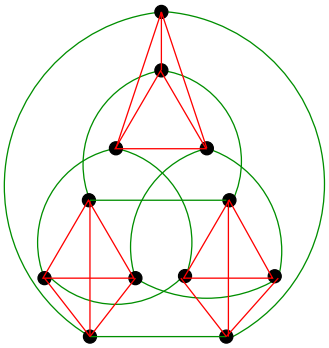
For $r = 3$, the set $\{k : r+4 \leq k \leq r + \sqrt{4r+9} - 1$ and $k - r$ is even$\}$ is empty. That is why no example is provided for this case.



(a) Bi–color component B_3



(b) Bi–color component B_1



(c) Bi–color component B_2

Figure 8: An IPP graph $G = B_1 \cup B_2 \cup B_3$ corresponding to $r = 3$, $k = 6$.

Now we consider $k \in I_5$.

Lemma 4.2.6. Let $q = r^2 + 2r + k$ with $r \geq 3$, and assume $k \in I_5$. Let $C \subseteq Q^3$ be a maximum IPP code and G be its associated graph. Then $|V(G)| \geq 3r^2 + 3k - 6$.

Proof. Since $k \in I_5$, $r + \sqrt{4r+21} - 2 < k \leq 2r+2$ when $k-r$ is odd, and $r + \sqrt{4r+9} - 1 < k \leq 2r+2$ when $k - r$ is even. It suffices to construct an IPP graph G_5 with $|V(G_5)| = 3r^2 + 3k - 6$.

For each $1 \leq m \leq 3$, let $\{i, j\} = \{1, 2, 3\} - \{m\}$, and let B'_m be obtained as in the proof of Lemma 4.2.3. Let B''_m be obtained from B'_m by adding $k - r - 2$ vertices $v^m_{s,r+2}$ $(1 \leq s \leq k - r - 2)$, joining $v^m_{s,r+2}$ to each vertex of $\{v^m_{s,1}, v^m_{s,2}, \cdots, v^m_{s,r+1}\}$ by an edge of color i for all $1 \leq s \leq k - r - 2$,

and joining every pair of vertices from $\{v^m_{1,r+2}, v^m_{2,r+2}, \cdots, v^m_{k-r-2,r+2}\}$ by an edge of color j.

Let Y_m, $1 \le m \le 3$, denote the set of codewords corresponding to the $k-r-2$ vertices added to B'_m, where

$$Y_3 = \{(\alpha_s, \alpha_{r^2+3r+2}, \alpha_{r^2+3r+1+s}), 1 \le s \le k-r-2\},$$
$$Y_1 = \{(\alpha_{r^2+3r+1+s}, \alpha_{r+s}, \alpha_{r^2+2r+k}), 1 \le s \le k-r-2\},$$
$$Y_2 = \{(\alpha_{r^2+2r+k}, \alpha_{r^2+3r+2+s}, \alpha_{r^2+r+s}), 1 \le s \le k-r-2\}.$$

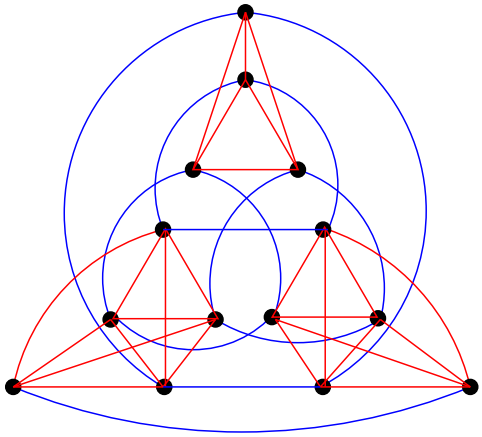
Let G_5 denote the disjoint union of B''_1, B''_2 and B''_3, and let $C_5 := C_3 \cup Y_3 \cup Y_1 \cup Y_2$. Note that C_3, Y_3, Y_1, Y_2 are pairwise disjoint. So G_5 is associated with the code C_5. By Lemma 3.2.2, B''_m is an IPP graph for each $1 \le m \le 3$. Therefore, G_5 is an IPP graph by Lemma 3.2.1. Note

$$|V(G_5)| = 3r^2 + 3r + 3(k-r-2) = 3r^2 + 3k - 6.$$

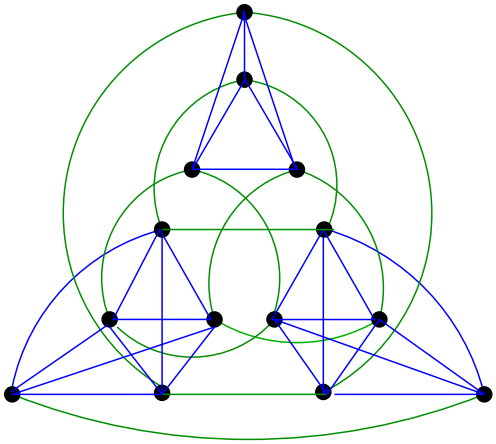
□

Corresponding to $r = 3$ and $k = 7$, we describe how to construct an IPP graph in Figure 9. B_3 in Figure 9(a) is a bi-color component whose edges use colors 1 and 2. $B_3(1)$ consists of three pairwise disjoint red complete graphs with order 4, 5, 5, respectively, and $B_3(2)$ consists of five pairwise disjoint blue complete graphs with order 2, 3, 3, 3, 3, respectively. B_1 in Figure 9(b) is a bi-color component whose edges use colors 2 and 3, and B_2 in Figure 9(c) is a bi-color component whose edges use colors 3 and 1. B_1 and B_2 have the same structure as B_3 except using different colors. Let G be the disjoint union of B_1, B_2, B_3. Since $|V(B_i)| = 14$ for $1 \le i \le 3$, $|V(G)| = 3r^2 + 3k - 6$.

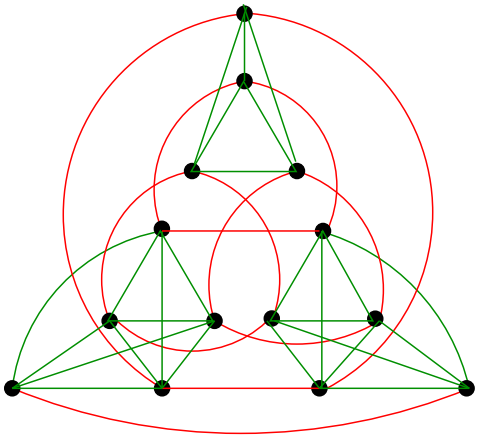
Corresponding to $r = 3$ and $k = 8$, we describe how to construct an IPP graph in Figure 10. B_3 in Figure 10(a) is a bi-color component whose edges use colors 1 and 2. $B_3(1)$ consists of three pairwise disjoint red complete graphs with order 5, 5, 5, respectively, and $B_3(2)$ consists of five pairwise disjoint blue complete graphs with order 3, 3, 3, 3, 3, respectively. B_1 in Figure 10(b) is a bi-color component whose edges use colors 2 and 3, and B_2 in Figure 10(c) is a bi-color component whose edges use colors 3 and 1. B_1 and B_2 have the same structure as B_3 except using different colors. Let G be the disjoint union of B_1, B_2, B_3. Since $|V(B_i)| = 15$ for $1 \le i \le 3$, $|V(G)| = 3r^2 + 3k - 6$.



(a) Bi−color component B_3

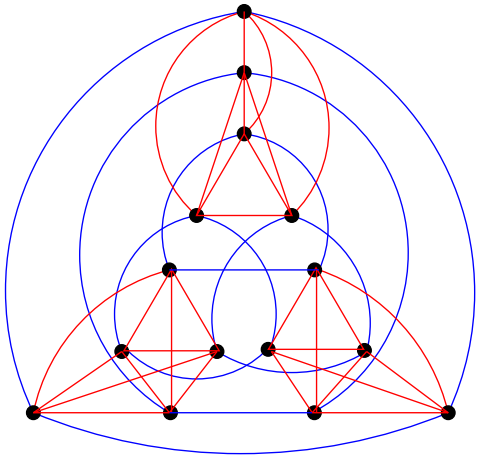


(b) Bi−color component B_1

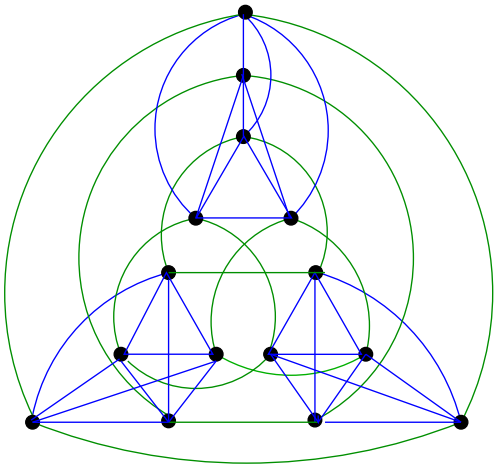


(c) Bi−color component B_2

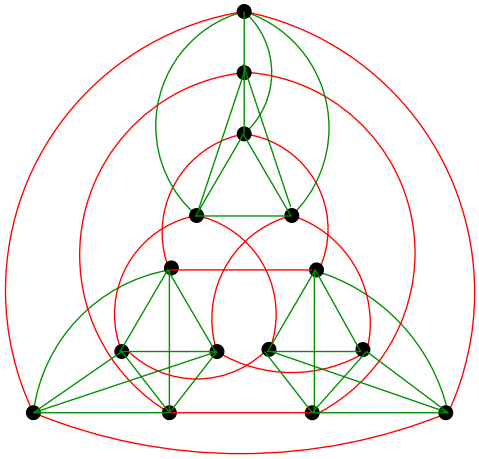
Figure 9: An IPP graph $G = B_1 \cup B_2 \cup B_3$ corresponding to $r = 3$, $k = 7$.



(a) Bi–color component B_3



(b) Bi–color component B_1



(c) Bi–color component B_2

Figure 10: An IPP graph $G = B_1 \cup B_2 \cup B_3$ corresponding to $r = 3$, $k = 8$.

As mentioned at the beginning of this chapter, for each integer $q \geq 15$ there exist unique integers r and k such that $r \geq 3$, $0 \leq k \leq 2r+2$, and $q = r^2 + 2r + k$. Hence throughout of the rest of the thesis, we express q in terms of r and k in this way. By Lemma 4.2.1–Lemma 4.2.6, we have proved the following lower bound on $F(3, q)$.

Theorem 4.2.7. *For $q \geq 15$,*

$$F(3,q) \geq \begin{cases} 3r^2, & k = 0 \\ 3r^2 + 3k - 2, & 1 \leq k \leq 2\sqrt{r+4} - 3 \text{ and } k \text{ is odd, or} \\ & 2 \leq k \leq 2\sqrt{r+2} - 2 \text{ and } k \text{ is even} \\ 3r^2 + 3k - 3, & 2\sqrt{r+4} - 3 < k \leq r+1 \text{ and } k \text{ is odd, or} \\ & 2\sqrt{r+2} - 2 < k \leq r+1 \text{ and } k \text{ is even} \\ 3r^2 + 3k - 4, & k = r+2 \\ 3r^2 + 3k - 5, & r+3 \leq k \leq r + \sqrt{4r+21} - 2 \text{ and } k-r \text{ is odd, or} \\ & r+4 \leq k \leq r + \sqrt{4r+9} - 1 \text{ and } k-r \text{ is even} \\ 3r^2 + 3k - 6, & r + \sqrt{4r+21} - 2 < k \leq 2r+2 \; k-r \text{ is odd, or} \\ & r + \sqrt{4r+9} - 1 < k \leq 2r+2 \text{ and } k-r \text{ is even} \end{cases} \tag{9}$$

CHAPTER V

MAXIMUM IPP GRAPHS

In Chapter III, we have explored some structural results on graphs associated with IPP codes of length 3. In this chapter, we aim to further study structure of graphs associated with maximum IPP codes of length 3. By using the lower bound obtained in Chapter IV and a simple graph theoretic approach, we completely characterize the structure of graphs associated with a class of maximum IPP codes of length 3. This eventually helps us to construct maximum IPP codes of length 3 over any Q with $|Q| \geq 15$.

For all figures in this chapter, we use red, blue and green to represent colors 1, 2 and 3, respectively.

5.1 Preliminaries

First, we need some notation. An edge colored graph G is *proper* if it consists of exactly three bi-color components S_1, S_2, S_3 such that for each $i \in \{1, 2, 3\}$, S_i does not use color i. We restate a result proved in [31], which says that the components of an IPP graph must satisfy certain properties.

Lemma 5.1.1. *Let $C \subseteq Q^3$ be an IPP code and G be its associated graph. Then the following hold.*
(i) For each uni-color component S of G whose edges use color i for some $i \in \{1, 2, 3\}$, $|Q_i(S)| = 1$ and $|Q_j(S)| = |V(S)|$ for all $j \in \{1, 2, 3\} - \{i\}$.
(ii) For each bi-color component S of G whose edges use color i and color j for some $\{i, j\} \subseteq \{1, 2, 3\}$, $|Q_k(S)| = |V(S)|$ for $k \in \{1, 2, 3\} - \{i, j\}$.
(iii) For each tri-color component S of G, there exist a vertex v of G and three complete subgraphs S_1, S_2, S_3 of G such that the edges of S_i use color i ($1 \leq i \leq 3$), $V(S_i \cap S_j) = \{v\}$ ($1 \leq i \neq j \leq 3$), and $|V(S)| = \frac{1}{2}(|Q_1(S)| + |Q_2(S)| + |Q_3(S)| - 1)$.

Using the above lemma, we can give an upper bound on the size of a maximum IPP code when its associated graph has no bi-color component.

Theorem 5.1.2. *Let $C \subseteq Q^3$ be an IPP code and G be its associated graph. If G contains no bi-color components, then $|C| < \frac{3q}{2}$.*

Proof. Let $S_1, S_2, \cdots, S_m$ be the components of G, which are either uni-color or tri-color. Then by (i) and (iii) of Lemma 5.1.1, we have

$$|V(S_i)| = \frac{|Q_1(S_i)| + |Q_2(S_i)| + |Q_3(S_i)| - 1}{2}.$$

Since $\sum_{i=1}^{m} |Q_j(S_i)| \leq q$ for all $1 \leq j \leq 3$, we have

$$\begin{aligned} |C| &= |V(G)| = \textstyle\sum_{i=1}^{m} |V(S_i)| \\ &= \textstyle\sum_{i=1}^{m} \frac{1}{2}(|Q_1(S_i)| + |Q_2(S_i)| + |Q_3(S_i)| - 1) \\ &\leq (3q - m)/2. \ \square \end{aligned}$$

Theorem 5.1.2 and Theorem 4.2.7 tell us that if the associated graph of an IPP code of length 3 contains no bi-color components, then it is not maximum. In fact, we shall prove that there exists a maximum IPP code whose associated graph consists of exactly three bi-color components.

5.2 Structure of Maximum IPP Graphs

First, we show that for any maximum IPP code, its associated graph must have at least three components.

Lemma 5.2.1. *Let $C \subseteq Q^3$ be a maximum IPP code and let G be its associated graph. Then G has at least three components and one of these is a bi-color component.*

Proof. Suppose G has at most two components. If G has exactly one component, then by (i) of Lemma 5.1.1, $|V(G)| \leq q$. If G has exactly two components, then again by (i) of Lemma 5.1.1 we have $|V(G)| \leq 2q - 2$. In both cases, we see that $|V(G)| < F(3, q)$. Hence, by Theorem 4.2.7, $|C|$ is not maximum, a contradiction.

Now assume G has no bi-color components. Then by Theorem 5.1.2, $|V(G)| < 3q/2 < h(q)$. In view of Theorem 4.2.7, $|C|$ is not maximum, a contradiction. $\square$

Next, we study maximum IPP graphs with minimum number of components. The following three lemmas show that the components of such an IPP graph must satisfy certain restrictions.

Lemma 5.2.2. *Suppose $C \subseteq Q^3$ is a maximum IPP code which is chosen so that its associated graph G has the minimum number of components. Then no two components of G use exactly the same colors.*

Proof. First, assume that there are two uni-color components S and T of G whose edges use the same color i for some $i \in \{1, 2, 3\}$. Let G' be the graph obtained from G by adding edges uv for all $u \in V(S)$ and $v \in V(T)$. Let H denote the component of G' containing S and T. Note that all other components of G' are components of G. It is easy to see that G' is the edge colored graph associated with a code C', where C' is obtained from C by changing the ith coordinate of every codeword in C corresponding to a vertex of T to the ith coordinate of the codewords corresponding to the vertices of S. Therefore, since H is a uni-color component, H is an IPP graph (by (i) of Lemma 3.2.2). Since $G - (V(S) \cup V(T))$ is a union of components of G, $G - (V(S) \cup V(T))$ is an IPP graph (by Lemma 2.2.3. Therefore, by Lemma 3.2.1, $G' = (G - (V(S) \cup V(T))) \cup H$ is also an IPP graph. However, $|V(G')| = |V(G)$ and the number of the components of G' is less than that of G, contradicting the choice of C and G.

Now assume that there are two bi-color components S and T of G whose edges use the same colors i and j for some $\{i, j\} \subseteq \{1, 2, 3\}$. Let S' be a component of $S(i)$ and T' be a component of $T(i)$. Let G' be the graph obtained from G by adding edges uv of color i for all $u \in V(S')$ and $v \in V(T')$. Let H denote the component of G' containing S and T. Note that all other components of G' are components of G. It is easy to see that G' is the edge colored graph associated with a code C', where C' is obtained from C by changing the ith coordinate of every codeword in C corresponding to a vertex of T' to the ith coordinate of the codewords corresponding to the vertices of S'. Therefore, since H is a bi-color component, H is an IPP graph by (ii) of Lemma 3.2.2. Since $G - (V(S) \cup V(T))$ is a union of components of G, $G - (V(S) \cup V(T))$ is an IPP graph (by Lemma 2.2.3). Therefore, by Lemma 3.2.1, $G' = (G - (V(S) \cup V(T))) \cup H$ is also an IPP graph. However, $|V(G')| = |V(G)$ and the number of the components of G' is less than that of G, contradicting the choice of C and G.

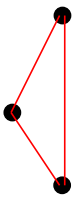
Finally, assume that there are two tri-color components S and T of G. By (iii) of Lemma 5.1.1, there exist a vertex v of S (respectively, w of T) and three complete subgraphs S_1, S_2, S_3 of S (respectively, T_1, T_2, T_3 of T) such that all edges of S_i (respectively, T_i) use color i (for $1 \leq i \leq 3$)

and $V(S_i \cap S_j) = \{v\}$ (respectively, $V(T_i \cap T_j) = \{w\}$) for all $1 \leq i \neq j \leq 3$. Let G' be the graph obtained from G by adding edges xy of color 1 for all $x \in V(S_1)$ and $y \in V(T_1)$, adding edges xy of color 2 for all $x \in V(S_2)$ and $y \in V(T_2) - \{w\}$, adding edges xy of color 3 for all $x \in V(S_3)$ and $y \in V(T_3) - \{w\}$, and deleting edges between w and $V(T_2 \cup T_3) - \{w\}$. Let H denote the component of G' containing S and T. Note that all other components of G' are components of G. It is easy to see that G' is the edge colored graph associated with a code C', where C' is obtained from C by changing the ith coordinate of each codeword in C corresponding to a vertex of $T_i - w$ to the ith coordinate of the codewords in C corresponding to the vertices of S_i $(1 \leq i \leq 3)$, and changing the 1st coordinate of the codeword corresponding to w to the 1st coordinate of the codewords corresponding to the vertices in S_1. Note that there are three complete subgraphs H_1, H_2 and H_3 of H such that all edges of each H_i are colored by i $(1 \leq i \leq 3)$ and $V(H_i \cap H_j) = \{v\}$ $(1 \leq i \neq j \leq 3)$. Hence, it follows from (iii) of Lemma 3.2.2 that H is an IPP graph. Since $G - (V(S) \cup V(T))$ is a union of components of G, $G - (V(S) \cup V(T))$ is an IPP graph (by Lemma 2.2.3). Therefore, by Lemma 3.2.1, $G' = (G - (V(S) \cup V(T))) \cup H$ is also an IPP graph. However, $|V(G')| = |V(G)$ and the number of the components of G' is less than that of G, contradicting the choice of C and G. □

In Figure 11, we describe how to combine two uni-color components of the same color into one uni-color component. S in Figure 11(a) is a uni-color component, and T in Figure 11(b) is a uni-color component T, both S and T use color 1 (red). Joining all pairs of vertices between $V(S)$ and $V(T)$ by edges of color 1, we obtain the uni-color component H in Figure 11(c).

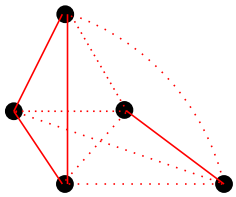
In Figure 12, we describe how to combine two bi-color components into one bi-color component. S in Figure 12(a) is a bi-color component S, and T Figure 12(b) is a bi-color component T; both use colors 1 (red) and 2 (blue). $S(1)$ contains a component S' which is a triangle, and $T(1)$ contains a component T' which is a path of length 2. Joining all pairs of vertices between $V(S')$ and $V(T')$ by edges of color 1, we obtain the bi-color component H in Figure 12(c).

As shown in Lemma 5.2.2, combining two tri-color components is a little different. An example is illustrated in Figure 13. Figure 13(a) shows a tri-color component $S_1 \cup S_2 \cup S_3$, where S_1, S_2, S_3 have a common vertex v and they use colors 1,2,3, respectively. Figure 13(b) shows a tri-color component $T_1 \cup T_2 \cup T_3$, where T_1, T_2, T_3 have a common vertex w and they use colors 1,2,3, respectively. Join all pairs of vertices between $V(S_1)$ and $V(T_1)$ by edges of color 1, join all pairs of



(a) uni−color component S

(b) uni−color component T



(c) uni−color component H

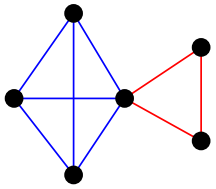
Figure 11: Combining two uni-color components

vertices between $V(S_2)$ and $V(T_2) - \{w\}$ by edges of color 2, and join all pairs of vertices between $V(S_3)$ and $V(T_3) - \{w\}$ by edges of color 3. Then deleting (three) edges between $V(T_2 \cup T_3)$ and $\{w\}$, we obtain the tri-color component H in Figure 13(c).

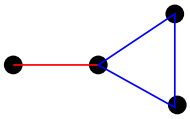
Lemma 5.2.3. *Suppose $C \subseteq Q^3$ is a maximum IPP code which is chosen so that its associated graph G has the minimum number of components. Then G has no uni-color components.*

Proof. Suppose on the contrary that G contains a uni-color component S, whose edges are colored with color i for some $i \in \{1, 2, 3\}$.

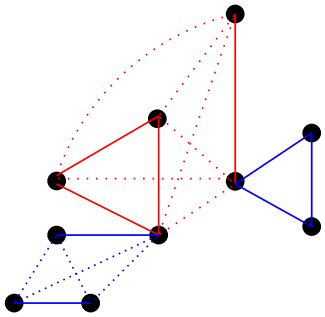
First, we show that we may choose S so that the color used in S is also used in another component T of G. Suppose this is not true. Then all other components of G are uni-color or bi-color components. By Lemma 5.2.1, let T be a bi-color component. Then the edges of T use colors from $\{1, 2, 3\} - \{i\}$. By Lemma 5.2.1, G has a component U other than S and T. If U is a uni-color component, then we see from Lemma 5.2.2 that the edges of U use a color from $\{1, 2, 3\} - \{i\}$, and therefore, U, T would give the desired choice. So we may assume that U is also a bi-color component. Then by Lemma 5.2.2 again, U and T cannot use the same two colors. Hence, color i is used in U. Therefore, S and U give the desired choice.



(a) bi−color component S



(b) bi−color component T



(c) bi−color component H

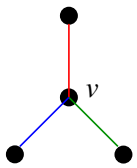
Figure 12: Combining two bi-color components

By Lemma 5.2.2, T is a bi-color or tri-color component of G. Let T' be a component of $T(i)$. Let G' be the graph obtained from G by adding edges uv of color i for all $u \in V(S)$ and $v \in V(T')$.

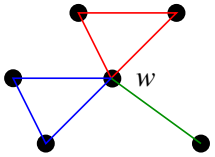
Clearly, G' is the graph associated with a code $C' \subseteq Q^3$ obtained from C by changing the ith coordinate of those codewords in C corresponding to vertices of T' to the ith coordinate of the codewords in C corresponding to vertices of S. Let H be the component of G' containing $S \cup T$. Note that $G - V(H)$ consists of components of G, and hence, is an IPP graph.

When T is a bi-color component of G, we see from (i) of Lemma 3.2.2 that H is an IPP graph. Now assume T is a tri-color component of G. Then by (iii) of Lemma 5.1.1, there exist a vertex v of T and complete subgraphs T_1, T_2, T_3 of T such that all edges of T_s use color s $(1 \leq s \leq 3)$ and $V(T_s \cap T_t) = \{v\}$ $(1 \leq s \neq t \leq 3)$. In this case, $T' = T_i$, and we see that H has three complete subgraphs H_1, H_2, H_3 such that $H_1 \cup H_2 \cup H_3 = H$, all edges of each H_s use color s $(1 \leq s \leq 3)$, and $V(H_s \cap H_t) = \{v\}$ $(1 \leq s \neq t \leq 3)$. In fact, $V(H_i) = V(S) \cup V(T_i)$. By (iii) of Lemma 3.2.2, H is an IPP graph.

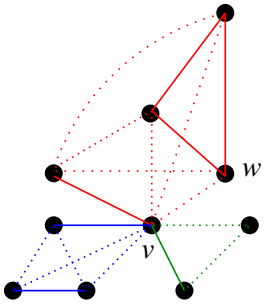
Since both H and $G - V(H)$ are IPP graphs, it follows from Lemma 3.2.1 that G' is an IPP graph. However, $|V(G')| = |V(G)|$ and G' has fewer components than G, contradicting the choice of C and



(a) tri−color component S



(b) tri−color component T



(c) tri−color component H

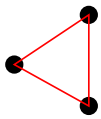
Figure 13: Combining two tri-color components

G. □

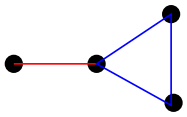
In Figure 14, we see how to combine a uni-color component and a bi-color component. Figure 14(a) shows a uni-color component S which uses color 1 (red), and Figure 14(b) shows a bi-color component T which uses colors 1 (red) and 2 (blue). $T(1)$ contains a component T' which is a path of length 2. Joining all pairs of vertices between $V(S)$ and $V(T')$ by edges of color 1, we obtain the bi-color component H in Figure 14(c).

