Cores of Vertex-Transitive Graphs

Ricky Rotheram

Submitted in total fulfilment of the requirements of the degree of Master of Philosophy

October 2013

Department of Mathematics and Statistics
The University of Melbourne
Parkville, VIC 3010, Australia

Produced on archival quality paper
Abstract

The core of a graph $\Gamma$ is the smallest graph $\Gamma^*$ for which there exist graph homomorphisms $\Gamma \to \Gamma^*$ and $\Gamma^* \to \Gamma$. Thus cores are fundamental to our understanding of general graph homomorphisms. It is known that for a vertex-transitive graph $\Gamma$, $\Gamma^*$ is vertex-transitive, and that $|V(\Gamma^*)|$ divides $|V(\Gamma)|$. The purpose of this thesis is to determine the cores of various families of vertex-transitive and symmetric graphs.

We focus primarily on finding the cores of imprimitive symmetric graphs of order $pq$, where $p < q$ are primes. We choose to investigate these graphs because their cores must be symmetric graphs with $|V(\Gamma^*)| = p$ or $q$. These graphs have been completely classified, and are split into three broad families, namely the circulants, the incidence graphs and the Marušič-Scapellato graphs. We use this classification to determine the cores of all imprimitive symmetric graphs of order $pq$, using different approaches for the circulants, the incidence graphs and the Marušič-Scapellato graphs.

Circulant graphs are examples of Cayley graphs of abelian groups. Thus, we generalise the approach used to determine the cores of the symmetric circulants of order $pq$, and apply it to other Cayley graphs of abelian groups. Doing this, we show that if $\Gamma$ is a Cayley graph of an abelian group, then $\text{Aut}(\Gamma^*)$ contains a transitive subgroup generated by semiregular automorphisms, and either $\Gamma^*$ is an odd cycle or $\text{girth}(\Gamma^*) \leq 4$. Consequently, we show that $\Gamma^*$ is not a cubic symmetric graph (unless $\Gamma^* \cong K_4$) or 3-arc-transitive (unless $\Gamma^*$ is an odd cycle). We also provide a partial confirmation of a conjecture by Samal, on the cores of Cayley graphs of elementary abelian groups.
Declaration

This is to certify that:

(i) the thesis comprises only my original work towards the MPhil;

(ii) due acknowledgement has been made in the text to all other material used; and

(iii) the thesis is less than 50 000 words in length.

Ricky Rotheram
Acknowledgements

My deepest and sincerest gratitude goes to my primary supervisor, Associate Professor Sanming Zhou, for his guidance and supervision throughout my work on this thesis. I am especially grateful to Sanming for introducing me to vertex-transitive and symmetric graphs, as well as graph homomorphisms and the cores of graphs. I also thank Sanming for being supportive during some difficult periods, both in my academic and personal lives.

I also wish to thank my co-supervisor, Professor Gordon Royle, for being a courteous host during my visit to the University of Western Australia in Semester 2 of 2010. I am especially grateful to Gordon for suggesting that I look at primitive Cayley graphs of elementary abelian groups. This suggestion led directly to Section 7.2, and specifically to Theorem 7.2.7.

I acknowledge the support of an Australian Postgraduate Award from the University of Melbourne.

Finally, I wish to thank my parents, who have provided me with constant encouragement and support over the course of my education. Without their support, this thesis could not have been finished.
List of Key Symbols

$\Omega, \Xi, \Delta$ Sets

$\Delta \subseteq \Omega$ $\Delta$ is a subset of $\Omega$

$\Delta \times \Xi$ Cartesian product of $\Delta$ and $\Xi$

$\Delta^l$ Cartesian product of $l$ copies of $\Delta$

$G, H, K$ Groups

$H \leq G$ $H$ is a subgroup of $G$

$H \trianglelefteq G$ $H$ is a normal subgroup of $G$

$\langle S \rangle$ Subgroup of $G$ generated by subset $S$

$1_G$ Identity element of $G$

$K \times H$ Direct product of $H$ by $K$

$K^l$ Direct product of $l$ copies of $K$

$K \rtimes H$ Semidirect product of $K$ by $H$

$K \wr H$ Wreath product of $K$ by $H$, with $H$ acting on $\Xi$

$G(\alpha)$ $G$-orbit containing $\alpha$

$G((\alpha, \beta))$ $G$-orbital containing $(\alpha, \beta)$

$G_\alpha$ Stabiliser of $\alpha$ in $G$
$G_\Delta$  Setwise stabiliser of $\Delta$ in $G$

$x(\Delta)$  Image of $\Delta$ under $x \in G$

$\text{Sym}(\Omega)$  Symmetric group of permutations of $\Omega$

$\text{Alt}(n)$  Alternating group

$\mathbb{Z}_n$  Additive group of integers mod $n$

$\mathbb{Z}_n^*$  Multiplicative group of integers mod $n$

$H(p, r)$  Unique subgroup of $\mathbb{Z}_p^*$ of order $r$

$\mathbb{Z}_p^l$  Elementary abelian group

$\text{GF}(n)$  Finite field with $n$ elements

$\text{GF}(n)^*$  Multiplicative group of $\text{GF}(n)$

$M_{10}, M_{11}, M_{22}, M_{23}$  Mathieu groups

$\text{SL}(n, q)$  Special linear group

$\text{Sp}(n, q)$  Symplectic group

$\text{GL}(n, q)$  General linear group

$\text{AGL}(n, q)$  Affine general linear group

$\Gamma\text{L}(n, q)$  Semilinear group

$\Gamma\text{Sp}(n, q)$  Symplectic semilinear group

$\text{PSL}(n, q)$  Projective special linear group

$\text{PSU}(n, q)$  Projective special unitary group

$\text{PSp}(n, q)$  Projective symplectic group

$\text{PΓSp}(n, q)$  Projective symplectic semilinear group

$H(11)$  Unique 2-$(11, 5, 2)$ design
$\text{PG}(d-1,n)$ $(d-1)$-dimensional projective space over $GF(n)$

$V(n,q)$ $n$-dimensional symplectic vector space over $GF(q)$

$W_{n-1}(q)$ Classical polar space with nondegenerate, alternating bilinear form on $V(n,q)$

$\Gamma, \Psi, \Lambda$ Graphs

$V(\Gamma)$ Vertex set of $\Gamma$

$E(\Gamma)$ Edge set of $\Gamma$

$A(\Gamma)$ Arc set of $\Gamma$

$N_{\Gamma}(u)$ Neighbourhood of $u$ in $\Gamma$

$\text{Aut}(\Gamma)$ Full automorphism group of $\Gamma$

$\phi, \psi$ Graph homomorphisms

$\phi(\Gamma)$ Homomorphic image of $\Gamma$ under $\phi$

$\phi^{-1}(u)$ Fibre of $\phi$

$\mathcal{P}$ Partition of $V(\Gamma)$

$\Gamma/\mathcal{P}$ Quotient graph of $\Gamma$ with respect to $\mathcal{P}$

$\Psi \leftrightarrow \Lambda$ $\Psi$ and $\Lambda$ are homomorphically equivalent

$\phi|_{\Lambda}$ Restriction of $\phi : V(\Gamma) \rightarrow V(\Lambda)$ to the subgraph $\Lambda$ of $\Gamma$

$\Gamma^*$ Core of $\Gamma$

$K_n$ Complete graph on $n$ vertices

$C_n$ Cycle of length $n$

$P_{n+1}$ Path of length $n$

$\overline{\Gamma}$ Complement of $\Gamma$
\( \overline{K}_n \)  Empty graph with \( n \) vertices

\( K(r, s) \)  Kneser graph for integers \( r, s \), with \( 1 \leq r < \frac{s}{2} \)

\( \Psi_r \)  Circular graph for integers \( r, s \) with \( 0 < r \leq s \)

\( \text{val}(\Gamma) \)  Valency of the regular graph \( \Gamma \)

\( \alpha(\Gamma) \)  Independence number of \( \Gamma \)

\( \mathcal{I}(\Gamma) \)  Set of all independent sets of \( \Gamma \)

\( \mathcal{I}(\Gamma, x) \)  Set of all independent sets of \( \Gamma \) containing vertex \( x \)

\( \omega(\Gamma) \)  Clique number of \( \Gamma \)

\( \delta(\Gamma, t) \)  Maximum number of vertices in an induced subgraph of \( \Gamma \) with no complete subgraph of order \( t \)

\( d_{\Gamma}(u, v) \)  Distance between \( u \) and \( v \) in \( \Gamma \)

\( \text{diam}(\Gamma) \)  Diameter of \( \Gamma \)

\( \text{girth}(\Gamma) \)  Girth of \( \Gamma \)

\( \text{oddg}(\Gamma) \)  Odd-girth of \( \Gamma \)

\( \chi(\Gamma) \)  Chromatic number of \( \Gamma \)

\( \chi_C(\Gamma) \)  Circular chromatic number of \( \Gamma \)

\( \chi_f(\Gamma) \)  Fractional chromatic number of \( \Gamma \)

\( \Gamma \square \Psi \)  Cartesian product of \( \Gamma \) and \( \Psi \)

\( \Gamma \times \Psi \)  Categorical product of \( \Gamma \) and \( \Psi \)

\( \Gamma \boxtimes \Psi \)  Strong product of \( \Gamma \) and \( \Psi \)

\( \Gamma[\Psi] \)  Lexicographic product of \( \Gamma \) and \( \Psi \)

\( \Psi[\Lambda] - d\Psi \)  Deleted lexicographic product of \( \Psi \) and \( \Lambda \)
\( \Box_{i=1}^n \Gamma_i \) Cartesian product of \( n \) graphs
\( \times_{i=1}^n \Gamma_i \) Categorical product of \( n \) graphs
\( \boxtimes_{i=1}^n \Gamma_i \) Strong product of \( n \) graphs
\( \Gamma^n \) \( n \)-th power of \( \Gamma \) with respect to the categorical product
\( \text{Cay}(G, S) \) Cayley graph of group \( G, S \subset G \)
\( G(p, r) \) Symmetric circulant of order \( p \) (where \( p \) is prime), valency \( r \)
\( G(2q, r) \) Bipartite, symmetric circulant
\( G(pq; r, s, u) \) General symmetric circulant of order \( pq \)
\( \mathcal{D} \) \( t - (v, k, \lambda) \) design
\( \mathcal{P} \) Set of points of design \( \mathcal{D} \)
\( \mathcal{B} \) Set of blocks of design \( \mathcal{D} \)
\( X(\mathcal{D}) \) Incidence graph of design \( \mathcal{D} \)
\( X'(\mathcal{D}) \) Complementary incidence graph of design \( \mathcal{D} \)
\( \Gamma(a, m, S, U) \) Marušič-Scapellato graph of order \( m(2^a + 1) \)
\( \Sigma \) System of imprimitivity of \( V(\Gamma) \), with \( \Gamma \cong \Gamma(a, m, S, U) \), under \( \text{SL}(2, 2^a) \leq \text{Aut}(\Gamma) \)
\( B_x \) Block of \( \Sigma \) containing all vertices \( (x, r) \), with \( x \in \text{PG}(1, 2^a) \)
\( F_s \) Fermat number
List of Tables

4.1 Symmetric Circulant Graphs of order $pq$, $p < q$, and their Cores . . . 43
4.2 Incidence and Marušič-Scapellato Graphs of order $pq$, $p < q$, and
their Cores . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 44
List of Figures

2.1 The categorical product $C_5 \times K_3$. ................................. 15
2.2 The lexicographic product $C_5 [K_3]$. ................................. 16
2.3 The deleted lexicographic product $C_5 [K_3] - 3C_5$. ................................. 18

4.1 The symmetric prime order circulant $G(13, 4)$. ................................. 45
4.2 The symmetric circulant $G(21; 3, 2, 6)$, with $t = 3$, $a = 2$ and $c = 2$ ................................. 48
4.3 The Marušič-Scapellato graph $\Gamma(2, 3, \emptyset, \{0\})$. ................................. 52
Contents

List of Key Symbols .............................................. i
List of Tables .................................................. vi
List of Figures .................................................. vii

1 Introduction .................................................. 1
  1.1 Introduction ............................................. 1
  1.2 Problems to be studied .................................. 2
  1.3 Main results and structure of the thesis ............... 3

2 Notation, definitions and preliminaries .................... 6
  2.1 Permutation groups, partitions, blocks and primitivity .... 6
  2.2 Graphs .................................................. 11
  2.3 Graph homomorphisms ................................... 19
    2.3.1 General graph homomorphisms ....................... 19
    2.3.2 Retractions, cores and homomorphic equivalence .... 21
    2.3.3 Homomorphisms of vertex-transitive graphs .......... 23
    2.3.4 Cores of graph products ............................ 26

3 Literature review ............................................ 28
  3.1 Graph homomorphisms ................................... 29
    3.1.1 Existence and nonexistence of graph homomorphisms .... 29
    3.1.2 Circular colourings .................................. 30
    3.1.3 Fractional colourings ................................ 32
    3.1.4 Graph products ...................................... 34
  3.2 Retracts and cores ....................................... 37
    3.2.1 General retracts and cores .......................... 37
### 3.2.2 Retracts and cores of vertex-transitive graphs

3.2.3 Retracts and cores of graph products

### 4 Cores of imprimitive, symmetric \( pq \) graphs

4.1 Imprimitive symmetric graphs of order \( pq \), and their cores

4.2 Symmetric circulants of orders \( p \) and \( pq \)

4.3 Incidence Graphs

4.4 Marušič-Scapellato graphs

4.4.1 Imprimitive Marušič-Scapellato graphs

4.4.2 Primitive Marušič-Scapellato graphs

### 5 Circulant Graphs

5.1 Lexicographic products and \( G(2q, r) \)

5.2 Deleted lexicographic products and categorical products

5.3 \( G(pq; r, s, u) \)

5.3.1 Categorical products

5.3.2 Candidates for core when \( t \notin H(q, r) \)

5.3.3 Core when \( t \notin H(q, r) \)

### 6 Marušič-Scapellato graphs

6.1 When \( |V(\Gamma^*)| = q \)

6.2 Bounding the clique number

6.3 Bounding the independence number

6.4 Cores of Marušič-Scapellato graphs

### 7 Cayley graphs of abelian groups

7.1 Cores of Cayley graphs of abelian groups

7.2 Primitive cores with prime power order

7.2.1 Primitive groups of prime power degree

7.2.2 Cayley graphs of abelian groups with primitive cores of prime power order
8 Conclusions

8.1 Summary of thesis ............................................. 102
8.2 Future work ..................................................... 103
  8.2.1 Symmetric graphs of orders $pq$, $p^2$ and $p^3$ .......... 103
  8.2.2 Cayley graphs of abelian groups .......................... 104
Chapter 1

Introduction

1.1 Introduction

A prominent field in the theory of graphs is Algebraic Graph Theory, which broadly speaking, is the application of various techniques from Algebra to the study of graphs. By definition, a finite graph $\Gamma$ consists of a nonempty set $V(\Gamma)$, known as the vertex set, and an edge set $E(\Gamma)$, whose elements are unordered pairs of distinct elements of $V(\Gamma)$ (if there exists an edge between two vertices, then these vertices are said to be adjacent). Each edge $[x, y]$ gives rise to two ordered pairs, $(x, y)$ and $(y, x)$, which are called arcs of $\Gamma$. The set of arcs of $\Gamma$ is denoted by $A(\Gamma)$.

Graph homomorphisms are a subbranch of Algebraic Graph Theory, and they have many useful applications to the study of graphs. By definition, for two graphs $\Gamma$ and $\Psi$, a homomorphism from $\Gamma$ to $\Psi$ is a map $\phi : V(\Gamma) \to V(\Psi)$, such that for each pair $x, y \in V(\Gamma)$, $\phi(x)$ and $\phi(y)$ are adjacent in $\Psi$ whenever $x$ and $y$ are adjacent in $\Gamma$.

A lot of research into graph homomorphisms focuses on three specific types of homomorphism and their applications. The first of these homomorphisms is the graph isomorphism, which is a means of determining equivalence between two graphs. The second type of homomorphism is the graph colouring, which can be viewed as a homomorphism from a graph to a complete graph. And the third type of homomorphism is the graph automorphism, which is an adjacency-preserving permutation of the vertex set of the graph.
Graph automorphisms are particularly significant as they allow the application of Permutation Group Theory to the study of graphs. With this application in mind, a graph $\Gamma$ is said to be $G$-vertex-transitive if $\Gamma$ admits $G$ as a group of automorphisms such that $G$ is transitive on $V(\Gamma)$. If $\Gamma$ admits $G$ as a group of automorphisms such that $G$ is transitive on $A(\Gamma)$, then $\Gamma$ is said to be a $G$-symmetric graph. If in addition to being $G$-vertex-transitive, $V(\Gamma)$ admits a nontrivial $G$-invariant partition, then $\Gamma$ is said to be a $G$-imprimitive graph. If the only $G$-invariant partitions of $V(\Gamma)$ are the trivial partitions, then $\Gamma$ is said to be a $G$-primitive graph.

The purpose of this thesis is to study another type of graph homomorphism, known as a retraction, for vertex-transitive and symmetric graphs. By definition, a retraction $\phi$ is a homomorphism from a graph $\Gamma$ onto an induced subgraph $\Psi$, for which the restriction of $\phi$ to $V(\Psi)$ is the identity map; in this case the subgraph $\Psi$ is called a retract of $\Gamma$. If a graph has no nontrivial retracts, then it is called a core. If a graph has nontrivial retracts, then the minimal retracts of the graph are cores. Importantly, every graph has minimal retracts, which are unique up to isomorphism. Thus for a graph $\Gamma$, we refer to any minimal retract as the core of $\Gamma$, which we denote by $\Gamma^*$.

We are interested in retracts because the core of a graph inherits many of the structural properties of the graph, notably the chromatic number and the odd-girth. Hence, many questions about a given graph $\Gamma$ can be simplified by focusing on $\Gamma^*$, provided that $\Gamma^*$ is known. Thus throughout this thesis, an emphasis will be placed on finding vertex-transitive and symmetric graphs which are cores, and in the event that a graph is not a core, in determining the core of that graph.

1.2 Problems to be studied

Usually, finding the core of a given graph is difficult. However, results exist which allow us to at least narrow the search for potential cores. One such result states that, for any vertex-transitive $\Gamma$, $\Gamma^*$ is vertex-transitive. Likewise, if $\Gamma$ is symmetric, $\Gamma^*$ is symmetric. Another result states that, for any vertex-transitive graph $\Gamma$, the number of vertices of $\Gamma^*$ divides the number of vertices of $\Gamma$. Likewise, if $\Gamma$ is symmetric, the number of arcs of $\Gamma^*$ divides the number of arcs of $\Gamma$. As a consequence, if $\Gamma$ is a vertex-transitive graph with a prime number of vertices, or a symmetric graph with
CHAPTER 1. INTRODUCTION

a prime number of arcs, then $\Gamma$ is a core.

These results suggest the possibility of determining the cores of symmetric graphs of small vertex order, or with vertex order containing a small number of prime factors. This idea constitutes the main focus of this thesis.

Problem 1.2.1 Determine the cores of all symmetric graphs whose order is the product of two primes.

Problem 1.2.1 appears feasible for two reasons. The first reason is the classifications of symmetric graphs of prime order and of order the product of two primes given in [8, 10, 61, 62, 81]. And the second reason is that symmetric graphs are a smaller family of graphs than the more general vertex-transitive graphs.

Following on from Problem 1.2.1, a natural question to ask is, do the techniques developed in determining the cores of symmetric graphs of order $pq$ generalise to graphs of other orders?

Research direction 1.2.2 Use the techniques developed in the investigation into Problem 1.2.1 to determine the cores of various families of vertex-transitive graphs.

In particular, we apply these techniques to a conjecture first stated by Samal.

Conjecture 1.2.3 ([70]) Let $\Gamma$ be isomorphic to a Cayley graph of an elementary abelian group. Then $\Gamma^*$ is isomorphic to a Cayley graph of an elementary abelian group.

1.3 Main results and structure of the thesis

This thesis is divided into two parts. The first part, which consists of the first three chapters, is a broad introduction to the thesis.

In Chapter 2 the notation, definitions and preliminary results required throughout this thesis are introduced. This chapter is split into three sections, which cover Permutation Groups, Graphs and Graph Homomorphisms.

In Chapter 3 we provide a literature review of graph homomorphisms, with a focus on retractions and cores of graphs. However, this literature review does not
CHAPTER 1. INTRODUCTION

cover either graph automorphisms or isomorphisms (even though both are special types of homomorphism), as each of these areas is quite broad and distinct from the study of general graph homomorphisms.

The second part, which is covered by Chapters 4, 5, 6 and 7, constitutes the main results of this thesis. In Chapter 4 we focus on the first step in answering Problem 1.2.1, that is to determine the cores of all imprimitive, symmetric graphs of order $pq$, where $p < q$ are primes.

Beginning with Section 4.1, the classification of imprimitive symmetric graphs of order $pq$ is stated in Theorem 4.1.1, along with Theorem 4.1.2, which gives the core of every imprimitive symmetric graph of order $pq$ (provided that certain necessary and sufficient conditions are met). In Sections 4.2, 4.3 and 4.4 we define each of the three classes of imprimitive, symmetric $pq$ graphs from Theorem 4.1.1 (namely the circulants, incidence graphs and Marușić-Scapellato graphs respectively). Further, since finding the cores of symmetric incidence graphs is relatively simple, their cores are determined in Section 4.3. To complete the proof of Theorem 4.1.2, the cores of all symmetric circulants and Marușić-Scapellato graphs are determined in Chapters 5 and 6 respectively.

In Chapter 7, the techniques developed in Chapter 5 are extended to other families of vertex-transitive graphs. In particular, during the proof of Theorem 5.3.7, the cores of some specific circulants are shown to have semiregular automorphisms. In Section 7.1 we develop this idea further, and show in Lemma 7.1.1 that if $\Gamma$ is isomorphic to a Cayley graph of an abelian group, then $\Gamma^*$ has semiregular automorphisms. Also in Lemma 7.1.1, these semiregular automorphisms are used to provide additional information on the automorphism group of $\Gamma^*$.

Lemma 7.1.1 is then used to prove Theorem 7.1.2, which is an upper bound on the girth of $\Gamma^*$, when $\Gamma^*$ is not an odd cycle. From Theorem 7.1.2, we prove Corollaries 7.1.3 and 7.1.5, which determine $\Gamma^*$ when $\Gamma$ is nonbipartite, and $\Gamma^*$ is either a cubic symmetric graph or a 3-arc-transitive graph.

In Section 7.2 we focus on graphs whose cores are primitive graphs. Specifically, Theorem 7.2.7 states that if a graph $\Gamma$ is isomorphic to a Cayley graph of an abelian group and $\Gamma^*$ is a primitive graph with $|V(\Gamma^*)| = p^n$ for a prime $p \neq 3$, then $\Gamma^*$ is isomorphic to a Cayley graph of an elementary abelian group. From Theorem 7.2.7 we obtain Corollary 7.2.8, which partially confirms Conjecture 1.2.3.
We conclude the thesis with Chapter 8, which contains a summary of the main results achieved (Section 8.1), along with some suggestions for future work (Section 8.2).
Chapter 2

Notation, definitions and preliminaries

In this chapter we present the required definitions and results on permutation groups, graphs and graph homomorphisms.

2.1 Permutation groups, partitions, blocks and primitivity

Let Ω be a nonempty set, the elements of which are called points. A bijection from Ω onto itself is called a permutation of Ω, and the set of all permutations of Ω forms a group under the composition of mappings. This group is called the symmetric group, and is denoted by Sym(Ω) (or Sym(n) if |Ω| = n). Any subgroup G of Sym(Ω) is naturally a group of permutations of Ω, and G is called a permutation group. If |Ω| = n, then G is said to be a permutation group of degree n.

Let G be a group and Ω be a nonempty set, such that for each α ∈ Ω and x ∈ G, there exists a mapping (x, α) → x(α) from G × Ω into Ω. We say that this mapping defines an action of G on Ω, or that G acts on Ω, if:

(i) 1_G(α) = α for all α ∈ Ω, where 1_G is the identity element of G; and

(ii) y(x(α)) = (yx)(α) for all α ∈ Ω and all x, y ∈ G.
The degree of the action of $G$ on $\Omega$ is $|\Omega|$. An element $x \in G$ is said to fix a point $\alpha \in \Omega$ if $x(\alpha) = \alpha$.

Note: many authors use different notation for a group action than the notation in this thesis. In particular, it is common to see the group acting on a set from the right rather than from the left. We choose our notation for a group action to ensure consistency with the notation used for graph homomorphisms in Section 2.3.

**Example 2.1.1** Every subgroup $G$ of $\text{Sym}(\Omega)$ acts naturally on $\Omega$, where $x(\alpha)$ is the image of $\alpha$ under the permutation $x$. Except when explicitly stated otherwise, we assume that this is the action we are dealing with whenever we have a permutation group.

Suppose a group $G$ acts on the nonempty set $\Omega$. Then for each element $x \in G$, there exists a mapping $\pi : \Omega \to \Omega$ defined by $\pi(\alpha) := x(\alpha)$. The map $\pi$ has an inverse $x^{-1}$, so that $\pi$ is a bijection, and thus a permutation of $\Omega$. Therefore there exists a mapping $\rho : G \to \text{Sym}(\Omega)$ defined by $\rho(x) := \pi$, which is a group homomorphism by Properties (i) and (ii) for a group action. This homomorphism is known as a permutation representation of $G$ on $\Omega$. The kernel of $\rho$ is the kernel of the action of $G$ on $\Omega$, and is defined as the subgroup of $G$ which contains all of the permutations which fix every element of $\Omega$. If the kernel of this action contains only the identity element of $G$, then $G$ is said to be faithful in its action on $\Omega$ (or is said to act faithfully).

The action of the group $G$ on the set $\Omega$ moves each point in $\Omega$ to various other points in $\Omega$. For a given point $\alpha \in \Omega$, the set of these images is called the orbit of $\alpha$ under $G$ (also known as a $G$-orbit), and is denoted by

$$G(\alpha) := \{x(\alpha) \mid x \in G \}.$$  

If the group $G$ acts on the set $\Omega$, then $G$ acts on the set $\Omega \times \Omega$ via the map $x((\alpha, \beta)) := (x(\alpha), x(\beta))$ for $x \in G$ and $\alpha, \beta \in \Omega$. We define the $G$-orbitals to be the $G$-orbits on $\Omega \times \Omega$, where the $G$-orbital for $(\alpha, \beta)$ is denoted by

$$G((\alpha, \beta)) := \{ (x(\alpha), x(\beta)) \mid x \in G \}.$$
Given $\alpha \in \Omega$, the subset
\[ G_\alpha := \{ x \in G \mid x(\alpha) = \alpha \} \]
of $G$ is a subgroup of $G$, called the stabiliser of $\alpha$ in $G$.

**Theorem 2.1.2 ([13, Theorem 1.4A])** Suppose that $G$ is a group acting on a set $\Omega$ and that $x, y \in G$ and $\alpha, \beta \in \Omega$. Then:

(i) Two orbits $G(\alpha)$ and $G(\beta)$ are either equal (as sets) or disjoint.

(ii) The stabiliser $G_\alpha$ is a subgroup of $G$ and $G_\beta = xG_\alpha x^{-1}$ whenever $\beta = x(\alpha)$. Moreover, $x(\alpha) = y(\alpha)$ if and only if $xG_\alpha = yG_\alpha$.

(iii) (The orbit-stabiliser lemma) $|G(\alpha)| = |G : G_\alpha|$ for all $\alpha \in \Omega$. In particular, if $G$ is finite then $|G(\alpha)| |G_\alpha| = |G|$.

If the group $G$ acting on $\Omega$ has only one orbit (that is, $G(\alpha) = \Omega$ for all $\alpha \in \Omega$), then $G$ is said to be transitive on $\Omega$. If $G$ has more than one orbit it is said to be intransitive. Equivalently, a group is transitive if for every pair of points $\alpha, \beta \in \Omega$ there exists some $x \in G$ such that $x(\alpha) = \beta$. If an element $x \in G$ does not fix any element of $\Omega$, $x$ is said to be semiregular. If every nonidentity element of $G$ is semiregular (that is, $G_\alpha = 1_G$ for all $\alpha \in \Omega$), then $G$ is said to be semiregular on $\Omega$. If $G$ acts both transitively and semiregularly on $\Omega$, we say that $G$ is regular on $\Omega$. If $G$ is transitive but nonregular on $\Omega$, and for any two distinct elements $\alpha, \beta \in \Omega$, $G_\alpha \cap G_\beta = 1_G$, then $G$ is called a Frobenius group acting on $\Omega$.

**Corollary 2.1.3 ([13, Corollary 1.4A])** Suppose that a group $G$ is transitive on a set $\Omega$. Then:

(i) The stabilisers $G_\alpha$ ($\alpha \in \Omega$) form a single conjugacy class of subgroups of $G$.

(ii) The index $|G : G_\alpha| = |\Omega|$ for each $\alpha$.

(iii) If $G$ is finite then the action of $G$ is regular if and only if $|G| = |\Omega|$.
For any subset $\Delta$ of $\Omega$ and $x \in G$, we define
\[ x(\Delta) := \{ x(\alpha) \mid \alpha \in \Delta \} . \]

A *partition* of a set $\Omega$ is a set $\mathcal{B}$ of subsets of $\Omega$ such that $\bigcup_{B \in \mathcal{B}} B = \Omega$, and for distinct $B, C \in \mathcal{B}$, $B \cap C = \emptyset$. The elements of $\mathcal{B}$ are called *blocks*, and if $\mathcal{B}$ has $n$ blocks then it is said to be an $n$-partition of $\Omega$. Two obvious partitions of $\Omega$ are $\{\Omega\}$ and $\{\{\alpha\} \mid \alpha \in \Omega\}$, which are known as the *trivial partitions* of $\Omega$. For any group $G$ acting on $\Omega$, the set of $G$-orbits is a partition of $\Omega$ by Theorem 2.1.2.

Let $\mathcal{B}$ be a partition of $\Omega$ and let $G$ act on $\Omega$. If $x(B) \in \mathcal{B}$ for all $B \in \mathcal{B}$ and $x \in G$ (so that $G$ permutes the blocks of $\mathcal{B}$ blockwise), then $\mathcal{B}$ is said to be $G$-invariant. The trivial partitions are naturally $G$-invariant. For $N \trianglelefteq G$, the $N$-orbits provide a $G$-invariant partition of $\Omega$.

**Lemma 2.1.4 ([60, Lemma 10.1])** Let $G$ be a permutation group on a set $\Omega$, and let $N$ be a normal subgroup of $G$. Then the set $\mathcal{B}_N$ of $N$-orbits in $\Omega$ is a $G$-invariant partition of $\Omega$.

Now let $G$ be a transitive group acting on $\Omega$. If the trivial partitions are the only $G$-invariant partitions of $\Omega$, then $G$ is said to be *primitive* on $\Omega$; otherwise $G$ is said to be *imprimitive* on $\Omega$. A subset $\Delta$ of $\Omega$ is called a *block of imprimitivity* if, for all $x \in G$, either $x(\Delta) = \Delta$ or $x(\Delta) \cap \Delta = \emptyset$. Clearly every block $B \in \mathcal{B}$ in a $G$-invariant partition $\mathcal{B}$ of $\Omega$ is a block of imprimitivity. Conversely, any block of imprimitivity $\Delta$ of the action of $G$ on $\Omega$ induces a $G$-invariant partition $\{x(\Delta) \mid x \in G\}$, and thus each block of imprimitivity is a block of a $G$-invariant partition. So for a transitive group $G$ acting on $\Omega$, a partition $\mathcal{B}$ of $\Omega$ is $G$-invariant if and only if each block of $\mathcal{B}$ is a block of imprimitivity. Thus $G$ is primitive on $\Omega$ if and only if the blocks of imprimitivity of $G$ in $\Omega$ are the trivial blocks. We refer to $\mathcal{B}$ as a *system of imprimitivity*.

For any subset $\Delta$ of $\Omega$, the *setwise stabiliser* of $\Delta$ in $G$ is defined by
\[ G_\Delta := \{ x \in G \mid x(\Delta) = \Delta \} . \]

Like the point stabiliser, the setwise stabiliser is a subgroup of $G$, and in particular if $\Delta = \{\alpha\}$ for some $\alpha \in \Omega$, then $G_\Delta = G_\alpha$. For a $G$-invariant partition $\mathcal{B}$ of $\Omega$ with
\( B \in \mathcal{B} \), if \( \alpha \in B \) then \( G_\alpha \leq G_B \). Conversely, for any \( H \) such that \( G_\alpha \leq H \leq G \), the \( H \)-orbit \( B := H(\alpha) \) is a block of imprimitivity for \( G \) in \( \Omega \), and thus induces a \( G \)-invariant partition of \( \Omega \), namely \( \mathcal{B} := \{ x(B) \mid x \in G \} \). Further, the lattice of \( G \)-invariant partitions is isomorphic to the lattice of subgroups of \( G \) containing \( G_\alpha \); hence \( G \) is primitive on \( \Omega \) if and only if \( G_\alpha \) is a maximal subgroup of \( G \).

Let \( H \) and \( K \) be groups. We define the \textit{direct product of \( H \) by \( K \)} to be the group
\[
D := \{ (u, x) \mid u \in K, x \in H \},
\]
with the product
\[
(u, x)(v, y) := (uv, xy)
\]
for all \( (u, x), (v, y) \in D \). We denote \( D \) by \( K \times H \).

We see that \( D \) contains the normal subgroups \( K^* := \{ (u, 1_H) \mid u \in K \} \cong K \) and \( H^* := \{ (1_K, x) \mid x \in H \} \cong H \), where \( D = K^*H^* \) and \( K^* \cap H^* = 1_D \).

Now let \( H \) and \( K \) be groups with \( H \) acting on \( K \), so that for each \( x \in H \) the mapping \( u \mapsto x(u) \) is an automorphism of \( K \). We define the \textit{semidirect product of \( K \) by \( H \)} to be the group
\[
S := \{ (u, x) \mid u \in K, x \in H \},
\]
with the product
\[
(u, x)(v, y) := (ux(v), xy)
\]
for all \( (u, x), (v, y) \in S \). We denote \( S \) by \( K \rtimes H \). We see that \( S \) contains the subgroups \( K^* := \{ (u, 1_H) \mid u \in K \} \) and \( H^* := \{ (1_K, x) \mid x \in H \} \), which are isomorphic to \( H \) and \( K \) respectively, and that \( S = K^*H^* \) with \( K^* \cap H^* = 1_S \). Moreover, \( K^* \subseteq S \), but \( H^* \) is not always normal in \( S \). When \( H^* \) is normal in \( S \), \( S \) is the direct product of \( H \) and \( K \).

Now let \( K \) and \( H \) be finite groups, where \( H \) acts on the finite nonempty set \( \Xi = \{ 1, 2, \ldots, l \} \), and let \( B = \prod_{\xi \in \Xi} K_\xi \), where \( K_\xi \cong K \) for all \( \xi \in \Xi \) (\( B \cong K^l \), the direct product of \( K \) with \( l \) factors). Then the \textit{wreath product of \( K \) by \( H \)} is defined as the semidirect product \( B \rtimes H \), where \( H \) acts on \( B \) via
\[
x((b_1, \ldots, b_l)) := (b_{x(1)}, \ldots, b_{x(l)})
\]
for all \((b_1, \ldots, b_l) \in B\) and \(x \in H\). The wreath product is denoted by \(K \wr H\).

Wreath products are useful as they provide a means of constructing both imprimitive and primitive permutation groups.

**Example 2.1.5** Let \(K\) be a group acting on \(\Delta\), \(H\) be a group acting on \(\Xi\) and \(W := K \wr H\). Then for \(b = (b_1, \ldots, b_l) \in B\), \(w = (b, x) \in W\) we define an action of \(W\) on the set \(\Delta \times \Xi\) by

\[
w((\delta, \xi)) := (b_{x(\xi)}(\delta), x(\xi))\text{ for all } (\delta, \xi) \in \Delta \times \Xi.
\]

**Example 2.1.6** Let \(K\) be a group acting on a finite set \(\Delta\), \(H\) be a group acting on \(\Xi = \{1, 2, \ldots, l\}\), \(W := K \wr H\) and \(\Delta^l\). Then for \(b = (b_1, \ldots, b_l) \in B\), \(w = (b, x) \in W\) and \((\delta_1, \ldots, \delta_l) \in \Delta^l\) we define an action of \(W\) on the set \(\Delta^l\) by

\[
w(\delta_\xi) := b_{x^{-1}(\xi)}(\delta_{x^{-1}(\xi)})\text{ for all } \xi \in \Xi.
\]

We call the action of \(W\) on \(\Delta^l\) in Example 2.1.6 the **product action** of the wreath product. A wreath product with the product action is primitive, under certain conditions.

