An Infinite Family of Kochen-Specker Sets in Four-Dimensional Real Spaces

by

Brandon Elford

B.Sc., Dalhousie University, 2016

Thesis Submitted in Partial Fulfillment of the
Requirements for the Degree of
Master of Science

in the
Department of Mathematics
Faculty of Science

SIMON FRASER UNIVERSITY
Fall 2018

Approval

Name:	**Brandon Elford**
Degree:	**Master of Science (Mathematics)**
Title:	**An Infinite Family of Kochen-Specker Sets in Four-Dimensional Real Spaces**
Examining Committee:	**Chair:** **Ladislav Stacho** Associate Professor **Petr Lisonek** Senior Supervisor Professor **Jonathan Jedwab** Supervisor Professor **Luis Goddyn** Examiner Professor
Date Defended:	**December 13, 2018**

Abstract

Contextuality is a feature differentiating between classical and quantum physics. It is anticipated that it may become an important resource for quantum computing and quantum information processing. Contextuality was asserted by the Kochen-Specker (KS) theorem. We study parity proofs of the KS theorem. Although many parity proofs exist, only finitely many of them have been discovered in any real or complex space of fixed dimension.

We study a special family of chordal ring graphs. We construct orthonormal representations of their line graphs in four-dimensional real spaces. Our construction takes advantage of the high degree of symmetry present in the special class of chordal rings that we use. In this way we find, for the first time, an infinite family of KS sets in a fixed dimension.

Keywords: Kochen-Specker Theorem; Chordal Ring Graph; Orthonormal Representation; Quantum Information Theory

Acknowledgements

I would like to thank Dr. Lisonek for the time and effort he spent on this thesis and research. His guidance has resulted in a project that I am truly proud of. I am grateful for the support from Dr. Lisonek's NSERC Discovery Grant, the NSERC Canadian Graduate Master's Scholarship and the Simon Fraser University Graduate Fellowship.

I would like to thank Dr. Goddyn and Dr. Jedwab for the helpful suggestions and time commitment necessary for my defence.

I would like to give thanks to my fiancée, Justine, who is always willing to give me her time and support. She is the reason I moved to Vancouver and I could not have finished this thesis without her.

I would like to thank my parents, Cathy and Trent, who have supported me throughout my entire education, all the way from Nova Scotia. As well I would like to thank my brother, Jesse, for providing much needed mental breaks in the form of video games.

Lastly, I would also like to acknowledge the Centre for Experimental and Constructive Mathematics (CECM) and my friends in the Mathematics Department at SFU. The resources available in CECM have been valuable to my research success and the community has been valuable to my sanity.

This thesis would not exist in this form without each and every one of these people.

Table of Contents

List of Figures

Chapter 1

Introduction

Quantum information theory relies on results from quantum mechanics. Contextuality is accepted by some as a feature of quantum mechanics. A proof of contextuality shows that the outcome of measuring an observable variable relies on its measurement context, and thus could not have existed before the measurement was made.

The Kochen-Specker (KS) Theorem is an important result in quantum physics demonstrating quantum contextuality. The phenomenon of contextuality is still under discussion among quantum physicists. We focus only on presenting the mathematical tools and structures which may be used in this argument. One such tool that is of interest as a combinatorial concept also provides proof of the KS Theorem. A common proof of the KS Theorem can be shown with a parity argument, which relies on the existence of a so-called KS set [15, 14]. It is worth noting that the parity proofs are possible only in even dimensions, though KS sets in odd dimensions do exist. The original KS set, presented in [12], requires 117 vectors contained in 132 bases over $\mathbb{R}^3$. Since this discovery, many simpler KS sets have been discovered. This includes a KS set discovered by Lisonek with 21 vectors and 7 bases [15], another with 18 vectors and 9 bases [3] and large finite families of KS sets (like those in [21] and [20]). Some of the previously discovered KS sets have been implemented in experiments. The KS set with 21 vectors and 7 bases published in [15] was immediately implemented in that same year [5]. Both papers were published in 2014, so shortly after a new KS set was discovered combinatorially, it was implemented for quantum information experiments. We aim to construct KS sets combinatorially and leave the experimental implementation to those knowledgeable in the topic.

With the amount of growth that the field of quantum computing has experienced in recent years, there has been a lot of time spent finding new and simpler KS sets. KS sets over $\mathbb{R}^3$ have been largely researched and the prospect of discovering new KS sets in $\mathbb{R}^3$ appears quite hopeless. Hence we decided to focus on discovering new KS sets in $\mathbb{R}^4$. Our target was to construct an infinite family of KS sets in $\mathbb{R}^4$, something that has not previously been done in fixed dimension. To build our KS sets, we focused on a certain type of vertex transitive graph whose orthonormal representation satisfies the requirements of a parity proof of the KS Theorem.

In this thesis, we begin by introducing necessary definitions and background. In Chapter 2 we review relevant concepts and results in graph theory, linear algebra, abstract algebra and complex numbers. We define orthonormal representations and further discuss KS sets. In Chapter 3 we outline the properties of our combinatorial model which we base our construction on. Chapter 4 is where we present our construction for an infinite family of KS sets in $\mathbb{R}^4$. This computer-free construction is proven rigorously and stands alone from numerical calculations which we discuss in Chapter 5. This last chapter reviews our process of discovery and is largely experimental. Before we started any analysis, we were able to collect a large data set which convinced us that a general construction was possible. We explain how we collected numerical data and we show how this data led us to the results given in Chapter 4. We include the details of the discovery process because we believe aspects of our approach may be applicable to other problems.

Chapter 2

Background

This chapter presents a review of necessary definitions and useful results for the rest of the thesis. We will discuss definitions in graph theory, abstract and linear algebra, complex numbers, group representations and orthonormal representations. We also state the requirements for a parity proof of the Kochen-Specker Theorem and define a KS set.

2.1 Graph Theory

Definition 2.1.1. *Let V be a finite set of vertices and E a set of unordered pairs of distinct vertices in V, also called edges. A* graph *G is the pair $G = (V, E)$. If the pairs of vertices are ordered, then we refer to the edges as arcs.*

Remark 2.1.2. *For the following definitions, assume that G is a graph with vertex set V and edge set E (sometimes denoted $V(G)$ and $E(G)$, respectively).*

Definition 2.1.3. *Two distinct vertices $x, y \in V$ are* adjacent *in G if and only if $\{x, y\} \in E$.*

Definition 2.1.4. *A vertex $x \in V$ is* incident *to an edge $e \in E$ in G if and only if $e = \{x, y\}$ for some vertex $y \in V$ such that $x \neq y$.*

Definition 2.1.5. *The* graph complement *of G is the graph $\overline{G} = (V, \overline{E})$ where $\overline{E}$ is the set of all edges between distinct vertices of V that are not in E.*

Definition 2.1.6. *The* line graph *of G, denoted $L(G)$, is the graph with vertex set E in which two edges in G are adjacent as vertices in $L(G)$ if and only if they are incident as edges in G.*

Definition 2.1.7. *The* degree of a vertex *$x \in V$ is the number of edges in G incident with x.*

Definition 2.1.8. *G is called* k-regular *if every vertex of G has degree k.*

Lemma 2.1.9. *If G is a k-regular graph, then $L(G)$ is $2(k-1)$-regular.*

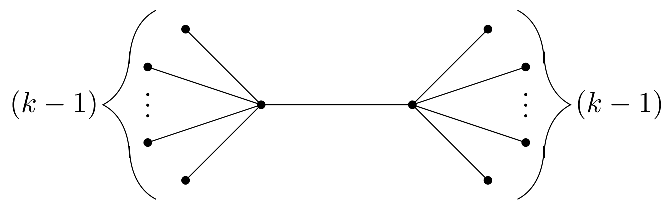

Figure 2.1: An edge in a k-regular graph.

Proof. Assume G is a k-regular graph. Then both endpoints of every edge of G are incident with exactly $k-1$ other edges in G (see Figure 2.1 below). Therefore each edge in G is incident with exactly $2(k-1)$ distinct edges. Thus each vertex of the line graph $L(G)$ is adjacent to exactly $2(k-1)$ distinct vertices. It immediately follows that $L(G)$ is $2(k-1)$-regular. □

Definition 2.1.10. *A* clique *in G is a set of mutually adjacent vertices in V. A maximal clique of G is a clique which is not properly contained within any other clique of G.*

Definition 2.1.11. *Let U be a subset of V such that no two vertices of U are adjacent in G. Then U is an* independent set *of G. The independence number of G is the cardinality of a largest independent set, denoted $\alpha(G)$.*

Definition 2.1.12. *A* fractional vertex packing *of G is a mapping $w : V \to \mathbb{R}_{\geq 0}$ such that*

$$\sum_{x \in C} w(x) \leq 1$$

for every clique C in G. The value

$$\sum_{x \in V} w(x)$$

is called the weight of the fractional vertex packing w.

Definition 2.1.13. *The maximum weight of any fractional vertex packing of G is called the* fractional packing number *of G and is denoted $\alpha^*(G)$.*

Definition 2.1.14. *An* automorphism *of G is a permutation of V that preserves adjacency for all pairs of vertices in V.*

Definition 2.1.15. *If for every $x, y \in V$ there exists an automorphism $\phi : V \to V$ such that $\phi(x) = y$, then G is called* vertex transitive.

Definition 2.1.16. *If for every pair of edges $\{x_1, y_1\}, \{x_2, y_2\} \in E$ there exists an automorphism $\phi : V \to V$ such that*

$$\{\phi(x_1), \phi(y_1)\} = \{x_2, y_2\}$$

then G is called edge transitive*.*

Definition 2.1.17. *If for every pair of arcs $(x_1, y_1), (x_2, y_2) \in E$ there exists an automorphism $\phi : V \to V$ such that*

$$(\phi(x_1), \phi(y_1)) = (x_2, y_2)$$

then G is called arc transitive*.*

2.2 Abstract Algebra

The following section is a survey material needed in this thesis. For further results, please refer to [8].

Definition 2.2.1. *Let G be a set and $\cdot$ is a mapping from $G \times G$ to G. Then $(G, \cdot)$ is called a* group *if it satisfies the following four axioms.*

- *If $g_1, g_2 \in G$, then $g_1 \cdot g_2 \in G$.*
- *For all $g_1, g_2, g_3 \in G$ we have $(g_1 \cdot g_2) \cdot g_3 = g_1 \cdot (g_2 \cdot g_3)$.*
- *There exists an identity element $e \in G$ such that for all $g \in G$ we have $g \cdot e = e \cdot g = g$.*
- *For every $g \in G$, there exists an element g^{-1} (called the inverse of g) such that $g \cdot g^{-1} = g^{-1} \cdot g = e$.*

Remark 2.2.2. *If the operation is clear from context, we will write $g_1 \cdot g_2$ as $g_1 g_2$.*

Definition 2.2.3. *Let A, B, C be sets and let $f : A \to B$ and $g : B \to C$ be two functions. The* composition *$g \circ f$ is the mapping from A to C defined by $(g \circ f)(a) = g(f(a))$ for all a in A.*

Definition 2.2.4. *For a graph G, the group of all automorphisms of G under the operation of function composition is called the* automorphism group *of G, denoted* $\mathrm{Aut}(G)$*.*

For the remainder of this section, we will assume that if $(G, \cdot)$ is a group, we denote it simply by G.

Definition 2.2.5. *Let $(G, \cdot)$ and $(H, *)$ be groups. If $\phi : G \to H$ is a bijection such that $\phi(x \cdot y) = \phi(x) * \phi(y)$, for all $x, y \in G$, then ϕ is an* isomorphism*.*

Definition 2.2.6. *Let G and H be groups. The* direct product *of G and H is the group $G \times H$ whose elements are pairs (g, h) for $g \in G, h \in H$, and whose group operation is defined by*

$$(g, h)\,(g', h') = (gg', hh')$$

for all $g' \in G, h' \in H$.

Definition 2.2.7. *Let G be a group and $H \subseteq G$. If H is a group with the same operation as G, then we say that H is a* subgroup *of G.*

Definition 2.2.8. *Let G be a group. If $g_1 g_2 = g_2 g_1$, for every $g_1, g_2 \in G$, then G is called an* abelian group.

Definition 2.2.9. *Let F be a set of elements. If $(F, +)$ is an abelian group with additive identity 0, $(F \backslash \{0\}, \cdot)$ is an abelian group with multiplicative identity and multiplication distributes over addition, then $(F, +, \cdot)$ is called a* field.

2.3 Linear Algebra

The following section is a survey of material needed in this thesis. For further results, please refer to [13].

Remark 2.3.1. *We will assume throughout this thesis that all vectors are column vectors.*

Definition 2.3.2. *The* norm *of a vector $v = (v_1, \ldots, v_n) \in \mathbb{R}^n$ is*

$$||v|| = \sqrt{v_1^2 + \ldots + v_n^2}.$$

Definition 2.3.3. *Let n be a positive integer and A be an $n \times n$ matrix. If v is a non-zero vector of dimension n such that*

$$Av = \lambda v$$

for some scalar λ, then we call v an eigenvector *of A. Additionally, λ is the* eigenvalue *of A corresponding to v.*

Definition 2.3.4. *Let $G = (V, E)$ be a graph such that $V = \{x_1, \ldots, x_n\}$. The* adjacency matrix *of G is the $n \times n$ matrix A such that $A_{i,j} = 1$ if and only if $\{x_i, x_j\} \in E$, and 0 otherwise, for $1 \leq i, j \leq n$.*

Since by definition an adjacency matrix is real and symmetric, it follows that all eigenvalues of any adjacency matrix are real numbers. For the remainder of this thesis, the eigenvalues of a graph will be taken as the eigenvalues of the graph's adjacency matrix. As well, we will always write them in non-increasing order, $\lambda_1 \geq \ldots \geq \lambda_n$.

Definition 2.3.5. *Let $G = (V, E)$ be a graph such that $V = \{x_1, \ldots, x_n\}$, $E = \{e_1, \ldots, e_m\}$. The* incidence matrix *of G is the $n \times m$ matrix B such that $B_{i,j} = 1$ if and only if x_i is incident to e_j, for $1 \leq i \leq n$ and $1 \leq j \leq m$.*

Lemma 2.3.6 (Lemma 8.6.22 of [24])**.** *Let G be a k-regular graph. Then the eigenvalue of G with the largest absolute value is k.*

Lemma 2.3.7 (Lemma 8.5.1 of [9]). *Let G be a k-regular graph on n vertices with eigenvalues $k, \lambda_2, \ldots, \lambda_n$ (from Lemma 2.3.6). Then G and its complement $\overline{G}$ have the same eigenvectors, and the corresponding eigenvalues of $\overline{G}$ are $n-k-1, -1-\lambda_2, \ldots, -1-\lambda_n$, respectively.*

Definition 2.3.8. *Let u, v be vectors in $\mathbb{R}^d$. The* dot product *of u and v is given as $u \cdot v = u^T v$.*

Definition 2.3.9. *Two vectors u, v in $\mathbb{R}^d$ are* orthogonal *if $u \cdot v = 0$.*

Definition 2.3.10. *The* Gram matrix *of a set of vectors $\{v_1, \ldots, v_n\}$ is the $n \times n$ matrix A whose elements are given by $A_{ij} = v_i \cdot v_j$, for $1 \leq i, j \leq n$.*

Definition 2.3.11. *Let M be a square matrix. Then M is called an* orthogonal matrix *if and only if $MM^T = I$.*

Proposition 2.3.12. *If M is an orthogonal matrix then $M^T M = I$ and $M^T = M^{-1}$.*

Proof. Assume M is an orthogonal matrix, so that $MM^T = I$. By elementary properties of inverse matrices, we see that $M^T = M^{-1}$. Then by multiplying on the right hand side by M we have $M^T M = M^{-1} M$, hence $M^T M = I$. □

Proposition 2.3.13. *The product of two orthogonal matrices is an orthogonal matrix.*

Proof. Let M, N be orthogonal matrices of the same dimension. Then we have

$$(MN)(MN)^T = MNN^T M^T = MM^T = I.$$

□

Proposition 2.3.14. *Linear transformations defined by orthogonal matrices preserve dot products between vectors.*

Proof. Let n be a positive integer and let M be an $n \times n$ orthogonal matrix. If u, v are n-dimensional vectors, then we have

$$(Mu) \cdot (Mv) = (Mu)^T (Mv) = u^T M^T M v = u^T v = u \cdot v.$$

□

Definition 2.3.15. *Let M be an $n \times m$ matrix for positive integers n, m. If N is a matrix then the* Kronecker (or tensor) product *of M and N is defined as*

$$M \otimes N = \begin{pmatrix} M_{1,1}N & \ldots & M_{1,m}N \\ \vdots & \ddots & \vdots \\ M_{n,1}N & \ldots & M_{n,m}N \end{pmatrix}.$$

Proposition 2.3.16 ([10]). *Let M, N, P, Q be matrices and let α be a scalar. Assuming the matrices MP,NQ,M^{-1} and N^{-1} exist, the Kronecker product has the properties below.*

$$(M \otimes N)(P \otimes Q) = (MP) \otimes (NQ) \tag{2.1}$$

$$(M + N) \otimes P = M \otimes P + N \otimes P \tag{2.2}$$

$$(M \otimes N) \otimes O = M \otimes (N \otimes O) \tag{2.3}$$

$$(M \otimes N)^{-1} = M^{-1} \otimes N^{-1} \tag{2.4}$$

$$(M \otimes N)^{T} = M^{T} \otimes N^{T} \tag{2.5}$$

Proposition 2.3.17. *Let M and N be orthogonal matrices. Then $M \otimes N$ is an orthogonal matrix.*

Proof. Assume that M, N are orthogonal matrices. Then using Proposition 2.3.16,

$$(M \otimes N)(M \otimes N)^T = (M \otimes N)\left(M^T \otimes N^T\right) = \left(MM^T\right) \otimes \left(NN^T\right) = I \otimes I = I.$$

□

Proposition 2.3.18. *Let M and N be matrices such that u and v are eigenvectors of M and N, with corresponding eigenvalues λ and μ, respectively. Then $u \otimes v$ is an eigenvector of $M \otimes N$ with eigenvalue $\lambda\mu$.*

Proof. Using (2.1), and regarding λ and μ as 1×1 matrices,

$$(M \otimes N)(u \otimes v) = (Mu) \otimes (Nv) = (\lambda u) \otimes (\mu v) = \lambda\mu (u \otimes v).$$

□

2.4 Group Representation

Definition 2.4.1. *Let K be a field and n be a positive integer. The group of all invertible $n \times n$ matrices over the field K under matrix product is the* general linear group *denoted $GL(n, K)$.*

Definition 2.4.2. *Let G be a group, K be a field and n be a positive integer. Then a* group representation *of G over K is a map $\rho : G \to GL(n, K)$ such that $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$ for all $g_1, g_2 \in G$.*

Definition 2.4.3. *Let G be a group, K be a field and n be a positive integer. A group representation $\rho : G \to GL(n, K)$ of G is called* orthogonal *if the representation $\rho(g)$ of g is an orthogonal matrix for all $g \in G$.*

Proposition 2.4.4. *Let K be a field and n, m be positive integers. For groups G and H, let ρ_G and ρ_H be orthogonal group representations of G and H in $GL(n, K)$ and $GL(m, K)$, respectively. Then the map $\rho_{G\times H}$ given by*

$$\rho_{G\times H}(g, h) = \rho_G(g) \otimes \rho_H(h) \tag{2.6}$$

is an orthogonal group representation of $G \times H$ in $GL(mn, K)$, for all $g \in G$ and $h \in H$.

Proof. Let $(g_1, h_1), (g_2, h_2) \in G \times H$. By equation (2.1) we have

$$\begin{aligned}\rho_{G\times H}(g_1, h_1)\rho_{G\times H}(g_2, h_2) &= (\rho_G(g_1) \otimes \rho_H(h_1)) (\rho_G(g_2) \otimes \rho_H(h_2)) \\ &= (\rho_G(g_1)\rho_G(g_2)) \otimes (\rho_H(h_1)\rho_H(h_2)) .\end{aligned}$$

Since ρ_G and ρ_H are group representations, we know that $\rho_G(g_1)\rho_G(g_2) = \rho_G(g_1g_2)$ and $\rho_H(h_1)\rho_H(h_2) = \rho_H(h_1h_2)$. Therefore we have

$$\rho_{G\times H}(g_1, h_1)\rho_{G\times H}(g_2, h_2) = \rho_G(g_1g_2) \otimes \rho_H(h_1h_2).$$

Lastly, from (2.6) we get

$$\rho_{G\times H}(g_1, h_1)\rho_{G\times H}(g_2, h_2) = \rho_{G\times H}(g_1g_2, h_1h_2)$$

and therefore $\rho_{G\times H}$ is a group representation of $G \times H$ in $\mathrm{GL}(nm, K)$. Also, since $\rho_G(g)$ and $\rho_H(h)$ are orthogonal matrices, for all $g \in G$ and $h \in H$ we have that $\rho_{G\times H}(g, h)$ is an orthogonal matrix by Proposition 2.3.17. Therefore, $\rho_{G\times H}$ is an orthogonal group representation in $GL(nm, K)$. □

2.5 Complex Numbers

Let $i = \sqrt{-1}$. We first state a well known formula.

Theorem 2.5.1 (Euler's Formula)**.** *For any real number x, we have the following relationship.*

$$\cos x + i \sin x = e^{xi}.$$

Using Euler's formula, any $z \in \mathbb{C}$ can be written in any of the three forms below.

$$z = a + bi = |z| \cos\theta + i|z| \sin\theta = |z|e^{\theta i} \tag{2.7}$$

where $|z| = \sqrt{a^2 + b^2}$ for $a, b \in \mathbb{R}$ and $\theta \in (-\pi, \pi]$. We will switch between these forms as necessary.