Lemma 5.2.4. *Suppose $C \subseteq Q^3$ is a maximum IPP code which is chosen so that its associated graph G has the minimum number of components. Then G has no tri-color components.*

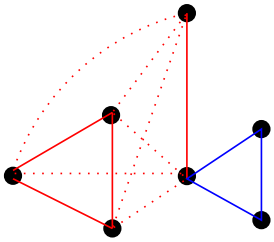
Proof. Suppose G contains a tri-color component S. By (iii) of Lemma 5.1.1 there exist a vertex v of S and complete subgraphs S_1, S_2, S_3 of S such that $S_1 \cup S_2 \cup S_3 = S$, all edges of each S_i use color i $(1 \leq i \leq 3)$, and $V(S_i \cap S_j) = \{v\}$ $(1 \leq i \neq j \leq 3)$. By Lemma 5.2.2, S is the only tri-component of G. By Lemma 5.2.3, all components of G other than S are bi-color components. Therefore, it follows from Lemma 5.2.1 that there are two bi-color components in G, say T and U. By Lemma 5.2.2, we may assume that T uses colors 1 and 2, and U uses colors 2 and 3.



(a) uni−color component S



(b) bi−color component T



(c) bi−color component H

Figure 14: Combining a uni-color component and a bi-color component

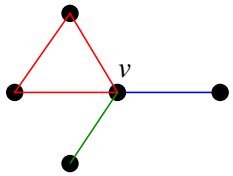
Next, we construct a new graph G'. Let T' be a component of $T(1)$, let T'' be a component of $T(2)$, and let U' be a component of $U(3)$. Let G' be obtained from G by adding edges xy of color 1 for all $x \in V(T')$ and $y \in V(S_1)$, adding edges xy of color 2 for all $x \in V(T'')$ and $y \in V(S_2) - \{v\}$, adding all edges of color 3 for all $x \in V(U')$ and $y \in V(S_3) - \{v\}$, and deleting all edges of S_2 and S_3 incident with v. Let H_1 denote the component of G' containing S_1, S_2 and T, and let H_2 denote the component of G' containing $S_3 - \{v\}$ and U. Note that both H_1 and H_2 are bi-color components of G'.

Clearly, G' is the graph associated with a code $C' \subseteq Q^3$, where C' is obtained from C by changing the first coordinate of the codewords in C corresponding to vertices of S_1 to the first coordinate of codewords in C corresponding to vertices of T', changing the second coordinate of the codewords in C corresponding to vertices of $S_2 - \{v\}$ to the second coordinate of codewords in C corresponding to vertices of T'', and changing the third coordinate of the codewords in C corresponding to vertices of $S_3 - \{v\}$ to the third coordinate of codewords in C corresponding to vertices of U'.

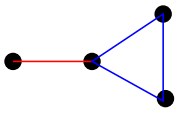
Since H_1 and H_2 are bi-color components, H_1 and H_2 are IPP graphs by (i) and (ii) of Lemma 3.2.2. Since G is an IPP graph, $G - (V(H_1) \cup V(H_2))$ (if non-empty) is also an IPP graph. So by Lemma 3.2.1, G' is an IPP graph. Clearly, $|V(G')| = |V(G)|$. However, G' has fewer components

than G, contradicting the choice of C and G. □

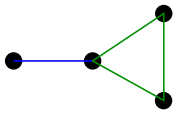
In Figure 15, we illustrate how to combine a tri-color component and two bi-color components. Figure 15(a) gives a tri-color component $S = S_1 \cup S_2 \cup S_3$, where S_1, S_2, S_3 have a common vertex v and they use colors 1, 2, 3, respectively. Figure 15(b) gives a bi-color component T which uses colors 1 and 2. $T(1)$ contains a component T' which is a path of length 2 and $T(2)$ contains a triangle T''. Figure 15(c) gives a bi-color component U which uses colors 2 and 3. $U(3)$ contains a component U' which is a triangle. Join all pairs of vertices between $V(S_1)$ and $V(T')$ by edges of color 1, join all pairs of vertices between $V(S_2) - \{v\}$ and $V(T'')$ by edges of color 2, and join all pairs of vertices between $V(S_3) - \{v\}$ and $V(U')$ by edges of color 3. Then delete (two) edges between $V(S_2 \cup S_3)$ and $\{v\}$, we obtain two bi-color components H_1 in Figure 15(d) and H_2 in Figure 15(e).



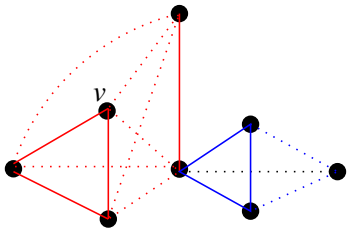
(a) tri−color component S



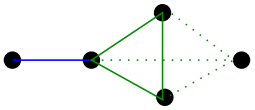
(b) bi−color component T



(c) bi−color component U



(d) bi−color component H_1



(e) bi−color component H_2

Figure 15: Combining a tri-color component and two bi-color components

We can now prove the main result of this section.

Theorem 5.2.5. *There exists a maximum IPP code $C \subseteq Q^3$ such that its associated graph is a proper graph.*

Proof. Choose a maximum IPP code C such that its associated graph G has the minimum number of components. By Lemma 5.2.3 and Lemma 5.2.4, all components of G are bi-color. Therefore, by Lemma 5.2.2, G has at most three components. It follows from Lemma 5.2.1 that G has exactly three bi-color components. Hence, G is proper. □

We point out that Theorem 5.2.5 was also proved in [36], but our approach is independent of [36] and is much simpler. This result provides explicit structure of a class of maximum IPP codes of length 3, which played a role in the code constructions in Chapter IV, and will play an important role in the remainder of the thesis.

CHAPTER VI

NONLINEAR PROGRAMMING PROBLEM

Recall from Theorem 5.2.5, there exists a maximum IPP code $C \subseteq Q^3$ such that its associated graph consists of exactly three bi-color components B_1, B_2, B_3, where B_i does not use color i. In this chapter, we use this result to reduce the problem of determining $F(3, q)$ to a nonlinear programming problem. We propose an algorithm which finds an optimal solution. We then show how to use an optimal solution of the nonlinear programming problem to construct IPP codes. Lemma 3.2.1 and Lemma 3.2.2 will be used to show that the codes we construct are indeed IPP codes. We shall see that our construction is efficient and the constructed codes are capable of tracing efficiently a parent of any descendant codeword.

6.1 A Nonlinear Programming Formulation

Let $q = |Q|$. Let $C \subseteq Q^3$ be a maximum IPP code and G be its associated graph. By Theorem 5.2.5, we may choose C so that G has exactly three components B_1, B_2, B_3, and for each $i \in \{1, 2, 3\}$, B_i is a bi-color component in which the color i does not occur. Then

$$|C| = |V(G)| = \sum_{i=1}^{3} |Q_i(B_i)| \tag{10}$$

and, for $j \in \{1, 2, 3\}$,

$$\sum_{i=1}^{3} |Q_j(B_i)| \leq q. \tag{11}$$

Moreover, it follows from Lemma 3.2.3 that, for each $k \in \{1, 2, 3\}$ and $\{i, j\} = \{1, 2, 3\} - \{k\}$,

$$|Q_i(B_k)| + |Q_j(B_k)| - 1 \leq |Q_k(B_k)| \leq |Q_i(B_k)||Q_j(B_k)| \tag{12}$$

Since B_1, B_2, B_3 are bi-color components of G, $|Q_j(B_i)| \geq 2$ for all $1 \leq i, j \leq 3$. Combining this with (11), we obtain $2 \leq |Q_j(B_i)| \leq q - 4$ for all $1 \leq i, j \leq 3$. For $1 \leq j \leq 3$, let $|Q_j(B_3)| = x_j, |Q_j(B_1)| = y_j, |Q_j(B_2)| = z_j$. Let $\mathcal{N} = \{2, 3, \cdots, q-4\}$. Then finding the maximum $|V(G)|$ in (10) subject to (11) and (12) is equivalent to solving the following nonlinear optimization problem:

$$\text{maximize } f(\mathbf{x}) = x_3 + y_1 + z_2 \tag{13}$$

subject to $\mathbf{x} = (x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3) \in N^9$ and

$$\begin{aligned}
&\text{(i)} && x_3 - x_1 x_2 \leq 0,\\
&\text{(ii)} && y_1 - y_2 y_3 \leq 0,\\
&\text{(iii)} && z_2 - z_1 z_3 \leq 0,\\
&\text{(iv)} && x_1 + y_1 + z_1 - q \leq 0,\\
&\text{(v)} && x_2 + y_2 + z_2 - q \leq 0,\\
&\text{(vi)} && x_3 + y_3 + z_3 - q \leq 0,\\
&\text{(vii)} && x_1 + x_2 - 1 - x_3 \leq 0,\\
&\text{(viii)} && y_2 + y_3 - 1 - y_1 \leq 0,\\
&\text{(ix)} && z_1 + z_3 - 1 - z_2 \leq 0.
\end{aligned} \tag{14}$$

We call $\mathbf{x} \in N^9$ *an optimal solution* if $f(\mathbf{x})$ is maximum subject to (14), the maximum is therefore $F(3, q)$. We note that the formulation without (vii), (viii) and (ix) is also given in [36]. But (vii), (viii) and (ix) are important for determining $F(3, q)$.

6.2 Algorithm to Compute $F(3, q)$

To find an optimal solution to the above nonlinear programming problem, exhaustive search has complexity of $O(q^9)$, which is not efficient.

Let us analyze the constraints in (14). Suppose $\mathbf{x} = (x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3) \in N^9$ is an optimal solution to (13) subject to (14). Then $F(3, q) = x_3 + y_1 + z_2$. Note that $F(3, q) \geq 3r^2 + 3k - 6 \geq 3q - 6\sqrt{q+1}$, hence

$$x_3 + y_1 + z_2 \geq 3q - 6\sqrt{q+1}. \tag{15}$$

So by (iv)-(vi) of (14) and (15), we have

$$x_1 + x_2 + y_2 + y_3 + z_1 + z_3 \leq 6\sqrt{q+1}. \tag{16}$$

Again by (15) and since $\mathbf{x} \in N^9$, we have

$$x_3 \geq q + 1 - 6\sqrt{q+1}, \quad y_1 \geq q + 1 - 6\sqrt{q+1}, \quad z_2 \geq q + 1 - 6\sqrt{q+1}. \tag{17}$$

Hence, by (i)-(iii) of (14) and (17), we obtain

$$x_2 \geq \frac{q + 1 - 6\sqrt{q+1}}{x_1}, \quad y_3 \geq \frac{q + 1 - 6\sqrt{q+1}}{y_2}, \quad z_1 \geq \frac{q + 1 - 6\sqrt{q+1}}{z_3}. \tag{18}$$

Since $\mathbf{x} \in N^9$ and by (16), we obtain

$$\begin{aligned} x_1 \le 6\sqrt{q+1}, \quad x_2 \le 6\sqrt{q+1}, \quad y_2 \le 6\sqrt{q+1}, \\ y_3 \le 6\sqrt{q+1}, \quad z_1 \le 6\sqrt{q+1}, \quad z_3 \le 6\sqrt{q+1}. \end{aligned} \tag{19}$$

Plug (19) into (18), we obtain

$$\begin{aligned} x_1 \ge \frac{\sqrt{q+1}}{6} - 1, \quad x_2 \ge \frac{\sqrt{q+1}}{6} - 1, \quad y_2 \ge \frac{\sqrt{q+1}}{6} - 1, \\ y_3 \ge \frac{\sqrt{q+1}}{6} - 1, \quad z_1 \ge \frac{\sqrt{q+1}}{6} - 1, \quad z_1 \ge \frac{\sqrt{q+1}}{6} - 1. \end{aligned} \tag{20}$$

Now if we plug (20) into (16), then we obtain a tighter upper bound on $x_1, x_2, y_2, y_3, z_3, z_1$ than that in (19). Plugging this new upper bound into (18), we can obtain a tighter lower bound on $x_1, x_2, y_2, y_3, z_3, z_1$ than that in (20). Hence, we are able to recursively improve (19) and (20) by using (16) and (18). Hence we are able to obtain a very tight range for $x_1, x_2, y_2, y_3, z_3, z_1$. Next, let us examine x_3, y_1, z_2.

Notice that at least two of (iv), (v), (vi) of (14) hold with equality since $\mathbf{x}$ is an optimal solution. Otherwise, assume that (iv) and (v) hold with strict inequality; then $\mathbf{x}' = (x_1, x_2, x_3, y_1 + 1, y_2 + 1, y_3, z_1, z_2, z_3)$, and hence, $\mathbf{x}' \in N^9$ and $\mathbf{x}'$ satisfies (14). However, $f(\mathbf{x}') = x_3 + y_1 + z_2 + 1 > f(\mathbf{x}')$, a contradiction. Hence, we may assume (iv) and (v) of (14) hold with equality.

We also notice that either (i) or (vi) of (14) holds with equality. Otherwise, let $\mathbf{x}' = (x_1, x_2, x_3 + 1, y_1, y_2, y_3, z_1, z_2, z_3)$, then $\mathbf{x}' \in N^9$ and it satisfies (14), but $f(\mathbf{x}') = x_3 + y_1 + z_2 + 1 > f(\mathbf{x}')$, a contradiction.

With the above analysis, we are now ready to design an efficient algorithm to compute $F(3, q)$. We use $lb = \sqrt{q+1}/6 - 1$ and $ub = 6\sqrt{q+1}$ to denote the lower bound and the upper bound, respectively. The following algorithm, named MAX-IPP, can be used to determine $F(3, q)$. This program searches for an optimal solution to maximize (13) subject to (14).

There are two outputs from the MAX-IPP algorithm: an optimal solution $\mathbf{x}$ to (13) subject to (14) and the value of $F(3, q)$ for each $q \ge 15$. The complexity of algorithm MAX-IPP is $O(q^3)$[49]. We remark that this algorithm is also presented in [36] independently.

6.3 Method to Construct Maximum IPP Codes

Next, we show that any feasible solution $\mathbf{x}$ to the above non-linear programming problem can be used to construct an IPP code C.

Input: The cardinality q of alphabet Q
Output: Optimal soulution $\mathbf{x} = (x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3)$ and $F(3, q)$

```
1   maximum ← 0;
2   for x_1 = lb to ub do
3     for x_2 = lb to ub do
4       for y_2 = lb to ub do
5         for y_3 = lb to ub do
6           for z_1 = lb to ub do
7             for z_3 = lb to ub do
8                 y_1 ← q − (x_1 + z_1);
9                 z_1 ← q − (x_2 + y_2);
10                x_3 ← q − (y_3 + z_3) or x_1 ∗ x_2;
11                if constraints (14) satisfied then
12                  temp ← x_3 + y_1 + z_2;
13                  if temp > maximum then
14                    maximum ← temp;
15                    x ← (x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3);
16                  end
17                end
18              end
19            end
20          end
21        end
22      end
23  end
24  return x = (x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3) and maximum
```

MAX-IPP algorithm: Compute the maximum size of IPP codes of length 3 over Q.

Theorem 6.3.1. *Let* $\mathbf{x} = (x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3) \in \mathcal{N}^9$ *satisfying (14). Then there exists a q-ary IPP code of length 3 with size* $x_3 + y_1 + z_2$.

Proof. We construct an IPP graph which consists of three bi-color components B_1, B_2, B_3 such that for each $i \in \{1, 2, 3\}$, the edges of B_i do not use color i. We also construct codes C_1, C_2, C_3 simultaneously such that B_i is the associated graph of C_i.

First, we construct B_3 whose edges use color 1 and color 2 only. Take x_1 disjoint complete graphs R_s^3, $1 \le s \le x_1$, such that $\min\{|V(R_s^3)| : 1 \le s \le x_1\} \ge 1$, $\max\{|V(R_s^3)| : 1 \le s \le x_1\} = x_2$, and $\sum_{s=1}^{x_1} |V(R_s^3)| = x_3$. This can be done because $x_1 x_2 \ge x_3$ (by (i) of (14)) and $x_3 \ge x_1 + x_2 - 1 \ge x_1 + 1$

(by (vii) of (14) and since $x_2 \geq 2$ because $\mathbf{x} \in \mathcal{N}^9$). Color all edges of each R_s^3 with color 1, and label the vertices of each R_s^3 as $v_{s,1}^3, v_{s,2}^3, \cdots, v_{s,|V(R_s^3)|}^3$. For each $1 \leq t \leq x_2$, let $J_t^3 = \{s : |V(R_s^3)| \geq t\}$ and, if $|J_t^3| \geq 2$ then join every pair of vertices from $\{v_{s,t}^3 : s \in J_t^3\}$ by an edge of color 2. Let B_3 denote the resulting edge colored graph. Note that $|V(B_3)| = x_3$ and the edges of B_3 do not use color 3. Also note that the components of $B_3(1)$ are the graphs R_s^3 $(1 \leq s \leq x_1)$, the components of $B_3(2)$ are the complete graphs with vertex set $\{v_{s,t} : s \in J_t^3\}$ $(1 \leq t \leq x_2)$, and the components of $B_3(3)$ are the isolated vertices $\{v_{s,t}^3\}$ $(1 \leq s \leq x_1$ and $1 \leq t \leq |V(R_s^3)|)$. Let

$$C_3 = \{(\alpha_s, \alpha_t, \alpha_{(\sum_{k=1}^{s-1} |V(R_k^3)|)+t}) : 1 \leq s \leq x_1, 1 \leq t \leq |V(R_s^3)|\}. \tag{21}$$

Clearly, the subscript of the first coordinate is between 1 and x_1, the subscript of the second coordinate is between 1 and x_2, and subscript of the third coordinate is between 1 and x_3. Note that the third subscript $(\sum_{k=1}^{s-1} |V(R_k^3)|) + t$ guarantees that all codewords in C_3 have distinct 3rd coordinates. It is straightforward to check that B_3 is the graph associated with $C_3 \subseteq Q^3$ by noticing that the codeword $(\alpha_s, \alpha_t, \alpha_{(\sum_{k=1}^{s-1} |V(R_k^3)|)+t})$ in C_3 corresponds to the vertex $v_{s,t}^3$ of B_3 for all $1 \leq s \leq x_1$ and $1 \leq t \leq |V(R_s^3)|$. Since B_3 is a bi-color component and by (i) of Lemma 3.2.2, B_3 is an IPP graph.

Now, we construct B_1 whose edges use color 2 and color 3 only. Take y_2 disjoint complete graphs R_s^1, $1 \leq s \leq y_2$, such that $\min\{|V(R_s^1)| : 1 \leq s \leq y_2\} \geq 1$, $\max\{|V(R_s^1)| : 1 \leq s \leq y_2\} = y_3$, and $\sum_{s=1}^{y_2} |V(R_s^1)| = y_1$. This can be done because $y_2 y_3 \geq y_1$ (by (ii) of (14)) and $y_1 \geq y_2 + y_3 - 1 \geq y_2 + 1$ (by (viii) (14) and because $\mathbf{x} \in \mathcal{N}^9$). Color all edges of each R_s^1 with color 2, and label the vertices of each R_s^1 as $v_{s,1}^1, v_{s,2}^1, \cdots, v_{s,|V(R_s^1)|}^1$. For each $1 \leq t \leq y_3$, let $J_t^1 = \{s : |V(R_s^1)| \geq t\}$ and, if $|J_t^1| \geq 2$, join every pair of vertices from $\{v_{s,t}^1 : s \in J_t^1\}$ by an edge of color 3. Let B_1 denote the resulting edge colored graph. Note that $|V(B_1)| = y_1$ and the edges of B_1 do not use color 1. Also note that the components of $B_1(2)$ are the graphs R_s^1 $(1 \leq s \leq y_2)$, the components of $B_1(3)$ are the complete graphs with vertex set $\{v_{s,t}^1 : s \in J_t^1\}$ $(1 \leq t \leq y_3)$, and the components of $B_1(1)$ are the isolated vertices $\{v_{s,t}^1\}$ $(1 \leq s \leq y_2$ and $1 \leq t \leq |V(R_s^1)|)$. Let

$$C_1 = \{(\alpha_{x_1+(\sum_{k=1}^{s-1} |V(R_k^1)|)+t}, \alpha_{x_2+s}, \alpha_{x_3+t}) : 1 \leq s \leq y_2, 1 \leq t \leq |V(R_s^1)|\}. \tag{22}$$

Clearly, the subscript of the first coordinate is between $x_1 + 1$ and $x_1 + y_1$, the subscript of the second coordinate is between $x_2 + 1$ and $x_2 + y_2$, and subscript of the third coordinate is between $x_3 + 1$ and $x_3 + y_3$. Note that the subscript $x_1 + (\sum_{k=1}^{s-1} |V(R_k^1)|) + t$ ensures that all codewords in C_1 have distinct

1st coordinates. It is straightforward to check that B_1 is the graph associated with $C_1 \subseteq Q^3$ by noticing that the codeword $(\alpha_{x_1+(\sum_{k=1}^{s-1}|V(R_k)|)+t}, \alpha_{x_2+s}, \alpha_{x_3+t})$ in C_1 corresponds to the vertex $v^1_{s,t}$ of B_1 for all $1 \le s \le y_2$ and $1 \le t \le |V(R^1_s)|$. Since B_1 is a bi-color component and by (i) of Lemma 3.2.2, B_1 is an IPP graph.

Finally, we construct B_2 whose edges use color 3 and color 1 only. Take z_3 disjoint complete graphs R^2_s, $1 \le s \le z_2$ such that $\min\{|V(R^2_s)| : 1 \le s \le z_3\} \ge 1$, $\max\{|V(R^2_s)| : 1 \le s \le z_3\} = z_1$, and $\sum_{s=1}^{z_3}|V(R^2_s)| = z_2$. This can be done because $z_1 z_3 \ge z_2$ (by (iii) of (14)) and $z_2 \ge z_1 + z_3 - 1 \ge z_3 + 1$ (by (ix) of (14) and because $\mathbf{x} \in \mathcal{N}^9$). Color all edges of each R^2_s with color 3, and label the vertices of each R^2_s as $v^2_{s,1}, v^2_{s,2}, \cdots, v_{s,|V(R^2_s)|}$. For each $1 \le t \le z_1$, let $J^2_t = \{s : |V(R^2_s)| \ge t\}$ and, if $|J^2_t| \ge 2$, join every pair of vertices from $\{v^2_{s,t} : s \in J^2_t\}$ by an edge of color 1. Let B_2 denote the resulting edge colored graph. Note that $|V(B_2)| = z_2$ and the edges of B_2 do not use color 2. Also note that the components of $B_2(3)$ are the graphs R^2_s $(1 \le s \le z_3)$, the components of $B_2(1)$ are the complete graphs with vertex set $\{v^2_{s,t} : s \in J^2_t\}$ $(1 \le t \le z_1)$, and the components of $B_2(2)$ are the isolated vertices $\{v^2_{s,t}\}$ $(1 \le s \le z_3$ and $1 \le t \le |V(R^2_s)|)$. Let

$$C_2 = \{(\alpha_{x_1+y_1+t}, \alpha_{x_2+y_2+(\sum_{k=1}^{s-1}|V(R^2_k)|)+t}, \alpha_{x_3+y_3+s}) : 1 \le s \le z_3, 1 \le t \le |V(R^2_s)|\}. \tag{23}$$

Clearly, the subscript of the first coordinate is between $x_1 + y_1 + 1$ and $x_1 + y_1 + z_1$, the subscript of the second coordinate is between $x_2 + y_2 + 1$ and $x_2 + y_2 + z_2$, and subscript of the third coordinate is between $x_3 + y_3 + 1$ and $x_3 + y_3 + z_3$. Note that the subscript $x_2 + y_2 + (\sum_{k=1}^{s-1}|V(R^2_k)|) + t$ shows that all codewords in C_2 have distinct 2nd coordinates. It is straightforward to check that B_2 is the graph associated with $C_2 \subseteq Q^3$ by noticing that the codeword $(\alpha_{x_1+y_1+t}, \alpha_{x_2+y_2+(\sum_{k=1}^{s-1}|V(R_k)|)+t}, \alpha_{x_3+y_3+t})$ in C_2 corresponds to the vertex $v^2_{s,t}$ of B_2 for all $1 \le s \le z_3$ and $1 \le t \le |V(R^2_s)|$. Since B_2 is bi-color and by (i) of Lemma 3.2.2, B_2 is an IPP graph.

Let G denote the disjoint union of B_1, B_2 and B_3. That is, B_1, B_2 and B_3 are the components of G. By looking at the subscripts of coordinates of codewords in C_1, C_2, C_3, we can check that C_1, C_2, C_3 are disjoint, and for any $1 \le i \ne j \le 3$ and $1 \le k \le 3$, no codeword of C_i shares the same kth coordinate with a codeword of C_j. Hence, G is the graph associated with

$$C := C_1 \cup C_2 \cup C_3. \tag{24}$$

Therefore, because B_1, B_2, B_3 are IPP graphs, it follows from Lemma 3.2.1 that G is an IPP graph.

Hence, C is an IPP code. □

6.4 Algorithm to Decode IPP Codes

From the construction in the proof of Theorem 6.3.1, it is easy to see that any two coordinates of a codeword in C uniquely determine the third coordinate of that codeword. If $\mathbf{a}, \mathbf{b} \in C$ and $\mathbf{c} \in desc(\mathbf{a}, \mathbf{b})$, then at least two coordinates of $\mathbf{c}$ come from $\mathbf{a}$ or come from $\mathbf{b}$ but not from both.

Next, we give an algorithm which shows that the maximum IPP code C in (24) can be used to trace, in constant time, a parent of any descendant codeword.