**Lemma 2.1.7** ([13, Lemma 2.7A]) Suppose that \(H\) and \(K\) are nontrivial groups acting on finite sets \(\Xi = \{1, 2, \ldots, l\}\) and \(\Delta\) respectively. Then the wreath product \(W := H \wr K\) is primitive in the product action on \(\Delta^l\) if and only if:

(i) \(K\) acts primitively but not regularly on \(\Delta\);

(ii) \(H\) acts transitively on \(\Xi\).

For more on permutation groups, see [13,60].

### 2.2 Graphs

A finite **graph** \(\Gamma\) is a pair of sets \((V, E)\), where \(V\) is a finite nonempty set of elements called **vertices**, and \(E\) is a set of unordered pairs of distinct vertices called **edges**. The sets \(V\) and \(E\) are called the **vertex set** and the **edge set** of \(\Gamma\), which we denote
by \( V(\Gamma) \) and \( E(\Gamma) \) respectively. The order of a graph is the size of the vertex set. An \( s \)-arc is an \((s+1)\)-tuple \((u_0, u_1, \ldots, u_s)\) of vertices of a graph \( \Gamma \) such that there exists an edge between vertices \( u_{i-1} \) and \( u_i \) for \( 1 \leq i \leq s \), and \( u_{i-1} \neq u_{i+1} \) for \( 1 \leq i \leq s - 1 \). A 1-arc is called an arc, and the set of all arcs is denoted by \( A(\Gamma) \).

If a pair of vertices \( u, v \) of \( \Gamma \) gives an edge, we denote the edge by \([u,v]\). A nonedge is a distinct pair of unordered vertices \( u \) and \( v \) for which \([u,v] \notin E(\Gamma)\). If \([u,v] \in E(\Gamma)\), we say that \( u \) joins \( v \), and that \([u,v]\) is incident with both \( u \) and \( v \). Further, \( u \) and \( v \) are said to be adjacent, or neighbours of each other. Thus for \( u \in V(\Gamma) \), the set of all adjacent vertices is the neighbourhood of \( u \), which we denote by \( N_\Gamma(u) \). The valency of \( u \) in \( \Gamma \) is the size of \( N_\Gamma(u) \). If all vertices of \( \Gamma \) have the same valency, then \( \Gamma \) is regular. When \( \Gamma \) is regular, the common valency is called the valency of \( \Gamma \), and is denoted by \( \text{val}(\Gamma) \).

A graph is complete if every pair of distinct vertices are adjacent; we denote the complete graph on \( n \) vertices by \( K_n \). A graph is empty if every pair of vertices are nonadjacent. For a graph \( \Gamma \), the complement \( \overline{\Gamma} \) is the graph with \( V(\Gamma) = V(\overline{\Gamma}) \), where vertices \( u \) and \( v \) are adjacent in \( \overline{\Gamma} \) if and only if they are nonadjacent in \( \Gamma \). Thus the empty graph on \( n \) vertices is the complement of the complete graph, which we denote by \( \overline{K_n} \).

If \( \Psi \) and \( \Gamma \) are graphs with \( V(\Psi) \subseteq V(\Gamma) \) and \( E(\Psi) \subseteq E(\Gamma) \), then \( \Psi \) is a subgraph of \( \Gamma \). If \( V(\Psi) = V(\Gamma) \), then \( \Psi \) is a spanning subgraph of \( \Gamma \). A subgraph \( \Psi \) of \( \Gamma \) is an induced subgraph if, for any two vertices \( u, v \in V(\Psi) \), \( u \) and \( v \) are adjacent in \( \Psi \) if and only if they are adjacent in \( \Gamma \). A clique is a complete induced subgraph of \( \Gamma \), and the order of the largest clique is the clique number of \( \Gamma \), which we denote by \( \omega(\Gamma) \). An independent set is an empty induced subgraph of \( \Gamma \), and the order of the largest independent set is the independence number of \( \Gamma \), which we denote by \( \alpha(\Gamma) \). Further, for \( u \in V(\Gamma) \), we denote the largest independent set in \( N_\Gamma(u) \) by \( \alpha_u(\Gamma) \). An upper bound exists on \( \alpha(\Gamma) \) which depends on \( \alpha_u(\Gamma) \).

**Theorem 2.2.1 ([66, Corollary 3])** For a graph \( \Gamma \) of minimum valency \( \delta(\Gamma) \), let \( r \geq \alpha_u(\Gamma) \) for any \( u \in V(\Gamma) \). Then

\[
\alpha(\Gamma) \leq \frac{r|V(\Gamma)|}{\delta(\Gamma) + r}.
\]
A path of length $n$ in a graph $\Gamma$ is a sequence $u_0, u_1, \ldots, u_n$ of $n + 1$ distinct vertices such that $u_{i-1}, u_i$ are adjacent for all $i = 1, 2, \ldots, n$. A cycle of length $n$ in $\Gamma$ is a path $u_0, u_1, \ldots, u_{n-1}$, together with the edge $[u_0, u_{n-1}]$. A graph $\Gamma$ is connected if there exists a path in $\Gamma$ between any distinct pair of vertices; otherwise $\Gamma$ is disconnected. A connected component of $\Gamma$ is a maximal induced subgraph of $\Gamma$ which is connected.

In a connected graph $\Gamma$, we define the distance between $u, v \in V(\Gamma)$, denoted by $d_\Gamma(u, v)$, to be the shortest length of a path between $u$ and $v$. The diameter of $\Gamma$, denoted by $diam(\Gamma)$, is the maximum $d_\Gamma(u, v)$ between any two vertices $u$ and $v$ of $\Gamma$. If $\Gamma$ has cycles, the girth of $\Gamma$, denoted by $girth(\Gamma)$, is the length of a shortest cycle in $\Gamma$; otherwise the girth of $\Gamma$ is defined to be $\infty$. Likewise, if $\Gamma$ has odd cycles, then the odd-girth of $\Gamma$, denoted by $oddg(\Gamma)$, is the length of a shortest odd cycle in $\Gamma$; otherwise $\Gamma$ is bipartite (see [12, Proposition 1.6.1]).

Let $\Gamma, \Psi$ be two graphs with $|V(\Gamma)| = |V(\Psi)|$. An isomorphism is a bijection $\phi : V(\Gamma) \to V(\Psi)$, such that for any pair $u, v \in V(\Gamma)$, $u$ and $v$ are adjacent in $\Gamma$ if and only if $\phi(u)$ and $\phi(v)$ are adjacent in $\Psi$. If an isomorphism exists between $\Gamma$ and $\Psi$, $\Gamma$ and $\Psi$ are said to be isomorphic, which we denote by $\Gamma \cong \Psi$. An automorphism of $\Gamma$ is an isomorphism of $\Gamma$ to itself. All automorphisms of $\Gamma$ are thus permutations of $V(\Gamma)$, and the set of all automorphisms of $\Gamma$ forms a subgroup of $\text{Sym}(V(\Gamma))$ known as the full automorphism group of $\Gamma$, denoted by $\text{Aut}(\Gamma)$. Any subgroup of $\text{Aut}(\Gamma)$ is called an automorphism group of $\Gamma$.

Since all automorphisms of a graph $\Gamma$ are permutations of $V(\Gamma)$, the notation and definitions from Section 2.1 apply to graphs and their automorphisms.

**Definition 2.2.2** For $G \leq \text{Aut}(\Gamma)$, a graph $\Gamma$ is a $G$-vertex-transitive graph, if the action of $G$ on $V(\Gamma)$ is transitive. Likewise $\Gamma$ is a $G$-edge-transitive graph if $G$ is transitive on $E(\Gamma)$, a $G$-nonedge-transitive graph if $G$ is transitive on the set of nonedges of $\Gamma$, a $(G, s)$-arc-transitive graph if $G$ is transitive on the set of $s$-arcs of $\Gamma$, and a $G$-distance-transitive graph if $G$ is transitive on the set of pairs of vertices at distance $i$ in $\Gamma$, for each $i = 0, 1, \ldots, \text{diam}(\Gamma)$.

If $\Gamma$ is $\text{Aut}(\Gamma)$-vertex-transitive, then we say that $\Gamma$ is vertex-transitive. Similar terminology is used for other kinds of transitivity.
Note: we typically refer to a \((G,1)\)-arc-transitive graph as a \(G\)-symmetric graph. Further, if \(\Gamma\) is a \((G,s)\)-arc-transitive graph and each vertex of \(\Gamma\) is the initial vertex of some \(s\)-arc in \(\Gamma\), then \(\Gamma\) is also \(G\)-vertex-transitive. In particular, if \(\Gamma\) is a \(G\)-symmetric graph with no isolated vertices, then every vertex is the initial vertex of some arc of \(\Gamma\). Thus, every connected \(G\)-symmetric graph is also \(G\)-vertex transitive.

For any vertex-transitive graph \(\Gamma\), an upper bound exists on the product of \(\alpha(\Gamma)\) and \(\omega(\Gamma)\).

**Theorem 2.2.3** ([24]) *If \(\Gamma\) is vertex-transitive, then*

\[\alpha(\Gamma)\omega(\Gamma) \leq |V(\Gamma)|.\]

Throughout this thesis, there are three fundamental constructions of \(G\)-vertex-transitive graphs. Two of these constructions use permutation group theory, whilst the third construction uses other vertex-transitive graphs. For the first construction, we take a group \(G\) acting on a set \(\Omega\), with \(G\)-orbitals \(G((\alpha,\beta))\) for all \(\alpha, \beta \in \Omega\). We define a union of these \(G\)-orbitals to be a *generalised orbital*. For each generalised orbital \(\Delta\), there is a *paired orbital* \(\Delta^* := \{(\beta, \alpha) \mid (\alpha, \beta) \in \Delta\}\). Whenever \(\Delta = \Delta^*\), we say that \(\Delta\) is *self-paired*. Thus \(\Delta\) is self-paired if and only if for every \((\alpha, \beta) \in \Delta, (\beta, \alpha) \in \Delta\). For every self-paired generalised orbital \(\Delta\), the *generalised orbital graph* for \(G\) is the graph \(\Gamma\) with vertex set \(V(\Gamma) = \Omega\) and edge set \(E(\Gamma) = \Delta\). Clearly, \((\alpha, \beta) \in \Delta\) if and only \(g((\alpha, \beta)) \in \Delta\) for each \(g \in G\). Thus \(G \leq \text{Aut}(\Gamma)\), and \(\Gamma\) is \(G\)-vertex-transitive.

**Theorem 2.2.4** ([60, Theorem 2.1]) *Let \(\Gamma\) be a graph, and \(G \leq \text{Aut}(\Gamma)\). Then \(\Gamma\) is \(G\)-vertex-transitive if and only if \(\Gamma\) is a generalised orbital graph for \(G\), namely for the self-paired generalised orbital \(\Delta := \{(\alpha, \beta) \mid [\alpha, \beta] \in E(\Gamma)\}\). Further, \(\Gamma\) is \(G\)-arc-transitive if and only if \(\Gamma\) is an orbital graph for \(G\), namely for the self-paired orbital \(\Delta := \{(\alpha, \beta) \mid [\alpha, \beta] \in E(\Gamma)\}\).*

The second construction of \(G\)-vertex-transitive graphs are the graph products. The four most commonly encountered graph products are the categorical, strong, cartesian and lexicographic products.

**Definition 2.2.5** Let \(\Gamma\) and \(\Psi\) two graphs. The following products of \(\Gamma\) and \(\Psi\) are defined on the vertex set \(V(\Gamma) \times V(\Psi)\).
(i) The cartesian product $\Gamma \square \Psi$, with

\[ E(\Gamma \square \Psi) = \{(u,x), (v,y) : \text{either } u = v \text{ and } [x, y] \in E(\Psi), \]
\[ \text{or } [u, v] \in E(\Gamma) \text{ and } x = y \}; \]

(ii) the categorical product $\Gamma \times \Psi$, with

\[ E(\Gamma \times \Psi) = \{[(u,x), (v,y)] : [u, v] \in E(\Gamma), [x, y] \in E(\Psi)\}; \]

(iii) the strong product $\Gamma \boxtimes \Psi$, with

\[ E(\Gamma \boxtimes \Psi) = E(\Gamma \times \Psi) \cup E(\Gamma \square \Psi); \]

(iv) the lexicographic product $\Gamma [\Psi]$, with

\[ E(\Gamma [\Psi]) = \{[(u,x), (v,y)] : \text{either } u = v \text{ and } [x, y] \in E(\Psi), \]
\[ \text{or } [u, v] \in E(\Gamma)\}. \]

The products $C_5 \times K_3$ and $C_5 [K_3]$ are shown in Figures 2.1 and 2.2. For each $x \in V(C_5)$, the symbols $x, x', x''$ denote $(x,0), (x,1), (x,2) \in V(C_5) \times C(K_3)$ respectively.

Figure 2.1: The categorical product $C_5 \times K_3$. 

All of these products are known to be associative [31, pp. 116], and all but the lexicographic product are commutative [31, pp. 116]. Thus the categorical, strong and cartesian products of $n$ graphs $\Gamma_1, \ldots, \Gamma_n$ are well defined, and are denoted by $\times_{i=1}^n \Gamma_i$, $\boxtimes_{i=1}^n \Gamma_i$ and $\square_{i=1}^n \Gamma_i$ respectively. Each graph $\Gamma_i$ for $1 \leq i \leq n$ is called a factor of the product.

From Definition 2.2.5 we see that for $\pi \in \text{Aut}(\Gamma)$, $\rho \in \text{Aut}(\Psi)$ and $(u, x) \in V(\Gamma \times \Psi)$, the mapping $(u, x) \mapsto (\pi(u), \rho(x))$ is an automorphism of $\Gamma \times \Psi$, $\Gamma \boxtimes \Psi$ and $\Gamma \square \Psi$. Thus vertex-transitivity is preserved under these three products.

**Proposition 2.2.6** ([40, Proposition 4.18]) Let $\Gamma$ be a graph isomorphic to either a categorical, strong or cartesian product of connected graphs. If each of the factors of $\Gamma$ is vertex-transitive, then $\Gamma$ is vertex-transitive. Further, if $\Gamma$ is a categorical product with arc-transitive factors, then $\Gamma$ is arc-transitive.

Note: [40, Proposition 4.18] states Proposition 2.2.6 only for the cartesian product. However, the proofs for the strong and categorical products are identical to the
proof for the cartesian product in [40, Proposition 4.18].

For the lexicographic product \( \Gamma = \Psi [\Lambda] \), [40, Section 6.3] tells us that \( \text{Aut}(\Gamma) \) contains as a subgroup the wreath product \( G = \text{Aut}(\Lambda) \wr V(\Psi) \text{Aut}(\Psi) \), where \( G \) acts on \( V(\Gamma) = V(\Lambda) \times V(\Psi) \) via the imprimitive action outlined in Example 2.1.5.

**Proposition 2.2.7** ( [40, Section 6.3, Theorem 6.14]) Let \( \Psi \) and \( \Lambda \) be graphs. If both \( \Psi \) and \( \Lambda \) are vertex-transitive, then \( \Gamma = \Psi [\Lambda] \) is vertex-transitive. Further, if \( \Psi \) is arc-transitive and \( \Lambda \cong K_n \) for some \( n \in \mathbb{N} \), then \( \Gamma \) is arc-transitive.

**Proof** Let \( \Gamma = \Psi [\Lambda] \). If \( \Psi \) and \( \Lambda \) are vertex-transitive, then \( \Gamma \) is vertex-transitive by [40, Theorem 6.14]. Assume that \( \Psi \) is arc-transitive with \( V(\Psi) = \{1, \ldots, l\} \), \( \Lambda \cong K_n \) for any \( n \in \mathbb{N} \), and that \( ((x, u), (y, v)), ((c, a), (d, b)) \in A(\Gamma) \). Then by Definition 2.2.5, \( (u, v), (a, b) \in A(\Psi) \) (since \( V(\Gamma) = V(\Lambda) \times V(\Psi) \)).

Since \( \Psi \) is arc-transitive, there exists some \( \pi \in \text{Aut}(\Psi) \) for which \( \pi((u, v)) = (a, b) \). Also, since \( \text{Aut}(K_n) \cong \text{Sym}(n) \), there exists some \( \rho = (\rho_1, \ldots, \rho_l) \in \text{Aut}(K_n)^l \) with \( \rho \pi(u)(x) = c \) and \( \rho \pi(v)(y) = d \). Hence,

\[
\gamma = (\rho, \pi) \in \text{Aut}(\Lambda) \wr V(\Psi) \text{Aut}(\Psi) \subseteq \text{Aut}(\Gamma),
\]

such that

\[
\gamma((x, u), (y, v)) = (\gamma(x, u), \gamma(y, v)) = ((\rho \pi(u)(x), \pi(u)), (\rho \pi(v)(y), \pi(v))) = ((c, a), (d, b)).
\]

Therefore \( \Gamma \) is arc-transitive. \( \square \)

If \( \Lambda \) has order \( d \) with \( V(\Lambda) = \{x_1, \ldots, x_d\} \), then the \( d \) subgraphs of \( \Psi [\Lambda] \) induced on the subsets \( \{(u, x_i) \mid u \in V(\Psi)\} \subseteq V(\Psi [\Lambda]) \) for \( 1 \leq i \leq d \) are isomorphic to \( \Psi \). Another graph product is obtained by deleting all the edges from each of these \( d \) copies.

**Definition 2.2.8** The **deleted lexicographic product**, denoted by \( \Psi [\Lambda] - d\Psi \), is the graph with vertex set

\[
V(\Psi [\Lambda] - d\Psi) = V(\Psi [\Lambda])
\]
and edge set

\[ E(\Psi [\Lambda] - d\Psi) = E(\Psi [\Lambda]) \setminus \{(u, x), (v, x) \mid [u, v] \in E(\Psi), x \in V(\Lambda)\} . \]

From Definition 2.2.8 we see that for \( \pi \in \text{Aut}(\Psi) \), \( \rho \in \text{Aut}(\Lambda) \) and \((u, x) \in V(\Psi [\Lambda] - d\Psi)\), the mapping \((u, x) \mapsto (\pi(u), \rho(x))\) is an automorphism of \( \Psi [\Lambda] - d\Psi \). Thus if \( \Psi \) and \( \Lambda \) are vertex-transitive, then \( \Psi [\Lambda] - d\Psi \) is vertex-transitive.

The deleted lexicographic product \( C_5 [K_3] - 3C_5 \) is shown in Figure 2.3. For each \( x \in V(C_5) \), the symbols \( x, x', x'' \) denote \((x, 0), (x, 1), (x, 2) \in V(C_5) \times C(K_3)\) respectively.

![Figure 2.3: The deleted lexicographic product \( C_5[K_3] - 3C_5 \).](image)

For more on graph products, see [40].

The third prominent construction of vertex-transitive graphs are the Cayley graphs.

**Definition 2.2.9** Let \( G \) be a group and \( S \) be a subset of \( G \) which is closed under taking inverses and does not contain the identity element of \( G \). Then the \( Cay- \)
ley graph $\Gamma = \text{Cay}(G, S)$ is the graph with vertex set $G$ and edge set $E(\Gamma) = \{[g, h] | g, h \in G, g^{-1}h \in S\}$. If $G \cong \mathbb{Z}_n$, where $\mathbb{Z}_n$ is the cyclic group of order $n$, then $\Gamma$ is a circulant graph.

Let $\Gamma = \text{Cay}(G, S)$. For each $g \in G$, there exists a permutation $\rho_g$ of $G$ for which $\rho_g(x) = gx$ for all $x \in G$. The map $g \mapsto \rho_g$ is a permutation representation of $G$, called the left regular representation. The image of the left regular representation of $G$ (denoted by $\overline{G}$) is a subgroup of $\text{Aut}(\Gamma)$ isomorphic to $G$, and acts transitively on $G$, so that $\overline{G}$ acts regularly by Corollary 2.1.3. Thus every Cayley graph has a regular subgroup of automorphisms.

**Theorem 2.2.10 ([23, Lemmas 3.7.1, 3.7.2])** A graph $\Gamma$ is isomorphic to the Cayley graph $\text{Cay}(G, S)$ if and only if $\text{Aut}(\Gamma)$ contains a regular subgroup isomorphic to $G$.

### 2.3 Graph homomorphisms

#### 2.3.1 General graph homomorphisms

**Definition 2.3.1** For graphs $\Gamma$ and $\Psi$, a function $\phi : V(\Gamma) \to V(\Psi)$ is a graph homomorphism from $\Gamma$ to $\Psi$ if $[\phi(u), \phi(v)]$ is an edge in $\Psi$ whenever $[u, v]$ is an edge in $\Gamma$. We simply write $\phi : \Gamma \to \Psi$. If there exists a homomorphism from $\Gamma$ to $\Psi$, then we write $\Gamma \to \Psi$. When $\phi : \Gamma \to \Psi$ is a homomorphism, $\phi$ induces a mapping

$$\phi_E : E(\Gamma) \to E(\Psi), \text{ where } \phi_E([u, v]) = [\phi(u), \phi(v)],$$

such that there exists a graph defined by $\phi(\Gamma) := (\phi(V(\Gamma)), \phi_E(E(\Gamma)))$, which is called the homomorphic image of $\Gamma$ in $\Psi$. For a vertex $u \in V(\Psi)$ the pre-image $\phi^{-1}(u)$ is called a fibre of $\phi$. If $\Gamma$ is a subgraph of $\Psi$, then the inclusion homomorphism is the homomorphism which maps each vertex of $\Gamma$ to itself in $\Psi$.

Clearly, graph isomorphisms and automorphisms are graph homomorphisms. More generally, if $\Gamma \to \Psi$ and $\Psi$ is a subgraph of $\Gamma$, then the homomorphism $\phi : \Gamma \to \Psi$ is an endomorphism. Other prominent examples of graph homomorphisms are graph colourings, and homomorphisms between two odd cycles.
CHAPTER 2. NOTATION, DEFINITIONS AND PRELIMINARIES

Definition 2.3.2 A proper \( k \)-colouring of a graph \( \Gamma \) is an assignment of colours to the vertices of \( \Gamma \) in such a way that adjacent vertices get different colours. If there exists a \( k \)-colouring of \( \Gamma \), \( \Gamma \) is said to be \( k \)-colourable. The chromatic number \( \chi(\Gamma) \) of \( \Gamma \) is the least \( k \) for which \( \Gamma \) has a \( k \)-colouring.

Example 2.3.3 From Definition 2.3.2, we treat a proper \( k \)-colouring as a function \( c : V(\Gamma) \to [k] \), where \([k] = \{0,1,\ldots,k-1\} \). Then from Definition 2.3.1, the map \( c \) is a graph homomorphism from \( \Gamma \) to \( K_k \) (where \( K_k \) is the complete graph on \( k \) vertices), such that any graph \( \Gamma \) has a \( k \)-colouring if and only if there exists a homomorphism \( \Gamma \to K_k \).

Example 2.3.4 Let \( C_m = u_0 \ldots u_{m-1} \) and \( C_n = v_0 \ldots v_{n-1} \) be odd cycles, with \( m > n \). Then there exists a homomorphism \( \phi : C_m \to C_n \) with
\[
\phi(u_i) = \begin{cases} 
v_i, & \text{if } 0 \leq i \leq n - 1, \\
v_0, & \text{if } n \leq i \leq m - 1 \text{ and } i \equiv 1 \mod 2, \\
v_1, & \text{if } n \leq i \leq m - 1 \text{ and } i \equiv 0 \mod 2.
\end{cases}
\]
However there is no homomorphism from \( C_n \) to \( C_m \).

Examples 2.3.3 and 2.3.4 are significant because they provide simple tools which prove the nonexistence of homomorphisms between general graphs.

Proposition 2.3.5 ( [31, pp.110]) Let \( \Gamma \) and \( \Psi \) be nonbipartite graphs and \( \phi : \Gamma \to \Psi \) a homomorphism. Then

(i) \( \text{oddg}(\Gamma) \geq \text{oddg}(\Psi) \),

(ii) \( \omega(\Gamma) \leq \omega(\Psi) \),

(iii) \( \chi(\Gamma) \leq \chi(\Psi) \).

Let \( \Gamma \) be a graph and let \( \mathcal{P} = \{V_1,\ldots,V_k\} \) be a partition of \( V(\Gamma) \) into \( k \) nonempty classes. The quotient \( \Gamma/\mathcal{P} \) of \( \Gamma \) by \( \mathcal{P} \) is the graph whose vertices are the sets \( V_1,\ldots,V_k \) and whose edges are the pairs \([V_i,V_j], i \neq j\), such that there are \( u_i \in V_i \) and \( u_j \in V_j \) with \([u_i,u_j] \in E(\Gamma)\). The mapping \( \pi_\mathcal{P} : V(\Gamma) \to V(\Gamma/\mathcal{P}) \) defined by \( \pi_\mathcal{P}(u) = V_i \) for every \( u \in V_i \) and \( 1 \leq i \leq k \), is the natural map for \( \mathcal{P} \).

A natural question to ask is, when is \( \pi_\mathcal{P} \) a homomorphism?
Lemma 2.3.6 ([31, Corollary 2.10]) Let $\Gamma$ be a graph and $\mathcal{P}$ be a partition of $V(\Gamma)$. Then $\pi_\mathcal{P} : V(\Gamma) \to V(\Gamma/\mathcal{P})$ is a homomorphism if and only if $V_i$ is an independent set for each $i$.

Thus any partition of the vertex set of a graph into independent sets induces a homomorphism, the image of which is given by the quotient graph. There is also a converse to Lemma 2.3.6.

Proposition 2.3.7 ([31, Proposition 2.11]) For every homomorphism $\phi : \Gamma \to \Psi$ there is a partition $\mathcal{P}$ of $V(\Gamma)$ into independent sets and an injective homomorphism $\psi : \Gamma/\mathcal{P} \to \Psi$ such that $\phi = \psi \circ \pi_\mathcal{P}$.

By Proposition 2.3.7, every homomorphism $\phi : \Gamma \to \Psi$ induces a partition $\mathcal{P}_\phi$ of $V(\Gamma)$ into independent sets, where $\phi(\Gamma) \cong \Gamma/\mathcal{P}_\phi$. Thus the fibres of any homomorphism $\phi : \Gamma \to \Psi$ are independent sets of $V(\Gamma)$ (since the fibres are the elements of $\mathcal{P}_\phi$), and the pre-image under $\phi$ of any independent set in $\Psi$ is an independent set in $\Gamma$.

2.3.2 Retractions, cores and homomorphic equivalence

Definition 2.3.8 Let $\Gamma$ be a graph and $\Lambda$ be a subgraph of $\Gamma$. $\Lambda$ is called a retract of $\Gamma$ if there exist homomorphisms $\phi : \Gamma \to \Lambda$ and $\rho : \Lambda \to \Gamma$ such that $\phi \circ \rho = 1_{\text{Aut}(\Lambda)}$. The homomorphism $\phi$ is called a retraction and $\rho$ a co-retraction.

Due to the existence of both a retraction $\phi : \Gamma \to \Lambda$ and a co-retraction $\rho : \Lambda \to \Gamma$, the retract $\Lambda$ of $\Gamma$ inherits many of the structural properties of $\Gamma$. For example, by Proposition 2.3.5, any retract of $\Gamma$ must have the same chromatic number, clique number and odd-girth as $\Gamma$. Consequently, a graph $\Gamma$ has a complete retract if and only if $\chi(\Gamma) = \omega(\Gamma)$.

For a graph $\Gamma$ with retract $\Lambda$, retraction $\phi : \Gamma \to \Lambda$ and co-retraction $\rho : \Lambda \to \Gamma$, the condition that $\phi \circ \rho = 1_{\text{Aut}(\Lambda)}$ is quite strict. By relaxing this condition, we obtain a more useful characterisation of retracts and retractions. To achieve this new characterisation, we denote by $\phi |_\Lambda$ the restriction of $\phi$ to $V(\Lambda)$, that is the map $\phi |_\Lambda : V(\Lambda) \to V(\Lambda)$. 
Lemma 2.3.9 ([31, Lemma 2.18]) Let \( \Gamma \) and \( \Lambda \) be graphs. Then \( \Lambda \) is a retract of \( \Gamma \) if and only if there exist homomorphisms \( \phi : \Gamma \to \Lambda \) and \( \rho : \Lambda \to \Gamma \) such that \( \phi \circ \rho \in \text{Aut}(\Lambda) \). In particular, if \( \Lambda \) is a subgraph of \( \Gamma \), then \( \Lambda \) is a retract of \( \Gamma \) if and only if there is a homomorphism \( \phi : \Gamma \to \Lambda \) such that \( \phi \mid \Lambda \in \text{Aut}(\Lambda) \).

Of most significance to this thesis is a particular image of these retractions, called the core of a graph [33,34].

Definition 2.3.10 A graph \( \Gamma \) is called a core if no proper subgraph of \( \Gamma \) is a retract of \( \Gamma \). A retract of \( \Gamma \) is called a core of \( \Gamma \) if it is a core (so cores are the minimal retracts of graphs).

The significance of the cores of a graph comes from their ubiquity and their uniqueness.

Proposition 2.3.11 ([36]) Every graph \( \Gamma \) has a core, which is an induced subgraph and is unique up to isomorphism.

Due to Proposition 2.3.11, we can refer to the core of a graph, which we denote by \( \Gamma^* \).

From Lemma 2.3.9, we see that every retraction of a core must be an automorphism. Interestingly, all endomorphisms (not just retractions) of a core are automorphisms.

Proposition 2.3.12 ([31, Proposition 2.22]) Let \( \Gamma \) be a graph. Then \( \Gamma \) is a core if and only if every endomorphism of \( \Gamma \) is an automorphism of \( \Gamma \).

Proposition 2.3.5 provides us with our first family of cores.

Example 2.3.13 Let \( \Gamma \) be a graph such that every proper subgraph has chromatic number strictly less than \( \chi(\Gamma) \), then \( \Gamma \) is called a \( \chi \)-critical graph. Examples of \( \chi \)-critical graphs include the complete graphs and the odd cycles. Now by Proposition 2.3.5 and Lemma 2.3.9, for any graph \( \Gamma \), \( \chi(\Gamma^*) = \chi(\Gamma) \). Therefore, if \( \Gamma \) is \( \chi \)-critical, then \( \Gamma^* \) cannot be a proper subgraph of \( \Gamma \); hence \( \Gamma \) is a core.
If there exist homomorphisms $\Psi \to \Lambda$ and $\Lambda \to \Psi$, then $\Psi$ and $\Lambda$ are said to be \textit{homomorphically equivalent}, which we denote by $\Psi \leftrightarrow \Lambda$. From Definition 2.3.8, for a graph $\Gamma$, $\Gamma \leftrightarrow \Gamma^*$. This implies that for any two graphs $\Psi$ and $\Lambda$, if $\Psi \leftrightarrow \Lambda$ then $\Psi^* \leftrightarrow \Lambda^*$. However, a stronger relationship between the cores of homomorphically equivalent graphs exists.

\textbf{Lemma 2.3.14} ([23, Lemma 6.2.3]) \textit{Two graphs $\Psi$ and $\Lambda$ are homomorphically equivalent if and only if their cores are isomorphic.}

From Lemma 2.3.14, homomorphic equivalence is an equivalence relation on the class of all graphs. Further, there is a unique graph (up to isomorphism) of smallest order within each homomorphic equivalence class, which is the core of every graph within the class.

### 2.3.3 Homomorphisms of vertex-transitive graphs

Although Proposition 2.3.5 is useful, proving the nonexistence of a homomorphism between two graphs is generally difficult. One approach is to focus on homomorphisms between vertex-transitive and/or symmetric graphs, since the automorphism group of a graph plays an important role in many graph homomorphisms, such as retractions.

\textbf{Lemma 2.3.15} (No-Homomorphism Lemma [2]) \textit{Let $\Gamma$ and $\Psi$ be graphs such that $\Psi$ is vertex-transitive and $\Gamma \to \Psi$. Then}

$$\frac{\alpha(\Gamma)}{|V(\Gamma)|} \geq \frac{\alpha(\Psi)}{|V(\Psi)|}.$$  \hfill (2.3.1)

Now let $\Gamma$ and $\Psi$ be vertex-transitive graphs with $\Gamma \leftrightarrow \Psi$. Lemma 2.3.15 applies to the homomorphisms $\phi : \Gamma \to \Psi$ and $\rho : \Psi \to \Gamma$, so that Equation 2.3.1 becomes

$$\frac{\alpha(\Gamma)}{|V(\Gamma)|} = \frac{\alpha(\Psi)}{|V(\Psi)|}.$$

Hence Lemma 2.3.15 is particularly useful when studying homomorphically equivalent vertex-transitive graphs.
More generally, if $\Gamma \rightarrow \Psi$ (where $\Psi$ is vertex-transitive) and there is equality in Equation 2.3.1 (for $\Gamma$ and $\Psi$), then a much stronger relationship exists between the independence numbers of these graphs.

**Lemma 2.3.16 ([31, Lemma 3.6])** Let $\Gamma$ and $\Psi$ be graphs such that $\Psi$ is vertex-transitive, $\frac{\alpha(\Gamma)}{|V(\Gamma)|} = \frac{\alpha(\Psi)}{|V(\Psi)|}$ and $\Gamma \rightarrow \Psi$. Then for any maximum independent set $I$ in $\Psi$ and any homomorphism $\phi : \Gamma \rightarrow \Psi$,

$$|\phi^{-1}(I)| = \alpha(\Gamma).$$

From Lemma 2.3.9, for a vertex-transitive graph $\Gamma$ and a retraction $\phi : \Gamma \rightarrow \Psi$, $\phi |_{\Psi} \in \text{Aut}(\Psi)$. Thus a relationship exists between the automorphism group of a graph and the automorphism groups of its retracts. This relationship is strong for the core of a graph.

**Theorem 2.3.17 ([82])** Let $\Gamma$ be a vertex-transitive graph. Then its core $\Gamma^*$ is vertex-transitive.

However, transitivity is not a property inherited by all retracts of a graph.

**Example 2.3.18** Let $C_4$ be the symmetric cycle on four vertices, and let $u, v \in V(C_4)$ be a specific pair of nonadjacent vertices. The map $\phi$ for which $\phi(u) = v$, but which fixes every other vertex in $C_4$, is a homomorphism from $C_4$ to $P_3$ (the path of length two). But $P_3$ is also a subgraph of $C_4$, so $\phi$ is a retraction. Thus $C_4$ has the retract $P_3$, which is not vertex-transitive.

By focusing on vertex-transitive graphs, Theorem 2.3.17 allows us to make use of Lemma 2.3.15 to investigate further properties of the cores of vertex-transitive graphs. Specifically, since $\Gamma \leftrightarrow \Gamma^*$, Lemma 2.3.15 says that

$$\frac{\alpha(\Gamma)}{|V(\Gamma)|} = \frac{\alpha(\Gamma^*)}{|V(\Gamma^*)|}. \quad (2.3.2)$$

Equation 2.3.2 provides us with our first family of vertex-transitive cores.

**Corollary 2.3.19 ([31, Corollary 3.8])** Let $\Gamma$ be a vertex-transitive graph. If $\alpha(\Gamma)$ and $|V(\Gamma)|$ are relatively prime, then $\Gamma$ is a core.
Corollary 2.3.20 Let \( \Gamma \) be a vertex-transitive graph of prime order. Then \( \Gamma \) is a core.

The proof of Theorem 2.3.17 uses Proposition 2.3.12, and is easily adapted to other types of transitive graphs, such as edge-transitive graphs and symmetric graphs ([31, pp. 121] and [24]).

Theorem 2.3.21 Let \( \Gamma \) be a symmetric graph. Then its core \( \Gamma^* \) is symmetric.

Proposition 2.3.12 produces other restrictions on the cores of vertex-transitive graphs.

