ISOMORPHISMS OF CAYLEY GRAPHS

by

Joy Morris

B.Sc.(Hon.), Trent University, 1992

Thesis submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

in the Department of

Mathematics and Statistics

©Joy Morris 1999
Simon Fraser University
November 1999

All rights reserved. This work may not be reproduced in whole or in part, by photocopy or other means, without permission of the author.
The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author’s permission.

L’auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L’auteur conserve la propriété du droit d’auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.
Abstract

The Cayley Isomorphism problem is a much-studied problem in algebraic graph theory. A group is a CI-group if for any two isomorphic Cayley graphs on that group, there is an automorphism of the group that maps one to the other. A (directed) graph is a CI-(di)graph on the group $G$ if for any two representations of that (di)graph as a Cayley (di)graph on the group $G$, there is an automorphism of $G$ that maps one of these representations to the other.

It was previously known that $\mathbb{Z}_4$ is a CI-group; this thesis provides an elementary proof of this result, which it is hoped may lead to results on $\mathbb{Z}_5$, thus resolving current uncertainty (the group $\mathbb{Z}_2^6$ is known not to be a CI-group). The thesis also proves the truth of a long-standing conjecture by Toida: If $\bar{X} = \bar{X}(\mathbb{Z}_n; S)$ is a Cayley digraph on a cyclic group $\mathbb{Z}_n$ with symbol set $S$ containing only units (modulo $n$), then $\bar{X}$ is a CI-digraph on $\mathbb{Z}_n$.

Finally, a natural extension of the Cayley Isomorphism problem is considered. The question of when a Cayley digraph $\bar{X} = \bar{X}(\mathbb{Z}_{p^n}; S)$ can be represented as a Cayley digraph on some other group of order $p^n$ is fully resolved, where $p$ is an odd prime.
Acknowledgements

Logic can be patient, for it is eternal.
Oliver Heaviside

Thanks to all those in whose footsteps I have followed along the way where logic is patiently leading us. In particular, my thanks are due to several people who have worked with me, sharing with me their own methods and ways of approaching mathematical problems. Ted Dobson of Mississippi State University, my coauthor for the results in Chapter 3 of this thesis, taught me a lot about techniques that were not intuitive to me. Dave Witte of Oklahoma State University was endlessly patient at explaining and helping out with the algebraic side of things when I ran into difficulties. My supervisor Brian Alspach brought two of these problems to my attention and suggested some techniques that proved very useful. Thanks also to Cai Heng Li of the University of Western Australia, who worked with me briefly on a different approach to the main result in Chapter 3 of this thesis. Although the method did not work out in this case, the techniques that he showed me have enhanced my understanding of these problems. Thanks to Peter Cameron of Queen Mary and Westfield College, University of London, who responded promptly when e-mailed by a graduate student desperate to finish her thesis! I must also thank my brother Douglas, who taught me the joys of truly understanding mathematics, rather than simply memorising.

Thanks to everyone whose patience with me gave me the room to be a whole person, and to accomplish things that are important to me, even if they didn’t relate
directly to my thesis. You helped me to be a better, more well-rounded individual, by not stifling me within a mold made for single-minded graduate students. The particular thanks here go again to my supervisor, and to Kathy Heinrich, Bruce Clayman, Jack Blaney and those other members of the administration at SFU who greeted my presence on so many committees with nothing worse than occasional gentle reminders about my thesis. However, thanks are also due to those of my friends and family who made sure that I ate and slept at the times when I was being single-minded, too deeply engrossed in some aspect of my thesis to take much heed of the outside world.

Thanks to the Natural Sciences and Engineering Research Council of Canada (NSERC), the Department of Mathematics and Statistics, and my supervisor for providing sufficient financial support that I did not have to rush through my thesis with a rapidly-growing debt load, as has become all too common for many graduate students.

In everything that I do, I am grateful to my friends and family for their unwaivering, unquestioning love and support that uplifts and empowers me. Mom, Dad, Peter, Corinne, Richard, Owen, Pippa and Douglas - this is for you. Thanks.

Finally, I would like to thank my fellow members of the Canadian Federation of Students, at the local, provincial and national levels, who taught me, learned from me, and stood by my side in the struggle to ensure that everyone can have access to the opportunities with which I have been blessed.
# Contents

Preliminaries ..............................................  ii  
  Approval ..................................................  ii  
  Abstract ...................................................  iii  
  Acknowledgements ......................................... iv  
  Contents ................................................... vi  

1 Introduction ...............................................  1  
  1.1 Plain English ...........................................  1  
  1.2 Background Definitions and Theory .....................  6  
    1.2.1 Graph Theory .......................................  6  
    1.2.2 Abstract Group Theory ............................... 10  
    1.2.3 Permutation Group Theory ............................ 14  
    1.2.4 Algebraic Graph Theory ............................... 20  
  1.3 History of the Cayley Isomorphism Problem ............. 23  

2 $\mathbb{Z}_p^4$ is a CI-group .............................. 26  
  2.1 History of the Problem ................................... 26  
  2.2 Background Definitions and Theory ..................... 27  
  2.3 Main Theorem ............................................ 32  
  2.4 The Action of Elements of $\sigma(\mathbb{Z}_p^4)L\sigma^{-1}$ 33  
  2.5 Conjugation of $\sigma(\mathbb{Z}_p^4)L\sigma^{-1}$ to Obtain a Group that Contains $\tau_3$ 34  
    2.5.1 Finding the conjugate $g\sigma(\mathbb{Z}_p^4)L\sigma^{-1}g^{-1}$ 34  
    2.5.2 Orbits of $G$ when $\tau'_3 \neq \tau_3$ ............... 39
2.6 Conjugation of $\sigma(Z^*_p)L\sigma^{-1}$ to Obtain a Group that Contains $\tau_2$ ........ 46
  2.6.1 Finding the conjugate $\phi\sigma(Z^*_p)L\sigma^{-1}\phi^{-1}$ ................. 46
  2.6.2 Orbits of $G$ when $\tau'_2 \neq \tau_2$ ........................................ 56
2.7 Conjugation of $\sigma(Z^*_p)L\sigma^{-1}$ to Obtain a Group that Contains $\tau_1$ ........ 76
  2.7.1 Finding the conjugate $\psi\sigma(Z^*_p)L\sigma^{-1}\psi^{-1}$ ................. 76
  2.7.2 Orbits of $G$ when $\tau'_1 \neq \tau_1$ ........................................ 79

3 Toida’s Conjecture is True ......................................................... 82
  3.1 History of the Problem .......................................................... 82
  3.2 Background Definitions and Theory ........................................... 82
  3.3 Main Theorem ........................................................................... 88
  3.4 Finding Blocks ........................................................................... 95
  3.5 Wreath Products ........................................................................ 95
  3.6 Not Wreath Products ................................................................... 107
    3.6.1 General Results ....................................................................... 107
    3.6.2 Results Dealing with $\text{PSL}(d, q)$ ........................................ 109
    3.6.3 Results dealing with $A_n$ and $S_n$ ....................................... 114

4 Isomorphic Cayley Graphs on Nonisomorphic Groups .......................... 116
  4.1 Preliminaries ............................................................................. 116
  4.2 Proof of $3 \Rightarrow 1, 4$ ........................................................... 120
  4.3 Proof of $2 \Rightarrow 3$ .................................................................. 122
  4.4 Proof of $1 \Rightarrow 2$ ................................................................. 123
  4.5 What happens if $p = 2$? ............................................................ 134
  4.6 Non-abelian groups ....................................................................... 136
  4.7 Further extensions ....................................................................... 137

Epilogue ......................................................................................... 139

Bibliography .................................................................................. 140
Chapter 1

Introduction

1.1 Plain English

The soul of immensity dwells in minutia
And in narrowest limits no limits inhere.

Jakob Bernoulli

I have been asked many times as a graduate student, "So, what is your thesis about?" At first, I found myself at a loss to respond. How, in five minutes or less, does one explain to a layperson concepts that are based on understanding that one has developed over the course of years? It took more years before I came to understand that the language that I had been learning over the course of my university education was a very complicated way of explaining ideas, some of which were not in themselves so complicated. The complexity of the language that had been developed was necessary for solving many problems in the field, and for generalising problems, but there was an essence to the problems that I study that could be explained in simple terms.

Here, then, is the section of my thesis that has been written for my friends, family, and other non-mathematicians. It contains the answers that I have developed to the questions of "What is your thesis about?" and "What use is that?" (The latter question is usually phrased more politely, as "What are the practical applications of that?" but the meaning is clear!)
A "graph." as the term is used in this thesis, is nothing more than a way of modelling a network. That can be a road network, a telephone network, a computer network, or any other sort of network. Think of a graph as an elaborate game of connect-the-dots - for each node (city/telephone/computer/whatever) in the network, we draw a dot, and when two nodes are directly connected (by a road/telephone line/cable/whatever), we draw a line between them.

Certain properties associated with networks are particularly important. I will give two examples of such properties. This will get a bit technical, but if you don’t understand, pass over it: these are nothing more than examples. A graph, or the network that it models, is disconnected if there is some node (city/telephone/computer) that cannot be reached from some other node (city/telephone/computer) by using the working connections (roads/telephone lines/cables, or lines in the graph). The connectivity of a network, or of the graph that models that network, is the number of connections (roads/telephone lines/cables, or lines in the graph) that have to be broken before the network becomes disconnected. The distance between two nodes in the network or graph is considered to be the minimum number of connections that must be used to get from one of the nodes to the other. The diameter of a network, or of the graph that models that network, is the greatest distance that exists between any two nodes in the network or graph.

It is not hard to realise that ideally, it would nice to have a very large connectivity. For the example of a telephone network, this simply means that it would be nice if a lot of telephone lines had to go down before two people would not be able to contact one another through some routing. It is equally clear that a small diameter is a good thing. In the same example, a connection will tend to lose clarity and also be more likely to occupy lines that other people may want to use, if it has to use up a lot of different lines along the way. If all that we had to consider were these two properties, then an ideal network would have a direct connection between every pair of nodes (direct telephone lines between every pair of telephones in the network, for example). However, there are trade-offs that must be made. It is pretty obvious that connections cost money to create - each road, line, or cable has
a cost associated with it. Networks that have a lot of symmetry seem to balance cost-efficiency against properties like connectivity and diameter fairly well, a vague statement for a mathematical work, but one that I shall not attempt to pin down more exactly. Suffice it to say that highly-symmetrical networks are very often used in practice when they are possible.

One of the simplest sorts of symmetry is rotational symmetry. All of the graphs in chapters 3 and 4 of this thesis have rotational symmetry. That means that there is a way of drawing the graph with the nodes equally spaced around a circle in such a way that we can rotate the entire figure clockwise by the distance between two nodes without changing the appearance of the figure. For example, a square (where the nodes are the corners and the lines are the edges) can be rotated by 90 degrees without changing its appearance. There are more complicated forms of symmetry, and some of the more complicated forms of symmetry are considered in chapters 2 and 4 of this thesis. A Cayley graph is a fancy name for a particular type of graph that has a high degree of symmetry.

By mentioning ways in which a graph can be drawn, I have already hinted at the next concept that I must introduce. Some networks may look different, but may actually for all intents and purposes be the same. The easiest way to see this may be by considering the example of a computer network, since computers are not fixed in space in the way that cities and wired-in telephones are. Suppose that there are five computers in a room, call them A, B, C, D and E, and that they are connected in a cyclic network - that is, there are cables between A and B, between B and C, between C and D, between D and E, and between E and A. If the computers are evenly spaced around a circle in the order A, B, C, D, E, then the natural way of drawing the graph that corresponds to this network will end up looking like a pentagon - a five-sided shape with the nodes, or computers, at the corners, and the cables forming the sides. But suppose that, without changing any of the cables around, the computers are moved around so that they are evenly spaced around a circle in the order A, C, E, B, D. Now the natural way of drawing the graph that corresponds to this network will end up looking like a pentagram - a drawing of
a five-pointed star, in which all of the lines go straight across between points. So the graph that looks like a pentagon and the graph that looks like a pentagram, although they look different, model the same network.

Whenever two graphs can be used to model the same network, for all intents and purposes these graphs might as well be the same. The mathematical term for this property is that the graphs are “isomorphic”. One means by which we can demonstrate that both graphs model the same network is by picking up the computers and moving them around appropriately, and this action is called an “isomorphism.” This thesis is primarily concerned with methods of determining when two graphs that have some specified symmetry are for all intents and purposes the same; in mathematical parlance, this thesis is concerned with determining when there is an isomorphism from one Cayley graph to another (hence the title).

More specifically, in Chapter 3 of this thesis I look at certain large families of graphs that have rotational symmetry, and determine every possible way of drawing those graphs while maintaining the rotational symmetry. The work in Chapters 2 and 4 is similar, but the types of symmetry involved are different, and the numbers of nodes permitted is more restricted in the results found in those chapters. In the case of the example from the paragraph before last, the pentagon, there are only two ways of drawing this graph while maintaining its rotational symmetry - as a pentagon or as a pentagram.

The results in this thesis actually allow for slightly more generality than I have described above. Instead of two-way connections between nodes, one-way connections can also be permitted. This allows for things like one-way roads in the network. However, requirements on the symmetry of the directions of connections in the graph must be met in this case if the results of this thesis are to apply. Similarly, colours can be assigned to different connections to indicate (for example) distances or terrain, but again there will be requirements on the symmetry of the colours in the graph if the results of this thesis are to apply.

Now to the second question - what use is this?

An example is the clearest form of demonstration. Suppose that a government,
telecommunications company, or computer company wishes to build a network. In the case of the computer company, they may wish to build a chip that will form a network connecting microprocessors or other pieces of hardware within a computer. Let us presume further that the organisation has a pretty clear idea of the sort of network that they would like to build - how many connections they can afford, and what diameter and connectivity they can tolerate. Suppose that they have managed to find one way of drawing a graph that models a network that will suit their requirements, but that they are not sure whether or not the way that they have found is ideal. If the graph that they have found is in one of the families considered in this thesis, then I will be able to provide them with a complete list of all possible ways of drawing that graph with the appropriate symmetry. From this list, they can find a model that best suits their needs.

Once again, let me be more specific in example. A computer company has decided that a pentagram will suit their needs for a chip in regard to connectivity, diameter and expense. Upon being told that a pentagon has the same numbers of connections, the same connectivity and the same diameter, they conclude that it is far more cost-efficient. After all, where the lines in the pentagram cross one another, the chip that is being designed would have to be built on multiple layers, with layers of insulation to prevent messages from jumping from one connection to another and being lost along the way. The pentagon, on the other hand, has no edges that cross one another, so could be built on a single layer.

Although this example is grossly oversimplified - it would not really require this thesis to realise that a pentagon would be a better design than a pentagram - networks with many connections are much more difficult to work out by trial and error.

The preceding is something of a glorification of the practicality of the results of this thesis. In practice, most network designs involve sufficiently few nodes that a computer could fairly quickly achieve the effect ascribed to this thesis for any specific example of a graph. However, the above serves to provide a general sense of one sort of application that the results of this thesis can have.
1.2 Background Definitions and Theory

Although the three problems considered in this thesis are quite diverse and will each require specialised definitions and notation, some language is common to all of the problems. We begin by introducing some of this general language of algebraic graph theory. The notation used in this thesis is something of a hodge-podge from a variety of sources, based sometimes on my personal preferences and sometimes on the need for consistency with earlier works. For any graph theory language that is not defined within this thesis, the reader is directed to [12]. In the case of language or notation relating to permutation groups, the reader is directed to Wielandt's authoritative work on permutation group theory [96], although not all of the notation used by Wielandt is the same as that employed in this thesis.

We will begin with some of the basics, and quickly work our way up to more complex concepts. Interspersed with the definitions will be some of the well-known basic results that are used within this thesis.

1.2.1 Graph Theory

Definition 1.2.1 A directed graph $\vec{X} = \vec{X}(V, A)$ is a collection of vertices $V = \{v_0, v_1, \ldots, v_n\}$ together with a set $A$ of ordered pairs of vertices. In the representation of the directed graph, we draw an arc from $v_i$ to $v_j$ if and only if the pair $(v_i, v_j)$ appears in $A$. The term "directed graph" is typically shortened to digraph. The pair $(v_i, v_j)$, if it appears in $A$, is called an arc of the digraph. If it does not appear in $A$, this pair is called a non-arc of the digraph.

A directed graph is a generalisation of a standard graph. In a standard graph, the set $A$ is denoted by $E$ and consists of unordered pairs, which are then represented by edges (undirected arcs) between the pairs in $E$. Many results for directed graphs have immediate analogues for graphs, as can be seen by substituting for a graph the directed graph obtained by replacing each edge of the graph with an arc in each direction between the two end vertices of the edge. Consequently, although the results of this thesis are proven to be true for all digraphs, the same proofs serve to
prove the results for all graphs.

Although for the sake of simplicity we assume in this thesis that directed graphs are simple (that is, \( A \) contains no pairs of the form \((v, v)\) that would form loops in the digraph, and \( A \), being a set, contains no ordered pair more than once, so there are no multiple arcs from any one fixed vertex to any other fixed vertex), neither of these assumptions is actually required in any of the proofs that follow. The degree of symmetry that is required on the digraphs within the assumptions is sufficient to prove the results for digraphs that are not simple. We do allow \( A \) to contain digons; that is, \( A \) may contain the pair \((u, v)\) even if it also contains the pair \((v, u)\).

We now define some of the basic terminology of graphs.

**Definition 1.2.2** In a graph, two vertices that appear as a pair in the set \( E \) of edges are said to be adjacent. The set of all vertices that are adjacent to some fixed vertex \( v \) are said to be the neighbours of \( v \). The set of all vertices that are adjacent to both the vertex \( v \) and the vertex \( u \) are called the mutual neighbours of \( u \) and \( v \).

If the arc \((u, v)\) is in the set \( A \), then we say that there is an arc from \( u \) to \( v \) in the digraph \( \vec{X} = \vec{X}(V, A) \).

**Definition 1.2.3** The order of a graph or a digraph is the cardinality of the set \( V \) of vertices.

**Definition 1.2.4** If the set \( A \) of arcs is empty, then the digraph \( \vec{X}(V, A) \) is called the trivial graph on \( n \) vertices (where \( n \) is the order of \( \vec{X} \)). It is denoted by \( E_n \).

**Definition 1.2.5** If \( V' \) is a subset of the set \( V \) of vertices of the digraph \( \vec{X} \), then the induced subdigraph of \( \vec{X} \) on the vertices of \( V' \) is defined to be the digraph \( \vec{X}'(V', A') \), where \( A' \) is the subset of \( A \) consisting of all directed pairs in \( A \) both of whose endpoints are in the set \( V' \). This induced subdigraph is generally denoted by \( \vec{X}[V'] \).
In other words, the induced subdigraph on the vertex set $V'$ consists of the vertices in $V'$ together with all arcs of $\tilde{X}$ that connect those vertices.

**Definition 1.2.6** A path in the graph $X$ is an ordered set of vertices, each of which is adjacent to the vertex that precedes it in the set (if any).

We now give some rather less basic definitions that are important to the results in this thesis.

**Definition 1.2.7** Two digraphs $\tilde{X} = \tilde{X}(V, A)$ and $\tilde{Y} = \tilde{Y}(V', A')$ are said to be isomorphic if there is a bijective mapping $\phi$ from the vertex set $V$ to the vertex set $V'$ such that $(u, v) \in A$ if and only if $(\phi(u), \phi(v)) \in A'$. The mapping $\phi$ is called an isomorphism. We denote the fact that $\tilde{X}$ and $\tilde{Y}$ are isomorphic by $\tilde{X} \cong \tilde{Y}$.

That is, an isomorphism between two digraphs is a bijection on the vertices that preserves arcs and non-arcs.

**Definition 1.2.8** An automorphism of the digraph $\tilde{X}$ is an isomorphism from $\tilde{X}$ to itself.

We sometimes refer to a mapping $\phi$ as being an automorphism within some induced subdigraph $\tilde{X}[V']$ of $\tilde{X}$. By this, we mean that it is a bijection on the vertices of $V'$, and that it preserves arcs and non-arcs within $\tilde{X}[V']$.

**Definition 1.2.9** The wreath product of two digraphs $\tilde{X}$ and $\tilde{Y}$, denoted by $\tilde{X} \wr \tilde{Y}$, is given as follows. The vertices of the new digraph are all pairs $(x, y)$ where $x$ is a vertex of $\tilde{X}$ and $y$ is a vertex of $\tilde{Y}$. The arcs of $\tilde{X} \wr \tilde{Y}$ are given by the pairs

$$\{((x_1, y_1), (x_1, y_2)) : (y_1, y_2) \text{ is an arc of } \tilde{Y}\},$$

together with

$$\{((x_1, y_1), (x_2, y_2)) : (x_1, x_2) \text{ is an arc of } \tilde{X}\}.$$

In other words, there is a copy of the digraph $\tilde{Y}$ for every vertex of $\tilde{X}$, and arcs exist from one copy of $\tilde{Y}$ to another if and only if there is an arc in the same direction.
between the corresponding vertices of $X$. If any arcs exist from one copy of $Y$ to another, then all arcs exist from that copy of $Y$ to the other.

The wreath product of digraphs is a far more natural concept than it might appear at first glance: it arises in all of the problems considered in this thesis. This concept will be considered in the fully generalised context of digraphs whose arcs have colours associated with them. In the context of digraphs whose arcs are not coloured, simply ignore all references to colour in this discussion.

The building blocks of the wreath product are sets of vertices each of whose cardinality is equal to the cardinality of the vertex set of $Y$. For any two of these sets, $V_1$ and $V_2$, if there is an arc of some colour (say red) from some vertex in $V_1$ to some vertex in $V_2$, then there is a red arc from each vertex of $V_1$ to each vertex of $V_2$. This gives rise to the following definition.

**Definition 1.2.10** Two sets of vertices $V_1$ and $V_2$ are said to be **wreathed** if for each possible colour $c$ that an arc can be, the existence of an arc of colour $c$ from some vertex in $V_1$ to some vertex in $V_2$ implies the existence of an arc of colour $c$ from each vertex of $V_1$ to each vertex of $V_2$, and furthermore if (symmetrically) the existence of an arc of colour $c$ from some vertex in $V_2$ to some vertex in $V_1$ implies the existence of an arc of colour $c$ from each vertex of $V_2$ to each vertex of $V_1$.

Sometimes we say (alternatively) that $V_1$ is wreathed with $V_2$ if the above conditions hold.

Another similar definition will appear later, once some additional terminology from permutation group theory has been defined.

**Definition 1.2.11** The digraph $X$ is said to be **reducible** with respect to $\mathcal{L}$ if there exists some digraph $Y$, such that $X$ is isomorphic to $Y \uparrow E_k$ for some $k > 1$.

If a digraph is not reducible with respect to $\mathcal{L}$, then it is said to be irreducible with respect to $\mathcal{L}$. 
1.2.2 Abstract Group Theory

Definition 1.2.12 A group $G = G(S, \times)$ is a set $S$ together with a binary operation $\times$ on $S$, where $\times$ has the following properties:

1. $S$ is closed under $\times$: that is, $s_1 \times s_2 \in S$ for any $s_1, s_2 \in S$;
2. $\times$ is associative: that is, $s_1 \times (s_2 \times s_3) = (s_1 \times s_2) \times s_3$ for any $s_1, s_2, s_3 \in S$;
3. $\times$ has a unique identity; that is, there exists $s_0 \in S$ such that $s_0 \times s = s \times s_0 = s$ for any $s \in S$ ($s_0$ is called the identity element of $G$); and
4. $\times$ has an inverse operation: that is, for any $s \in S$, there exists a unique $s' \in S$ such that $s \times s' = s' \times s = s_0$, where $s_0$ is the identity element of $G$.

Notice that a group does not have to be commutative (that is, there may exist $s_1, s_2 \in S$ such that $s_1 \times s_2 \neq s_2 \times s_1$). As is often done in standard arithmetic, we will generally abbreviate $s_1 \times s_2$ by $s_1 s_2$. The inverse element of $s \in S$, which was denoted above by $s'$, is generally denoted by $s^{-1}$. We generally eliminate $S$ from our notation and write $s \in G$ when we intend $s \in S$. We also generally denote the identity element $s_0$ by $1$.

Definition 1.2.13 A subgroup $G' = G'(S', \times)$ of $G = G(S, \times)$ is a subset of $G$ (that is, $S' \subseteq S$) that is itself a group with the same binary operation $\times$. Instead of writing that $G'$ is a subgroup of $G$, we denote this by $G' \leq G$.

Much like a subset, a subgroup is called proper if it is not the entire group. A subgroup is nontrivial if it is proper and is not the single-element subgroup $G'(1, \times)$, where $1$ is the identity element of $G$.

Definition 1.2.14 Let $g \in G$. The set $gG'$ consisting of all elements of the form $gg'$ where $g' \in G'$ is called a left coset of $G'$ in $G$. The number of distinct left cosets of $G'$ in $G$ (including $1G' = G'$) is called the index of the subgroup $G'$ in $G$. Right cosets are defined analogously.
Definition 1.2.15 Given a set of elements within some group $H$, the **group generated by this set of elements** is the smallest subgroup of $H$ that contains all of the elements in that set. We denote the group generated by the set $Y$ by $\langle Y \rangle$.

If the group $G$ is generated by the set $Y$, then we call $Y$ a generating set of $G$.

**Definition 1.2.16** The **order** of a group $G$ is the cardinality of the set $S$; that is, the cardinality of the set of elements of the group. The order of an element $g$ is the order of $\langle g \rangle$. The order of $G$ is denoted by $|G|$.

Within this thesis, all groups are assumed to have finite order.

**Definition 1.2.17** A group is **cyclic** if it can be generated by a single element; that is, if the group can be generated by a set of cardinality 1. We denote the cyclic group of order $n$ by $\mathbb{Z}_n$.

Notice that in the case of $\mathbb{Z}_4$, for example, where $\mathbb{Z}_4 = \langle g \rangle$, the group generated by $g^2$ satisfies $\langle g^2 \rangle = \{1, g^2\} \neq \mathbb{Z}_4$. This leads to the following definition.

**Definition 1.2.18** The element $g$ is a **unit** of $\mathbb{Z}_n$ if $\langle g \rangle = \mathbb{Z}_n$. We denote the set of all units of $\mathbb{Z}_n$ by $\mathbb{Z}_n^*$.

A closely related and simple result is the following. The proof is left to the reader.

**Theorem 1.2.19** The cyclic group $\mathbb{Z}_n$ has unique subgroups of order $d$ for every $d$ such that $d$ divides $n$.

Recall that, in the definition of a group, there is no requirement that elements commute. There do exist some groups $G$ for which it is possible to have $g, g' \in G$ such that $gg' \neq g'g$.

**Definition 1.2.20** Let $g, g' \in G$. If $gg' = g'g$ then we say that $g$ and $g'$ **commute**. If every pair of elements in $G$ commute, then we say that the group $G$ is **abelian**.
Sometimes, even if a group is not abelian, it is useful to know which elements do commute with one another.