For each $1 \leq m \leq 3$ and each $1 \leq i \leq 3$, let $f_i^m(s,t)$ denote the ith subscript of the codeword in C_m corresponding to $v_{s,t}^m$. For example, $f_1^1(s,t) = x_1 + (\sum_{k=1}^{s-1} |V(R_k^1)|) + t$ and $f_1^3(s,t) = s$. Note that any pair of subscripts $(f_i^m(s,t), f_j^m(s,t))$ uniquely determines (s,t) due to the special structure of our code in (24) . For each $1 \leq m \leq 3$, let D_m denote the set of all pairs of (s,t) that occur in the subscript of the codewords in C_m, that is,

$$D_1 = \{(s,t) : 1 \leq s \leq y_2, 1 \leq t \leq |V(R_s^1)|\},$$
$$D_2 = \{(s,t) : 1 \leq s \leq z_3, 1 \leq t \leq |V(R_s^2)|\},$$
$$D_3 = \{(s,t) : 1 \leq s \leq x_1, 1 \leq t \leq |V(R_s^3)|\}.$$

The following algorithm, named Decoding-IPP, traces a parent of any descendant codeword. The input of the algorithm is any descendant $\mathbf{c}$ of the code in (24). This algorithm always succeeds, since at least two coordinates of $\mathbf{c}$ are from one of its parents, there must exist some $l \in \{1,2,3\}$ such that line 6, 16 or 26 applies. Hence, when it terminates, the algorithm outputs an identifiable parent $\mathbf{a}$. In the worst case, the Decoding-IPP algorithm runs three loops (line 2), and in each loop, it solves two simple linear algebraic equations (line 5, 15, or 25). Thus, algorithm Decoding-IPP has a constant decoding complexity.

Input: descendant codeword $\mathbf{c} = (\alpha_{u_1}, \alpha_{u_2}, \alpha_{u_3})$
Output: identifiable parent $\mathbf{a}$ of $\mathbf{c}$

$l \leftarrow 1$; $boolean \leftarrow 0$;
while ($boolean == 0$) **do**
  $\{i, j\} \leftarrow \{1, 2, 3\} - \{l\}$;
  if $u_i \le x_i$ **and** $u_j \le x_j$ **then**
    solve (s, t) from $u_i = f_i^1(s, t)$, $u_j = f_j^1(s, t)$;
    if $(s, t) \in D_1$ **then**
      $w_i \leftarrow u_i; w_j \leftarrow u_j; w_l \leftarrow f_l^1(s, t)$;
      $[I, J, L] \leftarrow sort([i, j, l])$;
      $\mathbf{a} \leftarrow (\alpha_{w_I}, \alpha_{w_J}, \alpha_{w_L})$;
       $boolean \leftarrow 1$;
       return $\mathbf{a}$ with success; // $\mathbf{a}$ is an identifiable parent and $\mathbf{a} \in C_1$
    else $l \leftarrow l + 1$;
    end
  else if $x_i < u_i \le x_i + y_i$ **and** $x_j < u_j \le x_j + y_j$ **then**
      solve (s, t) from $u_i = f_i^2(s, t)$, $u_j = f_j^2(s, t)$;
      if $(s, t) \in D_2$ **then**
        $w_i \leftarrow u_i; w_j \leftarrow u_j; w_l \leftarrow f_l^2(s, t)$;
        $[I, J, L] \leftarrow sort([i, j, l])$;
        $\mathbf{a} \leftarrow (\alpha_{w_I}, \alpha_{w_J}, \alpha_{w_L})$;
        $boolean \leftarrow 1$;
        return $\mathbf{a}$ with success; // $\mathbf{a}$ is an identifiable parent and $\mathbf{a} \in C_2$
      else $l \leftarrow l + 1$;
      end
  else if $x_i + y_i < u_i$ **and** $x_j + y_j < u_j$ **then**
      solve (s, t) from $u_i = f_i^3(s, t)$, $u_j = f_j^3(s, t)$;
      if $(s, t) \in D_3$ **then**
        $w_i \leftarrow u_i; w_j \leftarrow u_j; w_l \leftarrow f_l^3(s, t)$;
        $[I, J, L] \leftarrow sort([i, j, l])$;
        $\mathbf{a} \leftarrow (\alpha_{w_I}, \alpha_{w_J}, \alpha_{w_L})$;
        $boolean \leftarrow 1$;
        return $\mathbf{a}$ with success; // $\mathbf{a}$ is an identifiable parent and $\mathbf{a} \in C_3$
      end
    end
  end
end

Decoding-IPP algorithm: Find an identifiable parent for any descendant of the IPP code in (24).

CHAPTER VII

THE PRECISE FORMULA

As proved in Chapter VI, in order to find $F(3,q)$, it suffices to solve the following nonlinear optimization problem, named Nonlinear-IPP problem,

$$\text{maximize } f(\mathbf{x}) = x_3 + y_1 + z_2 \tag{25}$$

subject to $\mathbf{x} = (x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3) \in N^9$ and

$$\begin{aligned}
&\text{(i)} \quad g_1(\mathbf{x}) = x_3 - x_1x_2 \le 0,\\
&\text{(ii)} \quad g_2(\mathbf{x}) = y_1 - y_2y_3 \le 0,\\
&\text{(iii)} \quad g_3(\mathbf{x}) = z_2 - z_1z_3 \le 0,\\
&\text{(iv)} \quad g_4(\mathbf{x}) = x_1 + y_1 + z_1 - q \le 0,\\
&\text{(v)} \quad g_5(\mathbf{x}) = x_2 + y_2 + z_2 - q \le 0,\\
&\text{(vi)} \quad g_6(\mathbf{x}) = x_3 + y_3 + z_3 - q \le 0,
\end{aligned} \tag{26}$$

and

$$\begin{aligned}
&\text{(vii)} \quad g_7(\mathbf{x}) = x_1 + x_2 - 1 - x_3 \le 0,\\
&\text{(viii)} \quad g_8(\mathbf{x}) = y_2 + y_3 - 1 - y_1 \le 0,\\
&\text{(ix)} \quad g_9(\mathbf{x}) = z_1 + z_3 - 1 - z_2 \le 0.
\end{aligned} \tag{27}$$

The maximum of (25) subject to (26) and (27) is exactly $F(3,q)$. In this chapter, we aim to prove (5).

Recall the partition of I defined in Section 4.1, for each integer $q \ge 15$, there exist unique integers r and k such that $r \ge 3$, $0 \le k \le 2r+2$, and $q = r^2 + 2r + k$. Hence, through this Chapter we consider q as such a function of r and k.

7.1 $F(3,q)$ *for small* q

For small values of $1 \le q \le 48$ (i.e., $1 \le r \le 5$), $F(3,q)$ is given in Table 1 by Tô and Safavi-Naini [36]. Let us compute the lower bound on $F(3,q)$ in (9) for $15 \le q \le 62$ (i.e., $3 \le r \le 6$) as

in Table 2. By checking these two tables, we find that (5) holds for $15 \le q \le 48$ (i.e., $3 \le r \le 5$, $0 \le k \le 2r+2$). Hence, we have the following,

Lemma 7.1.1. *(5) holds for* $15 \le q \le 48$.

Table 1: $F(3,q)$ for $1 \le q \le 48$

q	$F(3,q)$	q	$F(3,q)$	q	$F(3,q)$	q	$F(3,q)$
1	1	13	22	25	49	37	79
2	2	14	24	26	52	38	82
3	4	15	27	27	54	39	84
4	5	16	28	28	57	40	87
5	7	17	31	29	60	41	90
6	8	18	33	30	62	42	92
7	10	19	36	31	64	43	94
8	12	20	38	32	67	44	97
9	14	21	40	33	69	45	99
10	16	22	42	34	72	46	102
11	18	23	45	35	75	47	105
12	20	24	48	36	76	48	108

Table 2: (9) for $15 \le q \le 62$

q	(9)	q	(9)	q	(9)	q	(9)
15	27	27	54	39	84	51	115
16	28	28	57	40	87	52	117
17	31	29	60	41	90	53	120
18	33	30	62	42	92	54	123
19	36	31	64	43	94	55	126
20	38	32	67	44	97	56	128
21	40	33	69	45	99	57	130
22	42	34	72	46	102	58	133
23	45	35	75	47	105	59	136
24	48	36	76	48	108	60	138
25	49	37	79	49	109	61	141
26	52	38	82	50	112	62	144

Thus, to prove (5), we may assume $r \ge 6$. In what follows, we shall first establish (5) for some special values of k.

7.2 Critical Values of k

Notice that there exist some *special values* of k at which (5) changes: the smallest values in I_i for $0 \leq i \leq 5$. That is, $k = 0$, $k = 1$, k is odd and k is the smallest integer with $k > 2\sqrt{r+4} - 3$ or k is even and k is the smallest integer with $k > 2\sqrt{r+2} - 2$, $k = r + 2$, $k = r + 3$, and $k - r$ is odd and k is the smallest integer with $k > r + \sqrt{4r+21} - 2$ or $k - r$ is even and k is the smallest integer with $k > r + \sqrt{4r+9} - 1$. The number k satisfying one of the above properties is said to be *critical*. In this section, we prove (5) holds when k is critical.

7.2.1 Khun-Tuker Conditions

First, we prove (5) holds when $k = 0$ by techniques from non-linear optimization.

Let $E \subseteq R^n$ and $g_i(\mathbf{x}) \leq 0$ $(1 \leq i \leq m)$ be functional constraints. A point $\mathbf{x}$ that satisfies all functional constraints is said to be *feasible*. A functional constraint $g_i(\mathbf{x}) \leq 0$ is said to be *active* at a feasible point $\mathbf{x}$ if $g_i(\mathbf{x}) = 0$, and *inactive* if $g_i(\mathbf{x}) < 0$. Suppose $\mathbf{x}$ is a feasible point, and let J be the set of indices j for which $g_j(\mathbf{x}) = 0$. Then $\mathbf{x}$ is said to be a *regular point* of the constraints if the gradient vectors $\nabla g_j(\mathbf{x})$ $(j \in J)$ are linearly independent. The following result (see p. 314, [61]) gives necessary conditions for f to achieve a relative maximum at a regular point.

Khun-Tuker Conditions: Suppose $f(\mathbf{x})$ and $g_i(\mathbf{x})$ $(i = 1, 2, \cdots, m)$ possess continuous first order partial derivatives. Suppose $\mathbf{x}^*$ is a relative maximum point for the problem

$$\begin{aligned} &\text{maximize} \quad f(\mathbf{x}) \\ &\text{subject to} \quad g_i(\mathbf{x}) \leq 0, i = 1, 2, \cdots, m, \end{aligned}$$

and suppose $\mathbf{x}^*$ is a regular point for the constraints. Then there is a vector $(\mu_1, \mu_2, \cdots, \mu_m)$ with $\mu_i \geq 0$ such that

$$\frac{\partial f(\mathbf{x}^*)}{\partial x_j} - \sum_{i=1}^{m} \mu_i \frac{\partial g_i(\mathbf{x}^*)}{\partial x_j} = 0,$$

$$\mu_i g_i(\mathbf{x}^*) = 0, i = 1, 2, \cdots, m.$$

Next, we use Khun-Tuker Conditions to solve the above Nonlinear-IPP problem. We first show that every point $\mathbf{x}$ satisfying (26) is a regular point. To do this, we need to find gradient vector of

$g_i(\mathbf{x})$ at $\mathbf{x} = (x_1, \ldots, x_9)$. By simple calculations, we see that

$$\begin{aligned}
\nabla g_1(\mathbf{x}) &= (-x_2, -x_1, 1, 0, 0, 0, 0, 0, 0), \\
\nabla g_2(\mathbf{x}) &= (0, 0, 0, 1, -y_3, -y_2, 0, 0, 0), \\
\nabla g_3(\mathbf{x}) &= (0, 0, 0, 0, 0, 0, -z_3, 1, -z_1), \\
\nabla g_4(\mathbf{x}) &= (1, 0, 0, 1, 0, 0, 1, 0, 0), \\
\nabla g_5(\mathbf{x}) &= (0, 1, 0, 0, 1, 0, 0, 1, 0), \\
\nabla g_6(\mathbf{x}) &= (0, 0, 1, 0, 0, 1, 0, 0, 1).
\end{aligned} \tag{28}$$

It is an easy exercise to show that if $\sum_{i=1}^{6} c_i \nabla g_i(\mathbf{x}) = \mathbf{0}$ then $c_i = 0$ for all $1 \leq i \leq 6$. Hence these six vectors $\nabla g_i(\mathbf{x})$ are linearly independent. Therefore, we have the following.

Lemma 7.2.1. *Every nonzero point* $\mathbf{x}$ *satisfying (26) is a regular point of (26).*

The Khun-Tuker conditions are necessary conditions for $f(\mathbf{x})$ to achieve a relative maximum at regular points. For the Nonlinear-IPP problem, if we relax (27), it can be stated as follows.

Lemma 7.2.2. *Suppose* f *and* g_i, $1 \leq i \leq 6$, *are given as in (25) and (26). If* f *has a relative maximum at* $\mathbf{x} = (x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3)$, *then there is a vector* $(\mu_1, \mu_2, \cdots, \mu_6)$ *with* $\mu_i \geq 0$ *for all* $1 \leq i \leq 6$ *such that*

$$\begin{aligned}
\frac{\partial f(\mathbf{x})}{\partial x_j} - \sum_{i=1}^{6} \mu_i \frac{\partial g_i(\mathbf{x})}{\partial x_j} &= 0, \\
\frac{\partial f(\mathbf{x})}{\partial y_j} - \sum_{i=1}^{6} \mu_i \frac{\partial g_i(\mathbf{x})}{\partial y_j} &= 0, \\
\frac{\partial f(\mathbf{x})}{\partial z_j} - \sum_{i=1}^{6} \mu_i \frac{\partial g_i(\mathbf{x})}{\partial z_j} &= 0, \\
\mu_i g_i(\mathbf{x}) &= 0, 1 \leq i \leq 6.
\end{aligned}$$

Note that the conditions $\mu_i g_i(\mathbf{x}) = 0$ and $\mu_i \geq 0$ imply that if g_i is not active at $\mathbf{x}$ then $\mu_i = 0$. This shows that only active constraints will be used when determining potential maximum points.

Now we are ready to prove the following result.

Lemma 7.2.3. *(5) holds when* $q \geq 15$ *and* $k = 0$.

Proof. By the above analysis, our objective is to find a solution $\mathbf{x} = (x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3)$ which maximizes (25) subject to (26). It turns out that our optimal solution $\mathbf{x} \in N^9$ and also satisfies the constraints (vii)-(ix) in (27).

Let $L(\mathbf{x}) = f(\mathbf{x}) - \sum_{i=1}^{6} \mu_i g_i(\mathbf{x})$, $\mu_i \geq 0$ for $1 \leq i \leq 6$. By Lemma 7.2.2, we have

$$\begin{aligned}
&\frac{\partial L}{\partial x_1} = \mu_1 x_2 - \mu_4 = 0, && \frac{\partial L}{\partial x_2} = \mu_1 x_1 - \mu_5 = 0,\\
&\frac{\partial L}{\partial x_3} = 1 - \mu_1 - \mu_6 = 0, && \frac{\partial L}{\partial y_1} = 1 - \mu_2 - \mu_4 = 0,\\
&\frac{\partial L}{\partial y_2} = \mu_2 y_3 - \mu_5 = 0, && \frac{\partial L}{\partial y_3} = \mu_2 y_2 - \mu_6 = 0,\\
&\frac{\partial L}{\partial z_1} = \mu_3 z_3 - \mu_4 = 0, && \frac{\partial L}{\partial z_2} = 1 - \mu_3 - \mu_5 = 0,\\
&\frac{\partial L}{\partial z_3} = \mu_3 z_1 - \mu_6 = 0, && \mu_i \geq 0, \mu_i g_i = 0, 1 \leq i \leq 6.
\end{aligned}$$

If there is a feasible point $\mathbf{x}$ such that $g_i(\mathbf{x})$ is inactive for some $1 \leq i \leq 6$, then $\mu_i = 0$. In this case, it is easy to show $f(\mathbf{x}) \leq 2q - 2 < 3q - 6r$.

Therefore, it follows from Theorem 4.2.7 that we only need to consider those feasible points $\mathbf{x}$ such that all functional constraints $g_i(\mathbf{x})$, $1 \leq i \leq 6$, are active. Thus, we may assume that all μ_i are positive. Hence,

$$\begin{aligned}
&\mu_4 = 1 - \mu_2, \quad \mu_5 = 1 - \mu_3, \quad \mu_6 = 1 - \mu_1,\\
&x_1 = \frac{1 - \mu_3}{\mu_1}, \quad x_2 = \frac{1 - \mu_2}{\mu_1}, \quad y_2 = \frac{1 - \mu_1}{\mu_2},\\
&y_3 = \frac{1 - \mu_3}{\mu_2}, \quad z_1 = \frac{1 - \mu_1}{\mu_3}, \quad z_3 = \frac{1 - \mu_2}{\mu_3}.
\end{aligned}$$

Since all $g_i(\mathbf{x})$, $1 \leq i \leq 6$, are active, we have

$$\begin{aligned}
r^2 + 2r - \frac{1 - \mu_3}{\mu_2} - \frac{1 - \mu_2}{\mu_3} - \frac{(1 - \mu_2)(1 - \mu_3)}{\mu_1^2} = 0,\\
r^2 + 2r - \frac{1 - \mu_3}{\mu_1} - \frac{1 - \mu_1}{\mu_3} - \frac{(1 - \mu_3)(1 - \mu_1)}{\mu_2^2} = 0,\\
r^2 + 2r - \frac{1 - \mu_2}{\mu_1} - \frac{1 - \mu_1}{\mu_2} - \frac{(1 - \mu_1)(1 - \mu_2)}{\mu_3^2} = 0.
\end{aligned}$$

By using Maple 9, we obtain a unique positive solution

$$\mu_1 = \mu_2 = \mu_3 = \frac{1}{r+1}, \ \mu_4 = \mu_5 = \mu_6 = \frac{r}{r+1}.$$

It follows that $(r, r, r^2, r^2, r, r, r, r^2, r)$ is the unique regular point which satisfies the necessary conditions in Lemma 7.2.2 for a relative maximum. Note that $(r, r, r^2, r^2, r, r, r, r^2, r) \in N^9 \subseteq [2, q-4]^9$ and satisfies constraints (vii)-(ix) in (27). Since $f(x)$ is continuous on $[2, q-4]^9$, we see that $f(x)$ has a maximum. Hence by the uniqueness of $(r, r, r^2, r^2, r, r, r, r^2, r)$ as a regular point, we see that it is the absolute maximum point. Therefore, $F(3, q) = \max_{\mathbf{x} \in N^9} f(\mathbf{x}) = 3r^2$ for $k = 0$. □

7.2.2 Other Critical Values of k

In this section, we prove (5) holds for other critical values of k. Before stating next result, let us recall that for any finite real number x, $\lfloor x \rfloor$ denotes the greatest integer in x, $\lceil x \rceil$ designates the ceiling of x.

The following result is proved in [36] (Theorem 33).

Lemma 7.2.4. *$F(3,q) \leq 3q + 6 - \lceil 6\sqrt{q+1} \rceil$ when $q \geq 15$.*

Using Lemma 7.2.4, we prove (5) holds for $k = r + 2$ quickly.

Lemma 7.2.5. *(5) holds when $q \geq 15$ and $k = r + 2$.*

Proof. Since $q = r^2+2r+k$ and $k = r+2$, $\lceil 6\sqrt{q+1} \rceil = \lceil 6\sqrt{r^2+3r+3} \rceil = 6r+10$. By Lemma 7.2.4, $F(3,q) \leq 3(r^2+2r+k)+6-\lceil 6\sqrt{r^2+2r+k+1} \rceil = 3(r^2+3r+2)+6-(6r+10) = 3r^2+3r+2 = 3r^2+3k-4$. Note that $(efF(3,q)) = 3r^2+3k-4 = 3r^2+3r+2$ when $q \geq 15$ and $k = r+2$. Hence, (5) holds when $q \geq 15$ and $k = r+2$. □

Next, we shall establish (5) for critical values of k (except $k = 0$ and $k = r + 2$). The following fact will be convenient for that purpose.

Lemma 7.2.6. *Let $\beta, \gamma, s, t > 0$. If $\beta + \gamma \leq s$ and $\gamma \leq t \leq \frac{s}{2}$, then $\beta\gamma \leq (s-t)t$.*

Proof. Since $\beta + \gamma \leq s$ and $\beta, \gamma > 0$, $\beta\gamma \leq (s-\gamma)\gamma = (\frac{s}{2})^2 - (\gamma - \frac{s}{2})^2$. Since $\gamma \leq t \leq \frac{s}{2}$, $\beta\gamma \leq (\frac{s}{2})^2 - (t - \frac{s}{2})^2$, which implies $\beta\gamma \leq (s-t)t$. □

In order to combine similar arguments, we define

$$m = \begin{cases} 2 & \text{if } k = 1; \\ 3 & \text{if } k \text{ is odd and } k \text{ is the smallest integer with } k > 2\sqrt{r+4} - 3, \\ & \text{or } k \text{ is even and } k \text{ is the smallest integer with } k > 2\sqrt{r+2} - 2; \\ 5 & \text{if } k = r+3; \\ 6 & \text{if } k - r \text{ is odd and } k \text{ is the smallest integer with } k > r + \sqrt{4r+21} - 2, \\ & \text{or } k - r \text{ is even and } k \text{ is the smallest integer with } k > r + \sqrt{4r+9} - 1. \end{cases} \tag{29}$$

Note that if $q = r^2 + 2r + k$ and k is critical, then (5) is equal to $3r^2 + 3k - m$.

The following lemma can be easily verified.

Lemma 7.2.7. *Suppose $r \geq 6$. Then*

(i) if $m = 3$ then $4 \leq k < r$, $(k - \frac{1}{2})^2 > r + \frac{1}{4}$, $(\frac{r+4-k}{2})^2 \geq r$, and $(\frac{k+4}{2})^2 > r + 6$, and

(ii) if $m = 6$ then $r + 5 \leq k < 2r$, $(\frac{2r+5-k}{2})^2 > r$, $(\frac{2r+8-k}{2})^2 > 2r + \frac{5}{4}$, $(k - r - 2)^2 > r + 1$, $(\frac{k-r+2}{2})^2 > r + 5$ if $k - r$ is even, and $(\frac{k-r+3}{2})^2 > r + 6$ if $k - r$ is odd.

The remainder of this section is devoted to proving the following lemma. The proof is quite tedious; the reader may want to read Section 7.3 first to see how it is applied in the proof of (5).

Lemma 7.2.8. *(5) holds when $q \geq 24$ and k is critical.*

Proof. By Lemma 7.1.1, we may assume that $q \geq 49$, and hence, $r \geq 6$. Suppose for a contradiction that $F(3, q) \geq 3r^2 + 3k - m + 1$. Then by Theorem 5.2.5 and Theorem 6.3.1, there exists some $\mathbf{x} = (x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3) \in N^9$, where $N = \{2, \ldots, q - 4\}$, such that $\mathbf{x}$ satisfies (14) and $x_3 + y_1 + z_2 = F(3, q) \geq 3r^2 + 3k - m + 1$. By symmetry among x_3, y_1, z_2 in (14), we may assume $x_3 \geq y_1 \geq z_2$. For visual convenience, we express x_j, y_j, z_j for $1 \leq j \leq 3$ in a matrix form as follows,

$$\begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ z_1 & z_2 & z_3 \end{pmatrix} = \begin{pmatrix} r + a & r + b & r^2 + k - \lfloor \frac{m}{2} \rfloor + c \\ r^2 + k - \lfloor \frac{m}{2} \rfloor + d & r + e & r + f \\ r + g & z_2 & r + h \end{pmatrix}$$

where a, b, c, d, e, f, g and h are integers.

Because $x_3 + y_1 + z_2 \geq 3r^2 + 3k - m + 1$, we have

(P1) $z_2 \geq r^2 + k + 1 - m + 2\lfloor \frac{m}{2} \rfloor - (c + d)$.

Because $x_3 \geq y_1 \geq z_2$, we have $r^2 + k - \lfloor \frac{m}{2} \rfloor + c \geq r^2 + k - \lfloor \frac{m}{2} \rfloor + d \geq r^2 + k + 1 - m + 2\lfloor \frac{m}{2} \rfloor - (c + d)$, which implies

(P2) $\frac{3\lfloor \frac{m}{2} \rfloor - m + 1 - c}{2} \leq d \leq c$.

From (P2), we have $c \geq \lfloor \frac{m}{2} \rfloor - \frac{m-1}{3}$. Recall that $q = r^2 + 2r + k$. Since $x_3 \leq q - 4$, $c \leq 2r - 4 + \lfloor \frac{m}{2} \rfloor$. Hence, we have

(P3) $\lfloor \frac{m}{2} \rfloor - \frac{m-1}{3} \leq c \leq 2r - 4 + \lfloor \frac{m}{2} \rfloor$.

By (vi) of (14), $z_3 \leq q - (r^2 + k - \lfloor \frac{m}{2} \rfloor + c) - y_3$. Since $y_3 \geq 2$, we have

(P4) $z_3 \leq 2r + \lfloor \frac{m}{2} \rfloor - 2 - c$.

By (i) of (14), we have

(P5) $(r + a)(r + b) \geq r^2 + k - \lfloor \frac{m}{2} \rfloor + c$.

By (ii) of (14), we have

(P6) $(r + e)(r + f) \geq r^2 + k - \lfloor \frac{m}{2} \rfloor + d$.

By (iii) of (14) and by (P1), we have

(P7) $(r + g)(r + h) \geq r^2 + k + 1 - m + 2\lfloor \frac{m}{2} \rfloor - (c + d)$.

By adding (iv), (v), (vi) of (14) and by (P1), we have

(P8) $a + b + e + f + g + h \leq m - 1$.

By (vi) of (14) again, we have

(P9) $c + f + h \leq \lfloor \frac{m}{2} \rfloor$.

Note that for any real numbers x and y, $xy \leq (\frac{x+y}{2})^2$. Suppose $a + b \leq n$ for some integer n. Then $(r + a)(r + b) \leq (\frac{2r+a+b}{2})^2 \leq r^2 + nr + \frac{n^2}{4}$. On the other hand, it follows from (P5) that $(r + a)(r + b) \geq r^2 + k - \lfloor \frac{m}{2} \rfloor + c$. So $c \leq nr + \lfloor \frac{m}{2} \rfloor - k + \frac{n^2}{4}$. Similarly, if $e + f \leq n$ then by (P6) we have $d \leq nr + \lfloor \frac{m}{2} \rfloor - k + \frac{n^2}{4}$. Therefore, we have the following.

(P10) For any $n \in \{-1, 0, 1\}$, if $c \geq nr + \lfloor \frac{m}{2} \rfloor - k + 1$ then $a + b \geq n + 1$, and if $d \geq nr + \lfloor \frac{m}{2} \rfloor - k + 1$ then $e + f \geq n + 1$.

(P11) For any $n \in \{2, 3\}$, if $c \geq n(r + 1) + \lfloor \frac{m}{2} \rfloor - k$ then $a + b \geq n + 1$, and if $d \geq n(r + 1) + \lfloor \frac{m}{2} \rfloor - k$ then $e + f \geq n + 1$.