Theorem 2.3.22 ([31, Theorem 3.9]) Let \( \Gamma \) be a vertex-transitive graph, and let \( \phi : \Gamma \to \Gamma^* \). Then \( |V(\Gamma^*)| \) divides \( |V(\Gamma)| \), and for each \( u \in V(\Gamma^*) \), the fibres of \( \phi \) have order

\[
|\phi^{-1}(u)| = \frac{|V(\Gamma)|}{|V(\Gamma^*)|}.
\]

Like Theorem 2.3.17, the proof of Theorem 2.3.22 generalises to symmetric graphs, and this generalisation provides a family of symmetric cores.

Theorem 2.3.23 ([24]) Let \( \Gamma \) be a symmetric graph. Then the valency of \( \Gamma^* \) divides the valency of \( \Gamma \).

Corollary 2.3.24 Let \( \Gamma \) be a nonbipartite symmetric graph of prime valency. Then \( \Gamma \) is a core.

For any vertex-transitive graph \( \Gamma \), the primitivity of \( \text{Aut}(\Gamma) \) on \( V(\Gamma) \) also influences the structure of \( \text{Aut}(\Gamma^*) \).

Lemma 2.3.25 ([24]) Let \( \Gamma \) be a vertex-transitive graph, such that \( \text{Aut}(\Gamma) \) is primitive on \( V(\Gamma) \). Then \( \text{Aut}(\Gamma^*) \) is primitive on \( V(\Gamma^*) \).

If \( \Gamma \) is imprimitive, then the effect of this imprimitivity on the structure of \( \text{Aut}(\Gamma^*) \) is subtle. However, if \( \Gamma \) is also symmetric, then its imprimitivity induces a graph homomorphism, which is a natural candidate for a retraction of \( \Gamma \).
Lemma 2.3.26 ([10]) If $\Gamma$ is a connected, $G$-imprimitive symmetric graph, where $G \leq \text{Aut}(\Gamma)$, then every block of imprimitivity of the action of $G$ on $V(\Gamma)$ is an independent set.

By Lemma 2.3.26 if $\Gamma$ is a $G$-imprimitive symmetric graph, then any system of imprimitivity of $G$ partitions $V(\Gamma)$ into independent sets of equal size. By Theorem 2.3.22 and Proposition 2.3.7, the fibres of the retraction $\phi : \Gamma \to \Gamma^*$ partition $V(\Gamma)$ into independent sets of equal size. Therefore, the block systems of $G$-imprimitive symmetric graphs are a good starting point when searching for retractions of these graphs.

Unfortunately, the block systems of $G$-imprimitive symmetric graphs do not completely describe all retractions to the cores of these graphs. For example, there exist imprimitive symmetric graphs $\Gamma$ for which the fibres of the retraction $\phi : \Gamma \to \Gamma^*$ are not blocks of any symmetric $G \leq \text{Aut}(\Gamma)$. We will encounter a class of such graphs in Chapter 6.

The connection between $\text{Aut}(\Gamma)$ and $\text{Aut}(\Gamma^*)$ shows that $\Gamma^*$ inherits many properties from $\Gamma$. However, there exist important structural properties of $\Gamma$ and $\text{Aut}(\Gamma)$ which $\Gamma^*$ and $\text{Aut}(\Gamma^*)$ do not inherit.

Theorem 2.3.27 ([69]) Any connected vertex-transitive graph is a retract of a Cayley graph.

Theorem 2.3.27 was stated differently in [69]; our statement above is from [23, Theorem 3.1].

Example 2.3.28 Let $\Psi$ be the Petersen graph. We know that $\Psi$ is a core ([31, Example 2.33]), is vertex-transitive, but not a Cayley graph. By Theorem 2.3.27, $\Psi$ is the core of some Cayley graph $\Gamma$. Since $\Gamma$ is a Cayley graph, there exists some $G \leq \text{Aut}(\Gamma)$ where $G$ is regular on $V(\Gamma)$ (by Theorem 2.2.10). Yet under the retraction $\phi : \Gamma \to \Psi$, the elements of $G$ do not induce a regular subgroup of $\text{Aut}(\Gamma^*)$, since $\Gamma^*$ is isomorphic to $\Psi$ and thus $\text{Aut}(\Gamma^*)$ has no regular subgroups.

2.3.4 Cores of graph products

From Definition 2.2.5, we see that the strong, cartesian and lexicographic products all contain their factors as induced subgraphs. This suggests that for these three
products, the cores must be products of subgraphs or retracts of each factor. We show this result for the strong products in Theorem 3.2.6, for the lexicographic products in Proposition 3.2.7, and for the cartesian products with vertex-transitive factors in Proposition 3.2.8.

However, the case for the categorical product is more complicated. Unlike the other products, we cannot guaranteed that the categorical product has an induced subgraph isomorphic to either factor. However the categorical product has a homomorphism onto each factor.

**Lemma 2.3.29** ([37, Proposition 2.1]) Let $\Psi$, $\Gamma$ and $\Lambda$ be graphs. Then

(i) there exist homomorphisms $\pi : \Psi \times \Gamma \to \Psi$ and $\rho : \Psi \times \Gamma \to \Gamma$ defined by $\pi((i, x)) = i$ and $\rho((i, x)) = x$ for $(i, x) \in V(\Psi) \times V(\Gamma)$;

(ii) if $\Lambda \to \Psi$ and $\Lambda \to \Gamma$ then $\Lambda \to \Psi \times \Gamma$;

(iii) in particular, $\Gamma \to \Psi$ if and only if $\Psi \times \Gamma \leftrightarrow \Gamma$.

Note that if both $\Gamma \not\to \Psi$ and $\Psi \not\to \Gamma$, Lemma 2.3.29 does not rule out the existence of a retract $\Lambda$ of $\Psi \times \Gamma$ with $\Lambda \not\cong \Psi \times \Gamma$, $\Gamma \not\cong \Lambda$ and $\Psi \not\cong \Lambda$. So, although no examples are known, there may exist categorical products $\Psi \times \Gamma$ whose cores are neither themselves nor retracts of one of the factors.

For a graph $\Gamma$ and $n \in \mathbb{N}$, we define $\Gamma^n = \Gamma \times \Gamma \times \cdots \times \Gamma$ to be the $n$-th power of $\Gamma$, and define a projection to be a map from $\Gamma^n$ to one of its factors. If $\phi : \Gamma^n \to \Gamma$ is a homomorphism with $\phi(u, u, \cdots, u) = u$ for all $u \in V(\Gamma)$, then $\phi$ is idempotent. If the projections are the only idempotent homomorphisms from $\Gamma^n$ to $\Gamma$ for all $n \in \mathbb{N}$, then $\Gamma$ is projective. Vertex-transitive, projective cores are important to the study of the cores of categorical products, because vertex-transitive projective cores are always retracts of a factor.

**Theorem 2.3.30** ([46, Theorem 1.4]) Let $\Lambda$ be a vertex-transitive core. If $\Lambda$ is projective, then whenever $\Lambda$ is a retract of a categorical product of connected graphs, it is a retract of a factor.

One prominent family of projective graphs are the primitive graphs.

**Theorem 2.3.31** ([46, Theorem 1.5]) Let $\Lambda$ be a core with $\text{Aut}(\Lambda)$ primitive on $V(\Lambda)$. Then $\Lambda$ is projective.
Chapter 3

Literature review

In this chapter we present an historical overview of the theory of graph retractions. Since retractions are a specific example of a graph homomorphism, understanding when a homomorphism exists between two graphs is crucial to understanding graph retractions. Thus this chapter is split into two sections, Section 3.1 where we discuss general graph homomorphisms, and Section 3.2 where we discuss retracts and cores of graphs.

Beginning with Section 3.1.1, we discuss the origins of graph homomorphisms, some early results on the existence of homomorphisms between specific graphs, and some general tools for proving the existence or nonexistence of graph homomorphisms. One prominent and straightforward example of a graph homomorphism is the proper colouring from Definition 2.3.2. Proper colourings are particularly useful for studying general homomorphisms; comparing the chromatic numbers of two graphs is one method to prove the nonexistence of a homomorphism between those graphs. Thus in Sections 3.1.2 and 3.1.3, we discuss two generalisations of graph colourings (namely the circular and fractional colourings) which are also graph homomorphisms, and are used to prove the nonexistence of general graph homomorphisms. Then in Section 3.1.4, we discuss colourings of graph products.

In Section 3.2.1 we begin our discussion of retracts and cores of general graphs, giving the historical origins of this topic. Then in Section 3.2.2 we focus on retracts and cores of vertex-transitive graphs. Specifically, we discuss the origins of Theorems 2.3.17 and 2.3.22, which provided the motivation for our investigation into the cores
of vertex-transitive graphs, and the subsequent results given in this thesis. We then present some prominent families of vertex-transitive graphs which are either cores, or whose cores are known. The chapter ends with Section 3.2.3, where we cover the retracts and cores of various graph products.

3.1 Graph homomorphisms

3.1.1 Existence and nonexistence of graph homomorphisms

The study of isomorphisms and automorphisms is broad and distinct from that of general graph homomorphisms, as such we do not discuss the origins of graph isomorphisms and automorphisms. The study of general graph homomorphisms begins with Sabidussi, with Definition 2.3.1 first provided in [68]. In [68], graph homomorphisms are then used to obtain another proof of Whitney’s Theorem, which is a result giving necessary and sufficient conditions for two graphs to be isomorphic.

Having defined graph homomorphisms, the natural question to ask is, under what general conditions can we prove the existence or nonexistence of a homomorphism between two graphs? The only known results confirming the existence of homomorphisms between graphs are for small families of graphs. The most famous of these results is the Four-colour Theorem.

Theorem 3.1.1 (Four-colour Theorem) Let $\Gamma$ be a planar graph. Then $\Gamma$ is 4-colourable; in other words, $\Gamma \rightarrow K_4$.

Appel and Haken first proved the Four-colour Theorem in 1977 with the aid of computers (see [4] for the comprehensive proof). Using a similar technique (also with the aid of computers), a simpler proof was later given by Robertson, Sanders, Seymour and Thomas in [64].

Grötzsch’s Theorem is another result confirming the existence of homomorphisms between graphs.

Theorem 3.1.2 (Grötzsch’s Theorem [26]) Let $\Gamma$ be a triangle-free planar graph. Then $\Gamma$ is 3-colourable; in other words, $\Gamma \rightarrow K_3$. 
Using graph homomorphisms, Häggkvist and Hell proved a similar result to Grötzsch’s Theorem in [30]. This result proved the existence of a triangle-free graph to which all cubic triangle-free graphs are homomorphic.

Likewise, determining general rules for the nonexistence of a homomorphism between two graphs is challenging. Many of the methods hitherto developed to show the nonexistence of a graph homomorphism require the existence of homomorphisms to other graphs. Some simple examples of this approach, detailed in [31] and Proposition 2.3.5, are to compare the chromatic numbers, the lengths of the shortest odd cycles and the clique numbers of two graphs.

Stronger conditions preventing homomorphisms between graphs come from [2], where Albertson and Collins gave Lemma 2.3.15, known as the No-Homomorphism Lemma, for homomorphisms into vertex-transitive graphs. Fortunately, the proof of Lemma 2.3.15 in [2] is sufficiently general as to apply to other graph properties, other than the independence number. For example, in [2] Albertson and Collins suggest substituting $\alpha(\Gamma)$ and $\alpha(\Psi)$ in Equation 2.3.1 with $\delta(\Gamma, t)$ and $\delta(\Psi, t)$, where $\delta(\Gamma, t)$ is the maximum number of vertices in an induced subgraph of $\Gamma$ with no complete subgraph of order $t$. For another example, see [5].

Due to the inherent difficulties in showing the existence or nonexistence of a homomorphism $\Gamma \rightarrow \Psi$ between fixed graphs $\Gamma$ and $\Psi$ (known as the $\Psi$-colouring problem), the computational complexity of the $\Psi$-colouring problem has received considerable attention. In Karp’s famous paper [43], Karp proved that the standard graph colouring problem (for nonbipartite graphs) is NP-complete. Since the standard graph colouring problem is a specific example of the more general $\Psi$-colouring problem, Karp’s result suggests that for all nonbipartite graphs, the $\Psi$-colouring problem is also NP-complete. Hell and Nešetřil eventually proved this in [35].

### 3.1.2 Circular colourings

From Example 2.3.3, a proper colouring of a graph is equivalent to a homomorphism from the graph to a complete graph. This reformulation of graph colourings into the language of homomorphisms naturally lends itself to a generalisation of colourings, where the image of a given homomorphism is any family of graphs, not just the complete graphs. This approach inspired much study into possible alternatives to the
conventional graph colourings, one of the more prominent examples being circular colourings.

**Definition 3.1.3** A circular \( \frac{s}{r} \)-colouring is a homomorphism from a graph \( \Gamma \) to the circular graph \( \Psi_{\frac{s}{r}} \) for integers \( r, s \) with \( 0 < r \leq s \), where the graph \( \Psi_{\frac{s}{r}} \) has vertices \( \{0, 1, \ldots, s - 1\} \) and edges \( \{ij : r \leq |i - j| \leq s - r\} \). The circular chromatic number (or the star chromatic number) is then defined by

\[
\chi_C(\Gamma) = \inf \left\{ \frac{s}{r} : \Gamma \text{ is } \frac{s}{r}\text{-colourable} \right\}.
\]

Vince introduced circular colourings in [80], where he also proved some fundamental properties of these colourings, many of which are analogous to properties found for conventional colourings. (Note: Definition 3.1.3 comes from Bondy and Hell [5], as Vince’s definition for a circular colouring does not use graph homomorphisms.) The most significant of these properties are the upper and lower bounds on \( \chi_C(\Gamma) \) in terms of \( \chi(\Gamma) \), which show that for many graphs, circular colourings are a refinement of the conventional colourings.

**Theorem 3.1.4** \([80]\) For any graph \( \Gamma \),

\[
\chi(\Gamma) - 1 < \chi_C(\Gamma) \leq \chi(\Gamma).
\]

Theorem 3.1.4 suggests two obvious questions. The first question is, what is the circular chromatic number for given families of graphs? Vince [80] begun the investigation of this question, by determining the circular chromatic number for complete graphs and odd cycles. Vince’s work prompted many authors to investigate the circular chromatic numbers for other families of graphs. A good starting point for this work is the survey by Zhu [85].

The second question arising out of Theorem 3.1.4 is, for which graphs is \( \chi_C(\Gamma) = \chi(\Gamma) \)? In the investigation of this question, some strong sufficient conditions for \( \chi_C(\Gamma) = \chi(\Gamma) \) were determined. The first condition is due to Vince.

**Theorem 3.1.5** \([80]\) Let \( \Gamma \) be a graph with \( \omega(\Gamma) = \chi(\Gamma) \). Then \( \chi_C(\Gamma) = \chi(\Gamma) \).

The most notable condition under which \( \chi_C(\Gamma) = \chi(\Gamma) \) is due to Steffen and Zhu.
Theorem 3.1.6 ( [74]) Suppose \( \Gamma \) is a graph with \( \chi(\Gamma) = n \). If there exists a nontrivial subset \( A \subset V(\Gamma) \) such that for any proper \( n \)-colouring of \( \Gamma \), each colour class is either contained in \( A \) or disjoint from \( A \), then \( \chi_C(\Gamma) = \chi(\Gamma) \).

Theorem 3.1.6 has two interesting corollaries. The first, proven by Gao et al. [20] and independently by Abbott and Zhou [1] says that, if the complement of \( \Gamma \) is disconnected, then \( \chi_C(\Gamma) = \chi(\Gamma) \). The second corollary of Theorem 3.1.6 states that if \( \Gamma \) is uniquely colourable (that is, \( \Gamma \) has only one colouring), then \( \chi_C(\Gamma) = \chi(\Gamma) \).

In [27], Guichard showed that it is NP-hard to determine whether or not \( \chi_C(\Gamma) = \chi(\Gamma) \).

3.1.3 Fractional colourings

The second prominent generalisation of graph colourings which use graph homomorphisms are the fractional colourings.

Definition 3.1.7 Let \( \mathcal{I}(\Gamma) \) be the set of all independent sets of graph \( \Gamma \), and let \( \mathcal{I}(\Gamma, x) \) be the set of all independent sets of graph \( \Gamma \) that contain the vertex \( x \). A fractional colouring of \( \Gamma \) is a function \( \mu : \mathcal{I}(\Gamma) \to [0, 1] \) which satisfies

\[
\sum_{I \in \mathcal{I}(\Gamma, u)} \mu(I) \geq 1
\]

for all \( u \in V(\Gamma) \). This definition naturally leads to the fractional chromatic number \( \chi_f(\Gamma) \), which is defined by

\[
\chi_f(\Gamma) = \inf \left\{ \sum_{I \in \mathcal{I}(\Gamma)} \mu(I) : \mu \text{ is a fractional colouring of } \Gamma \right\}.
\]

Fractional colourings were first introduced by Geller and Stahl [21, 72], where they discuss an example known as a Kneser colouring (or an \( s \)-tuple \( r \)-colouring). A Kneser colouring is a homomorphism from a graph to the graph \( K(r, s) \).

Definition 3.1.8 Let \( r, s \) be integers such that \( 1 \leq r < \frac{s}{2} \). The Kneser graph \( K(r, s) \) is the graph whose vertices are the \( r \)-subsets of a fixed \( s \)-set, with two \( r \)-subsets being adjacent if and only if they are disjoint. Examples of Kneser graphs
include $K(1, s)$, which is the complete graph $K_s$, and $K(2, 5)$ which is the Petersen graph.

Kneser graphs and colourings play a central role in the study of fractional colourings, as seen in the following result.

**Theorem 3.1.9** ([23, Theorem 7.4.5]) *For any graph* $\Gamma$,

$$\chi_f(\Gamma) = \inf \left\{ \frac{s}{r} : \Gamma \rightarrow K(r, s) \right\}.$$

The appeal of fractional colourings is that, in many cases, they reduce the question of the existence (or nonexistence) of homomorphisms between graphs to the question of the existence (or nonexistence) of homomorphisms between Kneser graphs. With this question in mind, [21, 37, 72] prove the existence of homomorphisms between certain Kneser graphs.

**Proposition 3.1.10** ([37, Proposition 6.26]) *For all integers* $r, s$, with $s \geq 2r$ and $r \geq 1$,

(i) $K(r, s) \rightarrow K(r, s + 1)$,

(ii) $K(r, s) \rightarrow K(tr, ts)$ for every positive integer $t$,

(iii) $K(r, s) \rightarrow K(r - 1, s - 2)$ for $r > 1$.

From [37], the homomorphisms in Proposition 3.1.10 and their compositions are conjectured to be the only permissible homomorphisms between Kneser graphs. To verify this conjecture, conditions for the nonexistence of homomorphisms between Kneser graphs must be determined.

The strongest results concerning the nonexistence of homomorphisms between Kneser graphs are Lovász’s Theorem on the chromatic number of Kneser graphs, and the Erdős-Ko-Rado Theorem on the independence number of Kneser graphs.

**Theorem 3.1.11** (Lovász’s Theorem [50]) *For a Kneser graph* $K(r, s)$,

$$\chi(K(r, s)) = s - 2r + 2.$$
Theorem 3.1.12 (Erdős-Ko-Rado Theorem [19]) For a Kneser graph $K(r, s)$,

$$\alpha(K(r, s)) = \binom{s-1}{r-1}.$$

Since all complete graphs are Kneser graphs, the significance of Theorem 3.1.11 is clear. Whilst Theorem 3.1.12 is significant because it allows the use of Lemma 2.3.15 to determine the nonexistence of homomorphisms between Kneser graphs, since Kneser graphs are vertex-transitive by [9, Proposition 1]. Thus Theorem 3.1.11 and Theorem 3.1.12 show that in the majority of cases, there exist no homomorphisms between Kneser graphs other than those in Proposition 3.1.10 (for more examples of Kneser graphs with no homomorphisms between one another, see [37]). Thus the homomorphisms between Kneser graphs are explicitly determined, with the exception of one unresolved case.

Conjecture 3.1.13 ([37]) For all integers $r, s$, with $s \geq 2r$, $r \geq 1$ and $t \geq 2$,

$$K(r, s) \not\rightarrow K(tr - r + 1, ts - 2r + 1).$$

3.1.4 Graph products

Sections 3.1.1, 3.1.2 and 3.1.3 discussed the work done in finding homomorphisms between specific families of graphs. Another approach is to ask what role graph constructions play in determining the existence or nonexistence of graph homomorphisms. Graph products are graph constructions that have received considerable attention, with the cartesian, categorical, strong and lexicographic products from Definition 2.2.5 the most extensively studied.

Of these products, the categorical product is the only one to naturally induce graph homomorphisms (see Lemma 2.3.29), thus it is the most relevant product to this thesis. We refer the reader to Imrich and and Klavžar [40] for a comprehensive review of the other three products, and [31] for a survey of results on homomorphisms from these products.

Sabidussi first introduced the categorical product in [67]. Since this product has a homomorphism onto each of its factors (see Lemma 2.3.29), and each colouring of a graph is a homomorphism to a complete graph, we see that for graphs $\Gamma$ and $\Psi$, 
\(\chi(\Gamma \times \Psi) \leq \min \{\chi(\Gamma), \chi(\Psi)\}\). So the obvious question is, what is the lower bound on the chromatic number of a categorical product? Hedetniemi [32] first investigated this question.

**Conjecture 3.1.14 (Hedetniemi’s Conjecture [32])** For any graphs \(\Gamma\) and \(\Psi\),

\[
\chi(\Gamma \times \Psi) = \min \{\chi(\Gamma), \chi(\Psi)\}.
\]

This challenging problem has received considerable attention, yet has only been proven for a small number of graphs. The result is trivial whenever \(\min \{\chi(\Gamma), \chi(\Psi)\}\) \(\leq 2\). In [32] Hedetniemi showed that the categorical product of two odd cycles contains an odd cycle, thus proving Conjecture 3.1.14 when \(\min \{\chi(\Gamma), \chi(\Psi)\} = 3\). The strongest result to date is due to El-Zahar and Sauer. 

**Theorem 3.1.15 ( [18])** Let \(\Gamma\) and \(\Psi\) be graphs. If \(\chi(\Gamma) \geq 4\) and \(\chi(\Psi) \geq 4\), then

\[
\chi(\Gamma \times \Psi) \geq 4.
\]

The approach used by El-Zahar and Sauer in proving Theorem 3.1.15, when applied to known results for Hedetniemi’s conjecture, provides alternate, and in many cases simpler proofs. One such example of a result simplified by El-Zahar and Sauer’s approach is due to Duffus, Sands and Woodrow.

**Theorem 3.1.16 ( [17])** Let \(\Gamma\), \(\Psi\) be connected graphs, each with \(n\)-cliques, and with \(\chi(\Gamma), \chi(\Psi) > n\). Then

\[
\chi(\Gamma \times \Psi) > n.
\]

El-Zahar and Sauer’s approach also simplifies a result due to Burr, Erdős and Lovász.

**Theorem 3.1.17 ( [6])** Let \(\Psi\) be a graph such that each vertex of \(\Psi\) is contained in a clique of size \(n\), and \(\chi(\Psi) > n\). Then for any \(\Gamma\) such that \(\chi(\Gamma) > n\),

\[
\chi(\Gamma \times \Psi) > n.
\]
Restating Hedetniemi’s conjecture in the language of graph homomorphisms allows it to be generalised using graph homomorphisms. One such generalisation, introduced in [59] by Nešetřil and Pultr, replaces the homomorphism to a complete graph (i.e. the colouring) with a homomorphism to an arbitrary graph $\Lambda$.

**Definition 3.1.18** Let $\Gamma, \Psi$ and $\Lambda$ be arbitrary graphs. Then $\Lambda$ is said to be *multiplicative* if $\Gamma \times \Psi \rightarrow \Lambda$ implies that $\Gamma \rightarrow \Lambda$ or $\Psi \rightarrow \Lambda$.

Thus Hedetniemi’s conjecture asserts that every complete graph is multiplicative. Since Hedetniemi’s conjecture is true for $\chi(\Gamma \times \Psi) \leq 4$, the complete graphs of order up to four are multiplicative. In [29], Håggkvist et. al show that odd cycles are also multiplicative. The strongest result regarding multiplicativity of graphs is due to Tardif.

**Theorem 3.1.19 ([76])** Let $\Psi_s^r$ be a circular graph. If $\frac{s}{r} < 4$, then $\Psi_s^r$ is multiplicative.

To date the complete graphs of order up to four, the odd cycles and the circular graphs from Theorem 3.1.19 are the only known multiplicative cores (see Definition 2.3.10 for the definition of a core). However examples of nonmultiplicative graphs are known [84] (such as $\Gamma \times \Psi$, if no homomorphism exists between $\Gamma$ and $\Psi$), so it is difficult to tell whether studying multiplicativity will give any insight into Hedetniemi’s conjecture.

Circular and fractional colourings have also been investigated in relation to Hedetniemi’s conjecture. In [83,85], Zhu proposed a version of Hedetniemi’s conjecture for circular colourings.

**Conjecture 3.1.20 ([83,85])** For any graphs $\Gamma$ and $\Psi$,

$$\chi_C(\Gamma \times \Psi) = \min \{\chi_C(\Gamma), \chi_C(\Psi)\}.$$

The strongest result concerning Conjecture 3.1.20 is Theorem 3.1.19, which confirms Conjecture 3.1.20 for all $\Gamma$ and $\Psi$ for which $\min \{\chi_C(\Gamma), \chi_C(\Psi)\} \leq 4$.

In [86], Zhu conjectured a version of Hedetniemi’s conjecture for fractional colourings, and verified this conjecture for circulant graphs, Kneser graphs and for direct
sums of these graphs. Later, Zhu confirmed this fractional colourings version of Hedetniemi’s conjecture for fractional colourings of any two graphs.

Theorem 3.1.21 ([87]) For any graphs $\Gamma$ and $\Psi$,

$$\chi_f(\Gamma \times \Psi) = \min\{\chi_f(\Gamma), \chi_f(\Psi)\}.$$ 

3.2 Retracts and cores

3.2.1 General retracts and cores

Following on from Sabidussi’s original definition of a graph homomorphism, the Prague school of category theory attempted to develop a theory of graphs (and more general mathematical structures) in the framework of algebra and category theory. Under this framework, the category of graphs consists of all graphs, with the morphisms between them being graph homomorphisms. The book [63] by Pultr and Trnková details all this work, up to 1980.

As part of this work, Hell [33,34] took one of the fundamental morphisms found in category theory, the retraction, and applied it to the category of graphs (see Definition 2.3.8). Retractions play a fundamental role in both extending and simplifying graph homomorphisms. Specifically, whenever $\Gamma \rightarrow \Psi$, Definition 2.3.8 and Proposition 2.3.11 imply that $\Gamma^* \rightarrow \Psi^*$. Thus we can reduce many questions about homomorphisms between any graphs to questions about the homomorphisms between their respective cores.

The inherent usefulness of retractions in studying other graph homomorphisms motivates us to determine the cores of given graphs. However, since the general problem of finding homomorphisms between graphs is difficult, finding the cores of graphs appears to be similarly challenging. Unfortunately this difficulty is confirmed by Hell and Nešetřil [36], at least computationally, where they show that in general it is NP-complete to decide whether or not a graph is its own core.
3.2.2 Retracts and cores of vertex-transitive graphs

The difficulty in the general problem of finding the cores of graphs means that much of the effort is directed towards finding the cores of smaller families of graphs. For example, Theorem 2.3.17, due to Welzl [82], states that the core of a vertex-transitive graph is vertex-transitive. Thus, Theorem 2.3.17 allows us to focus on the cores of vertex-transitive graphs.

By focusing on vertex-transitive graphs in [31], Hahn and Tardif prove Theorem 2.3.22 ([31, Theorem 3.9]), which states that for a vertex-transitive graph $\Gamma$, $|V(\Gamma^*)|$ divides $|V(\Gamma)|$. Theorem 2.3.22 imposes tough restrictions on the order of $\Gamma^*$, and in Corollary 2.3.20, provides a family of vertex-transitive cores (namely, the vertex-transitive graphs of prime order).

There are a number of other prominent families of vertex-transitive graphs which are also cores. For example, as a consequence of Theorem 3.1.12, all Kneser graphs are cores.

Theorem 3.2.1 ([23, Theorem 7.9.1]) If $\Gamma$ is a Kneser graph, then $\Gamma$ is a core.

We have already seen in Corollary 2.3.24 that all nonbipartite symmetric graphs of prime valency are cores. On a similar note, Godsil and Royle found another family of symmetric graphs which are cores.

Theorem 3.2.2 ([23, Theorem 6.13.5]) If $\Gamma$ is a connected nonbipartite 2-arc-transitive graph, then $\Gamma$ is a core.

There are also some families of vertex-transitive graphs which are not necessarily cores, but whose cores are known. One example is due to Cameron and Kazanidis.

Proposition 3.2.3 ([7]) Let $\Gamma$ be a nonedge-transitive graph. Then either the core of $\Gamma$ is a complete graph, or $\Gamma$ is a core.

After proving Proposition 3.2.3, Cameron and Kazanidis then explicitly determined which case held for various families of nonedge-transitive graphs. A graph is said to be strongly regular if it is regular, every pair of adjacent vertices has a common neighbours, and every pair of distinct nonadjacent vertices has a common
neighbours, for some integers $a$ and $c$. All nonedge-transitive graphs are strongly regular. Thus, Cameron and Kazanidis conjectured that Proposition 3.2.3 held for all strongly regular graphs.

**Conjecture 3.2.4 ([7, 25])** Let $\Gamma$ be a strongly regular graph. Then either the core of $\Gamma$ is a complete graph, or $\Gamma$ is a core.

Godsil and Royle then attempted to answer Conjecture 3.2.4. In [25] they show that Conjecture 3.2.4 holds for three more families of strongly regular graphs. These results were then extended to similar graphs that are not necessarily strongly regular, most notably for distance-transitive graphs.

**Theorem 3.2.5 ([25])** Let $\Gamma$ be a distance-transitive graph. Then either the core of $\Gamma$ is a complete graph, or $\Gamma$ is a core.

Proposition 3.2.3 and Theorem 3.2.5 suggest the possibility that the cores of vertex-transitive graphs from a given family will also be members of that family. However, Sabidussi has shown in Theorem 2.3.27 that the core of a Cayley graph need not be a Cayley graph. Thus Theorem 2.3.27 suggests two important questions: for which families of Cayley graphs is the core a member of the same family? and under what conditions is the core of a Cayley graph not a Cayley graph?

### 3.2.3 Retracts and cores of graph products

As in Section 3.1.4, the graph products from Definition 2.2.5 provide another approach to studying the retractions and cores of graphs. Imrich and Klavžar were the first to investigate the retracts of graph products.

**Theorem 3.2.6 ([39])** Let $\Gamma$ and $\Psi$ be connected graphs, and $\Lambda$ a retract of $\Gamma \boxtimes \Psi$. Then there exist subgraphs $\Gamma'$ of $\Gamma$ and $\Psi'$ of $\Psi$ such that $\Lambda \cong \Gamma' \boxtimes \Psi'$. In particular, if both $\Gamma$ and $\Psi$ are triangle-free, then $(\Gamma \boxtimes \Psi)^* \cong \Gamma^* \boxtimes \Psi^*$.

Hahn and Tardif proved a similar result for the lexicographic product.

**Proposition 3.2.7 ([31, Propositions 5.32, 5.33])** Let $\Gamma$ and $\Psi$ be connected graphs. Then the core of $\Gamma [\Psi]$ is $\Gamma' [\Psi^*]$, where $\Gamma'$ is a subgraph of $\Gamma$ which is itself a core. In particular, if $\Gamma$ is triangle-free, then $\Gamma' \cong \Gamma^*$. 
The cases for the cartesian and categorical products are more complicated, as \( \Gamma \times \Gamma \) always has core \( \Gamma \) by Lemma 2.3.29, and \( \Gamma \square \Gamma \) has core \( \Gamma \) for some special graphs \( \Gamma \) (if \( \Gamma \) is a core). By focusing on vertex-transitive retracts, Tardif determined the structure of all vertex-transitive retracts of cartesian products.

**Proposition 3.2.8 ([75])** Let \( \Lambda \) be a vertex-transitive retract of the cartesian product \( \square_{i=1}^{n} \Gamma_i \). Then \( \Lambda \cong \square_{i=1}^{n} \Gamma'_i \), where each \( \Gamma'_i \) is a subgraph of \( \Gamma_i \).

Then, in an attempt to resolve Hedetniemi’s conjecture via retracts of categorical products, Larose and Tardif proved Theorem 2.3.30, which states that if a vertex-transitive core is also projective, then whenever it is the core of a categorical product, it is the core of one of the factors.
Chapter 4

Cores of imprimitive, symmetric $pq$ graphs

The purpose of this chapter is to state the main result of this thesis, Theorem 4.1.2, which is the complete classification of the cores of all imprimitive symmetric graphs of order $pq$, where $p$ and $q$ are prime. The proof of Theorem 4.1.2 will be given in Chapters 5 and 6.

Theorem 4.1.2 is based on the classification of imprimitive symmetric graphs of order $pq$. This classification begun with Cheng and Oxley in [10], where they classified all symmetric graphs of order $2q$. Subsequently, Wang and Xu [81] classified all symmetric graphs of order $3q$. Praeger, Wang and Xu then completed the classification in [61], by determining all imprimitive symmetric graphs of order $pq$, for $p \geq 5$. Three graph families arise from this classification, namely the circulants, incidence graphs and Marušič-Scapellato graphs.

In Section 4.1, we state the classification of imprimitive, symmetric $pq$ graphs in Theorem 4.1.1, along with the classification of the cores of these graphs in Theorem 4.1.2. In Section 4.2, we define the symmetric circulants of order $pq$. In Section 4.3, we define the symmetric incidence graphs of order $pq$, and determine their cores. Finally, in Section 4.4, we define both the imprimitive, and the primitive symmetric Marušič-Scapellato graphs of order $pq$. 
4.1 Imprimitive symmetric graphs of order $pq$, and their cores

Three distinct families of graphs arise from the classification given in Theorem 4.1.1, namely the circulants (given in Table 4.1), the incidence graphs and the Marušić-Scapellato graphs (both given in Table 4.2). We postpone the definitions of these graphs to Sections 4.2, 4.3 and 4.4.

**Theorem 4.1.1** ([10, 61, 81]) Let $p$ and $q$ be primes such that $p < q$, and let $\Gamma$ be an $\text{Aut}(\Gamma)$-imprimitive symmetric graph of order $pq$. Then $\Gamma$ is isomorphic to one of the graphs shown in Tables 4.1 and 4.2.

Following on from this classification, we now state the main result of this thesis.

**Theorem 4.1.2** Let $p$ and $q$ be primes such that $p < q$, and let $\Gamma$ be an $\text{Aut}(\Gamma)$-imprimitive symmetric graph of order $pq$. Then $\Gamma^*$ is given in the second last column of Tables 4.1 and 4.2.

As shown in Tables 4.1 and 4.2, in many cases we determine $\Gamma^*$ completely. In other cases we prove that either $\Gamma$ is a core or $\Gamma^*$ is isomorphic to one of two graphs. As seen in Table 4.1, determining the core of $G(q, r)[K_p] - pG(q, r)$ is reduced to the problems of computing the chromatic and clique numbers of a circulant graph. Unfortunately, the latter problems are both NP-hard even for circulant graphs [11]. (In fact, determining the clique number remains NP-hard even for circulant graphs of prime orders [11, Theorem 2].) Also in Table 4.1, we see that determining the core of $G(pq; r, s, u)$ is reduced to the problem of deciding whether there exists a homomorphism, or a homomorphism with certain properties, between $G(p, s)$ and $G(q, u)$. The latter problems are, once again, difficult in general.