Definition 2.5.2. *Let* $a, b \in \mathbb{R}$ *and* $z = a + bi$*. The* complex conjugate *of* z *is given by* $\overline{z} = a - bi$*.*

Definition 2.5.3. *For a complex number* $z = |z|e^{\theta i}$ *where* $\theta \in (-\pi, \pi]$*, the* argument (or phase) *of* z *is* θ *and is denoted* $\arg(z)$*.*

Remark 2.5.4. *For* $z = |z|\cos\theta + i|z|\sin\theta$*, its complex conjugate is*

$$\overline{z} = |z|\cos\theta - i|z|\sin\theta = |z|\cos(-\theta) + i|z|\sin(-\theta).$$

From this we can see that $\arg(z) = -\arg(\overline{z})$*, unless* $\arg(z) = \pi$*. Additionally for any* $z_1, z_2 \in \mathbb{C}$*, we have* $\arg(z_1 z_2) = \arg(z_1) + \arg(z_2)$*.*

Definition 2.5.5. *Let* $a, b \in \mathbb{R}$ *and* $z = a + bi$*. The* real part *of* z *is* $\Re(z) = a$ *and the* imaginary part *is* $\Im(z) = b$*.*

Notice that for a complex number z, we can compute the real and imaginary parts as follows

$$\Re(z) = \frac{1}{2}(z + \bar{z}),\ \Im(z) = \frac{i}{2}(\bar{z} - z). \tag{2.8}$$

Definition 2.5.6. *Let* ζ *be an element of* $\mathbb{C}$ *and* n *be a positive integer. Then* ζ *is an* n^{th} root of unity *if* $\zeta^n = 1$*. Additionally,* ζ *is a* primitive n^{th} root of unity *if* $\zeta^k \neq 1$ *for* $1 \leq k < n$ *and* $\zeta^n = 1$*. We denote* $\zeta_n = e^{\frac{2\pi i}{n}}$ *and note that* ζ_n *is a primitive* n^{th} *root of unity.*

Remark 2.5.7. *For integers* n *and* k*, we can write*

$$\zeta_n^k = e^{\frac{2\pi k i}{n}} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}.$$

Definition 2.5.8. *Let* n *be a positive integer and let* A *be an* $n \times n$ *matrix. The* Hermitian (or conjugate) transpose *of* A*, denoted* A^**, is defined in terms of its elements by*

$$(A^*)_{ij} = \overline{A_{ji}}$$

for $1 \leq i, j \leq n$*.*

Remark 2.5.9. *Notice that if* A *is a real matrix, then* $A^* = A^T$*.*

2.6 Orthonormal Representation

In 1979, László Lovász published a paper titled "On the Shannon Capacity of a Graph" [17]. He introduced his discovery of an upper bound for the Shannon capacity of a graph, an important value in the field of information theory. In the same paper, Lovász also discussed orthonormal representations of a graph. At several places in his recent book draft [16], Lovász points at the connections between the symmetries of a graph and symmetries of its orthonormal representations. Chapter 19 of [16] exposes further interesting connection between orthonormal representations and quantum physics, including also a discussion of the hidden variable theories in quantum physics.

Definition 2.6.1. *Let d be a positive integer. A d-*dimensional orthonormal representation *(henceforth referred to as an OR) of a graph $G = (V, E)$ is a mapping $f : V \to \mathbb{R}^d$ such that for each $x \in V$ we have $||f(x)|| = 1$ and if $\{x, y\} \in E$ then $f(x)$ and $f(y)$ are orthogonal vectors.*

Lovász defined the following two results relating to an OR of a graph.

Definition 2.6.2. *Let d be a positive integer and let $(u_1, \ldots, u_n) \subseteq \mathbb{R}^d$ be an OR of a graph. The* value of an OR *is given by*

$$\min_h \left[\max_{1 \leq i \leq n} \left(\frac{1}{(h^T u_i)^2} \right) \right] \tag{2.9}$$

where $h \in \mathbb{R}^d$ ranges over all unit vectors.

Definition 2.6.3. *Let G be a graph. The* Lovász theta number *of G is the minimum value over all ORs of $\overline{G}$, denoted $\vartheta(G)$.*

Lovász defines an OR of a graph to be a set of unit vectors where orthogonal vectors exactly correspond to non-adjacent vertices, [16] and [17]. Our definition of an OR is the complement definition to that of Lovász. We make this choice because the graph that is the subject of our study (which we will define in Chapter 3) is 6-regular. This implies that its complement graph is $(n-7)$-regular where n is the number of vertices in the graph. Using our definition, each vector of an OR must be orthogonal to only 6 others, rather than $n - 7$. We anticipate that some of the symmetries of the graph will be reflected in any OR, and this is our initial Ansatz as well. If we can find an infinite family of graphs who admit ORs in $\mathbb{R}^4$ which are KS sets, then we will have an infinite family of KS sets in $\mathbb{R}^4$. While searching for such a family, it is important that all of the vectors in the OR are distinct.

Definition 2.6.4. *Let G be a graph. An OR $(u_1, \ldots, u_n)$ of G is said to be a* faithful representation *of G if $u_i \neq \pm u_j$ for all $i \neq j$.*

Though most of these definitions come directly from Lovász, Definition 2.6.4 does not. This additional definition s common in quantum information literature.

Now we will review what structures are necessary within an OR so that it induces a KS set.

2.7 Kochen-Specker Set

The Kochen-Specker (KS) Theorem diverges from the Einstein's hidden variables model for quantum mechanics, Section 19.3 of [16]. We state the theorem below.

Theorem 2.7.1 (Kochen-Specker [12])**.** *In Hilbert spaces of dimension $d \geq 3$, quantum mechanics cannot be described by any non-contextual hidden variable model.*

The concept of contextuality does not exist in classical physics and states that the measurement of an observable depends on the context of other observables being jointly measured. It is thought to be a useful resource for quantum information theory, quantum processing, and hence, quantum computing. In fact, a recent paper in Nature journal emphasized the potential importance of contexuality to quantum information processing [11]. We will focus solely on the combinatorial tools that have practical applications. As we have mentioned earlier, the Kochen-Specker Theorem can be proven using a parity proof. One way to construct a parity proof of the KS Theorem is by constructing so-called KS sets.

Definition 2.7.2 ([14, 15])**.** *The pair $(\mathcal{V}, \mathcal{B})$ is a* Kochen-Specker set *(henceforth called a KS set) in $\mathbb{R}^d$ (or $\mathbb{C}^d$) if the following conditions are met.*

- *$\mathcal{V}$ is a finite set of vectors in $\mathbb{R}^d$ (or $\mathbb{C}^d$).*
- *$\mathcal{B} = (B_0, \ldots, B_{k-1})$ where k is odd, and for all $i = 0, \ldots, k-1$ we have that B_i is an orthogonal basis of $\mathbb{R}^d$ and $B_i \subset \mathcal{V}$.*
- *For each $v \in \mathcal{V}$ the number of indices i such that $v \in B_i$ is even.*

Remark 2.7.3. *The proof of Theorem 2.7.1, encoded in Definition 2.7.2, is based on a parity argument. We call any KS set as defined in Definition 2.7.2 a* parity proof *of the Kochen-Specker theorem.*

These sets of vectors are important objects in quantum mechanics and some have been implemented in experimental settings [14]. Even though KS sets exist in $\mathbb{C}^d$, we will primarily be considering KS sets over the real numbers in this thesis. Discovering KS sets in low dimensions is of interest as it may help to simplify practical experiments. The following result proves that $d = 4$ is the smallest dimension where a KS set can exist.

Proposition 2.7.4. *In a parity proof of the Kochen-Specker Theorem, the dimension d of the vectors must be even.*

Proof. Let $(\mathcal{V}, \mathcal{B})$ be a KS set in $\mathbb{R}^d$. We know that k, the number of orthogonal bases in $\mathcal{B}$, must be odd. Notice that $|B_i| = d$ for each orthogonal basis B_i in $\mathbb{R}^d$ (or $\mathbb{C}^d$). Therefore, the k bases each contain d vectors, which yields a total of kd not necessarily distinct vectors. Since we require each v to be in an even number of bases of $\mathcal{B}$, each vector v must appear an even number of times in the kd vectors mentioned above. Since k is odd, we conclude that d must be even. □

Now we discuss the result which immediately follows.

Corollary 2.7.5. *The smallest dimension d where parity proofs are possible is $d = 4$.*

Proof. By Theorem 2.7.1, the KS Theorem only holds when $d \geq 3$. From Proposition 2.7.4 we know that d must be even. Hence, $d \geq 4$. □

Many well-known KS sets occur in dimension 4 [3, 15, 21, 20]. Though there are many KS sets in $\mathbb{R}^4$, only finitely many of them are known at the time of writing this thesis. Since four is the smallest dimension which can support a KS set, it may be useful to discover more of them. Our goal was to find an infinite family of KS sets in $\mathbb{R}^4$. In [20], Pavičić presents his discovery of so called "master sets" which consist of KS sets with similar structures. Using exhaustive search algorithms and relating the structures of any discovered sets to those previously found, Pavičić was able to generate many distinct KS sets in $\mathbb{R}^4$. However, this study of master sets in four dimensional space still yielded only a finite number of KS sets. The master sets are sporadic and hence we are assured an infinite family of KS sets would not be contained in the master sets.

Chapter 3

Chordal Ring Graph

The chordal ring graph is a cycle graph with n vertices, and chords connecting vertices through the middle of the ring, defined by a parameter c. It is a popular structure often used when implementing local networks of computers. We discuss the structure of this graph in the first section. For some parameters c, the chordal ring can be highly symmetric. Since it is so symmetric, the automorphisms of the chordal ring act transitively on the vertices and edges. As we have mentioned, our goal was to find a graph whose orthonormal representations satisfy the conditions of a Kochen-Specker set in $\mathbb{R}^4$. We show that for certain parameters n and c, the line graph of the chordal ring admits an OR in $\mathbb{R}^4$, and thus is a KS set in $\mathbb{R}^4$. Lastly, we define the dihedral group and relate the automorphisms of the chordal ring to a product of two dihedral groups. Using this result, we are able to define linear transformations which act on the ORs of the chordal ring in a similar way to the automorphisms. This link is integral to our main construction of KS sets.

3.1 Structure of the Chordal Ring

Definition 3.1.1. *Let n, c be positive integers such that $1 < c < n - 1$. The* chordal ring *graph, denoted $CR_{n,c}$, is the graph with vertex set $\mathbb{Z}_n$ such that two vertices x, y are adjacent if and only if $(x - y) \pmod{n} \in \{\pm 1, \pm c\}$.*

The chordal ring graph $CR_{n,c}$ is a cycle of length n made up of ring edges and inner chord edges determined by c. The chordal ring graph can be obtained as the undirected graph corresponding to a Cayley graph [25]. The Cayley graph of a group G and a generating subset H of G is the directed graph where the vertices are the elements of G and there exists an edge $\{g, h\}$ if $gh^{-1} \in H$, for $g, h \in G$. All Cayley graphs are vertex transitive and in fact, for graphs with small order, most vertex transitive graphs are Cayley graphs as seen on page 737 of [22]. Vertex transitivity is a desired characteristic of our graph because, under this condition, the associated physical experiments become simpler and computing our OR also becomes simpler. Vertex transitive graphs are highly symmetric and we aimed to use the symmetries of the graph to construct an OR. For this reason, the chordal ring graph was very attractive to us.

Remark 3.1.2. *We will label the vertices of $CR_{n,c}$ in counter-clockwise, increasing order starting with vertex v_0 as in Figure 3.2. The edge labelled e_i has endpoints $v_i, v_{(i+1) \bmod n}$ and the edge labelled e_{i+n} has endpoints $v_i, v_{(i+c) \bmod n}$, for $0 \leq i \leq n-1$.*

Example 3.1.3. *An example of the vertex and edge labelling of $CR_{n,c}$, in Figure 3.1.*

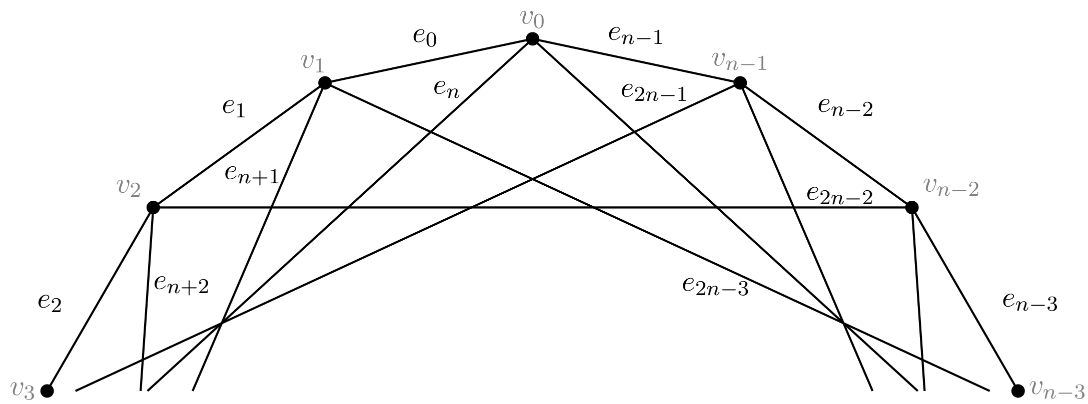

Figure 3.1: The vertex and edge labelling of $CR_{n,c}$.

Example 3.1.4. *Let $n = 15$ and $c = 4$, then $CR_{15,4}$ is given in Figure 3.2.*

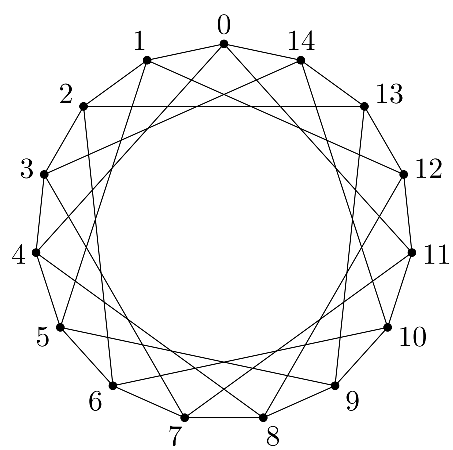

Figure 3.2: $CR_{15,4}$.

Proposition 3.1.5. *Let n, c be integers such that $1 < c < n-1$. If $c = \frac{n}{2}$, then $CR_{n,c}$ is 3-regular. Otherwise, $CR_{n,c}$ is 4-regular.*

Proof. The proof follows from the definition of $CR_{n,c}$. □

Not every n and c will yield a graph whose line graph admits an orthonormal representation in $\mathbb{R}^4$. We found that certain choices of c, for each value of n, have advantages when proving an OR is a KS set. Therefore we will introduce some additional requirements for n and c. We require that n be an odd integer that is not a prime power, and c must satisfy

$$c^2 \equiv 1 \pmod{n}. \tag{3.1}$$

We will explain the condition where n must be odd later in the thesis. For now, assume that n is odd. Notice that $c = \pm 1 \bmod n$ will satisfy equation (3.1), but we do not allow these solutions because by definition of the chordal ring, $1 < c < n-1$. Therefore, we need to find an n for which a non-trivial solution c for equation (3.1) exists. When n is an odd prime power, the only solutions to (3.1) are the trivial solutions.

Proposition 3.1.6. *Let p be an odd prime and q a positive integer. Then the equation $c^2 \equiv 1 \pmod{p^q}$ has exactly two solutions, namely $c = \pm 1 \bmod p^q$.*

Proof. Let c be an integer such that $1 \leq c < p^q$. We have

$$c^2 - 1 = kp^q$$

for some integer k. We can factor the left hand side to get

$$(c+1)(c-1) = kp^q.$$

This means that either p^q divides $c+1$ or $c-1$, or the powers of p are shared between $c+1$ and $c-1$. If $p|c+1$ and $p|c-1$, then $p|\gcd(c+1, c-1) = 2$. This contradicts the initial assumption that p is odd. So we must be in the case where p^q divides one of $c+1$ or $c-1$. Assume first that $p^q|c+1$, then we have

$$c + 1 = k_1 p^q$$

for some integer k_1. This implies that $c \equiv -1 \pmod{p^q}$. Now assume that $p^q|c-1$, then we have

$$c - 1 = k_2 p^q$$

for some integer k_2. This implies that $c \equiv 1 \pmod{p^q}$, which is also a solution to (3.1). Therefore, for any odd prime p and integer $q > 0$, the equation $c^2 \equiv 1 \pmod{p^q}$ has exactly two solutions, specifically $c = \pm 1 \bmod p^q$. □

Thus we require n to be the product of two coprime positive odd integers. For the rest of this thesis assume that $n = pq$ for coprime, odd integers $p, q > 1$. Below we show that this choice of n yields non-trivial roots to equation (3.1).

Theorem 3.1.7 (Chinese Remainder Theorem, [23])**.** *Suppose $m_1, m_2, \ldots, m_r$ are pairwise relatively prime positive integers, and suppose $a_1, \ldots, a_r$ are integers. Then the system of r congruences $x \equiv a_i \pmod{m_i}$ $(1 \le i \le r)$ has a unique solution modulo $M = m_1 \cdot m_2 \cdot \ldots \cdot m_r$, given by*

$$x = \sum_{i=1}^{r} a_i M_i y_i \bmod M,$$

where $M_i = M/m_i$ and $y_i = M_i^{-1} \bmod m_i$, for $1 \le i \le r$.

Corollary 3.1.8. *Let $n = pq$ for coprime, odd integers $p, q > 1$. Then the equation $c^2 \equiv 1 \pmod{n}$ from (3.1) has at least two non-trivial solutions.*

Proof. Let c be a solution to equation (3.1). If $c \equiv \pm 1 \pmod{n}$ then $c \equiv \pm 1 \pmod{p}$ and $c \equiv \mp 1 \pmod{q}$, taking the top or bottom sign consistently. These are the trivial solutions, so we will only consider the other possible solutions to $c^2 \equiv 1 \pmod{n}$. Let $c \equiv 1 \pmod{p}$ and $c \equiv -1 \pmod{q}$. Using Theorem 3.1.7, we know that there must exist a unique solution to $c \equiv A \pmod{n}$, for some A. Notice that by squaring both equations, we get $c^2 \equiv 1$ modulo p and modulo q. This implies $c^2 \equiv 1 \pmod{n}$. Therefore, $A \equiv 1 \pmod{n}$ and we have found a non-trivial solution to equation (3.1). The other non-trivial solution results from switching the values so that $c \equiv -1 \pmod{p}$ and $c \equiv 1 \pmod{q}$. □

Remark 3.1.9. *Notice that the non-trivial solutions to $c^2 \equiv 1 \pmod{n}$ are of the form $c \equiv \pm 1 \pmod{p}$ and $c \equiv \mp 1 \pmod{q}$. For the remainder of this thesis we will assume, without loss of generality, that the value of c is achieved from choosing $c \equiv 1 \pmod{p}$ and $c \equiv -1 \pmod{q}$. We can do this because the assignments of p, q are arbitrary. This assumption is made to simplify calculations in our construction.*

Now that we have shown our choice of n yields non-trivial solutions to equation (3.1), we can assume $1 < c < n - 1$. Using such a non-trivial solution c as a parameter in the chordal ring graph simplifies our proofs and calculations for the remainder of the thesis.

Corollary 3.1.10. *Let $n = pq$ for coprime, odd integers $p, q > 1$. Then*

$$\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q.$$

Proof. Let ϕ be the map from $\mathbb{Z}_n$ to $\mathbb{Z}_p \times \mathbb{Z}_q$ defined by

$$\phi(x) = (x \bmod p, x \bmod q)$$

for $x \in \mathbb{Z}_n$. Since p, q are coprime and $n = pq$, by Theorem 3.1.7, this map is bijective. Now let $x, y \in \mathbb{Z}_n$. Then we have

$$\begin{aligned}\phi(x +_{\mathbb{Z}_n} y) = \phi(x) +_{\mathbb{Z}_n} \phi(y)&\\ &= (x \bmod p, x \bmod q) +_{\mathbb{Z}_n} (y \bmod q, y \bmod q)\\ &= ((x \bmod p) +_{\mathbb{Z}_p} (y \bmod p), (x \bmod q) +_{\mathbb{Z}_q} (y \bmod q)) .\end{aligned}$$

Therefore, ϕ is an isomorphism and $\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q$. □

3.2 The Line Graph of the Chordal Ring

An orthonormal representation of $CR_{n,c}$ in $\mathbb{R}^4$ will not directly yield a KS set. To achieve this we must consider the line graph of the chordal ring, $L(CR_{n,c})$. Definition 2.7.2 specifies three conditions that must be met by a KS set in $\mathbb{R}^4$. They are

- $\mathcal{V}$ is a finite set of vectors in $\mathbb{R}^d$.
- $\mathcal{B} = (B_0, \ldots, B_{k-1})$ where k is odd, and for all $i = 0, \ldots, k-1$ we have that B_i is an orthogonal basis of $\mathbb{R}^d$ and $B_i \subset \mathcal{V}$.
- For each $v \in \mathcal{V}$ the number of i such that $v \in B_i$ is even.

We will now show that an OR of the line graph of $CR_{n,c}$ induces a KS set.

Theorem 3.2.1. *Let $n = pq$ for coprime, odd integers $p, q > 1$. A 4-dimensional orthonormal representation of $L(CR_{n,c})$ is a Kochen-Specker set in $\mathbb{R}^4$.*

Proof. Suppose $\mathcal{V}$ is an OR of $L(CR_{n,c})$ in $\mathbb{R}^4$. Since $CR_{n,c}$ is 4-regular by Proposition 3.1.5, each vertex x_i in $CR_{n,c}$ corresponds to a clique C_i of size 4 in $L(CR_{n,c})$. By our definition of an OR, these cliques C_i correspond to a basis B_i in $\mathbb{R}^4$. Since the number n of vertices of $CR_{n,c}$ is odd, then there are an odd number of these orthogonal bases in $\mathbb{R}^4$. So let $\mathcal{B} = (B_0, \ldots, B_{n-1})$. Lastly, because each edge of $CR_{n,c}$ is incident with exactly two vertices, x_i and x_j, in $CR_{n,c}$, each vertex of $L(CR_{n,c})$ is contained in exactly two cliques, C_i and C_j, of $L(CR_{n,c})$. Therefore each vector in an OR of $L(CR_{n,c})$ is contained in exactly two bases from $\mathcal{B}$. Since each vector is in an even number of bases in $\mathcal{B}$, we have satisfied all three of the above requirements of a KS set. □

Therefore, when $n = pq$ for coprime, odd integers $p, q > 1$ and c satisfying $c^2 \equiv 1 \pmod n$, any 4-dimensional OR of $L(CR_{n,c})$ satisfies the conditions necessary to be a KS set in $\mathbb{R}^4$. Implicitly, the remaining challenge is then to construct an OR of $L(CR_{n,c})$ in $\mathbb{R}^4$.

3.3 Automorphism Group of the Chordal Ring and Its Line Graph

As we have said above, the chordal ring graph is a widely used structure in networking and graph theory because of its symmetries and connectivity. Let $n = pq$ for $p, q > 1$ coprime, odd integers and c such that $c^2 \equiv 1 \pmod{n}$ and $1 < c < n - 1$. We will soon see how this choice of c simplifies calculations. Recall that we assumed $c \equiv 1 \pmod{p}$ and $c \equiv -1 \pmod{q}$. To illustrate how symmetric $CR_{n,c}$ is, we first find some automorphisms of the chordal ring. Recall that by Definition 3.1.1, the vertex set of $CR_{n,c}$ is $\mathbb{Z}_n$.