We shall derive a contradiction to (14) by showing $x_1x_2 < x_3$, or $y_2y_3 < y_1$, or $z_1z_3 < z_2$. To achieve this, we proceed to prove five claims concerning the ranges of c and d.

Claim 1. $c \leq 3r + 2 + \lfloor \frac{m}{2} \rfloor - k$.

Suppose Claim 1 is false. Then $c \geq 3r + 3 + \lfloor \frac{m}{2} \rfloor - k$, and hence $a + b \geq 4$ (by (P11)). By (P3), $3r + 3 + \lfloor \frac{m}{2} \rfloor - k \leq c \leq 2r - 4 + \lfloor \frac{m}{2} \rfloor$, and so, $k \geq r + 7$. Thus, $m = 6$. By (P4), $z_3 \leq 2r + 1 - c \leq 2r + 1 - (3r + 6 - k) = k - r - 5 < r - 5$ (by (ii) of Lemma 7.2.7).

Suppose $d \geq r + 4 - k$. Then $e + f \geq 2$ by (P10). Therefore, since $a + b \geq 4$ and by (P8), we have $g + h \leq -1$, and so, $z_1 + z_3 = r + g + r + h \leq 2r - 1$. Since $z_3 \leq 2r + 1 - c < r - 5 < \frac{2r-1}{2}$, it follows from Lemma 7.2.6 (with $z_1, z_3, 2r - 1, 2r + 1 - c$ as β, γ, s, t, respectively) that $z_1 z_3 \leq (2r - 1 - (2r + 1 - c))(2r + 1 - c)$. So by (P1),

$$\begin{aligned} z_1 z_3 - z_2 &\leq (c - 2)(2r + 1 - c) - (r^2 + k + 1 - (c + d)) \\ &\leq (c - 2)(2r + 1 - c) - (r^2 + k + 1 - 2c) \quad \text{(because } d \leq c\text{)} \\ &= -(c - 2 - (r + \tfrac{1}{2}))^2 + r - k + \tfrac{13}{4} \\ &< 0 \text{ (because } k \geq r + 7\text{), a contradiction.} \end{aligned}$$

Therefore, $d \leq r + 3 - k$. By (P2), $d \geq \frac{4-c}{2}$. Since $c \leq 2r - 1$ (by (P3)), $d \geq \frac{4-c}{2} > 2 - r$. Therefore, since $k \geq r + 7$, $d > 2 - (k - 7) = 9 - k$. So by (P10), $e + f \geq 1$. Hence, because $a + b \geq 4$ and by (P8), we have $g + h \leq 0$, and so, $z_1 + z_3 = r + g + r + h \leq 2r$. By Lemma 7.2.6 again, $z_1 z_3 \leq (2r - (2r + 1 - c))(2r + 1 - c)$. So by (P1),

$$\begin{aligned} z_1 z_3 - z_2 &\leq (c - 1)(2r + 1 - c) - (r^2 + k + 1 - (c + d)) \\ &\leq (c - 1)(2r + 1 - c) - (r^2 + k + 1) + c + (r + 3 - k) \\ &= -((c - 1) - (r + \tfrac{1}{2}))^2 - 2k + 2r + \tfrac{13}{4} \\ &< 0 \text{ (because } k \geq r + 7\text{), a contradiction.} \quad \square \end{aligned}$$

Claim 2. $c \leq 2r + 1 + \lfloor \frac{m}{2} \rfloor - k$.

Otherwise, $c \geq 2r + 2 + \lfloor \frac{m}{2} \rfloor - k$. Then $a + b \geq 3$ (by (P11)) and $m \neq 2$ (by (P3)). By (ii) and (iii) of Lemma 7.2.7, we have $k < 2r$. Hence $c \geq 5$ if $m = 5$ and $c \geq 6$ if $m = 6$.

Suppose $m = 3$. Then $c \geq 2r + 3 - k \geq r + 3$ (because $k < r$ by (i) of Lemma 7.2.7) and $z_3 \leq 2r - 1 - c$ (by (P4)), and so, $z_3 \leq 2r - 1 - c \leq r - 4 \leq \frac{2r-8}{2}$. Suppose $d \geq 2 - k$, then $e + f \geq 1$ by (P10). Hence, because $a + b \geq 3$ and by (P8), we have $g + h \leq -2$. Then $z_1 + z_3 = r + g + r + h \leq 2r - 2$.

By Lemma 7.2.6, $z_1z_3 \leq (2r-2-(2r-1-c))(2r-1-c)$. Thus, by (P1),

$$\begin{aligned} z_1z_3 - z_2 &\leq (c-1)(2r-1-c) - (r^2+k-(c+d)) \\ &\leq (c-1)(2r-1-c) - (r^2+k) + 2c \quad \text{(because } d \leq c\text{)} \\ &= -(c-1-r)^2 - k + 2 \\ &< 0 \text{ (because } k \geq 4 \text{ by (i) of Lemma 7.2.7), a contradiction.} \end{aligned}$$

So $d \leq 1-k$. Since $d \geq \frac{1-c}{2}$ (by (P2)) and $c \leq 2r-3$ (by (P3)), we have $d \geq 2-r$, and so, $e+f \geq 0$ by (P10). Since $a+b \geq 3$ and by (P8), $g+h \leq -1$. Therefore, $z_1+z_3 = r+g+r+h \leq 2r-1$. By Lemma 7.2.6, $z_1z_3 \leq (2r-1-(2r-1-c))(2r-1-c)$. Thus by (P1),

$$\begin{aligned} z_1z_3 - z_2 &\leq c(2r-1-c) - (r^2+k-(c+d)) \\ &= -(c-r)^2 - k + d \\ &\leq -(c-r)^2 - 2k + 1 \quad \text{(because } d \leq 1-k\text{)} \\ &< 0 \text{ (because } k \geq 4 \text{ by (i) of Lemma 7.2.7), a contradiction.} \end{aligned}$$

Therefore $m \in \{5, 6\}$. We consider three cases according to d.

Case 1. $d \geq 2r+2+\lfloor \frac{m}{2} \rfloor - k$.

Then $e+f \geq 3$ by (P11). Since $a+b \geq 3$ and by (P8), we have $g+h \leq m-7$, and so, $z_1+z_3 = r+g+r+h \leq 2r+m-7$. Thus $\min\{z_1, z_3\} \leq \frac{2r+m-7}{2}$. By applying Lemma 7.2.6 (with $\max\{z_1, z_3\}, \min\{z_1, z_3\}, 2r+m-7, \frac{2r+m-7}{2}$ as β, γ, s, t, respectively), we have $z_1z_3 \leq (2r+m-7-\frac{2r+m-7}{2})(\frac{2r+m-7}{2})$. Hence by (P1), we have

$$z_1z_3 - z_2 \leq (\frac{2r+m-7}{2})^2 - (r^2+k+1-m+2\lfloor \frac{m}{2} \rfloor - (c+d)).$$

Suppose $m=5$. Then $k=r+3$. So $0 \leq z_1z_3 - z_2 \leq (r-1)^2 - (r^2+k-(c+d)) \leq (r-1)^2 - r^2 - (r+3) + 2c$ (because $d \leq c$). This implies $c \geq \frac{3r+2}{2}$. Then by (P4), $z_3 \leq 2r-c \leq \frac{r-2}{2} < \frac{2r-2}{2}$. Because $z_1+z_3 \leq 2r-2$ and by Lemma 7.2.6, $z_1z_3 \leq (2r-2-(2r-c))(2r-c)$. Thus by (P1), we have

$$\begin{aligned} z_1z_3 - z_2 &\leq (c-2)(2r-c) - (r^2+k-(c+d)) \\ &\leq (c-2)(2r-c) - r^2 - k + 2c \quad \text{(because } d \leq c\text{)} \\ &= -(c-r-2)^2 + 4 - k \\ &< 0 \text{ (because } k = r+3\text{), a contradiction.} \end{aligned}$$

So $m = 6$. Then $k \geq r + 5$ (by (iii) of Lemma 7.2.7). So $0 \leq z_1 z_3 - z_2 \leq \frac{(2r-1)^2}{4} - (r^2 + k + 1 - (c + d)) \leq \frac{(2r-1)^2}{4} - (r^2 + (r + 5) + 1) + 2c$ (because $d \leq c$), which implies $c \geq r + 3$. Then by (P4), $z_3 \leq 2r + 1 - c \leq r - 2 < \frac{2r-1}{2}$. Because $z_1 + z_3 \leq 2r - 1$ and by Lemma 7.2.6, $z_1 z_3 \leq (2r - 1 - (2r + 1 - c))(2r + 1 - c)$. So by (P1), we have

$$\begin{aligned} z_1 z_3 - z_2 &\leq (c-2)(2r+1-c) - (r^2 + k + 1 - (c+d)) \\ &\leq (c-2)(2r+1-c) - r^2 - k - 1 + 2c \quad \text{(because } d \leq c\text{)} \\ &= -(c - r - \tfrac{5}{2})^2 + r - k + \tfrac{13}{4} \\ &\leq r - (r+5) + \tfrac{13}{4} \quad \text{(since } k \geq r+5\text{)} \\ &< 0, \text{ a contradiction.} \end{aligned}$$

Case 2. $r + 1 + \lfloor \frac{m}{2} \rfloor - k \leq d \leq 2r + 1 + \lfloor \frac{m}{2} \rfloor - k$.

Then $e + f \geq 2$ by (P10). Therefore, since $a + b \geq 3$ and by (P8), we have $g + h \leq m - 6$, and hence, $z_1 + z_3 = r + g + r + h \leq 2r + m - 6$. From (P9), $f + h \leq \lfloor \frac{m}{2} \rfloor - c$.

Suppose $h \leq \frac{\lfloor \frac{m}{2} \rfloor - c}{2} + 1$. Then $z_3 = r + h \leq r + \frac{\lfloor \frac{m}{2} \rfloor - c}{2} + 1 \leq r - \frac{1}{2}$ (since $c \geq 5$ when $m = 5$ and $c \geq 6$ when $m = 6$). So $z_3 \leq r + \frac{\lfloor \frac{m}{2} \rfloor - c}{2} + 1 \leq \frac{2r+m-6}{2}$. By Lemma 7.2.6, $z_1 z_3 \leq (2r + m - 6 - (r + \frac{\lfloor \frac{m}{2} \rfloor - c}{2} + 1))(r + \frac{\lfloor \frac{m}{2} \rfloor - c}{2} + 1)$. If $m = 5$, then $k = r + 3$ and, by (P1),

$$\begin{aligned} z_1 z_3 - z_2 &\leq (r - 2 - \tfrac{2-c}{2})(r + 1 + \tfrac{2-c}{2}) - (r^2 + k - (c+d)) \\ &= -(\tfrac{c-7}{2})^2 - r - k + \tfrac{25}{4} + d \\ &\leq r - 2k + \tfrac{37}{4} \quad \text{(because } d \leq 2r + 3 - k\text{)} \\ &= r - 2(r+3) + \tfrac{37}{4} \quad \text{(because } k = r + 3\text{)} \\ &< 0 \text{ (because } r \geq 6\text{), a contradiction.} \end{aligned}$$

So $m = 6$. Then $k \geq r + 5$ (by (ii) of Lemma 7.2.7) and $d \leq 2r + 4 - k$ (by assumption of Case 2). By (P1), we have

$$\begin{aligned} z_1 z_3 - z_2 &\leq (r - 1 - \tfrac{3-c}{2})(r + 1 + \tfrac{3-c}{2}) - (r^2 + k + 1 - (c+d)) \\ &= -(\tfrac{c-7}{2})^2 - k + d + 5 \\ &\leq -k + (2r + 4 - k) + 5 \quad \text{(because } d \leq 2r + 4 - k\text{)} \\ &\leq 2r + 9 - 2(r+5) \quad \text{(because } k \geq r + 5\text{)} \\ &< 0, \text{ a contradiction.} \end{aligned}$$

Therefore $h > \frac{\lfloor \frac{m}{2} \rfloor - c}{2} + 1$. Then $f < \frac{\lfloor \frac{m}{2} \rfloor - c}{2} - 1$. Because f is an integer, $f \leq \frac{\lfloor \frac{m}{2} \rfloor - c - 3}{2}$. We shall derive a contradiction by proving $y_2 y_3 < y_1$.

By Claim 1 and assumption of Case 2, $c + d \leq (3r + 2 + \lfloor \frac{m}{2} \rfloor - k) + (2r + 1 + \lfloor \frac{m}{2} \rfloor - k) = 5r + 3 + 2\lfloor \frac{m}{2} \rfloor - 2k$. It follows from (P7) that $(r+g)(r+h) \geq r^2 + k + 1 - m + 2\lfloor \frac{m}{2} \rfloor - (c+d) \geq r^2 + 3k - 5r - m - 2$. Then, since $k = r + 3$ when $m = 5$ and $k \geq r + 5$ when $m = 6$ (by (ii) of Lemma 7.2.7), we have $(r + g)(r + h) \geq r^2 - 2r + 2$. So $g + h \geq -1$; as otherwise, $(r + g)(r + h) \leq (\frac{2r+g+h}{2})^2 \leq r^2 - 2r + 1$, a contradiction. Since $a + b \geq 3$ and by (P8), $e + f \leq m - 3$. Hence, $y_2 + y_3 = r + e + r + f \leq 2r + m - 3$. Because $c \geq 5$, $y_3 = r + f \leq r + \frac{\lfloor \frac{m}{2} \rfloor - c - 3}{2} < r - 2 < \frac{2r+m-3}{2}$. Hence by Lemma 7.2.6, $y_2 y_3 \leq (2r + m - 3 - (r + \frac{\lfloor \frac{m}{2} \rfloor - c - 3}{2}))(r + \frac{\lfloor \frac{m}{2} \rfloor - c - 3}{2})$. If $m = 5$, then $c \geq 2r + 4 - k$ (by the assumption that Claim 2 fails) and $d \geq r + 3 - k$ (by assumption of Case 2), and

$$\begin{aligned}
y_2 y_3 - y_1 &\leq (r + 2 + \tfrac{c+1}{2})(r - \tfrac{c+1}{2}) - (r^2 + k - 2 + d) \\
&= -(\tfrac{c+3}{2})^2 + 2r - k - d + 3 \\
&\leq -(\tfrac{c+3}{2})^2 + r \quad \text{(because } d \geq r + 3 - k\text{)} \\
&\leq -(\tfrac{2r+7-k}{2})^2 + r \quad \text{(because } c \geq 2r + 4 - k\text{)} \\
&< 0 \text{ (by (ii) of Lemma 7.2.7), a contradiction.}
\end{aligned}$$

So $m = 6$. Then $c \geq 2r+5-k$ (by the assumption that Claim 2 fails) and $d \geq r+4-k$ (by assumption of Case 2). Hence,

$$\begin{aligned}
y_2 y_3 - y_1 &\leq (r + 3 + \tfrac{c}{2})(r - \tfrac{c}{2}) - (r^2 + k - 3 + d) \\
&= -(\tfrac{c+3}{2})^2 + 3r + \tfrac{21}{4} - k - d \\
&\leq -(\tfrac{c+3}{2})^2 + 2r + \tfrac{5}{4} \quad \text{(because } d \geq r + 4 - k\text{)} \\
&\leq -(\tfrac{2r+8-k}{2})^2 + 2r + \tfrac{5}{4} \quad \text{(because } c \geq 2r + 5 - k\text{)} \\
&< 0 \text{ (by (ii) of Lemma 7.2.7), a contradiction.}
\end{aligned}$$

Case 3. $d \leq r + \lfloor \frac{m}{2} \rfloor - k$.

We claim that $e + f \geq 0$. For otherwise, $(r + e)(r + f) \leq (\frac{2r+e+f}{2})^2 \leq r^2 - r + \frac{1}{4}$. So by (P6) and (P2), $r^2 - r + \frac{1}{4} \geq r^2 + k - \lfloor \frac{m}{2} \rfloor + \frac{3\lfloor \frac{m}{2} \rfloor - m + 1 - c}{2}$. Hence $c \geq 2k + 2r + \frac{1}{2} + \lfloor \frac{m}{2} \rfloor - m$, contradicting (P3) (because $m \in \{5, 6\}$ and $k \geq r + 3$ by (ii) of Lemma 7.2.7).

Therefore, since $a + b \geq 3$ and by (P8), we have $g + h \leq m - 4$. Hence, $z_1 + z_3 = r + g + r + h \leq 2r + m - 4$. By (P9), $f + h \leq \lfloor \frac{m}{2} \rfloor - c$.

Suppose $h \leq \frac{\lfloor \frac{m}{2} \rfloor - c + 1}{2}$. Then because $c \geq 5$ when $m = 5$ and $c \geq 6$ when $m = 6$, $z_3 = r + h \leq r + \frac{\lfloor \frac{m}{2} \rfloor - c + 1}{2} \leq r - 1 < \frac{2r+m-4}{2}$. By Lemma 7.2.6, $z_1 z_3 \leq (2r + m - 4 - (r + \frac{\lfloor \frac{m}{2} \rfloor - c + 1}{2}))(r + \frac{\lfloor \frac{m}{2} \rfloor - c + 1}{2})$. If $m = 5$, then $d \leq r + 2 - k$ (by assumption of Case 3) and $k = r + 3$ and, by (P1),

$$\begin{aligned} z_1 z_3 - z_2 &\leq (r + 1 - \tfrac{3-c}{2})(r + \tfrac{3-c}{2}) - (r^2 + k - (c + d)) \\ &= -(\tfrac{c-4}{2})^2 + r - k + d + \tfrac{13}{4} \\ &\leq -(\tfrac{c-4}{2})^2 + r - k + (r + 2 - k) + \tfrac{13}{4} \\ &\leq 2r - 2(r + 3) + \tfrac{13}{4} \quad \text{(because } k = r + 3\text{)} \\ &< 0, \text{ a contradiction.} \end{aligned}$$

So $m = 6$. Then $d \geq \frac{4-c}{2}$ (by (P2)), $d \leq r + 3 - k$ (by assumption of Case 3), and $k \geq r + 5$ (by (ii) of Lemma 7.2.7). Since $\frac{4-c}{2} \leq d \leq r + 3 - k$, we have $\frac{c-4}{2} \geq k - r - 3 > 0$. By (P1),

$$\begin{aligned} z_1 z_3 - z_2 &\leq (r + 2 - \tfrac{4-c}{2})(r + \tfrac{4-c}{2}) - (r^2 + k + 1 - (c + d)) \\ &= -(\tfrac{c-4}{2})^2 + 2r - k + d + 3 \\ &\leq -(\tfrac{c-4}{2})^2 + 3r - 2k + 6 \quad \text{(because } d \leq r + 3 - k\text{)} \\ &\leq -(k - r - 3)^2 - 2(k - r - 3) + r \quad \text{(because } \tfrac{c-4}{2} \geq k - r - 3 > 0\text{)} \\ &= -(k - r - 2)^2 + r + 1 \\ &< 0 \text{ (by (ii) of Lemma 7.2.7), a contradiction.} \end{aligned}$$

So $h > \frac{\lfloor \frac{m}{2} \rfloor - c + 1}{2}$. Then $f < \frac{\lfloor \frac{m}{2} \rfloor - c - 1}{2}$. Because f is an integer, $f \leq \frac{\lfloor \frac{m}{2} \rfloor - 2 - c}{2}$. By Claim 1 and by assumption of Case 3, $c + d \leq 4r + 2 + 2\lfloor \frac{m}{2} \rfloor - 2k$. Hence, by (P7),

$$\begin{aligned} (r + g)(r + h) &\geq r^2 + k - m + 1 + 2\lfloor \tfrac{m}{2} \rfloor - (c + d) \\ &\geq r^2 + k - m + 1 + 2\lfloor \tfrac{m}{2} \rfloor - (4r + 2 + 2\lfloor \tfrac{m}{2} \rfloor - 2k) \\ &= r^2 + 3k - 4r - m - 1 \\ &\geq r^2 - r + 2 \quad \text{(because } m \in \{5, 6\} \text{ and } k \geq r + 3\text{)}. \end{aligned}$$

So $g + h \geq 0$; for otherwise, $(r + g)(r + h) \leq (\frac{2r+g+h}{2})^2 \leq r^2 - r + \frac{1}{4}$. Since $a + b \geq 3$ and by (P8), we have $e + f \leq m - 4$, and so, $y_2 + y_3 = r + e + r + f \leq 2r + m - 4$. Since $y_3 = r + f \leq r + \frac{\lfloor \frac{m}{2} \rfloor - 2 - c}{2} < \frac{2r+m-4}{2}$ (because $c \geq 5$) and by Lemma 7.2.6, we have $y_2 y_3 \leq (2r + m - 4 - (r + \frac{\lfloor \frac{m}{2} \rfloor - 2 - c}{2}))(r + \frac{\lfloor \frac{m}{2} \rfloor - 2 - c}{2})$. If

$m = 5$ then $k = r + 3$ and

$$\begin{aligned} y_2y_3 - y_1 &\leq (r + 1 + \tfrac{c}{2})(r - \tfrac{c}{2}) - (r^2 + k - 2 + d) \\ &= -(\tfrac{c}{2})^2 - \tfrac{c}{2} + r - k + 2 - d \\ &\leq -(\tfrac{c}{2})^2 + r - k + 1 \quad \text{(because } d \geq \tfrac{2-c}{2} \text{ by (P2))} \\ &< 0 \text{ (since } k = r + 3\text{), a contradiction} \end{aligned}$$

So $m = 6$. Then $k \geq r + 5$ (by (ii) of Lemma 7.2.7) and $c \geq 2r + 5 - k$ (by the assumption that Claim 2 fails). Hence,

$$\begin{aligned} y_2y_3 - y_1 &\leq (r + 2 - \tfrac{1-c}{2})(r + \tfrac{1-c}{2}) - (r^2 + k - 3 + d) \\ &= -(\tfrac{c}{2})^2 - \tfrac{c}{2} + 2r - k + \tfrac{15}{4} - d \\ &\leq -(\tfrac{c}{2})^2 + 2r - k + \tfrac{7}{4} \quad \text{(because } d \geq \tfrac{4-c}{2} \text{ by (P2))} \\ &\leq -(\tfrac{c}{2})^2 + r - \tfrac{13}{4} \quad \text{(since } k \geq r + 5\text{)} \\ &\leq -(\tfrac{2r+5-k}{2})^2 + r - \tfrac{13}{4} \quad \text{(because } k \geq 2r + 5 - k\text{)} \\ &< 0 \text{ (by (ii) of Lemma 7.2.7), a contradiction.} \quad \square \end{aligned}$$

Claim 3. If $c \geq r + \lfloor \frac{m}{2} \rfloor - k + 1$ then $d \leq r + \lfloor \frac{m}{2} \rfloor - k$.

Suppose $c \geq r + \lfloor \frac{m}{2} \rfloor - k + 1$ and $d \geq r + \lfloor \frac{m}{2} \rfloor - k + 1$. Then by (P10), we have $a + b \geq 2$ and $e + f \geq 2$. So it follows from (P8) that $g + h \leq m - 5$. Thus, $z_1 + z_3 = r + g + r + h \leq 2r + m - 5$.

Suppose $m = 2$. Then $z_1 + z_3 \leq 2r - 3$, $d \leq c \leq 2r - 3$ (by (P2) and (P3)), and $c \geq r + 1$ (because $k = 1$ when $m = 2$). So by (P4), $z_3 \leq 2r - 1 - c \leq r - 2 < \frac{2r-3}{2}$. Hence by Lemma 7.2.6, $z_1z_3 \leq (2r - 3 - (2r - 1 - c))(2r - 1 - c)$. By (P1),

$$\begin{aligned} z_1z_3 - z_2 &\leq (c - 2)(2r - 1 - c) - (r^2 + 2 - (c + d)) \\ &= -(c - r - 1)^2 - 2r + d + 1 \\ &< 0 \text{ (because } d \leq c \leq 2r - 3\text{), a contradiction.} \end{aligned}$$

Now suppose $m = 3$. Then $k \geq 4$ (by (i) of Lemma 7.2.7) and $z_1 + z_3 \leq 2r - 2$. Suppose $c \geq r$. Then by (P4), $z_3 \leq 2r - 1 - c \leq \frac{2r-2}{2}$. By Lemma 7.2.6, $z_1z_3 \leq (2r - 2 - (2r - 1 - c))(2r - 1 - c)$. Hence by (P1),

$$\begin{aligned} z_1z_3 - z_2 &\leq (c - 1)(2r - 1 - c) - (r^2 + k - (c + d)) \\ &= -(c - r - 1)^2 - c + d + 2 - k \\ &< 0 \text{ (because } d \leq c \text{ and } k \geq 4\text{), a contradiction.} \end{aligned}$$

So $c \le r-1$. Since $z_1 z_3 \le (\frac{z_1+z_3}{2})^2 \le (r-1)^2$ and by (P1),

$$\begin{aligned} z_1 z_3 - z_2 &\le (r-1)^2 - (r^2 + k - (c+d)) \\ &= -2r - k + 1 + c + d \\ &< 0 \text{ (because } d \le c \le r-1 \text{ and } k \ge 4\text{), a contradiction.} \end{aligned}$$

So we have $m \in \{5, 6\}$. By Claim 2 and because $d \le c$ (by (P2)), $c + d \le 4r + 2 + 2\lfloor \frac{m}{2} \rfloor - 2k$. So by (P7), we have $(r+g)(r+h) \ge r^2 + k + 1 - m + 2\lfloor \frac{m}{2} \rfloor - (c+d) \ge r^2 + 3k - 4r - 1 - m$. Since $m \in \{5, 6\}$, $k \ge r + 3$ (by (ii) of Lemma 7.2.7). So $(r+g)(r+h) \ge r^2 - r + 2$. Therefore, $g + h \ge 0$; for otherwise, $(r+g)(r+h) \le (\frac{2r+g+h}{2})^2 \le r^2 - r + \frac{1}{4}$, a contradiction. We consider two cases.

Case 1. $g + h \ge 1$.

Then, since $m \le 6$ and $g + h \le m - 5$, we see that $m = 6$ and $g + h = 1$. Hence by (P8) and because $a + b \ge 2$ and $e + f \ge 2$, we have $a + b = 2$ and $e + f = 2$.

Since $g + h = 1$, $(r+g)(r+h) \le (\frac{2r+g+h}{2})^2 \le r^2 + r + \frac{1}{4}$. Hence by (P7), we have $c + d \ge r^2 + k + 1 - (r^2 + r + \frac{1}{4})$. Because $c + d$ is an integer, we have $c + d \ge k - r + 1$.