4.2 Symmetric circulants of orders $p$ and $pq$

By Theorem 2.3.22, for a vertex-transitive graph $\Gamma$, $|V(\Gamma^*)|$ divides $|V(\Gamma)|$. This implies that the core of any symmetric graph of order $pq$ (where $p$ and $q$ are prime)
CHAPTER 4. CORES OF IMPRIMITIVE, SYMMETRIC PQ GRAPHS

<table>
<thead>
<tr>
<th>Graph $\Gamma$</th>
<th>$pq$</th>
<th>Conditions</th>
<th>Core $\Gamma^*$</th>
<th>Proofs</th>
</tr>
</thead>
<tbody>
<tr>
<td>$G(2q, r)$</td>
<td>$2q$</td>
<td>$q \geq 3$</td>
<td>$K_2$</td>
<td>Lemma 5.1.1</td>
</tr>
<tr>
<td>$G(2, q, r) \cong G(q, r)$ [K₂]</td>
<td>$2q$</td>
<td>$q \geq 3$</td>
<td>$G(q, r)$</td>
<td>Lemma 5.1.2, Theorem 5.1.3</td>
</tr>
<tr>
<td>$G(3q, r) \cong G(3q; r, 2, r)$</td>
<td>$3q$</td>
<td>$q \geq 5$, $r$ even</td>
<td>$G(3q; r, s, r)^*$</td>
<td>Lemma 5.3.1</td>
</tr>
<tr>
<td>$G(3q, r) \cong G(3q; r, 2, 2r)$</td>
<td>$3q$</td>
<td>$q \geq 5$, $r$ odd</td>
<td>$G(3q; r, s, 2r)^*$</td>
<td>Lemma 5.3.1</td>
</tr>
<tr>
<td>$K_3 [K_q]$</td>
<td>$3q$</td>
<td>$q \geq 5$</td>
<td>$K_3$</td>
<td>Theorem 5.1.3</td>
</tr>
<tr>
<td>$G(p, s) [K_p]$</td>
<td>$pq$</td>
<td>$p \geq 2$</td>
<td>$G(p, s)$</td>
<td>Theorem 5.1.3</td>
</tr>
<tr>
<td>$G(q, r) [K_p]$</td>
<td>$pq$</td>
<td>$p \geq 5$</td>
<td>$G(q, r)$</td>
<td>Theorem 5.1.3</td>
</tr>
<tr>
<td>$G(p, s) [K_q] - qG(p, s)$</td>
<td>$pq$</td>
<td>$p \geq 5$</td>
<td>$G(p, s)$</td>
<td>Theorem 5.2.3</td>
</tr>
<tr>
<td>$G(q, r) [K_p] - pG(q, r)$</td>
<td>$pq$</td>
<td>$p \geq 5$, $\chi(G(q, r)) \leq p$</td>
<td>$G(q, r)$</td>
<td>Theorem 5.2.3</td>
</tr>
<tr>
<td>$G(q, r) [K_p] - pG(q, r)$</td>
<td>$pq$</td>
<td>$p \geq 5$, $\omega(G(q, r)) \geq p$</td>
<td>$K_p$</td>
<td>Theorem 5.2.3</td>
</tr>
<tr>
<td>$G(q, r) [K_p] - pG(q, r)$</td>
<td>$pq$</td>
<td>$p \geq 5$, $\chi(G(q, r)) &gt; p &gt; \omega(G(q, r))$</td>
<td>$\Gamma^* \cong \Gamma$</td>
<td>Theorem 5.2.3</td>
</tr>
<tr>
<td>$G(pq; r, s, u) \text{ with } t \in H(q, r)$</td>
<td>$pq$</td>
<td>$p \geq 3$, $G(p, s) \rightarrow G(q, u)$</td>
<td>$G(p, s)$</td>
<td>Theorem 5.3.3</td>
</tr>
<tr>
<td>$G(pq; r, s, u) \text{ with } t \in H(q, r)$</td>
<td>$pq$</td>
<td>$p \geq 3$, $G(q, u) \rightarrow G(p, s)$</td>
<td>$G(q, u)$</td>
<td>Theorem 5.3.3</td>
</tr>
<tr>
<td>$G(pq; r, s, u) \text{ with } t \notin H(q, r)$</td>
<td>$pq$</td>
<td>$p \geq 3$, $G(q, u) \rightarrow G(p, s), G(p, s) \rightarrow G(q, u)$</td>
<td>$\Gamma^* \cong \Gamma$</td>
<td>Theorem 5.3.3</td>
</tr>
<tr>
<td>$G(pq; r, s, u) \text{ with } t \notin H(q, r)$</td>
<td>$pq$</td>
<td>$p \geq 3$, $\exists \eta : G(p, s) \rightarrow G(q, u)$ such that each $(i, j) \in A(G(p, s))$ with $j - i = a^l$ satisfies $\eta(j) - \eta(i) \in \ell H(q, r)$</td>
<td>$G(p, s)$</td>
<td>Theorem 5.3.9</td>
</tr>
<tr>
<td>$G(pq; r, s, u) \text{ with } t \notin H(q, r)$</td>
<td>$pq$</td>
<td>$p \geq 3$, $\exists \zeta : G(q, u) \rightarrow G(p, s)$ such that each $(x, y) \in A(G(q, u))$ with $y - x \in \ell \ell H(q, r)$ satisfies $\zeta(y) - \zeta(x) = a^l$</td>
<td>$G(q, u)$</td>
<td>Theorem 5.3.9</td>
</tr>
<tr>
<td>$G(pq; r, s, u) \text{ with } t \notin H(q, r)$</td>
<td>$pq$</td>
<td>$p \geq 3$, neither $\eta$ nor $\zeta$ exist</td>
<td>$\Gamma^* \cong \Gamma$</td>
<td>Theorem 5.3.9</td>
</tr>
</tbody>
</table>

Table 4.1: Symmetric Circulant Graphs of order $pq$, $p < q$, and their Cores
CHAPTER 4. CORES OF IMPRIMITIVE, SYMMETRIC PQ GRAPHS

Table 4.2: Incidence and Marušić-Scapellato Graphs of order $pq$, $p < q$, and their Cores

has order $p$, $q$ or $pq$. So we must begin by providing the classifications for the symmetric graphs of order $p$, and the imprimitive symmetric graphs of order $pq$.

Before we state these classifications, we note that for any disconnected symmetric graph $\Gamma$, the connected components are all symmetric and isomorphic to one another. Hence there exists an isomorphism mapping each connected component of $\Gamma$ onto one specific connected component of $\Gamma$, and this isomorphism is a retraction of $\Gamma$. If $\Gamma$ has order $pq$, the connected components will be symmetric graphs of order $p$ or $q$ (all symmetric graphs of prime order are connected), so the core of $\Gamma$ will be one of the connected components. So for the rest of this thesis we assume that $\Gamma$ is connected.

We begin with symmetric graphs of order $p$. For any prime $p$, $\text{Aut}(\mathbb{Z}_p) = \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$, where $\mathbb{Z}_p^*$ is the multiplicative group of integers mod $p$.

**Definition 4.2.1 ($G(p, r)$)** For each divisor $r$ of $p-1$ there exists a unique subgroup $H(p, r) \leq \mathbb{Z}_p^*$ of order $r$, where $H(p, r) \cong \mathbb{Z}_r$. Define

$$G(p, r) := \text{Cay}(\mathbb{Z}_p, H(p, r)).$$

**Theorem 4.2.2 ([8, Theorem 3])** Let $p$ be a prime. Then $\Gamma$ is a connected symmetric graph of order $p$ if and only if $\Gamma \cong G(p, r)$ for some even divisor $r$ of $p-1$. Moreover, $G(p, r)$ has valency $r$, and if $r < p-1$, then $\text{Aut}(G(p, r)) \cong \mathbb{Z}_p \times H(p, r)$ is a Frobenius group in its action on the vertex set of $G(p, r)$, while $G(p, p-1) = K_p$.

In [79, Corollary 2.11], Thomson and Zhou note that $G(p, r)$ is a Frobenius graph.
in a different setting.

The symmetric circulant $G(13, 4) = \text{Cay}(\mathbb{Z}_{13}, H(13, 4))$ is shown in Figure 4.1, with $H(p, r) = \{1, 5, 8, 12\}$.

![Figure 4.1: The symmetric prime order circulant $G(13, 4)$.](image)

Circulant graphs also provide us with our first class of symmetric $pq$ graphs. In what follows we present a number of constructions, some of which are based on the symmetric circulants of prime order, which are symmetric $pq$ circulants by [10, 61, 81].

**Definition 4.2.3** ($G(2q, r)$ and $G(2, q, r)$) Let $\mathcal{A}$ and $\mathcal{A}'$ be two disjoint copies of $\mathbb{Z}_q$, where for each $i \in \mathbb{Z}_q$ we denote corresponding elements of $\mathcal{A}$ and $\mathcal{A}'$ by $i$ and $i'$ respectively. Also let $r$ be a divisor of $q - 1$ and $H(q, r)$ be the unique subgroup of $\mathbb{Z}_q^*$ of order $r$. We define $G(2q, r)$ [10] to be the graph with vertex set

$$V(G(2q, r)) = \mathcal{A} \cup \mathcal{A}'$$
and edge set
\[ E(G(2q, r)) = \{ [x, y'] \mid x, y \in \mathbb{Z}_q \text{ and } y - x \in H(q, r) \} . \]

Further, if \( r \) is an even divisor of \( q - 1 \), then \( G(2, q, r) \) from [10] is the graph with vertex set
\[ V(G(2, q, r)) = \mathcal{A} \cup \mathcal{A}' \]
and edge set
\[ E(G(2, q, r)) = \{ [x, y], [x', y], [x, y'], [x', y'] \mid x, y \in \mathbb{Z}_q \text{ and } y - x \in H(q, r) \} . \]

It was proved in [10, Lemmas 2.1 and 2.2] that both \( G(2q, r) \) and \( G(2, q, r) \) are symmetric. We now show that they are circulants.

**Proposition 4.2.4** The graphs \( G(2q, r) \) and \( G(2, q, r) \) are both circulants.

**Proof** In [10, Section 2] it was shown that both \( G(2q, r) \) and \( G(2, q, r) \) have automorphisms \( \tau, \rho \), where \( \tau(i) = i + 1, \tau(i') = (i + 1)' \), \( \rho(i) = (-i)' \) and \( \rho(i') = -i \). In fact, \( G(2q, r) \) and \( G(2, q, r) \) also have automorphisms \( \tau_a \) for each \( a \in H(q, r) \), where \( \tau_a(i) = ai + 1 \) and \( \tau_a(i') = (ai + 1)' \) (this is easy to check). So let \( a = -1 \). Then we have the automorphism \( \tau_{-1}\rho \), where
\[ \tau_{-1}\rho(i) = (i + 1)' \quad \text{and} \quad \tau_{-1}\rho(i') = i + 1. \] (4.2.1)

Since \( q \) is an odd prime, \( 2 \) generates \( \mathbb{Z}_q \). Thus, for each \( i, j \in \mathcal{A}, (\tau_{-1}\rho)^n(i) = i + n_1 = j \) for some even integer \( n_1 \). And for each \( i \in \mathcal{A} \) and \( j' \in \mathcal{A}', (\tau_{-1}\rho)^n(i) = (i + n_2)' = j' \) for some odd integer \( n_2 \). Hence \( \langle \tau_{-1}\rho \rangle \) is transitive on \( \mathcal{A} \cup \mathcal{A}' \).

Now, \( \langle \tau_{-1}\rho \rangle \) is a subgroup of the automorphism groups of \( G(2q, r) \) and \( G(2, q, r) \), and these automorphism groups both act faithfully on \( \mathcal{A} \cup \mathcal{A}' \). Thus \( \langle \tau_{-1}\rho \rangle \) is faithful on \( \mathcal{A} \cup \mathcal{A}' \), and as such the identity is the only element of \( \langle \tau_{-1}\rho \rangle \) which fixes every vertex of \( \mathcal{A} \cup \mathcal{A}' \). From Equation 4.2.1,
\[ (\tau_{-1}\rho)^n(i) = i + n \equiv i \mod q, \quad (\tau_{-1}\rho)^n(i') = (i + n)' \equiv i \mod q \]
and \( (\tau_{-1}\rho)^n \) fixes every vertex of \( \mathcal{A} \cup \mathcal{A}' \) if and only if \( n \) is a multiple of \( 2q \). Thus
\(|\langle\tau-1,\rho\rangle\) = 2q. So by Corollary 2.1.3, \(\langle\tau-1,\rho\rangle\) is regular on \(A \cup A'\). Therefore, by Definition 2.2.9 and Theorem 2.2.10, \(G(2q, r)\) and \(G(2, q, r)\) are circulants.

**Definition 4.2.5** \((G(3q, r))\) For each divisor \(r\) of \(q - 1\), \(G(3q, r)\) [81] is the graph with vertex set

\[ V(G(3q, r)) = \mathbb{Z}_3 \times \mathbb{Z}_q = \{(i, x) \mid i \in \mathbb{Z}_3, x \in \mathbb{Z}_q\} \]

and edge set

\[ E(G(3q, r)) = \{[(i, x), (i + 1, y)] \mid i \in \mathbb{Z}_3, x, y \in \mathbb{Z}_q \text{ and } y - x \in H(q, r)\} \].

It was proved in [81, Example 3.4] that \(G(3q, r)\) is a connected symmetric graph. Moreover, \(G(3q, r)\) is a circulant graph by [81, Lemma 3.6 and Theorem 3].

**Definition 4.2.6** \((G(pq; r, s, u))\) When \(p \geq 3\), let \(s\) be an even divisor of \(p - 1\) with \(H(p, s) = \langle a \rangle \leq \mathbb{Z}_p^*\), let \(r\) be a divisor of \(q - 1\) with \(H(q, r) = \langle c \rangle \leq \mathbb{Z}_q^*\). Further let \(t \in \mathbb{Z}_q^*\) such that \(t^s \in -H(q, r)\), and let \(u\) be the least common multiple of \(r\) and the order of \(t\) (which we denote by \(o(t)\)) in \(\mathbb{Z}_q^*\). Then \(G(pq; r, s, u)\) [61] is the graph with vertex set

\[ V(G(pq; r, s, u)) = \mathbb{Z}_p \times \mathbb{Z}_q = \{(i, x) \mid i \in \mathbb{Z}_p, x \in \mathbb{Z}_q\} \],

such that vertices \((i, x)\) and \((j, y)\) are adjacent if and only if there exists an integer \(l\) such that

\[ j - i = a^l \text{ and } y - x \in t^lH(q, r). \]

The graphs \(G(pq; r, s, u)\) are independent of the choice of \(a\) and \(t\) such that \(\text{lcm}\{o(t), r\} = u\), up to isomorphism, since \(G(pq; r, s, u) \cong G(pq; r', s', u')\) if and only if \(r = r', s = s'\) and \(u = u'\) by [61, Theorem 3.5]. It was proved in [61, Theorem 3.5] that \(G(pq; r, s, u)\) is symmetric whenever \(r < q - 1\) and \(s < p - 1\), or \(r < u\) and \(s = p - 1\). Furthermore, in the proof of [61, Theorem 3.5] it was shown that \(G(pq; r, s, u)\) is a Cayley graph on \(\mathbb{Z}_p \times \mathbb{Z}_q\). Since \(p \neq q\) are primes, \(\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}\) and hence \(G(pq; r, s, u)\) is a circulant graph.
The symmetric circulant $G(21; 3, 2, 6)$ is shown in Figure 4.2, with $t = 3, t \notin H(7, 3), a = 2$ and $c = 2$.

![Figure 4.2: The symmetric circulant $G(21; 3, 2, 6)$, with $t = 3, a = 2$ and $c = 2.$](image)

In addition to the constructions of symmetric circulants in Definitions 4.2.3, 4.2.5 and 4.2.6, we construct symmetric $pq$ circulants using the lexicographic product.

Denote by $K_{q,q}$ the complete bipartite graph and $K_{q,q,q}$ the complete tripartite graph, with each part having $q$ vertices.

**Example 4.2.7** From Proposition 2.2.7, the lexicographic product $\Gamma_1 [\Gamma_2]$ is symmetric if $\Gamma_1$ is symmetric and $\Gamma_2$ has no edges. Hence the following graphs are symmetric [10,61,81]:

- $K_2 [K_q] = K_{q,q}$, where $q > 2$;
- $K_3 [K_q] = K_{q,q,q}$ and $G(q,r) [K_3]$, where $q > 3$;
- $G(p,s) [K_q]$ and $G(q,r) [K_p]$, where $5 \leq p < q$.
- $G(p,s) [K_q] - qG(p,s)$ and $G(q,r) [K_p] - pG(q,r)$, where $5 \leq p < q$. 
As mentioned in [61, Section 3], the graphs in Example 4.2.7 are all circulants since each of them admits a cyclic group of order $pq$ acting regularly on the vertex set.

Definitions 4.2.3, 4.2.5, 4.2.6 and Example 4.2.7 define all graphs given in Table 4.1.

### 4.3 Incidence Graphs

The second class of imprimitive symmetric $pq$ graphs are the incidence graphs of two specific $t$-$(v, k, \lambda)$ designs. So firstly, we define $t$-$(v, k, \lambda)$ designs and incidence graphs.

**Definition 4.3.1** A $t$-$(v, k, \lambda)$ design $\mathcal{D}$ is a set $\mathcal{P}$ of $v$ points, along with a set $\mathcal{B}$ of $k$-subsets of points, called blocks, such that every set of $t$ points is contained in exactly $\lambda$ blocks.

**Definition 4.3.2** The incidence graph $X(\mathcal{D})$ of a design $\mathcal{D}$ is the graph with vertex set

$$V(X(\mathcal{D})) = \mathcal{P} \cup \mathcal{B}$$

and edge set

$$E(X(\mathcal{D})) = \{[u, v] \mid u \in \mathcal{P}, v \in \mathcal{B} \text{ and } u \in v\}.$$ 

The nonincidence graph $X'(\mathcal{D})$ of design $\mathcal{D}$ has

$$V(X(\mathcal{D})) = \mathcal{P} \cup \mathcal{B}$$

and

$$E(X(\mathcal{D})) = \{[u, v] \mid u \in \mathcal{P}, v \in \mathcal{B} \text{ and } u \not\in v\}.$$ 

We now give two designs whose incidence graphs have order $pq$, and are symmetric by [10].

**Example 4.3.3** $(X(PG(d - 1, r))$ and $X'(PG(d - 1, r)))$ Let $PG(d - 1, r)$ be the $(d - 1)$-dimensional projective space over the finite field $GF(r)$ (for any prime power
r and integer \( d > 2 \). Then \( PG(d - 1, r) \) is a design, with points and blocks the 1-dimensional and \((d - 2)\)-dimensional subspaces (points and hyperplanes) of \( PG(d - 1, r) \) respectively. \( X(PG(d - 1, r)) \) and \( X'(PG(d - 1, r)) \) have \( 2^{\frac{rd}{r-1}} \) vertices, which is a product of two primes when \( \frac{rd}{r-1} \) is prime.

**Example 4.3.4** (\( X(H(11)) \) and \( X'(H(11)) \)) The unique 2-(11, 5, 2) design \( H(11) \) has as its points the elements of the group \( \mathbb{Z}_{11} \), whilst the blocks are the sets \( R + i = \{ x + i \mid x \in R \} \), where \( i \in \mathbb{Z}_{11} \) and \( R = \{ 1, 3, 4, 5, 9 \} \). This design gives the graphs \( X(H(11)) \) and \( X'(H(11)) \), both of order 22 (note that \( X(H(11)) \cong G(22, 5) \)).

From Definition 4.3.2, all incidence graphs are bipartite, which means that for the incidence graph \( \Gamma \), \( \chi(\Gamma) = \omega(\Gamma) = 2 \) and \( \Gamma^* \cong K_2 \). So we end this section with a formal statement of this result, along with a short proof which uses the imprimitivity of these graphs.

**Theorem 4.3.5** Let \( \Gamma \) be isomorphic to one of the graphs \( X(H(11)) \), \( X'(H(11)) \), \( X(PG(d - 1, r)) \) or \( X'(PG(d - 1, r)) \), with \( p = 2 \) and \( q = \frac{rd-1}{r-1} \) a prime. Then \( \Gamma \) is bipartite and \( \Gamma^* \cong K_2 \).

**Proof** In [10, 54], these graphs were shown to be connected, imprimitive 2-arc transitive graphs with \( |V(\Gamma)| = 2q \) and a system of imprimitivity containing two blocks of size \( q \), where \( q = 11 \) for \( X(H(11)) \), \( X'(H(11)) \) and \( q = \frac{rd-1}{r-1} \) for \( X(PG(d - 1, r)) \), \( X'(PG(d - 1, r)) \). But by Lemma 2.3.26, these blocks must be independent sets, so the system of imprimitivity gives a bipartition of \( V(\Gamma) \). Hence \( \Gamma \to K_2 \), and since \( \Gamma \) contains an edge, \( \Gamma \) contains the induced subgraph \( K_2 \). So we have a retraction to \( K_2 \) which is a core. Hence \( \Gamma^* \cong K_2 \). \( \square \)

### 4.4 Marušič-Scapellato graphs

#### 4.4.1 Imprimitive Marušič-Scapellato graphs

The final class of imprimitive, symmetric \( pq \) graphs are the graphs which admit the group \( T = SL(2, 2^a) \) for some \( a > 1 \), as a group of automorphisms acting imprimitively on the vertex set. These graphs are known as Marušič-Scapellato...
graphs, and were first defined by these authors in [55]. We adopt the definition and notation in [61, Definition 3.6].

**Definition 4.4.1 (Γ(\(a, m, S, U\))** Let \(m > 1\) be a divisor of \(2^a - 1\), \(S = -S\) be a symmetric subset of \(\mathbb{Z}_m^*\), \(U\) be a subset of \(\mathbb{Z}_m\) and \(w\) be a primitive element of \(\text{GF}(2^a)\). Then the **Marušič-Scapellato graph** \(\Gamma = \Gamma(\(a, m, S, U\))\) is the graph with vertex set

\[
V(\Gamma) = \text{PG}(1, 2^a) \times \mathbb{Z}_m \ (\text{with } \text{PG}(1, 2^a) = \text{GF}(2^a) \cup \{\infty\}),
\]

such that \((\infty, r) \in V(\Gamma)\) has neighbourhood

\[
N_\Gamma((\infty, r)) = \{(\infty, r + s) \mid s \in S\} \cup \{(x, r + u) \mid x \in \text{GF}(2^a), u \in U\}
\]

and \((x, r) \in V(\Gamma) \ (x \in \text{GF}(2^a))\) has neighbourhood

\[
N_\Gamma((x, r)) = \{(x, r + s) \mid s \in S\} \cup \{(\infty, r - u) \mid u \in U\} \cup \{(x + w^i, -r + u + 2i) \mid i \in \mathbb{Z}_{2^a-1}, u \in U\}.
\]

From Definition 4.4.1, for the special case when \(S = \emptyset\), \((\infty, r) \in V(\Gamma)\) has neighbourhood

\[
N_\Gamma((\infty, r)) = \{(x, r + u) \mid x \in \text{GF}(2^a), u \in U\},
\]

\((x, r) \in V(\Gamma) \ (x \in \text{GF}(2^a))\) has neighbourhood

\[
N_\Gamma((x, r)) = \{(\infty, r - u) \mid u \in U\} \cup \{(x + w^i, -r + u + 2i) \mid i \in \mathbb{Z}_{2^a-1}, u \in U\},
\]

and \(\text{val}(\Gamma) = 2^a |U|\).

The Marušič-Scapellato graph \(\Gamma(2, 3, \emptyset, \{0\})\) is shown in Figure 4.3, where \(z = w^2\) and \(1 = w^3\).
Marušić and Scapellato [56] show that $SL(2, 2^a) \leq Aut(\Gamma)$, and that $\Gamma$ is $SL(2, 2^a)$-vertex-transitive. Further, they show that $\Gamma$ is $SL(2, 2^a)$-imprimitive with a complete block system $\Sigma = \{B_x \mid x \in PG(1, 2^a)\}$ ($B_x = \{(x, r) \mid r \in \mathbb{Z}_m\}$), and that $\Gamma$ is $SL(2, 2^a)$-symmetric if $\Gamma = \Gamma(a, m, \emptyset, \{u\})$ with $u \in \mathbb{Z}_m$. (A complete block system is a system of imprimitivity $\Sigma$ of a graph $\Gamma$ where, for any two distinct elements $B_1, B_2 \in \Sigma$, there exists vertices $b_1 \in B_1$ and $b_2 \in B_2$ such that $[b_1, b_2] \in E(\Gamma)$.)

In fact, the Marušić-Scapellato graphs are the only $SL(2, 2^a)$-imprimitive graphs, up to isomorphism, which admit a complete block system with $2^a + 1$ elements of order $m$.

**Theorem 4.4.2 ([56, Theorem 3.1])** Let $m > 1$ be a divisor of $2^a - 1$ and $T \cong SL(2, 2^a)$. A nontrivial graph $\Gamma$ is a $T$-imprimitive orbital graph of $T$ on $V(\Gamma)$, with $\Sigma = \{B_x \mid x \in PG(1, 2^a)\}$ ($|B_x| = m$) as the complete block system of imprimitivity, if and only if $\Gamma \cong \Gamma(a, m, \emptyset, \{u\})$ with $u \in \mathbb{Z}_m$.

In [81], Wang and Xu define graphs similar to the Marušić-Scapellato graphs of order $3q$. 
Definition 4.4.3 \((F(s) \text{ and } F'(s))\) For \(s \geq 1\), let \(T = \text{PSL}(2, 2^{2^s})\) be a group acting transitively on the set \(V\) of order \(3q\) (such an action exists; see [81, Lemma 4.6]). Then \(F_0(s), F_1(s)\) and \(F_2(s)\) are defined as orbital graphs of \(T\) on \(V\). These graphs are isomorphic, and the action of \(T\) on \(V\) is imprimitive, with a complete block system \(\Sigma = \{B_x \mid x \in \text{PG}(1, 2^{2^s})\}\) \((B_x = \{(x, r) \mid r \in \mathbb{Z}_3\})\) by [81, pp. 211,212]. We define \(F(s) = F_0(s)\) and \(F'(s) = F_1(s) \cup F_2(s)\) as in [81].

Since \(2^{2^s}\) is a power of two, \(\text{PSL}(2, 2^{2^s}) = \text{SL}(2, 2^{2^s})\), so that both \(F(s)\) and \(F'(s)\) are orbital graphs of \(\text{SL}(2, 2^{2^s})\). But by Theorem 4.4.2, \(F_0(s)\) is a nontrivial orbital graph of \(\text{SL}(2, 2^{2^s})\) with system of imprimitivity \(\Sigma\) if and only if \(F(s) \cong \Gamma(2^s, 3, \emptyset, \{0\})\). So

\[
F(s) \cong \Gamma(2^s, 3, \emptyset, \{0\})
\]

and

\[
F'(s) \cong \Gamma(2^s, 3, \emptyset, \{1, 2\})
\]

are both Marušić-Scapellato graphs, and are symmetric by [81].

Using Definition 4.4.1, Praeger, Wang and Xu show which Marušić-Scapellato graphs of order \(pq\) are symmetric for \(p \geq 5\). (Note: if \(2^a + 1\) is a prime, then \(a = 2^s\) where \(s \geq 0\), and \(2^{2^s} + 1\) is called a Fermat number (not all Fermat numbers are prime). For each integer \(s \geq 0\), the Fermat number \(2^{2^s} + 1\) is denoted by \(F_s\).

Theorem 4.4.4 ( [61, Theorem 3.7 (b) and Lemma 4.9 (a)]) Let \(q = 2^a + 1 = 2^{2^s} + 1\) be a Fermat prime, where \(a = 2^s\) with \(s \geq 1\), and let \(p\) be a prime divisor of \(2^{2^s} - 1\). Then

\[
G = \text{SL}(2, 2^{2^s}) \rtimes \mathbb{Z}_{2^s} \leq \text{SL}(2, 2^{2^s}) \rtimes \mathbb{Z}_{2^s} = \Gamma \text{L}(2, 2^{2^s})
\]

acts symmetrically on the Marušić-Scapellato graph \(\Gamma = \Gamma(2^s, p, S, U)\) if and only if \(S = \emptyset\) and either

\[
U = \{u\}
\]

for some \(u \in \mathbb{Z}_p\), or

\[
U = U_{e, i} := \{i 2^{cj} : 0 \leq j < \frac{d}{c}\}
\]

for some \(i \in \mathbb{Z}^*_p\) and divisor \(e \geq 1\) of \(\gcd(d, 2^s)\) with \(1 < \frac{d}{c} < p - 1\), where \(d\) is the
order of 2 in $\mathbb{Z}_p^*$. In the former case, $\Gamma \cong \Gamma(2^s, p, \emptyset, \{0\})$ and $\text{val}(\Gamma) = 2^{2s}$; in the latter case, $\text{val}(\Gamma) = 2^{2s} \frac{d}{e}$.

Note that

$$1 < |U_{e,i}| = \frac{d}{e} < p - 1$$

by [61, Lemma 4.9 (b)].

### 4.4.2 Primitive Marušič-Scapellato graphs

To determine the cores of imprimitive, symmetric Marušič-Scapellato graphs, we need a result [7, Section 3.5] on the cores of primitive Marušič-Scapellato graphs. So here we make a short digression to discuss primitive Marušič-Scapellato graphs.

Let $V$ be a vector space over a field $F$. A bilinear form is a function $B : V \times V \to F$ for which

(i) $B(u + v, w) = B(u, w) + B(v, w),$

(ii) $B(u, v + w) = B(u, v) + B(u, w),$

(iii) $B(\lambda u, v) = B(u, \lambda v) = \lambda B(u, v).$

A bilinear form $B$ is symplectic if it is

(i) totally isotropic: $B(v, v) = 0$ for all $v \in V$,

(ii) nondegenerate: if $B(u, v) = 0$ for all $v \in V$ then $u = 0$.

Totally isotropic forms are also called alternating forms. If $B(u, v) = 0$ for two vectors $u, v \in V$, then $u$ and $v$ are said to be orthogonal with respect to $B$. A symplectic vector space is a vector space equipped with a symplectic bilinear form.

Now let $V$ be a 4-dimensional vector space $V = V(4, 2^{2s-1})$ over the finite field $GF(2^{2s-1})$, where $s \geq 2$. We define a symplectic form $B(u, v) := u^T H v$, where

$$H := \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{pmatrix}.$$
The symplectic group \( \text{Sp}(4, 2^{2s-1}) \) is the group of all matrices \( M \in \text{GL}(4, 2^{2s-1}) \), for which \( M^T H M = H \). (Note: choosing a different \( H \) gives a subgroup conjugate to \( \text{Sp}(4, 2^{2s-1}) \) in \( \text{GL}(4, 2^{2s-1}) \).) Thus each element of \( \text{Sp}(4, 2^{2s-1}) \) acts on \( V \) via a linear transformation which preserves \( B \), so that \( B(Mu, Mv) = B(u, v) \).

The kernel of this action is the group \( Z \cap \text{Sp}(4, 2^{2s-1}) \), where

\[
Z = \left\{ \lambda I \mid \lambda \in \text{GF}(2^{2s-1}) \setminus \{0\} \right\}
\]

and \( I \) is the identity matrix. We define the projective symplectic group

\[
\text{PSp}(4, 2^{2s-1}) = \text{Sp}(4, 2^{2s-1})/(Z \cap \text{Sp}(4, 2^{2s-1}))
\]

to be the permutation group induced by the action of \( \text{Sp}(4, 2^{2s-1}) \) on the 1-dimensional subspaces of \( V \).

The map \( T : V \to V \) is semilinear if

\[
T(u + v) = T(u) + T(v)
\]

for all \( u, v \in V \), and there exists some \( \sigma \in \text{Aut}(\text{GF}(2^{2s-1})) \) such that

\[
T(\lambda v) = \sigma(\lambda) T(v)
\]

for all \( \lambda \in \text{GF}(2^{2s-1}) \) and \( v \in V \). The semilinear group \( \Gamma \text{L}(4, 2^{2s-1}) \) is the group of all semilinear transformations of \( V \). \( \text{GL}(4, 2^{2s-1}) \) is the subgroup of \( \Gamma \text{L}(4, 2^{2s-1}) \) consisting of all elements with \( \sigma = 1_{\text{Aut}(\text{GF}(2^{2s-1}))} \).

The symplectic semilinear group \( \Gamma \text{Sp}(4, 2^{2s-1}) \) is the group of all \( T \in \Gamma \text{L}(4, 2^{2s-1}) \) such that there exists some \( \lambda \in \text{GF}(2^{2s-1}) \) and \( \sigma \in \text{Aut}(\text{GF}(2^{2s-1})) \) with

\[
B(T(u), T(v)) = \lambda \sigma(B(u, v)).
\]

Each element of \( \Gamma \text{Sp}(4, 2^{2s-1}) \) acts on \( V \) via a semilinear transformation, and the kernel of this action is \( Z \). We define the projective symplectic semilinear group
PGSp(4, 2^{2s-1}) = ΓSp(4, 2^{2s-1})/Z to be the permutation group induced by the action of ΓSp(4, 2^{2s-1}) on V. For more on classical groups, see [77].

So for each PSp(4, 2^{2s-1}) ≤ G ≤ PGSp(4, 2^{2s-1}), G acts V. This action induces an orbital graph which admits PSp(4, 2^{2s-1}) as a group of automorphisms, with vertices the 1-dimensional subspaces of V.

**Theorem 4.4.5 ([62, Lemma 3.5])** Let PSp(4, 2^{2s-1}) ≤ G ≤ PGSp(4, 2^{2s-1}) act on the set Ω of all 1-dimensional subspaces of a 4-dimensional symplectic vector space V = V(4, 2^{2s-1}) over GF(2^{2s-1}), where s ≥ 2. Then the following hold:

(i) |Ω| = (2^{2s-1} + 1)(2^{2s} + 1), G has rank 3, the subdegrees of G are 1, 2^{2s-1} + 2^{s} and 2^{2s+1}, and all suborbits are self-paired.

(ii) The nontrivial orbital graphs Ψ and Ψ̄, with

\[ E(Ψ) = \{[u, v] ∈ Ω × Ω \mid u ≠ v, B(u, v) = 0}\]  (4.4.1)

are the only (incomplete, nonempty) vertex-primitive graphs on Ω admitting G, and each has automorphism group PGSp(4, 2^{2s-1}).

(iii) If |Ω| = pq, with p < q and p, q primes, then p = 2^{2s-1} + 1 and q = 2^{2s} + 1 are Fermat primes, and these graphs are non-Cayley graphs.

The graphs Ψ and Ψ̄, with |Ω| = pq, p < q and p, q primes are significant for two reasons. The first reason is that PSp(4, 2^{2s-1}) contains an isomorphic copy of PSL(2, 2^{s}) acting imprimitively on the 1-dimensional subspaces of V. Therefore, by Theorem 4.4.2, Ψ and Ψ̄ are primitive Marušič-Scapellato graphs.

**Theorem 4.4.6 ([52, Proof of Theorem 2.1, pp.193])** Let Ψ be the orbital graph outlined in Theorem 4.4.5, with edge set given by Equation 4.4.1. If |Ω| = pq, with p < q and p and q primes, then both Ψ and Ψ̄ are isomorphic to Marušič-Scapellato graphs.

The second reason that Ψ and Ψ̄ are significant is that their cores are known. (Ψ is the graph W_3(2^{2s-1}) in [7].)
Theorem 4.4.7 ([7, Section 3.5]) Let $\Psi$ be the orbital graph outlined in Theorem 4.4.5, with edge set given by Equation 4.4.1. If $|\Omega| = pq$, with $p < q$ and $p$ and $q$ primes, then both $\Psi$ and $\Psi$ have complete cores.
Chapter 5

Circulant Graphs

We now begin the proof of Theorem 4.1.2. The first class of graphs whose cores we determine are the circulants, which are split into four broad classes of graphs. These subclasses are the lexicographic products $\Gamma \left[ K_n \right]$ with $\Gamma$ a prime order circulant, the deleted lexicographic products of circulants of orders $p$ and $q$, $G(2q, r)$ and $G(pq; r, s, u)$. Splitting the circulant case into these specific subclasses has two benefits, the first being that it reduces the number of graphs that we need to determine the cores for (in comparison to the number of symmetric $pq$ circulants in Table 4.1). More importantly, splitting into these subclasses allows the use of the general results on the cores of graph products given in [31, 37, 46], simplifying each case.

In Section 5.1 we determine the core of $G(2q, r)$, along with the lexicographic products. In Section 5.2, we show that all deleted lexicographic products of $G(p, s)$ or $G(q, r)$ are isomorphic to the categorical products $G(p, s) \times K_q$ or $G(q, r) \times K_p$. Hence we determine the cores of all categorical products of symmetric circulants of orders $p$ and $q$ in Lemma 5.2.2, and use this result to determine the cores of all deleted lexicographic products of $G(q, s)$ or $G(q, r)$.