Theorem 3.3.1. *Let $n = pq$ for coprime, odd integers $p, q > 1$ and let c be an integer such that $c^2 \equiv 1 \pmod{n}$. Let $s, t \in \mathbb{Z}_2$, $d \in \mathbb{Z}_n$ and ϕ be the map from $V(CR_{n,c})$ to itself, defined by*

$$\phi(x) = (-1)^s c^t x + d \bmod n. \tag{3.2}$$

Then ϕ is an automorphism of $CR_{n,c}$.

Proof. Notice that by definition, c is coprime to n and hence so is $(-1)^s c^t$. Therefore, ϕ defined above is a bijection. If we show that ϕ preserves adjacency between vertices of $CR_{n,c}$, then ϕ is a homomorphism and therefore an automorphism. Let x, y be adjacent vertices in $CR_{n,c}$. Hence we know $(x - y) \in \{\pm 1, \pm c\}$. By applying ϕ to both vertices, we get

$$\phi(x) = (-1)^s c^t x + d \bmod n$$
$$\phi(y) = (-1)^s c^t y + d \bmod n.$$

To show ϕ preserves adjacency, we need to show that $\phi(x) - \phi(y) \in \{\pm 1, \pm c\} \pmod{n}$. We have

$$\phi(x) - \phi(y) = (-1)^s c^t (x - y) \bmod n.$$

Since $x - y \in \{\pm 1, \pm c\}$ and $c^2 \equiv 1 \pmod{n}$, we have that

$$(-1)^s c^t (x - y) \in \{\pm 1, \pm c\} \pmod{n}.$$

Therefore ϕ is an automorphism of $CR_{n,c}$. □

Now let us examine further the map ϕ defined above. If $s, t = 0$, then we get the map $\phi(x) = x + d \bmod n$, which yields rotational symmetry as d varies over $\mathbb{Z}_n$. If $s = 1$ and $d, t = 0$, then we get $\phi(x) = -x \bmod n$, which yields reflectional symmetry in the graph. Lastly, if $t = 1$ and $d, s = 0$, the map becomes $\phi(x) = cx \bmod n$. This form of ϕ results in a switching of ring edges and chords. We will look at some example images under these maps.

Example 3.3.2. *Let $d, x \in \mathbb{Z}_n$ and $s = t = 0$. Then we have $\phi(x) = x + d \bmod n$ which will represent a cyclic shift by d. If $d = 3$, the image of $CR_{15,4}$ is the resulting graph in Figure 3.3.*

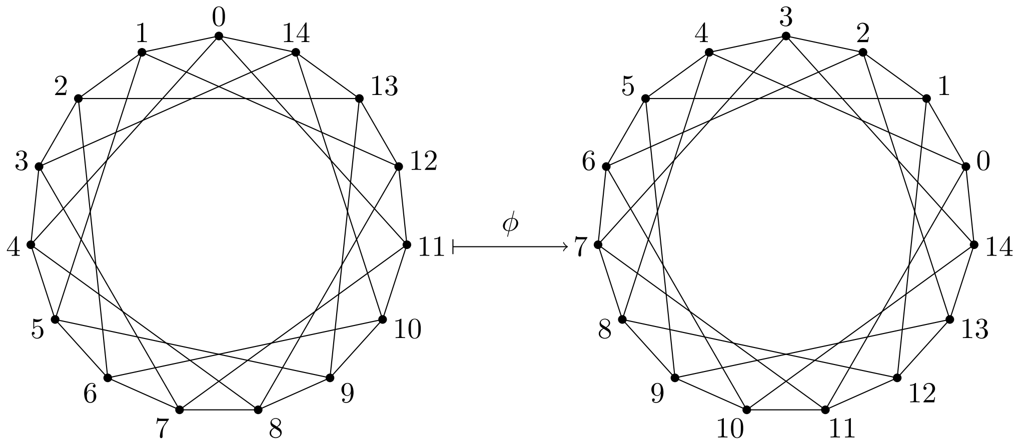

Figure 3.3: The image of $CR_{15,4}$ under ϕ with $s, t = 0$ and $d = 3$.

Example 3.3.3. *Let $x \in \mathbb{Z}_n$, $s = 1$ and $t = d = 0$. Then we have $\phi(x) = -x \bmod n$. In Figure 3.4 we see the image of $CR_{15,4}$ under ϕ, which reflects the vertices about the vertical line passing through the vertex labelled 0.*

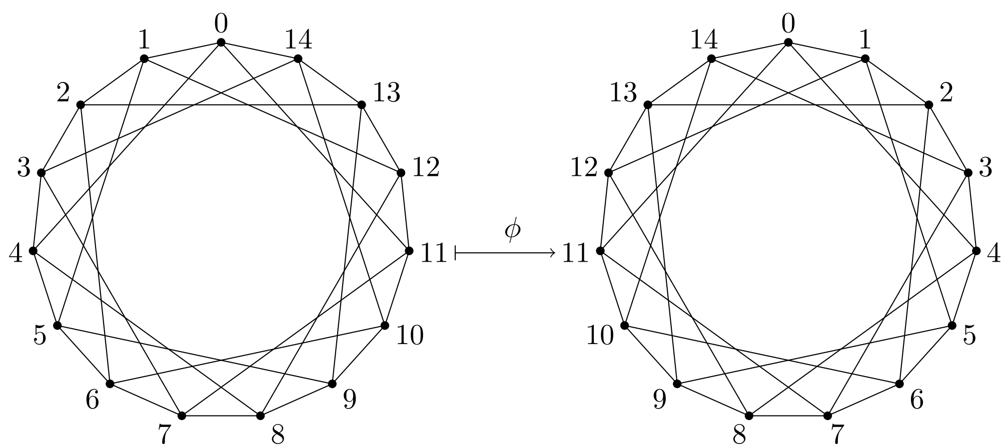

Figure 3.4: The image of $CR_{15,4}$ under ϕ with $d, t = 0$ and $s = 1$.

Example 3.3.4. *Let $x \in \mathbb{Z}_n$, $d = s = 0$ and $t = 1$. Then $\phi(x) = cx \bmod n$ sends each ring edge to a distinct chord edge and vice versa. The image of $CR_{15,4}$ under ϕ is the graph in Figure 3.5.*

Now that we have defined multiple automorphisms of $CR_{n,c}$, we state the following result.

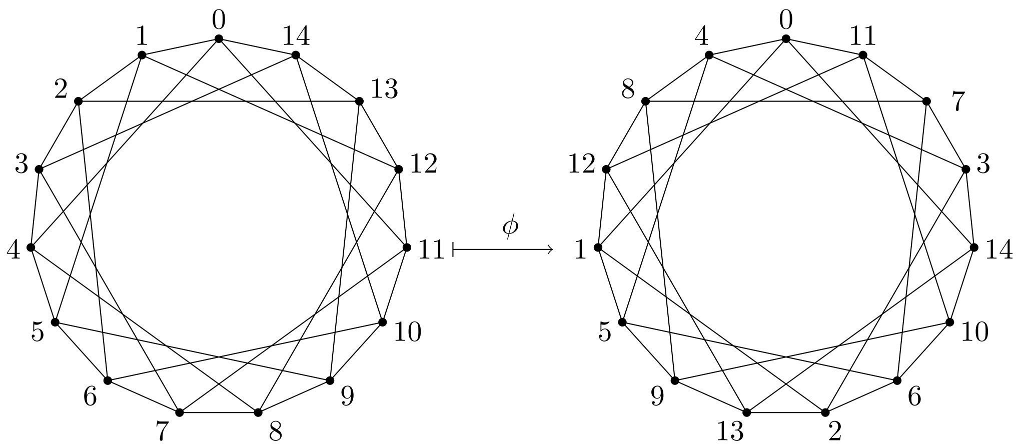

Figure 3.5: The image of $CR_{15,4}$ under ϕ with $d, s = 0$ and $t = 1$.

Theorem 3.3.5. *Let $n = pq$ for coprime, odd integers $p, q > 1$ and let c be such that $c^2 \equiv 1 \pmod{n}$. Let*

$$\mathcal{A} = \{\phi : \phi(x) = (-1)^s c^t x + d \pmod{n}\} \tag{3.3}$$

be the set of automorphisms such that $s, t \in \mathbb{Z}_2, d \in \mathbb{Z}_n$. Then $\mathcal{A}$ is a subgroup of $\text{Aut}(CR_{n,c})$.

Proof. By Theorem 3.3 in [8], since $\mathcal{A}$ is a finite subset of the automorphism group of $CR_{n,c}$, we need only show that $\mathcal{A}$ is closed under the group operation, which in our case is function composition given in Definition 2.2.3. Now let $\phi_1, \phi_2 \in \mathcal{A}$ with associated parameters s_1, t_1, d_1 and s_2, t_2, d_2. For $x \in V$ we have

$$\phi_1(\phi_2(x)) = (-1)^{s_1+s_2} c^{t_1+t_2} x + d_1 + (-1)^{s_1} c^{t_1} d_2 \pmod{n}. \tag{3.4}$$

The mapping in (3.4) is in $\mathcal{A}$ because $d_1 + (-1)^{s_1} c^{t_1} d_2 \in \mathbb{Z}_n$. □

We will not attempt to prove that $\mathcal{A} = \text{Aut}(CR_{n,c})$, although numerical calculations suggest that this is the case. This will be further explained in Theorem 3.5.11 and in the remarks immediately preceding it.

Corollary 3.3.6. *Let $n = pq$ for coprime, odd integers $p, q > 1$ and let c be an integer such that $c^2 \equiv 1 \pmod{n}$. Then $|\text{Aut}(CR_{n,c})| \geq 4n$.*

Proof. By Theorem 3.3.5, $\mathcal{A} \subseteq \text{Aut}(CR_{n,c})$. The rest of the proof follows from the number of choices we have for s, t and d (since $s, t \in \mathbb{Z}_2$ and $d \in \mathbb{Z}_n$). □

Remember that we are utilizing the symmetries of $L(CR_{n,c})$ and not $CR_{n,c}$. So our actual goal is to study the automorphism group of the line graph. To achieve this, we consider the automorphisms of $CR_{n,c}$ induced on the line graph. In 1932, Whitney proved that all edge permutations on finite, connected graphs are induced by graph automorphisms, with four exceptions.

Theorem 3.3.7 ([25]). *Let G and G' be connected graphs and σ be an injective function from $E(G)$ to $E(G')$. Then σ is induced by an isomorphism of G onto G' if and only if σ preserves stars, where a star is any set of edges incident with a single vertex of G, with four exceptions.*

Let $G' = G = CR_{n,c}$, which is a connected graph. The four pairs of graphs which do not follow the result are stated in [25], of which only three are such that $G = G'$. These three graphs are K_4, K_3 with a single pendant vertex and the diamond graph (a K_4 with one edge removed, seen in [7]). It is easy to see that $CR_{n,c}$ is not isomorphic to any of these three graphs, for all n and c defined above. We choose the vertex isomorphism to be ϕ, as in (3.2), which we proved is an automorphism in Theorem 3.3.1. Since by definition, automorphisms preserve adjacency for every pair of vertices, ϕ must preserve stars. So ϕ induces an isomorphism from the edges of $CR_{n,c}$ to itself. Therefore, ϕ actually induces an automorphism on the edges.

Corollary 3.3.8. *Let $n = pq$ for coprime, odd integers $p, q > 1$. Then* $\text{Aut}(CR_{n,c}) = \text{Aut}(L(CR_{n,c}))$.

Proof. This follows directly from Theorem 3.3.7. □

Naturally, we assume the automorphism induced on the edges of $CR_{n,c}$ by some vertex automorphism $\phi \in \mathcal{A}$ is the map $\psi : E(CR_{n,c}) \to E(CR_{n,c})$ defined by

$$\psi(\{x_1, x_2\}) = \{\phi(x_1), \phi(x_2)\} \tag{3.5}$$

where $\{x_1, x_2\}$ is any edge in $CR_{n,c}$. This implies that the subgroup $\mathcal{A}$ of the automorphism group of $CR_{n,c}$ induces a subset of the automorphism group of $L(CR_{n,c})$. In fact, it induces a subgroup of $\text{Aut}(L(CR_{n,c}))$.

Theorem 3.3.9. *Let $n = pq$ for coprime, odd integers $p, q > 1$ and let c satisfy $c^2 \equiv 1 \pmod{n}$. Let $\mathcal{A}$ be the subgroup of the automorphism group of $CR_{n,c}$ defined in Theorem 3.3.5. Let $\mathcal{A}_L$ be the set of automorphisms of the form in (3.5) which act on $L(CR_{n,c})$. Then $\mathcal{A}_L$ is a subgroup of the automorphism group of $L(CR_{n,c})$.*

Proof. Again, we need to show that $\mathcal{A}_L$ is closed under function composition. Let $\psi_1, \psi_2 \in \mathcal{A}_L$ and $\{x_1, x_2\}$ be an edge in $CR_{n,c}$. Then we have

$$\psi_1(\psi_2(\{x_1, x_2\})) = \{\phi_1(\phi_2(x_1)), \phi_1(\phi_2(x_2))\}.$$

Since $\phi_1, \phi_2 \in \mathcal{A}$, we conclude that $\mathcal{A}_L$ is a subgroup of $\text{Aut}(L(CR_{n,c}))$. □

Now that we have defined groups of automorphisms of $CR_{n,c}$ and $L(CR_{n,c})$, we can begin studying the symmetries that follow.

3.4 Vertex and Arc Transitivity of the Chordal Ring

As we have mentioned earlier, a vertex transitive graph containes structures that benefit quantum information theory, [1, 2, 4]. Our initial Ansatz was that some of the symmetries of a graph are mirrored in an orthonormal representation. Therefore, having a vertex transitive graph is an attractive characteristic for this thesis and the quantum theory applications. We now consider the transitivity of the chordal ring and its line graph induced by $\mathcal{A}$.

Theorem 3.4.1. *Let $n = pq$ for coprime, odd integers $p, q > 1$. If c such that $c^2 \equiv 1 \pmod{n}$, then $CR_{n,c}$ is vertex transitive.*

Proof. The proof follows directly from the cyclic symmetry of $CR_{n,c}$. Let x, y be two arbitrary vertices of $CR_{n,c}$. It is sufficient to show there exists an automorphism ϕ such that $\phi(x) = y$ for every pair of vertices x, y. If we choose ϕ as above with $s, t = 0$ and d to be the difference of the two vertices, $d \equiv y - x \pmod{n}$, then we have

$$\begin{aligned} \phi(x) &= x + (y - x) \bmod n \\ &= y \bmod n \end{aligned}$$

Thus $CR_{n,c}$ is vertex transitive. □

Even though $CR_{n,c}$ is undirected, we can replace each edge $\{x, y\}$ of the graph with two oppositely directed arcs, (x, y) and (y, x), for $x, y \in V$. Having the ability to send an arc to all other arcs in a graph is a much stronger result than being able to do the same with the edges.

Theorem 3.4.2. *Let $n = pq$ for coprime, odd integers $p, q > 1$. If c such that $c^2 \equiv 1 \pmod{n}$, then $CR_{n,c}$ is arc transitive.*

Proof. Let ϕ_1 and ϕ_2 be automorphisms in $\mathcal{A}$ such that

$$\begin{aligned} \phi_1(x) &= k_1 x + d_1 \pmod{n} \\ \phi_2(x) &= k_2 x + d_2 \pmod{n} \end{aligned}$$

for $k_1, k_2, d_1, d_2 \in \mathbb{Z}_n$. Consider the arc $(0, 1)$. Notice that

$$\begin{aligned} \phi_1(0) = \phi_2(0) &\implies d_1 = d_2 \\ \phi_1(1) = \phi_2(1) &\implies k_1 = k_2 \end{aligned}$$

and $\phi_1 = \phi_2$. Therefore, each element of $\mathcal{A}$ gives a distinct image of $(0,1)$. Now notice that there are $2n$ edges in $CR_{n,c}$, which can be replaced with $4n$ arcs. As well there are $4n$ automorphisms in the group $\mathcal{A}$. Then for any arc (x,y), there exists a map $\phi \in \mathcal{A}$ such that $\phi : (0,1) \to (x,y)$.

We want to show that there exists an automorphism ϕ that sends (x_1, y_1) to (x_2, y_2), for any two arcs $(x_1, y_1), (x_2, y_2)$ in $CR_{n,c}$. Since we showed that there exists a map which sends $(0,1)$ to an arbitrary arc of a graph, we can assume there exist $\phi_1, \phi_2 \in \mathcal{A}$ such that

$$(\phi_1(0), \phi_1(1)) = (x_1, y_1)$$
$$(\phi_2(0), \phi_2(1)) = (x_2, y_2).$$

Therefore, if we let $\phi = \phi_2 \circ \phi_1^{-1}$ then

$$\phi : (x_1, y_1) \to (\phi(x_1), \phi(y_1)) = (\phi_2 \circ \phi_1^{-1}(x_1), \phi_2 \circ \phi_1^{-1}(y_1)) = (x_2, y_2).$$

So we have found a map $\phi \in \mathcal{A}$ which sends any arc (x_1, y_1) to any arc (x_2, y_2) in $CR_{n,c}$. □

Corollary 3.4.3. *Let $n = pq$ for coprime, odd integers $p, q > 1$. If c is an integer such that $c^2 \equiv 1 \pmod{n}$, then $CR_{n,c}$ is edge transitive.*

Proof. This follows directly from Theorem 3.4.2. □

Theorem 3.4.4. *Let $n = pq$ for coprime, odd integers $p, q > 1$. If c is an integer such that $c^2 \equiv 1 \pmod{n}$, then $L(CR_{n,c})$ is vertex transitive.*

Proof. The vertex transitivity of $L(CR_{n,c})$ aligns with the edge transitivity of $CR_{n,c}$ from Corollary 3.4.3 and Theorem 3.3.7. □

Now that we have studied the symmetries of the graphs, it would be useful to be able to translate them to symmetries in the ORs, as has been our goal. The following section discusses our method to express the symmetries of the graph in an OR.

3.5 The Dihedral Group

In this section we will define the dihedral group. We will use this structure's natural symmetry to relate the automorphisms of $CR_{n,c}$ to linear transformations which act on ORs of $L(CR_{n,c})$.

Definition 3.5.1. *The* dihedral group *is the group denoted D_n with identity e and generators $\mathcal{R}$ and $\mathcal{S}$ subject to $\mathcal{R}^n = \mathcal{S}^2 = e$ and $\mathcal{SRS} = \mathcal{R}^{-1}$. To emphasize the value of n, we write the generators of D_n as $\mathcal{R}_n, \mathcal{S}_n$.*

Remark 3.5.2. *Notice that $\mathcal{SRS} = \mathcal{R}^{-1}$ is equivalent to $\mathcal{SR} = \mathcal{R}^{-1}\mathcal{S}$.*

Each element of D_n can be written as product of the generators $\mathcal{R}_n$ and $\mathcal{S}_n$, as $\mathcal{R}_n^\ell \mathcal{S}_n^j$. We say that an element of D_n is in canonical form when $0 \leq \ell < n$ and $j \in \{0, 1\}$.

Proposition 3.5.3. *Let D_n be the dihedral group. Then $|D_n| = 2n$.*

Proof. This follows from the fact that there are $2n$ canonically formed elements in D_n, all of which are distinct. □

Proposition 3.5.4. *The product of two elements of D_n, in canonical form, is given by*

$$\left(\mathcal{R}^i \mathcal{S}^j\right)\left(\mathcal{R}^s \mathcal{S}^t\right) = \mathcal{R}^{i+(-1)^j s} \mathcal{S}^{j+t}.$$

Proof. Let i, j, s, t be integers such that $0 \leq i, s < n$ and $0 \leq j, t \leq 1$. If $j = 0$, then we get

$$\left(\mathcal{R}^i \mathcal{S}^j\right)\left(\mathcal{R}^s \mathcal{S}^t\right) = \mathcal{R}^{i+s} \mathcal{S}^t.$$

If $j = 1$, then, using the equivalence from Remark 3.5.2, we get

$$\left(\mathcal{R}^i \mathcal{S}^j\right)\left(\mathcal{R}^s \mathcal{S}^t\right) = \mathcal{R}^{i-s} \mathcal{S}^{1+t}.$$

Since $j = 0, 1$, we can combine both cases to get

$$\left(\mathcal{R}^i \mathcal{S}^j\right)\left(\mathcal{R}^s \mathcal{S}^t\right) = \mathcal{R}^{i+(-1)^j s} \mathcal{S}^{j+t}.$$

□

It is well known that the group of symmetries of the regular n-gon in $\mathbb{R}^2$, centred at the origin with one of its nodes on the horizontal axis, is isomorphic to the dihedral group D_n. Here, $\mathcal{R}$ would be a rotation by $\frac{2\pi}{n}$ and $\mathcal{S}$ a reflection about the horizontal axis. It can be easily checked that $\rho : D_n \to GL(2, \mathbb{R})$ is a group representation where the images of the generators of D_n are

$$\rho(\mathcal{R}_n) = R_{n,k} = \frac{1}{2}\begin{pmatrix} \zeta_n^k + \zeta_n^{-k} & -i(\zeta_n^k - \zeta_n^{-k}) \\ -i(\zeta_n^k - \zeta_n^{-k}) & \zeta_n^k + \zeta_n^{-k} \end{pmatrix} = \begin{pmatrix} \cos\frac{2\pi k}{n} & -\sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{pmatrix} \tag{3.6}$$

and

$$\rho(\mathcal{S}_n) = S_n = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{3.7}$$

Recall $\zeta_n = e^{2\pi i/n}$ denotes a primitive n-th root of unity in $\mathbb{C}$ and k is a fixed integer.

Remark 3.5.5. *In general, by definition, ρ is a homomorphism for any fixed k. When $\gcd(n, k) \neq 1$, there will be fewer images of the elements of D_n under ρ. Since in the rest of the thesis we are interested in bijective representations, we will assume that n and k are coprime.*

This is important for the main result later in this chapter. Since all elements of the dihedral group can be written as a product of its generators and the group representation ρ is a homomorphism, all elements of the group can be written as a product of the matrix representations of the generators. Explicitly we can represent elements $\mathcal{R}^\ell \mathcal{S}^j \in D_n$ as

$$\rho(\mathcal{R}_n^\ell \mathcal{S}_n^j) = R_{n,k}^\ell S_n^j \tag{3.8}$$

for integers ℓ, j. We will now discuss some results regarding matrices $R_{n,k}, S_n$.

Proposition 3.5.6. *For integers n, k, the matrices*

$$R_{n,k} = \begin{pmatrix} \cos\frac{2\pi k}{n} & -\sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{pmatrix}, \;\; S_n = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

are orthogonal matrices.