**Definition 1.2.21** The center of the group $G$ is the subset of all $y \in G$ such that $y$ commutes with $g$ for every $g \in G$.

It is not hard to see that the identity element of $G$ is always in the center of $G$, and that when $G$ is abelian, the center of $G$ is $G$ itself. In fact, the center of $G$ is always a subgroup of $G$.

**Definition 1.2.22** The centraliser of a set $Y$ of elements of $G$ is the subset of all $g \in G$ such that $g$ commutes with every element of $Y$.

Clearly, if $Y$ is the center of $G$, then $G$ is the centraliser of $Y$. Sometimes, rather than saying that $G$ is the centraliser of $Y$, we say that $G$ centralises $Y$.

It is often of interest to study what complications can arise if we are working in a group that is not abelian. In the case of an abelian group $G$, if $g, g' \in G$, then $gg'g^{-1} = g'$. This is not true in a group that is not abelian; that is, there exist elements $g$ and $g'$ which do not commute.

**Definition 1.2.23** Let $g, g' \in G$. Then $gg'g^{-1}$ is the conjugate of $g'$ by $g$. Similarly, if $Y \subseteq G$, then $gYg^{-1}$ is the conjugate of $Y$ by $g$, where $gYg^{-1}$ denotes the set of all $gyg^{-1}$ satisfying $y \in Y$. We say that the sets $Y$ and $gYg^{-1}$ are conjugate to each other in $G$. The mapping taking $Y$ to $gYg^{-1}$ is called conjugation by $g$.

Now we can define something more general than the center of a group.

**Definition 1.2.24** A normal subgroup of the group $G$ is a subgroup $N \leq G$ such that for every $g \in G$, $gNg^{-1} = N$. This is denoted by $N \triangleleft G$.

It is not difficult to realise that when $N \triangleleft G$, the set of all cosets of $N$ in fact forms a group, where the binary operation is defined by $(g_1N)(g_2N) = (g_1g_2)N$ for $g_1, g_2 \in G$, where $g_1g_2$ is calculated as in the group $G$. This group is denoted by $G/N$. 
Definition 1.2.25 A mapping $\pi: G \to G'$ that has the property that for any $g, g' \in G$, $\pi(gg') = \pi(g)\pi(g')$ is called a homomorphism.

From this, we make the following definitions.

Definition 1.2.26 The groups $G$ and $G'$ are isomorphic if there is a homomorphism $\pi$ that is also bijective. We denote this by $G \cong G'$, and we call $\pi$ a group isomorphism.

Definition 1.2.27 If $G = G'$ in the last definition, then $\pi$ is a group automorphism.

Definition 1.2.28 The kernel of the mapping $\pi$ is the set of all elements $g \in G$ such that $\pi(g) = 1$. That is, the kernel of $\pi$ is the set of all elements of $G$ that are mapped to the identity element of $G'$ under $\pi$. This set is denoted by $\text{Ker}(\pi)$.

It is straightforward to verify that $\text{Ker}(\pi)$ is in fact a normal subgroup of $G$.

Definition 1.2.29 The image of the mapping $\pi$ is the set of all elements $g' \in G'$ for which there exists some $g \in G$ such that $\pi(g) = g'$. This set is denoted by $\text{Im}(\pi)$.

The set $\text{Im}(\pi)$ is always a subgroup of $G'$.

We now give one of the basic isomorphism theorems which will be used in the course of this thesis.

Theorem 1.2.30 Let $\pi$ be a homomorphism. Then

$$G/\text{Ker}(\pi) \cong \text{Im}(\pi).$$

Now we turn to a special class of groups that will prove very useful throughout this thesis.

Definition 1.2.31 A $p$-group is a group of order $p^i$ for some $i$, where $p$ is a prime number.

The following three results are known as Sylow theorems.
Theorem 1.2.32 Let \( G \) be a group and let \( p^r \) be the highest power of some prime \( p \) that divides \( |G| \). Then \( G \) contains a subgroup of order \( p^r \).

Definition 1.2.33 Let \( p \) be a prime number. A Sylow \( p \)-subgroup of the group \( G \) is a subgroup of \( G \) that has order \( p^r \), where \( p^r \) is the highest power of \( p \) that divides \( |G| \).

Theorem 1.2.34 Any two Sylow \( p \)-subgroups of the group \( G \) are conjugate to each other.

Theorem 1.2.35 Every subgroup of a group \( G \) whose order is a power of \( p \) is a subgroup of some Sylow \( p \)-subgroup of \( G \).

Finally in this subsection, we define one further class of groups that will be studied extensively in this thesis.

Definition 1.2.36 Let \( G \) and \( H \) be groups. The direct product of \( G \) with \( H \) is defined as follows. The elements of the new group are all of the ordered pairs \((g, h)\) such that \( g \in G \) and \( h \in H \). The binary operation is defined by

\[
(g, h)(g', h') = (gg', hh').
\]

The direct product of \( G \) with \( H \) is denoted by \( G \times H \). The group formed by taking the direct product of \( G \) with \( G \) repeatedly \((n \text{ times, say})\), is denoted by \( G^n \).

Definition 1.2.37 If every non-identity element of the group \( G \) has order \( n \), then we say that \( G \) has characteristic \( n \).

In the case where \( p \) is prime, it is easy to verify that \( \mathbb{Z}_p^n \) has characteristic \( p \), for any \( n \).

1.2.3 Permutation Group Theory

It is often useful, when studying groups that arise in a concrete context, to exploit properties that such groups have. This is what permutation group theory is about.
Definition 1.2.38 A permutation group $G = G(V)$ is a group $G$ that acts on a set $V$ in such a way that every element $g \in G$ is a bijective function from $V$ to $V$. Unlike some authors, if $g \in G$ (where $G$ is a permutation group), and $v \in V$, we denote the action of $g$ on $v$ by $g(v)$. If $h \in G$ is to act on $g(v)$, we denote this by $hg(v)$.

It is not hard to see that the identity element of the permutation group $G$ must in fact be the function that fixes every element of $V$.

Any abstract group can occur as a permutation group on some set $V$. For let $G$ be an abstract group. Then let the set $V$ consist of the group elements of $G$. Let the elements of $G$ act on the elements of $V$ in the following manner. Let $g \in G$, and let $v \in V$. Then $g(v) = gv$, where $gv$ is as defined under the binary operation in $G$. It is straightforward to verify that $G$ will then satisfy the definition of a permutation group on $V$.

As an example of the above, consider the cyclic group $\mathbb{Z}_4$, whose group elements are $\{0, 1, 2, 3\}$. The set $V$ becomes $\{0, 1, 2, 3\}$, and the permutation group elements have the following actions on this set:

\[
\begin{align*}
0(0) &= 0 & 0(1) &= 1 & 0(2) &= 2 & 0(3) &= 3 \\
1(0) &= 1 & 1(1) &= 2 & 1(2) &= 3 & 1(3) &= 0 \\
2(0) &= 2 & 2(1) &= 3 & 2(2) &= 0 & 2(3) &= 1 \\
3(0) &= 3 & 3(1) &= 0 & 3(2) &= 1 & 3(3) &= 2.
\end{align*}
\]

Definition 1.2.39 The permutation group formed from the abstract group $G$ in the manner described above is called the left regular representation of $G$. It is denoted by $G_L$.

Common examples of permutation groups are the groups of symmetries of geometric objects; for example, the set of all possible rotations and reflections of a square is a permutation group, where the group operation $\times$ simply indicates the composition of the functions.

We give some of the basic definitions of permutation group theory.
Definition 1.2.40 The degree of a permutation group is the cardinality of the set \( V \) upon which the group acts.

Definition 1.2.41 The image of the element \( v \) of \( V \) under the permutation \( g \in G \) is simply \( g(v) \). More generally, the image of the set \( Y \subseteq V \) under the permutation \( g \) is

\[
g(Y) = \{ v \in V : v = g(v') \text{ for some } v' \in Y \}.
\]

Definition 1.2.42 The symmetric group of degree \( n \), denoted by \( S_n \), is the group of all possible permutations of the set \( V \), where \( |V| = n \).

Clearly, any permutation group of degree \( n \) will be a subgroup of the symmetric group of degree \( n \).

Permutations can be written in disjoint cycle notation. This notation is formed as follows. Let \( v_1 \) be any element of \( V \). Then we will write one of the disjoint cycles of the permutation \( \phi \) as \( (v_1 v_2 \ldots v_k) \), where \( \phi(v_i) = v_{i+1} \) for \( 1 \leq i \leq k - 1 \), and \( \phi(v_k) = v_1 \). We then let \( v_{k+1} \) be any element of \( V \) that is not in \( \{v_1, \ldots, v_k\} \), and form a second disjoint cycle in the same manner. We repeat this process until all elements of \( V \) appear in some cycle. Singleton cycles are often omitted in this notation.

Definition 1.2.43 If two cycles are disjoint (that is, have no elements in common), we say that the cycles are independent.

Definition 1.2.44 The length of a cycle is the number of elements that appear in that cycle.

We often write that the permutation \( \phi \) is an \( n \)-cycle, if in disjoint cycle notation it consists of a single cycle of length \( n \).

Definition 1.2.45 The permutation group \( G \) acting on the set \( V \) is transitive if for every \( v_1, v_2 \in V \), there exists some \( g \in G \) such that \( g(v_1) = v_2 \).
If a permutation group is not transitive, it is sometimes referred to as intransitive.

It is sometimes useful to consider permutation groups that are, in a sense, minimally transitive. This leads to the following definition.

**Definition 1.2.46** The permutation group $G$ acting on the set $V$ is **regular** if $G$ is transitive on $V$ and if, for every $v_1, v_2 \in V$, the permutation $g \in G$ such that $g(v_1) = v_2$ is unique. Note that if $G$ is regular on $V$ then $|G| = |V|$.

We sometimes say instead, that the permutation group $G$ acts regularly on the set $V$.

**Definition 1.2.47** An **orbit** of the permutation group $G$ acting on the set $V$ is a maximal subset of $V'$ of $V$ for which $G$ acts transitively on $V'$. The **length** of an orbit $V'$ of $G$ is the cardinality of the set $V'$.

Clearly, a transitive permutation group will have a single orbit: the entire set $V$.

**Notation 1.2.48** Let $V'$ be any orbit of $G$. Then the restriction of the action of $g \in G$ to the set $V'$ is denoted by $g|_{V'}$.

This ignores what the action of $g$ may be within other orbits of $G$. For example, $g|_{V'} = 1$ indicates that for every element $v' \in V'$, $g(v') = v'$, but tells us nothing about how $g'$ may act elsewhere.

Sometimes the action of a permutation group $G$ will break down nicely according to its action on certain subsets of the set $V$. Certainly, this happens when $G$ is intransitive, with the orbits of $G$ being the subsets. However, it can also occur in other situations.

**Definition 1.2.49** The subset $B \subseteq V$ is a **$G$-block** if for every $g \in G$, either $g(B) = B$, or $g(B) \cap B = \emptyset$.

In some cases, the group $G$ is clear from the context and we simply refer to $B$ as a block.
It is a simple matter to realise that if $B$ is a $G$-block, then for any $g \in G$, $g(B)$ will also be a $G$-block. Also, intersections of $G$-blocks are themselves $G$-blocks.

**Definition 1.2.50** Let $G$ be a transitive permutation group, and let $B$ be a $G$-block. Then, as noted above, $\{g(B) : g \in G\}$ is a set of blocks that (since $G$ is transitive) partition the set $V$. We call this set the **complete block system** of $G$ generated by the block $B$.

Some of the basic language of blocks will be required in this thesis. Notice that any singleton in $V$, and the entire set $V$, are always $G$-blocks.

**Definition 1.2.51** The **size** of the block $B$ is the cardinality of the set $B$.

**Definition 1.2.52** A block $B$ is **nontrivial** if the size of $B$ is neither 1 nor the cardinality of $V$.

So the blocks of cardinality 1 and $|V|$ are considered to be trivial. As mentioned above, the trivial blocks are the ones that are always $G$-blocks.

**Definition 1.2.53** The transitive permutation group $G$ is said to be **primitive** if $G$ does not admit nontrivial blocks. If $G$ is transitive but not primitive, then $G$ is said to be **imprimitive**.

**Theorem 1.2.54** ([96], Proposition 6.3) *The size of a block $B$ of a transitive permutation group $G$ divides the degree of $G$, and the number of blocks in the complete block system generated by $B$ also divides the degree of $G$.*

This leads immediately to the following corollary.

**Corollary 1.2.55** A permutation group of prime degree is primitive.

**Theorem 1.2.56** ([96], Proposition 7.1) *The transitive permutation group $G$ is imprimitive if and only if $G$ contains an intransitive normal subgroup $N$ such that $N \neq \{1\}$. Furthermore, the orbits of $N$ form a complete block system of $G$.***
Using Theorems 1.2.56 and 1.2.19, the following theorem is straightforward to prove. The proof is left to the reader.

**Theorem 1.2.57** Every complete block system of \( \mathbb{Z}_n \) consists of the orbits of some subgroup of \( \mathbb{Z}_n \).

**Definition 1.2.58** The transitive permutation group \( G \) is said to admit blocks of size \( n \) for some integer \( n \) if there exists some \( G \)-block \( B \) such that the size of \( B \) is \( n \).

In this case, since \( G \) is transitive, there will in fact be a complete block system of blocks of size \( n \) generated by the block \( B \).

**Definition 1.2.59** Let \( H \) be a permutation group on the set \( V \), and let \( G \leq H \). Let \( B \) be a set of \( G \)-blocks. The permutation \( h \in H \) is said to respect the blocks of \( B \) if for every block \( B \in B \), either \( h(B) = B \), or \( h(B) \cap B = \emptyset \).

**Definition 1.2.60** The set \( B \subseteq V \) is said to be fixed setwise by the subset \( G' \) of \( G \) if for every \( g \in G' \), \( g(B) = B \).

**Definition 1.2.61** The set \( B \subseteq V \) is said to be fixed pointwise by the subset \( G' \) of \( G \) if for every \( g \in G' \) and for every \( v \in B \), \( g(v) = v \).

**Definition 1.2.62** The stabiliser subgroup in \( G \) of the set \( V' \) is the subgroup of \( G \) consisting of all \( g \in G \) such that \( g \) fixes \( V' \) pointwise. This is denoted by \( \text{Stab}_G(V') \), or sometimes, particularly if \( V' = \{v\} \) contains only one element, simply by \( G_{V'} \), or \( G_v \).

It is straightforward to verify that the stabiliser subgroup in \( G \) of \( V' \) is in fact a subgroup. In some cases, we allow the set \( V' \) to be a set of subsets of \( V \) (where \( V \) is the set upon which \( G \) acts) rather than a set of elements of \( V \). In this case, the requirement is that every element of \( \text{Stab}_G(V') \) fix every set in \( V' \) setwise. For example, if \( B \) is a complete block system of \( G \), then \( \text{Stab}_G(B) \) is the subgroup of \( G \)
that consists of all elements of \( G \) that fix every block in \( B \) setwise. Once again, it is not challenging to verify that this is indeed a subgroup of \( G \).

The notion of isomorphism is slightly different for permutation groups than for abstract groups.

**Definition 1.2.63** Let \( G \) and \( H \) be permutation groups, both of degree \( n \), acting on the sets \( V \) and \( V' \), respectively. Then \( G \) on \( V \) is **isomorphic** as a permutation group to \( H \) on \( V' \) if there is an isomorphism (in the sense of abstract groups) \( \phi \) from \( G \) to \( H \) and a bijection \( \psi \) from \( V \) to \( V' \), such that for every \( g \in G \) and for every \( v \in V \), \( \psi[g(v)] = \phi(g)[\psi(v)] \).

**Definition 1.2.64** Let \( U \) and \( V \) be sets, \( H \) and \( K \) groups of permutations of \( U \) and \( V \) respectively. The **wreath product** \( H \wr K \) is the group of all permutations \( f \) of \( U \times V \) for which there exist \( h \in H \) and an element \( k_u \) of \( K \) for each \( u \in U \) such that

\[
f((u, v)) = (h(u), k_{h(u)}(v))
\]

for all \((u, v) \in U \times V\).

### 1.2.4 Algebraic Graph Theory

On the surface, the mathematical disciplines of group theory and graph theory have little in common. It is in the area of symmetry that they meet and begin to have some association. Algebraic groups can be used to define large families of graphs that will have a lot of symmetry. The techniques of algebra can then be used to find solutions to some graph-theoretic problems as they relate to these families of graphs. This is essentially what the algebraic graph theory that is used in this thesis amounts to.

**Definition 1.2.65** Let \( S \) be a subset of a group \( G \). The **Cayley digraph** \( \vec{X} = \vec{X}(G; S) \) is the directed graph given as follows. The vertices of \( X \) are the elements of the group \( G \). If \( g, h \in G \), there is an arc from the vertex \( g \) to the vertex \( h \) if and
only if \( g^{-1}h \in S \). In other words, for every vertex \( g \in G \) and element \( s \in S \), there is an arc from \( g \) to \( gs \).

Notice that if the identity element \( 1 \in G \) is in \( S \), then the Cayley digraph will have a directed loop at every vertex, while if \( 1 \not\in S \), the digraph will have no loops. For convenience, we may assume that the latter case holds: it is immaterial to the results. Notice also that since \( S \) is a set, it contains no multiple entries and hence there are no multiple arcs. Finally, notice that if the inverse of every element in \( S \) is itself in \( S \), then the digraph is equivalent to a graph, since every arc can be paired with an arc going in the opposite direction between the same two vertices.

**Definition 1.2.66** The Cayley colour digraph \( \bar{X} = \bar{X}(G; S) \) is very similar to a Cayley digraph, except that each entry of \( S \) has a colour associated with it, and for any \( s \in S \) and any \( g \in G \), the arc in \( \bar{X} \) from the vertex \( g \) to the vertex \( gs \) is assigned the colour that has been associated with \( s \).

Results that hold true for Cayley colour digraphs would clearly also hold true for Cayley digraphs in which multiple arcs from one fixed vertex to another were permitted. This is true since we can achieve the effect of a directed graph with multiple arcs permitted, by assigning colour \( i \) to the single arc from \( g \) to \( h \) in the Cayley colour digraph if there were supposed to be \( i \) arcs from \( g \) to \( h \).

All of the results of this thesis also hold for Cayley colour digraphs. This is not always made explicit, but is a simple matter to verify without changing any of the proofs used.

**Definition 1.2.67** The set \( S \) of \( \bar{X}(G; S) \) is called the connection set of the Cayley digraph \( \bar{X} \).

**Definition 1.2.68** We say that the digraph \( \bar{Y} \) can be represented as a Cayley digraph on the group \( G \) if there is some connection set \( S \) such that \( \bar{Y} \cong \bar{X}(G; S) \).

Sometimes we say that \( \bar{Y} \) is a Cayley digraph on the group \( G \).
Definition 1.2.69 The automorphism group of the digraph $\bar{X}$ is the permutation group that is formed of all possible automorphisms of the digraph. This group is denoted by $\text{Aut}(\bar{X})$.

The reader can verify that $\text{Aut}(\bar{X})$ is in fact a group.

Definition 1.2.70 A vertex-transitive digraph is one for which the automorphism group is transitive on the vertices of the digraph.

Cayley digraphs are always vertex-transitive, as demonstrated by the fact that given any fixed element $g \in G$, left-multiplication of each vertex of $\bar{X}$ by $g$ is an automorphism of the digraph.

Theorem 1.2.71 (Sabidussi [87], pg. 694) Let $U$ and $V$ be digraphs. Then

$$\text{Aut}(U) \wr \text{Aut}(V) \leq \text{Aut}(U \wr V).$$

This follows immediately from the definition of wreath product of permutation groups, and is mentioned only as an aside in Sabidussi’s paper and in the context of graphs. It is equally straightforward for digraphs.

In the case where the digraph $U$ is irreducible with respect to $\wr$ and $V = E_k$ for some $k$, the group $\text{Aut}(U \wr V)$ will admit each set of vertices that corresponds to a copy of $E_k$ as a block. Consequently, there is a straightforward partial converse to the above theorem.

Corollary 1.2.72 If $U$ is a digraph that is irreducible with respect to $\wr$, then

$$\text{Aut}(U) \wr \text{Aut}(E_k) = \text{Aut}(U \wr E_k).$$

We now define some terms that classify the types of problems being studied in this thesis.

Definition 1.2.73 A group $G$ is a CI-group (CI stands for Cayley Isomorphism) if whenever $\bar{X} = \bar{X} (G; S_1) \cong \bar{Y} = \bar{Y} (G; S_2)$, there is a group automorphism $\phi$ of $G$ such that $\phi(S_1) = S_2$. 
First, notice that the notation $\phi(S_1)$ makes sense since $S_1$ is a subset of the elements of the group $G$. Then observe that $\phi(S_1) = S_2$ means precisely that $\phi$ is a graph isomorphism from $\tilde{X}$ to $\tilde{Y}$. If $G$ is a CI-group, then we will be able to use that fact together with the known automorphisms of $G$ to determine all Cayley digraphs on $G$ that are isomorphic to a fixed Cayley digraph $\tilde{X} = \tilde{X}(G; S)$.

Definition 1.2.74 The digraph $\tilde{X}$ is a CI-

**digraph** on the group $G$ if $\tilde{X} = \tilde{X}(G; S)$ is a Cayley digraph on the group $G$ and for any isomorphism of $\tilde{X}$ to another Cayley digraph $\tilde{Y} = \tilde{Y}(G; S')$ on the group $G$, there is a group automorphism $\phi$ of $G$ that maps $\tilde{X}$ to $\tilde{Y}$. That is, $\phi(S) = S'$.

Analogous to the comment above, if $\tilde{X}$ is a CI-digraph on the group $G$, we will be able to use that fact together with the known automorphisms of $G$ to determine all Cayley digraphs on $G$ that are isomorphic to $\tilde{X}$.

Finally, we will give one more definition about wreathing and sets of vertices in a digraph. Because this definition requires the notion of blocks, it could not be given with the other definition before any permutation group theory had been introduced.

**Definition 1.2.75** Let $G$ be a transitive permutation group acting on $\tilde{X}$. A $G$-

**block** $B$ of vertices of $\tilde{X}$ is a **wreathed block** if for every $g, h \in G$ and for every colour $c$, one of the following holds:

1. $gB = hB$

2. There is no arc (of colour $c$) from the vertices in $gB$ to those in $hB$, or

3. There is an arc (of colour $c$) from every vertex in $gB$ to every vertex in $hB$.

We are now equipped with the essential terminology that will be widely used in the rest of this thesis.

### 1.3 History of the Cayley Isomorphism Problem

Dr. Cai Heng Li of the University of Western Australia has recently written a comprehensive survey paper on the history of work on the Cayley Isomorphism
Problem [63]. It is by no means the intent of this section to duplicate his work. However, it is useful to give the reader a sense of the major results that have been achieved in working on this problem, and an idea of some of the approaches that have been employed.

The Cayley Isomorphism problem is the problem of determining whether or not a group or a digraph is a CI-group or a CI-digraph, respectively.

Study of this problem really began in 1967 when Ádám conjectured [1] that $\mathbb{Z}_n$ is a CI-group for every $n$. This conjecture was disproven by Elspas and Turner three years later [20]. The problem has subsequently aroused considerable interest, as indicated by the long list of related papers given in the bibliography.

One major angle from which the Cayley Isomorphism problem was considered was the question of which cyclic groups are in fact CI-groups. The problem raised by Ádám’s conjecture has now been completely solved by Muzychuk [78] and [79]. He proves that a cyclic group of order $n$ is a CI-group if and only if $n = k, 2k$ or $4k$ where $k$ is odd and square-free. The proof uses Schur rings and is very technical. Many special cases were obtained independently along the way to this result, by various authors cited in the bibliography.

One of the most useful approaches to proving whether or not a given Cayley digraph is a CI-digraph has been the following theorem by Babai. This theorem has been used in the vast majority of results to date on the Cayley Isomorphism problem.

**Theorem 1.3.1** (Babai, see [6]) Let $\bar{X}$ be a Cayley digraph on the group $G$. Then $\bar{X}$ is a CI-digraph if and only if all regular subgroups of $\text{Aut}(\bar{X})$ isomorphic to $G$ are conjugate to each other in $\text{Aut}(\bar{X})$.

One line of approach to the Cayley Isomorphism problem was to consider the question of whether or not all Cayley digraphs $\bar{X} = \bar{X}(G; S)$ were CI-digraphs if $S$ were required to be a minimal generating set of $G$. This question was stated as a conjecture by Xu [100], but counterexamples have been found (see [53]). A number of results that attempt to classify when such Cayley digraphs are CI-digraphs have
been obtained in some of the works listed in the bibliography.

A different method of considering the Cayley Isomorphism problem that has yielded many results is the problem of determining whether or not all Cayley digraphs \( \tilde{X} = \tilde{X}(G; S) \) on a fixed group \( G \) of order \( n \), with \( |S| \leq m \) (\( m < n \)), are CI-digraphs. Results of this nature have been too numerous to list here, but are included in the bibliography.

Families of groups that may be CI-groups have been limited quite severely by results of Babai and Frankl [8], [9], and have been further limited since by other results listed in the bibliography. However, the question of whether or not the groups that may be CI-groups actually are CI-groups remains open in many cases. One family of particular interest is the family of groups \( \mathbb{Z}_p^n \). The history of this question is given in more depth in Chapter 2 of this thesis.

With this general background, we are ready to introduce the specific problems studied and results obtained within this thesis.
Chapter 2

$\mathbb{Z}_p^4$ is a CI-group

2.1 History of the Problem

As mentioned in the introductory chapter, considerable work has been done over the years on the problem of determining which of all the groups that may be CI-groups actually are CI-groups. In [8], Babai and Frankl asked whether or not all groups of the form $\mathbb{Z}_p^n$ are CI-groups (where $p$ is a prime), and this question has been considered by several people.

In 1992, Lewis Nowitz constructed a Cayley graph on $\mathbb{Z}_2^6$ that was not a CI-graph, thus showing that not all groups of the form $\mathbb{Z}_p^n$ are CI-groups [80]. Alspach provided a simpler proof of the Nowitz result in [3].

From the other side of things, Godsil [30] first proved that $\mathbb{Z}_p^2$ is a CI-group for every prime $p$. The first proof that $\mathbb{Z}_p^3$ is a CI-group for every prime $p$ is by Dobson, and appears in [18]. A more elementary proof of this result is provided by Alspach and Nowitz in [4].

The object of this chapter is to provide the next natural step along these lines, by proving that $\mathbb{Z}_p^4$ is a CI-group for every prime $p$. Hirasaka and Muzychuk [40] have recently announced an independent proof of this result. The method used in this chapter is analogous to Alspach and Nowitz’s elementary proof for $\mathbb{Z}_p^3$ mentioned above. It is hoped that in the near future, the same method will serve to prove or disprove a similar result for $\mathbb{Z}_p^5$ and, if necessary, $\mathbb{Z}_p^6$, enabling us to determine
whether or not the Nowitz result can be generalised to primes other than 2.