In Section 5.3 we deal with $G(pq; r, s, u)$. Beginning with Section 5.3.1, we show that $G(pq; r, s, u)$ is isomorphic to a spanning subgraph of $G(p, s) \times G(q, r)$. Thus Lemma 5.2.2 gives the core of $G(pq; r, s, u)$ whenever $G(pq; r, s, u) \cong G(p, s) \times G(q, r)$. In Section 5.3.2 we show that even if $G(pq; r, s, u) \not\cong G(p, s) \times G(q, u)$, the core of $G(pq; r, s, u)$ must be $G(p, s)$, $G(q, u)$ or itself. Finally, in Section 5.3.3 we give the conditions under which $G(pq; r, s, u)$ has an induced subgraph isomorphic to either
Chapter 5. Circulant Graphs

$G(p, s)$ or $G(q, u)$.

5.1 Lexicographic products and $G(2q, r)$

Lemma 2.3.26 makes $G(2q, r)$ a straightforward case.

Lemma 5.1.1 Let $\Gamma \cong G(2q, r)$. Then $\Gamma^* \cong K_2$.

Proof By [10, Lemma 3.9], Aut($\Gamma$) has a system of imprimitivity consisting of two blocks of order $q$. By Lemma 2.3.26, these blocks are independent sets, so that this system of imprimitivity is a bipartition of $V(\Gamma)$ into independent sets. Hence $\Gamma \to K_2$.

Since $\Gamma$ has edges, $\Gamma$ contains an induced subgraph isomorphic to $K_2$. Thus the homomorphism $\phi : \Gamma \to K_2$ is a retraction. Finally, $K_2$ is a core, so that $\Gamma^* \cong K_2$. \qed

From Theorem 4.1.1 the graphs $G(q, r) [K_3], G(p, s) [K_q]$ and $G(q, r) [K_p]$ are lexicographic products of the form $\Gamma [K_n]$, where $n = p$ or $q$, and $\Gamma$ is a symmetric prime order circulant. Also, from Theorem 4.2.2, $K_3$ is a symmetric prime order circulant. Thus $K_3 [K_q]$ is a lexicographic product of the form $\Gamma [K_q]$. In addition to these graphs, $G(2, q, r)$ is also isomorphic to a lexicographic product of circulants.

Lemma 5.1.2 $G(2, q, r) \cong G(q, r) [K_2]$.

Proof From Definitions 2.2.5, 4.2.1 and 4.2.3, we define $\eta : V(G(2, q, r)) \to V(G(q, r) [K_2])$ to be the map with

$$\eta(x) = (x, 0)$$

for each $x \in A \subset V(G(2, q, r))$, and

$$\eta(x') = (x, 1)$$

for each $x' \in A' \subset V(G(2, q, r))$. The orders of $V(G(2, q, r))$ and $V(G(q, r) [K_2])$ are both equal to $2q$, and $\eta$ maps each element of $V(G(2, q, r))$ to a unique element in $V(G(q, r) [K_2])$, so both $\eta$ and $\eta^{-1}$ are bijections.
From Definitions 2.2.5, 4.2.1 and 4.2.3, for each edge \([x, y] \in E(G(2, q, r))\), \(y - x \in H(q, r)\), such that \([x, y] \in E(G(q, r))\) and 
\[
\eta([x, y]) = [\eta(x), \eta(y)] = [(x, 0), (y, 0)] \in E(G(q, r) [\overline{K}_2]).
\]
For \([x, y'] \in E(G(2, q, r))\), \(y - x \in H(q, r)\), such that \([x, y] \in E(G(q, r))\) and 
\[
\eta([x, y']) = [\eta(x), \eta(y')] = [(x, 0), (y, 1)] \in E(G(q, r) [\overline{K}_2]).
\]
For \([x', y] \in E(G(2, q, r))\), \(y - x \in H(q, r)\), such that \([x, y] \in E(G(q, r))\) and 
\[
\eta([x', y]) = [\eta(x'), \eta(y)] = [(x, 1), (y, 0)] \in E(G(q, r) [\overline{K}_2]).
\]
For \([x', y'] \in E(G(2, q, r))\), \(y - x \in H(q, r)\), such that \([x, y] \in E(G(q, r))\) and 
\[
\eta([x', y']) = [\eta(x'), \eta(y')] = [(x, 1), (y, 1)] \in E(G(q, r) [\overline{K}_2]).
\]
Hence \(\eta\) is a graph homomorphism.

Finally, \(\overline{K}_2\) has no edges, so by Definitions 2.2.5 and 4.2.1, 
\([[(x, u), (y, v)] \in E(G(q, r) [\overline{K}_2])\) if and only if \(y - x \in H(q, r)\) (for any \(u, v \in V(\overline{K}_2))\). Therefore,
\[
\eta^{-1}([(x, u), (y, v)]) = [\eta^{-1}((x, u)), \eta^{-1}((y, v))] = \begin{cases} 
[x, y] & \text{if } u = 0, v = 0 \\
[x, y'] & \text{if } u = 0, v = 1 \\
x', y & \text{if } u = 1, v = 0 \\
x', y' & \text{if } u = 1, v = 1.
\end{cases}
\]
So by Definition 4.2.3, \(\eta^{-1}([(x, u), (y, v)]) \in E(G(2, q, r))\), and thus \(\eta^{-1}\) is a graph homomorphism. Therefore \(\eta\) is an isomorphism. \(\square\)

So by finding the cores of the general lexicographic products \(G(p, s) [\overline{K}_q]\) and \(G(q, r) [\overline{K}_p]\), we also find the cores of \(G(q, r) [\overline{K}_3]\), \(K_3 [\overline{K}_q]\) and \(G(2, q, r)\).

**Theorem 5.1.3** If \(\Gamma \cong G(p, s) [\overline{K}_q]\), then \(\Gamma^* \cong G(p, s)\). If \(\Gamma \cong G(q, r) [\overline{K}_p]\), then \(\Gamma^* \cong G(q, r)\).
CHAPTER 5. CIRCULANT GRAPHS

Proof Let $\Gamma = G(p, s) \overline{K}_q$. From Definition 2.2.5, the subset

$$\{(u, x) \mid u \in V(G(p, s))\} \subset V(\Gamma)$$

induces a subgraph of $\Gamma$ isomorphic to $G(p, s)$. Therefore $G(p, s) \rightarrow \Gamma$.

Now we define a map $\phi : V(\Gamma) \rightarrow V(G(p, s))$ such that for each $(u, x) \in V(\Gamma)$, $\phi((u, x)) = u$. From Definition 2.2.5, $[(u, x), (v, y)] \in E(\Gamma)$ if and only if $[u, v] \in E(G(p, s))$ (since $\overline{K}_q$ has no edges). Thus, if $[(u, x), (v, y)] \in E(\Gamma)$, then

$$\phi([(u, x), (v, y)]) = [\phi((u, x)), \phi((v, y))] = [u, v] \in E(G(p, s)).$$

Hence $\phi$ is a graph homomorphism from $\Gamma$ to $G(p, s)$, and $\Gamma \leftrightarrow G(p, s)$. Therefore, by Corollary 2.3.20 and Lemma 2.3.14, $\Gamma^* \cong (G(p, s))^* = G(p, s)$.

Similarly, one can show that the core of $\Gamma = G(q, r) \overline{K}_p$ is $G(q, r)$.

5.2 Deleted lexicographic products and categorical products

The third class of symmetric $pq$ circulants are the deleted lexicographic products $G(p, s) \overline{K}_q - qG(p, s)$ and $G(q, r) \overline{K}_p - pG(q, r)$. We begin by proving that these graphs are isomorphic to the categorical products of a symmetric circulant and a complete graph.

Lemma 5.2.1 $G(p, s) \overline{K}_q - qG(p, s) = G(p, s) \times K_q$ and $G(q, r) \overline{K}_p - pG(q, r) = G(q, r) \times K_p$.

Proof Let $\Psi$ be an arbitrary symmetric graph, $n \in \mathbb{N}$ and $\Gamma = \Psi \overline{K}_n - n\Psi$. From Definitions 2.2.5 and 2.2.8,

$$V(\Gamma) = V(\Psi \overline{K}_n - n\Psi) = V(\Psi \overline{K}_n) = V(\Psi \times K_n).$$

From Definition 2.2.8, for $(u, x), (v, y) \in V(\Gamma)$, $[(u, x), (v, y)] \in E(\Gamma)$ if and only if either $[u, v] \in E(\Psi)$ and $x \neq y$, or $u = v$ and $[x, y] \in E(\overline{K}_n)$. However, $\overline{K}_n$ has
Then $\Gamma$ must find the cores of the categorical products $G$. Lemma 5.2.2 Let categorical products. simplifies our task, as more is known about homomorphisms and retractions from $G$. Hence $[(u, x), (v, y)] \in E(\Gamma)$ if and only if $[u, v] \in E(\Psi)$ and $x \neq y$.

Now $K_n$ is complete, so whenever $x \neq y$, $[x, y] \in E(K_n)$. Hence $[(u, x), (v, y)] \in E(\Gamma)$ if and only if $[u, v] \in E(\Psi)$ and $[x, y] \in E(K_n)$. But from Definition 2.2.5, $[(u, x), (v, y)] \in E(\Psi \times K_n)$ if and only if $[u, v] \in E(\Psi)$ and $[x, y] \in E(K_n)$. Hence

$$E(\Gamma) = E(\Psi \mathcal{K}_n) - n\Psi = E(\Psi \times K_n),$$

so that $\Psi [\mathcal{K}_n] - n\Psi = \Psi \times K_n$.

So if $\Psi = G(p, s)$ and $n = q$, then $G(p, s) [\mathcal{K}_q] - qG(p, s) = G(p, s) \times K_q$; if $\Psi = G(q, r)$ and $n = p$, then $G(q, r) [\mathcal{K}_p] - pG(q, r) = G(q, r) \times K_p$. □

Thus in order to determine the cores of the deleted lexicographic products, we must find the cores of the categorical products $G(p, s) \times K_q$ and $G(q, r) \times K_p$. This simplifies our task, as more is known about homomorphisms and retractions from categorical products.

So using Lemma 2.3.29, we determine the cores of $G(p, s) [\mathcal{K}_q] - qG(p, s)$ and $G(q, r) [\mathcal{K}_p] - pG(q, r)$. We begin by looking at the general case when $\Gamma \cong G(p, s) \times G(q, r)$.

**Lemma 5.2.2** Let $\Gamma \cong G(p, s) \times G(q, r)$, where $G(p, s)$ and $G(q, r)$ are symmetric. Then $\Gamma$ is not a core if and only if one of the following conditions hold:

1. $G(p, s) \rightarrow G(q, r)$, in which case $\Gamma^* \cong G(p, s)$;
2. $G(q, r) \rightarrow G(p, s)$, in which case $\Gamma^* \cong G(q, r)$.

**Proof** Let $\Gamma \cong G(p, s) \times G(q, r)$, where $G(p, s)$ and $G(q, r)$ are symmetric. Then by Proposition 2.2.6, $\Gamma$ is symmetric. If $G(p, s) \rightarrow G(q, r)$, then by Lemma 2.3.29, $\Gamma \leftrightarrow G(p, s)$, so that by Lemma 2.3.14, $\Gamma^* \cong G(p, s)^*$. But $G(p, s)$ is a vertex-transitive graph of prime order, so by Corollary 2.3.20, $G(p, s)$ is a core. Therefore, $\Gamma^* \cong G(p, s)$ and $\Gamma$ is not a core. Similarly, if $G(q, r) \rightarrow G(p, s)$, then $\Gamma^* \cong G(q, r)$.

If $\Gamma$ is not a core, then by Theorems 2.3.21 and 2.3.22, $\Gamma^*$ is a symmetric graph of prime order. Therefore, every $\text{Aut}(\Gamma^*)$-invariant partition of $V(\Gamma^*)$ is trivial (since the order of each block of $\text{Aut}(\Gamma^*)$ divides $|V(\Gamma^*)|$), so that $\text{Aut}(\Gamma^*)$ is primitive on $V(\Gamma^*)$. Thus, by Theorem 2.3.31, $\Gamma^*$ is projective.
Lemma 5.2.2, if $G \Gamma$, $G \ast \Gamma$ is not a core, then either $\Gamma$ of prime order, so by Corollary 2.3.20, both $G(p, s)$ and $G(q, r)$ are cores. Hence if $\Gamma$ is not a core, then either $\Gamma \cong G(p, s)$ or $\Gamma \cong G(q, r)$.

Finally, from Lemma 2.3.29, $\Gamma \rightarrow G(p, s)$ and $\Gamma \rightarrow G(q, r)$, thus $\Gamma \ast \rightarrow G(p, s)$ and $\Gamma \ast \rightarrow G(q, r)$ (since $\Gamma \leftrightarrow \Gamma^*$). So if $\Gamma \ast \cong G(p, s)$, then $G(p, s) \rightarrow G(q, r)$, and if $\Gamma \ast \cong G(q, r)$, then $G(q, r) \rightarrow G(p, s)$.

Using Lemma 5.2.2, we now determine the cores of $G(p, s) [\overline{K}_q] - qG(p, s)$ and $G(q, r) [\overline{K}_p] - pG(q, r)$.

**Theorem 5.2.3** If $\Gamma \cong G(p, s) [\overline{K}_q] - qG(p, s)$, then $\Gamma \ast \cong G(p, s)$. Whilst if $\Gamma \cong G(q, r) [\overline{K}_p] - pG(q, r)$, then exactly one of the following holds:

(i) $\chi(G(q, r)) \leq p$, in which case $\Gamma \ast \cong G(q, r)$;

(ii) $\omega(G(q, r)) \geq p$, in which case $\Gamma \ast \cong K_p$;

(iii) $\chi(G(q, r)) > p > \omega(G(q, r))$, in which case $\Gamma$ is a core.

**Proof** Let $\Gamma = G(p, s) [\overline{K}_q] - qG(p, s)$. From Theorem 4.2.2, $K_q \cong G(q, q - 1)$, and $G(q, q - 1)$ is symmetric. So by Lemma 5.2.1, $\Gamma \cong G(p, s) \times G(q, q - 1)$. Since $p < q$, $\chi(G(p, s)) < q$, and thus $G(p, s) \rightarrow G(q, q - 1)$. Therefore, by Lemma 5.2.2, $\Gamma \ast \cong G(p, s)$.

Now let $\Gamma = G(q, r) [\overline{K}_p] - pG(q, r)$. From Theorem 4.2.2, $K_p \cong G(p, p - 1)$, and $G(p, p - 1)$ is symmetric. So by Lemma 5.2.1, $\Gamma \cong G(q, r) \times G(p, p - 1)$. Therefore, by Lemma 5.2.2, if $G(q, r) \rightarrow G(p, p - 1)$ (that is, if $\chi(G(q, r)) \leq p$), then $\Gamma \ast \cong G(q, r)$; if $G(p, p - 1) \rightarrow G(q, r)$ (that is, if $\omega(G(q, r)) \geq p$), then $\Gamma \ast \cong G(p, p - 1) \cong K_p$; if both $G(q, r) \not\rightarrow G(p, p - 1)$ and $G(p, p - 1) \not\rightarrow G(q, r)$ (that is, if $\chi(G(q, r)) > p > \omega(G(q, r))$, then $\Gamma$ is a core. Therefore, at least one of the cases (i)-(iii) occurs.

Finally, for any integer $n < q$, if $\omega(G(q, r)) = \chi(G(q, r)) = n$, then $(G(q, r))^* \cong K_n$, which is a contradiction since $G(q, r)$ is a core by Corollary 2.3.20. Therefore, by Proposition 2.3.5, $\omega(G(q, r)) < \chi(G(q, r))$ (unless $\omega(G(q, r)) = q$), so exactly one of the cases (i)-(iii) occurs. \qed
5.3 $G(pq; r, s, u)$

5.3.1 Categorical products

The final circulant whose core we must find is $G(pq; r, s, u)$ for $p \geq 3$. We begin this case by looking at the graph $G(3q, r)$. The definition of $G(3q, r)$ is similar to that of the graphs $G(pq; r, s, u)$, and on closer inspection we see that $G(3q, r) \cong G(3q; r, 2, u)$ (see Definitions 4.2.5 and 4.2.6).

Lemma 5.3.1 $G(3q, r) \cong G(3q; r, 2, u)$, where $u = r$ if $r$ is even, and $u = 2r$ if $r$ is odd.

Proof From Definition 4.2.6, if $s = 2$, then
\[ t = t^2 \in -H(q, r), \quad t^2 \in H(q, r) \quad \text{and} \quad \langle t^2 \rangle \leq H(q, r). \] (5.3.1)

In addition, $\mathbb{Z}_q^*$ is cyclic, so it has a unique subgroup of order 2 (namely $\langle -1 \rangle$, with $-1 \in \mathbb{Z}_q^*$). Thus a subgroup of $\mathbb{Z}_q^*$ has even order if and only if it contains $\langle -1 \rangle$. Hence if $r$ is even, then
\[-1 \in H(q, r) \leq \mathbb{Z}_q^*, \quad H(q, r) = -H(q, r) \quad \text{and} \quad \langle t \rangle \leq H(q, r),\]

such that
\[ u = \text{lcm}(o(t), r) = r. \]

Whilst if $r$ is odd, then
\[-1 \notin H(q, r) \leq \mathbb{Z}_q^* \quad \text{and} \quad H(q, r) \neq -H(q, r). \]

So for some integer $m$, if $m$ is even then $t^m \in H(q, r)$, and if $m$ is odd then $t^m \in -H(q, r)$. Thus $t$ has even order and
\[ u = \text{lcm}(o(t), r) = 2r. \]

So we define a map $\eta : V(G(3q, r)) \to V(G(3q; r, 2, u))$ with
\[ \eta : (i, x) \mapsto (i, x), \]
where $i \in \mathbb{Z}_3$ and $x \in \mathbb{Z}_q$. Clearly both $\eta$ and $\eta^{-1}$ are bijections. Therefore, we show that $\eta$ and $\eta^{-1}$ are graph homomorphisms, thus proving that $\eta$ is an isomorphism.

From Definition 4.2.5 and Equation 5.3.1, if $[(i, x), (j, y)] \in E(G(3q, r))$ then

$$j - i \equiv 1 \mod 3 \equiv (-1)^2 \mod 3$$

and

$$y - x \in H(q, r) = t^2 H(q, r)$$

for any $t \in -H(q, r)$. Now $\langle -1 \rangle = H(3, 2)$ (with $-1 \in \mathbb{Z}_p^*$), so from Definition 4.2.6, if $[(i, x), (j, y)] \in E(G(3q, r))$ then $[(i, x), (j, y)] \in E(G(3q; r, 2, u))$. Hence, for $[(i, x), (j, y)] \in E(G(3q, r))$,

$$\eta([(i, x), (j, y)]) = [(i, x), (j, y)] \in E(G(3q; r, 2, u)),$$

so that $\eta$ is a homomorphism.

Now from Definition 4.2.6, if $[(i, x), (j, y)] \in E(G(3q; r, 2, u))$, then $j - i = (-1)^l$ and $y - x \in t^l H(q, r)$ for some integer $l$ and a fixed $t \in -H(q, r)$. When $l$ is even, $t^l \in H(q, r)$, so that $j - i = 1$, $y - x \in H(q, r)$ and $[(i, x), (j, y)] \in E(G(3q, r))$. Therefore,

$$\eta^{-1}([(i, x), (j, y)]) = [(i, x), (j, y)] \in E(G(3q, r)).$$

When $l$ is odd, $t^l \in -H(q, r)$, so that $i - j \equiv 1 \mod 3$ ($j - i \equiv -1 \mod 3$), $x - y \in H(q, r)$ ($y - x \in -H(q, r)$) and $[(j, y), (i, x)] \in E(G(3q, r))$. Therefore,

$$\eta^{-1}([(i, x), (j, y)]) = [(i, x), (j, y)] = [(j, y), (i, x)] \in E(G(3q, r)),$$

since edges are unordered. Hence, $\eta^{-1}$ is a homomorphism, and $\eta$ is an isomorphism.

Consequently, the techniques we use to determine the core of $G(pq; r, s, u)$ also apply to $G(3q, r)$, so we group these graphs together.

From Definition 4.2.6, for any fixed $t \in \mathbb{Z}_q^*$ such that $\text{lcm}\{o(t), r\} = u$ and $t^5 \in -H(q, r)$, the vertices $(i, x), (j, y) \in V(G(pq; r, s, u))$ are adjacent if and only if there exists an integer $l$ such that $j - i = a^l$ and $y - x \in t^l H(q, r)$. At first
glance, there are similarities between this definition for $G(pq; r, s, u)$ and that of the categorical product $G(p, s) \times G(q, u)$ in Definition 2.2.5. Further inspection shows that a relationship between $G(pq; r, s, u)$ and $G(p, s) \times G(q, u)$ exists.

**Lemma 5.3.2** Let $\Gamma = G(pq; r, s, u)$. Then $\Gamma$ is isomorphic to a spanning subgraph of the symmetric graph $\Psi = G(p, s) \times G(q, u)$. Further, $\Gamma \cong \Psi$ if and only if $t \in H(q, r).

**Proof** Let $\Gamma = G(pq; r, s, u)$, $c \in \mathbb{Z}_q^*$ with $H(q, r) = \langle c \rangle$, and $\Psi = G(p, s) \times G(q, u)$. To show that $\Psi$ is symmetric, we show that $u$ is even. From Definition 4.2.6, $t^2 \in -H(q, r)$, so that $t^2 = -w$ for some $w \in H(q, r)$. By Definition 4.2.1, $H(q, r) \leq \mathbb{Z}_q^*$ is a group, so that $w^{-1} \in H(q, r)$. Hence the group $\langle t, c \rangle \leq \mathbb{Z}_q^*$ contains the element

$$t^2w^{-1} = -ww^{-1} = -1.$$ 

Now $-1$ has order 2 in $\mathbb{Z}_q^*$, so $\langle t, c \rangle$ must have even order. Therefore,

$$|\langle t, c \rangle| = \text{lcm}(o(t), r) = u$$

(5.3.2)

is even.

Thus by Theorem 4.2.2, $G(p, s)$ and $G(q, u)$ are symmetric, and by Proposition 2.2.6, $\Psi$ is symmetric.

By Definitions 2.2.5 and 4.2.6, $V(\Psi) = V(\Gamma)$. So to show that $\Gamma$ is a spanning subgraph of $\Psi$, we show that $E(\Gamma) \subseteq E(\Psi)$.

If $[(i, x), (j, y)] \in E(\Gamma)$, then by Definition 4.2.6,

$$j - i = a^l \text{ and } y - x \in t^lH(q, r)$$

for some integer $l$. Further, $H(q, u)$ is the unique subgroup of $\mathbb{Z}_q^*$ of order $u$, so by Equation 5.3.2, $\langle t, c \rangle = H(q, u)$. Thus $t^lH(q, r) \subseteq H(q, u)$, so that

$$j - i \in H(p, s) \text{ and } y - x \in H(q, u).$$

Therefore, $[i, j] \in E(G(p, s))$ and $[x, y] \in E(G(q, u))$, so by Definition 2.2.5, $[(i, x), (j, y)] \in E(\Psi)$. Hence $E(\Gamma) \subseteq E(\Psi)$, and $\Gamma$ is a spanning subgraph of $\Psi$. 
In order to complete the proof, we need to show that $E(\Gamma) \supseteq E(\Psi)$ if and only if $t \in H(q, r)$. So let $[(i, x), (j, y)] \in E(\Psi)$, such that by Definition 2.2.5,

$$j - i \in H(p, s) \text{ and } y - x \in H(q, u).$$

If $t \in H(q, r)$, then $H(q, u) = \langle t, c \rangle = H(q, r)$, such that

$$j - i = a^l \text{ and } y - x \in t^l H(q, r)$$

for some integer $l$. Then from Definition 4.2.6, $[(i, x), (j, y)] \in E(\Gamma)$. So if $t \in H(q, r)$, then $E(\Gamma) \supseteq E(\Psi)$.

Conversely, if $E(\Gamma) \supseteq E(\Psi)$, then denote $N_{\Psi}^{a^{(t)}}((i, x)) \subseteq N_{\Psi}(i, x)$, such that

$$N_{\Psi}^{a^{(t)}}((i, x)) := \{(i + a^{(t)}, \hat{y}) \mid \hat{y} - x \in H(q, u)\},$$

where $|N_{\Psi}^{a^{(t)}}((i, x))| = |H(q, u)| = u$. For every $(i + a^{(t)}, \hat{y}) \in N_{\Psi}^{a^{(t)}}((i, x))$, $t^{a^{(t)}} = 1$ so that

$$\hat{y} - x \in t^{a^{(t)}} H(q, r) = H(q, r) \text{ and } u = |N_{\Psi}^{a^{(t)}}((i, x))| \leq r.$$ 

However $u = \text{lcm}(a(t), r)$, so that $u = r, H(q, r) = H(q, u) = \langle t, c \rangle$ and $t \in H(q, r)$. So if $E(\Gamma) \supseteq E(\Psi)$, then $t \in H(q, r)$. Therefore, $E(\Gamma) \supseteq E(\Psi)$ if and only if $t \in H(q, r)$.

Lemma 5.3.2 splits the case for $G(pq; r, s, u)$ into two subcases, namely when $t \in H(q, r)$ and $t \notin H(q, r)$. When $t \in H(q, r)$, we combine Lemma 5.2.2 and Lemma 5.3.2 to obtain:

**Theorem 5.3.3** Let $\Gamma \cong G(pq; r, s, u)$ with $t \in H(q, r)$. Then $\Gamma$ is not a core if and only if one of the following conditions hold:

(i) $G(p, s) \rightarrow G(q, u)$, in which case $\Gamma^* \cong G(p, s)$;

(ii) $G(q, u) \rightarrow G(p, s)$, in which case $\Gamma^* \cong G(q, u)$.
5.3.2 Candidates for core when \( t \notin H(q, r) \)

Let \( \Gamma = G(pq; r, s, u) \). Whenever \( t \notin H(q, r) \), Lemmas 2.3.29 and 5.3.2 imply the existence of homomorphisms

\[
\Gamma \to G(p, s) \quad \text{and} \quad \Gamma \to G(q, u).
\]

Hence \( G(p, s) \) and \( G(q, u) \) are candidates for the core of \( \Gamma \). We claim that \( \Gamma, G(p, s) \) and \( G(q, u) \) are the only candidates. To prove this claim, for a retraction \( \phi : \Gamma \to \Gamma^* \), we find \( \gamma \in \text{Aut}(\Gamma) \) for which \( (\phi \circ \gamma) \mid_{\Gamma^*} \) is semiregular on \( V(\Gamma^*) \), and then use the powers of \( \gamma \) to construct the fibres of \( \phi \).

In this section, we set \( H(q, r) = \langle c \rangle \) for \( c \in \mathbb{Z}_q^* \), \( \phi : \Gamma \to \Gamma^* \) to be a retraction with \( \phi \mid_{\Gamma^*} = 1_{\text{Aut}(\Gamma^*)} \), and fix \( l, m \in \mathbb{N} \). From Definition 4.2.6, for \( (i, x) \in V(\Gamma) \), the maps

\[
\pi : (i, x) \mapsto (i, x + 1) \quad \text{and} \quad \rho : (i, x) \mapsto (i + 1, x)
\]

are both semiregular automorphisms of \( \Gamma \). Therefore,

\[
\gamma := \rho^l \circ \pi^m \in \text{Aut}(\Gamma).
\]

We show that \( \gamma \) maps each element of \( V(\Gamma^*) \) to a new fibre.

**Lemma 5.3.4** Let \( \Gamma = G(pq; r, s, u) \) and \( \phi : \Gamma \to \Gamma^* \). Then \( \gamma((i, x)) = (i + a^l, x + t^l c^m) \) for all \( (i, x) \in V(\Gamma) \), and \( (\phi \circ \gamma) \mid_{\Gamma^*} \) is semiregular in its action on \( V(\Gamma^*) \) for any copy of \( \Gamma^* \) in \( \Gamma \).

**Proof** Let \( \Gamma = G(pq; r, s, u) \) and \( \phi : \Gamma \to \Gamma^* \) be a retraction from \( \Gamma \) to \( \Gamma^* \). For \( (i, x) \in V(\Gamma) \),

\[
\gamma((i, x)) = (i + a^l, x + t^l c^m).
\]

So \( \gamma \) is semiregular on \( V(\Gamma) \).

From Definition 4.2.6, \( (i, x) \) and \( (i + a^l, x + t^l c^m) \) are adjacent for all \( i \in \mathbb{Z}_p \) and \( x \in \mathbb{Z}_q \). And by Proposition 2.3.7 each fibre of \( \phi \) must be an independent set. Thus for all \( i \in \mathbb{Z}_p \) and \( x \in \mathbb{Z}_q \), \( (i, x) \) and \( (i + a^l, x + t^l c^m) \) are not in the same fibre of \( \phi \). Hence for any vertex in \( \Gamma \), \( \gamma \) must map that vertex from one fibre of \( \phi \) to a different fibre of \( \phi \). Thus for any copy of \( \Gamma^* \) in \( \Gamma \), \( (\phi \circ \gamma) \mid_{\Gamma^*} \in \text{Aut}(\Gamma^*) \) does not fix any element of \( V(\Gamma^*) \). So \( (\phi \circ \gamma) \mid_{\Gamma^*} \) is semiregular. \( \square \)
By Lemma 5.3.4, $\gamma \in \text{Aut}(\Gamma)$ maps any element of $V(\Gamma^*)$ from one fibre of $\phi$ to a different fibre of $\phi$. However, Lemma 5.3.4 does not show which fibre contains $\gamma((i, x))$ for each $(i, x) \in V(\Gamma^*)$. To overcome this problem, we show that $(\phi \circ \gamma) |_{r^*}$ is an element of a regular, cyclic subgroup of $\text{Aut}(\Gamma^*)$.

**Lemma 5.3.5** Let $\Gamma = G(pq; r, s, u)$, $\phi : \Gamma \to \Gamma^*$, $n = |V(\Gamma^*)|$ and $G \leq \text{Aut}(\Gamma^*)$ be regular with $G \cong \mathbb{Z}_n$. If $\Gamma \not\cong \Gamma^*$ and $\Gamma^*$ is not complete, then $(\phi \circ \gamma) |_{r^*} \in G$.

**Proof** From Theorems 2.3.21, 2.3.22 and 4.2.2, if $\Gamma \not\cong \Gamma^*$ then $\Gamma^* \cong G(n, \overline{s})$, where $n$ is either $p$ or $q$, $\overline{s}$ is a divisor of $n - 1$,

$$\text{Aut}(\Gamma^*) = \{x \mapsto m'x + b \mid x, b \in \mathbb{Z}_n, m' \in H(n, \overline{s})\} \cong \mathbb{Z}_n \times H(n, \overline{s})$$

and

$$G = \{x \mapsto x + b \mid x, b \in \mathbb{Z}_n\} \cong \mathbb{Z}_n.$$

So for $\eta = m'x + b \in \text{Aut}(\Gamma^*)$, if $m' \neq 1$ then $1 - m' \in \mathbb{Z}_n^* = \text{Aut}(\mathbb{Z}_n)$. Then for each $b \in \mathbb{Z}_n$, $b = u(1 - m')$ for some $u \in \mathbb{Z}_n$, and

$$\eta(u) = m'u + u(1 - m') = m'u + u - um' = u$$

such that $\eta \in \text{Aut}(\Gamma^*)_u$. Hence whenever $m' \neq 1$, $\eta \in \text{Aut}(\Gamma^*)$ must fix some vertex of $\Gamma^*$. Therefore the only semiregular elements of $\text{Aut}(\Gamma^*)$ are those elements for which $m' = 1$, which are the elements in $G$. So by Lemma 5.3.4, $(\phi \circ \gamma) |_{r^*} \in G$. □

By Definition 4.2.1 and Theorem 4.2.2, if $n = |V(\Gamma^*)|$ is prime, then $\Gamma^* \cong G(n, \overline{s}) = \text{Cay}(\mathbb{Z}_n, H(n, \overline{s}))$ for some $H(n, \overline{s}) \subseteq \mathbb{Z}_n^*$. So for a retraction $\phi : \Gamma \to \Gamma^*$ and an isomorphism $\eta : \Gamma^* \to \text{Cay}(\mathbb{Z}_n, H(n, \overline{s}))$,

$$\phi_k^n := \{(j, z) \mid (j, z) \in V(\Gamma) \text{ and } (\eta \circ \phi)((j, z)) = k\}$$

for each $k \in \mathbb{Z}_n$. Thus each $\phi_k^n$ is the fibre of $\phi$ which maps to each $k \in \mathbb{Z}_n$ under $\eta$.

Since $\Gamma$ and $\Gamma^*$ are symmetric, every arc of $\Gamma$ is contained within some copy of $\Gamma^*$. So without loss of generality, we assume that for fixed $(i, x), (i + a', x + t^lc^m) \in V(\Gamma)$, $(i, x), (i + a', x + t^lc^m) \in V(\Gamma^*)$. Thus we choose $\phi$ and $\eta$ such that for a fixed $b \in \mathbb{Z}_n$, $(i, x) \in \phi_0^n$ and $(i + a', x + t^lc^m) \in \phi_0^n$. Our choice of $\phi$ and $\eta$ ensures that $\gamma$ maps
Lemma 5.3.6 Let \( \Gamma = G(pq; r, s, u) \), \( \phi : \Gamma \to \Gamma^* \), \( n = |V(\Gamma^*)| \) and \( G \leq \text{Aut}(\Gamma^*) \) be regular with \( G \cong \mathbb{Z}_n \). If \( \Gamma \not\cong \Gamma^* \) and \( \Gamma^* \) is not complete, then for all \( k \in \mathbb{Z}_n \) and \( \hat{n} \in \mathbb{N} \), \( (\phi \circ \gamma^k) |_{\Gamma^*} \in \text{Aut}(\Gamma^*) \) maps the vertex of \( \Gamma^* \) in \( \phi_k^\eta \) to \( \phi_{k+\hat{n}b}^\eta \).

Proof We prove that \( (\phi \circ \gamma^k) |_{\Gamma^*} \in \text{Aut}(\Gamma^*) \) maps the vertex of \( \Gamma^* \) in \( \phi_k^\eta \) to \( \phi_{k+\hat{n}b}^\eta \) for any \( k \in \mathbb{Z}_n \), \( \hat{n} \in \mathbb{N} \) and \( \phi \) by induction on \( \hat{n} \). For the base case, let \( \hat{n} = 1 \). Then \( (\phi \circ \gamma) |_{\Gamma^*} \) maps the vertex \((i, x) \in V(\Gamma^*)\) from \( \phi_k^\eta \) to \( \phi_{k+1}^\eta \). By Lemma 5.3.5, \( (\phi \circ \gamma) |_{\Gamma^*} \in G \cong \mathbb{Z}_n \), so \( (\phi \circ \gamma) |_{\Gamma^*} \) maps the vertex of \( \Gamma^* \) in \( \phi_k^\eta \) to \( \phi_{k+1}^\eta \) for all \( k \in \mathbb{Z}_n \).

Therefore, for each \((j, z) \in V(\Gamma^*)\), if \((j, z) \in \phi_k^\eta \) then \( \gamma((j, z)) = (j + a', z + t'^m) \in \phi_{k+1}^\eta \).

Assume that, for any retraction \( \phi : \Gamma \to \Gamma^* \) that fixes every vertex of \( \Gamma^* \), the result is true for some \( \hat{n} > 1 \). In what follows we prove that \( (\phi \circ \gamma^k) |_{\Gamma^*} \in \text{Aut}(\Gamma^*) \) maps the vertex of \( \Gamma^* \) in \( \phi_k^\eta \) to \( \phi_{k+(\hat{n}+1)b}^\eta \) for any \( k \in \mathbb{Z}_n \).

Let \( \Gamma^\# := \gamma^k(\Gamma^*) \). Since \( \gamma^k \in \text{Aut}(\Gamma) \), \( \Gamma^\# \cong \Gamma^* \cong G(n, \bar{s}) \) and \( \Gamma^\# \) is a core of \( \Gamma \). The vertices of \( \Gamma^\# \) are \((j, z)^\# := \gamma^k((j, z)) \) (where \((j, z) \in V(\Gamma^*)\)). By the induction hypothesis, if \((j, z) = V(\Gamma^*) \cap \phi_k^\eta \), then

\[
\phi((j, z)^\#) = (\phi \circ \gamma^k)((j, z)) = V(\Gamma^*) \cap \phi_{k+1}^\eta \cdot \eta((j, z)^\#) \subset \phi_{k+(\hat{n}+1)b}^\eta.
\]

and \((j, z)^\# \in \phi_{k+(\hat{n}+1)b}^\eta \). Moreover, since \( \gamma^k \in \text{Aut}(\Gamma) \) and \( \phi \) is a retraction, \( \gamma^k \circ \phi : \Gamma \to \Gamma^\# \) is a retraction.