Proof. Notice that $S_n^T = S_n$. Then we have $S_n S_n^T = S_n^2 = I$ and S_n is orthogonal. For $R_{n,k}$ we have

$$\begin{aligned} R_{n,k}R_{n,k}^T &= \begin{pmatrix} \cos\frac{2\pi k}{n} & -\sin\frac{2\pi k}{n} \\ \sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{pmatrix} \begin{pmatrix} \cos\frac{2\pi k}{n} & \sin\frac{2\pi k}{n} \\ -\sin\frac{2\pi k}{n} & \cos\frac{2\pi k}{n} \end{pmatrix} \\ &= \begin{pmatrix} \cos^2\frac{2\pi k}{n} + \sin^2\frac{2\pi k}{n} & 0 \\ 0 & \cos^2\frac{2\pi k}{n} + \sin^2\frac{2\pi k}{n} \end{pmatrix} = I. \end{aligned}$$

□

Remark 3.5.7. *Since $R_{n,k}$ is orthogonal, $R_{n,k}^T = R_{n,k}^{-1}$.*

Theorem 3.5.8. *Let ρ be the group representation of D_n defined by*

$$\rho(\mathcal{R}_n^\ell \mathcal{S}_n^j) = R_{n,k}^\ell S_n^j$$

where $\mathcal{R}_n^\ell \mathcal{S}_n^j \in D_n$. Then ρ is an orthogonal group representation.

Proof. From Proposition 3.5.6, we know that the matrices in equations (3.6) and (3.7) are orthogonal matrices. Also from Proposition 2.3.13, we know any product of $R_{n,k}$ and S_n is an orthogonal matrix. Then by Definition 2.4.3, ρ is an orthogonal group representation. □

Proposition 3.5.9. *$R_{n,k}$ has eigenvalues ζ_n^k, ζ_n^{-k} with corresponding eigenvectors $\begin{pmatrix} 1 \\ -i \end{pmatrix}$ and $\begin{pmatrix} 1 \\ i \end{pmatrix}$, respectively.*

Proof. The proof is shown directly.

$$\begin{aligned}
R_{n,k}\begin{pmatrix} 1 \\ -i \end{pmatrix} &= \frac{1}{2}\begin{pmatrix} \zeta_n^k + \zeta_n^{-k} & i(\zeta_n^k - \zeta_n^{-k}) \\ -i(\zeta_n^k - \zeta_n^{-k}) & \zeta_n^k + \zeta_n^{-k} \end{pmatrix}\begin{pmatrix} 1 \\ -i \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} \zeta_n^k + \zeta_n^{-k} + \zeta_n^k - \zeta_n^{-k} \\ -i(\zeta_n^k - \zeta_n^{-k}) - i(\zeta_n^k + \zeta_n^{-k}) \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} 2\zeta_n^k \\ -2i\zeta_n^k \end{pmatrix} = \zeta_n^k \begin{pmatrix} 1 \\ -i \end{pmatrix}
\end{aligned}$$

$$\begin{aligned}
R_{n,k}\begin{pmatrix} 1 \\ i \end{pmatrix} &= \frac{1}{2}\begin{pmatrix} \zeta_n^k + \zeta_n^{-k} & i(\zeta_n^k - \zeta_n^{-k}) \\ -i(\zeta_n^k - \zeta_n^{-k}) & \zeta_n^k + \zeta_n^{-k} \end{pmatrix}\begin{pmatrix} 1 \\ i \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} \zeta_n^k + \zeta_n^{-k} - \zeta_n^k + \zeta_n^{-k} \\ -i(\zeta_n^k - \zeta_n^{-k}) + i(\zeta_n^k + \zeta_n^{-k}) \end{pmatrix} \\
&= \frac{1}{2}\begin{pmatrix} 2\zeta_n^{-k} \\ 2i\zeta_n^{-k} \end{pmatrix} = \zeta_n^{-k} \begin{pmatrix} 1 \\ i \end{pmatrix}
\end{aligned}$$

□

Corollary 3.5.10. *For any $\ell \in \mathbb{Z}$, the eigenvalues of $R_{n,k}^{\ell}$ are $\zeta_n^{k\ell}$, $\zeta_n^{-k\ell}$ and corresponding eigenvectors are $\begin{pmatrix} 1 \\ -i \end{pmatrix}$ and $\begin{pmatrix} 1 \\ i \end{pmatrix}$.*

Proof. From Proposition 3.5.9 we know that

$$R_{n,k}\begin{pmatrix} 1 \\ \pm i \end{pmatrix} = \zeta_n^{\mp k}\begin{pmatrix} 1 \\ \pm i \end{pmatrix}.$$

By induction, we reach the result

$$R_{n,k}^{\ell}\begin{pmatrix} 1 \\ \pm i \end{pmatrix} = \zeta_n^{\mp k\ell}\begin{pmatrix} 1 \\ \pm i \end{pmatrix}.$$

□

Using the computational algebra system Magma [18], we computed the automorphism groups of $CR_{n,c}$ for small admissible values $(15, 21, 33, 35, \ldots)$ of n and $c^2 \equiv 1 \pmod{n}$. In all cases, we observe that the automorphism group is isomorphic to $D_p \times D_q$ where $n = pq$ for coprime $p, q > 1$. Theorem 3.5.11 is the basis of our conjecture, mentioned earlier, that the group $\mathcal{A}$ from Theorem 3.3.5 is the full automorphism group of $CR_{n,c}$.

Theorem 3.5.11. *Let $n = pq$ where $p, q > 1$ are coprime, odd integers and c an integer such that $c^2 \equiv 1 \pmod{n}$. Let $\mathcal{A}$ be the subgroup of the automorphism group of $CR_{n,c}$, from*

Theorem 3.3.5, and let D_p and D_q be dihedral groups of order $2p$ and $2q$ respectively. Then

$$\mathcal{A} \cong D_p \times D_q. \tag{3.9}$$

Proof. Recall that for any $\phi \in \mathcal{A}$, we have

$$\phi : x \mapsto (-1)^s c^t x + d \bmod n \tag{3.10}$$

where $s, t \in \mathbb{Z}_2$ and $x, d \in \mathbb{Z}_n$. Let $\Phi : \mathcal{A} \to D_p \times D_q$ be the map given by

$$\Phi(\phi) = \left(\mathcal{R}_p^{(-1)^s d}\mathcal{S}_p^s, \mathcal{R}_q^{(-1)^{s+t}d}\mathcal{S}_q^{s+t}\right). \tag{3.11}$$

We aim to show that Φ is an isomorphism. To show this, we need to prove that $\Phi(\phi_1)\Phi(\phi_2) = \Phi(\phi_2 \circ \phi_1)$, for any $\phi_1, \phi_2 \in \mathcal{A}$, and that Φ is a bijection.

First, we compute the product of $\Phi(\phi_1)$ and $\Phi(\phi_2)$.

$$\Phi(\phi_1)\Phi(\phi_2) = \left(\mathcal{R}_p^{(-1)^{s_1}d_1}\mathcal{S}_p^{s_1}, \mathcal{R}_q^{(-1)^{s_1+t_1}d_1}\mathcal{S}_q^{s_1+t_1}\right)\left(\mathcal{R}_p^{(-1)^{s_2}d_2}\mathcal{S}_p^{s_2}, \mathcal{R}_q^{(-1)^{s_2+t_2}d_2}\mathcal{S}_q^{s_2+t_2}\right)$$

Using Proposition 3.5.4, we have

$$\begin{aligned}
\Phi(\phi_1)\Phi(\phi_2) &= \left(\left(\mathcal{R}_p^{(-1)^{s_1}d_1}\mathcal{S}_p^{s_1}\right)\left(\mathcal{R}_p^{(-1)^{s_2}d_2}\mathcal{S}_p^{s_2}\right), \left(\mathcal{R}_q^{(-1)^{s_1+t_1}d_1}\mathcal{S}_p^{s_1+t_1}\right)\left(\mathcal{R}_q^{(-1)^{s_2+t_2}d_2}\mathcal{S}_q^{s_2+t_2}\right)\right) \\
&= \left(\mathcal{R}_p^{(-1)^{s_1}d_1+(-1)^{s_1}(-1)^{s_2}d_2}\mathcal{S}_p^{s_1+s_2}, \mathcal{R}_q^{(-1)^{s_1+t_1}d_1+(-1)^{s_1+t_1}(-1)^{s_2+t_2}d_2}\mathcal{S}_q^{s_1+s_2+t_1+t_2}\right) \\
&= \left(\mathcal{R}_p^{(-1)^{s_1}(d_1+(-1)^{s_2}d_2)}\mathcal{S}_p^{s_1+s_2}, \mathcal{R}_q^{(-1)^{s_1+t_1}(d_1+(-1)^{s_2+t_2}d_2)}\mathcal{S}_q^{s_1+s_2+t_1+t_2}\right).
\end{aligned} \tag{3.12}$$

Next, we compute the composition of the two maps using Definition 2.2.3.

$$(\phi_2 \circ \phi_1)(x) = (-1)^{s_1+s_2}c^{t_1+t_2}x + (-1)^{s_2}c^{t_2}d_1 + d_2 \pmod n$$

Then we apply the map Φ to the composition of the two automorphisms.

$$\begin{aligned}
\Phi(\phi_2 \circ \phi_1) &= \left(\mathcal{R}_p^{(-1)^{s_1+s_2}[(-1)^{s_1}c^{t_1}d_2+d_1]}\mathcal{S}_p^{s_1+s_2}, \mathcal{R}_q^{(-1)^{s_1+s_2+t_1+t_2}[(-1)^{s_1}c^{t_1}d_2+d_1]}\mathcal{S}_q^{s_1+s_2+t_1+t_2}\right) \\
&= \left(\mathcal{R}_p^{(-1)^{s_2}c^{t_1}d_2+(-1)^{s_1+s_2}d_1}\mathcal{S}_p^{s_1+s_2}, \mathcal{R}_q^{(-1)^{s_2+t_1+t_2}c^{t_1}d_2+(-1)^{s_1+s_2+t_1+t_2}d_1}\mathcal{S}_q^{s_1+s_2+t_1+t_2}\right)
\end{aligned} \tag{3.13}$$

Recall that we assumed $c \equiv 1 \pmod p$ and $c \equiv -1 \pmod q$ in Remark 3.1.9. Since $c \equiv 1 \pmod p$, $c^u \equiv 1^u \pmod p$ for any value of u. From the definition of $\mathcal{R}_p$, this gives us $\mathcal{R}_p^{c^u} = \mathcal{R}_p$. Similarly, $c \equiv -1 \pmod q$ implies $\mathcal{R}_q^{c^u} = \mathcal{R}_q^{(-1)^u}$. Therefore we can further simplify (3.13) to

$$\begin{aligned}
\Phi(\phi_2 \circ \phi_1) &= \left(\mathcal{R}_p^{(-1)^{s_1}d_1+(-1)^{s_1+s_2}d_2}\mathcal{S}_p^{s_1+s_2}, \mathcal{R}_q^{(-1)^{t_2}(-1)^{s_1+t_1+t_2}d_1+(-1)^{s_1+s_2+t_1+t_2}d_2}\mathcal{S}_q^{s_1+s_2+t_1+t_2}\right) \\
&= \left(\mathcal{R}_p^{(-1)^{s_1}(d_1+(-1)^{s_2}d_2)}\mathcal{S}_p^{s_1+s_2}, \mathcal{R}_q^{(-1)^{s_1+t_1}(d_1+(-1)^{s_2+t_2}d_2)}\mathcal{S}_q^{s_1+s_2+t_1+t_2}\right).
\end{aligned} \tag{3.14}$$

By observation, we can see (3.12) is equal to (3.14) and we have shown that

$$\Phi(\phi_2 \circ \phi_1) = \Phi(\phi_1)\Phi(\phi_2).$$

Now we show Φ is injective. Let ϕ_1, ϕ_2 be as above. Assume that the images of ϕ_1 and ϕ_2 are equal under Φ.

$$\Phi(\phi_1) = \Phi(\phi_2)$$
$$\left(\mathcal{R}_p^{(-1)^{s_1} d_1} \mathcal{S}_p^{s_1}, \mathcal{R}_q^{(-1)^{s_1+t_1} d_1} \mathcal{S}_q^{s_1+t_1}\right) = \left(\mathcal{R}_p^{(-1)^{s_2} d_2} \mathcal{S}_p^{s_2}, \mathcal{R}_q^{(-1)^{s_2+t_2} d_2} \mathcal{S}_q^{s_2+t_2}\right).$$

Then, considering the exponents on $\mathcal{S}_p$, we conclude that $s_1 = s_2$. It then follows that $d_1 = d_2$ and $t_1 = t_2$. Thus, Φ is injective. Since $|\mathcal{A}| = |D_p \times D_q|$, we conclude that Φ is a bijection, and therefore an isomorphism and $\mathcal{A} \cong D_p \times D_q$. □

Now that we have related the automorphisms of $CR_{n,c}$ to the dihedral groups, remember that we defined a group representation ρ of the dihedral group, given in (3.6) and (3.7) and showed it is an orthogonal group representation in $\mathrm{GL}(2, \mathbb{R})$ in Theorem 3.5.8. We can conclude that there exists an orthogonal group representation of $D_p \times D_q$ in $\mathrm{GL}(4, \mathbb{R})$ by Proposition 2.4.4. A representation of an element of $D_p \times D_q$ in $\mathrm{GL}(4, \mathbb{R})$ is given by the product of the representation of an element in D_p and the representation of an element in D_q. If $(\mathcal{R}_p^{\ell_p} \mathcal{S}_p^{j_p}, \mathcal{R}_q^{\ell_q} \mathcal{S}_q^{j_q}) \in D_p \times D_q$, then by Proposition 2.4.4 and equation (3.8), a representation of this element is given by

$$\rho_{D_p \times D_q}\left(\mathcal{R}_p^{\ell_p} \mathcal{S}_p^{j_p}, \mathcal{R}_q^{\ell_q} \mathcal{S}_q^{j_q}\right) = R_{p,k_p}^{\ell_p} S_p^{j_p} \otimes R_{q,k_q}^{\ell_q} S_q^{j_q}. \tag{3.15}$$

Since $R_{p,k_p}, S_p, R_{q,k_q}, S_q$ are orthogonal matrices, Proposition 2.3.17 tells us that $R_{p,k_p}^{\ell_p} S_p^{j_p} \otimes R_{q,k_q}^{\ell_q} S_q^{j_q}$ is also an orthogonal matrix. Therefore, the representation in (3.15) is a 4×4 real valued matrix which preserves dot products by Proposition 2.3.14. Lastly, since each automorphism in $\mathcal{A}$ has a unique image in $D_p \times D_q$ by Theorem 3.5.11, we have mirrored the symmetries of the chordal ring in a 4-dimensional OR of $L(CR_{n,c})$.

To recapitulate this chapter, we compile all of the main results to describe the targeted relationship between the automorphisms of $L(CR_{n,c})$ and the corresponding linear transformations which act on the ORs of $L(CR_{n,c})$ in $\mathbb{R}^4$. Using a subgroup $\mathcal{A}$ of the automorphism group of $CR_{n,c}$, consisting of $\phi(x) = (-1)^s c^t x + d$, for $x, d \in \mathbb{Z}_n$ and $s, t \in \{0, 1\}$, we were able to show that $L(CR_{n,c})$ is vertex transitive. Therefore, we can send any vertex of the line graph to any other vertex. Once we knew this, we found an isomorphism which relates the rotational symmetry of the chordal ring to a product of elements of two dihedral groups. Combining these two concepts, we showed in Theorem 3.5.11 that there is a unique automorphism for each representation of the elements of the direct product of two dihedral groups.

Chapter 4

Computer-Free Construction

It is natural to anticipate that some of the symmetries of a graph will be reflected in any of its OR. Agreeing with our initial Ansatz, as well as the main result from the previous chapter, we present a construction of an OR of $L(CR_{n,c})$ in $\mathbb{R}^4$. This, together with Theorem 3.2.1, provides a KS set in $\mathbb{R}^4$. Since we have defined an infinite family of such graphs, we arrive at our goal of constructing an infinite family of KS sets in $\mathbb{R}^4$. Our method reduces the number of free variables needed to construct an OR of $L(CR_{n,c})$ from $8n$ ($2n$ vectors in $\mathbb{R}^4$) to 8 (just 2 vectors in $\mathbb{R}^4$) by exploiting the rotational symmetry of the chordal ring. The construction and proofs were done definitively without the use of numerical experiments. It was, however, motivated by numerical data. In the following chapter, we discuss the construction's derivation and the computational results which acted as motivation.

Let $n = pq$ for coprime, odd integers p and q. Let c be an integer where $1 < c < n - 1$ and $c^2 \equiv 1 \pmod{n}$. Let $\mathcal{A}$ be the subgroup of $\text{Aut}(CR_{n,c})$ given in Theorem 3.5.11. In the previous section, we showed the existence of an isomorphism from $\mathcal{A}$ to the product of two dihedral groups D_p and D_q. Though there are many symmetries available to us, we choose to use only rotational symmetry in our construction because it is the simplest symmetry to use.

Suppose σ is a map from edges of $CR_{n,c}$ to the vectors of an OR in $\mathbb{R}^4$. Let a and b be vectors of an OR of $L(CR_{n,c})$ corresponding to edges e_0 and e_n in $CR_{n,c}$, seen below in Figure 4.1. As we mentioned above, the chordal ring graph has two types of edges, chords and ring edges. The rotational symmetry has two orbits within the edges of $CR_{n,c}$. All ring edges comprise one orbit and the chords make up the other. Using just the cyclic symmetry of the chordal ring, we are able to send e_0 to all other ring edges and e_n to all other chord edges. We use automorphisms of the form

$$\phi(x) = x + d \bmod n, \tag{4.1}$$

where $d \in \mathbb{Z}_n$, to rotate the edges about the graph. Notice that because there is no c in this ϕ, there will not be a switch between chords and ring edges. Even though we proved earlier

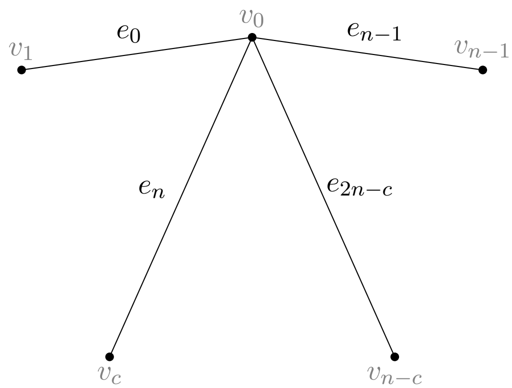

Figure 4.1: Edges incident with v_0 in $CR_{n,c}$.

that $CR_{n,c}$ and $L(CR_{n,c})$ are vertex transitive, we are only using some of the automorphisms of $\mathcal{A}$. However, the few we do use still act transitively on the vertices of $CR_{n,c}$, which can be seen in the proof of Theorem 3.4.1. Remember the map Φ, which sends automorphisms of $CR_{n,c}$ to dihedral group elements, given in the proof of Theorem 3.5.11. When it is applied to the automorphisms of the form in (4.1) we get

$$\Phi(\phi) = \left(\mathcal{R}_p^d, \mathcal{R}_q^d\right). \tag{4.2}$$

The linear transformations that act on the vectors a, b are the representations of the dihedral group elements in (4.2) under ρ from equation (3.6). Explicitly they yield

$$\rho_{D_p \times D_q}(\Phi(\phi)) = R_{p,k_p}^d \otimes R_{q,k_q}^d \tag{4.3}$$

where k_p, k_q are coprime to $p, q > 1$, respectively. By applying maps of this form to a and b, we will show how to generate a set of $2n$ vectors in $\mathbb{R}^4$ which preserve the structure of $L(CR_{n,c})$. To confirm that this set of vectors is an OR of $L(CR_{n,c})$, we need to check that all adjacent vertices of $L(CR_{n,c})$ correspond to orthogonal vectors in the set.

We have mentioned earlier that each degree 4 vertex of $CR_{n,c}$ induces a clique of size four in $L(CR_{n,c})$. From our assumed labelling, made in Remark 3.1.2, any vertex v_i in $CR_{n,c}$ is adjacent to vertices $v_{i+1}, v_{i-1}, v_{i+c}$ and v_{i-c} where all subscripts are modulo n. Consider the vertex v_0, in Figure 4.1, whose set of incident edges in $CR_{n,c}$ is $\{e_0, e_{n-1}, e_n, e_{2n-c}\}$. The vectors corresponding to these edges must make up a mutually orthogonal set of size four. Hence we require that the dot product of every pair of the vectors corresponding to these edges evaluates to zero. We will now derive the vectors of the two edges on the right of Figure 4.2 in terms of a and b. Using the main result from the last chapter, Theorem 3.5.11, as well as the representation from equation (4.3), we are able to use the linear transformations to transform the vectors a and b to all other vectors in the OR. We next find the rotational automorphisms which map e_0 to e_{n-1} and e_n to e_{2n-c}. Rotating e_0 to e_{n-1} amounts to

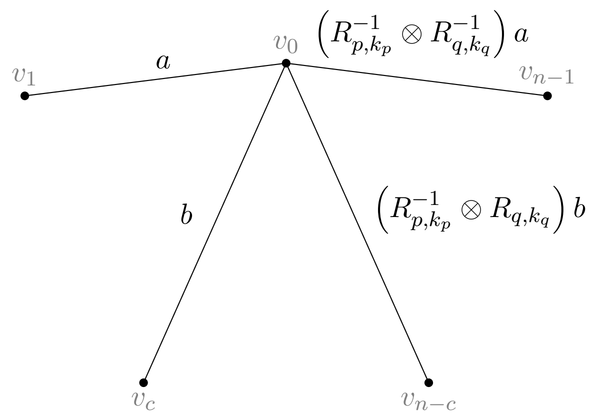

Figure 4.2: Vectors representing edges incident with v_0 in $CR_{n,c}$.

sending $\{v_0, v_1\}$ to $\{v_{n-1}, v_0\}$. By applying the automorphism ϕ from equation (4.1) where $d = n - 1$, to e_0 we have

$$\{0, 1\} \xrightarrow{\phi} \{\phi(0), \phi(1)\} = \{n - 1, 1 + n - 1\} \equiv \{n - 1, 0\} \pmod n$$

which corresponds to $\{v_{n-1}, v_0\} = e_{n-1}$. Using the group representation from (4.3), the linear transformation which will send a to a vector corresponding to e_{n-1} is given by

$$\rho(\Phi(\phi)) = R_{p,k_p}^{n-1} \otimes R_{q,k_q}^{n-1} = R_{p,k_p}^{-1} \otimes R_{q,k_q}^{-1}.$$

Similarly, since $e_{2n-c} = \{v_0, v_{n-c}\}$ is a chord, we must find a map which sends e_n to e_{2n-c}. We let $d = -c$ so that ϕ will send $e_n = \{v_0, v_c\}$ to

$$\{0, c\} \xrightarrow{\phi} \{\phi(0), \phi(c)\} = \{-c, c - c\} \equiv \{n - c, 0\} \pmod n$$

which corresponds to $\{v_{n-c}, v_0\} = e_{2n-c}$. Again using the representation in equation (4.3), the linear transformation which maps b to the vector corresponding to e_{2n-c} is

$$\rho(\Phi(\phi)) = R_{p,k_p}^{-c} \otimes R_{q,k_q}^{-c} = R_{p,k_p}^{-1} \otimes R_{q,k_q}$$

since we assumed without loss of generality that $c \equiv 1 \pmod p$ and $c \equiv -1 \pmod q$ from Remark 3.1.9. Since these are the linear maps needed to send a, b to the correct vectors, we have that

$$\sigma(e_{n-1}) = \left(R_{p,k_p}^{-1} \otimes R_{q,k_q}^{-1}\right) a, \quad \sigma(e_{2n-c}) = \left(R_{p,k_p}^{-1} \otimes R_{q,k_q}\right) b.$$

Now that we have the vectors corresponding to e_0, e_{n-1}, e_n and e_{2n-c} (see Figures 4.1 and 4.2), we can consider the dot products of these vectors.