2.2 Background Definitions and Theory

We now give definitions for some of the terms that are used only in this chapter of the thesis. Some of these are quite basic terminology from graph theory or group theory, but we present them here for the sake of completeness.

**Definition 2.2.1** The graph $X$ is said to be **connected** if for any two vertices $v_1$ and $v_2$ of $X$, there is a path from $v_1$ to $v_2$.

If a graph is not connected, it is said to be disconnected. In this case, it is of interest to consider subgraphs that are connected.

**Definition 2.2.2** The induced subgraph $X[V]$ of $X$ is said to be a **component** of $X$ if it is connected but there is no superset $V'$ of $V$ for which $X[V']$ is connected.

Although this chapter deals with both connected and disconnected graphs and digraphs, the notion of a (connected) component will be required in the proof.

Some basic terminology from linear algebra is useful in this chapter of the thesis.

**Definition 2.2.3** A vector is a directional marker that includes distance and direction. The vector $\vec{a}$ is denoted by the Cartesian coordinates that would mark its endpoint if its starting point were at the origin.

Linear combinations of vectors are calculated as follows. If $i, j$ are integers and $\vec{a} = (a_1, \ldots, a_n)$, $\vec{b} = (b_1, \ldots, b_n)$ are vectors, then $i\vec{a} + j\vec{b} = (ia_1 + jb_1, \ldots, ia_n + jb_n)$.

**Definition 2.2.4** If a vector is represented by $n$ Cartesian coordinates, we call it an $n$-dimensional vector.

**Definition 2.2.5** The set of vectors $\vec{a}_1, \ldots, \vec{a}_n$ is **linearly dependent** (over $\mathbb{Z}_p$) if there exist $i_1, \ldots, i_n \in \mathbb{Z}_p$, not all zero, such that

$$i_1\vec{a}_1 + \ldots + i_n\vec{a}_n = \vec{0},$$
where \( \vec{0} \) is the vector all of whose Cartesian coordinates are 0.

If a set of vectors is not linearly dependent, then it is linearly independent.

There are a number of special cases of linear dependence and independence for which it is useful to have their own terms.

**Definition 2.2.6** A set of vectors is **pairwise linearly independent** if any two vectors in the set are linearly independent. The set is **pairwise linearly dependent** or **collinear** if any two vectors in the set are linearly dependent.

**Definition 2.2.7** A set of vectors is **coplanar** if any subset of three vectors from the set is linearly dependent.

We now give a definition that is specifically for this chapter, although it uses some of the terminology of linear algebra.

**Definition 2.2.8** Beginning with some given vertex \( x_{i,j,k,l} \), we define the set of vertices within the block \( B_i \) spanned by the set of 3-dimensional vectors \( \vec{v}_1 = (r_1, s_1, t_1), \ldots, \vec{v}_z = (r_z, s_z, t_z) \) to be the set

\[
\{ x_{i,j+k_1 r_1 + \ldots + k_z r_z, k_1 s_1 + \ldots + k_z s_z, k_1 t_1 + \ldots + k_z t_z} : 0 \leq k_1, \ldots, k_z \leq p - 1 \}.
\]

For the purposes of this definition, \( B_i \) is assumed to have cardinality \( p^3 \) where \( p \) is prime. If no starting vertex is given, it is assumed that the starting vertex is \( x_{i,0,0,0} \) so long as the block is clear.

We proceed with a number of preliminaries that will be used throughout this chapter.

**Definition 2.2.9** Let \( H \) be a permutation group, and let \( B_1 \) and \( B_2 \) be \( H \)-blocks with \( B_1 \neq B_2 \). We say that the **action of \( H \) forces \( B_1 \) and \( B_2 \) to be wreathed** if given any \( v_1, v_2 \in B_1 \) and any \( u_1, u_2 \in B_2 \), there exists some \( h \in H \) such that \( h(v_1) = v_2 \) and \( h(u_1) = u_2 \).
It is apparent from this definition that whenever $H \leq \text{Aut}(\tilde{X})$, $B_1$ and $B_2$ are sets of vertices of $\tilde{X}$, and the action of $H$ forces $B_1$ and $B_2$ to be wreathed, the blocks $B_1$ and $B_2$ must in fact be wreathed according to Definition 1.2.10.

The notion of forced wreathing, as this is sometimes referred to, is an important one in the proof. It is possible for some pair of blocks $B_1$ and $B_2$ to be wreathed even if there is no automorphism of the digraph that takes some pair $(b_1, b_2)$ to some other pair $(b'_1, b'_2)$ where $b_1, b'_1 \in B_1$ and $b_2, b'_2 \in B_2$. However, when that is the case, we cannot draw many conclusions about whether or not other pairs of blocks may be wreathed with one another. Forced wreathing gives us a significant amount of information about the automorphism group of the digraph, from which we can generally draw other conclusions.

Based on calculations of size, it is not difficult to verify that the Sylow $p$-subgroups of $S_p^*$ are $\mathbb{Z}_p \wr \mathbb{Z}_p \wr \mathbb{Z}_p \wr \mathbb{Z}_p$. By the definition of wreath product of permutation groups, every Sylow $p$-subgroup of $S_p^*$ has unique block systems with blocks of size $p, p^2$, and $p^3$. Also by the same definition, any permutation of order $p$ that respects these blocks is in fact an element of $\mathbb{Z}_p \wr \mathbb{Z}_p \wr \mathbb{Z}_p \wr \mathbb{Z}_p$. Note that the group $\mathbb{Z}_p \wr \mathbb{Z}_p \wr \mathbb{Z}_p \wr \mathbb{Z}_p$ acts on the set $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$, where here $\mathbb{Z}_p$ is indicating the set $\{0, 1, \ldots, p - 1\}$ rather than the group, and $\times$ is denoting the standard Cartesian product of these sets.

Throughout this chapter, all calculations are taken modulo $p$, and the range of all variables is within $\{0, 1, \ldots, p - 1\}$, in addition to any other restrictions given.

Let $\tilde{X} = \tilde{X}(\mathbb{Z}_p^4; S)$ be a Cayley colour digraph on the group $\mathbb{Z}_p^4$. Because the group $\mathbb{Z}_p \wr \mathbb{Z}_p \wr \mathbb{Z}_p \wr \mathbb{Z}_p$ acts on the set $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$, we will label the vertices of $\tilde{X}$ with four subscripts according to this action, in a manner to be described below.

Suppose that $\sigma(\mathbb{Z}_p^4)_L \sigma^{-1} \leq \text{Aut}(\tilde{X})$ for some $\sigma \in S_{\mathbb{Z}_p^4}$. We want to show that $(\mathbb{Z}_p^4)_L$ and $\sigma(\mathbb{Z}_p^4)_L \sigma^{-1}$ are conjugate in $\text{Aut}(\tilde{X})$. By Theorem 1.3.1, this will be sufficient to complete the proof of the main theorem of this chapter.

By taking a conjugate of $\sigma(\mathbb{Z}_p^4)_L \sigma^{-1}$ if necessary, we may assume by Theorems 1.2.35 and 1.2.34 that $(\mathbb{Z}_p^4)_L$ and $\sigma(\mathbb{Z}_p^4)_L \sigma^{-1}$ are in the same Sylow $p$-subgroup $P$ of $\text{Aut}(\tilde{X})$. The group $P$ is contained in some Sylow $p$-subgroup $P^*$ of $S_{\mathbb{Z}_p^4}$, by Theorem
1.2.35. that has unique imprimitive blocks of size \( p \). Let the blocks be

\[
B_{i,j,k} = \{x_{i,j,k,l} : 0 \leq l \leq p - 1\}, 0 \leq i, j, k \leq p - 1.
\]

Furthermore, it also has unique imprimitive blocks of size \( p^2 \). Let

\[
B_{i,j} = B_{i,j,0} \cup B_{i,j,1} \cup \ldots \cup B_{i,j,p-1}
\]

be the blocks of size \( p^2 \). There are also unique imprimitive blocks of size \( p^3 \). Let

\[
B_i = B_{i,0} \cup \ldots \cup B_{i,p-1}
\]

be the blocks of size \( p^3 \). We call these the standard complete block systems. Whenever \( p^i \)-blocks are referred to in the proof, it is the blocks of the standard complete block system whose blocks have size \( p^i \) that are intended.

The group \( G \) is defined repeatedly below as the subgroup of \( \langle (\mathbb{Z}_p^4)_L, \sigma(\mathbb{Z}_p^4)_L\sigma^{-1} \rangle \) which fixes the vertex \( x_{0,0,0,0} \). However, the group \( \sigma(\mathbb{Z}_p^4)_L\sigma^{-1} \), upon which this definition depends, varies in the different contexts under which \( G \) is defined, so we will give the definition each time it is required.

We use an important property involving regular permutation groups several times in what follows. This is straightforward for the reader to verify. If a permutation group \( G \) is transitive and abelian then it is regular. As a result, if \( G \) is transitive, abelian and imprimitive, then any permutation in \( G \) that fixes some block setwise must fix all blocks setwise. This follows because the action of \( G \) on the set of blocks is also transitive and abelian, and consequently regular.

Let the permutation

\[
\theta_{i,j,k} = (x_{i,j,k,0} \ x_{i,j,k,1} \ldots \ x_{i,j,k,p-1}).
\]

Since both \( (\mathbb{Z}_p^4)_L \) and \( \sigma(\mathbb{Z}_p^4)_L\sigma^{-1} \) are abelian and transitive on the sets of blocks of each size, they are regular in their action on these sets of blocks. Without loss of
generality, assume that the blocks are coordinatised so that
\[
\tau_4(x_{i,j,k,l}) = x_{i,j,k,l+1} \quad \text{for all } i, j, k, l
\]
\[
\tau_3(x_{i,j,k,l}) = x_{i,j,k+1,l} \quad \text{for all } i, j, k, l
\]
\[
\tau_2(x_{i,j,k,l}) = x_{i,j+1,k,l} \quad \text{for all } i, j, k, l, \text{ and}
\]
\[
\tau_1(x_{i,j,k,l}) = x_{i+1,j,k,l} \quad \text{for all } i, j, k, l
\]
are all elements of the group \((\mathbb{Z}_p^4)_L\). Note that
\[
\tau_4 = \prod_{0 \leq i,j,k \leq p-1} \theta_{i,j,k}
\]
and \((\mathbb{Z}_p^4)_L = \langle \tau_1, \tau_2, \tau_3, \tau_4 \rangle\).

We also use some equally straightforward facts about \(p\)-groups. If \(g\) and \(g'\) are in the \(p\)-group \(P\), \(\langle g, g' \rangle\) fixes the block \(B\) of size \(p\) setwise, and \(g|_B \neq 1\), then \(g'|_B = (g')|_B\) for some \(i\). This is because otherwise there would be an element \(h \in \langle g, g' \rangle \leq P\) whose order would not be a power of \(p\).

For the same reason, any element \(g\) of a \(p\)-group \(P\) such that \(\langle g \rangle\) admits a block \(B\) of size \(p\), where \(g(B) = B\) and \(g|_B \neq 1\), must be transitive on \(B\).

The following lemma is useful in determining that two blocks are wreathed, and will be used often in this chapter.

**Lemma 2.2.10** Let \(G\) be a transitive subgroup of \(\text{Aut}(\tilde{X})\), and let \(B_1\) and \(B_2\) be \(G\)-blocks in the complete block system \(B\). If \(\text{Stab}_G(B)\) is transitive on each block \(B \in B, x \in B_1, \text{ and the orbit of } \text{Stab}_G(B)_x \text{ containing } y \in B_2 \text{ in fact contains all of } B_2, \text{ then } B_1 \text{ and } B_2 \text{ are wreathed.}

**Proof.** We begin by assuming that there is a red arc from \(x' \in B_1\) to \(y' \in B_2\), and prove that there must be a red arc from \(x'' \in B_1\) to \(y'' \in B_2\). This will be sufficient.

Since \(\text{Stab}_G(B)\) is transitive on \(B_1\), there exists some \(\phi \in \text{Stab}_G(B)\) such that \(\phi(x') = x\). Likewise, there exists some \(\delta \in \text{Stab}_G(B)\) such that \(\delta(x) = x''\). Clearly, \(\phi(y') \in B_2\) and \(\delta^{-1}(y'') \in B_2\). Since the orbit of \(\text{Stab}_G(B)_x\) containing \(y \in B_2\) in fact contains all of \(B_2\), there exists some \(\psi \in \text{Stab}_G(B)_x\) such that \(\psi(\phi(y')) = \delta^{-1}(y'')\).
Thus, $\delta\psi\phi(y') = y''$, and $\delta\psi\phi(x') = x''$. Since $\delta$, $\psi$ and $\phi$ were all automorphisms of $\overline{X}$, there must be a red arc from $x''$ to $y''$, and the proof is complete.

We now have the necessary background material, and can proceed with the proof of the main theorem.

### 2.3 Main Theorem

**Theorem 2.3.1** (See also [40]) *The group $\mathbb{Z}_p^4$ is a CI-group for every prime $p$.*

**Proof.** The first step is to find a conjugate of $\sigma(\mathbb{Z}_p^4)_L\sigma^{-1}$ containing $\tau_4$. Let $\tau'_4 \in \sigma(\mathbb{Z}_p^4)_L\sigma^{-1}$ be the unique element of that group that maps $x_{0,0,0,0}$ to $x_{0,0,0,1}$. It is an immediate consequence of Lemma 2.4.1 that $\tau'_4 = \tau_4$, so the group $\sigma(\mathbb{Z}_p^4)_L\sigma^{-1}$ already contains $\tau_4$, and we can proceed to finding a conjugate of $\sigma(\mathbb{Z}_p^4)_L\sigma^{-1}$ that contains $\tau_3$.

Lemma 2.5.1 gives us a conjugate $g\sigma(\mathbb{Z}_p^4)_L\sigma^{-1}g^{-1}$ of $\sigma(\mathbb{Z}_p^4)_L\sigma^{-1}$ that contains both $\tau_3$ and $\tau_4$, as required, and since $g \in P$, we still have $g\sigma(\mathbb{Z}_p^4)_L\sigma^{-1}g^{-1} \leq P$.

Lemma 2.6.1 produces a conjugate $\phi g\sigma(\mathbb{Z}_p^4)_L\sigma^{-1}g^{-1}\phi^{-1}$ of $g\sigma(\mathbb{Z}_p^4)_L\sigma^{-1}g^{-1}$ that contains $\tau_2$ as well as $\tau_3$ and $\tau_4$. Since $\phi \in P$, the group $\phi g\sigma(\mathbb{Z}_p^4)_L\sigma^{-1}g^{-1}\phi^{-1} \leq P$.

Finally, Lemma 2.7.1 produces a conjugate

$$\psi \phi g\sigma(\mathbb{Z}_p^4)_L\sigma^{-1}g^{-1}\phi^{-1}\psi^{-1}$$

of the group $\phi g\sigma(\mathbb{Z}_p^4)_L\sigma^{-1}g^{-1}\phi^{-1}$ that contains all of $(\mathbb{Z}_p^4)_L$. Since

$$|\psi \phi g\sigma(\mathbb{Z}_p^4)_L\sigma^{-1}g^{-1}\phi^{-1}\psi^{-1}| = |(\mathbb{Z}_p^4)_L|,$$

we have $\psi \phi g\sigma(\mathbb{Z}_p^4)_L\sigma^{-1}g^{-1}\phi^{-1}\psi^{-1} = (\mathbb{Z}_p^4)_L$.

Thus, we have satisfied the conditions of Theorem 1.3.1, so have indeed demonstrated that $\mathbb{Z}_p^4$ is a CI-group. $\square$
2.4 The Action of Elements of $\sigma(\mathbb{Z}_p^4)_L\sigma^{-1}$

For the purposes of the following lemma, in addition to the $p$-blocks, the $p^2$-blocks and the $p^3$-blocks defined earlier, we use the language that each individual vertex is a 1-block.

**Lemma 2.4.1** Let $\sigma(\mathbb{Z}_p^4)_L\sigma^{-1}$ be any conjugate of $(\mathbb{Z}_p^4)_L$ such that $\sigma(\mathbb{Z}_p^4)_L\sigma^{-1} \leq P$, where $P$ is a fixed Sylow $p$-subgroup of Aut(\(\bar{X}\)) that contains $(\mathbb{Z}_p^4)_L$. Let $\tau'_i \in \sigma(\mathbb{Z}_p^4)_L\sigma^{-1}$ be the element that maps $x_{0,0,0,0}$ to $x_{a_1,a_2,a_3,a_4}$, where $a_i = 1$ and $a_j = 0$ for $j \neq i$. Then $\tau'_i$ takes the standard $p^4-i$-block that contains $x_{a,b,c,d}$ to the standard $p^{4-i}$-block that contains $x_{a+a_1,b+a_2,c+a_3,d+a_4}$ for every $a,b,c,d$.

**Proof.** We know that $\sigma(\mathbb{Z}_p^4)_L\sigma^{-1}$ acts regularly on the vertices and the blocks of $\bar{X}$. By its definition and the definition of a block, the automorphism $\tau'_i$ clearly fixes the standard $p^{5-i}$-block that contains $x_{0,0,0,0}$ setwise. Consequently, $\tau'_i$ must fix all of the $p^{5-i}$-blocks in the standard complete block system setwise. Let $B$ be some fixed standard $p^{5-i}$-block. Since $\tau'_i \in P$, $\tau'_i$ must increase the $i$th subscript of every standard $p^{4-i}$-block in $B$ by some fixed $j$, while leaving the other subscripts unchanged.

Consider any $p^{5-i}$-block $B$ within which $\tau'_i$ increases the $i$th subscripts by $j$. Let $x_{a,b,c,d} \in B$, and let $\tau'$ be the element of $\sigma(\mathbb{Z}_p^4)_L\sigma^{-1}$ that maps $x_{a,b,c,d}$ to $x_{0,0,0,0}$. Then $\tau'_1 \tau'_2 \tau'_3 \tau'_4 \tau'$ fixes $x_{a,b,c,d}$, implying it fixes the $p^{4-i}$-block $C$ containing $x_{a,b,c,d}$ setwise, and thus fixes every $p^{4-i}$-block in $B$ setwise. Now, $\tau'_i$ and $\tau'$ commute, so we have

$$\tau'_i(x_{a,b,c,d}) = (\tau')^{-1} \tau'_i \tau'(x_{a,b,c,d})$$

$$= (\tau')^{-1} \tau'_i(x_{0,0,0,0})$$

$$= (\tau')^{-1} x_{a_1,a_2,a_3,a_4}$$

$$\in \tau'_i(C)$$

and we know that $(\tau')^{-1}(x_{a_1,a_2,a_3,a_4})$ is in the same $p^{4-i}$-block, $\tau'_i(C)$, as

$$\tau'_1 \tau'_2 \tau'_3 \tau'_4 \tau'(\tau')^{-1}(x_{a_1,a_2,a_3,a_4}) = x_{a+a_1,b+a_2,c+a_3,d+a_4}.$$
This completes the proof. \[\square\]

2.5 Conjugation of $\sigma(Z_p^4)L\sigma^{-1}$ to Obtain a Group that Contains $\tau_3$

2.5.1 Finding the conjugate $g\sigma(Z_p^4)L\sigma^{-1}g^{-1}$

Lemma 2.5.1 Let $\sigma(Z_p^4)L\sigma^{-1}$ be any conjugate of $(Z_p^4)L$ such that $\sigma(Z_p^4)L\sigma^{-1} \leq P$, where $P$ is a fixed Sylow $p$-subgroup of $\text{Aut}(\bar{X})$ that contains $(Z_p^4)L$, and $\tau_4 \in \sigma(Z_p^4)L\sigma^{-1}$. Then there exists some $g \in P$ such that $g\sigma(Z_p^4)L\sigma^{-1}g^{-1}$ contains $\tau_3$ and $\tau_4$.

Proof. Let $\tau_3'$ be the element of $\sigma(Z_p^4)L\sigma^{-1}$ that maps $x_{0,0,0,0}$ onto $x_{0,0,1,0}$. Then by Lemma 2.4.1 we have $\tau_3'(B_{i,j,k}) = B_{i,j,k+1}$ for every $i,j,k$.

If

$$\tau_3'(x_{i,j,k,l}) = x_{i,j,k+1,l+d_{i,j,k}},$$

then $\tau_3'(x_{i,j,k,l+m}) = x_{i,j,k+1,l+m+d_{i,j,k}}$

for every $m$, because $\tau_3'$ commutes with $\tau_4$. Note that the set

$$\{d_{i,j,k} : 0 \leq i,j,k \leq p-1\}$$

completely determines the action of $\tau_3'$.

Define the auxiliary graph $Y'$ whose vertices are the blocks $B_{i,j,k}$, where $B_{i,j,k}$ is adjacent to $B_{a,b,c}$ in $Y'$ if and only if the blocks $B_{i,j,k}$ and $B_{a,b,c}$ are not wreathed.

It can be verified that the components of $Y'$ must be blocks of $\text{Aut}(\bar{X})$. For if $B$ and $B'$ are $p$-blocks in the same component of $Y'$, then there is a path in $Y'$ from $B$ to $B'$. If $g \in \text{Aut}(\bar{X})$, then whenever $B_{i,j,k}$ and $B_{a,b,c}$ are not wreathed, neither are $g(B_{i,j,k})$ and $g(B_{a,b,c})$. Hence if we let $g$ act on the path in $Y'$ from $B$ to $B'$, we see that there must be a path in $Y'$ from $g(B)$ to $g(B')$. Thus $g(B)$ and $g(B')$ are both in some component of $Y'$. This is sufficient. Similar arguments can be used later to yield analogous results for other auxiliary graphs.
Notice that if \( B_{i,j,k} \) and \( B_{a,b,c} \) are in the same component of \( Y' \), then we must have \( d_{i,j,k} = d_{a,b,c} \). For if this were not true, consider a path from \( B_{i,j,k} \) to \( B_{a,b,c} \) in \( Y' \). There must be some pair of adjacent vertices of \( Y' \) along this path, say \( B_{a',b',c'} \) and \( B_{i',j',k'} \), such that \( d_{a',b',c'} \neq d_{i',j',k'} \). But then \( \tau_4^{-d_{a',b',c'}} \tau_3^{-1} \tau_3' \) fixes \( B_{a',b',c'} \) pointwise, but takes \( x_{i',j',k',l'} \) to \( x_{i',j',k',l'+d_{i',j',k'}-d_{a',b',c'}} \) for any \( l' \), meaning that \( B_{a',b',c'} \) and \( B_{i',j',k'} \) are welded, contradicting their adjacency in \( Y' \).

We assume that \( \tau_3' \neq \tau_3 \); otherwise we would be done. Since \( \tau_3' \neq \tau_3 \), there is some \( i, j, k \) such that \( d_{i,j,k} \neq 0 \), so \( Y' \) has more than one component.

The components of \( Y' \) must be blocks of \( \text{Aut}(\bar{X}) \) as noted above, and hence blocks of its subgroup \( \langle (\mathbb{Z}_p^d)_L, \sigma(\mathbb{Z}_p^d)_L \sigma^{-1} \rangle \), so there must be \( p \), \( p^2 \) or \( p^3 \) of them, by Theorem 1.2.54. We break this portion of the proof down into cases according to the composition of these components.

Let \( G \) be defined as the subgroup of \( \langle (\mathbb{Z}_p^d)_L, \sigma(\mathbb{Z}_p^d)_L \sigma^{-1} \rangle \) that fixes \( X_{0,0,0,0} \).

Notice that any two \( p \)-blocks in the same \( p^2 \)-block are always forced by the action of \( \text{Aut}(\bar{X}) \) to be welded. For let \( i, j, k \) be such that \( d_{i,j,k} \neq 0 \), and let \( \tau' \) be the element of \( \sigma(\mathbb{Z}_p^d)_L \sigma^{-1} \) that takes \( x_{0,0,0,0} \) to \( x_{i,j,k,0} \). Then

\[
\gamma = \tau_1^{-i} \tau_2^{-j} \tau_3^{-k} \tau' \in G
\]

but

\[
\gamma(x_{0,0,1,0}) = \gamma \tau_3'(x_{0,0,0,0}) = \tau_1^{-i} \tau_2^{-j} \tau_3^{-k} \tau_3'(x_{i,j,k,0}) = x_{0,0,1,d_{i,j,k}}.
\]

So the orbit of \( G \) containing \( x_{0,0,1,0} \) is \( B_{0,0,1} \), and by Lemma 2.2.10, \( B_{0,0,0} \) and \( B_{0,0,1} \) are welded. Suppose that for some \( s \), there exists some \( t \) such that \( B_{0,0,t} \) and \( B_{0,0,t+s} \) were not welded. Then by the action of \( \tau_3 \), for any \( t \), \( B_{0,0,t} \) and \( B_{0,0,t+s} \), cannot be welded. But then let \( r \) be such that \( rs \equiv 1 \) (mod \( p \)). Then since \( \gamma \) fixes \( B_{0,0,0} \) pointwise and fixes \( B_{0,0,t} \) setwise for all \( t \), we must have \( \gamma \) fixes \( B_{0,0,s} \) pointwise, so \( \gamma \) fixes \( B_{0,0,2s} \) pointwise, and so on, eventually concluding that \( \gamma \) fixes \( B_{0,0,rs} = B_{0,0,1} \) pointwise, a contradiction that proves the claim with which we began.
this paragraph. This explanation clearly shows that the orbit of \( G \) containing \( x_{0,0,t,0} \) is \( B_{0,0,t} \) for any \( t \), and Lemma 2.2.10 completes the proof of the claim that began this paragraph.

**Case 1.** The components of \( Y' \) are unions of \( p^2 \)-blocks. Notice that since \( B_{0,0,t} \) and \( B_{0,0,t+s} \) are wreathed for any \( s, t \), any path connecting \( B_{0,0,0} \) to \( B_{0,0,1} \) must pass through some \( p \)-block that is not in \( B_{0,0} \). Hence, the components of \( Y' \) must be nontrivial unions of \( p^2 \)-blocks. Since \( Y' \) has more than one component, by Theorem 1.2.54, there must be \( p \) components in \( Y' \), each consisting of a union of \( p \) of the \( p^2 \)-blocks.

Let the component of \( Y' \) containing \( B_{0,0,0} \) be \( C \), and let \( B_{i',j',k'} \subset C \) and \( B_{a',b',c'} \subset C \) be such that \( B_{i',j',k'} \) is adjacent to \( B_{a',b',c'} \) in \( Y' \). Since \( C \) is a block of \( \text{Aut}(\bar{X}) \), \( G \) must fix setwise every \( p^2 \)-block in \( C \). Furthermore, since \( \tau_1^{i'} \tau_2^{j'}(C) \cap C \neq \emptyset \), we must have \( \tau_1^{i'} \tau_2^{j'}(C) = C \), so \( B_{a',b',c'} = B_{ri',rj',rc'} \) for some \( r \). Define \( \tau_{i',j'} \) to be the element of \( \sigma(Z_p) \sigma^{-1} \) that takes \( x_{0,0,0,0} \) to \( x_{i',j',0,0} \).