By Theorem 4.2.2 there exists \( \tau \in \text{Aut}(G(n, \bar{s})) \) with \( \tau(k) := k - \hat{n}b \) for each \( k \in \mathbb{Z}_p \). So define \( \zeta : V(\Gamma^\#) \to V(G(n, \bar{s})) \) by \( \zeta((j, z)^\#) := (\eta \circ \phi)((j, z)^\#) \). We have:

\[
[(j_1, z_1)^\#, (j_2, z_2)^\#] \in E(\Gamma^\#) \iff [(j_1, z_1), (j_2, z_2)] \in E(\Gamma^*) \iff \\
\eta((j_1, z_1)) - \eta((j_1, z_1)^\#) = (\eta \circ \phi)((j_1, z_1)^\#) - (\eta \circ \phi)((j_1, z_1)^\#) \in H(n, \bar{s}).
\]

Thus by Definition 4.2.1, \( \zeta \) is an isomorphism. Further \( \zeta^{-1} \circ \tau \circ \zeta \in \text{Aut}(\Gamma^\#) \), where \( \zeta^{-1} \circ \tau \circ \zeta((j, z)^\#) \in \phi_k^\eta \) whenever \((j, z)^\# \in \phi_{k+(\hat{n}+1)b}^\eta \).
Now let
\[ \psi := \zeta^{-1} \circ \tau \circ \zeta \circ \gamma \circ \phi : \Gamma \to \Gamma^\# . \]

Then \( \psi : \Gamma \to \Gamma^\# \) is a retraction, and the set of fibres of \( \psi \) is the same as that of \( \gamma \circ \phi \). However, the fibres of \( \gamma \circ \phi \) are the subsets
\[
\{(j, z) \in V(\Gamma) \mid (\gamma \circ \phi)((j, z)) = (h, w)^\#\} = \{(j, z) \in V(\Gamma) \mid (\eta \circ \phi)(\eta \circ \gamma \circ \phi)((j, z)) = k\} = \phi_k^\#,
\]
where \( k \in \mathbb{Z}_n \) and \((h, w)^\# \in \phi_k^\# \). Therefore, the set of fibres of \( \psi \) is identical to the set of fibres \( \phi_k^\# \) of \( \phi \). Moreover, by the induction hypothesis, for \((j, z) = V(\Gamma^\ast) \cap \phi_k^\# \), \((j, z)^\# \in \phi_k^\# + \hat{n} \) and
\[
(\gamma \circ \phi \circ \gamma)((j, z)) = (\gamma \circ \phi)((j, z)^\#) \in \phi_k^\# + \hat{n} \),
\]
such that
\[
\psi((j, z)^\#) = (\zeta^{-1} \circ \tau \circ \zeta \circ \gamma \circ \phi)((j, z)) = (j, z)^\# .
\]

Thus, \( \psi \) fixes every vertex of \( \Gamma^\# \).

Since \((j, z)^\# \in \phi_k^\# + \hat{n} \) whenever \((j, z) \in \phi_k^\# \) as shown above, and the set of fibres of \( \psi \) is \( \{\phi_k^\# \mid k \in \mathbb{Z}_n\} \), it follows that the unique fibre of \( \psi \) containing \((j, z)^\# \), denoted by \( \psi_k^\# \), is given by \( \psi_k^\# = \phi_k^\# + \hat{n} \). In particular,
\[
(i, x)^\# = \gamma \circ \phi \circ \gamma((i, x)) = (i + \hat{n}a^l \cdot x + \hat{n}t\cdot c^m) \in \phi_k^\# + \hat{n} = \psi_k^\#
\]
and
\[
(i + a^l \cdot x + t\cdot c^m)^\# = \gamma \circ \phi \circ \gamma((i + a^l \cdot x + t\cdot c^m)) = (i + (\hat{n}+1)a^l \cdot x + (\hat{n}+1)t\cdot c^m) \in \phi_{(\hat{n}+1)\cdot b} = \psi_b^\#
\]
such that \( \gamma((i, x)^\#) = (i + a^l \cdot x + t\cdot c^m)^\# \). Since \( \psi \) fixes every vertex of \( \Gamma^\# \), we then have
\[
(\psi \circ \gamma)|_{\Gamma^\#}((i, x)^\#) = \psi((i + a^l \cdot x + t\cdot c^m)^\#) = (i + a^l \cdot x + t\cdot c^m)^\# .
\]

Thus \( (\psi \circ \gamma)|_{\Gamma^\#} \) maps \((i, x)^\# \in \psi_0^\# \) to \((i + a^l \cdot x + t\cdot c^m)^\# \in \psi_b^\# \). Now by Lemma 5.3.5, \( (\psi \circ \gamma)|_{\Gamma^\#} \in G \cong \mathbb{Z}_n \), so this implies that for all \( k \in \mathbb{Z}_n \) and \((j, z)^\# \in V(\Gamma^\#) \cap \psi_k^\# \),
\((\psi \circ \gamma) \mid_{\Gamma^*} ((j, z)^\#) \in \psi^\Gamma_{k+b}\). Therefore, \(\gamma((j, z)^\#) \in \psi^\Gamma_{k+b}\) and

\[\gamma^{\hat{n}+1}(j, z) = \gamma((j, z)^\#) \in \psi^{\Gamma}_{k+b} = \phi_k^n_{(\hat{n}+1)b},\]

such that for any \(k \in \mathbb{Z}_n\), \((\phi \circ \gamma^{\hat{n}+1}) \mid_{\Gamma^*} \in \text{Aut}(\Gamma^*)\) maps the vertex of \(\Gamma^*\) in \(\phi_k^n\) to \(\phi_k^n_{(\hat{n}+1)b}\) as required. \(\square\)

From Lemma 5.3.6, we now find powers of \(\gamma\) which fix each element of \(V(\Gamma^*)\) to their respective fibres of \(\phi\), and thus construct each fibre out of the powers of \(\gamma\).

**Theorem 5.3.7** Let \(\Gamma \cong G(pq; r, s, u)\) with \(t \notin H(q, r)\).

(i) If \(|V(\Gamma^*)| = p\), then \(\Gamma^* \cong G(p, s)\) and there exists a retraction \(\phi: \Gamma \rightarrow \Gamma^*\) whose fibres are the sets \(\{(i, x) \mid x \in \mathbb{Z}_q\}\) for \(i \in \mathbb{Z}_p\).

(ii) If \(|V(\Gamma^*)| = q\), then \(\Gamma^* \cong G(q, u)\) and there exists a retraction \(\phi: \Gamma \rightarrow \Gamma^*\) whose fibres are the sets \(\{(i, x) \mid i \in \mathbb{Z}_p\}\) for \(x \in \mathbb{Z}_q\).

**Proof** Let \(\Gamma^*\) be complete, so that \(\Gamma^* \cong G(n, n - 1)\) where \(n = p \text{ or } q\). Then \(\Gamma\) contains a subgraph isomorphic to \(G(n, n - 1)\). By Lemma 5.3.2, \(\Gamma\) is a spanning subgraph of \(\Psi = G(p, s) \times G(q, u)\), so that \(\Psi\) contains a subgraph isomorphic to \(G(n, n - 1)\), and thus \(G(n, n - 1) \rightarrow \Psi\). On the other hand, by Lemma 2.3.29, \(\Psi \rightarrow G(p, s)\) and \(\Psi \rightarrow G(q, u)\), where \(G(p, s) \rightarrow G(p, p - 1)\) and \(G(q, u) \rightarrow G(q, q - 1)\) by inclusion. Thus, \(\Psi \rightarrow G(n, n - 1)\), so that \(\Psi \leftrightarrow G(n, n - 1)\), and \(\Psi^* \cong G(n, n - 1)\). However, by Theorems 2.3.30 and 2.3.31, either \(\Psi^* \cong G(p, s)\) or \(\Psi^* \cong G(q, u)\). So if \(n = p\), then \(s = p - 1\); if \(n = q\), then \(u = q - 1\).

Now \(\Gamma\) is a spanning subgraph of \(\Psi\), so we have the inclusion homomorphism \(\delta: \Gamma \rightarrow \Psi\). So by Lemma 2.3.29, there exist homomorphisms

\[\pi \circ \delta: \Gamma \rightarrow G(p, s)\) and \(\rho \circ \delta: \Gamma \rightarrow G(q, u),\]

where the fibres of \(\pi \circ \delta\) are the sets \(\{(j, y) \mid y \in \mathbb{Z}_q\}\) for each \(j \in \mathbb{Z}_p\), and fibres of \(\rho \circ \delta\) are the sets \(\{(j, y) \mid j \in \mathbb{Z}_p\}\) for each \(y \in \mathbb{Z}_q\). So if \(n = p\), then \(\pi \circ \delta: \Gamma \rightarrow G(p, p - 1)\) is a retraction; if \(n = q\), then \(\rho \circ \delta: \Gamma \rightarrow G(q, q - 1)\) is a retraction.

Let \(|V(\Gamma^*)| = p\), with \(\Gamma^* \not\cong K_p\). By Lemma 5.3.6 for any \(\hat{n} \in \mathbb{N}\), \((\phi \circ \gamma^{\hat{n}p}) \mid_{\Gamma^*}\) maps each vertex of \(\Gamma^*\) in \(\phi_k^n\) to \(\phi_k^n_{\hat{n}p}\), for all \(k \in \mathbb{Z}_p\). But \(k + \hat{n}pb \equiv k \mod p\).
and as such \((\phi \circ \gamma^{np})|_{\Gamma^*}\) maps the vertex of \(\Gamma^*\) in \(φ_k^n\) to \(φ_k^n\), for all \(k \in \mathbb{Z}_p\). So if 

\((j, z) \in V(\Gamma^*)\) is in \(φ_k^n\), then

\[
\gamma^{np}(j, z) = (j + \hat{n}pa^l, z + \hat{n}pt^lc^m) = (j, z + \hat{n}pt^lc^m) \in φ_k^n
\]

for all \(\hat{n} \in \mathbb{N}\) and \(k \in \mathbb{Z}_p\). But by Definition 4.2.6, \(p\) and \(q\) are primes with \(p \neq q\), and \(t, c \in \mathbb{Z}_q^*\). Therefore, \(pt^lc^m \in \mathbb{Z}_q\) with \(pt^lc^m \neq 0 \mod q\), such that \(\langle pt^lc^m \rangle = \mathbb{Z}_q\). Thus for all \(k \in \mathbb{Z}_p\), if \((j, z) \in φ_k^n\), then \(\{(j, y) \mid y \in \mathbb{Z}_q\} \subseteq φ_k^n\). So by Theorem 2.3.22, each fibre of \(φ\) has order \(q\), such that for all \(k \in \mathbb{Z}_p\), if \((j, z) \in φ_k^n\), then \(φ^n_k = \{(j, y) \mid y \in \mathbb{Z}_q\}\). Hence each of the \(p\) fibres of \(φ\) are one of the \(p\) sets \(\{(j, y) \mid y \in \mathbb{Z}_q\}\) for all \(j \in \mathbb{Z}_p\).

By Lemma 5.3.2, \(Γ\) is a spanning subgraph of \(Ψ\), and moreover \(Γ \neq Ψ\) since \(t \notin H(q, r)\). Hence \(Γ^*\) is a subgraph of \(Ψ\), and we have the inclusion homomorphism \(δ : Γ^* \rightarrow Ψ\). By Lemma 2.3.29, \(Ψ\) has the surjective projection homomorphism \(π : Ψ \rightarrow G(p, s), (j, y) \mapsto y\). Further, since \(|V(\Gamma^*)| = p = |V(G(p, s))|\), \(π \circ δ\) is bijective. Hence \((π \circ δ)(Γ^*) \cong Γ^*\) and \((π \circ δ)(\Gamma^*)\) is a spanning subgraph of \(G(p, s)\).

We claim that \((π \circ δ)(\Gamma^*) = G(p, s)\). Let \(j_1, j_2 \in \mathbb{Z}_p\) be any two adjacent vertices of \(G(p, s)\), so that \(j_2 - j_1 = a^{l_0} \in H(p, s)\) for some integer \(l_0\). Then \(j_1\) and \(j_2\) each determine uniquely a vertex of \(Γ^*\), say, \((j_1, y_1)\) and \((j_2, y_2)\), respectively, with \((j_1, y_1) \in φ_{k_1}^n\) and \((j_2, y_2) \in φ_{k_2}^n\) for some \(k_1, k_2 \in \mathbb{Z}_p\). By Definition 4.2.6, each vertex \((j_1, z) \in φ_{k_1}^n\) is adjacent in \(Γ\) to \((j_2, z + t^lc) \in φ_{k_2}^n\), since \(j_2 - j_1 = a^{l_0} \in H(p, s)\). Thus \(φ((j_1, z)) = (j_1, y_1)\) and \(φ((j_2, z + t^lc)) = (j_2, y_2)\) are adjacent in \(Γ^*\), since \(φ\) is a homomorphism. In other words, if two vertices of \(G(p, s)\) are adjacent, then the corresponding vertices of \(Γ^*\) are adjacent in \(Γ^*\); hence \(|E(Γ^*)| \geq |E(G(p, s))|\). On the other hand, \(|E(Γ^*)| = |E((π \circ δ)(Γ^*))| \leq |E(G(p, s))|\) as \((π \circ δ)(Γ^*)\) is a spanning subgraph of \(G(p, s)\). Therefore, \(|E(Γ^*)| = |E((π \circ δ)(Γ^*))| = |E(G(p, s))|\) and so \((π \circ δ)(Γ^*) = G(p, s)\). Consequently, \(Γ^* \cong G(p, s)\), and the fibres of \(φ\) are the sets \(\{(i, x) : x \in \mathbb{Z}_q\}, i \in \mathbb{Z}_p\).

Now let \(|V(Γ^*)| = q\) with \(Γ^* \not\cong K_q\). The proof for this case is the same as above, so we omit it. □
5.3.3 Core when \( t \notin H(q, r) \)

Theorem 5.3.7 shows that when \( t \notin H(q, r) \) and \( G(pq; r, s, u) \) is not a core, the core of \( G(pq; r, s, u) \) must be isomorphic to either \( G(p, s) \) or \( G(q, u) \). Therefore we must determine the conditions under which \( G(pq; r, s, u) \) contains one of \( G(p, s) \) or \( G(q, u) \) as an induced subgraph.

**Lemma 5.3.8** Let \( \Gamma \cong G(pq; r, s, u) \) with \( t \notin H(q, r) \).

(i) \( \Gamma \) has an induced subgraph isomorphic to \( G(p, s) \) if and only if there exists a homomorphism \( \eta : G(p, s) \to G(q, u) \), such that for each \((i, j) \in A(G(p, s))\) with \( j - i = a^l \) for some integer \( l \), we have \( \eta(j) - \eta(i) \in t^l H(q, r) \).

(ii) \( \Gamma \) has an induced subgraph isomorphic to \( G(q, u) \) if and only if there exists a homomorphism \( \zeta : G(q, u) \to G(p, s) \), such that for each \((x, y) \in A(G(q, u))\) with \( y - x \in t^l H(q, r) \) for some integer \( l \), we have \( \zeta(y) - \zeta(x) = a^l \).

**Proof**

(i) If there exists a homomorphism \( \eta : G(p, s) \to G(q, u) \), such that each arc \((i, j) \in A(G(p, s))\) with \( j - i = a^l \) maps to an arc \((x, y) \in A(G(q, u))\) with \( \eta(j) - \eta(i) \in t^l H(q, r) \), we define \( \Delta \) to be the induced subgraph of \( \Gamma \) with

\[
V(\Delta) = \{(i, \eta(i)) \mid i \in \mathbb{Z}_p\}.
\]

Then by Definition 4.2.6, \( ((i, \eta(i)), (j, \eta(j))) \in A(\Delta) \) if and only if \((i, j) \in A(G(p, s))\), and as such \( \Delta \cong G(p, s) \).

By Lemma 5.3.2 \( \Gamma \) is a spanning subgraph of \( \Psi = G(p, s) \times G(q, u) \), so we have the inclusion homomorphism \( \delta : \Gamma \to \Psi \). And by Lemma 2.3.29, we have the projection \( \pi : \Psi \to G(p, s), (i, x) \mapsto i \). So if \( \Gamma \) contains an induced subgraph \( \Delta \cong G(p, s) \), then \( \Gamma \leftrightarrow G(p, s) \), so that \( \Delta \cong \Gamma^* \cong G(p, s) \). Then by Theorem 5.3.7 there is a retraction \( \phi : \Gamma \to \Gamma^* \) whose fibres are the sets \( \{(i, x) : x \in \mathbb{Z}_q\}, i \in \mathbb{Z}_p \). Thus \( \pi \circ \delta : \Gamma \to G(p, s), (i, x) \mapsto i \) is a homomorphism whose set of fibres is identical to the set of fibres of \( \phi \). Since \( \Delta \) is a copy of \( \Gamma^* \) in \( \Gamma \), \( \Delta \cong \phi(\Gamma) \), so \( \Delta \) has exactly one vertex in each fibre of \( \phi \). Thus each fibre of \( \pi \circ \delta \) contains exactly one vertex of \( \Delta \).
In other words, for each \( i \in \mathbb{Z}_p \), \( \Delta \) contains exactly one vertex of the form \((i, x)\). Thus
\[
\theta := (\pi \circ \delta) \mid_\Delta : V(\Delta) \to V(G(p, s)), (i, x) \mapsto i,
\]
is a bijection. Since \( \pi \circ \delta \) is a homomorphism, \( \theta : \Delta \to G(p, s) \) is a homomorphism. And since \( |E(\Delta)| = |E(G(p, s))| \) (as \( \Delta \cong G(p, s) \)), \( \theta \) is an isomorphism.

By Lemma 2.3.29, there exists a projection \( \rho : \Psi \to G(q, u), (i, x) \mapsto x \). Thus the projections \( \rho \circ \delta : \Gamma \to G(q, u), (i, x) \mapsto x \) and
\[
\psi := (\rho \circ \delta) \mid_\Delta : \Delta \to G(q, u), (i, x) \mapsto x
\]
are homomorphisms. Consequently,
\[
\eta := \psi \circ \theta^{-1} : G(p, s) \to G(q, u)
\]
is a homomorphism, and it maps each \( i \in \mathbb{Z}_p \) to the unique \( x(i) \in \mathbb{Z}_q \) such that \((i, x(i))\) is the unique vertex of \( \Delta \) contained in the fibre \( \{ (i, x) : x \in \mathbb{Z}_q \} \) of \( \phi \). If \((i, j) \in A(G(p, s))\), then \( j = i + al \) for some integer \( l \), and \((\theta^{-1}(i), \theta^{-1}(j)) \in A(\Delta) \subset A(\Gamma) \) (as \( \theta^{-1} \) is an isomorphism from \( G(p, s) \) to \( \Gamma^* \)). Since \( \theta^{-1}(i) = (i, x(i)) \), by Definition 4.2.6, \( \theta^{-1}(j) = (i + al, x(i) + tlcm) \) for some integer \( m \). Therefore,
\[
\eta(j) - \eta(i) = (x(i) + tlcm) - x(i) = tlcm \in tlH(q, r)
\]
as required.

(ii) The proof of (ii) is similar to the proof of (i), so we omit it. \( \square \)

To finish the case for \( G(pq; r, s, u) \) with \( t \notin H(q, r) \), we combine Theorem 5.3.7 and Lemma 5.3.8.

**Theorem 5.3.9** Let \( \Gamma \cong G(pq; r, s, u) \) with \( t \notin H(q, r) \). Then \( \Gamma \) is not a core if and only if one of the following conditions hold:

(i) there exists a homomorphism \( \eta : G(p, s) \to G(q, u) \), such that for each \((i, j) \in A(G(p, s))\) with \( j - i = al \) for some integer \( l \), we have \( \eta(j) - \eta(i) \in tlH(q, r) \).

In this case, \( \Gamma^* \cong G(p, s) \);
(ii) there exists a homomorphism \( \zeta : G(q, u) \rightarrow G(p, s) \), such that for each \((x, y) \in A(G(q, u)) \) with \( y - x \in t^lH(q, r) \) for some integer \( l \), we have \( \zeta(y) - \zeta(x) = a^l \).

In this case, \( \Gamma^* \cong G(q, u) \).

**Proof**  By Theorem 5.3.7, if \( G(pq; r, s, u) \) with \( t \notin H(q, r) \) is not a core, then its core is isomorphic to either \( G(p, s) \) or \( G(q, r) \). By Lemmas 2.3.29 and 5.3.2, \( G(pq; r, s, u) \rightarrow G(p, s) \) and \( G(pq; r, s, u) \rightarrow G(q, u) \). So \( G(pq; r, s, u) \) is not a core if and only if \( G(pq; r, s, u) \) contains an induced subgraph isomorphic to \( G(p, s) \) or \( G(q, u) \). Therefore, Lemma 5.3.8 gives the conditions under which \( G(pq; r, s, u) \) has a core isomorphic to \( G(p, s) \) or \( G(q, u) \). \qed
Chapter 6

Marušić-Scapellato graphs

To complete the proof of Theorem 4.1.2, we now determine the cores of the imprimitive symmetric Marušić-Scapellato graphs of order \( pq \). As in Section 5.3, for a Marušić-Scapellato graph \( \Gamma \), we first identify potential candidates for \( \Gamma^* \). We then find the conditions under which \( \Gamma \) contains these candidates as induced subgraphs.

This chapter proceeds as follows. In Section 6.1, we show that for an imprimitive Marušić-Scapellato graph \( \Gamma = \Gamma(2^s, p, S, U) \) of order \( pq \), when \( \Gamma^* \) has order \( q \), \( \Gamma^* \) is complete. In Section 6.2, we prove Theorems 6.2.2 and 6.2.3, which give the lower and upper bounds on \( \omega(\Gamma) \), along with necessary conditions on \( \Gamma \) for which these bounds are met. As a consequence of the lower bound, whenever \( \Gamma^* \) has order \( p \), \( \Gamma^* \) must be complete.

In Section 6.3, we use the bounds on the clique number to find an upper bound on \( \alpha(\Gamma) \) (and consequently a lower bound on \( \chi(\Gamma) \)), along with necessary conditions for the bound to be met. Finally in Section 6.4, we collect all the results from Sections 6.1, 6.2 and 6.3 in Theorem 6.4.1, which gives the cores of all imprimitive, symmetric Marušić-Scapellato graphs of order \( pq \).

6.1 When \(|V(\Gamma^*)| = q\)

Let \( \Gamma = \Gamma(2^s, p, S, U) \) be an imprimitive Marušić-Scapellato graph of order \( pq \). By Theorem 4.4.4, \( q = 2^{2^s} + 1 \) is a Fermat prime, \( p \) is a divisor of \( q - 2 \), \( S = \emptyset \) and the block system \( \Sigma = \{B_x \mid x \in \text{PG}(1, 2^s)\} \) with blocks \( B_x = \{(x, r) \mid r \in \mathbb{Z}_p\} \) gives
a partition of $V(\Gamma)$ into independent sets of size $p$. This partition induces a graph homomorphism into $K_q$, so $K_q$ is our first candidate for the core of $\Gamma$.

Before we show that $K_q$ is the only possibility for $\Gamma^*$ when $|V(\Gamma^*)| = q$, we must first state some useful properties of the number $q$ and the stabiliser $\text{Aut}(\Gamma)_{(\infty, r)}$ of $(\infty, r) \in V(\Gamma)$. As mentioned in Section 4.4, Fermat primes are the primes of the form $q = 2^{2^s} + 1$. More generally, Fermat numbers are any numbers of the form $F_s = 2^{2^s} + 1$, where $s \geq 0$. All Fermat numbers are pairwise coprime [45], and for $s \geq 1$, all Fermat numbers satisfy the recurrence relation

$$F_s = F_0 F_1 \ldots F_{s-1} + 2.$$  

(6.1.1)

Consequently, whenever $p \mid 2^{2^s} - 1$, $p$ must be a prime factor of exactly one of the Fermat numbers $F_l$ for $0 \leq l \leq s - 1$. For more on Fermat numbers, see [45].

Now as in [56, Equations 10,12 and 14], for each $b \in \text{GF}(2^{2^s})$, we define

$$\lambda_b((x, r)) = \begin{cases} (x, r) & x = \infty \\ (x + b, r) & x \in \text{GF}(2^{2^s}) \end{cases},$$  

(6.1.2)

and for our chosen primitive element $w \in \text{GF}(2^{2^s})^*$, we define

$$\rho((x, r)) = \begin{cases} (x, r + 1) & x \in \{\infty, 0\} \\ (xw, r + 1) & x \in \text{GF}(2^{2^s})^* \end{cases}.$$  

(6.1.3)

From Definition 4.4.1, $\lambda_b, \rho \in \text{Aut}(\Gamma)$. Thus $H := \{\lambda_b \mid b \in \text{GF}(2^{2^s})\} \leq \text{Aut}(\Gamma)$ with $H \cong \mathbb{Z}_{2^{2^s}}^*$, and $J := \langle \rho^i \rangle \leq \text{Aut}(\Gamma)$ with $J \cong \mathbb{Z}_{2^{2^s} - 1}$. Clearly $\lambda_b$ fixes $B_\infty$ pointwise for each $b \in \text{GF}(2^{2^s})$, and $\rho^i$ fixes $B_\infty \cup B_0$ pointwise for any integer $i$. Thus $J$ fixes $B_\infty \cup B_0$ pointwise, and $H$ fixes $B_\infty$ pointwise, such that $H \rtimes J \leq \text{Aut}(\Gamma)_{(\infty, r)}$ for every $r \in \mathbb{Z}_p$.

Now we show that when $\Gamma^*$ has order $q$, there is exactly one vertex of $\Gamma^*$ in each block of $\Sigma$.

**Lemma 6.1.1** Let $\Gamma = \Gamma(2^s, p, \emptyset, U)$ be an imprimitive symmetric Marušić-Scapellato graph ($p < q = 2^{2^s} + 1$, $p$ and $q$ are prime) such that $|V(\Gamma^*)| = 2^{2^s} + 1$. Then $V(\Gamma^*)$ contains exactly one vertex from each block of $\Sigma$. 
CHAPTER 6. MARUŠIČ-SCAPELLATO GRAPHS

Proof Assume that there exists a copy of $\Gamma^*$ containing multiple vertices from some block of $\Sigma$. Since $\Gamma$ is vertex-transitive, $\text{Aut}(\Gamma)$ is transitive on $\Sigma$. So without loss of generality, we assume that $(\infty, u, \infty, v) \in V(\Gamma^*) \cap B_\infty$, where $u \neq v$ and $B_\infty \in \Sigma$.

Now $\Gamma$ is symmetric, so by Theorem 4.4.4, $S = \emptyset$ such that $(\infty, u) \text{ and } (\infty, v)$ are nonadjacent. Thus $\Gamma^*$ is not complete, so by Theorems 2.3.21, 2.3.22 and 4.2.2, $\Gamma^* \cong G(q, r)$ for some proper even divisor $r$ of $q - 1$, and $\text{Aut}(\Gamma^*)$ is a Frobenius group in its action on $V(\Gamma^*)$.

From Equations 6.1.2 and 6.1.3,

$$\text{Aut}(\Gamma)_{(\infty, u)} \geq H \rtimes J \cong Z_2^{s} \rtimes Z_{2s-1}^\infty,$$

and $H \rtimes J$ fixes $B_\infty$ pointwise. So for any $\gamma \in H \rtimes J$ and retraction $\phi : \Gamma \to \Gamma^*$, $(\phi \circ \gamma) |_{\Gamma^*}$ fixes both $(\infty, u)$ and $(\infty, v)$. However $\text{Aut}(\Gamma^*)$ is a Frobenius group in its action on $V(\Gamma^*)$, so $(\phi \circ \gamma) |_{\Gamma^*} = 1_{\text{Aut}(\Gamma^*)}$. Hence $\gamma$ must map each element of $V(\Gamma^*)$ to another vertex of $\Gamma$ in the same fibre of $\phi$. Therefore, for any $(x, t) \in V(\Gamma^*)$,

$$H \rtimes J((x, t)) \subseteq \phi^{-1}((x, t)).$$

Now $|B_\infty| = p < q = |V(\Gamma^*)|$, so $V(\Gamma^*) \not\subseteq B_\infty$. Therefore, there exists some $(x, t) \in V(\Gamma^*)$ with $x \neq \infty$, so that by Equation 6.1.2

$$p < 2^{2s} = |H| = |H((x, t))| \leq |H \rtimes J((x, t))| \leq |\phi^{-1}((x, t))|.$$

However, $|V(\Gamma^*)| = q$, so by Theorem 2.3.22, the fibres of $\phi$ have order $p$. So we have a contradiction; consequently $V(\Gamma^*)$ contains at most one vertex from each block. Finally, since $|V(\Gamma^*)| = |\Sigma| = q$, there is exactly one vertex of $V(\Gamma^*)$ contained in each block of $\Sigma$. 

Using Lemma 6.1.1, we prove that if $|V(\Gamma^*)| = q$, then $\Gamma^*$ is complete.

**Theorem 6.1.2** Let $\Gamma = \Gamma(2^s, p, 0, U)$ be an imprimitive symmetric Marušić-Scafellato graph ($p < q = 2^{2s} + 1$, $p, q$ are prime and $pq \neq 15$) such that $|V(\Gamma^*)| = 2^{2s} + 1$. Then $\Gamma^* \cong K_{2^{2s}+1}$.

**Proof** Assume $\Gamma^*$ is a noncomplete graph, that $|V(\Gamma)| = pq \neq 15$, and let $\phi : \Gamma \to \Gamma^*$ be a retraction. By Theorems 2.3.21, 2.3.22 and 4.2.2, $\Gamma^* \cong G(q, r)$ for some
proper even divisor \( r \) of \( q - 1 \), and \( \text{Aut}(\Gamma^*) \) is a Frobenius group in its action on \( V(\Gamma^*) \).

By Definition 4.4.1, \( p \) is a prime divisor of \( 2^{2^s} - 1 \). Moreover, all Fermat numbers are coprime to one another, so by Equation 6.1.1, \( p \mid F_l \) for exactly one \( 0 \leq l \leq s - 1 \). Thus \( p \leq F_{s-1} = 2^{2^{s-1}} + 1 \), so by Equation 6.1.1,

\[
|B_\infty \cup B_0| = 2p \leq 2(2^{2^{s-1}} + 1) = 2F_{s-1} < F_0F_1 \ldots F_{s-1} + 2 = 2^{2^s} + 1.
\]

Since \( |V(\Gamma^*)| = 2^{2^s} + 1 \), there are \( 2^{2^s} + 1 \) fibres of \( \phi \). Hence there must be at least one fibre of \( \phi \) which contains no vertices from \( B_\infty \cup B_0 \). So for some \( x \in \text{GF}(2^{2^s})^* \), \( (x, t) \in V(\Gamma^*) \) where \( t \in \mathbb{Z}_p \) and

\[
\phi^{-1}((x, t)) \cap (B_\infty \cup B_0) = \emptyset.
\]

Since \( \Gamma \) is vertex-transitive, every vertex of \( \Gamma \) is contained in some copy of \( \Gamma^* \). In particular, for every vertex \( (y, z) \in \phi^{-1}((x, t)) \), there is a core \( \Gamma^\# \cong \Gamma^* \) of \( \Gamma \) such that \( (y, z) \in V(\Gamma^\#) \). (Note that \( \Gamma^\# \) depends on \( (y, z) \), though all of them are isomorphic to each other.) We claim that \( \phi \mid_{\Gamma^\#} \) is an isomorphism from \( \Gamma^\# \) to \( \Gamma^* \). Since \( \phi \) is a homomorphism, \( \phi \mid_{\Gamma^\#} : \Gamma^\# \to \Gamma^* \) is a homomorphism. Moreover, \( \phi \mid_{\Gamma^\#} \) is surjective for otherwise the composition of a retraction from \( \Gamma \) to \( \Gamma^\# \) and \( \phi \mid_{\Gamma^\#} \) is a homomorphism from \( \Gamma \) to a proper subgraph of \( \Gamma^* \), contradicting the assumption that \( \Gamma^* \) is a core of \( \Gamma \). Since \( \Gamma^\# \cong \Gamma^* \), there is an isomorphism \( \delta : \Gamma^* \to \Gamma^\# \). Then \( (\delta \circ \phi) \mid_{\Gamma^\#} : \Gamma^\# \to \Gamma^\# \) is an endomorphism, so by Proposition 2.3.12, \( (\delta \circ \phi) \mid_{\Gamma^\#} \in \text{Aut}(\Gamma^\#) \) since \( \Gamma^\# \) is a core. In particular, \( (\delta \circ \phi) \mid_{\Gamma^\#} \) is a bijection from \( V(\Gamma^\#) \) to itself. Therefore, \( \phi \mid_{\Gamma^\#} \) is a bijection from \( V(\Gamma^\#) \) to \( V(\Gamma^*) \) and hence an isomorphism from \( \Gamma^\# \) to \( \Gamma^* \). In particular, each fibre of \( \phi \) contains exactly one vertex of \( \Gamma^\# \).

Define \( \eta : V(\Gamma^*) \to V(\Gamma^\#) \) to be the inverse of the isomorphism \( \phi \mid_{\Gamma^\#} : V(\Gamma^\#) \to V(\Gamma^*) \). Then \( (y, z) = \eta((x, t)) \) and for each \( (j, k) \in V(\Gamma^*) \), \( \eta((j, k)) \in V(\Gamma^\#) \cap \phi^{-1}((j, k)) \) is the unique vertex of \( \Gamma^\# \) contained in the fibre \( \phi^{-1}((j, k)) \). Define \( \psi := \eta \circ \phi : \Gamma \to \Gamma^\# \). Then \( \psi \) is a retraction whose set of fibres is identical to the set of fibres of \( \phi \). More specifically, for \( (j, k) \in V(\Gamma^*) \), the fibre \( \psi^{-1}(\eta(j, k)) \) of \( \psi \) is equal to the fibre \( \phi^{-1}((j, k)) \) of \( \phi \). In particular, \( \psi^{-1}((y, z)) = \phi^{-1}((x, t)) \).

Applying Lemma 6.1.1 to \( \Gamma^\# \), we know that \( \Gamma^\# \) contains exactly one vertex from
each block of $\Sigma$. Clearly, $(y, z)$ is the unique vertex of $\Gamma^#$ in $B_y$. Let $(\infty, c), (0, d)$ be the vertices of $\Gamma^#$ contained in $B_\infty, B_0$, respectively, where $c, d \in \mathbb{Z}_p$. By Equation 6.1.3, $J$ fixes $B_\infty \cup B_0$ pointwise, so for any $\gamma \in J$, $(\psi \circ \gamma) \mid_{\Gamma^#} \in \text{Aut}(\Gamma^#)$ fixes both $(\infty, c)$ and $(0, d)$.

Since $\text{Aut}(\Gamma^#)$ is a Frobenius group on $V(\Gamma^#)$ (as $\Gamma^# \cong \Gamma^* \cong G(q,r)$), it follows that $(\psi \circ \gamma) \mid_{\Gamma^*} = 1_{\text{Aut}(\Gamma^*)}$. Hence for each $\gamma \in J$, $\gamma$ maps each vertex of $V(\Gamma^#)$ to a vertex of $\Gamma$ in the same fibre of $\psi$. Therefore, the $J$-orbit $J((y, z))$ containing $(y, z)$ satisfies

$$J((y, z)) \subseteq \psi^{-1}((y, z)) = \phi^{-1}((x, t)).$$

(6.1.4)

Since Equation 6.1.4 holds for every $(y, z) \in \phi^{-1}((x, t))$, by Theorem 2.1.2, $\phi^{-1}((x, t))$ is a (disjoint) union of $J$-orbits.

Now by Theorem 2.3.22 and our assumption $|V(\Gamma^*)| = q$, $|\phi^{-1}((x, t))| = p$. On the other hand, since $\phi^{-1}((x, t)) \cap (B_\infty \cup B_0) = \emptyset$, for each $(y, z) \in \phi^{-1}((x, t))$ we have $y \neq \infty, 0$. Thus by Theorem 2.1.2, $|J((y, z))|$ divides $|\phi^{-1}((x, t))|$, and by Equation 6.1.3,

$$|J((y, z))| = |J| = \frac{2^{2s} - 1}{p}.$$

Therefore, $\frac{2^{2s} - 1}{p}$ is a divisor of $p$, implying that either $\frac{2^{2s} - 1}{p} = p$ or $\frac{2^{2s} - 1}{p} = 1$.