Notice that we evaluate the dot product of vectors u and Mv as $u^T Mv$. By taking the dot product of each pair, we get the following six equations which must be satisfied to guarantee that our constructed set of vectors is indeed an OR of $L(CR_{n,c})$.

(i) $a^T b = 0$

(ii) $a^T \left(R_{p,k_p}^{-1} \otimes R_{q,k_q}^{-1}\right) a = 0$

(iii) $b^T \left(R_{p,k_p}^{-1} \otimes R_{q,k_q}\right) b = 0$

(iv) $a^T \left(R_{p,k_p}^{-1} \otimes R_{q,k_q}\right) b = 0$

(v) $\left(\left(R_{p,k_p}^{-1} \otimes R_{q,k_q}^{-1}\right) a\right)^T b = 0$

(vi) $\left(\left(R_{p,k_p}^{-1} \otimes R_{q,k_q}^{-1}\right) a\right)^T \left(R_{p,k_p}^{-1} \otimes R_{q,k_q}\right) b = 0$

Notice that even though the exponents on these matrices do not appear equal, this is because we can reduce ℓ modulo p and q, for R_{p,k_p} and R_{q,k_q}, respectively. We can get ℓ from any pair of exponents in the dot products using Theorem 3.1.7 since p and q are coprime. Though these equations are derived from a single vertex of $CR_{n,c}$ using the rotational symmetry of the graph, we are able to construct the same equations for every vector of the $CR_{n,c}$.

4.1 The Main Construction

In this section, we will present our construction and show that the set of vectors we obtain is in fact an OR of $L(CR_{n,c})$ and hence a KS set. We also discuss some characteristics of the resulting OR.

Theorem 4.1.1. *Let $n = pq$ for coprime, odd integers p, q such that $p, q > 1$ and let*

$$a = \begin{pmatrix} (1-C)\cos\frac{2\pi k_q}{q} \\ (1-C)\sin\frac{2\pi k_q}{q} \\ -(1+C)\sin\frac{2\pi k_q}{q} \\ (1+C)\cos\frac{2\pi k_q}{q} \end{pmatrix}, \quad b = \begin{pmatrix} C+1 \\ 0 \\ 0 \\ C-1 \end{pmatrix} \tag{4.4}$$

where

$$C = \sqrt{-\frac{\cos\left(2\pi\left(\frac{k_p}{p} - \frac{k_q}{q}\right)\right)}{\cos\left(2\pi\left(\frac{k_p}{p} + \frac{k_q}{q}\right)\right)}} \tag{4.5}$$

and k_p, k_q are chosen according to

$$k_x = \begin{cases} \left\lceil \dfrac{x}{4} \right\rceil, & x \equiv 3 \pmod 4 \\ \left\lfloor \dfrac{x}{4} \right\rfloor, & x \equiv 1 \pmod 4 \end{cases} \tag{4.6}$$

where $\lfloor\ \rfloor$ is the floor function and $\lceil\ \rceil$ is the ceiling function. Let

$$S = \{a^i : 0 \leq i < n\} \cup \{b^i : 0 \leq i < n\} \tag{4.7}$$

where

$$a^i = \left(R_{p,k_p} \otimes R_{q,k_q}\right)^i \cdot a$$
$$b^i = \left(R_{p,k_p} \otimes R_{q,k_q}\right)^i \cdot b.$$

Then S is an orthonormal representation of $L(CR_{n,c})$ in $\mathbb{R}^4$.

Proof. We will show in Theorem 4.1.4 that our choice of k_p and k_q implies that C is real, and hence, S is a set of real vectors. For now assume this to be true. The six dot products we wish to show evaluate to zero are stated below.

(i) $a^T b = 0$

(ii) $a^T \left(R^{-1}_{p,k_p} \otimes R^{-1}_{q,k_q}\right) a = 0$

(iii) $b^T \left(R^{-1}_{p,k_p} \otimes R_{q,k_q}\right) b = 0$

(iv) $a^T \left(R^{-1}_{p,k_p} \otimes R_{q,k_q}\right) b = 0$

(v) $\left(\left(R^{-1}_{p,k_p} \otimes R^{-1}_{q,k_q}\right) a\right)^T b = 0$

(vi) $\left(\left(R^{-1}_{p,k_p} \otimes R^{-1}_{q,k_q}\right) a\right)^T \left(R^{-1}_{p,k_p} \otimes R_{q,k_q}\right) b = 0$

We can simplify the dot product in (v) by expanding the transposed term.

$$\left(\left(R^{-1}_{p,k_p} \otimes R^{-1}_{q,k_q}\right) a\right)^T b = a^T \left(R^{-1}_{p,k_p} \otimes R^{-1}_{q,k_q}\right)^T b.$$

Using (2.5) and the fact that $R^{-1}_{n,k_n} = R^T_{n,k_n}$ from Remark 3.5.7, this simplifies to

$$a^T \left(R^{-1}_{p,k_p} \otimes R^{-1}_{q,k_q}\right)^T b = a^T \left(\left(R^{-1}_{p,k_p}\right)^T \otimes \left(R^{-1}_{q,k_q}\right)^T\right) b = a^T \left(R_{p,k_p} \otimes R_{q,k_q}\right) b = 0.$$

Similarly, we simplify the dot product of (vi) to

$$\begin{aligned}\left(\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}^{-1}\right)a\right)^T\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}\right)b &= a^T\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}^{-1}\right)^T\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}\right)b \\ &= a^T\left(R_{p,k_p}\otimes R_{q,k_q}\right)\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}\right)b.\end{aligned}$$

Using equation (2.1), we further simplify this to

$$a^T\left(R_{p,k_p}\otimes R_{q,k_q}\right)\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}\right)b = a^T\left(I\otimes R_{q,k_q}^2\right)b.$$

Additionally, notice that $I\otimes I = I$, so a^Tb can be written as $a^T(I\otimes I)b$. Therefore, we may restate all six equations in a uniform way.

(i) $a^T\left(I\otimes I\right)b = 0$

(ii) $a^T\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}^{-1}\right)a = 0$

(iii) $b^T\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}\right)b = 0$

(iv) $a^T\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}\right)b = 0$

(v) $a^T\left(R_{p,k_p}\otimes R_{q,k_q}\right)b = 0$

(vi) $a^T\left(I\otimes R_{q,k_q}^2\right)b = 0$

We will be referring to the equations in this form for the rest of the thesis.

Remember that $R_{n,k}^{\ell}$ is the rotation matrix given by

$$R_{n,k}^{\ell} = \begin{pmatrix}\cos\frac{2\pi\ell k}{n} & -\sin\frac{2\pi\ell k}{n}\\ \sin\frac{2\pi\ell k}{n} & \cos\frac{2\pi\ell k}{n}\end{pmatrix}$$

where ℓ is an integer. For all equations but the first, we must calculate the Kronecker product of the two rotation matrices $R_{p,k_p}^{\ell_p}$ and $R_{q,k_q}^{\ell_q}$. Notice that for any pair of exponents of the rotation matrices in equations (ii) through (vi), we can find an ℓ using Theorem 3.1.7 such that the product can be represented as $\left(R_{p,k_p}\otimes R_{q,k_q}\right)^{\ell}$. Additionally we will use the following trigonometric identities in the simplifications below.

$$\sin^2\theta + \cos^2\theta = 1 \tag{4.8}$$

$$\begin{aligned}\cos(\theta + (2m+1)\pi) &= -\cos\theta\\ \sin(\theta + (2m+1)\pi) &= -\sin\theta\end{aligned} \tag{4.9}$$

$$\begin{aligned}\cos(\theta_1 \mp \theta_2) &= \cos\theta_1\cos\theta_2 \pm \sin\theta_1\sin\theta_2\\ \sin(\theta_1 \pm \theta_2) &= \sin\theta_1\cos\theta_2 \pm \cos\theta_1\sin\theta_2\end{aligned} \tag{4.10}$$

where $m\in\mathbb{Z}$. We will now show each equation, from (i) to (vi), is satisfied.

Case 1 (Equation (i)). *We will confirm that the first dot product evaluates to zero.*

$$a^T b = (1+C)(1-C)\cos\frac{2\pi k_q}{q} + (1+C)(-1+C)\cos\frac{2\pi k_q}{q}$$
$$= \Big((1-C^2) - (1-C^2)\Big)\cos\frac{2\pi k_q}{q} = 0$$

Case 2 (Equation (ii)). *We will confirm that the second dot product evaluates to zero.*

$$a^T\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}^{-1}\right)a =$$
$$= a^T\begin{pmatrix} \cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & \cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & \sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & \sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} \\ -\cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & \cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & -\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & \sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} \\ -\sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & -\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & \cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & \cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} \\ \sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & -\sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & -\cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & \cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} \end{pmatrix} a$$
$$= a^T\begin{pmatrix} -(C-1)\cos\frac{2\pi k_p}{p}\cos^2\frac{2\pi k_q}{q} - (C-1)\cos\frac{2\pi k_p}{p}\sin^2\frac{2\pi k_q}{q} \\ (C+1)\sin\frac{2\pi k_p}{p}\sin^2\frac{2\pi k_q}{q} + (C+1)\sin\frac{2\pi k_p}{p}\cos^2\frac{2\pi k_q}{q} \\ (C-1)\sin\frac{2\pi k_p}{p}\cos^2\frac{2\pi k_q}{q} + (C-1)\sin\frac{2\pi k_p}{p}\sin^2\frac{2\pi k_q}{q} \\ (C+1)\cos\frac{2\pi k_p}{p}\sin^2\frac{2\pi k_q}{q} + (C+1)\cos\frac{2\pi k_p}{p}\cos^2\frac{2\pi k_q}{q} \end{pmatrix}$$

All of the elements of the vector above can be factored and simplified using (4.8).

$$a^T\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}\right)a = a^T\begin{pmatrix} -(C-1)\cos\frac{2\pi k_p}{p}\left(\cos^2\frac{2\pi k_q}{q}+\sin^2\frac{2\pi k_q}{q}\right) \\ (C+1)\sin\frac{2\pi k_p}{p}\left(\sin^2\frac{2\pi k_q}{q}+\cos^2\frac{2\pi k_q}{q}\right) \\ (C-1)\sin\frac{2\pi k_p}{p}\left(\cos^2\frac{2\pi k_q}{q}+\sin^2\frac{2\pi k_q}{q}\right) \\ (C+1)\cos\frac{2\pi k_p}{p}\left(\sin^2\frac{2\pi k_q}{q}+\cos^2\frac{2\pi k_q}{q}\right) \end{pmatrix}$$
$$= a^T\begin{pmatrix} -(C-1)\cos\frac{2\pi k_p}{p} \\ (C+1)\sin\frac{2\pi k_p}{p} \\ (C-1)\sin\frac{2\pi k_p}{p} \\ (C+1)\cos\frac{2\pi k_p}{p} \end{pmatrix}$$

Lastly, we multiply the remaining two vectors to get the following.

$$a^T\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}\right)a = -(C-1)^2\cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} + (1-C^2)\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}$$
$$+ (1-C^2)\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} + (C+1)^2\cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}$$
$$= 2C^2\left(\cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} - \sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}\right)$$
$$+ 2\left(\cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} + \sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}\right)$$
$$= 2C^2\cos\left(\frac{2\pi k_p}{p}+\frac{2\pi k_q}{q}\right) + 2\cos\left(\frac{2\pi k_p}{p}-\frac{2\pi k_q}{q}\right)$$

By substituting in the value of C, we see that this equation is verified.

$$
\begin{aligned}
a^T\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}\right)a &= -2\ \frac{\cos\left(\frac{2\pi k_p}{p}-\frac{2\pi k_q}{q}\right)}{\cos\left(\frac{2\pi k_p}{p}+\frac{2\pi k_q}{q}\right)}\cos\left(\frac{2\pi k_p}{p}+\frac{2\pi k_q}{q}\right)+2\cos\left(\frac{2\pi k_p}{p}-\frac{2\pi k_q}{q}\right)\\
&= -2\cos\left(\frac{2\pi k_p}{p}-\frac{2\pi k_q}{q}\right)+2\cos\left(\frac{2\pi k_p}{p}-\frac{2\pi k_q}{q}\right)=0
\end{aligned}
$$

Case 3 (Equation (iii))**.** *We will confirm that the third dot product evaluates to zero.*

$$
\begin{aligned}
&b^T\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}\right)b =\\
&= b^T\begin{pmatrix}
\cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & -\cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & \sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & -\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}\\
\cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & \cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & \sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & \sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}\\
-\sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & \sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & \cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & -\cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}\\
-\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & -\sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & \cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & \cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}
\end{pmatrix}b\\
&= b^T\begin{pmatrix}
(C+1)\cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}-(C-1)\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}\\
(C+1)\cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}+(C-1)\sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}\\
-(C+1)\sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}-(C-1)\cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}\\
-(C+1)\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}+(C-1)\cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}
\end{pmatrix}
\end{aligned}
$$

By multiplying on the left hand side by b^T, we get the following.

$$
\begin{aligned}
b^T\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}\right)b &= (C+1)^2\cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}-(C^2-1)\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}\\
&\quad-(C^2-1)\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}+(C-1)^2\cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}\\
&= 2C^2\left(\cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}-\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}\right)\\
&\quad+2\left(\cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}+\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}\right)\\
&= 2C^2\cos\left(\frac{2\pi k_p}{p}+\frac{2\pi k_q}{q}\right)+2\cos\left(\frac{2\pi k_p}{p}-\frac{2\pi k_q}{q}\right)
\end{aligned}
$$

Again, we expand this by substituting the value of C and the dot product evaluates to zero.

$$
\begin{aligned}
b^T\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}\right)b &= -2\frac{\cos\left(\frac{2\pi k_p}{p}-\frac{2\pi k_q}{q}\right)}{\cos\left(\frac{2\pi k_p}{p}+\frac{2\pi k_q}{q}\right)}\cos\left(\frac{2\pi k_p}{p}+\frac{2\pi k_q}{q}\right)+2\cos\left(\frac{2\pi k_p}{p}-\frac{2\pi k_q}{q}\right)\\
&= -2\cos\left(\frac{2\pi k_p}{p}-\frac{2\pi k_q}{q}\right)+2\cos\left(\frac{2\pi k_p}{p}-\frac{2\pi k_q}{q}\right)=0
\end{aligned}
$$

Case 4 (Equation (iv))**.** *We will confirm that the fourth dot product evaluates to zero. Notice that since the matrix in (iv) is the same as in (iii), we do not need to recalculate it. We are also multiplying by the same vector on the right hand side so we do not need to* *calculate this step either. Therefore, we can start with*

$$a^T\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}\right)b = a^T\begin{pmatrix}(C+1)\cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}-(C-1)\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}\\(C+1)\cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}+(C-1)\sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}\\-(C+1)\sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}-(C-1)\cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}\\-(C+1)\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}+(C-1)\cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}\end{pmatrix}.$$

From here we can immediately take the dot product of the two vectors.

$$\begin{aligned}a^T\left(R_{p,k_p}^{-1}\otimes R_{q,k_q}\right)b &= (C+1)-(C-1)\cos\frac{2\pi k_p}{p}\cos^2\frac{2\pi k_q}{q}-(C-1)\cos\frac{2\pi k_p}{p}\sin^2\frac{2\pi k_q}{q}\\&\quad+(C-1)(C+1)\cos\frac{2\pi k_p}{p}\sin^2\frac{2\pi k_q}{q}+(C+1)\cos\frac{2\pi k_p}{p}\cos^2\frac{2\pi k_q}{q}\\&=-(C^2-1)\cos\frac{2\pi k_p}{p}\cos^2\frac{2\pi k_q}{q}-(C^2-1)\cos\frac{2\pi k_p}{p}\sin^2\frac{2\pi k_q}{q}\\&\quad+(C^2-1)\cos\frac{2\pi k_p}{p}\sin^2\frac{2\pi k_q}{q}+(C^2-1)\cos\frac{2\pi k_p}{p}\cos^2\frac{2\pi k_q}{q}=0\end{aligned}$$

Case 5 (Equation (v))**.** *We will confirm that the fifth dot product evaluates to zero.*

$$\begin{aligned}&a^T\left(R_{p,k_p}\otimes R_{q,k_q}\right)b=\\&=a^T\begin{pmatrix}\cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & -\cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & -\sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & \sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}\\\cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & \cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & -\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & -\sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}\\\sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & -\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & \cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & -\cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}\\\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & \sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q} & \cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q} & \cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}\end{pmatrix}b\\&=a^T\begin{pmatrix}(C+1)\cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}+(C-1)\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}\\(C+1)\cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}-(C-1)\sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}\\(C+1)\sin\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}-(C-1)\cos\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}\\(C+1)\sin\frac{2\pi k_p}{p}\sin\frac{2\pi k_q}{q}+(C-1)\cos\frac{2\pi k_p}{p}\cos\frac{2\pi k_q}{q}\end{pmatrix}\end{aligned}$$

By multiplying on the left hand side by a^T, we get the following.

$$\begin{aligned}a^T\left(R_{p,k_p}\otimes R_{q,k_q}\right)b &= (C+1)\left(-(C-1)\cos\frac{2\pi k_p}{p}\cos^2\frac{2\pi k_q}{q}-(C-1)\cos\frac{2\pi k_p}{p}\sin^2\frac{2\pi k_q}{q}\right)\\&\quad+(C-1)\left((C+1)\cos\frac{2\pi k_p}{p}\sin^2\frac{2\pi k_q}{q}+(C+1)\cos\frac{2\pi k_p}{p}\cos^2\frac{2\pi k_q}{q}\right)\\&=-(C^2-1)\cos\frac{2\pi k_p}{p}\cos^2\frac{2\pi k_q}{q}-(C^2-1)\cos\frac{2\pi k_p}{p}\sin^2\frac{2\pi k_q}{q}\\&\quad+(C^2-1)\cos\frac{2\pi k_p}{p}\sin^2\frac{2\pi k_q}{q}+(C^2-1)\cos\frac{2\pi k_p}{p}\cos^2\frac{2\pi k_q}{q}=0\end{aligned}$$

Case 6 (Equation (vi)). *Lastly will confirm that the sixth dot product evaluates to zero.*

$$
\begin{aligned}
& a^T \left(I \otimes R_{q,k_q}^2\right) b = \\
& = a^T \begin{pmatrix} 2\cos^2 \frac{2\pi k_q}{q} - 1 & -\cos \frac{2\pi k_q}{q} \sin \frac{2\pi k_q}{q} & 0 & 0 \\ \cos \frac{2\pi k_q}{q} \sin \frac{2\pi k_q}{q} & 2\cos^2 \frac{2\pi k_q}{q} - 1 & 0 & 0 \\ 0 & 0 & 2\cos^2 \frac{2\pi k_q}{q} - 1 & -\cos \frac{2\pi k_q}{q} \sin \frac{2\pi k_q}{q} \\ 0 & 0 & \cos \frac{2\pi k_q}{q} \sin \frac{2\pi k_q}{q} & 2\cos^2 \frac{2\pi k_q}{q} - 1 \end{pmatrix} b
\end{aligned}
$$

By multiplying on the right hand side by b, we can simplify this to

$$
a^T \left(I \otimes R_{q,k_q}^2\right) b = a^T \begin{pmatrix} (C+1)\left(2\cos^2 \frac{2\pi k_q}{q} - 1\right) \\ 2(C+1)\cos \frac{2\pi k_q}{q} \sin \frac{2\pi k_q}{q} \\ -2(C+1)\cos \frac{2\pi k_q}{q} \sin \frac{2\pi k_q}{q} \\ (C-1)\left(2\cos^2 \frac{2\pi k_q}{q} - 1\right) \end{pmatrix}.
$$

By taking the dot product of the two remaining vectors, we have

$$
\begin{aligned}
a^T \left(I \otimes R_{q,k_q}^2\right) b &= (C+1)\left(-(C-1)\cos \frac{2\pi k_q}{q}\left(2\cos^2 \frac{2\pi k_q}{q} - 1\right) - 2(C-1)\cos \frac{2\pi k_q}{q} \sin^2 \frac{2\pi k_q}{q}\right) \\
&\quad + (C-1)\left(2(C+1)\cos \frac{2\pi k_q}{q} \sin^2 \frac{2\pi k_q}{q} + (C+1)\cos \frac{2\pi k_q}{q}\left(2\cos^2 \frac{2\pi k_q}{q} - 1\right)\right) \\
&= -2(C^2-1)\cos^3 \frac{2\pi k_q}{q} + (C^2-1)\cos \frac{2\pi k_q}{q} - 2(C^2-1)\cos \frac{2\pi k_q}{q} \sin^2 \frac{2\pi k_q}{q} \\
&\quad + 2(C^2-1)\cos^3 \frac{2\pi k_q}{q} - (C^2-1)\cos \frac{2\pi k_q}{q} + 2(C^2-1)\cos \frac{2\pi k_q}{q} \sin^2 \frac{2\pi k_q}{q} = 0.
\end{aligned}
$$

Since all six equations evaluate to zero for all coprime, odd integers $p, q > 1$, we can conclude that the set S as above in equation (4.7) is in fact an OR of $L(CR_{n,c})$ in $\mathbb{R}^4$. □

Remark 4.1.2. *The previous proof illustrates our original process of discovering an OR of $L(CR_{n,c})$, which is further detailed in Chapter 5. We did not take advantage of all symmetries of the chordal ring in this proof method. Due to the rotational symmetry that was used, our proofs contain a lot of trigonometric functions. Originally, we used the above proof because of the discovery process. It was also very simple to verify the proofs using Maple. Checking that we were on the right track was very simple because of this. There exists an alternate condensed proof, that follows this remark, which takes advantage of some of the additional symmetries of our graph and involves no trigonometric functions. For illustration, we show one of the six cases in the condensed form.*

Proof. [Equation (iv)] Notice that we can write vector a as

$$
a = \begin{pmatrix} 1-c \\ 0 \end{pmatrix} \otimes R_{q,k_q} \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 1+c \end{pmatrix} \otimes R_{q,k_q} \begin{pmatrix} 0 \\ 1 \end{pmatrix}
$$

and vector b as

$$b = \begin{pmatrix} c+1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ c-1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Then the dot product in (iv) becomes

$$\begin{aligned}
& a^T \left(R_{p,k_p}^{-1} \otimes R_{q,k_q} \right) b = \\
&= \left[\begin{pmatrix} 1-c & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \end{pmatrix} R_{q,k_q}^{-1} + \begin{pmatrix} 0 & 1+c \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \end{pmatrix} R_{q,k_q}^{-1} \right] \left[R_{p,k_p}^{-1} \otimes R_{q,k_q} \right] b \\
&= \Bigg[\left[\begin{pmatrix} 1-c & 0 \end{pmatrix} \otimes \begin{pmatrix} 1 & 0 \end{pmatrix} R_{q,k_q}^{-1} \right] \left[R_{p,k_p}^{-1} \otimes R_{q,k_q} \right] + \\
&\qquad\qquad \left[\begin{pmatrix} 0 & 1+c \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \end{pmatrix} R_{q,k_q}^{-1} \right] \left[R_{p,k_p}^{-1} \otimes R_{q,k_q} \right] \Bigg] b \\
&= \left[\begin{pmatrix} 1-c & 0 \end{pmatrix} R_{p,k_p}^{-1} \otimes \begin{pmatrix} 1 & 0 \end{pmatrix} R_{q,k_q}^{-1} R_{q,k_q} + \begin{pmatrix} 0 & 1+c \end{pmatrix} R_{p,k_p}^{-1} \otimes \begin{pmatrix} 0 & 1 \end{pmatrix} R_{q,k_q}^{-1} R_{q,k_q} \right] b \\
&= \left[\begin{pmatrix} 1-c & 0 \end{pmatrix} R_{p,k_p}^{-1} \otimes \begin{pmatrix} 1 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 1+c \end{pmatrix} R_{p,k_p}^{-1} \otimes \begin{pmatrix} 0 & 1 \end{pmatrix} \right] b \\
&= (1-c) \left(R_{p,k_p}^{-1} \right)_{1,1} (c+1) + (1+c) \left(R_{p,k_p}^{-1} \right)_{2,2} (c-1) \\
&= (1-c^2) \left(R_{p,k_p}^{-1} \right)_{1,1} - (1-c^2) \left(R_{p,k_p}^{-1} \right)_{2,2} = 0
\end{aligned}$$

since $\left(R_{p,k_p}^{-1} \right)_{1,1} = \left(R_{p,k_p}^{-1} \right)_{2,2}$. □

Now that we have an OR of $L(CR_{n,c})$ in $\mathbb{R}^4$ for any acceptable n and c, we can extend the result to KS sets.