Recall the matrix representation of x_i, y_i, z_i. By (P1), we have $\sum_{i=1}^{3}(x_i + y_i + z_i) \ge 3r^2 + 6r + 3k$. By (iv), (v) and (vi) of (14), $x_i + y_i + z_i \le r^2 + 2r + k$ for $1 \le i \le 3$. Hence, $x_i + y_i + z_i = r^2 + 2r + k$ for $1 \le i \le 3$ and (P1) holds with equality. Therefore, $a + d + g = 3$, $b + e + 1 - (c + d) = 0$, and $c + f + h = 3$. Because $c + d \ge k - r + 1$ and $c \ge d$, we have $b + e \ge k - r$ and $c \ge \frac{k-r+1}{2}$.

Subcase 1.1. $b \ge \frac{k-r}{2}$.

Then $b \ge \lceil \frac{k-r}{2} \rceil$. Hence, $x_1 = r + (2 - b) \le r + 2 - \lceil \frac{k-r}{2} \rceil < r$ (because $k \ge r + 5$). Since $x_1 + x_2 = 2r + 2$ and by Lemma 7.2.6, $x_1 x_2 \le (2r + 2 - (r + 2 - \lceil \frac{k-r}{2} \rceil))(r + 2 - \lceil \frac{k-r}{2} \rceil)$. Recall from the matrix representation that $x_3 = r^2 + k - 3 + c$.

Suppose $k - r$ is even. Then $k > r + \sqrt{4r+9} - 1$ and $c \ge \frac{k-r+2}{2}$, and we have

$$\begin{aligned} x_1 x_2 - x_3 &\le (r + \tfrac{k-r}{2})(r + 2 - \tfrac{k-r}{2}) - (r^2 + k - 3 + c) \\ &\le (r + \tfrac{k-r}{2})(r + 2 - \tfrac{k-r}{2}) - (r^2 + k - 3 + \tfrac{k-r+2}{2}) \\ &= -(\tfrac{k-r+1}{2})^2 + r + \tfrac{9}{4} \\ &< 0 \text{ (because } k > r + \sqrt{4r+9} - 1\text{), a contradiction.} \end{aligned}$$

So $k-r$ is odd. Then $k > r + \sqrt{4r+21} - 2$ and $c \geq \frac{k-r+1}{2}$. Hence

$$\begin{aligned} x_1x_2 - x_3 &\leq (r + \tfrac{k-r+1}{2})(r + 2 - \tfrac{k-r+1}{2}) - (r^2 + k - 3 + c) \\ &\leq (r + \tfrac{k-r+1}{2})(r + 2 - \tfrac{k-r+1}{2}) - (r^2 + k - 3 + \tfrac{k-r+1}{2}) \\ &= r + \tfrac{17}{4} - (\tfrac{k-r+2}{2})^2 \\ &< 0 \text{ (because } k > r + \sqrt{4r+21} - 2\text{), a contradiction.} \end{aligned}$$

Subcase 1.2. $e \geq \frac{k-r+2}{2}$.

Since $g+h = 1$ and by (P7), $r^2+k+1-(c+d) \leq (r+g)(r+h) = (r+1-h)(r+h) = r^2+r+h-h^2$. Hence, $h^2-h-(c+d)+(k-r+1) \leq 0$, and so, $h \geq \frac{1}{2} - \sqrt{\frac{1}{4} + c + d - (k-r+1)} \geq \frac{1}{2} - (\frac{\frac{1}{4}+c+d-(k-r+1)}{2} + 1)$. Hence, $\frac{c+d-(k-r+1)}{2} + h > -1$. Since $c+f+h = 3$, $f = 3-c-h = 3 - \frac{c-d+(k-r+1)}{2} - \frac{c+d-(k-r+1)}{2} - h < 4 - \frac{c-d+k-r+1}{2}$.

We claim that $d \geq 0$. For otherwise, $d \leq -1$, and hence, $c \geq k-r+2$. Therefore, $f \leq 4 - \frac{c-d+k-r+1}{2} \leq 2 + r - k$. So $y_3 = r + f \leq 2r + 2 - k < r$ (because $k \geq r+5$). Since $y_2 + y_3 = 2r+2$ and by Lemma 7.2.6, $y_2y_3 \leq (2r + 2 - (2r + 2 - k))(2r + 2 - k)$. By the assumption that Claim 3 fails, $d \geq r + 4 - k$. Therefore,

$$\begin{aligned} y_2y_3 - y_1 &\leq k(2r + 1 - k) - (r^2 + k - 3 + d) \\ &= -k^2 + 2rk - r^2 + 3 + k - d \\ &\leq -(k - r)^2 + 2k - r - 1 \quad (\text{since } d \geq r + 4 - k) \\ &= -(k - r - 1)^2 + r \\ &< 0 \text{ (by (ii) of Lemma 7.2.7), a contradiction.} \end{aligned}$$

Note that $y_3 = r + (2 - e) \leq r + 2 - \lceil \frac{k-r+2}{2} \rceil < \frac{2r+2}{2}$ (because $k \geq r + 5$). So by Lemma 7.2.6, $y_2y_3 \leq (2r + 2 - (r + 2 - \lceil \frac{k-r+2}{2} \rceil))(r + 2 - \lceil \frac{k-r+2}{2} \rceil)$.

If $k - r$ is odd then $e \geq \frac{k-r+3}{2}$. Hence

$$\begin{aligned} y_2y_3 - y_1 &\leq (r + \tfrac{k-r+3}{2})(r + 2 - \tfrac{k-r+3}{2}) - (r^2 + k - 3 + d) \\ &= -(\tfrac{k-r+3}{2})^2 + r + 6 - d \\ &\leq -(\tfrac{k-r+3}{2})^2 + r + 6 \quad (\text{since } d \geq 0) \\ &< 0 \text{ (by (ii) of Lemma 7.2.7), a contradiction.} \end{aligned}$$

So $k-r$ is even. Then

$$\begin{aligned} y_2y_3 - y_1 &\leq (r + \tfrac{k-r+2}{2})(r + 2 - \tfrac{k-r+2}{2}) - (r^2 + k - 3 + d) \\ &= -(\tfrac{k-r+2}{2})^2 + r + 5 - d \\ &\leq -(\tfrac{k-r+2}{2})^2 + r + 5 \quad (\text{since } d \geq o) \\ &< 0 \text{ (by (ii) of Lemma 7.2.7)), a contradiction.} \end{aligned}$$

Subcase 1.3. $b < \frac{k-r}{2}$ and $e < \frac{k-r+2}{2}$.

Since $b + e \geq k - r$. We must have $b = \frac{k-r-1}{2}$ and $e = 1 + \frac{k-r-1}{2}$, and hence $b + e = k - r$ is odd. Then $a = 2 - b = 2 - \frac{k-r-1}{2}$, $f = 2 - e = 1 - \frac{k-r-1}{2}$, and $c + d = b + e + 1 = k - r + 1$.

We claim that $d \geq \frac{k-r-1}{2}$. By (P7), $(r + g)(r + h) \geq r^2 + k + 1 - (c + d) = r^2 + r$, and therefore, because $g+h = 1$, we have $gh \geq 0$. Hence either $g = 1$ or $h = 1$. If $g = 1$, then $d = 3-a-g = \frac{k-r-1}{2}$; otherwise, $h = 1$, then $c = 3 - f - h = 1 + \frac{k-r-1}{2}$, and so, $d = k - r + 1 - c = 1 + \frac{k-r-1}{2}$. Hence, $d \geq \frac{k-r-1}{2}$.

Note that $y_3 = r + f \leq r + 1 - \frac{k-r-1}{2} < \frac{2r+2}{2}$ (because $k \geq r + 5$ by (ii) of Lemma 7.2.7). So by Lemma 7.2.6, $y_2y_3 \leq (2r + 2 - (r + 1 - \frac{k-r-1}{2}))(r + 1 - \frac{k-r-1}{2})$. Hence,

$$\begin{aligned} y_2y_3 - y_1 &\leq (r + 1 + \tfrac{k-r-1}{2})(r + 1 - \tfrac{k-r-1}{2}) - (r^2 + k - 3 + d) \\ &\leq (r + 1)^2 - (\tfrac{k-r-1}{2})^2 - (r^2 + k - 3 + \tfrac{k-r-1}{2}) \quad (\text{because } d \geq \tfrac{k-r-1}{2}) \\ &= -(\tfrac{k-r+2}{2})^2 + r + \tfrac{21}{4} \\ &< 0 \text{ (because } k > r + \sqrt{4r + 21} - 2), \text{ a contradiction.} \end{aligned}$$

Case 2. $g + h = 0$.

Then $z_1 + z_3 = 2r$. Moreover, $c + d \geq k - m + 2\lfloor \frac{m}{2} \rfloor + 1$; for otherwise, by (P7), $r^2 + gh = (r + g)(r + h) \geq r^2 + k + 1 - m + 2\lfloor \frac{m}{2} \rfloor - (c + d) \geq r^2 + 1$, acontradiction.

Since $c \geq d$, we have $c \geq \frac{k-m+2\lfloor \frac{m}{2} \rfloor+1}{2}$. Hence $c \geq \frac{k}{2}$ if $m = 5$ and $c \geq \frac{k+1}{2}$ if $m = 6$. Since $k = r + 3$ when $m = 5$ and $k \geq r + 5$ when $m = 6$, $c \geq \frac{r+3}{2}$, which implies $c \geq 5$ (since $r \geq 6$). By (P9), $f + h \leq \lfloor \frac{m}{2} \rfloor - c$.

Subcase 2.1. $f \leq \frac{\lfloor \frac{m}{2} \rfloor - c - 1}{2}$.

Then $y_3 = r + f \leq r + \frac{\lfloor \frac{m}{2} \rfloor - c - 1}{2} < r$ (because $c \geq 5$). Since $a + b \geq 2$ and $g + h = 0$, it follows from (P8) that $e + f \leq m - 3$, and hence, $y_2 + y_3 \leq 2r + m - 3$. In view of Lemma 7.2.6, $y_2y_3 \leq (2r + m - 3 - (r + \frac{\lfloor \frac{m}{2} \rfloor - c - 1}{2}))(r + \frac{\lfloor \frac{m}{2} \rfloor - c - 1}{2})$.

Suppose $m = 5$. Then $c \geq \frac{k}{2}$, $k = r + 3$, and $d \geq r + 3$ (by the assumption that Claim 3 fails). Hence,

$$\begin{aligned} y_2y_3 - y_1 &\leq (r + 2 - \tfrac{1-c}{2})(r + \tfrac{1-c}{2}) - (r^2 + k - 2 + d) \\ &= -(\tfrac{c+1}{2})^2 + 2r + 3 - k - d \\ &\leq -(\tfrac{c+1}{2})^2 + r \quad (\text{since } d \geq r + 3 - k) \\ &\leq -(\tfrac{k+2}{4})^2) - r \quad (\text{since } c \geq \tfrac{k}{2}) \\ &= -(\tfrac{r+5}{4})^2) - r \quad (\text{since } k = r + 3) \\ &< 0 \text{ (because } r \geq 6), \text{ a contradiction.} \end{aligned}$$

Therefore, $m = 6$. Then $c \geq \frac{k+1}{2}$ and $k \geq r + 5$ (by (ii) of Lemma 7.2.7). If $d \geq 1$, then

$$\begin{aligned} y_2y_3 - y_1 &\leq (r + 3 - \tfrac{2-c}{2})(r + \tfrac{2-c}{2}) - (r^2 + k - 3 + d) \\ &= -(\tfrac{c+1}{2})^2 + 3r - k + \tfrac{21}{4} - d \\ &\leq -(\tfrac{c+1}{2})^2 + 2r - \tfrac{3}{4} \quad (\text{since } d \geq 1 \text{ and } k \geq r + 5) \\ &\leq -(\tfrac{k+3}{4})^2 + 2r - \tfrac{3}{4} \quad (\text{since } c \geq \tfrac{k+1}{2}) \\ &\leq -(\tfrac{r+8}{4})^2 + 2r - \tfrac{3}{4} \quad (\text{since } k \geq r + 5) \\ &< 0 \text{ (because } r \geq 6), \text{ a contradiction.} \end{aligned}$$

So $d \leq 0$. Then $c \geq k + 1$, because $c + d \geq k + 1$. By the assumption that Claim 3 fails, $d \geq r + 4 - k$. Hence

$$\begin{aligned} y_2y_3 - y_1 &\leq (r + 3 - \tfrac{2-c}{2})(r + \tfrac{2-c}{2}) - (r^2 + k - 3 + d) \\ &= -(\tfrac{c+1}{2})^2 + 3r - k + \tfrac{21}{4} - d \\ &\leq -(\tfrac{c+1}{2})^2 + 2r + \tfrac{5}{4} \quad (\text{since } d \geq r + 4 - k) \\ &\leq -(\tfrac{k+2}{2})^2 + 2r + \tfrac{5}{4} \quad (\text{since } c \geq k + 1) \\ &< -(\tfrac{r+7}{2})^2 + 2r + \tfrac{5}{4} \quad (\text{since } k \geq r + 5) \\ &< 0 \text{ (because } r \geq 6), \text{ a contradiction.} \end{aligned}$$

Subcase 2.2. $f > \frac{\lfloor \frac{m}{2} \rfloor - c - 1}{2}$.

Therefore, since $f + h \leq \lfloor \frac{m}{2} \rfloor - c$, we have $h < \frac{\lfloor \frac{m}{2} \rfloor - c + 1}{2}$, and so, $h \leq \frac{\lfloor \frac{m}{2} \rfloor - c}{2}$ (because h is an integer). Then $z_3 = r + h \leq r + \frac{\lfloor \frac{m}{2} \rfloor - c}{2} < r$ (because $c \geq 5$). Recall that $z_1 + z_3 = 2r$. So by Lemma 7.2.6, $z_1z_3 \leq (2r - (r + \frac{\lfloor \frac{m}{2} \rfloor - c}{2}))(r + \frac{\lfloor \frac{m}{2} \rfloor - c}{2})$.

If $m = 5$ then by (P1),

$$\begin{aligned} z_1z_3 - z_2 &\leq (r - \tfrac{2-c}{2})(r + \tfrac{2-c}{2}) - (r^2 + k - (c + d)) \\ &\leq -(\tfrac{c-2}{2})^2 - k + 2c \quad (\text{since } d \leq c) \\ &= -(\tfrac{c-6}{2})^2 + 8 - k \\ &\leq 0 \text{ (because } k = r + 3 \geq 9), \text{ a contradiction.} \end{aligned}$$

So $m = 6$. Then $c + d \geq k + 1$. Again by (P1),

$$\begin{aligned} z_1z_3 - z_2 &\leq (r - \tfrac{3-c}{2})(r + \tfrac{3-c}{2}) - (r^2 + k + 1 - (c + d)) \\ &\leq -(\tfrac{c-3}{2})^2 - k + 2c - 1 \quad (\text{since } d \leq c) \\ &= -(\tfrac{c-7}{2})^2 - k + 9 \\ &< 0 \text{ (since } k \geq r + 5 \geq 11 \text{ by (ii) of Lemma 7.2.7), a contradiction.} \quad \square \end{aligned}$$

Claim 4. $c \leq r + \lfloor \frac{m}{2} \rfloor - k$.

Suppose $c \geq r + \lfloor \frac{m}{2} \rfloor - k + 1$. Then $a + b \geq 2$ (by (P10)) and $d \leq r + \lfloor \frac{m}{2} \rfloor - k$ (by Claim 3). In particular, $d < c$. We consider two cases.

Case 1. $d \leq \lfloor \frac{m}{2} \rfloor - k$.

Then by (P2), $\lfloor \frac{m}{2} \rfloor - k \geq \frac{3\lfloor \frac{m}{2} \rfloor - m + 1 - c}{2}$. Thus, $c \geq \lfloor \frac{m}{2} \rfloor - m + 1 + 2k$. Since $c \leq 2r + 1 + \lfloor \frac{m}{2} \rfloor - k$ (by Claim 2), we have $2r + m \geq 3k$, which implies $m \in \{2, 3\}$.

Suppose $m = 2$. Then $k = 1$, $d \leq 0$, and $c \geq r + 1$. So by (P4), $z_3 \leq 2r - 1 - c \leq r - 2 < \frac{2r-1}{2}$. By (P3), $c \leq 2r - 3$. Then by (P2), $d \geq \frac{2-c}{2} > 2 - r$, and so, $e + f \geq 0$ by (P10). Therefore, since $a + b \geq 2$ and by (P8), we have $g + h \leq -1$. Hence, $z_1 + z_3 = r + g + r + h \leq 2r - 1$. By Lemma 7.2.6, $z_1z_3 \leq (2r - 1 - (2r - 1 - c))(2r - 1 - c)$. Then by (P1), $z_1z_3 - z_2 \leq c(2r - 1 - c) - (r^2 + 2 - (c + d)) = -(c - r)^2 - 2 + d < 0$ (because $d \leq 0$), a contradiction.

Thus, $m = 3$. Then $d \leq 1 - k$ and $c \geq r + 2 - k$. In particular, $c \geq 3$ because $k < r$ (by (i) of Lemma 7.2.7). By (P2) and since $c \leq 2r + 2 - k$ (by Claim 2), $d \geq \frac{1-c}{2} \geq \frac{k-1}{2} - r > 2 - r - k$ (because $k \geq 4$ by (i) of Lemma 7.2.7). Hence $e + f \geq 0$ (by (P10)). Since $a + b \geq 2$ and by (P8), we have $g + h \leq 0$. Hence, $z_1 + z_3 = r + g + r + h \leq 2r$. By (P9), $f + h \leq 1 - c$.

Suppose $h \leq \frac{1-c}{2}$. Then, $z_3 = r + h \leq r + \frac{1-c}{2} < r$ (because $c \geq 3$). Therefore, by Lemma 7.2.6,

we have $z_1z_3 \leq (2r-(r+\frac{1-c}{2}))(r+\frac{1-c}{2})$. So by (P1),

$$\begin{aligned} z_1z_3 - z_2 &\leq (r-\tfrac{1-c}{2})(r+\tfrac{1-c}{2}) - (r^2+k-(c+d)) \\ &= -(\tfrac{1-c}{2})^2 - k + c + d \\ &\leq -\tfrac{(c-3)^2}{4} - 2k + 3 \quad \text{(because } d \leq 1-k\text{)} \\ &< 0 \text{ (because } k \geq 4 \text{ by (i) of Lemma 7.2.7), a contradiction.} \end{aligned}$$

So $h > \frac{1-c}{2}$. Then $f \leq 1-c-h < \frac{1-c}{2}$. Since f is an integer, $f \leq -\frac{c}{2}$. Note that $c+d \leq (2r+2-k)+(1-k) = 2r+3-2k$. By (P7), $(r+g)(r+h) \geq r^2+k-(c+d) \geq r^2+3k-2r-3 \geq r^2-2r+9$ (because $k \geq 4$ by (i) of Lemma 7.2.7), we see that $g+h \geq -1$; otherwise, $(r+g)(r+h) \leq (\frac{2r+g+h}{2})^2 \leq r^2-2r+1$, a contradiction. Since $a+b \geq 2$ and by (P8), $e+f \leq 1$. Hence, $y_2+y_3 = r+e+r+f \leq 2r+1$. Since $y_3 = r+f \leq r-\frac{c}{2} < \frac{2r+1}{2}$, we have from Lemma 7.2.6 that $y_2y_3 \leq (2r+1-(r-\frac{c}{2}))(r-\frac{c}{2})$. Hence,

$$\begin{aligned} y_2y_3 - y_1 &\leq (r+1+\tfrac{c}{2})(r-\tfrac{c}{2}) - (r^2+k-1+d) \\ &= -(\tfrac{c}{2})^2 - \tfrac{c}{2} + r + 1 - k - d \\ &\leq -(\tfrac{c}{2})^2 + r - k + \tfrac{1}{2} \quad \text{(because } d \geq \tfrac{1-c}{2} \text{ by (P2))} \\ &\leq -(\tfrac{c-2}{2})^2 - \tfrac{1}{2} \quad \text{(because } c \geq r+2-k\text{)} \\ &< 0, \text{ a contradiction.} \end{aligned}$$

Case 2. $d \geq \lfloor \frac{m}{2} \rfloor - k + 1$.

Then by (P10), $e+f \geq 1$. Since $a+b \geq 2$ and by (P8), we have $g+h \leq m-4$. Hence $z_1+z_3 = r+g+r+h \leq 2r+m-4$.

Suppose $m = 2$. Then $k = 1$, $c \geq r+1$, $d \leq r$ (by Claim 3), and $z_1+z_3 \leq 2r-2$. By (P4), $z_3 \leq 2r-1-c \leq r-2 < \frac{2r-2}{2}$. Hence, by Lemma 7.2.6, we have $z_1z_3 \leq (2r-2-(2r-1-c))(2r-1-c)$. Therefore, by (P1), $z_1z_3 - z_2 \leq (c-1)(2r-1-c) - (r^2+2-(c+d)) < -(c-r-1)^2 \leq 0$ (because $d < c$), a contradiction.

Therefore, $m \in \{3,5,6\}$.

Subcase 2.1. $m = 3$.

Then $z_1+z_3 \leq 2r-1$, $c \geq r+2-k$ (by the assumption that Claim 4 fails), $d \geq 2-k$ (by assumption of Case 2), and $d \leq r+1-k$. By (P9), $f+h \leq 1-c$.

Suppose $h \leq \frac{2-c}{2}$. Since $c \geq r+2-k \geq 3$ (because $k < r$ by (i) of Lemma 7.2.7), $z_3 = r+h \leq$

$r + \frac{2-c}{2} \leq \frac{2r-1}{2}$. By Lemma 7.2.6, $z_1 z_3 \leq (2r - 1 - (r + \frac{2-c}{2}))(r + \frac{2-c}{2})$. By (P1),

$$\begin{aligned} z_1 z_3 - z_2 &\leq (r - 1 - \tfrac{2-c}{2})(r + \tfrac{2-c}{2}) - (r^2 + k - (c + d)) \\ &= -(\tfrac{c-5}{2})^2 - r - k + d + \tfrac{17}{4} \\ &\leq -(\tfrac{c-5}{2})^2 - 2k + \tfrac{21}{4} \quad \text{(because } d \leq r + 1 - k\text{)} \\ &< 0 \text{ (because } k \geq 4 \text{ by (i) of Lemma 7.2.7), a contradiction.} \end{aligned}$$

So $h > \frac{2-c}{2}$. Then $f \leq 1 - c - h < -\frac{c}{2}$. Since f is an integer, $f \leq -\frac{c+1}{2}$. Since $c + d \leq (2r + 2 - k) + (r + 1 - k) = 3r + 3 - 2k$ and by (P7), $(\frac{2r+g+h}{2})^2 \geq (r + g)(r + h) \geq r^2 + k - (c + d) \geq r^2 + 3k - 3r - 3 \geq r^2 - 3r + 9$ (because $k \geq 4$ by (i) of Lemma 7.2.7), we see that $g + h \geq -2$. By the same argument, if $c + d \leq 2r + k - 2$ then we must have $g + h \geq -1$. Because $a + b \geq 2$ and by (P8), we have $e + f \leq 2$, and $e + f \leq 1$ if $c + d \leq 2r + k - 2$. Note that $y_3 = r + f \leq r - \frac{c+1}{2} < \frac{2r+1}{2}$ (because $c > 0$ by (P3)).

Suppose $c + d \geq 2r + k - 1$. Since $y_2 + y_3 = r + e + r + f \leq 2r + 2$ and by Lemma 7.2.6, $y_2 y_3 \leq (2r + 2 - (r - \frac{c+1}{2}))(r - \frac{c+1}{2})$. Hence,

$$\begin{aligned} y_2 y_3 - y_1 &\leq (r + 2 + \tfrac{c+1}{2})(r - \tfrac{c+1}{2}) - (r^2 + k - 1 + d) \\ &= -(\tfrac{c+1}{2})^2 + 2r - k - (c + d) \\ &\leq -(\tfrac{c+1}{2})^2 - 2k + 1 \quad \text{(because } c + d \geq 2r + k - 1\text{)} \\ &< 0 \text{ (because } k \geq 4 \text{ by (i) of Lemma 7.2.7), a contradiction.} \end{aligned}$$

Thus, $c + d \leq 2r + k - 2$. Then $y_2 + y_3 = r + e + r + f \leq 2r + 1$. By Lemma 7.2.6, $y_2 y_3 \leq (2r + 1 - (r - \frac{c+1}{2}))(r - \frac{c+1}{2})$. Hence,

$$\begin{aligned} y_2 y_3 - y_1 &\leq (r + 1 + \tfrac{c+1}{2})(r - \tfrac{c+1}{2}) - (r^2 + k - 1 + d) \\ &= -(\tfrac{c+2}{2})^2 + r - k - d + \tfrac{5}{4} \\ &\leq -(\tfrac{c+2}{2})^2 + r - \tfrac{3}{4} \quad \text{(because } d \geq 2 - k\text{)} \\ &\leq -(\tfrac{r+4-k}{2})^2 + r - \tfrac{3}{4} \quad \text{(because } c \geq r + 2 - k\text{)} \\ &< 0 \text{ (by (i) of Lemma 7.2.7), a contradiction.} \end{aligned}$$

Subcase 2.2. $m \in \{5, 6\}$.

First, we show that if $m = 6$ then $c \geq 2k - 2r - 2 > 0$. Suppose $m = 6$. Then $d \leq r + 3 - k$, $d \geq \frac{4-c}{2}$ (by (P2)), and $k \geq r + 5$ (by (iii) of Lemma 7.2.7). Thus $c \geq 4 - 2d \geq 2k - 2r - 2 > 0$.

By (P9), $f + h \leq \lfloor \frac{m}{2} \rfloor - c$.