If $\frac{2^{2s} - 1}{p} = 1$, then by Equation 6.1.1

$$2^{2s} - 1 = F_s - 2 = F_0 F_1 \ldots F_{s-1} = p.$$

But $F_0 = 3$ and $F_1 = 5$, so $F_0 F_1 \ldots F_{s-1}$ is prime only if $s = 1$, such that $p = F_0 = 3$ and $q = F_1 = 5$. Thus $\frac{2^{2s} - 1}{p} = 1$ only if $|V(\Gamma)| = 15$.

However we assume that $|V(\Gamma)| \neq 15$, so $s \geq 2$ and $\frac{2^{2s} - 1}{p} = p$. Then by Equation 6.1.1,

$$2^{2s} - 1 = F_0 F_1 \ldots F_{s-1} = p^2.$$

But $F_0 = 3$ and $F_1 = 5$, so $2^{2s} - 1 = F_0 F_1 \ldots F_{s-1}$ must have prime factors 3 and 5. Hence $2^{2s} - 1 \neq p^2$, and we have a contradiction. Thus if $|V(\Gamma)| = pq \neq 15$, then $\Gamma^* \cong K_{2^{2s}+1}$. \qed
6.2 Bounding the clique number

We now investigate the clique number of $\Gamma$. Generally, determining the exact clique number is difficult, so instead we prove lower and upper bounds. These bounds on the clique number are dependent on the subfield structure of $\text{GF}(2^{2^s})$.

**Lemma 6.2.1** Let $\text{GF}(2^d)$ be a subfield of $\text{GF}(2^{2^s})$, and $w$ be a primitive element of $\text{GF}(2^{2^s})$. Then $\text{GF}(2^d)^* = \langle w^{F_iF_{i+1}...F_{s-1}} \rangle$.

**Proof** By [65, Theorem 9.1.1], the multiplicative group of any finite field is cyclic. So let $w$ be a primitive element of $\text{GF}(2^{2^s})$, such that

$$\langle w \rangle \cong \text{GF}(2^{2^s})^* \cong \mathbb{Z}_{2^{2^s} - 1}.$$ 

By Equation 6.1.1, $2^{2^s} - 1 = F_0F_1...F_{s-1}$, so $w^{F_iF_{i+1}...F_{s-1}}$ has order $F_0F_1...F_{i-1}$ in $\text{GF}(2^{2^s})^*$. Thus

$$\langle w^{F_iF_{i+1}...F_{s-1}} \rangle \cong \mathbb{Z}_{F_0F_1...F_{i-1}}.$$ 

Now $2^d | 2^s$, so by [65, Theorem 9.3.1], $\text{GF}(2^{2^s})$ has exactly one subfield $M \cong \text{GF}(2^d)$. Therefore, $M^* \leq \text{GF}(2^{2^s})^*$, and by Equation 6.1.1,

$$M^* \cong \mathbb{Z}_{2^{2^d} - 1} = \mathbb{Z}_{F_0F_1...F_{i-1}}.$$ 

By [38, Chapter 1, Exercise 3.6], for any cyclic group of order $n$, there exists exactly one subgroup of order $m$ for each $m | n$. And by Equation 6.1.1,

$$F_0F_1...F_{i-1} | F_0F_1...F_{i-1}F_iF_{i+1}...F_{s-1} = 2^{2^s} - 1 = |\text{GF}(2^{2^s})^*|.$$ 

Thus $\text{GF}(2^{2^s})^*$ has exactly one subgroup isomorphic to $\mathbb{Z}_{F_0F_1...F_{i-1}}$. Therefore

$$M^* = \langle w^{F_iF_{i+1}...F_{s-1}} \rangle.$$ 

Using Lemma 6.2.1, we obtain a lower bound on the clique number $\omega(\Gamma)$ of $\Gamma$. 
Theorem 6.2.2 Let $\Gamma = \Gamma(2^s, p, S, U)$, where $p < q = 2^{2^x} + 1$, $p$ and $q$ are prime. Then $\omega(\Gamma) \geq p$, and equality occurs only if $p = 2^{2^l} + 1$ is a Fermat prime for some $0 \leq l \leq s - 1$.

Proof By Definition 4.4.1 and Theorem 4.4.4, for each $u \in \mathbb{Z}_p$,

$$\Gamma(2^s, p, \emptyset, \{u\}) \cong \Gamma(2^s, p, \emptyset, \{0\}).$$

Therefore, from Definition 4.4.1, $\Gamma(2^s, p, S, U)$ contains a spanning subgraph isomorphic to $\Gamma(2^s, p, \emptyset, \{0\})$, which implies that

$$\omega(\Gamma(2^s, p, \emptyset, \{0\})) \leq \omega(\Gamma(2^s, p, S, U)).$$

So it suffices to prove that $\omega(\Gamma) \geq p$ for $\Gamma = \Gamma(2^s, p, \emptyset, \{0\})$.

From Definition 4.4.1 and Equation 6.1.1,

$$p | 2^{2^s} - 1 = F_0F_1 \ldots F_{s-1}.$$

But all Fermat numbers are coprime to one another, so if $p$ is a prime then $p$ divides exactly one Fermat number $F_l$, for some $0 \leq l \leq s - 1$. Now since $l \leq s - 1$, $2^l | 2^s$. So by [65, Theorem 9.3.1], there exists exactly one subfield $GF(2^{2^l}) \leq GF(2^{2^s})$, where by Lemma 6.2.1, $GF(2^{2^l})^* = \langle w^{F_l+F_{l+1}+\ldots+F_{s-1}} \rangle$. Hence for each $w^{iF_l+F_{l+1}+\ldots+F_{s-1}} \in GF(2^{2^l})^*$,

$$2^{iF_l+F_{l+1}+\ldots+F_{s-1}} \equiv 0 \mod p. \quad (6.2.1)$$

Now $GF(2^{2^l})$ is a field, so its additive group is isomorphic to $\mathbb{Z}_2^{2^l}$. Therefore, for any two distinct elements $x, y \in GF(2^{2^l})$,

$$y = x + w^{iF_l+F_{l+1}+\ldots+F_{s-1}} \quad (6.2.2)$$

for some $w^{iF_l+F_{l+1}+\ldots+F_{s-1}} \in GF(2^{2^l})^*$.

So we define $C \subseteq V(\Gamma)$ to be the set

$$C := \{(x, 0) \mid x \in GF(2^{2^l})\}.$$
By Equations 6.2.1 and 6.2.2, for any two distinct vertices \((x, 0), (y, 0) \in C\),

\[(y, 0) = (x + w^{iF_iF_{i+1}...F_{s-1}}, 2iF_iF_{i+1}...F_{s-1})\]

for some \(w^{iF_iF_{i+1}...F_{s-1}} \in \text{GF}(2^{2l})^*\). Therefore, by Definition 4.4.1, \([ (x, 0), (y, 0) ] \in E(\Gamma)\), such that \(C\) is a clique of order \(2^{2l}\). Furthermore, by Definition 4.4.1, \((\infty, 0) \in V(\Gamma)\) is adjacent to every vertex in \(C\), so \(\{ (\infty, 0) \} \cup C\) is a clique of order \(2^{2l} + 1\).

Hence \(\omega(\Gamma) \geq 2^{2l} + 1\), and since \(p\) is a prime factor of \(2^{2l} + 1\), \(\omega(\Gamma) \geq p\) with equality only if \(p = 2^{2l} + 1\) is a Fermat prime.

There are two significant consequences of Theorem 6.2.2. The first consequence is that \(\omega(\Gamma^*) = \omega(\Gamma) \geq p\), which implies that if the order of \(\Gamma^*\) is \(p\), then \(\Gamma^* \cong K_p\). So by Theorem 6.2.2, every imprimitive Marušič-Scapellato graph of order \(pq\) is either a core or has a complete core.

The second consequence of Theorem 6.2.2 is that if \(p\) is not a Fermat prime, then for \(\Gamma = \Gamma(2^s, p, S, U)\) and \(u \in U\),

\[\omega(\Gamma^*) = \omega(\Gamma) \geq \omega(\Gamma(2^s, p, \emptyset, \{u\})) = \omega(\Gamma(2^s, p, \emptyset, \{0\})) > p,\]

which implies that \(\Gamma^*\) does not have order \(p\). Further, since every Marušič-Scapellato graph is edge-disjoint from \(\Gamma(2^s, p, \emptyset, \{v\}) \cong \Gamma(2^s, p, \emptyset, \{0\})\) for each \(v \in \mathbb{Z}_p \setminus U\), we have \(\alpha(\Gamma) > p\). Thus \(\omega(\Gamma) < q\) by Theorem 2.2.3, which by Theorem 6.1.2 implies that the core does not have order \(q\). So \(\Gamma\) must be a core if \(p\) is not a Fermat prime.

So with these consequences in mind, we give the upper bound on the clique number. Let \(\Gamma = \Gamma(2^s, p, S, U)\). For any \(u \in \mathbb{Z}_p\), we define \(\Gamma_u\) to be the induced subgraph of \(\Gamma\) with

\[V(\Gamma_u) = \{ (x, u) \mid x \in \text{GF}(2^{2^s}) \}.\]

In Section 6.1, the subgroup \(H \rtimes J < \text{SL}(2, 2^{2s}) < \text{Aut}(\Gamma)\) generated by the automorphisms \(\lambda_b\) and \(\rho^p\) (see Equations 6.1.2 and 6.1.3), fixes pointwise the block \(B_\infty\). Further, each \(\gamma \in H \rtimes J\) acts on \(V(\Gamma_u)\) via the mapping

\[\gamma((x, u)) = (\gamma(x), u) = (xw^{ip} + b, u)\]
(where \((x,u) \in V(\Gamma_u), w^p \in GF(2^s)^*\) and \(b \in \mathbb{Z}_2^2\)) by [56], so \(\gamma\) is an automorphism of \(\Gamma_u\). Hence \(\Gamma_u\) is vertex-transitive, with \(H \cong \mathbb{Z}_2^s\) regular on \(V(\Gamma_u)\) (since \(\mathbb{Z}_2^s\) is regular on \(GF(2^s)\)), and \(J \leq \text{Aut}(\Gamma_u)\).

**Theorem 6.2.3** Let \(\Gamma = \Gamma(2^s, p, S, U)\), where \(p < q = 2^{2s} + 1\), \(p\) and \(q\) are prime.

If \(S = \emptyset\), then \(\omega(\Gamma) \leq |U| \frac{2^{s^2}}{p-1} + 1\). If \(S \neq \emptyset\), then \(\omega(\Gamma) \leq |U| \frac{2^{s^2} + p - 1}{p-1}\).

**Proof** Fix \(r \in \mathbb{Z}_p \setminus U\), and denote \(\Gamma' := \Gamma(2^s, p, \emptyset, \{r\})\). Then \(\Gamma\) is edge-disjoint from \(\Gamma'\), and for any \(u \in \mathbb{Z}_p\), \(\Gamma_u\) is edge-disjoint from \(\Gamma'_u\). Hence any clique in \(\Gamma'_u\) is an independent set in \(\Gamma_u\). So \(\omega(\Gamma'_u) \leq \alpha(\Gamma_u)\).

Since \(\Gamma'\) is vertex-transitive, every vertex of \(\Gamma'\) is contained in some maximum clique. In particular, for each \(u \in \mathbb{Z}_p\), \((\infty, u - r)\) is contained in a maximum clique of \(\Gamma'\). By Definition 4.4.1, \(N_{\Gamma'}((\infty, u - r)) = V(\Gamma_u)\), so any maximum clique of \(\Gamma'\) which contains \((\infty, u - r)\) must be a subset of \(\{(\infty, u - r)\} \cup V(\Gamma'_u)\). Therefore, \(\omega(\Gamma'_u) = \omega(\Gamma') - 1\), where by Theorem 6.2.2, \(\omega(\Gamma') \geq p\). Thus for each \(u \in \mathbb{Z}_p\),

\[
p - 1 \leq \omega(\Gamma'_u) \leq \alpha(\Gamma_u),
\]

so by Theorem 2.2.3,

\[
\omega(\Gamma_u) \leq \frac{|V(\Gamma_u)|}{\alpha(\Gamma_u)} \leq \frac{2^{s^2}}{p-1}.
\] (6.2.3)

Now let \(C\) be a fixed maximum clique of \(\Gamma\) containing \((\infty, 0)\) (such a maximum clique exists since \(\Psi\) is vertex-transitive), and let \(N\) be the set of elements \(u \in \mathbb{Z}_p\) such that \(C \cap V(\Gamma_u) \neq \emptyset\). By Definition 4.4.1, whenever \(u \notin U\), \((\infty, 0)\) is not adjacent in \(\Gamma\) to any vertex of \(V(\Gamma_u)\), such that

\[
N = \{u \in U : C \cap V(\Gamma_u) \neq \emptyset\}.
\]

Since \(|C \cap V(\Gamma_u)| \leq \omega(\Gamma_u) \leq \frac{2^{s^2}}{p-1}\) by Equation 6.2.3, we obtain

\[
|C| = |C \cap B_\infty| + \sum_{u \in N} |C \cap V_u| \leq |C \cap B_\infty| + \frac{2^s}{p-1} |N|.
\] (6.2.4)

Set

\[
T_1 := \{(\infty, z) \in C \cap B_\infty : z + r \in U\}, \quad T_2 := \{(\infty, z) \in C \cap B_\infty : z + r \notin U\}.
\]
Then $|C \cap B_{\infty}| = |T_1| + |T_2|$. Since $r \notin U$, by Definition 4.4.1 no vertex $(\infty, z) \in C \cap B_{\infty}$ is adjacent to any vertex in $V(\Gamma_{z+r})$. Thus, for each $(\infty, z) \in T_1$, we have $C \cap V(\Gamma_{z+r}) = \emptyset$ and so $z + r \notin N$. Consequently $|N| \leq |U| - |T_1|$. So by Equation 6.2.4, noting that $\frac{2^{2^s}}{p-1} > 1$, we obtain
\[
\omega(\Gamma) = |C| \leq |T_1| + |T_2| + \frac{2^{2^s}}{p-1}(|U| - |T_1|)
\]
\[
= \frac{2^{2^s}}{p-1}|U| + |T_1| \left(1 - \frac{2^{2^s}}{p-1}\right) + |T_2|
\]
\[
\leq \frac{2^{2^s}}{p-1}|U| + |T_2|.
\]

If $S = \emptyset$, then $C \cap B_{\infty} = \{(\infty,0)\}$. Since $0 + r \notin U$, we then have $|T_2| = 1$ and
\[
\omega(\Gamma) \leq \frac{2^{2^s}}{p-1}|U| + 1.
\]

Assume that $S \neq \emptyset$. If $|C \cap B_{\infty}| \leq p - 1$, then $|T_2| \leq p - 1$. If $|C \cap B_{\infty}| = p$, then $C \cap B_{\infty} = B_{\infty}$ and so $T_1 \neq \emptyset$, implying $|T_2| = |C \cap B_{\infty}| - |T_1| \leq p - 1$. In either case we obtain
\[
\omega(\Gamma) \leq \frac{2^{2^s}}{p-1}|U| + p - 1.
\]

From Theorem 6.2.3, $\omega(\Gamma) < q$ unless $|U| = p - 1$, so the core of $\Gamma$ does not have order $q$ unless $|U| = p - 1$.

### 6.3 Bounding the independence number

By Theorem 6.2.2, $\omega(\Gamma) \geq p$, with equality only if $p$ is a Fermat prime. Therefore, to determine whether or not $|V(\Gamma^*)| = p$, we must determine whether or not $\Gamma \to K_p$. Thus, we prove an upper bound on $\alpha(\Gamma)$.

Let $p = 2^l + 1$ with $0 \leq l \leq s - 1$, $n = F_l \ldots F_{s-1}$, and
\[
C = \left\{(x, 0) \mid x \in \text{GF}(2^l)\right\}.
\]
By Theorem 6.2.2, for each $1 \leq h \leq F_0 \ldots F_{l-1}$, both $C$ and $\lambda_{w^{hn}}(C)$ are $(p-1)$-cliques of $\Gamma_0$. To prove an upper bound on $\alpha(\Gamma)$, we show that $C$ and $J(\lambda_{w^{hn}}(C))$ partition $V(\Gamma_0)$ into distinct $(p-1)$-cliques. We begin by showing that $C$ and $\lambda_{w^{hn}}(C)$ are distinct.

**Lemma 6.3.1** Let $\Gamma = \Gamma(2^s, p, \emptyset, \{0\})$, where $0 \leq l \leq s - 1$ and $p = 2^{2l} + 1 < q = 2^{2^s} + 1$ are Fermat primes. Then for each $1 \leq h \leq F_0 \ldots F_{l-1}$, both $C$ and $\lambda_{w^{hn}}(C)$ are blocks $H \cong \mathbb{Z}_2^{2^s}$ in its action on $V(\Gamma_0)$, and cliques of $V(\Gamma_0)$. Further, $C \cap \lambda_{w^{hn}}(C) = \emptyset$.

**Proof** Define

$$L := \left\{ \lambda_b \mid \hat{b} \in \text{GF}(2^{2l}) \right\}.$$  

Then by Equation 6.1.2, $L \leq H \leq \text{Aut}(\Gamma)_{(\infty,0)}$. Thus, for $(0,0) \in V(\Gamma_0)$,

$$L((0,0)) = \left\{ (\hat{b},0) \mid \hat{b} \in \text{GF}(2^{2l}) \right\} = C.$$

Now $H \cong \mathbb{Z}_2^{2^s}$, so every subgroup of $H$ is a normal subgroup; thus $L \leq H$. Further, $H$ is transitive on $V(\Gamma_0)$, so by Lemma 2.1.4, $C$ is a block of $H$ in its action on $V(\Gamma_0)$. Thus, for each $\lambda_0 \in H$, $\lambda_0(C)$ is a block of $H$, and a clique of $\Gamma_0$. Specifically, by Lemma 6.2.1, $(w^{hn}, 0) \notin C$. Therefore,

$$\lambda_{w^{hn}}(C) = \left\{ (x + w^{hn}, 0) \mid x \in \text{GF}(2^{2l}) \right\} \neq C,$$

such that $C \cap \lambda_{w^{hn}}(C) = \emptyset$.  

Now we determine which elements of $V(\Gamma_0)$ are contained within $\lambda_{w^{hn}}(C)$.

**Lemma 6.3.2** Let $\Gamma = \Gamma(2^s, p, \emptyset, \{0\})$, where $0 \leq l \leq s - 1$ and $p = 2^{2l} + 1 < q = 2^{2^s} + 1$ are Fermat primes. Further, let $(w^j, 0) \in \lambda_{w^{hn}}(C)$ with $1 \leq h \leq F_0 \ldots F_{l-1}$, $1 \leq j \leq F_0 \ldots F_{s-1}$ and $w^j \neq h^{\text{mod } p}$. Then $j \neq hn \text{ mod } p$.

**Proof** Let $(w^j, 0) \in \lambda_{w^{hn}}(C)$ with $1 \leq j \leq F_0 \ldots F_{s-1}$ and $w^j \neq h^{\text{mod } p}$. Then $(w^j, 0) = (x + h^{\text{mod } p}, 0)$, where $x \in \text{GF}(2^{2l}) \setminus \{0\}$. Thus by Lemma 6.2.1, $x = w^{tpn}$, with $p = F_i$ and $1 \leq t \leq F_0 \ldots F_{l-1}$. Therefore,

$$w^j = w^{hn} + w^{tpn} = w^{hn}(w^0 + w^{(t-p)hn})$$
and
\[ w^0 + w^{(tp-h)n} = w^{j-hn}. \]

From Lemma 6.2.1, \( w^0, w^{(tp-h)n} \in GF(2^{2l+1}) \), where \( GF(2^{2l+1}) \) is a subfield of \( GF(2^s) \), so that \( w^0 + w^{(tp-h)n} \in GF(2^{2l+1}) \). Thus, by Lemma 6.2.1,
\[ w^{j-hn} = w^0 + w^{(tp-h)n} = w^zn \]
for some \( 1 \leq z \leq F_0 \ldots F_l \).

So we assume that \( j \equiv hn \mod p \). Then
\[ j - hn = zn \equiv 0 \mod p. \tag{6.3.1} \]

Since all Fermat numbers are coprime, \( n \) is coprime with \( p \), so Equation 6.3.1 implies that \( z \equiv 0 \mod p \). So by Lemma 6.2.1, \( w^0, w^zn \in GF(2^{2l}) \), so that \( w^0 - w^zn \in GF(2^{2l}) \), where
\[ w^0 - w^zn = w^0 - w^0 - w^{(tp-h)n} = -w^{(tp-h)n}. \]

Thus \( w^{(tp-h)n} \in GF(2^s) \). From Lemma 6.2.1, \( w^{(tp-h)n} \in GF(2^s) \) implies that \( (tp-h)n \equiv 0 \mod pn \). Now \( p \) is a Fermat prime, and all Fermat numbers are coprime, so \( tp-h \equiv 0 \mod p \). However, \( 1 \leq h \leq F_0 \ldots F_{l-1} \), so \( p \nmid h \), and we have a contradiction. Therefore \( j \not\equiv hn \mod p \). \( \square \)

**Lemma 6.3.3** Let \( \Gamma = \Gamma(2^s, p, \emptyset, \{0\}) \), where \( 0 \leq l \leq s - 1 \) and \( p = 2^l + 1 < q = 2^s + 1 \) are Fermat primes. Further, let \((w^i, 0), (w^j, 0) \in \lambda_{w^{hn}}(C)\) with \( 1 \leq h \leq F_0 \ldots F_{l-1}, 1 \leq i, j \leq F_0 \ldots F_{s-1} \) and \( w^i \neq w^j \). Then \( j \not\equiv i \mod p \).

**Proof** Let \((w^i, 0), (w^j, 0) \in \lambda_{w^{hn}}(C)\) with \( 1 \leq h \leq F_0 \ldots F_{l-1} \) and \( w^i \neq w^j \). Then \( w^i = w^{hn} + x \) and \( w^j = w^{hn} + y \) for some \( x, y \in GF(2^{2l}) \). By Lemma 6.2.1, \( w^{hn} \in GF(2^{2l+1}) \setminus GF(2^s) \), where \( GF(2^{2l}) < GF(2^{2l+1}) \) and \( GF(2^{2l+1}) \) is closed under addition. Thus, \( w^i, w^j \in GF(2^{2l+1}) \setminus GF(2^s) \), and by Lemma 6.2.1, \( w^i = w^{hn} \) for some \( 1 \leq h \leq F_0 \ldots F_{l-1} \).
By Lemma 6.3.1, \((w^i, 0) \in \lambda_w(C)\) implies that
\[
\lambda_w(C) = \lambda_w(C) = \lambda_w(C),
\]
such that \((w^j, 0) \in \lambda_w(C)\). So by Lemma 6.3.2 \(j \not\equiv \bar{hn} \mod p = i \mod p\). □

Using Lemmas 6.3.1, 6.3.2 and 6.3.3, we now show that \(C\) and \(J(\lambda_w(C))\) partition \(V(\Gamma_0)\) into distinct \((p - 1)\)-cliques, and thus give an upper bound on \(\alpha(\Gamma)\).

**Theorem 6.3.4** Let \(\Gamma = \Gamma(2^s, p, \emptyset, \{0\})\), where \(0 \leq l \leq s - 1\) and \(p = 2^{2^l} + 1 < q = 2^{2^s} + 1\) are Fermat primes. Then \(\alpha(\Gamma) \leq 2^{2^s} + 1\), with equality only if \(p = 2^{2^s-1} + 1\).

**Proof** Let \(n = F_{l+1} \ldots F_{s-1}\), and \(h = 1\). By Lemma 6.3.1 both \(C\) and \(\lambda_w(C)\) are \((p - 1)\)-cliques of \(\Gamma_0\), with \(C \cap \lambda_w(C) = \emptyset\). Thus for any \((w^j, 0) \in \lambda_w(C) \neq C\), \(w^j \not\in GF(2^{2^l})\), so by Lemma 6.2.1, \(j \not\equiv 0 \mod p\). Further, by Lemma 6.3.3, the \((p - 1)\)-clique \(\lambda_w(C)\) contains exactly one element \((w^j, 0)\), such that \(j \equiv d \mod p\) for each \(d \in \mathbb{Z}_p \setminus \{0\}\).

By Equation 6.1.3, for each \((w^j, 0) \in \lambda_w(C)\) and \(1 \leq t \leq 2^{2^s-1}p\),
\[
\rho^{tp}((w^j, 0)) = (w^{j+tp}, 0),
\]
where \(j + tp \equiv j \mod p\). Further,
\[
\langle \rho^p \rangle = J \leq \text{Aut}(\Gamma_0)_{(0,0)} \text{ (with } J \cong \mathbb{Z}_{2^{2^s-1}})\]
is abelian and acts faithfully on \(V(\Gamma_0)\), so by Theorem 2.1.2, \(J\) acts regularly on its orbits in \(V(\Gamma_0) \setminus \{(0,0)\}\). Therefore, by Corollary 2.1.3, for each \((w^j, 0) \in \lambda_w(C)\),
\[
|J((w^j, 0))| = |J| = \frac{2^{2^s} - 1}{p}.
\]
However, for each \(j \in \mathbb{Z}_p \setminus \{0\}\), \(|\{(w^{j+tp}, 0) \mid 1 \leq t \leq \frac{2^{2^s-1}}{p}\}| = \frac{2^{2^s-1}}{p}\), so that
\[
J((w^j, 0)) = \left\{(w^{j+tp}, 0) \mid 1 \leq t \leq \frac{2^{2^s-1}}{p}\right\}.
\]
Hence for any integers $1 \leq t_1, t_2 \leq \frac{2^{2s}-1}{p}$ with $t_1 \neq t_2$, $\rho^{t_1p}(\lambda_{w^n}(C))$ and $\rho^{t_2p}(\lambda_{w^n}(C))$ are both $(p-1)$-cliques with

$$\rho^{t_1p}(\lambda_{w^n}(C)) \cap \rho^{t_2p}(\lambda_{w^n}(C)) = \emptyset.$$  

Therefore, since $N_{\Gamma_0}((0,0)) = \{(w^{tp},0) \mid 1 \leq t \leq \frac{2^{2s}-1}{p}\}$ by Definition 4.4.1, $J(\lambda_{w^n}(C))$ partitions $V(\Gamma_0) \setminus \{N_{\Gamma_0}((0,0)) \cup \{(0,0)\}\}$ into $\frac{2^{2s}-1}{p}$ distinct $(p-1)$-cliques.

Now $\Gamma_0$ is vertex-transitive, so every element of $V(\Gamma_0)$ is contained within a maximum independent set. So let $A$ be a maximum independent set of $\Gamma_0$, with $(0,0) \in A$. Clearly, $A \cap N_{\Gamma_0}((0,0)) = \emptyset$. Furthermore, for each $\rho^{tp} \in J$, $\rho^{tp}(\lambda_{w^n}(C))$ is a clique, so that $|A \cap \rho^{tp}(\lambda_{w^n}(C))| = \{0,1\}$. Hence $\alpha(\Gamma_0) \leq 1 + \frac{2^{2s}-1}{p}$.

Now $\Gamma$ is vertex-transitive, so for every $u \in V(\Gamma)$,

$$\alpha(N_\Gamma(u)) = \alpha(N_\Gamma((\infty,0))) = \alpha(\Gamma_0).$$

Therefore, by Equation 6.1.1 and Theorems 2.2.1 and 4.4.4,

$$\alpha(\Gamma) \leq \frac{\alpha(\Gamma_0)|V(\Gamma)|}{\alpha(\Gamma_0) + \text{val}(\Gamma)} \leq \frac{(1 + \frac{2^{2s}-1}{p})p(2^{2s} + 1)}{1 + \frac{2^{2s}-1}{p} + 2^{2s}}$$

$$= (2^{2s} + 1) \frac{2^{2s} + (p-1)}{2^{2s} + (1 + \frac{2^{2s}-1}{p})}$$

$$\leq 2^{2s} + 1,$$

since $p - 1 \leq \frac{2^{2s}-1}{p} + 1$. Moreover, by Equation 6.1.1, the equality holds only if $p = 2^{2s-1} + 1$. \hfill \Box

### 6.4 Cores of Marušić-Scapellato graphs

Collecting all the results from Sections 6.1, 6.2 and 6.3, we now determine the cores of all imprimitive, symmetric Marušić-Scapellato graphs of order $pq$. 
**Theorem 6.4.1** Let $\Gamma = \Gamma(2^s, p, \emptyset, U)$ be an imprimitive symmetric Marušič-Scape\-llato graph, where $3 \leq p < q = 2^{2s} + 1$ are prime. Then either:

(i) $pq = 15$ and either $\Gamma = \Gamma(2, 3, \emptyset, \{u\})$, in which case $\Gamma$ is a core, or $\Gamma = \Gamma(2, 3, \emptyset, \{1, 2\})$, in which case $\Gamma^* \cong K_5$;

(ii) $pq \neq 15$ and $p$ is not a Fermat prime, in which case $\Gamma$ is a core;

(iii) $pq \neq 15$, $0 \leq l < s - 1$ and $p = 2^{2l} + 1$ is a Fermat prime, in which case $\Gamma$ is a core;

(iv) $pq \neq 15$, $p = 2^{2s-1} + 1$ is a Fermat prime and $U = \{u\}$ where $u \in \mathbb{Z}_p$, in which case $\Gamma^* \cong K_p$;

(v) $pq \neq 15$, $p = 2^{2s-1} + 1$ is a Fermat prime and $2 \leq |U| < p - 1$, in which case $\Gamma$ is a core.

**Proof** Since $\Gamma$ is vertex-transitive, by Theorem 2.3.22, if $\Gamma$ is not a core then either $|V(\Gamma^*)| = p$ or $|V(\Gamma^*)| = q$. By Proposition 2.3.5, $\omega(\Gamma) = \omega(\Gamma^*)$. So by Theorem 6.2.2, $\omega(\Gamma^*) = \omega(\Gamma) \geq p$. Thus if $|V(\Gamma^*)| = p$, then $\Gamma^* \cong K_p$. Whilst by Theorem 6.1.2, if $pq \neq 15$ and $|V(\Gamma^*)| = q = 2^{2s} + 1$, then $\Gamma^* \cong K_{2^{2s} + 1}$.

Further, by Definition 4.4.1, whenever $pq \neq 15$ and $p = 2^{2s-1} + 1$, $q = 2^{2s} + 1 > 5 = 2^2 + 1$. Therefore, $p \geq 2^2 + 1 = 5$, so by Theorem 4.4.4, $1 \leq |U| < p - 1$.

(i) Let $pq = 15$. By Theorem 4.4.4, $\Gamma = \Gamma(2,3,\emptyset,\{0\})$ or $\Gamma = \Gamma(2,3,\emptyset,\{1,2\})$. If $\Gamma = \Gamma(2,3,\emptyset,\{0\})$, then computations performed using Mathematica show that $\omega(\Gamma) = \chi(\Gamma) = 5$, such that $\Gamma^* \cong K_5$. Whilst if $\Gamma = \Gamma(2,3,\emptyset,\{0\})$, then computations show that $\chi(\Gamma) = 4$ and $\omega(\Gamma) = 3$, so that $\Gamma^* \ncong K_3$. Further, by Theorem 4.2.2, if $|V(\Gamma^*)| = 5$ then either $\Gamma^* \cong K_5$ or $\Gamma^* \cong C_5$. However, $\chi(K_5) \neq 4$ and $\chi(C_5) \neq 4$. So by Proposition 2.3.5, $|V(\Gamma^*)| \neq 5$. Therefore $\Gamma$ is a core.

(ii) Let $pq \neq 15$ with $p$ not a Fermat prime. By Proposition 2.3.5 and Theorem 6.2.2, $\omega(\Gamma^*) > p$; thus $|V(\Gamma^*)| > p$. Further, by Theorem 4.4.4, $U \neq \mathbb{Z}_p$. So for any $u \in \mathbb{Z}_p \setminus U$, there exists a graph $\Gamma' = \Gamma(2^s, p, \emptyset, \{u\})$, with $V(\Gamma) = V(\Gamma^*)$, $E(\Gamma) \cap E(\Gamma') = \emptyset$ and thus $\omega(\Gamma') \leq \alpha(\Gamma)$. Now by Theorem 6.2.2, $p < \omega(\Gamma') \leq \alpha(\Gamma)$. However, by Lemmas 2.3.15 and 2.3.16, if $\Gamma^* \cong K_q$, then $\alpha(\Gamma) = p$; thus $|V(\Gamma^*)| \neq q$. Hence $\Gamma$ is a core.
(iii) Let \( pq \neq 15 \), \( p \) be a Fermat prime with \( p \leq 2^{2s-2} + 1 \), \( u \in \mathbb{Z}_p \setminus U \) and \( \Gamma' = \Gamma(2^s, p, \emptyset, \{u\}) \). Then \( \Gamma \) is a spanning subgraph of \( \overline{\Gamma} \), so that \( \omega(\Gamma) \leq \omega(\overline{\Gamma}) = \alpha(\Gamma') \). By Theorem 4.4.4, \( \Gamma' \cong \Gamma(2^s, p, \emptyset, \{0\}) \). Thus by Theorem 6.3.4, \( \omega(\Gamma) < 2^{2^s} + 1 \). Therefore, by Theorem 6.1.2, \( |V(\Gamma)| \neq q \). Further, by Theorem 4.4.4, \( \Gamma \) contains a spanning subgraph isomorphic to \( \Gamma' \). Therefore, by Theorem 6.3.4, \( \alpha(\Gamma) \leq \alpha(\Gamma') < 2^{2^s} + 1 \). However, by Lemmas 2.3.15 and 2.3.16, if \( \Gamma^* \cong K_p \), then \( \alpha(\Gamma) = q \); thus \( |V(\Gamma^*)| \neq p \). Hence \( \Gamma \) is a core.

(iv) Let \( 5 \leq p = 2^{2^s-1} + 1 \), \( |U| = 1 \) and \( \Psi \) be the primitive symmetric graph outlined in Theorem 4.4.5, with edge set given by Equation 4.4.1. Then by Theorem 4.4.5, \( |V(\Psi)| = p(2^{2^s} + 1) \) and \( \text{val}(\Psi) = (2^{2^s-1}) + (2^{2^s-1})^2 \). Further by Theorem 4.4.6, \( \Psi \) is isomorphic to a Marušić-Scapellato graph. Thus by Definition 4.4.1 and Theorem 4.4.4, \( \Gamma \) is isomorphic to a spanning subgraph of \( \Psi \).

Now by Theorem 4.4.7, \( \Psi \) has a complete core, so either \( \Psi^* \cong K_p \) or \( \Psi^* \cong K_{2^{2^s+1}} \). However, \( 2^{2^s} \nmid \text{val}(\Psi) \), so by Theorem 2.3.23, \( \Psi^* \neq K_{2^{2^s+1}} \). Thus \( \Psi^* \cong K_p \).

Therefore, there exists a homomorphism \( \Gamma \rightarrow K_p \). By Theorem 6.2.2, \( \omega(\Gamma) \geq p \), so \( \Gamma \) contains a copy of \( K_p \) as an induced subgraph. Hence \( \Gamma \leftrightarrow K_p \), so by Lemma 2.3.14, \( \Gamma^* \cong K_p \).