Theorem 4.1.3. *Let $n > 1$ be an odd integer and assume that n is not a prime power. Then there exists a KS set with $2n$ vectors and n bases in $\mathbb{R}^4$.*

Proof. Since n is not a prime power, we can factor it into two coprime factors, let these be p and q. Hence, there exists an integer c such that $1 < c < n-1$ and $c^2 \equiv 1 \pmod{n}$, by Corollary 3.1.8. By Theorem 4.1.1, we can construct an OR of $L(CR_{n,c})$ in $\mathbb{R}^4$ with $2n$ vectors. Secondly, by Theorem 3.2.1 we know that an OR of $L(CR_{n,c})$ in $\mathbb{R}^4$ is also a KS set in $\mathbb{R}^4$ with n orthogonal bases. Therefore, we have constructed a KS set of $2n$ vectors and n bases in $\mathbb{R}^4$, for any n as above. □

We will now show that our choices of k_p, k_q above result in a real valued C.

Theorem 4.1.4. *Let C be defined as in (4.5) and let $p, q > 1$ be coprime, odd integers. If k_p and k_q are chosen as*

$$k_x = \begin{cases} \left\lceil \dfrac{x}{4} \right\rceil, & x \equiv 3 \pmod{4} \\ \left\lfloor \dfrac{x}{4} \right\rfloor, & x \equiv 1 \pmod{4} \end{cases}$$

then C is a real number.

Proof. Notice that when $x \equiv 1 \pmod 4$, we have

$$\left\lfloor \frac{x}{4} \right\rfloor = \frac{x-1}{4} \tag{4.11}$$

and when $x \equiv 3 \pmod 4$ that

$$\left\lceil \frac{x}{4} \right\rceil = \frac{x+1}{4}. \tag{4.12}$$

Let $p, q > 1$ be coprime, odd integers and let k_p, k_q be as above. We mentioned earlier that we require k_p, k_q to be coprime to p, q respectively. Before we prove that C will be real for these choices, we will first prove that this choice satisfies the coprime requirement.

Notice that $k_x = \frac{x \pm 1}{4}$ for any odd integer x. Assume for a contradiction that $\gcd(x, k_x) > 1$. Therefore there exists a prime r which divides both x and k_x. Then we know $r|x$ and $r|x \pm 1$, which is a contradiction. Hence by our choice of k_x, $\gcd(x, k_x) = 1$ for any odd, positive integer x.

Now, recall that

$$C = \sqrt{-\frac{\cos\left(2\pi\left(\frac{k_p}{p} - \frac{k_q}{q}\right)\right)}{\cos\left(2\pi\left(\frac{k_p}{p} + \frac{k_q}{q}\right)\right)}}.$$

We will show that the above choice of k_p and k_q imply C is real. Consider that for any p, q odd integers, we have

$$\frac{k_p}{p} + \frac{k_q}{q} = \frac{\frac{p\pm1}{4}}{p} + \frac{\frac{q\pm1}{4}}{q} = \frac{1}{2} \pm \frac{p+q}{4pq}.$$

Also, we know that $\frac{p+q}{pq} < 1$, for $p, q > 1$. This implies that $\frac{p+q}{4pq} < \frac{1}{4}$ for $p, q > 1$ which gives us the following inequality

$$\frac{1}{2} - \frac{1}{4} < \frac{k_p}{p} + \frac{k_q}{q} < \frac{1}{2} + \frac{1}{4}$$

from which we get

$$\frac{1}{4} < \frac{k_p}{p} + \frac{k_q}{q} < \frac{3}{4}. \tag{4.13}$$

Similarly, we have

$$\frac{k_p}{p} - \frac{k_q}{q} = \frac{\frac{p\pm1}{4}}{p} - \frac{\frac{q\pm1}{4}}{1} = \pm\frac{q-p}{4pq}.$$

If $p < q$ then $\frac{q-p}{pq} < 1$ and $\frac{q-p}{4pq} < \frac{1}{4}$. If $p > q$, we can switch the values of p and q and the statement still holds. Taking both branches gives a similar inequality to the one in (4.13).

$$-\frac{1}{4} < \frac{k_p}{p} - \frac{k_q}{q} < \frac{1}{4} \tag{4.14}$$

If we multiply both inequalities from lines (4.13) and (4.14) by 2π, we get

$$\frac{\pi}{2} < 2\pi\left(\frac{k_p}{p} + \frac{k_q}{q}\right) < \frac{3\pi}{2},\ -\frac{\pi}{2} < 2\pi\left(\frac{k_p}{p} - \frac{k_q}{q}\right) < \frac{\pi}{2}.$$

This immediately tells us that

$$\cos\left(2\pi\left(\frac{k_p}{p} + \frac{k_q}{q}\right)\right) < 0,\ \cos\left(2\pi\left(\frac{k_p}{p} - \frac{k_q}{q}\right)\right) > 0$$

for our choices of k_p, k_q. Combining these two cosines, we know that their quotient will always be a negative number.

$$\frac{\cos\left(2\pi\left(\frac{k_p}{p} - \frac{k_q}{q}\right)\right)}{\cos\left(2\pi\left(\frac{k_p}{p} + \frac{k_q}{q}\right)\right)} < 0$$

From the definition of C, this C will always be real. □

Thus, our construction creates an infinite family of KS sets in $\mathbb{R}^4$. The last two results of this chapter pertain to additional orthogonalities which resulted from our construction. The extra orthogonalities are not an issue because, by Definition 2.6.4, the ORs are still faithful.

Theorem 4.1.5. *Let $p, q > 1$ be coprime, odd integers, k_p, k_q be integers coprime to p, q respectively and let S be the vector set defined above in equation (4.7). Every vector in the set S is orthogonal to at least $p + q + 1$ other vectors in S.*

Proof. We will aim to show that there are at least $p + q + 1$ vectors orthogonal to each of a and b from Theorem 4.1.1. Then by rotating a and b, we are able to confirm that all vectors of S are orthogonal to at least $p + q + 1$ vectors since the rotational matrix is orthogonal. Below is the general form of a vector corresponding to a chord.

$$\left(R^{\ell}_{p,k_p} \otimes R^{\ell}_{q,k_q}\right) b$$

We will consider the dot product of all such vectors with a to determine for what values ℓ they are orthogonal. We have that

$$
\begin{aligned}
a^T\left(R^\ell_{p,k_p}\otimes R^\ell_{q,k_q}\right)b &= \\
&= a^T\begin{pmatrix}
\cos\frac{2\pi\ell k_p}{p}\cos\frac{2\pi\ell k_q}{q} & \cos\frac{2\pi\ell k_p}{p}\sin\frac{2\pi\ell k_q}{q} & \sin\frac{2\pi\ell k_p}{p}\cos\frac{2\pi\ell k_q}{q} & \sin\frac{2\pi\ell k_p}{p}\sin\frac{2\pi\ell k_q}{q}\\
-\cos\frac{2\pi\ell k_p}{p}\sin\frac{2\pi\ell k_q}{q} & \cos\frac{2\pi\ell k_p}{p}\cos\frac{2\pi\ell k_q}{q} & -\sin\frac{2\pi\ell k_p}{p}\sin\frac{2\pi\ell k_q}{q} & \sin\frac{2\pi\ell k_p}{p}\cos\frac{2\pi\ell k_q}{q}\\
-\sin\frac{2\pi\ell k_p}{p}\cos\frac{2\pi\ell k_q}{q} & -\sin\frac{2\pi\ell k_p}{p}\sin\frac{2\pi\ell k_q}{q} & \cos\frac{2\pi\ell k_p}{p}\cos\frac{2\pi\ell k_q}{q} & \cos\frac{2\pi\ell k_p}{p}\sin\frac{2\pi\ell k_q}{q}\\
\sin\frac{2\pi\ell k_p}{p}\sin\frac{2\pi\ell k_q}{q} & -\sin\frac{2\pi\ell k_p}{p}\cos\frac{2\pi\ell k_q}{q} & -\cos\frac{2\pi\ell k_p}{p}\sin\frac{2\pi\ell k_q}{q} & \cos\frac{2\pi\ell k_p}{p}\cos\frac{2\pi\ell k_q}{q}
\end{pmatrix} b\\
&= a^T\begin{pmatrix}
(C+1)\cos\frac{2\pi\ell k_p}{p}\cos\frac{2\pi\ell k_q}{q}+(C-1)\sin\frac{2\pi\ell k_p}{p}\sin\frac{2\pi\ell k_q}{q}\\
(C+1)\cos\frac{2\pi\ell k_p}{p}\sin\frac{2\pi\ell k_q}{q}-(C-1)\sin\frac{2\pi\ell k_p}{p}\cos\frac{2\pi\ell k_q}{q}\\
(C+1)\sin\frac{2\pi\ell k_p}{p}\cos\frac{2\pi\ell k_q}{q}-(C-1)\cos\frac{2\pi\ell k_p}{p}\sin\frac{2\pi\ell k_q}{q}\\
(C+1)\sin\frac{2\pi\ell k_p}{p}\sin\frac{2\pi\ell k_q}{q}+(C-1)\cos\frac{2\pi\ell k_p}{p}\cos\frac{2\pi\ell k_q}{q}
\end{pmatrix}.
\end{aligned}
$$

Again we expand this to get that

$$
\begin{aligned}
&a^T\left(R^\ell_{p,k_p}\otimes R^\ell_{q,k_q}\right)b = \\
&= -(C+1)(C-1)\cos\frac{2\pi\ell k_p}{p}\cos\frac{2\pi\ell k_q}{q}\cos\frac{2\pi k_q}{q}-(C-1)^2\sin\frac{2\pi\ell k_p}{p}\sin\frac{2\pi\ell k_q}{q}\cos\frac{2\pi k_q}{q}\\
&\quad -(C+1)(C-1)\cos\frac{2\pi\ell k_p}{p}\sin\frac{2\pi\ell k_q}{q}\sin\frac{2\pi k_q}{q}+(C-1)^2\sin\frac{2\pi\ell k_p}{p}\cos\frac{2\pi\ell k_q}{q}\sin\frac{2\pi k_q}{q}\\
&\quad +(C+1)(C-1)\cos\frac{2\pi\ell k_p}{p}\sin\frac{2\pi\ell k_q}{q}\sin\frac{2\pi k_q}{q}-(C+1)^2\sin\frac{2\pi\ell k_p}{p}\cos\frac{2\pi\ell k_q}{q}\sin\frac{2\pi k_q}{q}\\
&\quad +(C+1)(C-1)\cos\frac{2\pi\ell k_p}{p}\cos\frac{2\pi\ell k_q}{q}\cos\frac{2\pi k_q}{q}+(C+1)^2\sin\frac{2\pi\ell k_p}{p}\sin\frac{2\pi\ell k_q}{q}\cos\frac{2\pi k_q}{q}.
\end{aligned}
$$

Half of the terms above cancel and are left with the following.

$$
\begin{aligned}
a^T\left(R^\ell_{p,k_p}\otimes R^\ell_{q,k_q}\right)b &= \left((C+1)^2-(C-1)^2\right)\sin\frac{2\pi\ell k_p}{p}\sin\frac{2\pi\ell k_q}{q}\cos\frac{2\pi k_q}{q}\\
&\quad+\left(-(C+1)^2+(C-1)^2\right)\sin\frac{2\pi\ell k_p}{p}\cos\frac{2\pi\ell k_q}{q}\sin\frac{2\pi k_q}{q}\\
&= 4C\sin\frac{2\pi\ell k_p}{p}\left(\sin\frac{2\pi\ell k_q}{q}\cos\frac{2\pi k_q}{q}-\cos\frac{2\pi\ell k_q}{q}\sin\frac{2\pi k_q}{q}\right)\\
&= 4C\sin\frac{2\pi\ell k_p}{p}\sin\frac{2\pi k_q(\ell-1)}{q}
\end{aligned}
$$

We already know that $C\neq 0$ for all integers k_p, k_q and coprime, odd integers $p, q > 1$. Therefore, for the dot product to evaluate to zero, either $\ell \equiv 0 \pmod p$ or $\ell \equiv 1 \pmod q$ because $\gcd(k_p, p) = \gcd(k_q, q) = 1$. If ℓ is divisible by p, there are q distinct vectors orthogonal to a. When $\ell - 1$ is divisible by q, there are p distinct vectors orthogonal to a. However, one vector is counted in both cases, namely $\left(I_2 \otimes R_{q,k_q}\right)b$. Hence, there are $p+q-1$ distinct vectors corresponding to chords orthogonal to a. Together with the two ring edges, there are at least $p+q+1$ distinct vectors in S orthogonal to a.

Now when considering b, remember that the transpose operation preserves the dot product. Therefore we can see that

$$\left(a^T \left(R^{\ell}_{p,k_p} \otimes R^{\ell}_{q,k_q}\right) b\right)^T = b^T \left(R^{-\ell}_{p,k_p} \otimes R^{-\ell}_{q,k_q}\right) a.$$

Therefore we know that there are the same number of vectors orthogonal to b as there are orthogonal to a. Since each ring edge in $CR_{n,c}$ can be represented by $\left(R^{\ell}_{p,k_p} \otimes R^{\ell}_{q,k_q}\right) a$, b is orthogonal to $p + q - 1$ distinct vectors corresponding to ring edges and two vectors corresponding to chords. □

Conjecture 4.1.6. *Let p, q, k_p, k_q and S be as above. Every vector in S is orthogonal to exactly $p + q + 1$ distinct vectors in S.*

When $p \approx q$, $p+q \approx 2\sqrt{n}$ and the proportion of those pairs that are orthogonal is small. The orthogonalities of the graph are sparse.

Chapter 5

Discovery of the Main Construction

We attempted to find ORs of the line graph of the chordal ring in $\mathbb{R}^4$ numerically for different values of n and c. Using Maple's continuous optimization package, we defined an objective function which, when minimized, found an OR in $\mathbb{R}^4$. Even though this is a discrete mathematics problem, using a continuous optimiser was very useful. This gave us a lot of data to parse through, looking for common patterns which could hint towards a computer-free construction. From these computed ORs of $L(CR_{n,c})$, we found a general form of the solution vectors a and b as given in Theorem 4.1.1. To find such solutions, we transformed the dot products by utilizing the method of diagonalization on the product of the two rotation matrices that appear in each dot product. Then, by finding solutions with these easier dot products and transforming them back to the original vectors, we were able to find the forms of a and b used in the main construction. Notice that we only considered real solutions to these dot products (though in principle it would have been possible to model the OR as complex vectors by representing a complex number in Maple as a pair of real numbers). In the derivation below however, we must deal with complex matrices due to the rotational matrices having complex eigenvalues and eigenvectors. Notice that the previous chapter uses real vectors throughout, and so is self contained.

This chapter is an outline of the process which produced the discoveries reported above. Some steps in this chapter are mathematically rigorous while others should be considered as deliberate assumptions. All steps were checked against the numerical data that we had collected in advance. For example, it was only later in the process that we learned of the freedom of k_p, k_q and its importance when finding real solutions as opposed to complex solutions. Lastly, we discuss the future of this project and possible future projects.

5.1 Numerical Solutions

Let $n = pq$ for coprime, odd integers $p, q > 1$ and let c be $1 < c < n-1$ and $c^2 \equiv 1 \pmod{n}$. The key to discovering ORs of $L(CR_{n,c})$ numerically relied on minimizing the objective function $F : \mathbb{R}^{8n} \to \mathbb{R}$, defined by

$$F\left(v^0, \ldots, v^{2n-1}\right) = \sum_{i=1}^{n} \left(||v^i||^2 - 1\right)^2 + \sum_{\{i,j\} \in E} \left(v^i \cdot v^j\right)^2, \tag{5.1}$$

where $v^i \in \mathbb{R}^4$ corresponds to the edge labelled e_i in $CR_{n,c}$ and E is the edge set of the line graph. Notice that the total number of unknowns is $(4)(2n) = 8n$. F takes in a set of $2n$ general vectors and when it equals zero, two characteristics are forced: (1) all vectors are unit vectors and (2) all adjacent vertices in $L(CR_{n,c})$ correspond to orthogonal vectors in the OR. By Definition 2.6.1, these are the only requirements for a set of vectors to be an OR of a graph.

This function has the advantage of being a polynomial and it was very efficient to use this in the optimizer. The first summation checks for unit length while the second checks for the required orthogonalities. Notice that for any set of vectors, F is non-negative.

Proposition 5.1.1. *Let n be any positive integer and F be defined as above in line (5.1). If $(v^0, \ldots, v^{2n-1})$ is any sequence of $2n$ vectors, then $F\left((v^0, \ldots, v^{2n-1})\right) \geq 0$. For n an odd and that is not a prime power and c where $1 < c < n-1$ and $c^2 \equiv 1 \pmod{n}$, $F\left((v^0, \ldots, v^{2n-1})\right) = 0$ if and only if $(v^0, \ldots, v^{2n-1})$ is an OR of $L(CR_{n,c})$.*

Proof. F above is greater than or equal to zero since it is a sum of squares. Also by Definition 2.6.1, $F\left(v^0, \ldots, v^{2n-1}\right) = 0$ if and only if all $2n$ vectors have length one and and the required orthogonalities exist. □

Therefore F is only minimized when the necessary characteristics for an OR of $L(CR_{n,c})$ in $\mathbb{R}^4$ exist in $(v^0, \ldots, v^{2n-1})$. So we continue to minimize F using Maple's optimizer. We use Maple because of the ability to customize the precision of computations and the option to define an initial point. Since these methods are prone to numerical inaccuracies, it is very useful to be able to include "guard" digits where we do not care about losing precision. We observe that only about the first half of the digits are correct in any numerical solution. Therefore we focus on finding solutions with high precision to confirm that our results are not coincidental. Our problem is special because we have no constraints, so any sequence of real vectors is a feasible solution. We are able to find many different KS sets relatively quickly with low levels of precision, roughly 1000 ORs for each small value $(15, 21, 33, 35, \ldots)$ of n. However when raising the level of precision to confirm the KS sets are not coincidental, the run time of the optimizer increases until we had code running for multiple days. To work around the computational time issues, we utilize the second useful characteristic of Maple's optimization package. The optimizer allows the user to input a starting point. So once we find a solution that is sufficiently minimal, for a low number of digits, we raise the precision and use the previous solution as a starting point for the next run of the optimizer. If the new solution is not closer to zero than the less precise solution, we discard it and we restart the optimizer with a new, random starting point. If this method continues to yield local minimums which get closer to 0, then there must exist an OR of the graph. As well, employing the optimizer this way reduces the run time by an enormous amount since we are not running the optimizer from scratch each time. Still, our code had to minimize a function involving $8n$ variables ($2n$ vectors in $\mathbb{R}^4$) and was still very slow for large values of n.

Once we have a possible KS set, we make sure to check that it is faithful. We do this by computing the Gram matrix for the set of vectors and counting the number of elements sufficiently close to ± 1 and 0. If there are no parallel vectors, we say it is a faithful representation and we accept it as an OR of $L(CR_{n,c})$.

Our method gave us a lot of possible solutions, but it might have also been possible to use a semi-definite optimizer. However, because of the positive results we obtained and the beautiful support by Maple, we decided to stick with this process. By increasing the precision, we were able to convince ourselves that we were on the right track and continued to examine the data.

Our Ansatz was assuming our OR contained the symmetries of the chordal ring graph. The first reason to use a highly symmetric graph is that vertex transitive graphs are very popular for physicists working with contextuality. The second reason was the possibility of reducing the number of variables. The whole goal of the computational work in this chapter was to reduce the number of variables. As we have seen above, we were able to do this by reducing from $8n$ variables to eight by using the rotational symmetry of $L(CR_{n,c})$. We altered the objective function to become $F : \mathbb{R}^4 \times \mathbb{R}^4 \to \mathbb{R}$ with only two inputs $(a, b) \in \mathbb{R}^4 \times \mathbb{R}^4$ instead of a set of $2n$ vectors. For the objective function to evaluate to zero (the optimal solution), the necessary orthogonalities must exist in the set of vectors. This is where the six dot products from the main construction (Theorem 4.1.1) are derived from. In the next section, we focus on finding simpler solutions to these six equations.