If the components are the blocks \( B_0, \ldots, B_{p-1} \), then we have \( i' = 0 \) so \( \tau_{i',j'} = (\tau_2^{j'})' \), and clearly \( \tau_1^{-i'} \tau_2^{-j'} \tau_{i',j'} \) must fix every \( p^2 \)-block setwise by Lemma 2.4.1. If, on the other hand, the components are not the blocks \( B_0, \ldots, B_{p-1} \), then each component intersects each \( p^3 \)-block in a unique \( p^2 \)-block. Since \( \tau_{i',j'} \) fixes each component setwise, and takes \( B_a \) to \( B_{a+i'} \) for any \( a \), we must have \( \tau_{i',j'}(B_{a,b}) = B_{a+i',b+j'} \) for any \( a, b \) so again \( \tau_1^{-i'} \tau_2^{-j'} \tau_{i',j'} \) fixes every \( p^2 \)-block setwise.

By Lemma 2.5.2 (stated and proven in the next subsection), notice that since \( B_{i',j',k'} \) is adjacent to \( B_{ri',rj',rc'} \) in \( Y' \), the intersection of the orbit of \( G \) containing the vertex \( x_{s(r-1)i',s(r-1)j',s(c'-k')}0 \) with the block \( B_{s(r-1)i',s(r-1)j',s(c'-k')} \) is a singleton for any \( s \). Since \( C \) is a connected component of \( Y' \), this shows that for any \( s \) there must be at least two \( p \)-blocks \( B_{si',sj',c'} \) and \( B_{si',sj',c'} \) in \( B_{si',sj'} \) such that if \( O \subseteq B_{si',sj'} \) is any orbit of \( G \), then \( |O \cap B_{si',sj',c'}| \leq 1 \) and \( |O \cap B_{si',sj',c'}| \leq 1 \).

Towards a contradiction, suppose that \( G \) fixes all of the \( p \)-blocks in \( B_{si',sj'} \) setwise for some \( s \). Then with the same \( \gamma \) as above, \( \gamma \in G \) so \( \gamma \) must fix every \( p \)-block in \( B_{si',sj'} \) setwise. But then let \( B_{si',sj',c'} \) and \( B_{si',sj',c'} \) be two \( p \)-blocks in \( B_{si',sj'} \) whose vertices form singleton orbits of \( G \). These exist from the argument of the last
paragraph. Clearly, we have
\[ \tau_{1-1}^{-s_{1'}} \tau_{2-1}^{-s_{2'}} \tau_{3}^{-c} \tau_{3}^{c} \tau_{2}^{-s_{2'}} \tau_{1}^{-s_{1'}} = G \]
so \[ \tau_{1-1}^{-s_{1'}} \tau_{2-1}^{-s_{2'}} \tau_{3}^{-c} \tau_{3}^{c} \tau_{2}^{-s_{2'}} \tau_{1}^{-s_{1'}} = G; \]
also, \[ \tau_{1-1}^{-s_{1'}} \tau_{2-1}^{-s_{2'}} \tau_{3}^{-c} \tau_{3}^{c} \tau_{2}^{-s_{2'}} \tau_{1}^{-s_{1'}} = G. \]

But then \( \tau_{3}^{c} \tau_{3}^{c} \tau_{3}^{c} = G. \) and since \( c \neq c' \), we have \( G \) fixing every \( p \)-block in \( B_{0,0} \) pointwise, the desired contradiction. This means that the action of \( G \) cannot force any \( p \)-block within \( C \setminus B_{0,0} \) to be wreathed with \( B_{0,0,0} \).

Again towards a contradiction, suppose that the intersection of the orbit of \( G \) containing the vertex \( x_{a,b,0,0} \) with the block \( B_{a,b} \) were contained in the block \( B_{a,b,0,0} \), where the pairs \((a, b)\) and \((i', j')\) are not collinear when considered as vectors over \( \mathbb{Z}_p \). Then we must have
\[ \tau_{i',j'}(B_{a'+a,b'+b,0}) = \tau_{a,\tau_{2}^{-b},\tau_{1}}(B_{a',b',0}) \]
for any \( a', b' \). Choose \( a' \) such that \( d_{a'+a,b,0} \neq d_{a',0,0} \), and define \( \tau' \) to be the element of \( \sigma(\mathbb{Z}_p^4)L\sigma^{-1} \) that takes \( x_{a',0,0,0} \) to \( x_{a'+a,b,0,0} \). Then \( \tau_{1-1}^{-a} \tau_{2}^{-b} \tau' \) fixes \( x_{a',0,0,0} \) and takes \( \tau_{i',j'}(B_{a',0,0,0}) \) to
\[ \tau_{1-1}^{-a} \tau_{2}^{-b} \tau_{i',j'}(B_{a'+a,b,0,0}) = \tau_{i',j'}(B_{a',0,0,0}). \]
Hence \( \tau_{1-1}^{-a} \tau_{2}^{-b} \tau' \) fixes every \( p \)-block in \( B_{a'+a,b,0} \) setwise. However, because \( d_{a'+a,b,0} \neq d_{a',0,0} \), there must be some \( c' \) such that \( \tau_{1-1}^{-a} \tau_{2}^{-b} \tau' \) does not fix \( B_{a'+i',j',c'} \) pointwise. Since \( \tau_{1-1}^{-a} \tau_{2}^{-b} \tau' \in \tau_{1}^{a'} G \tau_{1}^{-a'} \), we have \( \delta = \tau_{1-1}^{-a} \tau_{2}^{-b} \tau' \tau_{1}^{a} \in G \), and \( \delta \) fixes \( B_{i',j',c'} \) setwise but not pointwise. This contradicts the conclusion of the last paragraph.

Hence the orbit of \( G \) containing the vertex \( x_{a,b,0,0} \) must contain at least one vertex from every \( p \)-block in \( B_{a,b} \), for any \( a, b \) with \( B_{a,b} \notin C \). Let \( C_{a,b} \) be the component of \( Y' \) containing \( B_{a,b} \). Whenever \( C \) and \( C_{a,b} \) are distinct components of \( Y' \), we have that \( B_{0,0,0} \) is wreathed with every \( p \)-block in \( C_{a,b} \), so this means that \( B_{0,0} \) is in fact wreathed with every \( p^2 \)-block in \( C_{a,b} \).

Now we define \( g \) as follows. Let \( \tau_{a,b} \in \sigma(\mathbb{Z}_p^4)L\sigma^{-1} \) be defined to be the element of \( \sigma(\mathbb{Z}_p^4)L\sigma^{-1} \) that maps \( x_{0,0,0,0} \) to \( x_{a,b,0,0} \). Then
\[ g|_{C_{a,b}} = \tau_{1}^{a} \tau_{2}^{b}(\tau_{a,b})^{-1}. \]
It is clear that $g$ fixes every $p^2$-block in $\tilde{X}$ setwise, and that $g|_{C_{a,b}}$ is an automorphism of $\tilde{X}[C_{a,b}]$ for any $a, b$. So the observations of the last paragraph make it clear that $g$ is in fact an automorphism of $\tilde{X}$. Furthermore, since $g$ respects all of the standard block systems, it is not hard to see that $g \in P$.

We certainly have $g$ commutes with $\tau_4$, so it only remains to show that $g\tau'_3g^{-1} = \tau_3$. We have

$$g\tau'_3g^{-1}(x_{i,j,k,l}) = g\tau'_3\tau_{i,j}(x_{0,0,k,l})$$

$$= \tau'_3\tau'_2(\tau_{i,j})^{-1}\tau'_3\tau_{i,j}(x_{0,0,k,l})$$

$$= \tau'_3\tau'_2\tau'_3(x_{0,0,k,l})$$

$$= x_{i,j,k+1,l}$$

since $d_{0,0,k} = d_{0,0,0} = 0$ because $B_{0,0}$ is a subset of $C$. This completes the proof for Case 1.

**Case 2.** The components of $Y'$ meet each $p^2$-block in a unique $p$-block. For each component $C$ of $Y'$, we choose one $p$-block to represent that component. We make this choice in such a way that if we choose one block in $B_{i,j}$ to represent some component, then we choose every block in $B_{i,j}$ to represent some component. It is clear that this can be done if there are just $p$ components, by the case that we are in; in fact, in this case, we choose the representatives to be all of the $p$-blocks in $B_{0,0}$. It is equally clear that this can be done if there are $p^3$ components, since every $p$-block will be a representative in this case. If there are $p^2$ components, and each component is contained within some block $B_i$, then we choose the $p$-blocks in $B_{i,0}$ (over all $i$) to be the $p^2$ representatives. It is clear that these will all represent distinct components. If there are $p^2$ components, and some component $C$ intersects but is not contained in $B_i$, say $\tau'_1\tau'_2\tau'_3(C) \cap C \neq \emptyset$, then since $C$ is a block, $\tau'_1\tau'_2\tau'_3(C) = C$, so $C$ must intersect each block $B_i$ in a single $p$-block. It is easy to see that the same will be true for every component, so in this case, we can choose the representatives to be every $p$-block in $B_0$. Now, if $B_{i,j,k}$ is in the component represented by $B_{i',j',k'}$, then $B_{i',j',k'+1}$ is in the same component as $B_{i,j,k+1}$ by the action of $\tau_3$, and since $B_{i',j',k'}$ is
a representative. \( B_{i',j',k'+1} \) must also be a representative, so it is the representative of the component that contains \( B_{i,j,k+1} \).

Now we define

\[ g^{-1} = \Pi_{i,j,k} \theta_{i,j,k}^{e_{i,j,k}}, \]

where \( e_{i,j,k} = d_{i,j,0} + \ldots + d_{i,j,k-1} \)

if \( B_{i,j,k} \) represents the component of \( Y' \) that contains \( B_{i,j,k} \), and

\[ e_{i,j,k} = e_{i',j',k'} \]

if \( B_{i,j,k} \) is in the component represented by \( B_{i',j',k'} \). In this definition, if \( B_{i,j,0} \) represents a component, then \( e_{i,j,0} = e_{i,j,p} = 0 \).

It is easy to see that \( g \) is an automorphism of \( \tilde{X} \), since \( g \) fixes every \( p \)-block in \( \tilde{X} \) setwise, any \( p \)-blocks in distinct components of \( \tilde{X} \) are wreathed, and \( g| C = \tau_{4}^{e_{i,j,k}}| C \) for any component \( C \) of \( Y' \), where \( e_{i,j,k} \) does not vary within the component.

We certainly have \( g \) commutes with \( \tau_{4} \), so it only remains to show that \( g\tau_{3}^{e_{i,j,k}}g^{-1} = \tau_{3} \). We have

\[ g\tau_{3}^{e_{i,j,k}}g^{-1}(x_{i,j,k,l}) = g\tau_{3}^{e_{i,j,k}+d_{i',j',0}+\ldots+d_{i',j',k'-1}}(x_{i,j,k,l+d_{i',j',0}+\ldots+d_{i',j',k'-1}+d_{i,j,k}}) = x_{i,j,k+1,l} \]

where \( d_{i',j',0} + \ldots + d_{i',j',k'-1} = 0 \) when \( k = 0 \), and \( B_{i,j,k} \) is in the component represented by \( B_{i',j',k'} \), since, as noted above, \( B_{i,j,k+1} \) is in the component represented by \( B_{i',j',k'+1} \). This completes the proof. \( \square \)

### 2.5.2 Orbits of \( G \) when \( \tau_{3} \neq \tau_{3} \)

Let \( G \) be the subgroup of \( \langle (\mathbb{Z}_{p}^{4})_{L}, \sigma(\mathbb{Z}_{p}^{4})_{L}\sigma^{-1} \rangle \) that fixes the vertex \( x_{0,0,0,0} \). For the purposes of this lemma, we assume that \( \tau_{4} \) is in both \( \sigma(\mathbb{Z}_{p}^{4})_{L}\sigma^{-1} \) and \( (\mathbb{Z}_{p}^{4})_{L} \); we also assume that \( \tau_{3} \neq \tau_{3} \). Let \( C' \) be any block of \( \langle (\mathbb{Z}_{p}^{4})_{L}, \sigma(\mathbb{Z}_{p}^{4})_{L}\sigma^{-1} \rangle \) that is a union of
the $p^2$-blocks $B_{i,j}$ that are formed by the orbits of $(\tau_3, \tau_4)$. Let $C$ be the complete block system generated by $C'$. and let $C \in C$ be such that $B_{0,0} \in C$. Since $C$ is a block of $\langle (\mathbb{Z}_p^4)_{L}, \sigma(\mathbb{Z}_p^4)L\sigma^{-1} \rangle$, it is clear that $C$ must have the form

$$\{\tau_1^{r'}\tau_2^{r''}(B_{0,0}) : 0 \leq r \leq p-1\}$$

for some $i', j'$.

Let $\{d_{i,j,k} : 0 \leq i, j, k \leq p-1\}$ be defined by $\tau_3^t(x_{i,j,k,0}) = x_{i,j,k+1,d_{i,j,k}}$. Then we further assume in what follows that $d_{i,j,k}$ depends only on $i$ and $j$, and we commonly denote $d_{i,j,k}$ by $d_{i,j}$.

**Lemma 2.5.2** Suppose that the intersection of the orbit $O$ of $G$ that contains $x_{r',r'',k',0}$ with the block $B_{r',r'',k'}$ is the entire block $B_{r',r'',k'}$. Then the intersection of the orbit of $G$ that contains $x_{r's',r's'',k's'}$ with the block $B_{r's',r's'',k's'}$ will be the entire block $B_{r's',r's'',k's'}$ for any $s \neq 0$, meaning that $B_{s't',s't'',s't'}$ and $B_{t't',t't'',t't'}$ must be wreathed for any $s, t$ with $s \neq t$.

**Proof.** We break the proof of this lemma down into two cases.

**Case 1.** The orbit $O$ is precisely the block $B_{r',r'',k'}$. We begin by proceeding by induction to prove that the orbit of $G$ containing the vertex $x_{r's',r's'',k's'}$ is contained within the block $B_{r's',r's'',k's'}$. The base case is given by the assumption of Case 1, so we assume the result to be true for $x_{r's',r's'',k's'}$ and prove it for $x_{r(s+1)i',r(s+1)j',r(s+1)k',0}$.

Let $\theta$ be any element of $G$. Then by our induction hypothesis,

$$\theta(x_{r's',r's'',k's'}) = x_{r's',r's'',k's',l}$$

for some $l$. Hence,

$$\tau_4^{-l}\theta \in \tau_1^{r's'_{1}}\tau_2^{r's'_{2}}\tau_3^{sk'}G_{r's'}\tau_2^{-r's'_{1}}\tau_1^{-r's'}.$$ 

It is clear from the Case 1 assumption that the orbit of $\tau_1^{r's'_{1}}\tau_2^{r's'_{2}}\tau_3^{sk'}G_{r's'}\tau_2^{-r's'_{1}}\tau_1^{-r's'}$ that contains the vertex $x_{r(s+1)i',r(s+1)j',r(s+1)k',0}$ must be contained within the block $B_{r(s+1)i',r(s+1)j',(s+1)k'}$. Thus,

$$\tau_4^{-l}\theta(x_{r(s+1)i',r(s+1)j',(s+1)k',0}) = x_{r(s+1)i',r(s+1)j',(s+1)k',0}$$
for some \( l' \). But this means that

\[
\theta(x_{r(s+1)i',r(s+1)j',(s+1)k',0}) = x_{r(s+1)i',r(s+1)j',(s+1)k',l+l'} \in B_{r(s+1)i',r(s+1)j',(s+1)k'}.
\]

Since \( \theta \) was an arbitrary element of \( G \), this completes the induction.

The only possibility remaining to be eliminated is that for some \( s \neq 0 \), the orbit of \( G \) containing \( x_{rsi',rjs',sk',0} \) is the singleton \( \{ x_{rsi',rjs',sk',0} \} \). Then we can use an inductive argument precisely like the one above to show that the orbit of \( G \) containing \( x_{rsi',rjs',sk',0} \) must be the singleton \( \{ x_{rsi',rjs',sk',0} \} \) for any \( s' \). Since we are working modulo \( p \), we can choose \( s' \) such that \( ss' = 1 \). But then the orbit of \( G \) containing \( x_{rsi',rjs',sk',0} \) is the singleton \( \{ x_{rsi',rjs',sk',0} \} \), a contradiction.

This yields the result.

Case 2. The orbit \( O \) strictly contains the block \( B_{ri',rj',k'} \). Since \( C \) is a block containing \( p \) blocks of size \( p^2 \), and \( G \) fixes \( B_{0,0} \in C \) setwise, \( G \) must fix \( B_{ri',rj'} \) setwise. So the orbit \( O \) must in fact be the entire block \( B_{ri',rj'} \). If \( p = 2 \) then we are done. trivially, so in what follows, we assume \( p > 2 \).

Suppose that for some \( s \), the orbit \( O' \) of \( G \) containing \( x_{rsi',rjs',sk',0} \) were not the entire block \( B_{rsi',rjs'} \). If this orbit were a singleton, or \( O' = B_{rsi',rjs',sk'} \), then we could use the arguments of Case 1 to arrive at a contradiction. The possibility remains that \( O' \) has length \( p \) and meets each block \( B_{rsi',rjs',c} \) in a single vertex.

Now, since \( \tau_3' \neq \tau_3 \), there exists some \( i, j \) such that \( d_{i,j} \neq 0 \). Define \( \tau' \) to be the element of \( \sigma(Z_p^*) \cdot \sigma^{-1} \) that maps \( x_{0,0,0,0} \) to \( x_{i,j,0,0} \). Then

\[
\delta = \tau_1^{-i} \tau_2^{-j} \tau' \in G.
\]

Now, suppose that

\[
\delta(B_{rsi',rjs',sk'}) = B_{rsi',rjs',sk'}
\]

If \( \delta(x_{rsi',rjs',sk',0}) \neq x_{rsi',rjs',sk',0} \),
then $O'$ must contain all of $B_{rsi',rsj',sk',0}$, contradicting our assumptions about this orbit. So we may assume that

$$\delta(x_{rsi',rsj',sk',0}) = x_{rsi',rsj',sk',0}. $$

But then we have

$$\delta(x_{0,0,1,0}) = \tau_1^{-i} \tau_2^{-j} \tau_3^{-1}(x_{i,j,0,0})$$

$$= x_{0,0,1,d_{i,j}}.$$  

This means that $\tau_4^{-d_{i,j}} \tau_3^{-1} \delta \tau_3 \in G$, but

$$\tau_4^{-d_{i,j}} \tau_3^{-1} \delta \tau_3(x_{rsi',rsj',sk'-1,0}) = \tau_4^{-d_{i,j}} \tau_3^{-1}(x_{rsi',rsj',sk',0})$$

$$= x_{rsi',rsj',sk'-1,-d_{i,j}}.$$  

This means that the entire block $B_{rsi',rsj',sk'-1}$ must be in the orbit $O'$ (since $O'$ intersects every $p$-block in $B_{rsi',rsj'}$). This again contradicts our assumptions about this orbit.

The only remaining possibility is that

$$\delta(B_{rsi',rsj',sk'}) \neq B_{rsi',rsj',sk'}.$$  

Let us say that

$$\delta(x_{rsi',rsj',sk',0}) = x_{rsi',rsj',sk'+k,l_1}$$

where $k \neq 0$. Then since $\delta(x_{0,0,k,0}) = x_{0,0,k,d_{i,j}}$, we have

$$\delta' = \tau_4^{-kd_{i,j}} \tau_3^{-k} \delta \tau_3^{k} \in G.$$  

Since $\delta$ is in a $p$-group that fixes $B_{rsi',rsj'}$ setwise, we must have

$$\delta(B_{rsi',rsj',c}) = B_{rsi',rsj',c+k}$$

for every $c$. The same is true of $\delta'$ by the same argument. So we must have

$$\delta'(x_{rsi',rsj',sk',0}) = x_{rsi',rsj',sk'+k,l_1},$$

meaning that $\delta(x_{rsi',rsj',sk'+k,l_1}) = x_{rsi',rsj',sk'+2k,2l_1+d_{i,j}}$. 
Continuing in this fashion, we can calculate that

$$O' \cap B_{rs'i',rs'j',as'k',0} = \{x_{rs'i',rs'j',as'k',0} + tk : 0 \leq t \leq p - 1\}.$$  

We proceed by induction to show that the orbit of $G$ containing the vertex $x_{rs'i',rs'j',as'k',0}$ must have length $p$ and meet each $p$-block in $B_{rs'i',rs'j',as'k'}$ in a single point. Before we begin, notice that if this orbit is contained within the block $B_{rs'i',rs'j',as'k'}$ then we can return to Case 1, and obtain a contradiction. So the only way the induction can fail is if the orbit of $G$ containing $x_{rs'i',rs'j',as'k',0}$ is the entire block $B_{rs'i',rs'j'}$. Notice that whenever the induction hypothesis is true, the preceding arguments hold, so the orbit will take the form

$$\{x_{rs'i',rs'j',as'k',0} + tk : 0 \leq t \leq p - 1\},$$

for some fixed $k$ and $l_i$.

The base case is done, so the last sentence of the preceding paragraph forms our induction hypothesis. Now, let $\theta$ be any element of $G$. Then

$$\theta(x_{rs'i',rs'j',as'k',0}) = x_{rs'i',rs'j',as'k',0} + tk, \text{ for some } t.$$  

So

$$\theta' = r_{l_i}^{-1} - r_{l_{i+1}}^{-1} + [t - 1] k d_{i,j} \theta$$

fixes $x_{rs'i',rs'j',as'k',0}$. Hence (by the base case) we must have

$$\theta'(x_{rs(s'+1)i',rs(s'+1)j',as(s'+1)k',0}) = x_{rs(s'+1)i',rs(s'+1)j',as(s'+1)k',0} + tk, t_{i+1} + [t - 1] k d_{i,j}$$

for some fixed $l_{i+1}$ and some $t_2$. This means that

$$\theta(x_{rs(s'+1)i',rs(s'+1)j',as(s'+1)k',0}) = x_{rs(s'+1)i',rs(s'+1)j',as(s'+1)k',0} + [t_1 + t_2] k d_{i,j} / 2.$$  

Now, the only way in which the induction can fail, as noted earlier, is if the orbit of $G$ in $B_{rs'i',rs'j'}$ has length $p^2$. Our above calculations show that for each of the $p$ possible images of $x_{rs'i',rs'j',as'k',0}$ under $\theta$, there are $p$ possible images
of $x_{rs(s'+1)i',rs(s'+1)j',s(s'+1)k',0}$. Since $\theta$ is an arbitrary element of $G$, in order for the orbit of $G$ containing $x_{rs(s'+1)i',rs(s'+1)j',s(s'+1)k',0}$ to have length $p^2$, all of these images would have to be distinct. We will show that the images are not all distinct, thus completing the induction.

Choose $t_2$ arbitrarily, and let

$$t_1' = t_2 + (l_{s'+1} - l_s)/(kd_{i,j}).$$

Choose $t_1$ in such a way that $t_1 \neq t_1'$. and let

$$t_2' = t_1 - (l_{s'+1} - l_s)/(kd_{i,j}).$$

Then we claim that

$$x_{rs(s'+1)i',rs(s'+1)j',s(s'+1)k' + (t_1 + t_2)k,l_{s'+1} + [t_1 (s'-1) + t_2 (s'-1)]kd_{i,j}/2}$$

$$= x_{rs(s'+1)i',rs(s'+1)j',s(s'+1)k' + (t_1' + t_2')k,l_{s'+1} + [t_1' (s'-1) + t_2' (s'-1)]kd_{i,j}/2}.$$

It is clear that each of the first three subscripts are the same; tedious calculations (performed below) verify that the fourth subscript will also be the same. These calculations will complete the induction, and the conclusion of the induction contradicts our assumption that the orbit of $G$ containing $x_{ri',rj',k',0}$ is the entire block $B_{ri',rj'}$. Thus, the calculations will complete the proof of this lemma.

We will use the equation $t_1 + t_2 = t_1' + t_2'$ repeatedly in the following calculations.
We have
\[
\begin{align*}
t_1 l_s' + t_2 l_{s+1} &+ \frac{[t_1(t_1 - 1) + t_2(t_2 - 1)]kd_{i,j}}{2} \\
&= t_1' l_{s'} + t_2' l_{s'+1} + (t_1 - t_1')l_s' + (t_2 - t_2')l_{s+1} + \frac{[t_1'(t_1' - 1) + t_2'(t_2' - 1)]kd_{i,j}}{2} \\
&+ [t_1(t_1 - 1) + t_2(t_2 - 1) - t_1'(t_1' - 1) - t_2'(t_2' - 1)]kd_{i,j} \\
&= t_1' l_{s'} + t_2' l_{s'+1} + \frac{[t_1'(t_1' - 1) + t_2'(t_2' - 1)]kd_{i,j}}{2} + (t_1 - t_1')l_s' - (t_1 - t_1')l_{s+1} \\
&+ \frac{[(t_1^2 + t_2^2) - (t_1')^2 - (t_2')^2]kd_{i,j}}{2} \\
&= t_1' l_{s'} + t_2' l_{s'+1} + \frac{[t_1'(t_1' - 1) + t_2'(t_2' - 1)]kd_{i,j}}{2} + (t_1 - t_1')(l_{s'} - l_{s'+1}) \\
&+ \frac{[(t_1 + t_1')(t_1 - t_1') + (t_2 + t_2')(t_2 - t_2')]kd_{i,j}}{2} \\
&= t_1' l_{s'} + t_2' l_{s'+1} + \frac{[t_1'(t_1' - 1) + t_2'(t_2' - 1)]kd_{i,j}}{2} + (t_1 - t_1')(l_{s'} - l_{s'+1}) \\
&+ \frac{(t_1 + t_1' - t_2 - t_2')(t_1 - t_1')kd_{i,j}}{2} \\
&= t_1' l_{s'} + t_2' l_{s'+1} + \frac{[t_1'(t_1' - 1) + t_2'(t_2' - 1)]kd_{i,j}}{2} + (t_1 - t_1')(l_{s'} - l_{s'+1}) \\
&+ \frac{2(t_1 - t_2')(t_1 - t_1')kd_{i,j}}{2} \\
&= t_1' l_{s'} + t_2' l_{s'+1} + \frac{[t_1'(t_1' - 1) + t_2'(t_2' - 1)]kd_{i,j}}{2} + (t_1 - t_1')(l_{s'} - l_{s'+1}) \\
&+ \frac{(l_{s'+1} - l_{s'})(t_1 - t_1')}{2} \\
&= t_1' l_{s'} + t_2' l_{s'+1} + \frac{[t_1'(t_1' - 1) + t_2'(t_2' - 1)]kd_{i,j}}{2}.
\end{align*}
\]

As noted, this completes the proof. \qed
2.6 Conjugation of $\sigma(Z_p^4)_L \sigma^{-1}$ to Obtain a Group that Contains $\tau_2$

2.6.1 Finding the conjugate $\phi \sigma(Z_p^4)_L \sigma^{-1} \phi^{-1}$

Lemma 2.6.1 Let $\sigma(Z_p^4)_L \sigma^{-1}$ be any conjugate of $(Z_p^4)_L$ such that $\sigma(Z_p^4)_L \sigma^{-1} \leq P$, where $P$ is a fixed Sylow $p$-subgroup of $\text{Aut}(\bar{X})$ that contains $(Z_p^4)_L$, and $\tau_3, \tau_4 \in \sigma(Z_p^4)_L \sigma^{-1}$. Then there exists some $\phi \in P$ such that $\phi \sigma(Z_p^4)_L \sigma^{-1} \phi^{-1}$ contains $\tau_2, \tau_3$ and $\tau_4$.