Assume $h \leq \frac{\lfloor \frac{m}{2} \rfloor - c}{2}$. Since $c \geq 1$ (by (P3)), $z_3 = r + h \leq r + \frac{\lfloor \frac{m}{2} \rfloor - c}{2} \leq \frac{2r+m-4}{2}$. By Lemma 7.2.6, $z_1 z_3 \leq (2r + m - 4 - (r + \frac{\lfloor \frac{m}{2} \rfloor - c}{2}))(r + \frac{\lfloor \frac{m}{2} \rfloor - c}{2})$. If $m = 5$ then $d \leq r + 2 - k$, and by (P1),

$$\begin{aligned} z_1 z_3 - z_2 &\leq (r + 1 - \tfrac{2-c}{2})(r + \tfrac{2-c}{2}) - (r^2 + k - (c + d)) \\ &= -(\tfrac{c-3}{2})^2 - k + d + r + \tfrac{9}{4} \\ &\leq -(\tfrac{c-3}{2})^2 - 2k + 2r + \tfrac{17}{4} \quad \text{(because } d \leq r + 2 - k\text{)} \\ &< 0 \text{ (because } k = r + 3\text{), a contradiction.} \end{aligned}$$

So $m = 6$. Then $d \leq r + 3 - k$ and $c \geq 2k - 2r - 2$. By (P1),

$$\begin{aligned} z_1 z_3 - z_2 &\leq (r + 2 - \tfrac{3-c}{2})(r + \tfrac{3-c}{2}) - (r^2 + k + 1 - (c + d)) \\ &= -(\tfrac{c-3}{2})^2 - k + 2r + d + 2 \\ &\leq -(\tfrac{c-3}{2})^2 - 2k + 3r + 5 \quad \text{(because } d \leq r + 3 - k\text{)} \\ &\leq -(\tfrac{2k-2r-5}{2})^2 - 2k + 3r + 5 \quad \text{(because } c \geq 2k - 2r - 2\text{)} \\ &= -(k - r - \tfrac{3}{2})^2 + r + 1 \\ &< 0 \text{ (by (ii) of Lemma 7.2.7), a contradiction.} \end{aligned}$$

So $h > \frac{\lfloor \frac{m}{2} \rfloor - c}{2}$. Then $f < \frac{\lfloor \frac{m}{2} \rfloor - c}{2}$. Since f is an integer, $f \leq \frac{\lfloor \frac{m}{2} \rfloor - c - 1}{2}$. By Claim 2 and since $d \leq r + \lfloor \frac{m}{2} \rfloor - k$, $c + d \leq 3r + 2\lfloor \frac{m}{2} \rfloor + 1 - 2k$. By (P7), $(r + g)(r + h) \geq r^2 + k + 1 - m + 2\lfloor \frac{m}{2} \rfloor - (c + d) \geq r^2 + 3k - 3r - m \geq r^2 + 3$ (because $k \geq r + 3$). So we must have $g + h \geq 1$; for otherwise, $(r + g)(r + h) \leq (\frac{2r+g+h}{2})^2 \leq r^2$, a contradiction. Since $a + b \geq 2$ and by (P8), $e + f \leq m - 4$. So $y_2 + y_3 = r + e + r + f \leq 2r + m - 4$. Since $f \leq \frac{\lfloor \frac{m}{2} \rfloor - c - 1}{2}$ and $c \geq 1$, $y_3 = r + f \leq r + \frac{\lfloor \frac{m}{2} \rfloor - c - 1}{2} < \frac{2r+m-4}{2}$. By Lemma 7.2.6, $y_2 y_3 \leq (2r + m - 4 - (r + \frac{\lfloor \frac{m}{2} \rfloor - c - 1}{2}))(r + \frac{\lfloor \frac{m}{2} \rfloor - c - 1}{2})$. If $m = 5$, then

$$\begin{aligned} y_2 y_3 - y_1 &\leq (r + 1 - \tfrac{1-c}{2})(r + \tfrac{1-c}{2}) - (r^2 + k - 2 + d) \\ &= -(\tfrac{c-1}{2})^2 - \tfrac{c}{2} - d - k + r + \tfrac{5}{2} \\ &\leq -(\tfrac{c-1}{2})^2 - k + r + \tfrac{3}{2} \quad \text{(because } d \geq \tfrac{2-c}{2} \text{ by (P2))} \\ &< 0 \text{ (because } k = r + 3\text{), a contrdiction.} \end{aligned}$$

So $m = 6$. Then

$$\begin{aligned} y_2y_3 - y_1 &\leq (r + 2 - \tfrac{2-c}{2})(r + \tfrac{2-c}{2}) - (r^2 + k - 3 + d) \\ &= -(\tfrac{c-2}{2})^2 - c - d - k + 2r + 5 \\ &\leq -(\tfrac{c-1}{2})^2 - k + 2r + \tfrac{9}{4} \quad \text{(because } d \geq \tfrac{4-c}{2} \text{ by (P2))} \\ &\leq -(\tfrac{c-1}{2})^2 + r - \tfrac{11}{4} \quad \text{(because } k \geq r + 5) \\ &\leq -(k - r - \tfrac{3}{2})^2 + r - \tfrac{9}{11}4 \quad \text{(because } c \geq 2k - 2r - 2) \\ &< 0 \text{ (by (ii) of Lemma 7.2.7), a contradiction.} \quad \square \end{aligned}$$

Claim 5. $d \leq \lfloor \frac{m}{2} \rfloor - k$.

Otherwise, by Claim 3 and Claim 4, we have $\lfloor \frac{m}{2} \rfloor - k + 1 \leq d \leq c \leq r + \lfloor \frac{m}{2} \rfloor - k$. By (P10), $a + b \geq 1$ and $e + f \geq 1$. Therefore, it follows from (P8) that $g + h \leq m - 3$, and so, $z_1 + z_3 = r + g + r + h \leq 2r + m - 3$.

We claim $g + h \geq -1$. For otherwise, $(r + g)(r + h) \leq (\frac{2r+g+h}{2})^2 \leq r^2 - 2r + 1$. However, since $c+d \leq 2r+2\lfloor \frac{m}{2} \rfloor - 2k$ and by (P7), $(r+g)(r+h) \geq r^2+k+1-m+2\lfloor \frac{m}{2} \rfloor - (c+d) = r^2-2r+3k+1-m \geq r^2 - 2r + 2$, a contradiction. The final inequality holds because $k = 1$ when $m = 1$, $k \geq 4$ when $m \in \{3, 5, 6\}$ (see Lemma 7.2.7).

By (P3), we have $c \geq 1$. Hence, $1 \leq c \leq r + \lfloor \frac{m}{2} \rfloor - k$, which implies $k \leq r + \lfloor \frac{m}{2} \rfloor - 1$. So by (ii) of Lemma 7.2.7, we have $m \in \{2, 3\}$.

Case 1. $m = 2$.

Then $k = 1$ and $d \geq 2 - k = 1$. We claim that $c + d \geq r + 2$. For otherwise, it follows from (P7) that $(r + g)(r + h) \geq r^2 + 2 - (c + d) \geq r^2 - r + 1$. However, since $g + h \leq m - 3 = -1$, we have $(r + g)(r + h) \leq (\frac{2r+g+h}{2})^2 \leq r^2 - r + \frac{1}{4}$, a contradiction. In particular, $c \geq \frac{r+2}{2} \geq 4$ (because $r \geq 6$).

Since $-1 \leq g + h \leq m - 3 = -1$, we have $g + h = -1$. Because $a + b \geq 1$ and $c + d \geq 1$, we have $a + b = 1$ and $e + f = 1$. By (P9), $f + h \leq 1 - c$.

Suppose $f \leq \frac{1-c}{2}$. Then $y_3 = r + f \leq r + \frac{1-c}{2} < \frac{2r-1}{2}$ (because $c \geq 4$). Hence, since $y_2 + y_3 =$

$r+e+r+f = 2r+1$, it follows from Lemma 7.2.6 that $y_2y_3 \le (2r+1-(r+\frac{1-c}{2}))(r+\frac{1-c}{2})$. Therefore,

$$\begin{aligned} y_2y_3 - y_1 &\le (r-1-\tfrac{1-c}{2})(r+\tfrac{1-c}{2}) - (r^2+d) \\ &= -(\tfrac{1-c}{2})^2 - \tfrac{1-c}{2} - d - r \\ &\le -(\tfrac{1-c}{2})^2 - 3\tfrac{1-c}{2} - 1 - 2r \quad \text{(because } d \ge r+2-c\text{)} \\ &= -(\tfrac{4-c}{2})^2 - 2r + \tfrac{5}{4} \\ &< 0 \text{ (because } r \ge 6\text{), a contradiction.} \end{aligned}$$

So $f > \frac{1-c}{2}$. Then $h \le 1-c-f < \frac{1-c}{2}$. Since h is an integer, we have $h \le -\frac{c}{2}$. Hence, $z_3 = r+h \le r-\frac{c}{2} < \frac{2r-1}{2}$ (because $c \ge 4$). Because $z_1+z_3 = r+g+r+h = 2r-1$, it follows from Lemma 7.2.6 that $z_1z_3 \le (2r-1-(r-\frac{c}{2}))(r-\frac{c}{2})$. Hence by (P1), we have

$$\begin{aligned} z_1z_3 - z_2 &\le (r-1+\tfrac{c}{2})(r-\tfrac{c}{2}) - (r^2+2-(c+d)) \\ &= -(\tfrac{c}{2})^2 + \tfrac{c}{2} - r - 2 + (c+d) \\ &\le -(\tfrac{c}{2})^2 + 5\tfrac{c}{2} - r - 2 \quad \text{(because } d \le c\text{)} \\ &= -(\tfrac{c-5}{2})^2 - r + \tfrac{17}{4} \\ &< 0 \text{ (because } r \ge 6\text{), a contradiction.} \end{aligned}$$

Case 2. $m = 3$.

Then $c+d \ge k$. For otherwise, we have $r^2+1 \le r^2+k-(c+d) \le (r+g)(r+h)$ (by (P7)). However, since $g+h \le m-3 = 0$, we have $(r+g)(r+h) \le (\frac{2r+g+h}{2}) \le r^2$, a contradiction.

Subcase 2.1. $c+d \ge r+k$.

Then $c \ge \frac{r+k}{2}$. By (i) of Lemma 7.2.7, $r \ge k+1$. Hence $c \ge k+\frac{1}{2}$, and so, $c \ge k+1 \ge 5$ (because c is an integer and $k \ge 4$). Because $g+h \ge -1$ and $a+b \ge 1$, it follows from (P8) that $e+f \le 2$. So $y_2+y_3 = r+e+r+f \le 2r+2$. By (P9), $f+h \le 1-c$.

Suppose $f \le \frac{1-c}{2}$. Then $y_3 = r+f \le r+\frac{1-c}{2} < \frac{2r+2}{2}$. By Lemma 7.2.6, $y_2y_3 \le (2r+2-(r+$

$\frac{1-c}{2}))(r+\frac{1-c}{2})$. Hence,

$$\begin{aligned} y_2y_3 - y_1 &\leq (r+2-\tfrac{1-c}{2})(r+\tfrac{1-c}{2}) - (r^2+k-1+d) \\ &= -(\tfrac{c-1}{2})^2 - c - d - k + 2r + 2 \\ &\leq -(\tfrac{c-1}{2})^2 - 2k + r + 2 \quad \text{(because } c+d \geq r+k\text{)} \\ &< -(\tfrac{k}{2})^2 - 2k + r + 2 \quad \text{(because } c \geq k+1\text{)} \\ &= -(\tfrac{k+4}{2})^2 + r + 6 \\ &< 0 \text{ (by (i) of Lemma 7.2.7), a contradiction.} \end{aligned}$$

So $f > \frac{1-c}{2}$. Then $h \leq 1-c-f < \frac{1-c}{2}$. Since h is an integer, $h \leq -\frac{c}{2}$. Then $z_3 = r+h \leq r-\frac{c}{2} < \frac{2r}{2}$. Since $z_1 + z_3 \leq 2r$, it follows from Lemma 7.2.6 that $z_1z_3 \leq (2r-(r-\frac{c}{2}))(r-\frac{c}{2})$. Then by (P1),

$$\begin{aligned} z_1z_3 - z_2 &\leq (r+\tfrac{c}{2})(r-\tfrac{c}{2}) - (r^2+k-(c+d)) \\ &= -(\tfrac{c}{2})^2 - k + c + d \\ &\leq -(\tfrac{c-4}{2})^2 - k + 4 \quad \text{(because } d \leq c\text{)} \\ &< 0 \text{ (because } k \geq 4 \text{ and } c \geq k+1 \geq 5\text{), a contradiction.} \end{aligned}$$

Subcase 2.2. $k \leq c+d \leq r+k-1$.

Then by (P7), $(r+g)(r+h) \geq r^2+k-(c+d) \geq r^2-r+1$. This implies that $g+h \geq 0$. Recall that $g+h \leq m-3 = 0$. So $g+h = 0$. Hence $(r-h)(r+h) \geq r^2+k-(c+d)$, which implies $|h| \leq \lfloor \sqrt{c+d-k} \rfloor$.

Because $g+h = 0$, $a+b \geq 1$, and $e+f \geq 1$, it follows from (P8) that $a+b = 1$ and $e+f = 1$. Thus from our matrix representation of $\mathbf{x}$ and by (P1), we have $\sum_{i=1}^{3}(x_i+y_i+z_i) \geq 3r^2+6r+3k$. By (iv), (v) and (vi) of (14), $x_i+y_i+z_i \leq r^2+2r+k$ for $1 \leq i \leq 3$. Hence, $x_i+y_i+z_i = r^2+2r+k$ for $(1 \leq i \leq 3)$ and $z_2 = r^2+k-(c+d)$. Therefore, $a+d+g = 1$, $c+f+h = 1$, and $c+d = b+e$.

Since $m = 3$, we have $k > 2\sqrt{r+2}-2$ when k is even, and $k > 2\sqrt{r+4}-3$ when k is odd. Hence, $r < \frac{k^2}{4}+k-1$ when k is even, and $r < \frac{k^2}{4}+\frac{3k}{2}-\frac{7}{4}$ when k is odd. We consider three cases.

First, suppose $h \geq 0$. Then by (P9), $f \leq 1-c$, and hence, $y_3 = r+f \leq r+1-c < \frac{2r+1}{2}$ (because $c \geq 1$ by (P2)). Since $y_2+y_3 = r+e+r+f = 2r+1$, it follows from Lemma 7.2.6 that

$y_2y_3 \le (2r+1-(r+1-c)))(r+1-c)$. Hence,

$$\begin{aligned} y_2y_3 - y_1 &\le (r+c)(r+1-c) - (r^2+k-1+d) \\ &= -c^2+c+r-k+1-d \\ &\le -c^2+2c+r-2k+1 \quad (\text{because } d \ge k-c) \\ &= -(c-1)^2+r+2-2k. \end{aligned}$$

If k is even, then $c \ge \frac{k}{2} \ge 2$ (because $c+d \ge k \ge 4$ and $c \ge d$) and $r < \frac{k^2}{4}+k-1$, and so, $y_2y_3 - y_1 < -(\frac{k}{2}-1)^2 + \frac{k^2}{4} - k + 1 = 0$, a contradiction. So k is odd. Then $c \ge \frac{k+1}{2}$ and $r < \frac{k^2}{4} + \frac{3k}{2} - \frac{7}{4}$, and hence, $y_2y_3 - y_1 < -(\frac{k+1}{2}-1)^2 + \frac{k^2}{4} - \frac{k}{2} + \frac{1}{4} = 0$, a contradiction.

Now suppose $h = -1$. Then $g = 1$, $a = -d, b = 1+d, e = c-1$, and $f = 2-c$. Also, $\sqrt{c+d-k} \ge |h| = 1$ implies $c+d \ge k+1$. If $d \ge \frac{k-1}{2}$, then

$$\begin{aligned} x_1x_2 - x_3 &= (r-d)(r+1+d) - (r^2+k-1+c) \\ &= -d^2-k+r+1-(c+d) \\ &\le -d^2-2k+r \quad (\text{because } c+d \ge k+1) \\ &< -d^2+\frac{k^2}{4}-\frac{k}{2}-\frac{7}{4} \quad (\text{since } r < \frac{k^2}{4}+\frac{3}{2}k-\frac{7}{4}) \\ &< 0 \text{ (bceause } d \ge \tfrac{k-1}{2}\text{), a contradiction.} \end{aligned}$$

So $d \le \frac{k-2}{2}$. Then $c \ge k+1-d \ge \frac{k+4}{2}$. Hence,

$$\begin{aligned} y_2y_3 - y_1 &= (r+c-1)(r+2-c) - (r^2+k-1+d) \\ &= -(c-2)^2+r-k+3-(c+d) \\ &\le -(c-2)^2+r-2k+2 \quad (\text{because } c+d \ge k+1) \\ &< -(c-2)^2+\frac{k^2}{4}-\frac{k}{2}+\frac{1}{4} \quad (\text{since } r < \frac{k^2}{4}+\frac{3}{2}k-\frac{7}{4}) \\ &< 0 \text{ (bceause } c \ge \tfrac{k+4}{2} \text{ and } k \ge 4\text{), a contradiction.} \end{aligned}$$

Therefore, we have $h \le -2$. This implise that $c+d-k \ge h^2 \ge 4$. Thus $c+d \ge k+4$ and $|h| \le \sqrt{c+d-k} < \frac{c+d-k}{2}$. Hence, $f = 1-h-c \le 1-c+\frac{c+d-k}{2} = 1-\frac{k+c-d}{2}$. Since f is an integer, $f \le 1-\lceil\frac{k+c-d}{2}\rceil$. Hence $y_3 = r+f \le r+1-\lceil\frac{k+c-d}{2}\rceil < r$ (because $c \ge d$ and $k \ge 4$). Since $y_2+y_3 = r+e+r+f = 2r+1$, it follows from Lemma 7.2.6 that $y_2y_3 \le (2r+1-(r+1-\lceil\frac{k+c-d}{2}\rceil))(r+1-\lceil\frac{k+c-d}{2}\rceil)$. Hence,

$$\begin{aligned} y_2y_3 - y_1 &\le (r+\lceil\tfrac{k+c-d}{2}\rceil)(r+1-\lceil\tfrac{k+c-d}{2}\rceil) - (r^2+k-1+d) \\ &= -\lceil\tfrac{k+c-d}{2}\rceil^2 + \lceil\tfrac{k+c-d}{2}\rceil + r - k - d + 1 \\ &= -(\lceil\tfrac{k+c-d}{2}\rceil - \tfrac{1}{2})^2 + r - k - d + \tfrac{5}{4}. \end{aligned}$$

If $c - d \geq 5$, then because $d \geq 2 - k$ and $k \geq 4$, we have $y_2y_3 - y_1 < -(\frac{k+5}{2} - \frac{1}{2})^2 + (\frac{k^2}{4} + \frac{3k}{2} - \frac{7}{4}) - k - (2 - k) + \frac{5}{4} \leq 0$, a contradiction. So $c - d \leq 4$. Since $c + d \geq k + 4$, we have $d \geq \frac{k}{2}$. If k is even then $y_2y_3 - y_1 < -(\frac{k}{2} - \frac{1}{2})^2 + (\frac{k^2}{4} + k - 1) - k - \frac{k}{2} + \frac{5}{4} = 0$, a contradiction. So k is odd. Then $\lceil \frac{k+c-d}{2} \rceil \geq \frac{k+1}{2}$. Hence $y_2y_3 - y_1 < -(\frac{k+1}{2} - \frac{1}{2})^2 + (\frac{k^2}{4} + \frac{3k}{2} - \frac{7}{4}) - k - \frac{k}{2} + \frac{5}{4} < 0$, a contradiction. □

By Claim 4 and Claim 5, $c \leq r + \lfloor \frac{m}{2} \rfloor - k$ and $d \leq \lfloor \frac{m}{2} \rfloor - k$. By (P3), $c \geq \lfloor \frac{m}{2} \rfloor - \frac{m-1}{3} > 0$. So $r + \lfloor \frac{m}{2} \rfloor - k \geq c \geq 1$, which implies $m \in \{2, 3\}$ (by definition of m). Since $c \geq 1$, we have $c \geq \lfloor \frac{m}{2} \rfloor - k + 1$, and hence, $a + b \geq 1$ (by (P10)). Since $c \leq r + \lfloor \frac{m}{2} \rfloor - k$ and $d \geq \frac{3\lfloor \frac{m}{2} \rfloor - m + 1 - c}{2}$ (by (P2)), we have $d > \lfloor \frac{m}{2} \rfloor - k - r + 1$, and hence, $e + f \geq 0$ (by (P10)). Thus, $g + h \leq m - 2$ (by (P8)), and so, $z_1 + z_3 = r + g + r + h \leq 2r + m - 2$.

Note that, when $m = 2$ we have $\frac{2-c}{2} \leq d$ (by (P2)) and $d \leq 1 - k = 0$, and when $m = 3$ we have $\frac{1-c}{2} \leq d$ (by (P2)) and $d \leq 1 - k$ (which implies $c \geq 2k - 1$). By (P9), $f + h \leq 1 - c$.

Assume $h \leq -\frac{c}{2}$. Then $z_3 = r + h \leq r - \frac{c}{2} < \frac{2r+m-2}{2}$ (because $c \geq 1$). By Lemma 7.2.6, $z_1z_3 \leq (2r + m - 2 - (r - \frac{c}{2}))(r - \frac{c}{2})$. If $m = 2$, then $d \leq 0$ and, by (P1),

$$\begin{aligned} z_1z_3 - z_2 &\leq (r + \tfrac{c}{2})(r - \tfrac{c}{2}) - (r^2 + 2 - (c + d)) \\ &= -(\tfrac{c}{2})^2 + c + d - 2 \\ &\leq -(\tfrac{c-2}{2})^2 - 1 \quad \text{(because } d \leq 0\text{)} \\ &< 0, \text{ a contradiction.} \end{aligned}$$

So $m = 3$. Then by (P1),

$$\begin{aligned} z_1z_3 - z_2 &\leq (r + 1 + \tfrac{c}{2})(r - \tfrac{c}{2}) - (r^2 + k - (c + d)) \\ &= -(\tfrac{c-1}{2})^2 + \tfrac{1}{4} + r - k + d \\ &\leq -(\tfrac{c-1}{2})^2 + r + \tfrac{5}{4} - 2k \quad \text{(because } d \leq 1 - k\text{)} \\ &\leq -(k - 1)^2 + r + \tfrac{5}{4} - 2k \quad \text{(because } c \geq 2k - 1\text{)} \\ &= -k^2 + r + \tfrac{1}{4} \\ &< 0 \text{ (by (i) of Lemma 7.2.7), a contradiction.} \end{aligned}$$

Therefore, $h > -\frac{c}{2}$. Then $f \leq 1 - c - h < 1 - \frac{c}{2}$. Since f is an integer, $f \leq \frac{1-c}{2}$. Note that $c + d \leq r + 2\lfloor \frac{m}{2} \rfloor - 2k$. Hence by (P7), $(r + g)(r + h) \geq r^2 + k + 1 - m + 2\lfloor \frac{m}{2} \rfloor - (r + 2\lfloor \frac{m}{2} \rfloor - 2k) = r^2 - r + 3k + 1 - m \geq r^2 - r + 1$ (because $k \geq 1$ and $m \leq 3$). We see that $g + h \geq 0$; for otherwise, $(r + g)(r + h) \leq (\frac{2r+g+h}{2})^2 \leq r^2 - r + \frac{1}{4}$, a contradiction. Since $a + b \geq 1$ and by (P8), $e + f \leq m - 2$.

This implies $y_2 + y_3 = r + e + r + f \leq 2r + m - 2$. Since $y_3 = r + f \leq r + \frac{1-c}{2} \leq \frac{2r+m-2}{2}$ (because $c \geq 1$), it follows from Lemma 7.2.6 that $y_2 y_3 \leq (2r + m - 2 - (r + \frac{1-c}{2}))(r + \frac{1-c}{2})$. If $m = 2$, then

$$\begin{aligned} y_2 y_3 - y_1 &\leq (r - \tfrac{1-c}{2})(r + \tfrac{1-c}{2}) - (r^2 + d) \\ &= -(\tfrac{1-c}{2})^2 - d \\ &\leq -(\tfrac{2-c}{2})^2 - \tfrac{1}{4} \quad \text{(because } d \geq \tfrac{2-c}{2} \text{ by (P2))} \\ &< 0, \text{ a contrdiction.} \end{aligned}$$

So $m = 3$. Then

$$\begin{aligned} y_2 y_3 - y_1 &\leq (r + 1 - \tfrac{1-c}{2})(r + \tfrac{1-c}{2}) - (r^2 + k - 1 + d) \\ &= -(\tfrac{1-c}{2})^2 + \tfrac{1-c}{2} - d - k + r + 1 \\ &\leq -(\tfrac{1-c}{2})^2 - k + r + 1 \quad \text{(because } d \geq \tfrac{1-c}{2} \text{ by (P2))} \\ &\leq -k^2 + k + r \quad \text{(because } c \geq 2k - 1) \\ &= -(k - \tfrac{1}{2})^2 + r + \tfrac{1}{4} \\ &< 0 \text{ (by (i) of Lemma 7.2.7), a contradiction.} \end{aligned}$$

□

7.3 The Proof of (5)

In this section, we complete the proof of (5). We first prove $F(3, q)$ increases linearly in q. Because $r \geq \sqrt{q+2} - 2$, we see that $F(3, q) \geq 3r^2 > 2q - 5$. This fact will be used in the proof of next lemma.

Lemma 7.3.1. *For any integer $q \geq 15$, $F(3, q) + 1 \leq F(3, q + 1) \leq F(3, q) + 3$.*

Proof. To see $F(3, q) + 1 \leq F(3, q + 1)$, let C be a maximum IPP code over Q of length 3, where $Q = \{\alpha_1, \ldots, \alpha_q\}$. Let $Q' := \{\alpha_1, \ldots, \alpha_{q+1}\}$. Define $C' := C \cup \{(\alpha_{q+1}, \alpha_{q+1}, \alpha_{q+1})\}$. Clearly, the codeword $(\alpha_{q+1}, \alpha_{q+1}, \alpha_{q+1})$ does not share any coordinate with codewords in C, and hence, C' is an IPP code over Q' of length 3. This shows $F(3, q) + 1 \leq F(3, q + 1)$.

To prove $F(3, q+1) \leq F(3, q)+3$, we assume for a contradiction that $F(3, q+1) \geq F(3, q)+4$ for some integer $q \geq 1$. Let $N_{q+1} = \{2, 3, \cdots, q - 3\}$, and $N_q = \{2, 3, \cdots, q - 4\}$. Because $F(3, q + 1) \geq F(3, q) + 4$ and by Theorem 6.3.1, there exists $\mathbf{x} = (x_1, x_2, x_3, y_1, y_2, y_3, z_1, z_2, z_3) \in N_{q+1}^9$ satisfying (14) (with q replaced by $q + 1$), such that $x_3 + y_1 + z_2 = F(3, q + 1) \geq F(3, q) + 4$.

In what follows, we shall find $\mathbf{x}' = (x_1', x_2', x_3', y_1', y_2', y_3', z_1', z_2', z_3') \in N_q^9$ satisfying (14) such that $x_3' + y_1' + z_2' \geq F(3,q) + 1$, a contradiction. Recall from (14) that $x_3 \geq x_1 + x_2 - 1$, $y_1 \geq y_2 + y_3 - 1$, and $z_2 \geq z_1 + z_3 - 1$.