5.2 Analysis of the Computed Kochen-Specker Sets

After running the optimizer and analysing the roughly 1000 vector sequences we computed for small n, we repeatedly found relationships of the form of the six dot products from Theorem 4.1.1. For the set of vectors to be an OR of the line graph of the chordal ring, all six dot products needed to evaluate to zero. These six equations are restated for reference.

(i) $a^T (I \otimes I)\, b = 0$

(ii) $a^T \left(R_{p,k_p}^{-1} \otimes R_{q,k_q}^{-1}\right) a = 0$

(iii) $b^T \left(R_{p,k_p}^{-1} \otimes R_{q,k_q}\right) b = 0$

(iv) $a^T \left(R_{p,k_p}^{-1} \otimes R_{q,k_q}\right) b = 0$

(v) $a^T \left(R_{p,k_p} \otimes R_{q,k_q}\right) b = 0$

(vi) $a^T \left(I \otimes R_{q,k_q}^2\right) b = 0.$

As we mentioned earlier, the symmetry of the chordal ring implies that if we find a solution (a, b) to this set of equations, that we can generate an OR of $L(CR_{n,c})$ in $\mathbb{R}^4$ and hence, a KS set in $\mathbb{R}^4$. Using the numerical solutions (a, b) found from the optimizer, we looked for patterns in the solutions to find any simplifications of the vectors a and b. The process to find solutions to these dot products was not so simple and required trying multiple different attacks. The first method we used was to transform these vectors using the diagonalization of the product of the rotation matrices. This method allowed us to find suitable solutions to easier equations, which we were able to transform back to the original vectors. While studying the transformed vectors, we noticed that equations (ii) and (iii) were similar in that they each involved only one vector, a or b. We examined the solutions to these equations separately from the others. Both the symmetric and asymmetric dot products gave us important simplifications resulting from all dot products. As well we also found useful reductions in the number of variables which was the overall goal of this study. By the end of this chapter, we will have derived a, b and C that we presented in the main construction, Theorem 4.1.1.

Notice that each of the dot products (i) to (vi) above can be written in the following form

$$\gamma^T M \delta = 0 \tag{5.2}$$

for γ and δ equalling a or b and $M = \left(R_{p,k_p} \otimes R_{q,k_q}\right)^{\ell} = R_{p,k_p}^{\ell} \otimes R_{q,k_q}^{\ell}$. Remember that we can switch between the two forms of M by using Theorem 3.1.7 and reducing ℓ modulo p and q. Each dot product above has a different value for ℓ. We will denote the value of ℓ for equation (e) as $\ell_{(e)}$. Since the Kronecker product of two square matrices is itself a square matrix, we can decompose M to

$$M = PDP^{-1} \tag{5.3}$$

where P is a matrix whose columns are eigenvectors of M and D is the diagonal matrix of the corresponding eigenvalues of M. From Corollary 3.5.10 we know the eigenvectors and eigenvalues of $R_{p,k_p}^{\ell_{(e)}}$ and $R_{q,k_q}^{\ell_{(e)}}$. Then, using Proposition 2.3.18, we can compute the eigenvectors, with corresponding eigenvalues, of $\left(R_{p,k_p} \otimes R_{q,k_q}\right)^{\ell_{(e)}}$. Explicitly, M has eigenvalues

$$\zeta_n^{\ell_{(e)}(k_p q + k_q p)},\ \zeta_n^{\ell_{(e)}(k_p q - k_q p)},\ \zeta_n^{\ell_{(e)}(-k_p q + k_q p)},\ \zeta_n^{\ell_{(e)}(-k_p q - k_q p)} \tag{5.4}$$

with corresponding eigenvectors

$$\begin{pmatrix} 1 \\ -i \end{pmatrix} \otimes \begin{pmatrix} 1 \\ -i \end{pmatrix} = \begin{pmatrix} 1 \\ -i \\ -i \\ -1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ -i \end{pmatrix} \otimes \begin{pmatrix} 1 \\ i \end{pmatrix} = \begin{pmatrix} 1 \\ i \\ -i \\ 1 \end{pmatrix},$$
$$\begin{pmatrix} 1 \\ -i \end{pmatrix} \otimes \begin{pmatrix} 1 \\ i \end{pmatrix} = \begin{pmatrix} 1 \\ -i \\ i \\ 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ i \end{pmatrix} \otimes \begin{pmatrix} 1 \\ i \end{pmatrix} = \begin{pmatrix} 1 \\ i \\ i \\ -1 \end{pmatrix}. \tag{5.5}$$

Remark 5.2.1. *For ease of discussion let*

$$\alpha = \zeta_n^{k_p q + k_q p} \text{ and } \beta = \zeta_n^{k_p q - k_q p}. \tag{5.6}$$

Since D will vary among the six dot products, we will denote the diagonal matrix in terms of the equation being used. The diagonal matrix for equation (e) is denoted $D_{(e)}$. Notice that every vector is an eigenvector of I, and so P remains constant over all six equations if the order of the eigenvalues in each $D_{(e)}$ remain consistent. Now we can state $D_{(e)}$ and P explicitly below.

$$D_{(e)} = \begin{pmatrix} \alpha^{\ell_{(e)}} & 0 & 0 & 0 \\ 0 & \beta^{\ell_{(e)}} & 0 & 0 \\ 0 & 0 & \beta^{-\ell_{(e)}} & 0 \\ 0 & 0 & 0 & \alpha^{-\ell_{(e)}} \end{pmatrix}, \quad P = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ -i & i & -i & i \\ -i & -i & i & i \\ -1 & 1 & 1 & -1 \end{pmatrix}$$

Notice that the eigenvalues $\alpha^{\ell_{(e)}}, \beta^{\ell_{(e)}}, \beta^{-\ell_{(e)}}$ and $\alpha^{-\ell_{(e)}}$ come in two inverse pairs for all six dot products. Combining both results from (5.2) and (5.3) we have

$$\gamma^T P D_{(e)} P^{-1} \delta = 0. \tag{5.7}$$

P was chosen specifically to have the following relationship.

Proposition 5.2.2. *Let P be defined as above. Then $P^{-1} = P^*$.*

This can be easily computed. Recall that for any real vector γ, $\gamma^T = \gamma^*$. These two facts allow us to simplify the general equation (5.7) and write all six dot products in the following form.

$$\gamma^* P D_{(e)} P^* \delta = 0 \tag{5.8}$$

where γ and δ are a or b. With the dot products now in this form, we are able to make a transformation on the vectors which simplifies the equations and hopefully results in vectors that are easier to work with. Let

$$A = P^* a \text{ and } B = P^* b \tag{5.9}$$

whose elements are denoted

$$A = \begin{pmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \end{pmatrix}, \ B = \begin{pmatrix} B_1 \\ B_2 \\ B_3 \\ B_4 \end{pmatrix}. \tag{5.10}$$

With this transformation, the equations of the form in (5.2) can now be written as

$$\Gamma^* D_{(e)} \Delta = 0 \tag{5.11}$$

where Γ and Δ are either A or B. Notice that

$$A^* = a^* P \text{ and } B^* = b^* P. \tag{5.12}$$

This will allow us to write equation (5.8) in terms of only A, B and $D_{(e)}$. In the original equations, expanding the dot products would result in 16 terms. Since $D_{(e)}$ is a diagonal matrix for all six equations, we can expand all the dot products from (5.11) above to linear equations with just four terms. Finding solutions to these equations becomes much simpler than before the transformation. Afterwards, we will undo the linear map P^* to get solutions in the original form, (a, b). We will now split up the equations into the symmetric and asymmetric cases.

5.2.1 Symmetric Case

In this section we outline all variable reductions and requirements gained from the equations (ii) and (iii), restated below.

(ii) $a^T \left(R_{p,k_p}^{-1} \otimes R_{q,k_q}^{-1} \right) a = 0 \to A^* D_{(ii)} A = 0$

(iii) $b^T \left(R_{p,k_p}^{-1} \otimes R_{q,k_q} \right) b = 0 \to B^* D_{(iii)} B = 0$

The constant C is derived in this section, as well as a reduction from eight variables to four.

Recall that $\alpha = \zeta_n^{k_p q + k_q p}$ and $\beta = \zeta_n^{k_p q - k_q p}$, from (5.6). We can read from the dot products that $\ell_{(ii)} \equiv -1 \pmod p$, $\ell_{(ii)} \equiv -1 \pmod q$, $\ell_{(iii)} \equiv -1 \pmod p$ and $\ell_{(iii)} \equiv 1 \pmod q$. Therefore we can easily write $D_{(ii)}$ and $D_{(iii)}$ using Remark 5.6. With our assignments of A and B stated in (5.9), we can expand the dot products in (ii) and (iii). Since $D_{(e)}$ is a diagonal matrix, we get

$$\begin{aligned}
A^* D_{(ii)} A &= \begin{pmatrix} \overline{A_1} & \overline{A_2} & \overline{A_3} & \overline{A_4} \end{pmatrix} \begin{pmatrix} \alpha^{-1} & 0 & 0 & 0 \\ 0 & \beta^{-1} & 0 & 0 \\ 0 & 0 & \beta & 0 \\ 0 & 0 & 0 & \alpha \end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \end{pmatrix} \\
&= \begin{pmatrix} \alpha^{-1}\overline{A_1} & \beta^{-1}\overline{A_2} & \beta\overline{A_3} & \alpha\overline{A_4} \end{pmatrix} \begin{pmatrix} A_1 \\ A_2 \\ A_3 \\ A_4 \end{pmatrix} \\
&= |A_1|^2\alpha^{-1} + |A_2|^2\beta^{-1} + |A_3|^2\beta + |A_4|^2\alpha = 0. \qquad (5.13)
\end{aligned}$$

Similarly

$$\begin{aligned}
B^* D_{(iii)} B &= \begin{pmatrix} \overline{B_1} & \overline{B_2} & \overline{B_3} & \overline{B_4} \end{pmatrix} \begin{pmatrix} \beta & 0 & 0 & 0 \\ 0 & \alpha & 0 & 0 \\ 0 & 0 & \alpha^{-1} & 0 \\ 0 & 0 & 0 & \beta^{-1} \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \\ B_3 \\ B_4 \end{pmatrix} \\
&= \begin{pmatrix} \beta\overline{B_1} & \alpha\overline{B_2} & \alpha^{-1}\overline{B_3} & \beta^{-1}\overline{B_4} \end{pmatrix} \begin{pmatrix} B_1 \\ B_2 \\ B_3 \\ B_4 \end{pmatrix} \\
&= |B_1|^2\beta + |B_2|^2\alpha + |B_3|^2\alpha^{-1} + |B_4|^2\beta^{-1} = 0. \qquad (5.14)
\end{aligned}$$

Since $A, B \in \mathbb{C}^4$, we make sure that both the real and imaginary parts of (5.13) and (5.14) evaluate to zero. Note that the real and imaginary parts of α, β are given by

$$\begin{aligned}
\Re(\alpha) &= \frac{1}{2}(\alpha + \alpha^{-1}) = \Re(\alpha^{-1}), \quad \Im(\alpha) = \frac{i}{2}(\alpha^{-1} - \alpha) = -\Im(\alpha^{-1}) \\
\Re(\beta) &= \frac{1}{2}(\beta + \beta^{-1}) = \Re(\beta^{-1}), \quad \Im(\beta) = \frac{i}{2}(\beta^{-1} - \beta) = -\Im(\beta^{-1})
\end{aligned}$$

The real part of (5.13) is given by

$$\left(|A_1|^2 + |A_4|^2\right)\left(\frac{1}{2}(\alpha + \alpha^{-1})\right) + \left(|A_2|^2 + |A_3|^2\right)\left(\frac{1}{2}(\beta + \beta^{-1})\right) = 0$$

or simply

$$\left(|A_1|^2 + |A_4|^2\right) \Re(\alpha) + \left(|A_2|^2 + |A_3|^2\right) \Re(\beta) = 0. \tag{5.15}$$

Similarly, the real part of (5.14) is given by

$$\left(|B_2|^2 + |B_3|^2\right) \Re(\alpha) + \left(|B_1|^2 + |B_4|^2\right) \Re(\beta) = 0. \tag{5.16}$$

The imaginary parts of equations (5.13) and (5.14) are given by

$$(|A_1|^2 - |A_4|^2)\Im(\alpha) + (|A_2|^2 - |A_3|^2)\Im(\beta) = 0 \tag{5.17}$$

$$(|B_2|^2 - |B_3|^2)\Im(\alpha) + (|B_1|^2 - |B_4|^2)\Im(\beta) = 0. \tag{5.18}$$

Each of these must evaluate to zero. Given the large number of solutions (a, b) we computed, after transforming them by P in (5.9), we were able to search for patterns in A, B. Within all of the solutions we observed the following relationships.

$$A_1 = \overline{A_4},\ A_2 = \overline{A_3},\ B_1 = \overline{B_4},\ B_2 = \overline{B_3} \tag{5.19}$$

This held for every pair of vectors A and B. This was very positive because the whole aim of this exploration was to reduce the number of variables, and this cuts down the number of variables from eight to four. For the rest of the derivation, we assume the relationships in line (5.19) hold for A and B. This forces vectors A and B to have the form

$$A = \begin{pmatrix} A_1 \\ A_2 \\ \overline{A_2} \\ \overline{A_1} \end{pmatrix},\ B = \begin{pmatrix} B_1 \\ B_2 \\ \overline{B_2} \\ \overline{B_1} \end{pmatrix}. \tag{5.20}$$

Additionally, this implies $|A_1| = |A_4|$, $|A_2| = |A_3|$, $|B_1| = |B_4|$ and $|B_2| = |B_3|$. This assumption causes both imaginary parts (5.17) and (5.18) to evaluate to zero, while the real parts (5.15) and (5.16) become

$$2\left(|A_1|^2\Re(\alpha) + |A_2|^2\Re(\beta)\right) = 0$$

$$2\left(|B_2|^2\Re(\alpha) + |B_1|^2\Re(\beta)\right) = 0.$$

Using Euler's formula, Theorem 2.5.1, and the fact that $\ell \equiv -1 \pmod{p}$, $\ell \equiv \pm 1 \pmod{q}$ for both equations, the real part of α, β are given by

$$\Re(\alpha) = \cos\left(2\pi\left(\frac{k_p}{p} \pm \frac{k_q}{q}\right)\right)$$
$$\Re(\beta) = \cos\left(2\pi\left(\frac{k_p}{p} \mp \frac{k_q}{q}\right)\right)$$

where we take the top or bottom sign consistently. By substituting this into (5.15) and (5.16), we are left with

$$|A_1|^2 \cos\left(2\pi\left(\frac{k_p}{p} \pm \frac{k_q}{q}\right)\right) + |A_2|^2 \cos\left(2\pi\left(\frac{k_p}{p} \mp \frac{k_q}{q}\right)\right) = 0 \tag{5.21}$$

and

$$|B_2|^2 \cos\left(2\pi\left(\frac{k_p}{p} \pm \frac{k_q}{q}\right)\right) + |B_1|^2 \cos\left(2\pi\left(\frac{k_p}{p} \mp \frac{k_q}{q}\right)\right) = 0. \tag{5.22}$$

Again searching through the numerical solutions (a, b), we consistently noticed that

$$|A_1| = |B_2|, \quad |B_1| = |A_2|. \tag{5.23}$$

We assume this to be true for the remainder of the construction. This assumption, along with the assumption in line (5.19), implies that

$$|A_1| = |A_4| = |B_2| = |B_3|, \quad |B_1| = |B_4| = |A_2| = |A_3|. \tag{5.24}$$

This also results in (5.21) and (5.22) being equivalent. Notice that since a and b are nonzero vectors and P is an invertible matrix, A and B are non-zero vectors as well. Therefore, at least one of $|A_1|, |B_1|$ must be non-zero. If one of them is zero, then (5.21) would only hold if the other was also zero. Therefore, $|A_1|$ and $|B_1|$ must be positive, real numbers.

Since all the equations are homogeneous, we have the ability to scale the variables. Let

$$C = \frac{|A_1|}{|A_2|} \tag{5.25}$$

so we can reduce the number of variables in this equation from two to one. Now we can rewrite both equations (5.21) and (5.22) as a single equation.

$$C^2 \cos\left(2\pi\left(\frac{k_p}{p} \pm \frac{k_q}{q}\right)\right) + \cos\left(2\pi\left(\frac{k_p}{p} \mp \frac{k_q}{q}\right)\right) = 0 \tag{5.26}$$

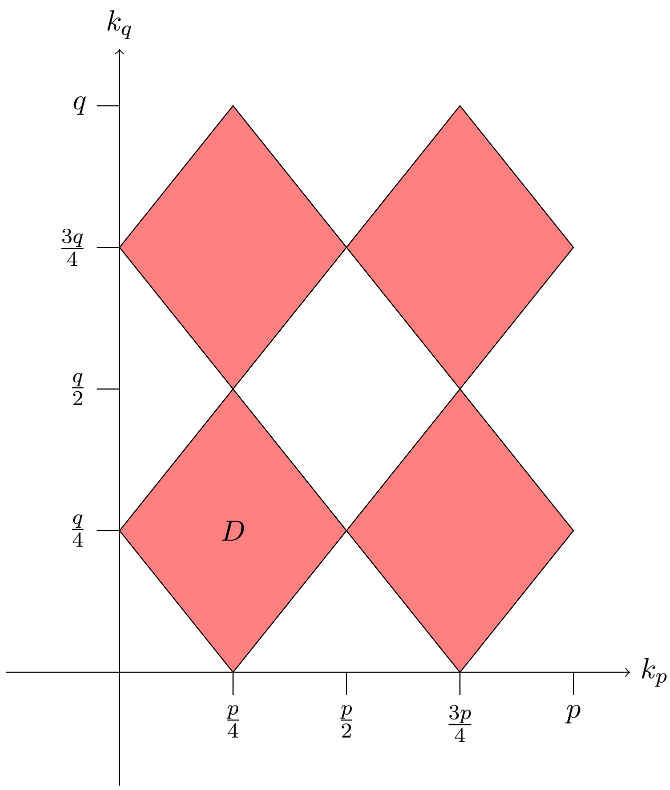

Figure 5.1: The feasible region resulting in a real valued C.

Since $|A_1|$ and $|B_2|$ are positive, real numbers, C must also be a positive, real number. Solving (5.26) for C yields the following formula

$$C = \sqrt{-\frac{\cos\left(2\pi\left(\frac{k_p}{p} \mp \frac{k_q}{q}\right)\right)}{\cos\left(2\pi\left(\frac{k_p}{p} \pm \frac{k_q}{q}\right)\right)}}. \tag{5.27}$$

We have already discussed what inequalities need to be satisfied by k_p, k_q so that C is real in Theorem 4.1.4. By plotting the inequalities from (4.13) and (4.14) we get the feasible region in Figure 5.1. In our construction, we chose k_p and k_q to follow

$$k_x = \begin{cases} \left\lceil \dfrac{x}{4} \right\rceil, & x \equiv 3 \pmod 4 \\ \left\lfloor \dfrac{x}{4} \right\rfloor, & x \equiv 1 \pmod 4 \end{cases}$$

which we showed yields a real valued C in Theorem 4.1.4. Notice that our choice always results in k_p, k_q being within the section of the feasible region labelled D in Figure 5.1.

To review the results from equations (ii) and (iii), we now have solutions

$$A = \begin{pmatrix} A_1 \\ A_2 \\ \overline{A_2} \\ \overline{A_1} \end{pmatrix} = \begin{pmatrix} Ce^{i\cdot\arg(A_1)} \\ e^{i\cdot\arg(A_2)} \\ e^{-i\cdot\arg(A_2)} \\ Ce^{-i\cdot\arg(A_1)} \end{pmatrix}, \; B = \begin{pmatrix} B_1 \\ B_2 \\ \overline{B_2} \\ \overline{B_1} \end{pmatrix} = \begin{pmatrix} e^{i\cdot\arg(B_1)} \\ Ce^{i\cdot\arg(B_2)} \\ Ce^{-i\cdot\arg(B_2)} \\ e^{-i\cdot\arg(B_1)} \end{pmatrix} \tag{5.28}$$

and have derived

$$C = \sqrt{-\frac{\cos\left(2\pi\left(\frac{k_p}{p} \mp \frac{k_q}{q}\right)\right)}{\cos\left(2\pi\left(\frac{k_p}{p} \pm \frac{k_q}{q}\right)\right)}}.$$

In the main construction, we took the top signs consistently. Now we will examine the other four equations (i), (iv), (v) and (vi), which all contain both a and b.

5.2.2 Asymmetric Case

In this section we study the consequences resulting from equations (i), (iv), (v) and (vi), which are reiterated below.

(i) $a^T\left(I \otimes I\right) b = 0 \to A^* D_{(i)} B = 0$

(iv) $a^T\left(R_{p,k_p}^{-1} \otimes R_{q,k_q}\right) b = 0 \to A^* D_{(iv)} B = 0$

(v) $a^T\left(R_{p,k_p} \otimes R_{q,k_q}\right) b = 0 \to A^* D_{(v)} B = 0$

(vi) $a^T\left(I \otimes R_{q,k_q}^2\right) b = 0 \to A^* D_{(vi)} B = 0$

Notice that $\ell_{(i)} \equiv 0 \pmod p$ and $\ell_{(i)} \equiv 0 \pmod q$, $\ell_{(iv)} \equiv -1 \pmod p$ and $\ell_{(iv)} \equiv 1 \pmod q$, $\ell_{(v)} \equiv 1 \pmod p$ and $\ell_{(v)} \equiv 1 \pmod q$, $\ell_{(vi)} \equiv 0 \pmod p$ and $\ell_{(vi)} \equiv -2 \pmod q$. Let (e) be any of (i), (iv), (v) or (vi).

Remark 5.2.3. *Notice that* $\ell_{(i)} \equiv \ell_{(vi)} \pmod p$ *and* $\ell_{(iv)} \equiv \ell_{(v)} \pmod q$.