Proof. We consider the element $\tau'_2$ of $\sigma(Z_p^4)_L \sigma^{-1}$ satisfying $\tau'_2(x_{0,0,0,0}) = x_{0,1,0,0}$. By Lemma 2.4.1, $\tau'_2(B_{i,j}) = B_{i,j+1}$ for all $i, j$. If

$$\tau'_2(x_{i,j,k,l}) = x_{i,j+1,k+a_{i,j},l+b_{i,j}},$$

$$\tau'_2(x_{i,j,k',l'}) = x_{i,j+1,k'+a_{i,j},l'+b_{i,j}};$$

that is, the action of $\tau'_2$ is completely determined by the pairs $(a_{i,j}, b_{i,j})$ over all $i, j$.

For any $i, j$, define $a_{i,j}$ and $b_{i,j}$ to be such that

$$\tau'_2(x_{i,j,0,0}) = x_{i,j+1,a_{i,j},b_{i,j}}.$$

Let $G$ be the subgroup of $\langle (Z_p^4)_L, \sigma(Z_p^4)_L \sigma^{-1} \rangle$ consisting of all elements that fix the vertex $x_{0,0,0,0}$.

We break this section of the proof down into several cases. Define the auxiliary graph $Y'$ whose vertices are the blocks $B_{i,j}$, where $B_{i,j}$ is adjacent to $B_{a,b}$ in $Y'$ if and only if $B_{i,j}$ is not wreathed with $B_{a,b}$.

We assume that $\tau'_2 \neq \tau_2$, since otherwise we would be done and could move on to considering $\tau'_i$.

Case 1. The graph $Y'$ has more than one component. For each component of this graph, we will choose a representative block in what follows.

Subcase (a). The blocks $B_0, B_1, \ldots, B_{p-1}$ are the components of $Y'$. Let $\tau'_{2,j} \in \sigma(Z_p^4)_L \sigma^{-1}$ be the element taking $x_{0,0,0,0}$ to $x_{0,i,0,0}$ for any $j \neq 0$. Then there
exist $a, b$ such that

$$\tau'_{2,j}(x_{a,b,0,0}) = x_{a,b+j,c,d} \neq x_{a,b,0,0}.$$ 

(Otherwise if $k$ is such that $kj \equiv 1 \pmod{p}$, then $(\tau'_{2,j})^k = \tau'_{2,j}$, so for any $a, b$, we have

$$\tau'_{2,j}(x_{a,b,0,0}) = (\tau'_{2,j})^k(x_{a,b,0,0})$$

$$= x_{a,b+1,0,0}.$$ 

contradicting the assumption that $\tau'_{2,j} \neq \tau_{2,j}$.)

Let $\tau'$ be the element of $\sigma(\mathbb{Z}_p^d)\sigma^{-1}$ taking $x_{0,0,0,0}$ to $x_{a,b,0,0}$. Then $\tau'$ and $\tau'_{2,j}$ commute, so

$$\tau_1^{-a} \tau_2^{-b} \tau'(x_{0,0,0,0}) = \tau_1^{-a} \tau_2^{-b} \tau'_{2,j}(x_{a,b,0,0})$$

$$= x_{0,j,c,d}$$

$$\neq x_{0,j,0,0}.$$ 

Hence the orbit of $G$ containing $x_{0,j,0,0}$ is the set

$$\{x_{0,j,kc,kd} : 0 \leq k \leq p-1\}.$$ 

By Lemma 2.6.5 (stated and proven later), $c$ and $d$ do not depend on $j$; furthermore, $c$ and $d$ are independent of the choice of $a, b$.

Let $\phi$ be defined by

$$\phi^{-1}(x_{i,j,k,l}) = \tau_3^{e_{i,j}} \tau_4^{f_{i,j}}(x_{i,j,k,l}),$$

where

$$e_{i,j} = a_{i,0} + \ldots + a_{i,j-1}$$

and

$$f_{i,j} = b_{i,0} + \ldots + b_{i,j-1}.$$ 

Here $e_{i,0} = 0 = f_{i,0}$. Then $\phi$ is an automorphism of $\tilde{X}$. To see this, we note that $\phi$ fixes all $p^2$-blocks setwise, so by the definition of $Y'$, we need only verify that $\phi$
is an automorphism within each component. Suppose, therefore, that there is a red arc from \(x_{i,j,k,l}\) to \(x_{i,j',k',l'}\). We have

\[
\phi^{-1}(x_{i,j,k,l}) = x_{i,j,k+a_i,0+\ldots+a_{i,j-1},l+b_i,0+\ldots+b_{i,j-1}} \quad \text{and} \quad \phi^{-1}(x_{i,j'+k',l'}) = x_{i,j'+k'+a_i,0+\ldots+a_{i,j'+k'-1},l'+b_i,0+\ldots+b_{i,j'+k'-1}}.
\]

So in order to show that \(\phi\) is an automorphism, we need only show that there is a red arc from \(x_{i,j,k,l}\) to

\[
x_{i,j'+k'+a_i,0+\ldots+a_{i,j'+k'-1},l'+b_i,0+\ldots+b_{i,j'+k'-1}}.
\]

Notice that \(\tau'_{2,1} = \tau'_2\), and by the independence of \(c, d\) from the choice of \(a, b\), we see that \((a_{i,j+k''}, b_{i,j+k''})\) is collinear with \((c, d)\) for any \(j''\). Hence

\[
x_{i,j+k',k'+a_i,j+a_{i,j+k'-1},l'+b_i,0+\ldots+b_{i,j+k'-1}} = x_{i,j+k'+c_i,l'+rd} \in \{x_{i,j+k'+c_i,l'+rd} : 0 \leq r \leq p-1\}.
\]

Since we already know that the orbit of \(x_{i,j+k',k''}\) under the action of \(\tau'_1 \tau'_2 \tau'_{-1}\) is the set

\[
\{x_{i,j+k',k'+c_i,l'+rd} : 0 \leq r \leq p-1\},
\]

the existence of a red arc from \(x_{i,j,k,l}\) to \(x_{i,j+k',k''}\) implies the existence of a red arc from \(x_{i,j,k,l}\) to

\[
x_{i,j+k',k'+a_i,j+a_{i,j+k'-1},l'+b_i,0+\ldots+b_{i,j+k'-1}}.
\]

Hence \(\phi\) is indeed an automorphism.

Now,

\[
\phi \tau'_2 \phi^{-1}(x_{i,j,k,l}) = \phi \tau'_2(\phi(x_{i,j,k+a_i,0+\ldots+a_{i,j-1},l+b_i,0+\ldots+b_{i,j-1}})) = \phi(x_{i,j+1,k+a_i,0+\ldots+a_{i,j-1},l+b_i,0+\ldots+b_{i,j}}) = x_{i,j+1,k,l} = \tau_2(x_{i,j,k,l}).
\]

So \(\phi \tau'_2 \phi^{-1} = \tau_2\), as required, and we have completed Subcase (a).

**Subcase (b).** The components of \(Y'\) are not the blocks \(B_0, B_1, \ldots, B_{p-1}\). If \(B_{i,j}\) and \(B_{i,j'+k'}\) are in the same component for any values of \(j, j'\), then by the action of
we have $B_{0,k}$ and $B_{0,k+j}$ are in the same component for every value of $k$. But then every block in $B_0$ is in the same component of $Y'$, and since $Y'$ has more than one component, it is clear that the components must be $B_0, \ldots, B_{p-1}$, a contradiction. So we see that in this case, any two $p^2$-blocks in $B_0$ are in distinct components of $Y'$.

Now, $Y'$ has either $p$ or $p^2$ components, by Theorem 1.2.54. If there are $p$ components, let them be represented by the blocks $B_{0,0}, B_{0,1}, \ldots, B_{0,p-1}$. If there are $p^2$ components, then every $p^2$-block represents itself.

Define $\phi$ by

$$\phi^{-1}(x_{i,j,k,l}) = \tau_3^{e_{i,j}} \tau_4^{f_{i,j}}(x_{i,j,k,l}),$$

where

$$e_{i,j} = a_{i,0} + \ldots + a_{i,j-1}$$

and $f_{i,j} = b_{i,0} + \ldots + b_{i,j-1}$

and if $j = 0$, $e_{i,j} = 0 = f_{i,j}$ if $B_{i,j}$ serves as a representative for some component of $Y'$, while

$$e_{i,j} = e_{0,b} + a_{0,b} - a_{i,j}$$

and $f_{i,j} = f_{0,b} + b_{0,b} - b_{i,j}$

otherwise, where $b$ is such that $B_{i,j}$ is in the component represented by $B_{0,b}$.

First we show that $\phi$ is an automorphism. Suppose that there is a red arc from $x_{i,j,k,l}$ to $x_{a,b,c,d}$. If $B_{i,j}$ and $B_{a,b}$ are in the same component of $Y'$, suppose first that $(i, j) = (a, b)$. Then the image of this arc under $\phi$ is the same as its image under $\tau_3^{e_{i,j}} \tau_4^{b_{i,j}}$, and thus a red arc of $\tilde{X}$. So we assume that $(i, j) \neq (a, b)$. Since no two $p^2$-blocks in the same $p^3$-block are in the same component of $Y'$, we know that $i \neq a$.

Now,

$$\phi^{-1}(x_{i,j,k,l}) = x_{i,j,k+a_{0,0} + \ldots + a_{0,\nu} + a_{0,\nu} - a_{i,j}, l+b_{0,0} + \ldots + b_{0,\nu} - b_{i,j}}$$

where $B_{0,b'}$ is the block representing the component of $Y'$ that contains both $B_{i,j}$ and $B_{a,b}$. Also,

$$\phi^{-1}(x_{a,b,c,d}) = x_{a,b,c+a_{0,0} + \ldots + a_{0,\nu} - a_{a,b}, d+b_{0,0} + \ldots + b_{0,\nu} - b_{a,b}}.$$

So in order to show that $\phi$ is an automorphism, we need only show that there is a red arc from $x_{i,j,k,l}$ to $x_{a,b,c-a_d,b+1,j,d-b_a,b+d}$. Notice that these vertices are precisely the images of $x_{i,j,k,l}$ and $x_{a,b,c,d}$ under $\tau_3^{a_d} \tau_4^{b_1}(\tau_2')^{-1} \tau_2$. This is sufficient.

If $B_{i,j}$ and $B_{a,b}$ are in different components of $Y'$, then $B_{i,j}$ and $B_{a,b}$ are wreathed and both fixed setwise by $\phi$, so the image of the arc is again clearly another red arc. Thus $\phi$ is an automorphism. It is clear that $\phi$ conjugates both $\tau_3$ and $\tau_4$ to themselves.

Now we show that $\phi \tau_2' \phi^{-1} = \tau_2$. If every block is its own representative, then

$$
\phi \tau_2' \phi^{-1}(x_{i,j,k,l}) = \phi \tau_2'(x_{i,j,k+a_1,0+...+a_{i,j-1},l+b_0,0+...+b_{i,j-1}})
= \phi(x_{i,j+1,k+a_1,0+...+a_{i,j},l+b_0,0+...+b_{i,j}}) \\
= x_{i,j+1,k,l}
= \tau_2(x_{i,j,k,l})
$$

and we are done.

Otherwise, if there are $p$ components, we have

$$
\phi \tau_2' \phi^{-1}(x_{i,j,k,l})
= \phi \tau_2'(x_{i,j,k+a_0,0+...+a_0,0'-1+a_0,0'-a_{i,j},l+b_0,0+...+b_0,0'-1+b_0,0'-b_{i,j}}),
$$

where $B_{i,j}$ is in the block represented by $B_{0,0'}$. This is

$$
= \phi(x_{i,j+1,k+a_0,0+...+a_0,0',l+b_0,0+...+b_0,0'})
= x_{i,j+1,k,l},
$$

since $B_{i,j+1}$ is in the component represented by $B_{0,0'}$. This is true for the following reason. If $B_{i,j}$ is in the component represented by $B_{0,b}$, then the action of $\tau_2$ on the components of $Y'$ shows that $B_{i,j+1}$ is in the component represented by $B_{0,b+1}$. This completes Case 1.

**Case 2.** The graph $Y'$ has only one component. Hence, there are at least two linearly independent vectors $(\alpha_1, \alpha_2)$ and $(\beta_1, \beta_2)$ such that neither $B_{a_1, a_2}$ nor
$B_{\beta_1,\beta_2}$ is forced by the action of $\langle (\mathbb{Z}_p^4)_L, \sigma(\mathbb{Z}_p^4) \rangle_{L^2}^{-1}$ to be wreathed with $B_{0,0}$. Let the intersection of the orbit of $x_{a_1,a_2,0,0}$ under $G$ with the block $B_{a_1,a_2}$ be the set
\[ \{x_{a_1,a_2,ka_1,a_2,kb_1,a_2} : 0 \leq k \leq p-1 \}, \]
and the intersection of the orbit of $x_{\beta_1,\beta_2,0,0}$ under $G$ with the block $B_{\beta_1,\beta_2}$ be the set
\[ \{x_{\beta_1,\beta_2,ka_1,\beta_2,kb_1,\beta_2} : 0 \leq k \leq p-1 \}. \]

Subcase (a). The vectors $(a_{a_1,a_2}, b_{a_1,a_2})$ and $(a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2})$ are linearly dependent. Then by Lemma 2.6.7 (stated and proven later), there is an appropriate conjugate of $\tau_2'$ and we can proceed to consider $\tau_2''$.

Subcase (b). The vectors $(a_{a_1,a_2}, b_{a_1,a_2})$ and $(a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2})$ are linearly independent. Suppose there is a third vector $(\gamma_1, \gamma_2)$ such that $B_{\gamma_1,\gamma_2}$ is not forced by the action of $\langle (\mathbb{Z}_p^4)_L, \sigma(\mathbb{Z}_p^4) \rangle_{L^2}^{-1}$ to be wreathed with $B_{0,0}$ and $(\gamma_1, \gamma_2)$ is not collinear with either $(\alpha_1, \alpha_2)$ or $(\beta_1, \beta_2)$. Let $a_{\gamma_1,\gamma_2}, b_{\gamma_1,\gamma_2}$ be such that the intersection of the orbit of $x_{\gamma_1,\gamma_2,0,0}$ under $G$ with the block $B_{\gamma_1,\gamma_2}$ is the set
\[ \{x_{\gamma_1,\gamma_2,ka_{\gamma_1,\gamma_2},kb_{\gamma_1,\gamma_2}} : 0 \leq k \leq p-1 \}. \]
Then by Lemma 2.6.6 (stated and proven later), $(a_{\gamma_1,\gamma_2}, b_{\gamma_1,\gamma_2})$ must be collinear with either $(a_{a_1,a_2}, b_{a_1,a_2})$ or $(a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2})$. So we use the two collinear vectors in Lemma 2.6.7 to find an appropriate conjugate of $\tau_2''$.

Thus we may assume that for any vector $(\gamma_1, \gamma_2)$ such that $(\gamma_1, \gamma_2)$ is not collinear with either $(\alpha_1, \alpha_2)$ or $(\beta_1, \beta_2)$, the action of $\langle (\mathbb{Z}_p^4)_L, \sigma(\mathbb{Z}_p^4) \rangle_{L^2}^{-1}$ must force $B_{0,0}$ and $B_{\gamma_1,\gamma_2}$ to be wreathed.

Suppose that one of $\alpha_1, \beta_1$ is 0. They cannot both be 0 since the vectors $(\alpha_1, \alpha_2)$ and $(\beta_1, \beta_2)$ are linearly independent. Without loss of generality, we assume $\alpha_1 = 0$.

In this case, we define $\phi$ as follows:
\[ \phi \text{ commutes with } \tau_3 \text{ and } \tau_4; \]
\[ \phi^{-1}(x_{s\beta_1, s\beta_2,0,0}) = x_{s\beta_1, s\beta_2,0,0} \text{ for any } s, \text{ and} \]
\[ \phi^{-1}(x_{s\beta_1, s\beta_2+t,0,0}) = (\tau_2')^s \phi^{-1}(x_{s\beta_1, s\beta_2,0,0}) \text{ for all } s, t. \]
We demonstrate that $\phi$ is an automorphism in this case. Suppose that there is a red arc from the vertex $x_{s\beta_1, s\beta_2 + t, c, d}$ to the vertex $x_{s'\beta_1, s'\beta_2 + t', k, l}$. We will show that there is a red arc from $\phi^{-1}(x_{s\beta_1, s\beta_2 + t, c, d})$ to the vertex $\phi^{-1}(x_{s'\beta_1, s'\beta_2 + t', k, l})$. If $s = s'$ and $t = t'$, then the result is clear since $\phi$ commutes with $\tau_3$ and $\tau_4$.

Suppose there is some $y_1, y_2$ such that

$$\tau'_2(x_{y_1, y_2, a, 0}) \notin \{x_{y_1, y_2 + 1, ra_1, a_2, rb_1, a_2} : 0 \leq r \leq p - 1\}.$$  

Then let $\tau'$ be the element of $\sigma(Z)^G \sigma^{-1}$ taking $x_{0, 0, 0, 0}$ to $x_{y_1, y_2, 0, 0}$. Since $\tau'_2$ and $\tau'$ commute, we have

$$\tau'(x_{0, 1, 0, 0}) \notin \{x_{y_1, y_2 + 1, ra_1, a_2, rb_1, a_2} : 0 \leq r \leq p - 1\}.$$  

But then $\tau_2^{-1}x_{y_1, y_2} \tau_2^{-1} \tau' \in G$ and

$$\tau_2^{-1}x_{y_1, y_2} \tau'_2 (x_{0, 1, 0, 0}) \notin \{x_{0, 1, ra_1, a_2, rb_1, a_2} : 0 \leq r \leq p - 1\}.$$  

This contradicts the composition of the known orbit of $x_{0, 1, 0, 0}$ under $G$. So for any $y_1, y_2$, we have

$$\tau'_2(x_{y_1, y_2, 0, 0}) \in \{x_{y_1, y_2 + 1, ra_1, a_2, rb_1, a_2} : 0 \leq r \leq p - 1\}.$$  

If $s = s'$ and $t \neq t'$, then we have

$$\phi^{-1}(x_{s\beta_1, s\beta_2 + t, c, d}) = (\tau'_2)^t(x_{s\beta_1, s\beta_2, c, d}) \text{ and}$$

$$\phi^{-1}(x_{s\beta_1, s\beta_2 + t', k, l}) = (\tau'_2)^t(x_{s\beta_1, s\beta_2, k, l}).$$  

By the argument of the last paragraph together with the known orbits of $x_{0, t'-t, k-c, l-d}$ under $G$, it is clear that there must be a red arc from the first of these vertices to the second.

The case remains that $s \neq s'$. In this case, the blocks $B_{s\beta_1, s\beta_2 + t}$ and $B_{s'\beta_1, s'\beta_2 + t'}$ are wreathed and we are done unless $t = t'$. In this case, we have

$$\phi^{-1}(x_{s\beta_1, s\beta_2 + t, c, d}) = (\tau'_2)^t(x_{s\beta_1, s\beta_2, c, d}) \text{ and}$$

$$\phi^{-1}(x_{s'\beta_1, s'\beta_2 + t, k, l}) = (\tau'_2)^t(x_{s'\beta_1, s'\beta_2, k, l}).$$
There is clearly a red arc from the first of these vertices to the second.

Hence \( \phi \) is an automorphism. Demonstrating that \( \phi \) conjugates \( \tau_2 \) appropriately is the same in this case as in the case that follows, so we will make the argument subsequently.

So in what follows, we assume that \( \alpha_1, \beta_1 \neq 0 \). Hence all of the \( p^2 \)-blocks in any \( p^3 \)-block must be wreathed. Let \( r \) be such that \( r\beta_1 = \alpha_1 \).

For any \( m \), define \( k_m \) and \( k'_m \) to be the unique values satisfying the equation
\[
\begin{align*}
k_m(a_{\alpha_1, \alpha_2}, b_{\alpha_1, \alpha_2}) + (a_{m\alpha_1, m\alpha_2} + \ldots + a_{m\alpha_1, m\alpha_2}, b_{m\alpha_1, m\alpha_2} + \ldots + b_{m\alpha_1, m\alpha_2}) &= k'_m(a_{\beta_1, \beta_2}, b_{\beta_1, \beta_2}).
\end{align*}
\]

Define the function \( \phi \) as follows:
\[
\begin{align*}
\phi \text{ commutes with } \tau_3 \text{ and } \tau_4; \\
\phi(x_{s\alpha_1, s\alpha_2, 0, 0}) = x_{s\alpha_1, s\alpha_2, k_s a_{\alpha_1, \alpha_2}, k_s b_{\alpha_1, \alpha_2}} \text{ for all } s; \text{ and} \\
\phi(x_{s\alpha_1, s\alpha_2 + t, 0, 0}) = (\tau_2)^t \phi(x_{s\alpha_1, s\alpha_2, 0, 0}) \text{ for all } s, t.
\end{align*}
\]

Note that \( \phi \) fixes every \( p^2 \)-block setwise.

First we show that \( \phi \) is an automorphism of \( \bar{X} \). Suppose that there is a red arc from \( x_{s\alpha_1, s\alpha_2 + t, c, d} \) to \( x_{s'\alpha_1, s'\alpha_2 + t', k, l} \). We will show that there is a red arc from \( \phi(x_{s\alpha_1, s\alpha_2 + t, c, d}) \) to \( \phi(x_{s'\alpha_1, s'\alpha_2 + t', k, l}) \), which is sufficient. If \( s = s' \) and \( t = t' \) then we are done since \( \phi \) commutes with \( \tau_3 \) and \( \tau_4 \). If \( s = s' \) and \( t \neq t' \) then we are done since all of the \( p^2 \)-blocks in a fixed \( p^3 \)-block are pairwise wreathed. So we may assume \( s \neq s' \). Now, unless
\[
\begin{align*}
(s'\alpha_2 + t') - (s\alpha_2 + t) = (s' - s)\alpha_2 \text{ or} \\
(s'\alpha_2 + t') - (s\alpha_2 + t) = (s' - s)\beta_2,
\end{align*}
\]
the \( p^2 \)-blocks containing these two vertices are wreathed and again we are done.

Suppose first that
\[
(s'\alpha_2 + t') - (s\alpha_2 + t) = (s' - s)\alpha_2,
\]
that is, \( t' = t \). Then we have
\[
\phi(x_{s_0, s_0, c + t, c, d}) = (\tau_2')^t(x_{s_0, s_0, c + k, s_0, a_1, a_2, d + k, b_{a_1, a_2}) \quad \text{and} \\
\phi(x_{s', a_1, s', a_2 + t, k, l}) = (\tau_2')^t(x_{s', a_1, s', a_2, k + k, s_0, a_1, a_2, l + k, b_{a_1, a_2}).
\]

So we are done if there is a red arc from the vertex \( x_{s_0, s_0, c + k, s_0, a_1, a_2, d + k, b_{a_1, a_2}} \) to the vertex \( x_{s', a_1, s', a_2, k + k, s_0, a_1, a_2, l + k, b_{a_1, a_2}} \).

Since the intersection of the orbits of \( x_{(s'-s)a_1, (s'-s)a_2, 0, 0} \) under \( G \) with the block \( B_{(s'-s)a_1, (s'-s)a_2} \) are known, we can see that the known red arc from \( x_{s_0, s_0, c, d} \) to \( x_{s', a_1, s', a_2, k + k, s_0, a_1, a_2, l + k, b_{a_1, a_2}} \) forces there to be a red arc from \( x_{s_0, s_0, c, d} \) to \( x_{s', a_1, s', a_2, k + k, s_0, a_1, a_2, l + k, b_{a_1, a_2}} \) for every value of \( x \). In particular, this is true when \( x = k_1 - k_2 \). This yields the result.

The possibility remains that
\[
(s' a_2 + t') - (s a_2 + t) = (s' - s)r \beta_2; \quad \text{that is,}
\]
\[
s' r \beta_2 - s' a_2 - t' = sr \beta_2 - s a_2 - t.
\]

Now,
\[
\phi(x_{s_0, s_0, c + t, c, d}) = (\tau_2')^t(x_{s_0, s_0, c + k, s_0, a_1, a_2, d + k, b_{a_1, a_2})
\]
\[
= x_{s_0, s_0, c + t + k, s_0, a_1, a_2 + s_0 a_1, a_2 + \ldots + s_0 a_1, a_2 + t - 1, d + k, b_{a_1, a_2} + b_{s_0 a_1, a_2} + \ldots + b_{s_0 a_1, a_2 + t - 1}
\]
and
\[
\phi(x_{s', a_1, s', a_2 + t', k, l}) = (\tau_2')^t(x_{s', a_1, s', a_2, k + k, s_0, a_1, a_2, l + k, b_{a_1, a_2})
\]
\[
= x_{s', a_1, s', a_2 + t' + k, s_0 a_1, a_2 + s_0 a_1, a_2 + \ldots + s_0 a_1, a_2 + t' - 1, l + k, b_{a_1, a_2} + b_{s_0 a_1, a_2} + \ldots + b_{s_0 a_1, a_2 + t' - 1}
\]

So we are done if there is a red arc from the vertex \( x_{s_0, s_0, c + t, c, d} \) to the vertex
\[
x_{s', a_1, s', a_2 + t'} + k + k, a_1, a_2 + a_1, a_2 + \ldots + a_1, a_2 + t' - 1 - k, b_{a_1, a_2} - s a_1, a_2 + a_1, a_2 - a_1, a_2 - a_1, a_2 + t - 1
\]
\[
+ k, b_{a_1, a_2} - b_{s_0 a_1, a_2} - b_{s_0 a_1, a_2} + b_{s_0 a_1, a_2 + t' - 1}.\]
We know that the intersection of the orbit of $x(s'-s)\alpha_1,s'+t'-s\alpha_2-t,k-c,l-d$ under $G$ with the block
\[
B(s'-s)\alpha_1,s'+t'-s\alpha_2-t = B(s'-s)r\beta_1,(s'-s)r\beta_2
\]
is the set
\[
\{x(s'-s)r\beta_1,(s'-s)r\beta_2,k-c+m\alpha_1,\beta_2,l-d+mb_1,\beta_2 : 0 \leq m \leq p-1\}.
\]
Thus, we need to show that the vector
\[
(k_s'a_{\alpha_1,\alpha_2} + a_s'a_{\alpha_1,\alpha_2} + \ldots + a_{s'}'a_{\alpha_1,\alpha_2} - k_s'a_{\alpha_1,\alpha_2} - a_{s\alpha_1,\alpha_2} - \ldots - a_{s\alpha_1,\alpha_2+t-1},
\]
\[
k_s'b_{\alpha_1,\alpha_2} + b_{s'}'a_{\alpha_1,\alpha_2} + \ldots + b_{s'}'a_{\alpha_1,\alpha_2} - k_s'b_{\alpha_1,\alpha_2} - b_{s\alpha_1,\alpha_2} - \ldots - b_{s\alpha_1,\alpha_2+t-1}
\]
is collinear with the vector $(a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2})$.