Let $x_3' = x_3 - 1$, $y_1' = y_1 - 1$, and $z_2' = z_2 - 1$. If $x_3 \geq x_1 + x_2$, then let $x_1' = x_1$ and $x_2' = x_2$; if $x_3 = x_1 + x_2 - 1$, let $x_1' = x_1 - 1$ and $x_2' = x_2$ when $x_1 \geq x_2$, and let $x_1' = x_1$ and $x_2' = x_2 - 1$ when $x_1 < x_2$. If $y_1 \geq y_2 + x_3$, then let $y_2' = y_2$ and $y_3' = y_3$; if $y_1 = y_2 + y_3 - 1$, then let $y_2' = y_2 - 1$ and $y_3' = y_3$ when $y_2 \geq y_3$, and let $y_2' = y_2$ and $y_3' = y_3 - 1$ when $y_2 < y_3$. If $z_2 \geq z_1 + z_3$, then let $z_1' = z_1$ and $z_3' = z_3$; if $z_2 = z_1 + z_3 - 1$, let $z_1' = z_1 - 1$ and $z_3' = z_3$ when $z_1 \geq z_3$, and let $z_1' = z_1$ and $z_3' = z_3 - 1$ when $z_1 < z_3$.

When $x_3 \geq x_1 + x_2$, $x_3' - x_1'x_2' = (x_3 - 1) - x_1x_2 < x_3 - x_1x_2 \leq 0$. So we may assume $x_3 = x_1 + x_2 - 1$. Suppose $x_1 \geq x_2$. Then $x_3' - x_1'x_2' = (x_1 + x_2 - 2) - (x_1 - 1)x_2 = x_1 + 2x_2 - x_1x_2 - 2$. If $x_2 = 2$, then $x_3' - x_1'x_2' = 2 - x_1 \leq 0$; otherwise, $x_2 \geq 3$, and so, $x_3' - x_1'x_2' \leq 2x_2 - 2x_1 - 2 < 0$. Hence, $x_3' - x_1'x_2' \leq 0$. By exchanging the roles of x_1 and x_2 in the above argument, we can show $x_3' - x_1'x_2' \leq 0$ when $x_1 < x_2$. Similarily, we can show $y_1' - y_2'y_3' \leq 0$ and $z_2' - z_1'z_3' \leq 0$. So $\mathbf{x}'$ satisfies (i), (ii) and (iii) of (14).

Clearly, for $1 \leq i \leq 3$, $x_i' + y_i' + z_i' \leq x_i + y_i + z_i - 1 \leq (q+1) - 1 = q$. So $\mathbf{x}'$ satisfies (iv), (v) and (vi) of (14).

If $x_3 \geq x_1 + x_2$ then $x_1' + x_2' - 1 - x_3' = x_1 + x_2 - x_3 \leq 0$; if $x_3 = x_1 + x_2 - 1$ then $x_1' + x_2' - 1 - x_3' = x_1 + x_2 - 1 - x_3 = 0$. So $x_1' + x_2' - 1 - x_3' \leq 0$. Similarly, we have $y_2' + y_3' - 1 - y_1' \leq 0$, and $z_1' + z_3' - 1 - z_2' \leq 0$. Hence $\mathbf{x}'$ satisfies (vii), (viii) and (ix) of (14).

Therefore, we have shown that $\mathbf{x}'$ satisfies (14). It remains to show that $\mathbf{x}' \in N_q^9$. In fact, it suffices to show $x_i', y_i', z_i' \geq 2$ for $1 \leq i \leq 3$, because x_i', y_i', z_i' satisfy (iv)-(vi) of (14).

Since $\mathbf{x} \in N_{q+1}^9$, $x_i, y_i, z_i \geq 2$ for $i = 1, 2, 3$. Therefore, if $x_3 \geq x_1 + x_2$, then $x_1' = x_1 \geq 2$, $x_2' = x_2 \geq 2$, and $x_3' = x_3 - 1 \geq x_1' + x_2' - 1 > 2$. So we may assume $x_3 = x_1 + x_2 - 1$. We may further assume $x_1 \geq x_2$, as the case $x_2 > x_1$ can be treated in the same way. So $x_1' = x_1 - 1 \geq 1$, $x_2' = x_2 \geq 2$, and $x_3' = x_1' + x_2' - 1 \geq 2$. If $x_1' = 1$ then $x_1 = 2$, and $x_2 = 2$ (since $x_1 \geq x_2$), which implies $x_3 = 3$. Then because $y_1 \leq q - 3$ and $z_2 \leq q - 3$, $F(3, q+1) = x_3 + y_1 + z_2 \leq 2q - 3$. However, from Lemma 4.2.7, we know that $F(3, q+1) \geq 2q - 3$, a contradiction. Hence, $x_2' \geq 2$. Thus, we have shown $x_i' \geq 2$ for $i = 1 \leq i \leq 3$. By similar arguments, we can show $y_i', z_i' \geq 2$ for

$1 \le i \le 3$. Therefore, $\mathbf{x}' \in N_q^9$. □

We proceed according to the values of $k = q - (r^2 + 2r)$.

Lemma 7.3.2. *Let $q = r^2 + 2r + k$ for some integer $r \ge 6$. Then (5) holds when $k \in I_1$.*

Proof. We apply induction on k. When $k = 1$, $F(3, q) = 3r^2 + 1$ by Lemma 7.2.8. So assume that k is odd and $3 \le k \le 2\sqrt{r+4} - 3$ or k is even and $2 \le k \le 2\sqrt{r+2} - 2$, and assume $F(3, r^2 + 2r + k - 1) = h(r^2 + 2r + k - 1) = 3r^2 + 3(k-1) - 2$. From Lemma 7.3.1, we have $F(3, r^2 + 2r + k) \le F(3, r^2 + 2r + k - 1) + 3$. So $F(3, r^2 + 2r + k) \le 3r^2 + 3k - 2 = h(r^2 + 2r + k)$. Since we already know from Lemma 4.2.7 that $F(3, r^2 + 2r + k) \ge 3r^2 + 3k - 2$ when k is odd and $2 \le k \le 2\sqrt{r+4} - 3$ or when k is even and $2 \le k \le 2\sqrt{r+2} - 2$, we have $F(3, q) = 3r^2 + 3k - 2$. □

By the same proof as for Lemma 7.3.2, we can prove the following three lemmas.

Lemma 7.3.3. *Let $q = r^2 + 2r + k$ for some integer $r \ge 6$. Then (5) holds when $k \in I_2$.*

Lemma 7.3.4. *Let $q = r^2 + 2r + k$ for some integer $r \ge 6$. Then (5) holds when $k \in I_4$.*

Lemma 7.3.5. *Let $q = r^2 + 2r + k$ for some integer $r \ge 6$. Then (5) holds when $k \in I_5$.*

Now (5) holds by Lemmas 7.1.1, 7.2.3, 7.2.5, 7.3.2, 7.3.3, 7.3.4, 7.3.5, and Theorem 4.2.7.

CHAPTER VIII

IPP CODES OF LENGTH 5

In this Chapter, we study IPP codes of length 5 over an alphabet Q when $q = |Q|$ is a prime power. For each code $C \subseteq Q^5$, we associate an edge colored graph G with C. The vertices of G represent the codewords in C, and two vertices of G are joined by an edge of color i if their corresponding codewords have the same ith coordinate, $1 \leq i \leq 5$. Hence, edges of an associated graph of an IPP code of length 5 may use colors from $\{1, 2, 3, 4, 5\}$.

Unless stated explicitly otherwise we assume through this Chapter, q is a prime power.

8.1 Bounds on $F(5, q)$

As a trivial case, $F(5, 1) = 1$. We next develop bounds on $F(5, q)$ when q is a prime power.

Lemma 8.1.1. $F(5, 2) = 2$.

Proof. Let $Q = \{\alpha_1, \alpha_2\}$. It is easy to see that $F(5, 2) \geq 2$, since we can simply construct an IPP code $C \subseteq Q^5$ with $C = \{(\alpha_i, \alpha_i, \alpha_i, \alpha_i, \alpha_i) : \alpha_i \in Q, i = 1, 2\}$.

To prove $F(5, 2) \leq 2$, we consider any code $C \subseteq Q^5$ with $|C| \geq 3$. Let $\mathbf{a} = (a_1, a_2, a_3, a_4, a_5)$, $\mathbf{b} = (b_1, b_2, b_3, b_4, b_5)$, and $\mathbf{c} = (c_1, c_2, c_3, c_4, c_5)$ be three distinct codewords in C. So for each $1 \leq i \leq 5$, $\{a_i, b_i, c_i\} \subseteq Q$ and since Q is a binary alphabet, at least two of $\{a_i, b_i, c_i\}$ are the same, that is, $|(\{a_i\} \cap \{b_i\}) \cup (\{a_i\} \cap \{c_i\}) \cup (\{b_i\} \cap \{c_i\})| = 1$. For $1 \leq i \leq 5$, let $\{x_i\} = (\{a_i\} \cap \{b_i\}) \cup (\{a_i\} \cap \{c_i\}) \cup (\{b_i\} \cap \{c_i\})$, then

$$\mathbf{x} = (x_1, x_2, x_3, x_4, x_5) \in desc(\mathbf{a}, \mathbf{b}) \cap desc(\mathbf{a}, \mathbf{c}) \cap desc(\mathbf{b}, \mathbf{c}).$$

This implies $\mathbf{x}$ has no identifiable parent. Hence, C has no IPP. This proves $F(5, 2) \leq 2$. Therefore, $F(5, 2) = 2$. □

The proof of Lemma 8.1.1 in fact shows $F(n, 2) = 2$ for all $n \geq 1$.

Lemma 8.1.2. $F(5, 3) \geq 9$.

Proof. Without loss of generality, suppose $Q = GF(3) = \{0, 1, 2\}$. Recall the ternary Hamming code mentioned in Chapter1, we can extend the ternary Hamming code to obtain an IPP code of length 5 over Q by a very simple encoding procedure. Choose the parity check matrix

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 2 & 1 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \tag{30}$$

and let $C = \{\mathbf{c} \in Q^5 : H\mathbf{c} = \mathbf{0}\}$, then C is an extended (5,3,2)-code as follows,

$$C = \begin{Bmatrix} \mathbf{c}_1 = (0,0,0,0,0), & \mathbf{c}_4 = (1,0,1,1,0), & \mathbf{c}_7 = (2,0,2,2,0) \\ \mathbf{c}_2 = (0,1,1,2,0), & \mathbf{c}_5 = (1,1,2,0,0), & \mathbf{c}_8 = (2,1,0,1,0) \\ \mathbf{c}_3 = (0,2,2,1,0), & \mathbf{c}_6 = (1,2,0,2,0), & \mathbf{c}_9 = (2,2,1,0,0) \end{Bmatrix}. \tag{31}$$

Or, we can think the above extended Hamming code is obtained by adding 0 as the 5th coordinate to each codeword in the ternary Hamming code. Since the ternary Hamming code is an IPP code, it follows quickly from Lemma 2.2.1 that the extended code above is also an IPP code. Therefore, $F(5,3) \geq 9$. □

Next, we consider $q \geq 4$ and q is a prime power. The following two results are proved in [31] (Theorem 4).

Lemma 8.1.3. *Let C be a q-ary code of length n. If the minimum distance d_{min} of C satisfies $d_{min} > \frac{3n}{4}$, then C has the IPP.*

Lemma 8.1.4. *Let q be a prime power. If $q \geq n-1$ then a (shortened, extended, or doubly extended) $(n, \lceil n/4 \rceil, n - \lceil n/4 \rceil + 1)$-Reed-Solomon code over $GF(q)$ exists and has the IPP.*

As a consequence of Lemma 8.1.4, when $n = 5$ and $q \geq 4$ is a prime power, then there exists a (shorted, extended, or doubly extended) (5,2,4)-IPP Reed-Solomon code, and this IPP code has q^2 codewords. From Lemma 8.1.4, we also realize that when $q \geq 4$ and q is a prime power, there exists an IPP code $C \subseteq Q^5$ with size q^2 and its associated graph is a simple graph. By combining it with Lemma 8.1.2, we obtain the following result.

Theorem 8.1.5. *Let $q \geq 3$ be a prime power. Then $F(5,q) \geq q^2$. Moreover, if $q \geq 4$ and q is a prime power, then there exists an IPP code $C \subseteq Q^5$ with size q^2 whose associated graph is a simple graph.*

With the help of Theorem 8.1.5, we are now ready to study the structure of the associated graphs of IPP codes of length 5. If the associated graph of an IPP code $C \subseteq Q^5$ consists of only isolated vertices, then clearly $|C| \leq q$ and hence is not a maximum IPP code. Therefore, we may assume from now on the edge set of any associated graph is not empty.

8.2 Structural Characterization of IPP Graphs

We saw that the associated graphs of all maximum IPP codes of length 3 are simple graphs and they consist of three bi-color components. Now, some natural questions come up: Are the associated graphs of maximum IPP codes of length 5 simple? Should they also contain some special components? In this section, we look for answers to these questions.

The following result gives an upper bound on the size of an IPP code of length 5 if its associated graph is simple. It is a direct consequence of Lemma 8.1.3.

Lemma 8.2.1. *Let $C \subseteq Q^5$ be an IPP code and G be its associated graph. If G is simple then G is an IPP graph and hence C is an IPP code. Moreover, $|C| \leq q^2$.*

Proof. Suppose G is simple then any two vertices of G are joined by at most one edge, so any two codewords in C share at most one coordinate. This means the Hamming distance of any two codewords in C is 4 or 5, thus, the minimum distance of C is 4. By Lemma 8.1.3, C has the IPP. For any pair (α_i, α_j), α_i and α_j occur as the first and second coordinate in at most one codeword, so $|C| \leq q^2$. □

The following result describes an upper bound on the size of an IPP code of length 5 if two vertices of its associated graph are joined by more than two edges.

Lemma 8.2.2. *Let $C \subseteq Q^5$ be an IPP code and G be its associated graph. If there exist two vertices of G which are joined by more than two edges, then $|V(G)| \leq q^2$.*

Proof. Without loss of generality, suppose two vertices $u, v \in V(G)$, which correspond to two codewords $(\alpha_1, \alpha_1, \alpha_1, \beta_1, \beta_2)$ and $(\alpha_1, \alpha_1, \alpha_1, \gamma_1, \gamma_2)$ in C, are joined by three edges using colors 1, 2, 3, respectively. Now let $w = (\alpha_i, \alpha_j, \alpha_k, x, y)$. Then the descendant $d = (\alpha_1, \alpha_1, \alpha_1, x, y)$ shows that $(x, y) \neq (\beta_1, \beta_2)$, $(x, y) \neq (\gamma_1, \gamma_2)$ and that no other codeword has (x, y) as the fourth and fifth coordinate simultaneously. Hence $|V(G)| = |C| \leq q^2$. □

As a result of Lemma 8.2.2 and Theorem 8.1.5, we obtain the following,

Theorem 8.2.3. *There exists a maximum IPP code of length 5 so that any two vertices in its associated graph are joined by no more than two edges.*

Thus, in the rest of this chapter, we consider these IPP codes whose associated graphs have multiplicity less than or equal to 2. That is, we assume any two vertices of associated graphs of IPP codes of length 5 are joined by no more than two edges. Next, let us consider the components of associated IPP graphs.

Lemma 8.2.4. *Let $C \subseteq Q^5$ and G be its associated graph, and let S, T be unions of components of G such that $S \cap T = \emptyset$ and $S \cup T = G$. If S and T are IPP graphs and no two vertices of G are joined by more than two edges, then G is an IPP graph.*

Proof. This proof is slightly different from Lemma 3.2.1. We mark the following fact: (*) Since S, T are unions of components of G such that $S \cap T = \emptyset$ and $S \cup T = G$, for each $i \in \{1, 2, 3, 4, 5\}$, a component of $S(i)$ or a component of $T(i)$ is a component of $G(i)$. This fact will be used heavily through the rest of this proof.

It suffices to prove that G satisfies (IPP1) and (IPP2) of Lemma 2.2.2. To prove that G satisfies (IPP1) of Lemma 2.2.2, let u, v, w be three distinct vertices of G. We need to show that there exists some $i \in \{1, 2, 3, 4, 5\}$ such that u, v, w belong to three different components of $G(i)$.

First, assume $\{u, v, w\} \subseteq V(S)$. Since S is an IPP graph, there exists some $i \in \{1, 2, 3, 4, 5\}$ such that u, v, w belong to three different components of $S(i)$. By (*), u, v, w belong to three different components of $G(i)$.

So we may assume that $\{u, v, w\} \nsubseteq V(S)$. Similarly, we may assume that $\{u, v, w\} \nsubseteq V(T)$.

Then by symmetry, we may assume that $u, v \in V(S)$ and $w \in V(T)$. Since S is an IPP graph, there exists some $i \in \{1, 2, 3, 4, 5\}$ such that u and v belong to two different components of $S(i)$. Because $S \cap T = \emptyset$, the component of $T(i)$ containing w is disjoint from $S(i)$. By (*), u, v, w belong to three different components of $G(i)$. So G satisfies (IPP1) of Lemma 2.2.2.

To prove that G satisfies (IPP2) of Lemma 2.2.2, let u, v, w, x be four distinct vertices of G. We need to show that there exists some $i \in \{1, 2, 3, 4, 5\}$, no component of $G(i)$ containing u or v contains w or x.

Suppose $\{u, v, w, x\} \subseteq V(S)$. Since S is an IPP graph, there exists some $i \in \{1, 2, 3, 4, 5\}$ such that no component of $S(i)$ containing u or v contains w or x. By (*), no component of $G(i)$ containing u or v contains w or x.

Therefore, we may assume that $\{u, v, w, x\} \nsubseteq V(S)$. Similarly, we may assume that $\{u, v, w, x\} \nsubseteq V(T)$.

Assume for the moment that one of S and T contains three of $\{u, v, w, x\}$, and the other contains one of $\{u, v, w, x\}$. By symmetry, we may assume that $u, v, w \in V(S)$ and $x \in V(T)$. Since S is an IPP graph, there exists some $i \in \{1, 2, 3, 4, 5\}$ such that u, v, w belong to three different components of $S(i)$. Because $S \cap T = \emptyset$, the component of $T(i)$ containing x is disjoint from $S(i)$. By (*), no component of $G(i)$ containing u or v contains w or x.

Thus, we may assume that each of S and T contains exactly two vertices from $\{u, v, w, x\}$. We need to consider two cases.

First, one of S and T contains $\{u, v\}$ and the other contains $\{w, x\}$. By symmetry, we may assume $\{u, v\} \subseteq V(S)$ and $\{w, x\} \subseteq V(T)$. Since S is an IPP graph, there exists some $i \in \{1, 2, 3, 4, 5\}$ such that u, v belong to different components of $S(i)$. Note that any component of $T(i)$ containing w or x is contained in T, and hence, is disjoint from $S(i)$. By (*), no component of $G(i)$ containing u or v contains w or x.

The remaining case to be considered is when neither S nor T contains $\{u, v\}$ or $\{w, x\}$. By symmetry, we may assume $\{u, w\} \subseteq V(S)$ and $\{v, x\} \subseteq V(T)$. Since $u, w \in V(S)$ are joined by no more than two edges, there exists $\{i_1, i_2, i_3\} \in \{1, 2, 3, 4, 5\}$, such that for each $i \in \{i_1, i_2, i_3\}$, u, w belong to different components of $S(i)$. Since $v, x \in V(S)$ are joined by no more than two edges, there exists $\{j_1, j_2, j_3\} \in \{1, 2, 3, 4, 5\}$, such that for each $j \in \{j_1, j_2, j_3\}$, u, w belong to different components of $S(j)$. Note that $\{i_1, i_2, i_3\} \cap \{j_1, j_2, j_3\} \neq \phi$. Choose some $k \in \{i_1, i_2, i_3\} \cap \{j_1, j_2, j_3\}$, by (*), u, v, w, x belong to four different components of $G(k)$. Therefore, G satisfies (IPP2) of Lemma 2.2.2. □

Lemma 8.2.5. *Let $C \subseteq Q^5$ be a maximum IPP code and G be its associated graph. Then G contains at least one five-color component.*

Proof. Assume G does not contain any five-color components. Let $S_1, S_2, \cdots, S_m$ be the components of G, each S_i for $1 \leq i \leq m$ is uni-color, bi-color, tri-color or four color component. Then $|S_i| \leq q$ and the inequality holds if $m \geq 2$. Clearly $m \leq q$, so $\sum_{i=1}^{m} |S_i| < q^2$. Hence, C is not maximum, a contradiction. □

Lemma 8.2.6. *Suppose $C \subseteq Q^5$ is a maximum IPP code which is chosen so that its associated graph G has the minimum number of components. Then G contains no uni-color component and bi-color component.*

Proof. Assume G contains a uni-color component (respectively, a bi-color component) S, whose edges are colored by color i for some $i \in \{1, 2, 3, 4, 5\}$ (respectively, whose edges are colored by colors i, j for $\{i, j\} \subset \{1, 2, 3, 4, 5\}$). Let $\mathcal{A} = \{i\}$ (respectively, $\mathcal{A} = \{i, j\}$). By Lemma 8.2.5, let T be a five-color component. Then the edges of T use five colors from $\{1, 2, 3, 4, 5\}$. Then $T(i)$ contains a component with at least two vertices, let T' be such a component of $T(i)$. Let S' be a component of $S(i)$ (If S is a uni-color component, then $S' = S(i) = S$). Let G' be the graph obtained from G by adding edges uv of color i for all $u \in V(S')$ and $v \in V(T')$.

Clearly, G' is the graph associated with a code $C' \subseteq Q^5$ obtained from C by changing the ith coordinate of those codewords in C corresponding to vertices of S' to the ith coordinate of the codewords in C corresponding to vertices of T'. Let H be the component of G' containing $S' \cup T$. Note that $G - V(H)$ consists of components of G, and hence, is an IPP graph.

To prove H is an IPP graph, it suffices to prove that H satisfies (IPP1) and (IPP2) of Lemma 2.2.2. Since G is an IPP graph, S and T are also IPP graphs. We mark the following fact: (**) for each $l \in \{1, 2, 3, 4, 5\}$, a component of $T(l)$ other than T' is a component of $H(l)$, a component of $S(l)$ other than S' is a component of $H(l)$, and $T' \cup S'$ is a component of $H(i)$. This fact will be used heavily through the rest of the proof.

First, assume $\{u, v, w\} \subseteq V(S)$. Choose $k \in \{1, 2, 3, 4, 5\} - \mathcal{A}$, u, v, w belong to three different components of $S(k)$. Since a component of $S(k)$ is also a component of $H(k)$, u, v, w belong to three different components of $H(k)$.

Now assume $\{u, v, w\} \subseteq V(T)$. Since T is an IPP graph, there exists some $k \in \{1, 2, 3, 4, 5\}$ such that u, v, w belong to three different components of $T(k)$. Let these three components be T_1, T_2, T_3.

By (**), if T_1, T_2, T_3 are distinct from T', then u, v, w belong to three different components T_1, T_2, T_3 of $H(k)$. Otherwise, one of T_1, T_2, T_3 is T', say T_1 is T', then u, v, w belong to three different components $T' \cup S', T_2, T_3$ of $H(k)$.

So we may assume that one of $V(S)$ and $V(T)$ contains two of $\{u, v, w\}$ and the other one contains one of $\{u, v, w\}$.

First assume $u, v \in V(S)$ and $w \in V(T)$. Choose $k \in \{1, 2, 3, 4, 5\} - \mathcal{A}$, then u, v belong to two different components of $S(k)$, w belong to a component of $T(k)$. By (**), u, v, w belong to three different components of $H(k)$.

Otherwise, suppose $u, v \in V(T)$ and $w \in V(S)$. Since any two vertices of T are joined by no more than two edges, there exist at lease three colors $k_1, k_2, k_3 \in \{1, 2, 3, 4, 5\}$ such that u, v belong to different components of $T(k)$ for each $k \in \{k_1, k_2, k_3\}$. Choose $k \in \{k_1, k_2, k_3\} - \mathcal{A}$, then u, v belong to two different components of $T(k)$, w belong to a component of $S(k)$. By (**), u, v, w belong to three different components of $H(k)$.

To prove that H satisfies (IPP2) of Lemma 2.2.2, let u, v, w, x be four distinct vertices of H. We need to show that there exists some $k \in \{1, 2, 3, 4, 5\}$, no component of $H(k)$ containing u or v contains w or x.

First, assume $\{u, v, w, x\} \subseteq V(S)$. Choose $k \in \{1, 2, 3, 4, 5\} - \mathcal{A}$, u, v, w, x belong to four different components of $S(k)$. By (**), no component of $H(k)$ containing u or v contains w or x.

Now assume $\{u, v, w, x\} \subseteq V(T)$. Since T is an IPP graph, there exists some $k \in \{1, 2, 3, 4, 5\}$ such that no component of $T(k)$ containing u or v contains w or x. By (**), if $k \neq i$, clearly no component of $H(k)$ containing u or v contains w or x. If $k = i$ and T' contains neither u nor v, then $T' \cup S$ contains neither u nor v, and so no component of $H(k)$ containing u or v contains w or x. Finally, if $k = i$ and T' contains u or v, since T' contains neither w neither x and so does S, $T' \cup S$ contains neither w nor x. Hence, no component of $H(k)$ containing u or v contains w or x.

Therefore, we may assume that $\{u, v, w, x\} \not\subseteq V(S)$ and $\{u, v, w, x\} \not\subseteq V(T)$.

Assume for the moment that one of S and T contains three of $\{u, v, w, x\}$, and the other contains one of $\{u, v, w, x\}$.

We first consider $V(S)$ contains three of $\{u, v, w, x\}$ and $V(T)$ contains one of $\{u, v, w, x\}$. By symmetry, there are two cases: $u, v, w \in V(S)$ and $x \in V(T)$, or $u, w, x \in V(S)$ and $v \in V(T)$.

Assume $u, v, w \in V(S)$ and $x \in V(T)$, then choose $k \in \{1,2,3,4,5\} - \mathcal{A}$, it follows that u, v, w belong to three different components of $S(k)$, and x belong to some component of $T(k)$. By (**), u, v, w, x belong to four different components of $H(k)$. In the same way, we can show if $u, w, x \in V(S)$ and $v \in V(T)$ then $\{u, v, w, x\}$ belong to four different components of $H(k)$. Hence, no component of $H(k)$ containing u or v contains w or x.