In this section, we will make our final reduction from four variables to two, a major success that helps to simplify the construction presented in Chapter 4. Recall that we let $\alpha = \zeta_n^{k_p q + k_q p}$ and $\beta = \zeta_n^{k_p q - k_q p}$. Let A, B be with the same assumptions above in (5.19) and (5.24). Since $D_{(e)}$ is a diagonal matrix for each dot product, we can expand all equations to

$$\overline{A_1} B_1 \alpha^{\ell_{(e)}} + \overline{A_2} B_2 \beta^{\ell_{(e)}} + A_2 \overline{B_2} \beta^{-\ell_{(e)}} + A_1 \overline{B_1} \alpha^{-\ell_{(e)}} = 0.$$

This equation must hold for all four of the asymmetric dot products. By grouping like terms, we rearrange to get

$$\overline{A_1} B_1 \alpha^{\ell_{(e)}} + A_1 \overline{B_1} \alpha^{-\ell_{(e)}} = -\left(\overline{A_2} B_2 \beta^{\ell_{(e)}} + A_2 \overline{B_2} \beta^{-\ell_{(e)}}\right).$$

Using the definition of a complex conjugate in Definition 2.5.2, we can see that this is equivalent to

$$\overline{A_1}B_1\alpha^{\ell(e)} + \overline{\overline{A_1}B_1\alpha^{\ell(e)}} = -\left(\overline{A_2}B_2\beta^{\ell(e)} + \overline{\overline{A_2}B_2\beta^{\ell(e)}}\right).$$

It follows, using our assumption in (5.24), that

$$\Re\left(\overline{A_1}B_1\alpha^{\ell(e)}\right) = -\Re\left(\overline{A_2}B_2\beta^{\ell(e)}\right). \tag{5.29}$$

for equations (i), (iv), (v) and (vi). In Figure 5.2 we can see that, because both terms have

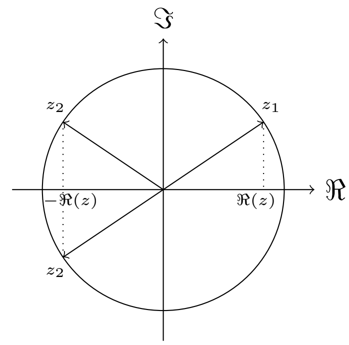

Figure 5.2: $\Re(z_1) = -\Re(z_2)$ on the complex plane.

the same norm, (5.29) implies there are two possibilities for the value of $arg\left(\overline{A_2}B_2\beta^{\ell(e)}\right)$ within $(-\pi, \pi]$. Specifically, we can choose exactly one of the two branches in the following equation.

$$arg\left(\overline{A_1}B_1\alpha^{\ell(e)}\right) = \pi \pm \arg(\overline{A_2}B_2\beta^{\ell(e)}).$$

This is equivalent to

$$arg\left(\overline{A_1}B_1\alpha^{\ell(e)}\right) = \pm arg\left(\overline{A_2}B_2\beta^{\ell(e)}\right) + (2m+1)\pi \tag{5.30}$$

for some integer m. Due to the periodic nature of the argument we must include m. As we will see shortly, m will cancel out prior to the final solutions and does not contribute to the main construction. We utilize the rule regarding the complex argument from Remark 2.5.4 to expand equation (5.30). We get

$$-\,arg\,(A_1) + arg\,(B_1) + arg\left(\alpha^{\ell(e)}\right) = \pm\left(-\arg(A_2) + \arg(B_2) + arg\left(\beta^{\ell(e)}\right)\right) + (2m+1)\pi$$

The arguments of $\alpha^{\ell(e)}$ and $\beta^{\ell(e)}$ are known and have the same form for each dot product. Therefore we substitute these values into the above relationship and collect free variables on the left hand side. We are left with

$$\pm\arg(A_2)-\arg(A_1)\mp\arg(B_2)+\arg(B_1)= \left[\pm\left(\frac{k_p}{p}+\frac{k_q}{q}\right)-\left(\frac{k_p}{p}-\frac{k_q}{q}\right)\right]2\pi\ell_{(e)}+(2m+1)\pi \tag{5.31}$$

where the top or bottom sign is taken consistently. We require that one branch of (5.31) be satisfied for each of the four asymmetric equations. In Remark (5.2.3), we noticed that there were two values of $\ell_{(e)}$'s in common between two pairs of the four asymmetric dot products. We will therefore consider $\ell_{(i)}$, $\ell_{(v)}$ and choose the signs which do not contradict one another. Hence we can get the following two equations in terms of the arguments.

$$-\arg(A_2)-\arg(A_1)+\arg(B_2)+\arg(B_1)=(2m+1)\pi \tag{5.32}$$

$$\arg(A_2)-\arg(A_1)-\arg(B_2)+\arg(B_1)=\frac{4\pi k_q}{q}+(2m+1)\pi \tag{5.33}$$

Even though we did not show that these values of $\ell_{(e)}$ satisfy all four equations, we will assume that this holds because the resulting simplifications survive the rigorous proofs in Chapter 4.

Taking the sum of the two equations (5.32) and (5.33) give us

$$-2\arg(A_1)+2\arg(B_1)=\left(\frac{2k_q}{q}+(2m+1)\right)2\pi.$$

We can solve this equation for $\arg(A_1)$ in terms of $\arg(B_1)$, which is reducing the number of variables from four to three.

$$\arg(A_1)=\arg(B_1)-\left(\frac{2k_q}{q}+2m+1\right)\pi. \tag{5.34}$$

Taking the difference of (5.32) and (5.33) gives us a relation involving $\arg(A_2)$ and $\arg(B_2)$. We can solve for $\arg(A_2)$ and reduce the number of variables from three to two.

$$-2\arg(A_2)+2\arg(B_2)=-\frac{4\pi k_q}{q}.$$

Then we have the following equation for $\arg(A_2)$ in terms of $\arg(B_2)$.

$$\arg(A_2)=\arg(B_2)+\frac{2\pi k_q}{q} \tag{5.35}$$

For any values $\arg(B_1)$ and $\arg(B_2)$, with fixed p, qk_p, k_q and m, we can calculate $\arg(A_1)$ and $\arg(A_2)$. By combining this reduction with the assumptions above, seen in (5.19) and (5.23), we have much simpler vectors A and B. By inputting equations (5.34) and (5.35) into (5.28), we get

$$A = \begin{pmatrix} Ce^{i\left(\arg(B_1)-\left(\frac{2k_q}{q}+1\right)\pi\right)} \\ e^{i\left(\arg(B_2)+\frac{2\pi k_q}{q}\right)} \\ e^{-i\left(\arg(B_2)+\frac{2\pi k_q}{q}\right)} \\ Ce^{-i\left(\arg(B_1)-\left(\frac{2k_q}{q}+1\right)\pi\right)} \end{pmatrix}, \; B = \begin{pmatrix} e^{i\cdot\arg(B_1)} \\ Ce^{i\cdot\arg(B_2)} \\ Ce^{-i\cdot\arg(B_2)} \\ e^{-i\cdot\arg(B_1)} \end{pmatrix}. \tag{5.36}$$

Using the roughly 1000 ORs for small values of n ($n = 15, 21, 33, 35, \ldots$), we plotted the values of $\arg(B_1)$ against $\arg(B_2)$. At this point, we found no other relationships to simplify the solutions A and B. Therefore we conjecture that the solutions have two free variables. This may be due to the fact that there are two independent rotation matrices in the Kronecker product. Recall that our linear transformations are in $\mathbb{R}^{4\times4}$. One of the rotation matrices acts on the first two dimensions and the second matrix acts on the last two dimensions. Then by taking the product of the two, we achieve a projection in four dimensions. This seems to explain why it is a system with 2 free variables. Regardless, we found no further relationship between $\arg(B_1)$ and $\arg(B_2)$. Therefore, we will now begin to undo all of the transformations and simplifications we made. By stepping backwards along this process, we will be able to define vectors A and B in terms of only two free variables, $\arg(B_1)$ and $\arg(B_2)$. Then we will undo the linear transformation by P^* to arrive at the original solutions (a, b), which will now be simplified down from eight variables to just two.

To undo the map P which was applied to a and b in (5.9), we use the relations $a = PA$ and $b = PB$. By expanding and reducing the vector components, we get the general form of a and b.

$$a = \begin{pmatrix} \Re\left(Ce^{i\left(\arg(B_1)-\left(\frac{2k_q}{q}+1\right)\pi\right)}\right) + \Re\left(e^{i\left(\arg(B_2)+\frac{2\pi k_q}{q}\right)}\right) \\ -\Im\left(Ce^{i\left(\arg(B_1)-\left(\frac{2k_q}{q}+1\right)\pi\right)}\right) + \Im\left(e^{i\left(\arg(B_2)+\frac{2\pi k_q}{q}\right)}\right) \\ -\Im\left(Ce^{i\left(\arg(B_1)-\left(\frac{2k_q}{q}+1\right)\pi\right)}\right) - \Im\left(e^{i\left(\arg(B_2)+\frac{2\pi k_q}{q}\right)}\right) \\ -\Re\left(Ce^{i\left(\arg(B_1)-\left(\frac{2k_q}{q}+1\right)\pi\right)}\right) + \Re\left(e^{i\left(\arg(B_2)+\frac{2\pi k_q}{q}\right)}\right) \end{pmatrix} \tag{5.37}$$

$$b = \begin{pmatrix} \Re\left(Ce^{i(\arg(B_1)}\right) + \Re\left(e^{i(\arg(B_2)}\right) \\ -\Im\left(Ce^{i(\arg(B_1)}\right) + \Im\left(e^{i(\arg(B_2)}\right) \\ -\Im\left(Ce^{i(\arg(B_1)}\right) - \Im\left(e^{i(\arg(B_2)}\right) \\ \Re\left(Ce^{i(\arg(B_1)}\right) - \Re\left(e^{i(\arg(B_2)}\right) \end{pmatrix} \tag{5.38}$$

Before we continue our simplification, notice that even though the elements of A, B and P are in general complex values, a and b will be real vectors as long as C is real. If we expand the real and imaginary parts of the vectors in (5.37) and (5.38), we get

$$a = \begin{pmatrix} C\cos\left(\arg(B_1) - \left(\frac{2k_q}{q}+1\right)\pi\right) + \cos\left(\arg(B_2) + \frac{2\pi k_q}{q}\right) \\ -C\sin\left(\arg(B_1) - \left(\frac{2k_q}{q}+1\right)\pi\right) + \sin\left(\arg(B_2) + \frac{2\pi k_q}{q}\right) \\ -C\sin\left(\arg(B_1) - \left(\frac{2k_q}{q}+1\right)\pi\right) - \sin\left(\arg(B_2) + \frac{2\pi k_q}{q}\right) \\ -C\cos\left(\arg(B_1) - \left(\frac{2k_q}{q}+1\right)\pi\right) + \cos\left(\arg(B_2) + \frac{2\pi k_q}{q}\right) \end{pmatrix} \tag{5.39}$$

$$b = \begin{pmatrix} C\cos(\arg(B_1)) + \cos(\arg(B_2)) \\ -C\sin(\arg(B_1)) + \sin(\arg(B_2)) \\ -C\sin(\arg(B_1)) - \sin(\arg(B_2)) \\ C\cos(\arg(B_1)) - \cos(\arg(B_2)) \end{pmatrix}. \tag{5.40}$$

Since we have freedom for the values of $\arg(B_1)$ and $\arg(B_2)$, we can arbitrarily choose them both to be zero. This might not be the best choice for our free variables, but it seems to simplify the vectors. Another choice could possibly result in simpler proofs of the construction in Chapter 4. For now we let $\arg(B_1) = \arg(B_2) = 0$. After simplifying, we are left with vectors which we used in our main construction in Theorem 4.1.1.

$$a = \begin{pmatrix} (1-C)\cos\left(\frac{2\pi k_q}{q}\right) \\ (1-C)\sin\left(\frac{2\pi k_q}{q}\right) \\ -(1+C)\sin\left(\frac{2\pi k_q}{q}\right) \\ (1+C)\cos\left(\frac{2\pi k_q}{q}\right) \end{pmatrix}, \quad b = \begin{pmatrix} C+1 \\ 0 \\ 0 \\ C-1 \end{pmatrix} \tag{5.41}$$

Notice that using all of these simplifications from the numerical data, we have reduced the number of variables in the model of KS sets from $8n$ variables to two complex arguments. This is an amazing result considering that when we began to develop the construction we were dealing with a varying number of variables, and now we need only a constant number of variables for any value n. Since we could not find any further relationships between the variables, this is where we stopped simplifying and brought the vectors into the main construction. Even though we based many of our reductions on numerical data, we have shown in Chapter 4 that the construction stands alone. We wanted to present the exact process we took to discover the computer-free construction.

5.3 Outlook

During the early days of our research, we applied some methods which were not used in the Kochen-Specker proofs outlined above. They may, however, provide further information and enticement for further research. Hence, in this section we will present the other approaches and some additional discoveries. A second method which we considered but did not use, is based on semidefinite programming formulation of the ORs. This work was done in parallel early in the research. We chose to use the continuous optimization formulation for our work as it seemed to be much easier to use and was better supported for high precision computations in the software available to us. We studied the Lovász ϑ value for our graphs. We also discuss some possible future projects which may be of interest to the reader.

5.3.1 Semidefinite Programming

This was another direction we began looking into, but it was not pursued to the same extent as the numerical method outlined above. In the beginning we considered multiple approaches to construct a KS set. We decided that the best approach was to collect lots of data of some kind and rigorously analyse it for patterns. We started on both methods, and to get more understanding of the ORs we did some research to see how the ORs of the line graph would behave [17].

Theorem 8 from [17] says that if a graph G is vertex transitive, then $\vartheta(G)\vartheta\left(\overline{G}\right) = |V(G)|$. Since our graph $G = L(CR_{n,c})$ is vertex transitive by Theorem 3.4.4, this holds for our graph. Lovász was also able to relate the theta number of a graph to the eigenvalues of its adjacency matrix. Theorem 6 of [17] shows that $\vartheta(G)$ is bounded by a function of the largest and smallest eigenvalues of G. Lastly, Theorem 11 of [17] says that if G admits an OR in dimension d, then the theta number of $\overline{G}$ is bounded above by 4. We were able to prove that $\vartheta\left(\overline{G}\right) = 4$ and $\vartheta\left(G\right) = \frac{n}{2}$. We proved the theta number of $\overline{G}$ by examining the eigenvalues of G and applying Theorem 6 of to bound the value above and Theorem 11 to bound it below. The theta value of G was proved by defining the primal and dual linear programming problems and finding optimal solutions that were equal.

We were also able to prove that, for our graph $G = L(CR_{n,c})$, that several of the bounds on $\vartheta\left(G\right)$ and $\vartheta\left(\overline{G}\right)$ in [17] are tight. Consider Lemma 3 and Theorem 10 from [17] which relate $\vartheta(G)$ to the independence number, Definition 2.1.11, and fractional packing number, Definition 2.1.13, respectively. Using the fact that $L(CR_{n,c})$ contains maximal cliques of size 4, we were able to show that $\alpha^*\left(\overline{G}\right) = 4$. Also, by relating the primal and dual linear programming solutions, we were able to show that $\alpha\left(G\right) = \frac{n}{2}$. Since these are exactly the theta numbers for these graphs which we mentioned above, these bounds are tight.

Since we observed that several inequalities in the Lovász paper [17] are tight for our family of graphs, this gives encouragement for studying these chordal ring graphs in the context of the semidefinite programming because apparently there exist some features which may assist in finding the ORs.

Our results about ϑ were motivated by our computations using a semidefinite program in Sage which computes the Lovász Theta number of a graph in polynomial time, from [19]. When we generated these values for graphs $L(CR_{n,c})$ for varying values of n and c, we saw that the numerical data agreed with the results above. However there arose possible issues with the precision of these results. Since Sage is a Python based language, the precision of the numerical calculations relies on the hardware of the computer being used at that time. Therefore, we were not able to work with the same level of precision as we had with Maple. Consider the multiple assumptions we made which were based entirely on the data computed with Maple. Numerical data found in this way will lose about half of its precision. If we were not able to increase the precision, we would be making these assumptions on a very small number of digits. By increasing the digits, were able to differentiate a true result from a coincidental result. Thus, with just the hardware precision, any conjectures we made on the data computed with Sage would have been made on between 5-10 digits of precision. Though they were not sufficient conditions, they were necessary. If we had failed these necessary conditions, we would have known to stop our other numerical method. We looked into this as a safeguard from spending time on something which led nowhere.

In the next section, we briefly discuss some future projects which stemmed from our work in this thesis. Hopefully these quick explanations of possible research will motivate a reader.

5.3.2 Future Research

There is a possibility that our choices of $\arg(B_1)$ and $\arg(B_2)$ being zero was not the simplest solution. This may depend on the particular measure of simplicity. The different choices of these arguments might lead to a simpler solution set (a, b) or simpler proofs of Theorem 4.1.1.

Recall that we presented a simplified form of the proofs for Theorem 4.1.1. Seeing that this alternate proof is possible, it would be interesting to try and unify the original proofs to fewer than six cases. This would not make any substantial difference to the result. We are expecting to submit our results to a journal shortly and this is a goal for that paper.

When we began this thesis, we set out to find an infinite family of KS sets in a fixed dimension. Not only were we able to find such a family of KS sets, but our family exists in the smallest possible dimension.

Bibliography

[1] Amaral, Barbara; Cunha, Marcelo Terra; Cabello, Adán; Quantum theory allows for absolute maximal contextuality. Phys. Rev. Lett. A 92 (2015), 062125.

[2] Amaral, Barbara; Cunha, Marcelo Terra; Cabello, Adán; The exclusivity principle forbids sets of correlations larger than the quantum set. Phys. Rev. Lett. A 89 (2014), 030101.

[3] Cabello, Adán; Estebaranz, José; García-Alcaine, Guillermo; Bell-Kochen-Specker theorem: A proof with 18 vectors. Phys. Rev. Lett. A 212 (1996), pg. 183–187.

[4] Cabello, Adán; Simple explanation of the quantum violation of a fundamental inequality. Phys. Rev. Lett. 110 (2013), 060402.

[5] Cañas, G.; Arias, M.; Etcheverry, S.; Gómez, E.S.; Cabello, A.; Xavier, G.B.; Lima, G.; Applying the simplest Kochen-Specker set for quantum information processing. Phys. Rev. Lett. 113 (2014), 090404.

[6] Diestel, Reinhard; *Graph Theory, 5th ed.* Graduate Texts in Mathematics. Vol. 173. Springer, Berlin, 1997.

[7] Ellingham, Mark; Plummer, Michael David; Yu, Gexin; Linkage for the diamond and the path with four vertices. Journal of Graph Theory 70 (2011), pg. 241–261.

[8] Gallian, Joseph; *Contemporary Abstract Algebra. Seventh Edition.* Brooks/Cole, Boston, 2010.

[9] Godsil, Chris; Royle, Gordon; *Algebraic Graph Theory.* Graduate Texts in Mathematics. Vol. 207. Springer, New York, 2001.

[10] Hardy, Yorick; Steeb, Willi-Hans; *Matrix Calculus and Kronecker Product: A Practical Approach to Linear and Multilinear Algebra. Second Edition.* World Scientific, 2011.

[11] Howard, Mark; Wallman, Joel; Veitch, Victor; Emerson, Joseph; Contextuality supplies the 'magic' for quantum computation. Nature 510 (2014), pg 351–355.

[12] Kochen, Simon; Specker, Ernst; The problem of hidden variables in quantum mechanics. Journal of Mathematics and Mechanics 17 (1967), pg. 59–87.

[13] Lay, David; *Linear Algebra and Its Applications. Third Edition.* Addison Wesley, 2003.

[14] Lisonek, Petr; Kochen-Specker sets and Hadamard matrices. To appear in Theoretical Computer Science (2018). (arXiv:1612.02901).

[15] Lisonek, Petr; Badziąg, Piotr; Portillo, José; Cabello, Adán; Kochen-Specker set with seven contexts. Phys. Rev. Lett. A 89 (2014), 042101.

[16] Lovász, László; *Graphs and Geometry*. Institute of Mathematics, Eötvös Loránd University and Hungarian Academy of Sciences, Budapest, Hungary. `https://web.cs.elte.hu/~lovasz/bookxx/geombook20-09-18.pdf`. Retrieved on December 17, 2018.

[17] Lovász, László; On the Shannon capacity of a graph. IEEE Transactions of Information Theory 25 (1979), no. 1, pg. 1–7.

[18] Bosma, Wieb; Cannon, John; Playoust, Catherine; The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (1997), pg 235–265.

[19] Pasechnik, Dima; Lovász theta-function of graphs. `doc.sagemath.org/html/en/reference/graphs/sage/graphs/lovasz_theta.html`, 2015. Retrieved on December 17, 2018.

[20] Pavičić, Mladen; Arbitrarily exhaustive hypergraph generation of 4-,6-,8-,16-, and 32-dimensional quantum contextual sets. Phys. Rev. Lett. A 95 (2017), 062121.

[21] Pavičić, Mladen; Megill, Norman; Merlet, Jean-Pierre; New Kochen-Specker sets in four dimensions. Phys. Rev. Lett. A 374 (2010), no. 21, pg. 2122–2128.

[22] Royle, Gordon; Graphs and Multigraphs. In: *Handbook of Combinatorial Designs*. Colbourn, Charles J.; Dinitz, Jeffrey H.; Eds. Chapman and Hall/CRC, 2006.

[23] Stinson, Douglas; *Cryptography: Theory and Practice. Third Edition*. Discrete Mathematics and its Applications. CRC Press, Boca Raton, 2006.

[24] West, Douglas; *Introduction to Graph Theory. Second Edition*. Prentice Hall, Upper Saddle River, New Jersey, 2001.

[25] White, Arthur; *Graphs of Groups on Surfaces*. Western Michigan University. Elsevier, Michigan, 2001.

Appendix A

Code

A.1 Optimizer

A sample of our Maple code implementing the objective function (5.1) and numerical search for ORs.

```
edges := [ seq( { (i mod v) + 1, ( (i + 1) mod v) + 1 } , i = 0..v-1 ),
           seq( { (i mod v) + 1, ( (i + c) mod v) + 1 } , i = 0..v-1 ) ]:

orthp := select( p -> ( nops( edges[p[1]] intersect edges[p[2]] ) > 0 ),
                 [ seq(seq([i,j],j=i+1..nops(edges)),i=1..nops(edges)) ] ):

objf := add( ( add( (v||j||i)^2 , i=1..d ) - 1   )^2 , j=1..n ) +
          add( ( dp( V[p[1]], V[p[2]] ) )^2 , p=orthp ):

ip:= initialpoint = { seq( va =r()/M, va=indets(objf) ) }:

  Digits := 10:
  while Digits < 100 do
      Val := 100:
      while not(is(Val<10^(-floor(Digits*(1/3))))) do
         opt := Minimize(objf, {}, ip, iterationlimit=10^5):
         Val := opt[1]:
         if Val>(10^(-floor(Digits*(1/3)))) then
            ip := initialpoint = { seq( va =r()/M, va=indets(objf) ) }:
         fi:
      od:
      ip := initialpoint = opt[2]:
      Digits := Digits+10
   od:
```