Notice that for any $m$, the vector
\[
(a_{s'}'a_{\alpha_1,\alpha_2}+m - a_{s\alpha_1,\alpha_2+t+m}, b_{s'}'a_{\alpha_1,\alpha_2}+m - b_{s\alpha_1,\alpha_2+t+m})
\]
is collinear with the vector $(a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2})$. This is true because the automorphism
\[
\tau_3^{-a_{s\alpha_1,\alpha_2+t+m}}\tau_4^{-b_{s\alpha_1,\alpha_2+t+m}}\tau_2^{-1}\tau_2' \in \tau_1\tau_2\tau_2\tau_1^{-1}G_{\tau_2^{-1}}
\]
and we know the orbits of $G$ within the block $B(s'-s)\alpha_1,s'+t'-s\alpha_2-t$, which is the block $B(s'-s)r\beta_1,(s'-s)r\beta_2$. So we can add any of these vectors to the vector (2.1) above without disturbing its possible collinearity with $(a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2})$. We will add the vectors corresponding to $m = 0, m = 1, \ldots$, and $m = s'r\beta_2-s'\alpha_2-t'-1 = sr\beta_2-s\alpha_2-t-1$.

From this, vector (2.1) becomes:
\[
(k_s'a_{\alpha_1,\alpha_2} + a_s'a_{\alpha_1,\alpha_2} + \ldots + a_{s'}'a_{\alpha_1,\alpha_2}, b_{s'}'a_{\alpha_1,\alpha_2} - k_s'b_{\alpha_1,\alpha_2} - b_{s\alpha_1,\alpha_2} - \ldots - b_{s\alpha_1,\alpha_2+s\beta_2-1} = (k_s'a_{\beta_1,\beta_2} - k_s'b_{\beta_1,\beta_2}, k_s'a_{\beta_1,\beta_2} - k_s'b_{\beta_1,\beta_2})
\]
so the vector was indeed collinear with $(a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2})$ and we have shown that $\phi$ is an automorphism of $\tilde{X}$. 
Now we check that $\phi^{-1}\tau'_2 \phi = \tau_2$. We have
\[
\phi^{-1}\tau'_2 \phi(x_{s_0,s_0+t,c,d}) = \phi^{-1}(\tau'_2)^t \phi \tau_2^{-t}(x_{s_0,s_0+t,c,d}) \\
= \tau_2^{t+1} \phi^{-1}(\tau'_2)^{-t-1}(\tau'_2)^{t+1} \phi \tau_2^{-t}(x_{s_0,s_0+t,c,d}) \\
= \tau_2(x_{s_0,s_0+t,c,d}).
\]
In each of the above cases, the $\phi$ that was found respects all of the standard blocks, so we have $\phi \in P$ as required. This completes the proof. \qed

2.6.2 Orbits of $G$ when $\tau'_2 \neq \tau_2$

Let $G$ be (as in the proof above) the subgroup of $\langle \sigma(Z_p^4)_L \sigma^{-1}, (Z_p^4)_L \rangle$ that fixes the vertex $x_{0,0,0,0}$. For the purposes of these lemmata, we assume that both $\tau_3$ and $\tau_4$ are in both $\sigma(Z_p^4)_L \sigma^{-1}$ and $(Z_p^4)_L$; we also assume that $\tau'_2 \neq \tau_2$.

Lemma 2.6.2 If the orbit of the vertex $x_{a,b,0,0}$ under $G$ is the set
\[
\{x_{a,b,rt_1,rt_2} : 0 \leq r \leq p - 1\}
\]
for some $t_1$ and $t_2$, then the orbit of the vertex $x_{y_1+s_1,y_2+s_2,0,0}$ under $\tau_1^{y_1} \tau_2^{y_2} G \tau_1^{-y_1} \tau_2^{-y_2}$ must be the set
\[
\{x_{y_1+s_1,y_2+s_2,rt_1,rt_2} : 0 \leq r \leq p - 1\}
\]
for the same $t_1, t_2$.

Proof. First we show that the statement holds true when $(y_1, y_2) = (0, 0)$. We work by induction on $s$. The base case is the assumption of the lemma, so we need only complete the inductive step.

So we inductively assume that the orbit of the vertex $x_{s_1,s_2,0,0}$ under $G$ is the set
\[
\{x_{s_1,s_2,rt_1,rt_2} : 0 \leq r \leq p - 1\}.
\]
Let $\theta$ be any automorphism in $G$. Then clearly,
\[
\theta(x_{s_1,s_2,0,0}) = x_{s_1,s_2,rt_1,rt_2}
\]
for some \( r_1 \). Now consider the automorphism \( \tau_3^{-r_1} \tau_4^{-r_1} \). This is in the group \( \tau_1^{s_1} \tau_2^{s_2} G \tau_1^{-s_1} \tau_2^{-s_2} \) since it fixes the vertex \( x_{s_1, s_2, 0, 0} \).

Since the orbit of \( x_{a, b, 0, 0} \) under \( G \) is

\[ \{ x_{a, b, r_1, r_2} : 0 \leq r \leq p - 1 \}, \]

we certainly have the orbit of \( x_{(s+1)a, (s+1)b, 0, 0} \) under \( \tau_1^{s_1} \tau_2^{s_2} G \tau_1^{-s_1} \tau_2^{-s_2} \) is

\[ \{ x_{(s+1)a, (s+1)b, r_1, r_2} : 0 \leq r \leq p - 1 \}. \]

So we have

\[ \tau_3^{-r_1} \tau_4^{-r_1} \theta(x_{(s+1)a, (s+1)b, 0, 0}) = x_{(s+1)a, (s+1)b, r_2 r_1, r_2 r_2} \]

for some \( r_2 \). Hence

\[ \theta(x_{(s+1)a, (s+1)b, 0, 0}) = x_{(s+1)a, (s+1)b, (r_1 + r_2) t_1, (r_1 + r_2) t_2}. \]

Since \( \theta \) was an arbitrary element of \( G \), this shows that the orbit of the vertex \( x_{(s+1)a, (s+1)b, 0, 0} \) under \( G \) is some subset of

\[ \{ x_{(s+1)a, (s+1)b, r_1, r_2} : 0 \leq r \leq p - 1 \}. \]

Since \( G \) is a \( p \)-group, the orbit must either be this entire set (in which case our induction is complete), or the single vertex \( x_{(s+1)a, (s+1)b, 0, 0} \).

Suppose that the orbit of the vertex \( x_{(s+1)a, (s+1)b, 0, 0} \) under \( G \) were this single vertex. Then

\[ G = \tau_1^{(s+1)a} \tau_2^{(s+1)b} G \tau_2^{-(s+1)b} \tau_1^{-(s+1)a}. \]

We can repeat this argument inductively to see that in fact,

\[ G = \tau_1^{k(s+1)a} \tau_2^{k(s+1)b} G \tau_2^{-k(s+1)b} \tau_1^{-k(s+1)a}, \]

for any \( k \). In particular, when \( k(s + 1) \equiv 1 \) (mod \( p \)), we see that the orbit of \( x_{a, b, 0, 0} \) under \( G \) is in fact just the vertex \( x_{a, b, 0, 0} \). Hence we must have \( t_1 = t_2 = 0 \) and again the induction is complete.

Now, for any \( y_1, y_2 \), the orbit of \( x_{y_1 + c, y_2 + d, 0, 0} \) under \( \tau_1^{y_1} \tau_2^{y_2} G \tau_2^{-y_2} \tau_1^{-y_1} \) is simply \( \tau_1^{y_1} \tau_2^{y_2} \) acting on the orbit of \( x_{a, b, 0, 0} \) under \( G \). This completes the proof. \( \square \)
Lemma 2.6.3 Suppose that the intersection of the orbit of the vertex \( x_{a,b,0,0} \) under \( G \) with the block \( B_{a,b} \) is
\[
\{x_{a,b,rt_1,rt_2} : 0 \leq r \leq p - 1\}
\]
for some \( t_1 \) and \( t_2 \), and that this orbit is not contained within the block \( B_{a,b} \). Then there exist some \( b' \neq 0, c, d \) such that for any \( r \neq 0 \), the orbit of the vertex \( x_{ra,rb,0,0} \) under \( G \) is
\[
\{x_{ra,rb+sb',sc+st_1,t_2,td+st'_{t_2}} : 0 \leq s, s' \leq p - 1\}
\]
and the orbit of the vertex \( x_{0,rb,0,0} \) under \( G \) is
\[
\{x_{0,rb,s't_1,s't_2} : 0 \leq s' \leq p - 1\}
\]
for the same \( t_1, t_2 \).

PROOF. Since \( G \) is a p-group that fixes \( B_0 \) setwise, the orbit of \( x_{a,b,0,0} \) under \( G \) is certainly contained within \( B_a \). Now, \( G \) is a subgroup of
\[
\langle \sigma(\mathbb{Z}_p^d)\sigma^{-1}, (\mathbb{Z}_p^d)L \rangle = \langle \tau_4, \tau_3, \tau_2, \tau'_2, \tau'_1, \tau'_1 \rangle.
\]
It is not hard to see that if \( \tau'_1(B_{r,s}) = B_{r+1,s} \) for every \( r, s \), then \( G \) in fact fixes all \( p^2 \)-blocks setwise, contradicting the information assumed about the orbit of \( x_{a,b,0,0} \) under \( G \) in the statement of this lemma. So we must have \( \tau'_1(B_{z_1,z_2}) \neq B_{z_1+1,z_2} \) for some \( z_1, z_2 \). Notice that there must be some \( \theta \in G \) such that \( \theta(B_{a,b}) = B_{a,b+1} \). (The orbit of \( x_{a,b,0,0} \) under \( G \) is not contained in the block \( B_{a,b} \), and \( G \) is a p-group.) We set this aside for now and look at the action of \( \tau'_2 \).

We claim that \( \tau_2^{-1}\tau'_2(x_{y_1,y_2,0,0}) \) is contained in the set
\[
\{x_{y_1,y_2,rt_1,rt_2} : 0 \leq r \leq p - 1\}
\]
for any \( y_1, y_2 \).

First, note that since \( \theta \in G \), we have \( \theta \) commutes with \( \tau_3 \) and \( \tau_4 \). Hence the intersection of the orbit of \( x_{a,b,0,0} \) under \( G \) with the block \( B_{a,b+1} \) is the set
\[
\{x_{a,b+1,c'+rt_1,d'+rt_2} : 0 \leq r \leq p - 1\}
\]
for some $c', d'$. Hence the intersection of the orbit of $x_{a,b,c',d'}$ under $G$ with the block $B_{a,b+1}$ is the set
\[
\{x_{a,b+1,r_1,r_2} : 0 \leq r \leq p - 1\},
\]
which is therefore also the intersection of the orbit of $x_{a,b+1,0,0}$ under $G$ with the block $B_{a,b+1}$. Similarly, we can show that the intersection of the orbit of $x_{a,b+s,0,0}$ under $G$ with the block $B_{a,b+s}$ is the set
\[
\{x_{a,b+s,r_1,r_2} : 0 \leq r \leq p - 1\}
\]
for any $s$.

Next we prove our claim by induction. Let $y_1 = sa$ and $y_2 = sb + s'$; we will induct on $s$. The base case $s = 1$ has been shown. We assume the result holds for all $s'$ when $y_1 = sa$ and $y_2 = sb + s'$, and suppose that the image of $x_{sa, sb+s', 0, 0}$ under $r_2^{-1}r_2'$ is $x_{sa, sb+s', r_1, r_1}$.

We know that $r_2^{-1}r_2'$ fixes every $p^2$-block in $\hat{X}$ setwise. If $y_1 = (s + 1)a$ and $y_2 = (s + 1)b + s'$, we see that $r_3^{-r_4s+t_1, d_4^{-r_4s't_2}r_2^{-1}r_2'}$ fixes the vertex $x_{sa, sb+s', 0, 0}$, so is in the group $r_1^{-sa}r_2^{sa+s'}G r_2^{-sb-s'}, r_1^{-sa}$. From our knowledge of the orbit of $x_{a,b,0,0}$ under $G$, it is clear that the intersection of the orbit of $x_{y_1, y_2, 0, 0}$ under $r_1^{sa}r_2^{sb+s'}G r_2^{-sb-s'}, r_1^{-sa}$ with the block $B_{y_1, y_2}$ must be the set
\[
\{x_{y_1, y_2, r_1t_1, r_2t_2} : 0 \leq r' \leq p - 1\}.
\]

So we have
\[
\tau_3^{-r_4s+t_1, d_4^{-r_4s't_2}r_2^{-1}r_2'}(x_{y_1, y_2, 0, 0}) = x_{y_1, y_2, t_1, t_2} \text{ for some } t.
\]
Hence
\[
r_2^{-1}r_2'(x_{y_1, y_2, 0, 0}) = x_{y_1, y_2, (s+t), (s+t)}.
\]
This completes the induction and proves the claim.

The claim has shown that for any $y_1, y_2, y_3, y_4, b'$, we have
\[
(\tau_2')^{b'}(x_{y_1, y_2, y_3, y_4}) = x_{y_1, y_2, b', y_3 + s_{y_1, y_2, b'}, y_4 + s_{y_1, y_2, b'}, t_1, t_2},
\]
for some $s_{y_1, y_2, b'}$. 

Our earlier observations about the action of $\tau'_1$ have some further consequences that we now explore. Let $\tau'$ be the element of $\sigma(Z_p^*)L\sigma^{-1}$ that maps $x_{0,0,0,0}$ to $x_{a,b,0,0}$. Let $\alpha$ be the least value such that $\tau'(B_{a\alpha,0}) \neq B_{(\alpha+1)a,b}$. Clearly, $\alpha \geq 1$, and by our observations about $\tau'_1$ combined with the fact that $(\tau')^p$ is the identity, $\alpha \leq p - 1$.

Let $b', c, d$ be such that

$$\tau'(x_{a\alpha,0,b,0,0}) = x_{(\alpha+1)a,(\alpha+1)b+b',c,d}.$$

Since $\tau'$ and $\tau'_2$ commute, $b' \neq 0$ by the definition of $\alpha$.

Notice that for $\beta < \alpha$, we have

$$\tau'(x_{\beta a,\beta b,0,0}) \in \{x_{(\beta+1)a,\beta b+st_1, st_2} : 0 \leq s \leq p - 1\}.$$

We show this by induction on $\beta$. The base case of $\beta = 0$ is the definition of $\tau'$. We assume the result for $\beta$ and show that it is true for $\beta + 1$ provided that $\beta + 1 < \alpha$. By assumption, there exists some $s$ such that $\tau_4^{-st_2} \tau_3^{-st_1} \tau_2^{-b} \tau_1^{-a} \tau'$ fixes the vertex $x_{\beta a,\beta b,0,0}$. Since $\beta + 1 < \alpha$ and by the definition of $\alpha$, we have

$$\tau_4^{-st_2} \tau_3^{-st_1} \tau_2^{-b} \tau_1^{-a} \tau' \in \{x_{(\beta+1)a,\beta b+st_1, st_2} : 0 \leq s \leq p - 1\}.$$

But we know the intersection of the orbit of $x_{(\beta+1)a,\beta b+st_1, st_2}$ and the block $B_{(\beta+1)a,\beta b+st_1, st_2}$ that fixes $x_{\beta a,\beta b,0,0}$ under the subgroup of $\langle \sigma(Z_p^*)L\sigma^{-1}, (Z_p^*)L \rangle$ that fixes $x_{\beta a,\beta b,0,0}$ with the block $B_{(\beta+1)a,\beta b+st_1, st_2}$. Hence for some $s'$, we have

$$\tau_4^{-st_2} \tau_3^{-st_1} \tau_2^{-b} \tau_1^{-a} \tau'(x_{(\beta+1)a,\beta b+st_1, st_2}) = x_{(\beta+1)a,\beta b+s't_1, s't_2}.$$

So, as desired, we have

$$\tau'(x_{(\beta+1)a,\beta b+st_1, st_2}) = x_{(\beta+2)a,\beta b+s+t_1, (s+s')t_2}.$$

This completes the induction; in particular, we have

$$\tau'(x_{(\alpha-1)a,(\alpha-1)b,0,0}) \in \{x_{\alpha a,\alpha b, st_1, st_2} : 0 \leq s \leq p - 1\}.$$

Hence for some $s$, we have $\tau_4^{-st_2} \tau_3^{-st_1} \tau_2^{-b} \tau_1^{-a} \tau'$ fixes the vertex $x_{(\alpha-1)a,(\alpha-1)b,0,0}$. 
We use induction on \( k \) to show two things for every value of \( k \). Firstly, that

\[
\tau'(x_{a+kb'+b,0,0}) \in \{x_{(a+1)b+(k+1)b',c+s't_1,d+s't_2} : 0 \leq s' \leq p - 1\}. 
\]

Secondly, that the intersection of the orbit of the vertex \( x_{a,b,0,0} \) under \( G \) with the block \( B_{a,b+(k+1)b'} \) is the set

\[
\{x_{a,b+(k+1)b',(k+1)c+s't_1,(k+1)d+s't_2} : 0 \leq s' \leq p - 1\}.
\]

Notice that

\[
\tau_4^{-st_2} \tau_3^{-st_1} \tau_2^{-b} \tau_1^{-a} \tau'(x_{a,a+b',0,0}) = x_{a,a+b',c-st_1,d-st_2}.
\]

This shows that the orbit of \( x_{a,b,0,0} \) under \( G \) contains the vertex \( x_{a,b+b',c-st_1,d-st_2} \), and by our earlier argument involving \( \theta \) about this orbit, we have that the intersection of this orbit with the block \( B_{a,b+b'} \) must be the set

\[
\{x_{a,b+b',c+s't_1,d+s't_2} : 0 \leq s' \leq p - 1\}.
\]

The base case of \( k = 0 \) is now clear. We assume the induction hypothesis for \( k \) and show that it holds for \( k + 1 \). Now, as noted above, we have

\[
(\tau_2')^{b'}(x_{a,a+b+kb',0,0}) \in \{x_{a,a+b+(k+1)b',s't_1,s't_2} : 0 \leq s' \leq p - 1\} \quad \text{and}
\]

\[
(\tau_2')^{b'} \tau'(x_{a,a+b+kb',0,0}) = (\tau_2')^{b'}(\{x_{(a+1)a,(a+1)b+(k+1)b',c+s't_1,d+s't_2} : 0 \leq s' \leq p - 1\})
\]

\[= \{x_{(a+1)a,(a+1)b+(k+2)b',c+s't_1,d+s't_2} : 0 \leq s' \leq p - 1\}.
\]

Since \( \tau_2' \) and \( \tau' \) commute, this means that

\[
\tau'(x_{a,a+b+(k+1)b',0,0}) \in \{x_{(a+1)a,(a+1)b+(k+2)b',c+s't_1,d+s't_2} : 0 \leq s' \leq p - 1\}.
\]

This completes the induction for the first of the two statements. Recall that the automorphism \( \tau_4^{-st_2} \tau_3^{-st_1} \tau_2^{-b} \tau_1^{-a} \tau' \) fixes the vertex \( x_{(a-1)a,(a-1)b,0,0} \). Now,

\[
\tau_4^{-st_2} \tau_3^{-st_1} \tau_2^{-b} \tau_1^{-a} \tau'(x_{a,a+b+(k+1)b',0,0}) \in \{x_{a,a+b+(k+2)b',c+s't_1,d+s't_2} : 0 \leq s' \leq p - 1\}.
\]
This shows that some element of the set
\[ \{ x_{a,b+(k+2)b'},c+s't_1,d+s't_2 : 0 \leq s' \leq p - 1 \} \]
is in the intersection of the orbit of \( x_{a,b+(k+1)b',0,0} \) under \( G \) with the block \( B_{a,b+(k+2)b'} \). Now, the vertex \( x_{a,b+(k+1)b',(k+1)c,(k+1)d} \) is in the orbit of \( x_{a,b,0,0} \) under \( G \), by our induction hypothesis. Since every element of \( G \) commutes with \( \tau_3 \) and \( \tau_4 \), we see that some element of the set
\[ \{ x_{a,b+(k+2)b',c+s't_1,(k+2)d+s't_2} : 0 \leq s' \leq p - 1 \} \]
is in the intersection of the orbit of the vertex \( x_{a,b,0,0} \) under \( G \) with the block \( B_{a,b,(k+2)b'} \). By our earlier argument involving \( \theta \) about this orbit, we see that the intersection of the orbit of \( x_{a,b,0,0} \) under \( G \) with the block \( B_{a,b,(k+2)b'} \) must in fact be precisely the set
\[ \{ x_{a,b+(k+2)b',c+s't_1,(k+2)d+s't_2} : 0 \leq s' \leq p - 1 \} . \]
This completes the induction.

This inductive argument has provided the base case for one final inductive argument. We see that for \( k = 1 \), the orbit of \( x_{ka, kb, 0, 0} \) under \( G \) is as required for the theorem. Now, let \( \psi \) be any element of \( G \). We assume that the orbit of \( x_{ka, kb, 0, 0} \) under \( G \) is as required for the theorem. Then there exist \( l, m \) such that
\[ \psi(x_{ka, kb, 0, 0}) = x_{ka, kb+lb', lc+mt_1, ld+mt_2} . \]
Hence \( \tau_4^{-ld-mt_2} \tau_3^{-lc-mt_1} \tau_2^{-lb'} \psi \) fixes \( x_{ka, kb, 0, 0} \), so by the known orbit of \( x_{a,b,0,0} \) under \( G \), we must have
\[ \tau_4^{-ld-mt_2} \tau_3^{-lc-mt_1} \tau_2^{-lb'} \psi(x_{a,(k+1)b,0,0}) = x_{a,(k+1)b+lb', lc+mt_1, ld+mt_2} . \]
Hence
\[ \psi(x_{a,(k+1)b,0,0}) = x_{a,(k+1)b+(l+l')b', (l+l')c+(m+m')t_1, (l+l')d+(m+m')t_2} . \]
Since \( \psi \) was an arbitrary element of \( G \), this shows that the orbit of \( G \) is contained within the required set. If the orbit of \( G \) on some vertex \( x_{(k+1)a,(k+1)b,0,0} \) were contained within the block \( B_{(k+1)a,(k+1)b} \), where \( k + 1 \neq 0 \), then we could use Lemma 2.6.2 to contradict the fact that the orbit of \( x_{a,b,0,0} \) under \( G \) is not contained within \( B_{a,b} \). If \( m + m' = 0 \) for any such element of \( G \), then we repeat the entire argument substituting this block for \( B_{a,b} \) to contradict the known length of the orbit of \( x_{a,b,0,0} \) under \( G \). This completes the induction and most of the theorem.

It remains to be shown that the orbit of \( x_{0,r,b,0,0} \) under \( G \) cannot be the singleton \( x_{0,r,b,0,0} \) when \( r \neq 0 \). Since \( \tau'_2 \neq \tau_2 \), there is some vertex \( x_{\gamma_1,\gamma_2,0,0} \) such that

\[
\tau'_2(x_{\gamma_1,\gamma_2,0,0}) = x_{\gamma_1,\gamma_2+1,kt_1,kt_2}
\]

for some \( k \neq 0 \). Let \( \tau' \) be the element of \( \sigma(Z^4)_{L1}L^{-1} \) mapping \( x_{0,0,0,0} \) to \( x_{\gamma_1,\gamma_2,0,0} \). Then since \( \tau' \) and \( \tau'_2 \) commute, we have

\[
\tau'(x_{0,1,0,0}) = x_{\gamma_1,\gamma_2+1,kt_1,kt_2}.
\]

Now, \( \tau_1^{-\gamma_1} \tau_2^{-\gamma_2} \tau' \in G \), and

\[
\tau_1^{-\gamma_1} \tau_2^{-\gamma_2} \tau'(x_{0,1,0,0}) = x_{0,1,0,0}.
\]

Hence the orbit of \( x_{0,1,0,0} \) under \( G \) is the set

\[
\{ x_{0,1,kt_1,kt_2} : 0 \leq k \leq p - 1 \},
\]

as required. By Lemma 2.6.2, the other orbits in \( B_0 \) are also as required.

\[ \square \]

**Corollary 2.6.4** Suppose that the block \( B_{0,0} \) were not forced by the combined actions of \( \sigma(Z^4)_{L1}L^{-1} \) and \( (Z^4)_{L1} \) to be wreathed with the block \( B_{a,b} \). Then for any \( y_1, y_2, s \), these actions do not force the block \( B_{y_1,y_2} \) to be wreathed with the block \( B_{y_1+s,a,y_2+s,b} \).

**Proof.** This is an immediate consequence of the two lemmata above. \[ \square \]
Lemma 2.6.5 Suppose there are two $p^2$-blocks $B_{\alpha_1, \alpha_2}$ and $B_{\beta_1, \beta_2}$ and automorphisms $\tau_{2,j_1}', \tau_{2,j_2}' \in \langle \tau_2, \tau_3, \tau_4 \rangle$ that fix the last two coordinates of any vertex in $B_0$, such that

$$
\tau_{2,j_1}'(x_{\alpha_1, \alpha_2, 0, 0}) = x_{\alpha_1, \alpha_2 + j_1, \alpha_1, \alpha_2},
$$
$$
\tau_{2,j_2}'(x_{\beta_1, \beta_2, 0, 0}) = x_{\beta_1, \beta_2 + j_2, \beta_1, \beta_2},
$$

and the vectors $(a_{\alpha_1, \alpha_2}, b_{\alpha_1, \alpha_2})$ and $(a_{\beta_1, \beta_2}, b_{\beta_1, \beta_2})$ are linearly independent. Then the action of $\langle (Z_p^4)_L \sigma(Z_p^4)_L \sigma^{-1} \rangle$ forces any two $p^2$-blocks in the same $p^3$-block to be wreathed.