(v) Let \( 5 \leq p = 2^{2^s-1} + 1 \) and \( 2 \leq |U| < p - 1 \). Then \( \overline{\Gamma} = \Gamma(2^s, p, \mathbb{Z}_p^*, \overline{U}) \), where \( \overline{U} = \mathbb{Z}_p \setminus U \) so that \( |\overline{U}| = p - |U| \). So by Theorem 6.2.3,

\[
\alpha(\Gamma) = \omega(\overline{\Gamma}) \leq (p - |U|) \frac{2^{2^s}}{p - 1} + p - 1 \\
\leq (p - 2) \frac{2^{2^s}}{p - 1} + p - 1 \\
= 2^{2^s} < 2^{2^s} + 1.
\]

By Lemmas 2.3.15 and 2.3.16, if \( \Gamma^* \cong K_p \), then \( \alpha(\Gamma) = q \); thus \( |V(\Gamma^*)| \neq p \). Further, by Theorem 6.2.3,

\[
\omega(\Gamma) \leq |U| \frac{2^{2^s}}{p - 1} + 1 < 2^{2^s} + 1.
\]

Hence \( \omega(\Gamma) \neq 2^{2^s} + 1 \). Thus \( |V(\Gamma^*)| \neq q \). Hence \( \Gamma \) is a core. \qed
Chapter 7

Cayley graphs of abelian groups

In the proof of Theorem 4.1.2, if an imprimitive symmetric $pq$ graph $\Gamma$ is not a core, $\Gamma^*$ is a symmetric graph of prime order. Thus $\Gamma^*$ has semiregular automorphisms, and a primitive automorphism group. In this chapter, we generalise the proof of Theorem 4.1.2, and investigate Cayley graphs of abelian groups whose cores either have semiregular automorphisms, or primitive automorphism groups.

In Section 7.1, with Lemma 7.1.1 we show that for any Cayley graph $\Gamma = \text{Cay}(G, S)$ of an abelian group $G$, there exists a subgroup of $\text{Aut}(\Gamma^*)$ which is generated by semiregular automorphisms, is transitive and is potentially abelian. Using Lemma 7.1.1, we prove Theorem 7.1.2, which is an upper bound on the girth of $\Gamma^*$, when $\Gamma^*$ is not an odd cycle. From Theorem 7.1.2, we prove Corollaries 7.1.3 and 7.1.5, which determine $\Gamma^*$ when $\Gamma$ is nonbipartite, and $\Gamma^*$ is either a cubic symmetric graph or a 3-arc-transitive graph.

Finally, in Section 7.2 we prove Theorem 7.2.7, which states that if $\Gamma^*$ is a primitive graph with $|V(\Gamma^*)| = p^n$ for prime $p \neq 3$, then $\Gamma^*$ is a Cayley graph of an elementary abelian group. From Theorem 7.2.7 we obtain Corollary 7.2.8, which partially confirms Conjecture 1.2.3.

7.1 Cores of Cayley graphs of abelian groups

In Lemma 5.3.4 we show that for $\Gamma = G(pq; r, s, u)$ and a retraction $\phi : \Gamma \to \Gamma^*$ with $\phi |_{\Gamma^*} = 1_{\text{Aut}(\Gamma^*)}$, there exists $\gamma \in \text{Aut}(\Gamma)$ such that $(\phi \circ \gamma) |_{\Gamma^*} \in \text{Aut}(\Gamma^*)$ is semiregular.
CHAPTER 7. CAYLEY GRAPHS OF ABELIAN GROUPS

in its action on $V(\Gamma^*)$. The proof of Lemma 5.3.4 requires that $[u, \gamma(u)] \in E(\Gamma)$ for all $u \in V(\Gamma)$. Now from Definition 2.2.9, if $G$ is an abelian group and $S \subseteq G$, then for $\Gamma = \text{Cay}(G, S)$, there exists some $\rho \in \text{Aut}(\Gamma^*)$ such that $[u, \rho(u)] \in E(\Gamma)$ for all $u \in V(\Gamma)$. Thus in Lemma 7.1.1 we generalise Lemma 5.3.4, showing that if $\Gamma$ is a Cayley graph of an abelian group and $\phi : \Gamma \to \Gamma^*$ is a retraction with $\phi |_{\Gamma^*} = 1_{\text{Aut}(\Gamma^*)}$, then $(\phi \circ \rho) |_{\Gamma^*} \in \text{Aut}(\Gamma^*)$ is semiregular on $V(\Gamma^*)$. We also prove some useful properties of the subgroups of $\text{Aut}(\Gamma^*)$ generated by these semiregular elements.

But first let $\Gamma = \text{Cay}(G, S)$, with $G$ an abelian group. Throughout this chapter we assume that $V(\Gamma^*) \subseteq V(\Gamma) = G$, with $0_G \in V(\Gamma^*)$ the identity element of $G$ (the vertex-transitivity of $\Gamma$ implies that every vertex of $\Gamma$ is contained in some copy of $\Gamma^*$). Then for each $v \in V(\Gamma)$ we define $\rho_v \in \text{Aut}(\Gamma)$ such that $\rho_v(u) := u + v$ for all $u \in V(\Gamma)$. Further, we define $C \subseteq S$ such that

$$C := \{c \mid c \in N_{\Gamma^*}(0_G)\},$$

with

$$A(\phi, \Gamma, \Gamma^*) := \{(\phi \circ \rho_c) |_{\Gamma^*} \mid c \in C\},$$

where $N_{\Gamma^*}(0_G)$ is the neighbourhood of $0_G$ in $\Gamma^*$, and $\phi : \Gamma \to \Gamma^*$ is a retraction with $\phi |_{\Gamma^*} = 1_{\text{Aut}(\Gamma^*)}$.

**Lemma 7.1.1** Let $\Gamma = \text{Cay}(G, S)$ be connected, undirected, with $G$ an abelian group. Then:

(i) $(\phi \circ \rho_s) |_{\Gamma^*}$ is semiregular on $V(\Gamma^*)$ for each $s \in S$;

(ii) for $u \in V(\Gamma^*)$, $N_{\Gamma^*}(u) = \{((\phi \circ \rho_c) |_{\Gamma^*})(u) \mid c \in C\}$,

(iii) $\langle A(\phi, \Gamma, \Gamma^*) \rangle$ is transitive on $V(\Gamma^*)$;

(iv) for $c_1, c_2 \in C$, $\eta_1 = (\phi \circ \rho_{c_1}) |_{\Gamma^*}$ and $\eta_2 = (\phi \circ \rho_{c_2}) |_{\Gamma^*}$,

$$\eta_1 \eta_2(0_G) = \eta_2 \eta_1(0_G) = \phi(c_1 + c_2);$$
(v) if \( \langle A(\phi, \Gamma, \Gamma^*) \rangle \) is semiregular on \( V(\Gamma^*) \), then it is an abelian group.

Proof

(i) Let \( \Gamma = \text{Cay}(G, S) \) with \( S \subseteq G \), \( G \) be an abelian group, and \( \phi : \Gamma \to \Gamma^* \) be a retraction from \( \Gamma \) to \( \Gamma^* \) with \( \phi \mid_{\Gamma^*} = 1_{\text{Aut}(\Gamma^*)} \). For each \( s \in S \), there exists some \( \rho_s \in \text{Aut}(\Gamma) \) such that \( \rho_s(u) = u + s \) for all \( u \in V(\Gamma) \). So \( \rho_s \) is semiregular on \( V(\Gamma) \).

Now \( \Gamma \) is undirected, so by Definition 2.2.9, \( S = -S \) and \( [v, v + s] \in E(\Gamma) \) for all \( v \in V(\Gamma) \). So by Proposition 2.3.7 each fibre of \( \phi \) must be an independent set. Thus for all \( v \in V(\Gamma) \), \( v \) and \( v + s \) are not in the same fibre of \( \phi \). Hence for any vertex in \( \Gamma \), \( \rho_s \) must map that vertex from one fibre of \( \phi \) to a different fibre of \( \phi \). Thus for any copy of \( \Gamma^* \) in \( \Gamma \), \( (\phi \circ \rho_s) \mid_{\Gamma^*} \in \text{Aut}(\Gamma^*) \) does not fix any element of \( V(\Gamma^*) \), so \( (\phi \circ \rho_s) \mid_{\Gamma^*} \) is semiregular. Therefore, by [71, pg. 357], \( \langle (\phi \circ \rho_s) \mid_{\Gamma^*} \rangle \leq \text{Aut}(\Gamma^*) \) is also semiregular.

(ii) Let \( c, \overline{c} \in C \) with \( c \neq \overline{c} \), and \( 0_G, v \in V(\Gamma^*) \). Then by Lemma 2.3.9, \( (\phi \circ \rho_c) \mid_{\Gamma^*} \in \text{Aut}(\Gamma^*) \), so that \( ((\phi \circ \rho_c) \mid_{\Gamma^*})(c) \neq ((\phi \circ \rho_c) \mid_{\Gamma^*})(\overline{c}) \). Further,
\[
((\phi \circ \rho_c) \mid_{\Gamma^*})(c) = \phi(v + c) = ((\phi \circ \rho_c) \mid_{\Gamma^*})(v)
\]
and
\[
((\phi \circ \rho_c) \mid_{\Gamma^*})(\overline{c}) = \phi(v + \overline{c}) = ((\phi \circ \rho_{\overline{c}}) \mid_{\Gamma^*})(v),
\]
so that
\[
((\phi \circ \rho_c) \mid_{\Gamma^*})(v) \neq ((\phi \circ \rho_{\overline{c}}) \mid_{\Gamma^*})(v).
\] (7.1.1)
Since \( \phi \) is a retraction with \( \phi \mid_{\Gamma^*} = 1_{\text{Aut}(\Gamma^*)} \), and \( [v, v + c] \in E(\Gamma) \) for \( c \in C \), \( \{((\phi \circ \rho_c) \mid_{\Gamma^*})(v) \mid c \in C \} \subseteq N_{\Gamma^*}(v) \). Now by Equation 7.1.1,
\[
\vert \{((\phi \circ \rho_c) \mid_{\Gamma^*})(v) \mid c \in C \} \vert = \vert C \vert = \vert N_{\Gamma^*}(0_G) \vert. \] And by Theorem 2.3.17, \( \Gamma^* \) is vertex-transitive, so that \( \vert N_{\Gamma^*}(0_G) \vert = \vert N_{\Gamma^*}(v) \vert \). Therefore, \( \{((\phi \circ \rho_c) \mid_{\Gamma^*})(v) \mid c \in C \} = N_{\Gamma^*}(v) \), and for each \( u \in N_{\Gamma^*}(v) \), there exists some \( \eta \in A(\phi, \Gamma, \Gamma^*) \) for which \( \eta(v) = u \).
(iii) Now \( \Gamma \) is connected, so \( \Gamma^* \) is connected. So for any two vertices \( u_1, u_n \in V(\Gamma^*) \), there exists a path \( P = u_1, u_2, \ldots, u_n \) of length \( n \) in \( \Gamma^* \). Then by (ii), for each \( 1 \leq i \leq n-1 \) there exists \( \eta_i \in A(\phi, \Gamma, \Gamma^*) \subseteq \text{Aut}(\Gamma^*) \) such that \( \eta_i(u_i) = u_{i+1} \). Thus

\[
\eta_{n-1}\eta_{n-2}\ldots\eta_1 \in \langle A(\phi, \Gamma, \Gamma^*) \rangle
\]

with \( \eta_{n-1}\eta_{n-2}\ldots\eta_1(u_1) = u_n \). Hence \( \langle A(\phi, \Gamma, \Gamma^*) \rangle \) is transitive on \( V(\Gamma^*) \).

(iv) Let \( c_1, c_2 \in C \) with \( c_1 \neq c_2 \), \( \eta_1 = (\phi \circ \rho_{c_1}) |_{\Gamma^*} \) and \( \eta_2 = (\phi \circ \rho_{c_2}) |_{\Gamma^*} \). Since \( G \) is abelian, \( \rho_{c_1} \) and \( \rho_{c_2} \) commute, so that

\[
\rho_{c_1}\rho_{c_2}(0_G) = \rho_{c_2}\rho_{c_1}(0_G) = c_1 + c_2 \in G.
\]

Further, since \( c_1, c_2 \in V(\Gamma^*) \) and \( \phi \) is a retraction with \( \phi |_{\Gamma^*} = 1_{\text{Aut}(\Gamma^*)} \), \( \phi(c_1) = c_1 \) and \( \phi(c_2) = c_2 \). Hence

\[
\eta_1\eta_2(0_G) = \eta_1(\rho_{c_2}(0_G)) = \phi(\rho_{c_1}\rho_{c_2}(0_G)) = \phi(c_1 + c_2)
\]

and

\[
\eta_2\eta_1(0_G) = \eta_2(\rho_{c_1}(0_G)) = \phi(\rho_{c_2}\rho_{c_1}(0_G)) = \phi(c_1 + c_2).
\]

(v) If \( \langle A(\phi, \Gamma, \Gamma^*) \rangle \) is semiregular on \( V(\Gamma^*) \), then by (iii) it must be regular on \( V(\Gamma^*) \). Therefore, there is exactly one element of \( \langle A(\phi, \Gamma, \Gamma^*) \rangle \) which maps \( 0_G \) to \( \phi(c_1 + c_2) \). So by (iv), for all \( c_1, c_2 \in C \) with \( c_1 \neq c_2 \), if \( \eta_1 = (\phi \circ \rho_{c_1}) |_{\Gamma^*} \) and \( \eta_2 = (\phi \circ \rho_{c_2}) |_{\Gamma^*} \), then \( \eta_1\eta_2 = \eta_2\eta_1 \). So \( \langle A(\phi, \Gamma, \Gamma^*) \rangle \) is abelian. \( \Box \)

Note: \( \langle A(\phi, \Gamma, \Gamma^*) \rangle \) is not necessarily faithful in its action on \( V(\Gamma^*) \).

If \( \Gamma \) is a Cayley graph of an abelian group, then Lemma 7.1.1 provides a considerable amount of information on the structure of \( \text{Aut}(\Gamma^*) \). Further, Lemma 7.1.1 provides information on the structure of \( \Gamma^* \) itself.

**Theorem 7.1.2** Let \( \Gamma = \text{Cay}(G, S) \) be a connected, undirected Cayley graph with \( G \) an abelian group. Then \( \Gamma^* \) is either an odd cycle, \( K_2 \), or \( \text{girth}(\Gamma^*) \leq 4 \)

**Proof** If \( \Gamma^* \) is not an odd cycle or \( K_2 \), then \( \text{val}(\Gamma^*) \geq 3 \) and \( |C| \geq 3 \). By Lemma 7.1.1, for \( u \in V(\Gamma^*) \), \( N_{\Gamma^*}(u) = \{((\phi \circ \rho_c) |_{\Gamma^*})(u) | c \in C \} \). Thus, for \( c_1 \in C \) and
\( \eta_1 = (\phi \circ \rho_{c_1}) \mid_{\Gamma^*} \), there exists some \( c_2 \in C \) and \( \eta_2 = (\phi \circ \rho_{c_2}) \mid_{\Gamma^*} \), where \( c_2 \neq c_1, -c_1 \), and
\[
\eta_2(c_1) = \eta_2\eta_1(0_G) = \phi(c_1 + c_2) \neq \phi(0_G).
\]
Further, by Lemma 7.1.1,
\[
\eta_2\eta_1(0_G) = \eta_1\eta_2(0_G) = \phi(c_1 + c_2),
\]
and
\[
[0_G, c_1], [c_1, \phi(c_1 + c_2)], [0_G, c_2], [c_2, \phi(c_1 + c_2)] \in E(\Gamma^*).
\]
Hence, \( 0_G, c_1, \phi(c_1 + c_2), c_2 \in V(\Gamma^*) \) is a cycle of length 4.

Lemma 7.1.1 and Theorem 7.1.2 are the first tools specifically designed to study the cores of Cayley graphs of abelian groups. If \( G \) is an abelian group and \( \Gamma = \text{Cay}(G, S) \), then these results are particularly useful for proving the nonexistence of a retraction from \( \Gamma \) to a given core \( \Psi \), based on either \( \text{girth}(\Psi) \) or the semiregular elements of \( \text{Aut}(\Psi) \).

Unfortunately, applicable general results on the semiregular automorphisms of vertex-transitive graphs do not exist. An open question posed independently by Marušić and Jordan [42,53] asks whether every vertex-transitive graph has a semiregular automorphism; this problem remains unresolved. However, if a vertex-transitive graph with no semiregular automorphisms does exist, then by Lemma 7.1.1 it is not the core of a Cayley graph of an abelian group.

So we focus instead on vertex-transitive graphs with large girth. The symmetric graphs of valency three form an infinite family of graphs, all but three of which have girth greater than four [57].

**Corollary 7.1.3** Let \( \Gamma = \text{Cay}(G, S) \) be a connected, undirected, nonbipartite Cayley graph with \( G \) an abelian group. Assume \( \text{val}(\Gamma^*) = 3 \). Then either \( \Gamma^* \cong K_4 \) or \( \Gamma^* \) is not symmetric.

**Proof** By Theorem 7.1.2, \( \Gamma^* \) is either an odd cycle, \( K_2 \), or \( \text{girth}(\Gamma^*) \leq 4 \). So let \( \Gamma^* \) be a symmetric graph with \( \text{val}(\Gamma^*) = 3 \) and \( \text{girth}(\Gamma^*) \leq 4 \). By [57], either \( \Gamma^* \cong K_4 \), \( \Gamma^* \cong K_{3,3} \), or \( \Gamma^* \cong Q_3 \) (the cube). Both \( K_{3,3} \) and \( Q_3 \) are bipartite, so \( K_{3,3}^* \cong K_2 \) and \( Q_3^* \cong K_2 \). Therefore, \( \Gamma^* \cong K_4 \). \( \square \)
Corollary 7.1.4 Let $\Gamma = \text{Cay}(G, S)$ be a connected, undirected, symmetric, nonbipartite Cayley graph with $G$ an abelian group. If $\text{val}(\Gamma) = 6$, then either $\Gamma \cong \Gamma^*$, $\Gamma^* \cong K_4$ or $\Gamma^* \cong C_n$ for odd $n$. If $\text{val}(\Gamma) = 9$, then either $\Gamma \cong \Gamma^*$, or $\Gamma^* \cong K_4$.

Proof By Theorems 2.3.21 and 2.3.23, $\Gamma^*$ is symmetric with $\text{val}(\Gamma^*) | \text{val}(\Gamma)$. So if $\text{val}(\Gamma) = 6$, then $\text{val}(\Gamma^*) = 2, 3$ or $6$. If $\text{val}(\Gamma^*) = 6$, then $\Gamma \cong \Gamma^*$; if $\text{val}(\Gamma^*) = 3$, then by Corollary 7.1.3, $\Gamma^* \cong K_4$; and if $\text{val}(\Gamma^*) = 2$, then $\Gamma^* \cong C_n$ for odd $n$.

If $\text{val}(\Gamma) = 9$, then $\text{val}(\Gamma^*) = 3$ or $9$. So if $\text{val}(\Gamma^*) = 9$, then $\Gamma \cong \Gamma^*$; if $\text{val}(\Gamma^*) = 3$, then by Corollary 7.1.3, $\Gamma^* \cong K_4$. \hfill $\square$

By [23, Lemma 4.1.3], for an $s$-arc-transitive graph $\Psi$, $\text{girth}(\Psi) \geq 2s - 2$. Further, by [23, Lemma 4.1.4], if $\text{girth}(\Psi) = 2s - 2$, then $\Psi$ is bipartite.

Corollary 7.1.5 Let $\Gamma = \text{Cay}(G, S)$ be a connected, undirected, nonbipartite Cayley graph with $G$ an abelian group. Then either $\Gamma^*$ is an odd cycle with $|V(\Gamma^*)| \geq 5$, or $\Gamma^*$ is not 3-arc-transitive.

Proof Let $\Gamma^*$ be a 3-arc-transitive graph. By [23, Lemma 4.1.3], $\text{girth}(\Gamma^*) \geq 4$. If $\text{girth}(\Gamma^*) = 4$, then $\Gamma^*$ is bipartite, and $\Gamma^* \cong K_2$. So $\text{girth}(\Gamma^*) > 4$, and by Theorem 7.1.2, $\Gamma^*$ is an odd cycle with $|V(\Gamma^*)| \geq 5$. \hfill $\square$

7.2 Primitive cores with prime power order

7.2.1 Primitive groups of prime power degree

We now turn our attention to Cayley graphs of abelian groups whose cores are primitive graphs of prime power order. So let $\Gamma = \text{Cay}(G, S)$, where $G$ is an abelian group. If $\text{Aut}(\Gamma^*)$ is primitive in its action on $V(\Gamma^*)$, then the O’Nan-Scott Theorem, which details the structure of all primitive permutation groups, also details the structure of $\Gamma^*$.

So in Section 7.2.1, we give the O’Nan-Scott Theorem for primitive permutation groups of prime power degree (see [49]). For the more general version of the O’Nan-Scott Theorem, we refer the reader to [13, Chapter 4] or [60, Section 6].
Let $X$ be a primitive permutation group acting on $\Omega$, with degree $p^n$ (where $p$ is prime), and let $N$ be the minimal normal subgroup of $X$. Then $N \cong T^l$, where $T$ is a finite simple group and $l \geq 1$. Also, since $X$ is primitive on $\Omega$, $X$ is transitive on $\Omega$ and has no nontrivial blocks. But by Lemma 2.1.4, the orbits of $N$ must be blocks of $\Omega$, so $N$ must also be transitive on $\Omega$.

We now give three examples of primitive groups, one with $T$ abelian and the other two with $T$ nonabelian.

**Example 7.2.1** Let $T$ be abelian and $\alpha \in \Omega$. Then $T \cong \mathbb{Z}_p$ and $N \cong \mathbb{Z}_p^l$. In this case $X = N \rtimes X_\alpha$ with $N$ regular on $\Omega$ and $X_\alpha$ an irreducible subgroup of $\text{GL}(l, p)$. $X$ is then said to be of affine type since $\mathbb{Z}_p^l \triangleleft X \leq \text{AGL}(l, p)$, where $\text{AGL}(l, p)$ is the affine group.

**Example 7.2.2** Let $T$ be nonabelian, with $l = 1$ and $\alpha \in \Omega$. Then $X = T \rtimes X_\alpha$, with $T \not\leq X_\alpha$ and $X_\alpha$ maximal in $X$. In this case $T \leq X \leq \text{Aut}(X)$, so $X$ is said to be of almost simple type.

**Example 7.2.3** Let $T$ be nonabelian, with $l \geq 2$. Then $K$ is a primitive, almost simple group (with $T \leq K$) acting on set $\Delta$, $H$ is a finite group acting transitively on $\Xi = \{1, 2, \ldots, l\}$, and $X = K \wr \Xi H$ is the wreath product acting via the product action on $\Omega = \Delta^l$ (see Example 2.1.6). By Lemma 2.1.7, $X$ is primitive, and is said to be of product action type.

In order to explicitly state all almost simple and product action permutation groups of prime power degree, we need to know which nonabelian simple groups contain a subgroup of prime power index.

**Theorem 7.2.4** ([28]) Let $T$ be a nonabelian simple group that has a subgroup $H$ of index $p^r$ with $p$ prime. Then one of the following holds:

(i) $T \cong \text{Alt}(p^r)$, and $H \cong \text{Alt}(p^{r-1})$;

(ii) $T \cong \text{PSL}(d, q)$, $H$ is a maximal subgroup of $T$, and $p^r = \frac{q^d-1}{q-1}$;

(iii) $T \cong \text{PSL}(2, 11)$, $H \cong \text{Alt}(5)$ and $p^r = 11$;

(iv) $T \cong M_{11}$, $H \cong M_{10}$ and $p^r = 11$.
(v) $T \cong M_{23}$, $H \cong M_{22}$ and $p^r = 23$; or

(vi) $T \cong \text{PSU}(4,2)$, $H \cong \mathbb{Z}_4 \rtimes \text{Alt}(5)$ and $p^r = 27$.

**Corollary 7.2.5** ([28]) Let $T$ be a nonabelian simple group acting transitively on $\Omega$ with $|\Omega| = p^n$, where $p$ is a prime. Then $T$ acts 2-transitively on $\Omega$ unless $T = \text{PSU}(4,2)$ and $|\Omega| = 27$, in which case $T$ acts as a rank 3 primitive permutation group and $T_\alpha$ has orbits of size 1, 10 and 16.

We now state the O’Nan-Scott Theorem, which classifies all primitive groups of prime power degree.

**Theorem 7.2.6** ([49]) Let $X$ be a primitive permutation group on $\Omega$ of degree $p^n$ with $p$ a prime, and let $N$ be a minimal normal subgroup of $X$. Then one of the following holds:

(i) $X$ is an affine group, $N = \mathbb{Z}_p^l$, and $G \leq AGL(l, p)$, where $l \geq 1$;

(ii) $X$ is an almost simple group; in particular, $G$ is either 2-transitive, or $G = \text{PSU}(4,2)$ or $\text{PSU}(4,2) \rtimes \mathbb{Z}_2$; or

(iii) $X$ is of product action type, $N = T^l$ with $l \geq 2$, and $T$ lies in the list of Theorem 7.2.4.

### 7.2.2 Cayley graphs of abelian groups with primitive cores of prime power order

By Theorem 7.2.6, if $\Gamma$ is a Cayley graph of an abelian group with $\Gamma^*$ a primitive graph of order $p^n$ for prime $p \neq 3$, then either;

(i) $\text{Aut}(\Gamma^*)$ is an affine group, and contains a regular elementary abelian subgroup;

(ii) $\text{Aut}(\Gamma^*)$ is 2-transitive on $V(\Gamma^*)$, and $\Gamma^*$ is complete; or

(iii) $\text{Aut}(\Gamma^*)$ is of product action type.

We show that in (iii), $\text{Aut}(\Gamma^*)$ contains a regular elementary abelian subgroup.
Theorem 7.2.7 Let \( \Gamma = \text{Cay}(G,S) \) be a connected, undirected Cayley graph with \( G \) an abelian group. If \( \text{Aut}(\Gamma^*) \) is a primitive group in its action on \( V(\Gamma^*) \), and if \( \Gamma^* \) has order \( p^n \) for prime \( p \neq 3 \), then either \( \Gamma^* \) is complete, \( \text{Aut}(\Gamma^*) \) is of affine type or \( \text{Aut}(\Gamma^*) \) is of product action type with regular elementary abelian subgroup.

Proof Let \( N \leq \text{Aut}(\Gamma^*) \) be the minimal normal subgroup of \( \text{Aut}(\Gamma^*) \). If \( \text{Aut}(\Gamma^*) \) is of almost simple type, then by Corollary 7.2.5, \( \text{Aut}(\Gamma^*) \) is 2-transitive, and thus \( \Gamma^* \) is a complete graph.

If \( \text{Aut}(\Gamma^*) \) is of product action type, then \( N = T^l \leq \text{Aut}(\Gamma^*) \), where \( T \) is a simple group acting on \( \Delta \) as outlined in Theorem 7.2.6, and \( V(\Gamma^*) = \Delta^l \). By Corollary 7.2.5, \( T \) is 2-transitive on \( \Delta \). So let \( G \) be a regular elementary abelian group acting on \( \Delta \), and \( \lambda \in G \). Then for each pair \( x,y \in \Delta \) with \( x \neq y \), there exists some \( t \in T \) such that \( \{t(x),t(y)\} = \{\lambda(x),\lambda(y)\} \).

Thus for any edge \([u,v] \in E(\Gamma^*)\) with \( u = (u_1,u_2,\ldots,u_l) \), \( v = (v_1,v_2,\ldots,v_l) \) and permutation \( \gamma = (\gamma_1,\gamma_2,\ldots,\gamma_l) \in G^l \) acting on \( V(\Gamma^*) = \Delta^l \) via the product action, there exists some \( n = (n_1,n_2,\ldots,n_l) \in N \cong T^l \) with \( \{n_i(u_i),n_i(v_i)\} = \{\gamma_i(u_i),\gamma_i(v_i)\} \) for each \( 1 \leq i \leq l \). Therefore,

\[
\gamma([u,v]) = [\gamma(u),\gamma(v)] \\
= [(\gamma_1(u_1),\gamma_2(u_2),\ldots,\gamma_l(u_l)),(\gamma_1(v_1),\gamma_2(v_2),\ldots,\gamma_l(v_l))] \\
= [(n_1(u_1),n_2(u_2),\ldots,n_l(u_l)),(n_1(v_1),n_2(v_2),\ldots,n_l(v_l))] \\
= [n([u,v]) \in E(\Gamma^*)].
\]

Hence, \( G^l \) is an elementary abelian subgroup of \( \text{Aut}(\Gamma^*) \) acting regularly on \( V(\Gamma^*) \). So by Theorem 2.2.10, \( \Gamma^* \) is a Cayley graph of an elementary abelian group.

Corollary 7.2.8 Let \( \Gamma = \text{Cay}(G,S) \) be a connected, undirected graph with \( G \cong \mathbb{Z}_p^n \) (where \( p \neq 3 \) is prime) and \( \text{Aut}(\Gamma^*) \) primitive in its action on \( V(\Gamma^*) \). Then \( \Gamma^* \) is a Cayley graph of the group \( H \cong \mathbb{Z}_p^m \), where \( 1 \leq m \leq n \).

Proof By Theorem 2.3.22, \( |V(\Gamma^*)| \) divides \( |V(\Gamma)| \), such that \( |V(\Gamma^*)| = p^m \). By Lemma 2.3.25, \( \text{Aut}(\Gamma^*) \) is primitive on \( V(\Gamma^*) \). The result then follows from Theorem 7.2.7.
Chapter 8

Conclusions

8.1 Summary of thesis

This thesis presents the first step towards the determination of the cores of all symmetric graphs whose order is the product of two primes (Problem 1.2.1). Specifically, we prove Theorem 4.1.2, which gives the cores of all imprimitive symmetric graphs of order $pq$, with $p$ and $q$ prime. The proof of Theorem 4.1.2 utilises the classification of all imprimitive symmetric graphs of order $pq$ provided in [10, 61, 81], in order to split the imprimitive symmetric graphs of order $pq$ into three subclasses, namely the circulants, incidence graphs and the Marušić-Scapellato graphs. Thus, the cores of these graphs are determined in Section 4.3, Chapter 5 and Chapter 6 respectively.

This thesis also presents generalisations of the techniques developed in the proof of Theorem 4.1.2, and applies these techniques to all Cayley graphs of abelian groups (Research Direction 1.2.2). In Section 7.1, the proof of Lemma 5.3.4 is generalised to all Cayley graphs of abelian groups. This generalisation yields Lemma 7.1.1, which shows that if $\Gamma$ is Cayley graph of an abelian group, then $\Gamma^*$ has a transitive group of automorphisms generated by semiregular elements. Using Lemma 7.1.1 we prove Theorem 7.1.2, which shows that $\text{girth}(\Gamma^*) \leq 4$ whenever $\Gamma^*$ is not an odd cycle. Then from Theorem 7.1.2, we prove Corollaries 7.1.3 and 7.1.5, which determine $\Gamma^*$ when $\Gamma$ is nonbipartite, and $\Gamma^*$ is either a cubic symmetric graph or a 3-arc-transitive graph.

Finally, in Section 7.2 we investigate Cayley graphs of abelian groups with prim-
itive cores. This investigation culminates in Theorem 7.2.7, which states that if $\Gamma$ is a Cayley graph of an abelian group, and $\Gamma^*$ is a primitive graph with $|V(\Gamma^*)| = p^n$ for prime $p \neq 3$, then $\Gamma^*$ is a Cayley graph of an elementary abelian group. From Theorem 7.2.7 we obtain Corollary 7.2.8, which states that if $\Gamma$ is a primitive Cayley graph of an elementary abelian group (with $p \neq 3$), then $\Gamma^*$ is a primitive Cayley graph of an elementary abelian group (with $p \neq 3$). Therefore Corollary 7.2.8 confirms Conjecture 1.2.3, for all primitive Cayley graphs of elementary abelian groups with $p \neq 3$.

\section*{8.2 Future work}

\subsection*{8.2.1 Symmetric graphs of orders $pq$, $p^2$ and $p^3$}

Theorems 4.1.2, 7.2.7 and Lemma 7.1.1, along with the various approaches used to prove these results, suggest many possibilities for future work in studying cores of vertex-transitive graphs. The first possibility is to complete Problem 1.2.1, since Theorem 4.1.2 provides only a partial solution to Problem 1.2.1.

\begin{problem}
Determine the cores of all primitive, symmetric graphs whose order is the product of two primes.
\end{problem}

As in the imprimitive case, all primitive symmetric graphs of order $pq$ are classified [62]. This classification splits the graphs into four subcases, namely the rank three graphs, the sporadic graphs and the graphs $\Gamma$ with either $\text{PSL}(2, p^2)$ or $\text{PSL}(2, q)$ the minimal normal subgroup of $\text{Aut}(\Gamma)$.

From [7], all rank three graphs are either cores, or have complete cores. From this result, [7] explicitly states the cores of all rank three graphs of order $pq$. Whilst for the sporadic primitive symmetric graphs of order $pq$, [62] states that all of these graphs have small orders, and this means that it is feasible to determine their cores computationally. Thus to solve Problem 8.2.1, we must determine the cores of the symmetric graphs with minimal normal subgroups isomorphic to either $\text{PSL}(2, p^2)$ or $\text{PSL}(2, q)$.

The success of Theorem 4.1.2, along with the feasibility of Problem 8.2.1, motivates us to determine the cores of all symmetric graphs of a given order $n$, where $n$
has a small number of prime factors. (Note: restricting $n$ to prime powers allows the use of Theorem 7.2.7, and thus is more promising than if $n$ is not a prime power.)

**Problem 8.2.2** Determine the cores of all symmetric graphs of order $p^2$, $p^3$.

In [51], Marušić shows that all vertex-transitive graphs of orders $p^2$ are either circulants, or Cayley graphs of elementary abelian groups. Fortunately, symmetric circulants are classified in [44], whilst Dobson states the automorphism groups of Cayley graphs of $\mathbb{Z}_p^2$ in [16]. Thus Problem 8.2.2 is feasible for symmetric graphs of order $p^2$.

Unfortunately, Problem 8.2.2 for graphs of order $p^3$ is challenging, since no complete classification exists for the symmetric graphs of order $p^3$. Thus, a more realistic approach is to determine the cores of all symmetric circulants of order $p^3$ (which were classified in [44]) and Cayley graphs of $\mathbb{Z}_p^3$ (whose automorphism groups are given in [15]).

### 8.2.2 Cayley graphs of abelian groups

Corollary 7.2.8 confirms Conjecture 1.2.3 for all primitive Cayley graphs of abelian $p$-groups (with $p \neq 3$ prime). However when $p = 3$, Conjecture 1.2.3 for primitive graphs remains unsolved.

**Conjecture 8.2.3** Let $\Gamma$ be a primitive Cayley graph of an abelian 3-group. Then $\Gamma^*$ is a Cayley graph of an abelian 3-group.

By Lemma 2.3.25, if $\Gamma$ is primitive then so is $\Gamma^*$. Thus by Corollary 7.2.5 and Theorem 7.2.6, if $\Gamma$ is a counterexample to Conjecture 8.2.3, then $\text{Aut}(\Gamma^*)$ will either be almost simple with minimal normal subgroup $\text{PSU}(4, 2)$, or be of product action type with minimal normal subgroup $\text{PSU}(4, 2)^l$ for $l \geq 2$.

The O’Nan-Scott Theorem (Theorem 7.2.6) classifying all primitive groups of prime power degree, along with the classification of all primitive groups with a regular abelian subgroup [47], provide a lot of information about primitive symmetric Cayley graphs of elementary abelian groups. Thus using Corollary 7.2.8, explicitly determining the cores of primitive symmetric Cayley graphs of elementary abelian groups seems feasible.
Problem 8.2.4 Determine the cores of all primitive, symmetric Cayley graphs of elementary abelian groups.

The symmetric circulant graphs were classified in [44]. Using this classification, Lemma 7.1.1 and the classifications of symmetric graphs of orders $p$ and $pq$ for primes $p < q$ [8, 10, 61, 62, 81], finding the cores of all symmetric circulants of order $pqr$ seems achievable.

Problem 8.2.5 Determine the cores of all symmetric circulants of order $pqr$ for primes $p < q < r$.

If Problems 8.2.2 and 8.2.5 can be resolved, then we might be able to find the cores of all symmetric circulants.

Problem 8.2.6 Determine the cores of all symmetric circulants.
Bibliography


Minerva Access is the Institutional Repository of The University of Melbourne

Author/s:
Rotheram, Ricky

Title:
Cores of vertex-transitive graphs

Date:
2013

Citation:

Persistent Link:
http://hdl.handle.net/11343/39734

File Description:
Cores of vertex-transitive graphs

Terms and Conditions:
Terms and Conditions: Copyright in works deposited in Minerva Access is retained by the copyright owner. The work may not be altered without permission from the copyright owner. Readers may only download, print and save electronic copies of whole works for their own personal non-commercial use. Any use that exceeds these limits requires permission from the copyright owner. Attribution is essential when quoting or paraphrasing from these works.