Now consider $V(T)$ contains three of $\{u, v, w, x\}$ and $V(S)$ contains one of $\{u, v, w, x\}$. By symmetry, there are also two cases: $u, v, w \in V(T)$ and $x \in V(S)$, or $u, w, x \in V(T)$ and $v \in V(S)$. Assume that $u, v, w \in V(T)$ and $x \in V(S)$. Since T is an IPP graph, there exists some $k \in \{1,2,3,4,5\}$ such that u, v, w belong to three different components of $T(k)$, say these three components are T_1, T_2, T_3, and $u \in V(T_1)$, $v \in V(T_2)$, $w \in V(T_3)$. Let x belong to some component of $S(k)$. By (**), if either T_1, T_2, T_3 are all distinct from T' or $x \notin V(S')$, then $\{u, v, w, x\}$ belong to four different components of $H(k)$. So no component of $H(k)$ containing u or v contains w or x in this case. If one of $\{T_1, T_2, T_3\}$ is T' and $x \in V(S')$, then $k = i$. We may assume $T_1 = T'$. Since $|V(T')| \geq 2$, there must be $x' \in V(T')$ with $x' \neq u$. Since T is an IPP graph, there exists some $k' \in \{1,2,3,4,5\} - \{k\}$, such that no component of $T(k')$ containing u or v contains w or x'. By (**), no component of $H(k')$ containing u or v contains w or x'. Hence, no component of $H(k')$ containing u or v contains w or x. We can show in the same way that if $u, w, x \in V(T)$ and $v \in V(S)$, then no component of $H(k)$ containing u or v contains w or x.

Thus, we may assume that each of S and T contains exactly two vertices from $\{u, v, w, x\}$. We need to consider two cases.

First, one of S and T contains $\{u, v\}$ and the other contains $\{w, x\}$. Assume that $u, v \in V(S)$ and $w, x \in V(T)$. Then for each $k \in \{1,2,3,4,5\} - \mathcal{A}$, u, v belong to different components of $S(k)$. Since any two vertices of T are joined by no more than two edges, there exists $\{k_1, k_2, k_3\} \subseteq \{1,2,3,4,5\}$ such that for each $k \in \{k_1, k_2, k_3\}$, w, x belong to different components of $T(k)$. Choose some $k \in \{k_1, k_2, k_3\} \cap (\{1,2,3,4,5\} - \mathcal{A})$. By (**), $\{u, v, w, x\}$ belong to four different components of $H(k)$. Hence, no component of $H(k)$ containing u or v contains w or x. Again, we can show in the same way that if $u, v \in V(T)$ and $w, x \in V(S)$, then there exists some $k \in \{1,2,3,4,5\}$ such that no component of $H(k)$ containing u or v contains w or x.

The remaining case to be considered is when neither S nor T contains $\{u, v\}$ or $\{w, x\}$. By

symmetry, we may assume $\{u, w\} \subseteq V(S)$ and $\{v, x\} \subseteq V(T)$. For each $k \in \{1, 2, 3, 4, 5\} - \mathcal{A}$, u, w belong to different components of $S(k)$. Since $v, x \in V(T)$ are joined by no more than two edges, there exists $\{k_1, k_2, k_3\} \subseteq \{1, 2, 3, 4, 5\}$, such that for each $k \in \{k_1, k_2, k_3\}$, v, x belong to different components of $T(k)$. Note that $(\{1, 2, 3, 4, 5\} - \mathcal{A}) \cap \{k_1, k_2, k_3\} \neq \phi$. Choose some $k \in (\{1, 2, 3, 4, 5\} - \{i\}) \cap \{k_1, k_2, k_3\}$. By (**), u, v, w, x belong to four different components of $H(k)$. Therefore, H satisfies (IPP2) of Lemma 2.2.2.

Since both H and $G - V(H)$ are IPP graphs, it follows from Lemma 8.2.4 that G' is an IPP graph. However, $|V(G')| = |V(G)|$ and G' has fewer components than G, contradicting the choice of C and G. □

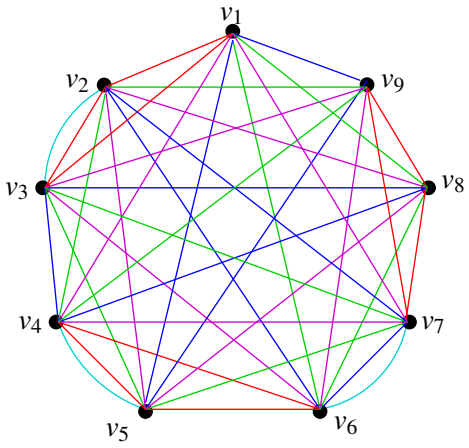
In Figure 16, we use red, blue, green, magenta and cyan to represent colors 1, 2, 3, 4, 5, respectively. A five-color component T is given in (a) and a bi-color component S is given in (b). Let T' be a subgraph of T spanned by $\{v_7, v_8, v_9\}$, then T' is a component of $G(1)$. Let S' be a subgraph of S spanned by $\{u_2, u_3\}$, then S' is a component of $S(1)$. Join every pair of vertices between $V(T')$ and $V(S')$ by an edge of color 1, we obtain the resulted graph H in (c), which is a new five-color component. It is easy to check that S, T, H are all IPP graphs.

Lemma 8.2.7. *Let $C \subseteq Q^5$ and G be the associated graph of C. Let S be a component of G. If S is a uni-color component, a bi-color component, a tri-color component or a four-color component of G, then S is an IPP graph.*

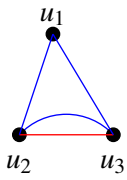
Proof. Suppose S is a uni-color, a bi-color component, a tri-color component or a four-color component. Let $i \in \{1, 2, 3, 4, 5\}$ be a color not used by edges of S. Then every component of $S(i)$ is an isolated vertex. Hence, (IPP1) and (IPP2) of Lemma 2.2.2 hold. Since G is associated with C, S is also associated with a code (whose codewords are the codewords in C corresponding to the vertices of S). Hence, S is an IPP graph. □

Lemma 8.2.8. *There exists a maximum IPP code of length 5 such that its associated graph has the minimum number of components and contains no tri-color component.*

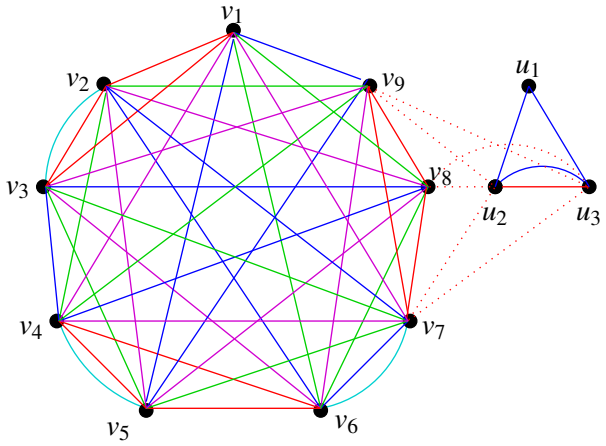
Proof. Suppose $C \subseteq Q^5$ is a maximum IPP code and its associated graph G has the mimum number of components. If G contains a tri-color component S, then $|E(S)| \geq 3$. Let the three colors used by the edges of S belong to $\{i, j, k\} \subseteq \{1, 2, 3, 4, 5\}$. It is easy to see that $|V(S)| \geq 3$, since any two



(a) A five−color component T



(b) A bi−color component S



(c) A new five−color component H

Figure 16: Combining a bi-color component and a five-color component

vertices of S are joined by no more than two edges, if $|V(S)| \leq 2$, then $|E(S)| \geq 2$, a contradiction. Hence, $|V(S)| \geq 3$.

We claim that there exist two vertices in $V(S)$ such that these two vetices are joined by no more than one edge. Suppose this is not true, then any two vertices of $V(S)$ are joined by two edges. Since S is a tri-color component, there must exist three vertices $v_1, v_2, v_3 \in V(S)$ such that v_1, v_2 are joined by two edges, say e_1, e_2, v_1, v_3 are joined by two edges, say e_3, e_4, v_2, v_3 are joined by two edges, say e_5, e_6, and the six edges e_m $(1 \leq m \leq 6$ use three colors. By the definition of the associated graph, two edges incident with the same two vertices use different colors. Hence, e_1 and

e_2 use different colors, e_3 and e_4 use different colors, and e_5 and e_6 use different colors. Since six edges e_k ($1 \leq m \leq 6$ use three colors, by the Pigeon-hole Principle, at least one color is used by two edges. Without loss of generality, say e_1, e_3 use color i. e_1 using color i implies that the two codewords corresponding to vertices v_1, v_2 share the ith coordinate, e_2 using color i implies that the two codewords corresponding to vertices v_1, v_3 share the ith coordinate, so the two codewords corresponding to vertices v_1, v_3 also share the ith coordinate. Hence, there is an edge incident with v_1, v_3 that uses color i, say this edge is e_5. Again, since e_k ($1 \leq m \leq 6$) use three colors and e_1, e_3, e_5 all use color i, it follows that e_2, e_4, e_6 use colors j, k. By the symmetry, assume e_2, e_4 use color j and e_6 uses color k. As before, e_2 using color j implies that the two codewords corresponding to vertices v_1, v_2 share the jth coordinate, e_4 using color j implies that the two codewords corresponding to vertices v_1, v_3 share the jth coordinate, so the two codewords corresponding to vertices v_1, v_3 also share the jth coordinate. Hence, there is an edge, say e_8, incident with v_1, v_3 that uses color j. So there are three edges e_3, e_4, e_8 incident with v_1, v_3, a contradiction. Therefore, there must exist two vertices in $V(s)$ that are joined by no more than one edge. Let such two vertices be u, v.

Let H be the four-color component obtained from S by joining u, v by an edge of color l for some $l \in \{1, 2, 3, 4, 5\} - \{i, j, k\}$, and let $G' = (G - V(S)) \cup H$. Clearly, G' is the graph associated with $C' \subseteq Q^5$ obtained from C by changing the lth coordinate of the codeword in C corresponding to vertex v to the lth coordinate of the codeword in C corresponding to vertex u. Note that $G - V(S)$ consists of components of G, and hence, is an IPP graph. H is a four-color component, by Lemma 8.2.7, H is an IPP graph. Since $G' = (G - V(S)) \cup H$ and $(G - V(S)) \cap H = \phi$, by Lemma 8.2.4, G' is an IPP graph. However, $|V(G)| = |V(G')|$ and G' has no tri-color component. □

By Lemma 8.2.5, Lemma 8.2.6 and Lemma 8.2.8, we obtain the following result to close this section.

Theorem 8.2.9. *There exists a maximum IPP code of length 5 such that its associated graph has at least one five-color component, but it has no uni-color component, bi-color component and tri-color component.*

8.3 Forbidden Subgraphs

In this section, we characterize that a code $C \subseteq Q^5$ has the IPP if and only if its associated graph does not contain certain edge colored subgraphs.

In Figure 17, four edge colored graphs are given, where $\{i_1, i_2, i_3, i_4, i_5\} = \{1, 2, 3, 4, 5\}$ represents five different colors. For example, in the edge colored graph (a), the two edges incident with u, v are colored by i_1 and i_2 respectively, and the edge incident with u, w is colored by i_5. Define the four edge colred graphs in Figure 17 as *forbidden graphs*,

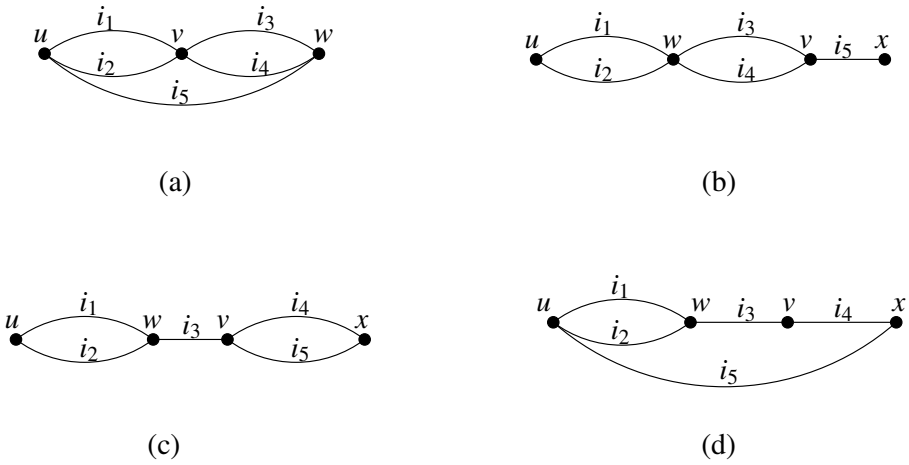


Figure 17: Forbidden edge-colored subgraphs

Lemma 8.3.1. *Let $C \subseteq Q^5$ be a code and G be its associated graph. If G is an IPP graph then G doesn't contain any forbidden graphs.*

Proof. Assume G contains a forbidden graph (a) as its subgraph, then $u, v, w \in V(G)$ and there exists no $i \in \{1, 2, 3, 4, 5\}$ such that u, v, w belong to three different components of $G(i)$, a contradiction to (IPP1) of Lemma 2.2.2.

Assume G contains a forbidden graph (b), then $u, v, w, x \in V(G)$ and there does not exist $i \in \{1, 2, 3, 4, 5\}$ such that no component of $G(i)$ containing u or v contains w or x, a contradiction to (IPP2) of Lemma 2.2.2. In the same way, we can show that if G contains a forbidden graph (c) or (d), then G doesn't satisfy (IPP2) of Lemma 2.2.2. □

Lemma 8.3.2. *Let $C \subseteq Q^5$ be a code and G be its associated graph. If G is not an IPP graph, then G must has a subgraph isomorphic to one of the forbidden graphs.*

Proof. Suppose G is not an IPP graph. Then either there exist three vertices $u, v, w \in V(G)$ such that u, v, w contradict (IPP1) of Lemma 2.2.2, or there exist four vertices $u, v, w, x \in V(G)$ such that u, v, w, x contradict (IPP2) of Lemma 2.2.2.

First, we assume there exist three vertices $u, v, w \in V(G)$ such that u, v, w contradict (IPP1) of Lemma 2.2.2. Let H be a subgraph of G such that $V(H) = \{u, v, w\}$ and $E(H)$ consists of edges incident with $\{u, v\}$, $\{u, w\}$ or $\{v, w\}$. Then $E(H)$ must contain five edges which use five different colors. Since any two vertices of G are joined by no more than two edges, we see that H contains a subgraph isomorphic to forbidden graph (a). A subgraph of H is also a subgraph of G, so G contains a subgraph isomorphic to forbidden graph (a).

Thus, we may assume there exist four vertices $u, v, w, x \in V(G)$ such that u, v, w, x contradict (IPP2) of Lemma 2.2.2. That is, there does not exist any $i \in \{1, 2, 3, 4, 5\}$ such that no component of $G(i)$ containing u or v contains w or x. Note that any edge incident with $\{u, v\}$ or $\{w, x\}$ does not contribute to the violation of (IPP2) here. Hence, let H be a subgraph of G such that $V(H) = \{u, v, w, x\}$ and $E(H)$ consist of edges incident with $\{u, w\}$, $\{u, x\}$, $\{v, w\}$ or $\{v, x\}$. It suffices to assume $E(H)$ is minimal so that u, v, w, x contradict (IPP2). Then $E(H)$ contains exactly five edges which use five different colors. Since there is no edge incident with $\{u, v\}$ and $\{w, x\}$, H is a bipartite graph and hence all cycles of H have even length. Since $V(H) = 4$ and $E(H) = 5$, H has at least one cycle with possible length 2 or 4. Hence, we discuss in two cases according to $g(H)$, the girth of H. If $g(H) = 2$, then H must be isomorphic to forbidden graph (b) or forbidden graph (c). If $g(H) = 4$, then H must be isomorphic to forbidden graph (d). □

By Lemma 8.3.1 and Lemma 8.3.2, we characterize the structure of IPP graphs associated with IPP codes of length 5.

Theorem 8.3.3. *Let $C \subseteq Q^5$ be a code and G be its associated graph. Then G is an IPP graph if and only if G does not contain any forbidden subgraphs.*

REFERENCES

[1] G. D. Cohen, Applications of coding theory to communication combinatorial problems, *Discr. Math*, **83** (1990), pp. 237-248.

[2] C. J. Colbourn abd P. C. van Oorschot, Applications of combinatorial designs in computer science, *ACM Computing Surveys* **21** (1981), pp. 223-250.

[3] D. R. Stison, Combinatorial designs and cryptography, *Surveys in Combinatorics*, Cambridge University Press (1993), pp. 257-287.

[4] C. J. Colbourn, J. H. Dinitz, and D. R. Stison, Applications of combinatorial designs to communications, cryptography, and networking, *Surveys in Combinatorics (J.D. Lamb and D.A. Preece, eds.)*, Cambridge University Press (1999), pp. 37-100.

[5] D. R. Stinson and R. Wei and L. Zhu, New constructions for perfect hash families and related structures using combinatorial designs and codes, *J. Combin. Designs*, **8** (2000), pp. 189–200.

[6] N. Wagner, Fingerprinting, *Proceedings of the 1983 IEEE Symposium on Security and Privacy* (April 1983), pp. 18–22.

[7] N. Heintze, Scalable document fingerprinting, in *Proc. USENIXWorkshop Electron. Commerce*, Nov. 1996.

[8] I. Cox, J. Bloom, and M. Miller, Digital Watermarking: Principles and Practice. San Francisco, CA: Morgan Kaufmann, 2001.

[9] D. Boneh and J. Shaw, Collusion-secure fingerprinting for digital data, *IEEE Trans. Inform. Theory*, **44** (1998), pp. 1897-1905.

[10] B. Chor, A. Fiat, M. Naor, and B. Pinkas, Tracing Traitors, *IEEE Trans. Inform. Theory*, **46** (2000), pp. 893–910.

[11] B. Chor, A. Fiat, and M. Naor, Tracing Traitors, in advanced in Cryptology (CRYPTO '94), Lecture Notes in Comput. Sci. **839** (1994), pp. 25–270.

[12] M. Naor and B. Pinkas, Threshold traitor tracing, in *Proc. Advances in CryptologyCrypto '98*, LNCS 1462 (1998), pp. 502-517.

[13] D. Boneh and M. Franklin, An efficient public key tracing scheme, in *Proc. Advances in CryptologyCrypto '99*, LNCS 1666 (1999), pp. 338-353.

[14] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, Multicast security: A taxonomy and some efficient constructions, in *Proc. INFOCOM '99*, **2**, New York (1999), pp. 708-716.

[15] I. Cox, J. Kilian, F. Leighton, and T. Shamoon, Secure spread spectrum watermarking for multimedia, *IEEE Trans. Image Processing*, **6** (1997), pp. 1673-1687.

[16] C. Dwork, J. Lotspiech, and M. Naor, Digital signets: Self-enforcing protection of digital information, in *28th Symp. Theory of Computation* (1996), pp. 489-498.

[17] C. Podilchuk and W. Zeng, Image adaptive watermarking using visual models, *IEEE J. Select. Areas Commun.*, **16** (1998), pp. 525-540.

[18] R. B. Wolfgang, C. I. Podilchuk, and E. J. Delp, Perceptual watermarks for digital images and video, *Proc. IEEE*, **87** (1999), pp. 1108-1126.

[19] F. A. P. Petitcolas, R. J. Anderson, and M. G. Kuhn, Information hidingA survey, *Proc. IEEE*, **87** (1999), pp. 1062-1078.

[20] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, Multimedia dataembedding and watermarking technologies, *Proc. IEEE*, **87** (1998), pp. 1064-1087.

[21] F. Hartung and M. Kutter, Multimediawatermarking techniques, *Proc. IEEE*, **87** (1999), pp. 1079-1107.

[22] H. S. Stone, Analysis of attacks on image watermarks with randomized coefficients, NEC Res. Inst. (1996), Tech. Rep. 96–045.

[23] B. Chen and G. W. Wornell, Quantization index modulation: A class of provably good methods for digital watermarking and information embedding, *IEEE Trans. Inform. Theory*, **47** (2001), pp. 14231443.

[24] F. Ergun, J. Kilian, and R. Kumar, A note on the limits of collusionresistant watermarks, in *Proc. Eurocrypt* (1999), pp. 140-149.

[25] M. Wu and B. Liu, Modulation and multiplexing techniques for multimedia data hiding, in *Proc. SPIE ITcom*, (2001) pp. 4518.

[26] H. V. Poor, *An Introduction to Signal Detection and Estimation*, 2nd ed. New York: Springer-Verlag, 1994.

[27] W. Trappe, M. Wu, Z. J. Wang, and K. J. R. Liu, Anti-collusion Fingerprinting for Multimedia, *IEEE Trans. Signal Processing.*, **51** (2003), pp. 1069–1086.

[28] J. N. Staddon, A combinatorial study of communication, storage and traceability in broadcast encryption systems, Ph.D. dissertation, Univ. Calif. Berkeley, 1997.

[29] D. M. Wallner, E. J. Harder, and R. C. Agee, Key Management for Multicast: Issues and Architectures, *RFC 2627*, June 1999.

[30] D. R. Stinson and R. Wei, "Combinatorial Properties and constructions of traceability Schemes and Frameproof Codes," *SIAM J. Discrete Math.*, **11** (1998), pp. 41–53.

[31] H. D. L. Hollmann, J. H. van Lint, J. Linnartz and L. M. G. M. Tolhuizen, On codes with the identifiable parent property, *J. Combin. Theory Ser. A* **82** (1998) 121–133.

[32] A. Barg, G. Cohen, S. Encheva, G. Kabatiansky and G. Zemor, "A hypergraph approach to the identifying parent property: the case of multiple parents," *SIAM J. Disc. Math.* **14** (2001), pp. 423–431.

[33] J. N. Staddon, D. R. Stinson, and R. Wei, Combinatorial Properties of Frameproof and Traceability Codes, *IEEE Trans. Inform. Theory*, **47** (2001), pp. 1042–1049.

[34] N. Alon, E. Fischer and M. Szegedy, Parent-identifying codes, *J. Combin. Theory Ser. A* **95** (2001), pp. 349–359.

[35] N. Alon, U. Stav, New bounds on parent-identifying codes: The case of multiple parents, *Combinatorics, Probability and Computing*, **13** (2004), pp. 795–807, Cambridge University Press.

[36] V. Tô and R. Safavi-Naini, On the maximal codes of length 3 with the 2-identifiable parent property, *SIAM J. Discrete Math.* **17** (2004) 548–570.

[37] S. Blackburn, An upper bound on the size of a code with the k-identifiable parent property, *J. Combin. Theory Ser. A*, **102** (2003), pp. 179–185.

[38] Tran van Trung and S. Martirosyan, New Constructions for IPP Codes, *Designs, Codes and Cryptography*, **35** (2005), pp. 227–239.

[39] R. Safavi-Naini and Y. Wang, New results on frameproof codes and traceability schemes, *IEEE Trans. Inform. Theory*, **47** (2001), pp. 3029–3033.

[40] P. Sarkar, D. R. Stinson, Frameproof and IPP Codes, *Proceedings of the Second International Conference on Cryptology in India: Progress in Cryptology*, (2001) pp.117–126.

[41] A. Silverberg, J. Staddon, J. L. Walker, Efficient traitor tracing algorithms using list decoding, *Proceedings of the 7th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology* (2001) pp. 175–192.

[42] F. Zane, Efficient Watermark Detection and Collusion Security, *Proceedings of Financial Cryptography 2000*, Feb. 2000.

[43] A. Silverberg, J. Staddon, and J. L. Walker, Applications of list decoding to tracing traitors, *IEEE Trans. Inform. Theory*, **49** (2003), pp. 1312–1318.

[44] M. Fernandz, M. Soriano, Decoding codes with the identifiable parent property, *Proceedings of the Seventh IEEE International Symposium on Computers and Communications* (2002), pp. 1–6.

[45] A. Fiat and T. Tassa, Dynamic traitor tracing, in *Proc. Advances in CryptologyCrypto '99*, LNCS 1666 (1999), pp. 388-397.

[46] J. Kerner and K. Marton, New bounds for perfect hashing via information theory, *Europ. J. Combin.*, **9** (1986), pp. 523–530.

[47] Y. Yemane, Codes with the *k*-identifiable parent property, PhD Thesis, Royal Holloway, University of London, 2002.

[48] N. Alon, J. Bruck, J. Naor, M. Naor, and R. Roth, Construction of asymptotically good low-rate error-correcting codes through pseudorandom graphs, *IEEE Trans. Inform. Theory*, **38** (1992), pp. 509-516.

[49] T. Cormen, C. Leiserson, and R. Rivest, *Introduction to Algorithms*, New York: McGraw-Hill, 1989.

[50] N. Alon, R. A. Duke, H. Lefmann, V. Rodl and R. Yuster, The algorithmic aspects of the Regularity Lemma, *Proceedings of the 33rd IEEE FOCS* at Pittsburgh (1992), pp. 473–481. Also: *Journal of Algorithms* **16** (1994), pp. 80–109.

[51] D. R. Stinson, Tran van Trung and R. Wei, Secure frameproof codes, key distribution patterns, group testing algorithms and related structures, *J. Statist. Planning Inference*, **86** (2000), pp. 595–617.

[52] Tran Van Trung, S. Martirosyan, On a class of traceability codes, designs, *Codes and Cryptography*, **31** (2004), pp. 125–132.

[53] Stephen B. Wicker, *Error Control Systems for Digital Communication and Storage*, Prentice-Hall, Inc., 1995.

[54] S. Roman, *Coding and Information Theory*, Springer-Verlag, Berlin, New York, 1992.

[55] J. H. van Lint, *Introduction to Coding Theory*, Springer-Verlag, Berlin, New York, 1982.

[56] J. Korner and A. Orlitski, Zero-error information theory, *IEEE Trans. Inform. Theory*, **44** (1998), pp. 2207-2229.

[57] F. J. MacWilliams and N. J. A. Sloane, *The Theorey of Error-Correcting Codes*, Elsevier, Amsterdam, 1977.

[58] I. Ruzsa, Solving a linear equation in a set of integers I, *Acta Arithmetica* **65** (1993), pp. 259–282.

[59] L. A. Bassalygo, S. I. Gelfand, and M. S. Pinsker, Simple methods for obtaining lower bounds in coding theory, *Problems Inform. Transmission*, **27** (1991), pp. 277-281.

[60] J. A. Bondy and U. S. R. Murty, *Graph theory with applications*, Macmillan Press Ltd, 1976.

[61] D. G. Luenberger, *Linear and Nonlinear Programming*, Second Edition, Kluwer Academic Publishers, 1987.