**Proof.** We show that $B_{0,0}$ must be wreathed with $B_{0,k}$ for any $k$, which is sufficient.

Let $\tau' \in \sigma(Z_p^4)_L \sigma^{-1}$ be the automorphism taking $x_{0,0,0,0}$ to $x_{\alpha_1, \alpha_2, 0,0}$, and let $\tau'' \in \sigma(Z_p^4)_L \sigma^{-1}$ be the automorphism taking $x_{0,0,0,0}$ to $x_{\beta_1, \beta_2, 0,0}$. Then

$$
\tau_1^{-\alpha_1} \tau_2^{-\alpha_2} \tau' \in G, \quad \text{and}
$$
$$
\tau_1^{-\beta_1} \tau_2^{-\beta_2} \tau'' \in G.
$$

Consider the action of $\tau_1^{-\alpha_1} \tau_2^{-\alpha_2} \tau'$ on the vertex $x_{0,j_1,0,0}$. We have

$$x_{0,j_1,0,0} = \tau_{2,j_1}'(x_{0,0,0,0}),$$
$$\tau_1^{-\alpha_1} \tau_2^{-\alpha_2} \tau'(x_{0,j_1,0,0}) = \tau_1^{-\alpha_1} \tau_2^{-\alpha_2} \tau_{2,j_1}'(x_{\alpha_1, \alpha_2, 0,0})
= x_{0,j_1,\alpha_1,\alpha_2,0,0}.
$$

Similarly,

$$\tau_1^{-\beta_1} \tau_2^{-\beta_2} \tau''(x_{0,j_2,0,0}) = x_{0,j_2,\beta_1,\beta_2,0,0}.
$$

Since the vectors $(a_{\alpha_1, \alpha_2}, b_{\alpha_1, \alpha_2})$ and $(a_{\beta_1, \beta_2}, b_{\beta_1, \beta_2})$ are linearly independent, we can use Lemma 2.6.2 to show that the orbit of $x_{0,k,0,0}$ under $G$ will be the entire block $B_{0,k}$, showing that the blocks $B_{0,0}$ and $B_{0,k}$ are indeed wreathed by Lemma 2.2.10. 

$\Box$
Lemma 2.6.6 Suppose that \( \tau'_2 \neq \tau_2 \), and that there are three pairwise linearly independent two-dimensional vectors \((\alpha_1, \alpha_2), (\beta_1, \beta_2), (\gamma_1, \gamma_2)\) with integral coordinates, such that the combined actions of \(\sigma(\mathbb{Z}_p^2)\sigma^{-1}^{L} \) and \((\mathbb{Z}_p^2)^{L} \) do not force \( B_{0,0} \) to be wreathed with \( B_{\alpha_1,\alpha_2}, B_{\beta_1,\beta_2}, \) or \( B_{\gamma_1,\gamma_2} \). Let \( a_{\alpha_1,\alpha_2}, b_{\alpha_1,\alpha_2}, a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2}, a_{\gamma_1,\gamma_2}, b_{\gamma_1,\gamma_2} \) be such that the intersection of the orbit of \( x_{\alpha_1,\alpha_2,0,0} \) under \( G \) with the block \( B_{\alpha_1,\alpha_2} \) is the set
\[
\{ x_{\alpha_1,\alpha_2,k_a\alpha_1, a_2} : 0 \leq k \leq p - 1 \},
\]
the intersection of the orbit of \( x_{\beta_1,\beta_2,0,0} \) under \( G \) with the block \( B_{\beta_1,\beta_2} \) is the set
\[
\{ x_{\beta_1,\beta_2,k_{a_{\beta_1,\beta_2}}a_2} : 0 \leq k \leq p - 1 \},
\]
and the intersection of the orbit of \( x_{\gamma_1,\gamma_2,0,0} \) under \( G \) with the block \( B_{\gamma_1,\gamma_2} \) is the set
\[
\{ x_{\gamma_1,\gamma_2,k_{a_{\gamma_1,\gamma_2}}a_2} : 0 \leq k \leq p - 1 \}.
\]
Then the vectors \((a_{\alpha_1,\alpha_2}, b_{\alpha_1,\alpha_2}), (a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2})\) and \((a_{\gamma_1,\gamma_2}, b_{\gamma_1,\gamma_2})\) are not pairwise linearly independent.

PROOF. First, if there is some \( \theta \in G \) and some block \( B_{i,j} \) such that \( \theta(B_{i,j}) = B_{i,j} \), then by Lemma 2.6.3, it is clear that the three vectors \((a_{\alpha_1,\alpha_2}, b_{\alpha_1,\alpha_2}), (a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2})\) and \((a_{\gamma_1,\gamma_2}, b_{\gamma_1,\gamma_2})\) are in fact collinear, and we are done. So we may assume that the action of \( G \) fixes every \( p^2 \)-block in \( \tilde{X} \) setwise.

We assume that the three vectors \((a_{\alpha_1,\alpha_2}, b_{\alpha_1,\alpha_2}), (a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2})\) and \((a_{\gamma_1,\gamma_2}, b_{\gamma_1,\gamma_2})\) are pairwise linearly independent, and work towards a contradiction.

Consider the action of \( \tau_2^{-1}\tau'_2 \in G \) on the vertices \( x_{\alpha_1,\alpha_2,0,0}, x_{\beta_1,\beta_2,0,0}, x_{\gamma_1,\gamma_2,0,0} \). Suppose that \( \tau_2^{-1}\tau'_2 \) fixes \( x_{ka_1,ka_2,0,0} \) for every possible value of \( k \). Let \( r_1 \) and \( r_2 \) be the unique solutions (modulo \( p \)) to the equation
\[
r_1(\beta_1, \beta_2) + r_2(\gamma_1, \gamma_2) = (\alpha_1, \alpha_2).
\]
Due to the pairwise linear independence of the vectors, this can be solved for \( r_1 \) and \( r_2 \), and neither \( r_1 \) nor \( r_2 \) will be \( 0 \).
For any value $z$, we have $z = z'r_1$ for some $z'$. Consider the action of $\tau_2^{-1}\tau_2'$ on $x_1, x_2, 0, 0$. We have $\tau_2^{-1}\tau_2' \in G$, so by Lemma 2.6.2,

$$\tau_2^{-1}\tau_2'(x_1, x_2, 0, 0) \in \{x_1, x_2, k x_1, x_2, k x_1, x_2 : 0 \leq k \leq p - 1\}.$$  

However, we also have the automorphism

$$\tau_1^{-1}\tau_1' \in \tau_1^{-1,\alpha_1} \tau_2^{-1,\alpha_2} G \tau_2^{-1,\alpha_2} \tau_1^{-1,\alpha_1},$$

so by Lemma 2.6.2 and the fact that

$$x_1, x_2, 0, 0 = \tau_1^{-1,\alpha_1} \tau_2^{-1,\alpha_2} G \tau_2^{-1,\alpha_2} \tau_1^{-1,\alpha_1},$$

we see that we must have

$$\tau_2^{-1}\tau_2'(x_1, x_2, 0, 0) \in \{x_1, x_2, k x_1, x_2, k x_1, x_2 : 0 \leq k \leq p - 1\}.$$  

Clearly, then,

$$\tau_2^{-1}\tau_2'(x_1, x_2, 0, 0) = x_1, x_2, 0, 0.$$  

Likewise, we can show that we must have

$$\tau_2^{-1}\tau_2'(x_2, x_1, 0, 0) = x_2, x_1, 0, 0.$$  

Since $z$ was arbitrary, these statements are true for all values of $z$.

Let $y_1, y_2$ be arbitrary values. Let $\delta_1, \delta_2$ be such that

$$(y_1, y_2) = \delta_1(\beta_1, \beta_2) + \delta_2(\gamma_1, \gamma_2).$$

We can find such values since the vectors are linearly independent. By the arguments of the last paragraph, we have

$$\tau_2^{-1}\tau_2' \in \tau_1^{\delta_1,\beta_1} \tau_2^{\delta_1,\beta_2} G \tau_2^{-\delta_1,\beta_2} \tau_1^{-\delta_1,\beta_1} \text{ and}$$

$$\tau_2^{-1}\tau_2' \in \tau_1^{\delta_2,\gamma_1} \tau_2^{\delta_2,\gamma_2} G \tau_2^{-\delta_2,\gamma_2} \tau_1^{-\delta_2,\gamma_1}.$$
By Lemma 2.6.2, this means that \( \tau_2^{-1} \tau'_2(x_{y_1,y_2}) \) must be in the intersection of the sets

\[
\{x_{y_1,y_2, k\alpha_1, \beta_1, \beta_2 : 0 \leq k \leq p - 1}\} \quad \text{and} \quad \{x_{y_1,y_2, k\beta_1, \beta_2 : 0 \leq k \leq p - 1}\}.
\]

We have now shown (since \( y_1 \) and \( y_2 \) were arbitrary, and since \( \tau_3 \) and \( \tau_4 \) commute with every element of \( G \)) that \( \tau'_2 = \tau_2 \), contradicting our initial assumption. So we must have some \( k \) such that

\[
\tau_2^{-1} \tau'_2(x_{k\alpha_1,k\beta_2,0,0}) \neq x_{k\alpha_1,k\beta_2,0,0}.
\]

Without loss of generality, due to Lemma 2.6.2, we may assume that

\[
\tau_2^{-1} \tau'_2(x_{\alpha_1,\alpha_2,0,0}) = x_{\alpha_1,\alpha_2,\alpha_1,\alpha_2}.
\]

We can repeat this argument, interchanging first \( \alpha \) with \( \beta \) and then again interChanging \( \alpha \) with \( \gamma \) to show that we may assume that

\[
\tau_2^{-1} \tau'_2(x_{\beta_1,\beta_2,0,0}) = x_{\beta_1,\beta_2,\beta_1,\beta_2} \quad \text{and that}
\]

\[
\tau_2^{-1} \tau'_2(x_{\gamma_1,\gamma_2,0,0}) = x_{\gamma_1,\gamma_2,\gamma_1,\gamma_2}.
\]

By Lemma 2.6.5, we must have \( \alpha_1 \neq 0, \beta_1 \neq 0 \) and \( \gamma_1 \neq 0 \).

We begin by showing that, under the given assumptions, whenever we have \( y_1, y_2 \) such that

\[
\tau_2^{-1} \tau'_2(x_{y_1+y_1, y_2+y_2,0,0}) = \tau_1^{-1} \tau_2^{-1} \tau_3^{-1} \tau_4^{-1} \tau_2^{-1} \tau'_2(x_{y_1,y_2,0,0}),
\]

we also have

\[
\tau_2^{-1} \tau'_2(x_{y_1+r_1\beta_1+y_1, y_2+r_1\beta_2+y_2,0,0}) = \tau_1^{-1} \tau_2^{-1} \tau_3^{-1} \tau_4^{-1} \tau_2^{-1} \tau'_2(x_{y_1+r_1\beta_1+y_1, y_2+r_1\beta_2+y_2,0,0}), \quad \text{and}
\]

\[
\tau_2^{-1} \tau'_2(x_{y_1+r_2\gamma_1+y_1, y_2+r_2\gamma_2+y_2,0,0}) = \tau_1^{-1} \tau_2^{-1} \tau_3^{-1} \tau_4^{-1} \tau_2^{-1} \tau'_2(x_{y_1+r_2\gamma_1+y_1, y_2+r_2\gamma_2+y_2,0,0}).
\]

By Lemma 2.6.2, the lack of forced wreathing between \( B_{0,0} \) and \( B_{\beta_1, \beta_2} \) and the known action of \( \tau_2^{-1} \tau'_2 \in G \) on \( x_{\beta_1, \beta_2, 0,0} \), it is not hard to see that the orbit of the vertex \( x_{y_1+r_1\beta_1+y_1, y_2+r_1\beta_2+y_2,0,0} \) under the group \( \tau_1^{-1} \tau_2^{-1} G \tau_2^{-1} \tau_1^{-1} \) is the set

\[
\{x_{y_1+r_1\beta_1+y_1, y_2+r_1\beta_2+r_2\beta_1, \beta_2 : 0 \leq r \leq p - 1}\}.
\]
Define $a_{v_1,v_2}, b_{v_1,v_2}$ to be such that
\[ \tau_2^{-1} \tau'_2(x_{v_1,v_2,0,0}) = x_{v_1,v_2,a_{v_1,v_2}b_{v_1,v_2}}. \]

Then we have
\[ \tau_3^{-a_{v_1,v_2}} \tau_4^{-b_{v_1,v_2}} \tau_2^{-1} \tau'_2 \in \tau_1 \tau_2 \gamma_2 G \tau_2 \tau_1^{-v_1}. \]

Hence there exists some $k_1$ such that
\[ \tau_2^{-1} \tau'_2(x_{v_1+1,3_1,v_2+r_1,3_2,0,0}) = x_{v_1+r_1,3_1,v_2+r_1,3_2+k_1a_{v_1,a_2}+a_{v_1,v_2},k_1b_{v_1,a_2}+b_{v_1,v_2}}. \]

Hence the automorphism
\[ \tau_3^{-k_1a_{v_1,a_2}+a_{v_1,v_2}} \tau_4^{-k_1b_{v_1,a_2}+b_{v_1,v_2}} \tau_2^{-1} \tau'_2 \]
fixes the vertex $x_{v_1+r_1,3_1,v_2+r_1,3_2,0,0}$.

Meanwhile,
\[ \tau_3^{-k_1a_{v_1,a_2}+a_{v_1,v_2}} \tau_4^{-k_1b_{v_1,a_2}+b_{v_1,v_2}} \tau_2^{-1} \tau'_2(x_{v_1+1,3_1,v_2+2,0,0}) = x_{v_1+a_1,v_2+a_2,a_1,a_2-k_1a_{v_1,a_2}+b_{v_1,a_2}-k_1b_{v_1,a_2}}. \]

By Lemma 2.6.2 again, since
\[ (\alpha_1, \alpha_2) = r_1(\beta_1, \beta_2) + r_2(\gamma_1, \gamma_2), \]
and we know the orbit of $x_{v_1,3_1,0,0}$ under $G$, there must be some fixed $k_2$ such that
\[ a_{\alpha_1,\alpha_2} - k_1a_{\beta_1,\beta_2} = k_2a_{v_1,\gamma_2}, \text{ and } \]
\[ b_{\alpha_1,\alpha_2} - k_1b_{\beta_1,\beta_2} = k_2b_{v_1,\gamma_2}. \]

It is clear from the pairwise linear independence that $k_1$ and $k_2$ are the unique solutions (modulo $p$) to the equation
\[ (a_{\alpha_1,\alpha_2}, a_{\beta_1,\beta_2}) = k_1(a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2}) + k_2(a_{v_1,\gamma_2}, b_{v_1,\gamma_2}), \]
and that neither $k_1$ nor $k_2$ can be 0.
Now, by Lemma 2.6.2, the lack of forced wreathing between $B_0,0$ and $B_{a,1},a_2$ and the known action of $G$ on $x_{a,1},a_2,0,0$, it is not hard to see that the orbit of the vertex $x_{y_1+r_1,1,1+y_2+r_1,1,2+2,0,0}$ under the group

$$\tau_1 y_1+r_1,1,1 y_2+r_1,1,2 G \tau_2 y_2-r_1,1,2 \tau_1 y_1-r_1,1,1$$

is the set

$$\{x_{y_1+r_1,1,1+y_2+r_1,1,2+2,0,0} : 0 \leq r \leq p-1\}.$$

We know from above that the automorphism

$$\tau_3^{-k_1} a_1,1,2-a y_1,y_2 \tau_4^{-k_1} b_1,2,-b y_1,y_2 \tau_2^{-1} \tau'_2$$

is in this group, so we must have

$$\tau_3^{-k_1} a_1,1,2-a y_1,y_2 \tau_4^{-k_1} b_1,2,-b y_1,y_2 \tau_2^{-1} \tau'_2 (x_{y_1+r_1,1,1+y_2+r_1,1,2+2,0,0})$$

$$= x_{y_1+r_1,1,1+y_2+r_1,1,2+2,0,0} \cdot k_{3,a_1,1,2}$$

for some $k_3$. Hence

$$\tau_2^{-1} \tau'_2 (x_{y_1+r_1,1,1+y_2+r_1,1,2+2,0,0})$$

$$= x_{y_1+r_1,1,1+y_2+r_1,1,2+2,0,0} \cdot k_{3,a_1,1,2}.$$ 

However, we also know that the automorphism

$$\tau_3^{-a_1,1,2-a y_1,y_2} \tau_4^{-b_1,2,-b y_1,y_2} \tau_2^{-1} \tau'_2 \in \tau_1 y_1+a_1,1,2 \tau_2 y_2+a_2 \tau_1 y_1-a_1,1,2.$$ 

Due to Lemma 2.6.2 again, we see that we must have

$$\tau_3^{-a_1,1,2-a y_1,y_2} \tau_4^{-b_1,2,-b y_1,y_2} \tau_2^{-1} \tau'_2 (x_{y_1+r_1,1,1+y_2+r_1,1,2+2,0,0})$$

$$= x_{y_1+r_1,1,1+y_2+r_1,1,2+2,0,0} \cdot k_{4,b_1,2}.$$ 

for some $k_4$. So

$$\tau_2^{-1} \tau'_2 (x_{y_1+r_1,1,1+y_2+r_1,1,2+2,0,0})$$

$$= x_{y_1+r_1,1,1+y_2+r_1,1,2+2,0,0} \cdot k_{4,b_1,2,b_1,2}.$$
Combining these two expressions, we see that we must have

\[ k_4(a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2}) + (a_{\alpha_1,\alpha_2}, b_{\alpha_1,\alpha_2}) = k_3(a_{\alpha_1,\alpha_2}, b_{\alpha_1,\alpha_2}) + k_1(a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2}). \]

Hence

\[ (k_4 - k_1)(a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2}) = (k_3 - 1)(a_{\alpha_1,\alpha_2}, b_{\alpha_1,\alpha_2}). \]

Since \((a_{\alpha_1,\alpha_2}, b_{\alpha_1,\alpha_2}) \) and \((a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2}) \) are linearly independent, we must have \(k_3 = 1\) and \(k_4 = k_1\). Hence

\[
\tau_2^{-1} \tau'_2(x_{y_1+r_1\beta_1+\alpha_1, y_2+r_1\beta_2+\alpha_2, 0, 0}) = x_{y_1+r_1\beta_1+\alpha_1, y_2+r_1\beta_2+\alpha_2, a_{\alpha_1,\alpha_2}+k_1 a_{\beta_1,\beta_2}+b_{\beta_1,\beta_2}, b_{\beta_1,\beta_2}+b_{\beta_1,\beta_2}}.
\]

We already know from earlier calculations that

\[
\tau_2^{-1} \tau'_2(x_{y_1+r_1\beta_1+\alpha_1, y_2+r_1\beta_2+\alpha_2, 0, 0}) = x_{y_1+r_1\beta_1+\alpha_1, y_2+r_1\beta_2+\alpha_2, a_{\alpha_1,\alpha_2}+k_1 a_{\beta_1,\beta_2}+b_{\beta_1,\beta_2}, b_{\beta_1,\beta_2}+b_{\beta_1,\beta_2}}.
\]

so we have

\[
\tau_1^{-1} \tau_2^{-1} \tau_3^{-1} \tau_4^{-1} \tau_2^{-1} \tau'_2(x_{y_1+r_1\beta_1+\alpha_1, y_2+r_1\beta_2+\alpha_2, 0, 0}) = x_{y_1+r_1\beta_1+\alpha_1, y_2+r_1\beta_2+\alpha_2, a_{\alpha_1,\alpha_2}+k_1 a_{\beta_1,\beta_2}+b_{\beta_1,\beta_2}, b_{\beta_1,\beta_2}+b_{\beta_1,\beta_2}}
\]

as required. By interchanging the symbols \(\beta\) and \(\gamma\) in the above argument, we get an analogous result for \(\gamma\).

Let \(z_1, z_2\) be such that

\[ z_1 r_1(\beta_1, \beta_2) + z_2 r_2(\gamma_1, \gamma_2) = (0, 1). \]

Then we have in fact shown, through the above argument, that

\[ \tau_2^{-1} \tau'_2(x_{0, 1, 0, 0}) = x_{0, 1, z_1 k_1 a_{\alpha_1,\alpha_2}+z_2 k_2 a_{\gamma_1,\gamma_2}, z_1 k_1 b_{\alpha_1,\alpha_2}+z_2 k_2 b_{\gamma_1,\gamma_2}}. \]

Let \(\tau'\) be the element of \(\sigma(Z_2^2)\sigma^{-1}\) that takes \(x_{0, 0, 0, 0}\) to \(x_{\alpha_1, \alpha_2, 0, 0}\). There was nothing special about the choice of \(\tau_2^{-1} \tau'_2\) in the part of the above argument that
followed the determination of the images of $x_{\alpha_1,\alpha_2,0,0}$, $x_{\beta_1,\beta_2,0,0}$ and $x_{\gamma_1,\gamma_2,0,0}$ under $\tau_2^{-1}\tau_2'$, other than its inclusion in the group $G$. So we could repeat that part of the argument with $\tau_1^{-\alpha_1}\tau_2^{-\alpha_2}\tau'$ replacing $\tau_2^{-1}\tau_2'$ wherever it appears. Due to the known orbits, we will have

$$\tau_1^{-\alpha_1}\tau_2^{-\alpha_2}\tau'(x_{\alpha_1,\alpha_2,0,0}) = x_{\alpha_1,\alpha_2,ca_{\alpha_1,\alpha_2},cb_{\alpha_1,\alpha_2}}$$

for some $c$. Hence, $k_1$ will be replaced by $ck_1$ wherever it appears, and $k_2$ by $ck_2$. We will eventually conclude that

$$\tau_1^{-\alpha_1}\tau_2^{-\alpha_2}\tau'(x_{0,1,0,0}) = x_{0,1,z_1ck_1a_{\beta_1,\beta_2} + z_2ck_2a_{\gamma_1,\gamma_2}}, z_1ck_1b_{\beta_1,\beta_2} + z_2ck_2b_{\gamma_1,\gamma_2}.$$

Now,

$$\tau_1^{-\alpha_1}\tau_2^{-\alpha_2}\tau'(x_{0,1,0,0}) = \tau_1^{-\alpha_1}\tau_2^{-\alpha_2}\tau'(x_{0,0,0,0})$$

$$= \tau_1^{-\alpha_1}\tau_2^{-\alpha_2}\tau'(x_{\alpha_1,\alpha_2,0,0})$$

$$= x_{0,1,ca_{\alpha_1,\alpha_2},cb_{\alpha_1,\alpha_2}}.$$

Hence we must have

$$(a_{\alpha_1,\alpha_2}, b_{\alpha_1,\alpha_2}) = z_1ck_1(a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2}) + z_2ck_2(a_{\gamma_1,\gamma_2}, b_{\gamma_1,\gamma_2}).$$

But we know that the unique solution (modulo $p$) to the equation

$$(a_{\alpha_1,\alpha_2}, b_{\alpha_1,\alpha_2}) = x(a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2}) + y(a_{\gamma_1,\gamma_2}, b_{\gamma_1,\gamma_2})$$

is $x = k_1, y = k_2$. So we must have $z_1c = z_2c = 1$. Hence $z_1 = z_2 \neq 0$. But then, since

$$z_1r_1(\beta_1,\beta_2) + z_2r_2(\gamma_1,\gamma_2) = (0,1),$$

we have

$$z_1[r_1(\beta_1,\beta_2) + r_2(\gamma_1,\gamma_2)] = z_1(a_{\alpha_1,\alpha_2})$$

$$= (0,1).$$

Since $z_1 \neq 0$, this contradicts the fact that $\alpha_1 \neq 0$, and we are done. So the vectors $(a_{\alpha_1,\alpha_2}, b_{\alpha_1,\alpha_2}), (a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2})$ and $(a_{\gamma_1,\gamma_2}, b_{\gamma_1,\gamma_2})$ cannot be pairwise linearly independent. $\square$
Lemma 2.6.7 Suppose that there are two two-dimensional linearly independent vectors with integral coordinates, \((\alpha_1, \alpha_2)\) and \((\beta_1, \beta_2)\), such that the combined actions of \(\sigma(\mathbb{Z}_p^4)\sigma^{-1}\) and \((\mathbb{Z}_p^4)_L\) do not force \(B_{0,0}\) to be wreathed with \(B_{\alpha_1,\alpha_2}\) or \(B_{\beta_1,\beta_2}\). Let \(a_{\beta_1,\beta_2}, b_{\alpha_1,\alpha_2}, a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2}\) be such that the intersection of the orbit of \(x_{\alpha_1,\alpha_2,0,0}\) under \(G\) with the block \(B_{\alpha_1,\alpha_2,0,0}\) is the set

\[
\{x_{\alpha_1,\alpha_2,k\alpha_1,\alpha_2,kb_{\alpha_1,\alpha_2} : 0 \leq k \leq p - 1\},
\]

and the intersection of the orbit of the vertex \(x_{\beta_1,\beta_2,0,0}\) under \(G\) with the block \(B_{\beta_1,\beta_2,0,0}\) is the set

\[
\{x_{\beta_1,\beta_2,k\beta_1,\beta_2,kb_{\beta_1,\beta_2} : 0 \leq k \leq p - 1\}.
\]

If the vectors \((a_{\alpha_1,\alpha_2}, b_{\alpha_1,\alpha_2})\) and \((a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2})\) are linearly dependent, then there is an element \(h\) of \(P \leq \text{Aut}(\tilde{X})\) such that \(h^{-1}r_2h = r_2\).

**Proof.** Let \(k\) be such that

\[
k(a_{\beta_1,\beta_2}, b_{\beta_1,\beta_2}) = (a_{\alpha_1,\alpha_2}, b_{\alpha_1,\alpha_2}).
\]

Consider any vertex \(x_{y_1,y_2,0,0}\). There exist some \(z_1, z_2\) such that

\[
(y_1, y_2) = z_1(\alpha_1, \alpha_2) + z_2(\beta_1, \beta_2),
\]

since \((\alpha_1, \alpha_2)\) and \((\beta_1, \beta_2)\) are linearly independent.

If Lemma 2.6.3 applies, then we can use that lemma to conclude that the orbit of \(x_{y_1,y_2,0,0}\) under \(G\) is (for some fixed \(b' \neq 0, c, d\)) the set

\[
\{x_{r\beta_1, r\beta_2 + sb', sc + s'c_1, \beta_2 + c'd + s'b_{\beta_1, \beta_2} + d' : 0 \leq s, s' \leq p - 1\},
\]

where \(r\) is such that \(y_1 = r\beta_1\), and \(c', d'\) are such that for the value of \(s\) for which \(r\beta_2 + sb' = y_2\), we have \(c' = -sc\) and \(d' = -sd\). In this case, the intersection of the orbit of \(x_{y_1,y_2,0,0}\) under \(G\) with the block \(B_{y_1,y_2}\) is the set

\[
\{x_{y_1,y_2,s'c_1, \beta_2 + s'b_{\beta_1, \beta_2} : 0 \leq s' \leq p - 1\}.
\]
If Lemma 2.6.3 does not apply, then Lemma 2.6.2 does. Let $\gamma$ be any element of the group $G$. By Lemma 2.6.2, we can see that there is some $k_1$ such that

$$\gamma(x_{z_1}a_1,z_1a_2,0,0) = x_{z_1}a_1,z_1a_2,k_1a_1,a_2,k_1b_{a_1,a_2}.$$ 

Using Lemma 2.6.2 again, there is some $k_2$ such that

$$\gamma(x_{y_1,y_2,0,0}) = x_{y_1,y_2,k_1a_1,a_2+k_2a_1,a_2,k_1b_{a_1,a_2}+k_2b_{a_1,a_2}} = x_{y_1,y_2,(kk_1+k_2)a_1,a_2,(kk_1+k_2)b_{a_1,a_2}}.$$ 

So for any $y_1, y_2$, the intersection of the orbit of $x_{y_1,y_2,0,0}$ under $G$ with the block $B_{y_1,y_2}$ is either

$$\{x_{y_1,y_2,ra_1,a_2,rb_{a_1,a_2}} : 0 \leq r \leq p - 1\} \text{ or } \{x_{y_1,y_2,0,0}\}.$$ 

Suppose first that there is some $(y_1,y_2) \neq (0,0)$ such that the orbit of $x_{y_1,y_2,0,0}$ under $G$ is $\{x_{y_1,y_2,0,0}\}$. Then we have

$$\tau_1^{y_1}\tau_2^{y_2}G\tau_2^{-y_2}\tau_1^{-y_1} = G.$$ 

If $y_1 = 0$, then we will show that $\tau_2' = \tau_2$. Notice that when $y_1 = 0$, since $(y_1,y_2) \neq (0,0)$, we have $y_2 \neq 0$, so the action of $G$ fixes every vertex in $B_0$. Now, if $\tau_2' \neq \tau_2$, then there must be some $y_1', y_2'$ such that

$$\tau_2'(x_{y_1',y_2',0,0}) = x_{y_1',y_2'+1,a_{y_1',y_2'},b_{y_1',y_2'}} \neq x_{y_1,y_2,0,0}.$$ 

Let $\tau'$ be the element of $\sigma(Z_\mu)\sigma^{-1}$ taking $x_{0,0,0,0}$ to $x_{y_1',y_2',0,0}$. Then $\tau_1^{-y_1'}\tau_2^{-y_2'}\tau' \in G$. Since $x_{0,1,0,0} = \tau_2'(x_{0,0,0,0})$, we have

$$\tau_1^{-y_1'}\tau_2^{-y_2'}\tau'(x_{0,1,0,0}) = \tau_1^{-y_1'}\tau_2^{-y_2'}\tau'_2(x_{y_1',y_2',0,0}) = x_{0,1,a_{y_1',y_2'},b_{y_1',y_2'}} \neq x_{0,1,0,0}.$$
This is a contradiction, so as noted, we have \( \tau'_2 = \tau_2 \), completing the proof in this case.

Also, if there were some \((y'_1, y'_2)\) linearly independent from \((y_1, y_2)\) such that the orbit of \(x_{y'_1, y'_2, 0, 0}\) under \(G\) were \(\{x_{y'_1, y'_2, 0, 0}\}\), then

\[
\tau'_{y_1} \tau'_{y_2} G \tau_{y_2} \tau_{y_2}^{-y_1} \tau_{y_1}^{-y_1} = G = \tau'_{y_1} \tau'_{y_2} G \tau_{y_2} \tau_{y_2}^{-y_2} \tau_{y_1}^{-y_1},
\]

so \(G\) fixes every vertex of \(\tilde{X}\). Since \(\tau_2^{-1} \tau'_2 \in G\), we would have \(\tau'_2 = \tau_2\), completing the proof in this case.

If there is no \(y_1, y_2\) as defined above, then we set \(y_1 = 1, y_2 = 0\) in the remainder of the proof.

Define blocks \(C_0, \ldots, C_{p-1}\) by

\[
C_r = \bigcup_{s=0}^{s=p-1} B_{s y_1, s y_2 + r}.
\]

Since \(y_1 \neq 0\), these blocks are distinct, and cover all vertices of \(\tilde{X}\).

We define \(h\) as follows: for vertices in \(C_r\), \(h = (\tau'_2)^r \tau_2^{-r}\). We need to show that \(h\) is an automorphism, and that it conjugates \(\tau'_2\) to \(\tau_2\) to complete the proof.

First,

\[
h^{-1} \tau'_2 h(x_{s y_1, s y_2 + r, c, d}) = h^{-1}(\tau'_2)^r h(x_{s y_1, s y_2, c, d}), \text{ and}
\]

\[
(\tau'_2)^r h(x_{s y_1, s y_2, c, d}) \in C_{r+1}, \text{ so}
\]

\[
h^{-1}(\tau'_2)^r h(x_{s y_1, s y_2, c, d}) = (\tau'_2)^{r+1}(\tau'_2)^{-(r+1)}(\tau'_2)^{r+1}(x_{s y_1, s y_2, c, d})
\]

\[
= x_{s y_1, s y_2 + r+1, c, d}
\]

\[
= \tau_2(x_{s y_1, s y_2 + r+1, c, d}).
\]

Since \(x_{s y_1, s y_2 + r, c, d}\) was an arbitrary vertex of \(\tilde{X}\), we have \(h^{-1} \tau'_2 h = \tau_2\), as required.

It remains only to show that \(h\) is an automorphism of \(\tilde{X}\).

Recall that since \(\tau_2^{-1} \tau'_2 \in G\), for any \(i, j, l, m\) we have

\[
\tau_2^{-1} \tau'_2(x_{i, j, l, m}) = x_{i, j, l + sa_1, a_2, m + sb_1, a_2}
\]
for some \( s \). Hence,

\[
\tau'_2(x_{i,j,l,m}) = x_{i,j+1,l+s_2a_1,a_2,m+sb_3,a_3}
\]

and, since this holds for any \( i, j, l, m \), we in fact see that

\[
(\tau'_2)^r(x_{i,j,l,m}) = x_{i,j+r,l+s'_2a_1,a_2,m+s'lb_3,a_3}
\]

for some \( s' \).

Now, let \( x_{s_1y_1,s_2y_2+b,c,d} \) and \( x_{s'_1y_1,s'_2y_2+j,l,m} \) be two arbitrary vertices of \( \tilde{X} \). If \( b = j \), then \( h = (\tau'_2)^b \tau'^{-b}_2 \) on both of these vertices, so will certainly take an arc to an arc and a non-arc to a non-arc. So we assume \( b \neq j \).

Then for some \( s_1 \), we have

\[
h(x_{s_1y_1,s_2y_2+b,c,d}) = (\tau'_2)^b(x_{s_1y_1,s_2y_2,c,d})
= x_{s_1y_1,s_2y_2+b,c+s_1a_1,a_2,d+s_1b_3,a_3}.
\]

Similarly, for some \( s_2 \), we have

\[
h(x_{s'_1y_1,s'_2y_2+j,l,m}) = x_{s'_1y_1,s'_2y_2+j,l+s_2a_1,a_2,m+s_2b_3,a_3}.
\]

Now, the intersection of the orbit of \( x_{(s'-s)y_1,(s'-s)y_2+(j-b),l-c,m-d} \) under the action of \( G \) with the block \( B_{(s'-s)y_1,(s'-s)y_2+(j-b)} \) is the set

\[
\{ x_{(s'-s)y_1,(s'-s)y_2+(j-b),l-c+t(a_1,a_2,m-d+tb_3,a_3) : 0 \leq t \leq p-1 \}.
\]

This is true because otherwise the vector

\[
((s'-s)y_1,(s'-s)y_2+j-b),
\]

being linearly independent from \((y_1, y_2)\), would place us back in an earlier case with the existence of a \((y'_1, y'_2)\). So there is some element \( \theta \in G \) such that

\[
\theta(x_{(s'-s)y_1,(s'-s)y_2+(j-b),l-c,m-d})
= x_{(s'-s)y_1,(s'-s)y_2+(j-b),l-c+(s_2-s_1)a_1,a_2,m-d+(s_2-s_1)b_3,a_3}.
\]
Now,

\[
\tau_1^{s_1 y_1} \tau_2^{s_2 y_2} e^{c+s_1 a_1 a_2} \tau_4^{d+s_1 b_1 a_2 \theta} \tau_4^{-c} \tau_2^{-s_2 y_2} \tau_1^{-s_1 y_1} (x_{s_1 y_1, s_2 y_2 + b, c, d})
\]

\[
= \tau_1^{s_1 y_1} \tau_2^{s_2 y_2 + b} \tau_3^{c+s_1 a_1 a_2} \tau_4^{d+s_1 b_1 a_2 \theta} \theta(x_{0,0,0,0})
\]

and

\[
\tau_1^{s_1 y_1} \tau_2^{s_2 y_2 + b} \tau_3^{c+s_1 a_1 a_2} \tau_4^{d+s_1 b_1 a_2 \theta} \tau_4^{-c} \tau_2^{-s_2 y_2} \tau_1^{-s_1 y_1} (x_{s_1 y_1, s_2 y_2 + j, l, m})
\]

\[
= \tau_1^{s_1 y_1} \tau_2^{s_2 y_2 + b} \tau_3^{c+s_1 a_1 a_2} \tau_4^{d+s_1 b_1 a_2 \theta} \theta(x_{(s'-s)y_1,(s'-s)y_2+j-b,l-c,m-d})
\]

\[
= \tau_1^{s_1 y_1} \tau_2^{s_2 y_2 + b} \tau_3^{c+s_1 a_1 a_2} \tau_4^{d+s_1 b_1 a_2 \theta}
\]

\[
(x_{(s'-s)y_1,(s'-s)y_2+j-b,l-c,m-d+s_2-s_1)b_1, a_2)
\]

\[
= x_{s_1 y_1, s_2 y_2 + j+l+s_2 a_1, a_2, m+s_2 b_1, a_2}.
\]

This has shown that \( h \) is indeed an automorphism of \( \tilde{X} \), completing the proof, since \( h \) respects all of the standard blocks and so is in \( P \).

\[
\square
\]

## 2.7 Conjugation of \( \sigma(Z_p^4)_L \sigma^{-1} \) to Obtain a Group that Contains \( \tau_1 \)

### 2.7.1 Finding the conjugate \( \psi \sigma(Z_p^4)_L \sigma^{-1} \psi^{-1} \)

**Lemma 2.7.1** Let \( \sigma(Z_p^4)_L \sigma^{-1} \) be any conjugate of \( (Z_p^4)_L \) such that \( \sigma(Z_p^4)_L \sigma^{-1} \leq P \), where \( P \) is a fixed Sylow \( p \)-subgroup of \( \text{Aut}(\tilde{X}) \) that contains \( (Z_p^4)_L \), and \( \tau_2, \tau_3, \tau_4 \in \sigma(Z_p^4)_L \sigma^{-1} \). Then there exists some \( \psi \in P \) such that \( \psi \sigma(Z_p^4)_L \sigma^{-1} \psi^{-1} \) contains \( \tau_1, \tau_2, \tau_3 \) and \( \tau_4 \).

**Proof.** We consider \( \tau'_1 \), the element of \( \sigma(Z_p^4)_L \sigma^{-1} \) satisfying \( \tau'_1(x_{0,0,0,0}) = x_{1,0,0,0} \). It is certainly apparent that \( \tau'_1(B_i) = B_{i+1} \) for any \( i \). If we also have that

\[
\tau'_1(x_{i,j,k,l}) = x_{i+1,j+a,k+b,l+c}, \quad \text{then}
\]

\[
\tau'_1(x_{i,j',k',l'}) = x_{i+1,j'+a,k'+b,l'+c},
\]

then
for any $j', k', l'$ since $\tau'_1$ commutes with $\tau_2, \tau_3$ and $\tau_4$. Hence the action of $\tau'_1$ is completely determined by the $p$ triples

$$(a_0, b_0, c_0) = (0, 0, 0), (a_1, b_1, c_1), \ldots, (a_{p-1}, b_{p-1}, c_{p-1}).$$

Define the function $\psi$ as follows:

$\psi$ commutes with $\tau_2, \tau_3$ and $\tau_4$, and

$$\psi^{-1}(x_{i,0,0,0}) = (\tau'_1)^i(x_{0,0,0,0})$$

for any $i$, where $(\tau'_1)^0$ is considered to be the identity.

First we show that $\psi \tau'_1 \psi^{-1} = \tau_1$. For any $i, j, k, l$, we have

$$\psi \tau'_1 \psi^{-1}(x_{i,j,k,l}) = \psi((\tau'_1)^i + 1 \tau_1^{-1})(x_{i,j,k,l})$$

$$= \tau_1^{i+1} \tau_1^{-1}(x_{i,j,k,l})$$

$$= \tau_1(x_{i,j,k,l}),$$

as required.

There is an alternative and perhaps more intuitive way of showing this. Notice that the disjoint cycle notation for $\tau'_1$ consists of $p^3$ cycles of the form

$$(x_{0,k,j,k,l} x_{1,j,k,l} x_{2,j+a_1,k+a_2,l+a_3} \cdots x_{p-1,j+a_1 \cdots a_{p-2}, k+b_1 \cdots b_{p-2}, l+c_1 \cdots c_{p-2}}).$$

Also,

$$\psi(x_{i,j+a_1 \cdots a_{i-1}, k+b_1 \cdots b_{i-1}, l+c_1 \cdots c_{i-1}}) = x_{i,j,k,l}$$

for any $i > 1$, while $\psi(x_{1,j,k,l}) = x_{1,j,k,l}$ and $\psi(x_{0,j,k,l}) = x_{0,j,k,l}$. From this, it is easy to verify that the disjoint cycle notation for $\psi \tau'_1 \psi^{-1}$ will consist of $p^3$ cycles of the form

$$(x_{0,j,k,l} x_{1,j,k,l} \cdots x_{p-1,j,k,l}),$$

which is precisely the form of $\tau_1$.

Now we must show that $\psi$ is an automorphism of $\bar{X}$. Suppose that there is a red arc from the vertex $x_{i,j,k,l}$ to the vertex $x_{i',j',k',l'}$. Then showing that there must be
a red arc from \( \psi^{-1}(x_{i,j,k,l}) \) to \( \psi^{-1}(x_{i',j',k',l'}) \) will be sufficient to complete the entire proof.

If \( i = i' \), then since \( \psi \) commutes with \( \tau_2, \tau_3 \) and \( \tau_4 \), it is immediately apparent that the appropriate red arc will exist. So we assume \( i \neq i' \). Now,

\[
\psi^{-1}(x_{i,j,k,l}) = (\tau_1')^i(x_{0,j,k,l})
= x_{i,j+a_0+...+a_{i-1}, k+b_0+...+b_{i-1}, l+c_0+...+c_{i-1}}, \quad \text{and}
\psi^{-1}(x_{i',j',k',l'}) = (\tau_1')^{i'}(x_{0,j',k',l'})
= x_{i',j'+a_0+...+a_{i'-1}, k'+b_0+...+b_{i'-1}, l'+c_0+...+c_{i'-1}}.
\]

Let \( B_r \) be any \( p^3 \)-block of \( \text{Aut}(\tilde{X}) \), with \( r \neq 0 \). We show that the orbit of \( x_{r,0,0,0} \) under \( G \) contains the set of vertices in \( B_r \) spanned by the vectors

\[
\{(a_s, b_s, c_s) : 0 \leq s \leq p - 1\}
\]

as defined in Definition 2.2.8. Towards a contradiction, suppose that this were not the case. Then there must be some vector \( (a_s, b_s, c_s) \) and some \( b', c', d', z \) such that the vertex \( x_{s,b',c',d'} \) is in the orbit of \( x_{r,0,0,0} \) under \( G \), but the vertex \( x_{r,b'+za_s,c'+zb_s,d'+zc_s} \) is not in this orbit. Since \((a_0, b_0, c_0) = (0,0,0)\), this clearly cannot occur if \( s = 0 \). So by Lemma 2.7.2 (stated and proven later), the vertex \( x_{s,b',c',d'} \) must be in the orbit of \( x_{r,0,0,0} \) under \( G \). We know that \((\tau_2^{-1} \tau_1')^z \in G\), and

\[
(\tau_2^{-1} \tau_1')^z(x_{s,b',c',d'}) = x_{s,b'+za_s,c'+zb_s,d'+zc_s},
\]

so \( x_{s,b'+za_s,c'+zb_s,d'+zc_s} \) is in the orbit of \( x_{r,0,0,0} \) under \( G \). But then by Lemma 2.7.2, it is also in the orbit of \( x_{r,0,0,0} \) under \( G \), the desired contradiction.

In particular, we have shown that the orbit of \( x_{i'-i,0,0,0} \) under \( G \) contains the vertex \( x_{i'-i,a,...+a_{i-1},b,...+b_{i-1},c,...+c_{i-1}} \). This has shown that there must be a red arc from \( \psi^{-1}(x_{i,j,k,l}) \) to \( \psi^{-1}(x_{i',j',k',l'}) \) above, as required. So \( \psi \) is an automorphism of \( \tilde{X} \). Since \( \psi \) respects all of the standard blocks, it is clear that \( \psi \in P \). \qed
2.7.2 Orbits of $G$ when $\tau'_1 \neq \tau_1$

The group $G$ is defined to be the subgroup of $(\tau'_1, \tau_1, \tau_2, \tau_3, \tau_4)$ that fixes $x_{0,0,0,0}$. Notice since every element of $G$ commutes with $\tau_2, \tau_3, \tau_4$, that every element of $G$ in fact fixes every vertex in $B_0$.

Lemma 2.7.2 Suppose that the orbit of $x_{i,0,0,0}$ ($i \neq 0$) under $G$ is known to be the set in $B_i$ spanned by the vectors $v_1, v_2$ and $v_3$. Then the orbit of $x_{ri,0,0,0}$ under $G$ is the set in $B_{ri}$ spanned by the vectors $v_1, v_2$ and $v_3$ for any $r \neq 0$.

Proof. We break the proof down into four cases, depending on the length of the known orbit.

Case 1. The set in $B_i$ spanned by the vectors $v_1, v_2$ and $v_3$ has cardinality 1; that is, $v_1 = v_2 = v_3 = (0,0,0)$. Clearly in this case, we have $G = \tau'_1G\tau_1^{-i}$, so $G = \tau_1^rG\tau_1^{-ri}$ for any $r$. Hence $G$ fixes every vertex in $X$, and the result is apparent.

Case 2. The set in $B_i$ spanned by the vectors $v_1, v_2$ and $v_3$ has cardinality $p$; that is, $v_1, v_2$ and $v_3$ are collinear but not all $0$. Without loss of generality, suppose that

$$v_2 = (s_2, s_3, s_4) \neq (0,0,0).$$

We claim that the orbit of $x_{ki,0,0,0}$ under $G$ is contained within the set in $B_{ki}$ spanned by $v_2$ for any $k$.

We prove the claim by induction on $k$. The base case $k = 1$ is the hypothesis of the lemma. Suppose that the claim is true for $k$, and we will show that it must be true for $k + 1$.

Let $\theta$ be any element of $G$. By the induction hypothesis,

$$\theta(x_{ki,0,0,0}) = x_{ki,s_2,s_3,s_4},$$

for some $s$. Hence

$$\tau_2^{-s_2} \tau_3^{-s_3} \tau_4^{-s_4} \theta \in \tau_1^k G \tau_1^{-ki}.$$
From the hypothesis of the theorem, we know that the orbit of $x_{(k+1)i,0,0,0}$ under $\tau_1^k G \tau_1^{-k_i}$ must be the set in $B_{(k+1)i}$ spanned by the vector $\vec{v}_2$. Thus,

$$\tau_2^{-ss_2} \tau_3^{-ss_3} \tau_4^{-ss_4} \theta(x_{(k+1)i,0,0,0}) = x_{(k+1)i,0,0,0}$$

for some $s'$. So we have

$$\theta(x_{(k+1)i,0,0,0}) = x_{(k+1)i,0,0,0}.$$

This is within the set claimed, and since $\theta$ was an arbitrary element of $G$, we have proven the claim.

So we see that the orbit of $x_{ri,0,0,0}$ under $G$ is contained within the set in $B_{ri}$ spanned by $\vec{v}_1, \vec{v}_2$ and $\vec{v}_3$. If for some $r \neq 0$ the orbit of $x_{ri,0,0,0}$ under $G$ were not the entire set given, then this orbit would have to be the singleton $\{x_{ri,0,0,0}\}$. But then we could use $x_{ri,0,0,0}$ in Case 1 of this lemma to show that the orbit of $x_{i,0,0,0}$ must be the singleton $\{x_{i,0,0,0}\}$, a contradiction. This concludes the result for Case 2.

Case 3. The set in $B_i$ spanned by the vectors $\vec{v}_1, \vec{v}_2$ and $\vec{v}_3$ has cardinality $p^2$; that is, $\vec{v}_1, \vec{v}_2$ and $\vec{v}_3$ are coplanar but not collinear. Without loss of generality, suppose that $\vec{v}_2$ and $\vec{v}_3$ are linearly independent. Then clearly they span the subspace spanned by the three coplanar vectors, so the set in $B_i$ spanned by these two vectors is the same as the set in $B_i$ spanned by all three vectors.

We claim that for any $k$, the orbit of $x_{ki,0,0,0}$ under $G$ is contained within the set in $B_{ki}$ spanned by the vectors $\vec{v}_1$ and $\vec{v}_2$. We will prove this claim by induction on $k$. The base case of $k = 1$ is given by the hypothesis of the lemma. Suppose that the claim is true for $k$, and we will show that it must be true for $k + 1$.

Let $\theta$ be any element of $G$. By the induction hypothesis,

$$\theta(x_{ki,0,0,0}) = x_{ki,0,0,0}$$

for some $s, t$. Hence

$$\tau_2^{-ss_2-tt_2} \tau_3^{-ss_3-tt_3} \tau_4^{-ss_4-tt_4} \theta \in \tau_1^k G \tau_1^{-k_i}.$$
From the hypothesis of the theorem, we know that the orbit of $x_{(k+1)i,0,0,0}$ under $\tau_1^{k_1} G\tau_1^{-k_1}$ must be the set in $B_{(k+1)i}$ spanned by the vectors $\vec{v}_2$ and $\vec{v}_3$. Thus,

$$\tau_2^{s_2+t_2} \tau_3^{s_3+t_3} \tau_4^{s_4+t_4} \theta(x_{(k+1)i,0,0,0}) = x_{(k+1)i,s's_2+t_2,s's_3+t_3,s's_4+t_4}$$

for some $s', t'$. So we have

$$\theta(x_{(k+1)i,0,0,0}) = x_{(k+1)i,(s+s')s_2+(t+t')t_2,(s+s')s_3+(t+t')t_3,(s+s')s_4+(t+t')t_4}.$$

This is within the set claimed, and since $\theta$ was an arbitrary element of $G$, we have proven the claim.

So we see that the orbit of $x_{ri,0,0,0}$ under $G$ is contained within the set in $B_{ri}$ spanned by $\vec{v}_1, \vec{v}_2$ and $\vec{v}_3$. If for some $r \neq 0$ the orbit of $x_{ri,0,0,0}$ under $G$ were not the entire set given, then this orbit would have to be the singleton $\{x_{ri,0,0,0}\}$ or the set in $B_{ri}$ spanned by a single vector. But then we could use $x_{ri,0,0,0}$ in Case 1 or Case 2 of this lemma respectively to show that the orbit of $x_{ri,0,0,0}$ must be the singleton $\{x_{i,0,0,0}\}$ or a set in $B_i$ spanned by a single vector, a contradiction. This concludes the result for Case 3.

Case 4. The set in $B_i$ spanned by the vectors $\vec{v}_1, \vec{v}_2$ and $\vec{v}_3$ has cardinality $p^3$; that is, $\vec{v}_1, \vec{v}_2$ and $\vec{v}_3$ are linearly independent. So the block $B_0$ is forced by the action of $G$ to be wreathed with the block $B_i$. If for some $r \neq 0$, the block $B_0$ were not wreathed with the block $B_{ri}$, then using Case 1, 2 or 3 of this lemma, we could show that the block $B_i$ could not be forced by the action of $G$ to be wreathed with the block $B_0$, a contradiction. This concludes the proof of the lemma. \[\square\]
Chapter 3

Toida’s Conjecture is True

3.1 History of the Problem

The following result was first proven by Turner in 1967.

Theorem 3.1.1 (Turner, [95]) The permutation group $\mathbb{Z}_n$ is a CI-group for any prime $p$.

In 1977, Toida published a conjecture refining the conjecture that had been proposed by Ádám in 1967 and disproven in 1970. Toida’s conjecture [94] suggests that if $\vec{X} = \vec{X}(\mathbb{Z}_n; S)$ and if $S$ is a subset of $\mathbb{Z}_n$, then $\vec{X}$ is a CI-digraph.

Although this conjecture has aroused some interest, prior to this thesis, it had only been proven in the special case where $n$ is a prime power. This proof was given by Klin and Pöschel [46], [47] and Golpand, Najmark and Pöschel [32].

This chapter provides a proof that Toida’s conjecture is in fact true. The work in this chapter was conducted jointly with Dr. Edward Dobson of Mississippi State University, with some assistance from Dr. David Witte of Oklahoma State University, as noted later.

3.2 Background Definitions and Theory

We include here a number of definitions and results from graph theory and group theory that are not used in the other chapters of this thesis.
Theorem 3.2.1 ([96], Proposition 6.2) If $g \in G$, $H \leq G$, and $B$ is an $H$-block, then $g(B)$ is a $gHg^{-1}$-block. In particular, if $N \trianglelefteq G$ and $B$ is an $N$-block, then $g(B)$ is an $N$-block for all $g \in G$.

Theorem 3.2.2 Let $x$ be an $n$-cycle in $S_n$ and $n = mk$. The centraliser in $S_n$ of $(x^m)$ is isomorphic to $S_m \wr \mathbb{Z}_k$.

**Proof.** Let the elements of the set $V$ upon which $S_n$ is acting be the pairs $(a, b)$, where $0 \leq a \leq m - 1$ and $0 \leq b \leq k - 1$. Without loss of generality, we can relabel the elements of $V$ if necessary to enable us to assume that $x^m(a, b) = (a, b + 1)$ for every $0 \leq a \leq m - 1$ and $0 \leq b \leq k - 1$, where calculations in the second coordinate are performed modulo $k$.

If $g$ is in the centraliser in $S_n$ of $(x^m)$, then for any $i$, $gx^mg = x^mg$, so $g(a, b + i) = x^m(a, b)$ for any $0 \leq a \leq m - 1$ and $0 \leq b \leq k - 1$. Let $\alpha \in S_m$, $\beta_a \in S_k$ (for every $a$) be defined in such a way that $g(a, b) = (\alpha(a), \beta_a(b))$. Then we have $(\alpha(a), \beta_a(b + i)) = (\alpha(a), \beta_a(b) + i)$, meaning that $\beta_a(b + i) = \beta_a(b) + i$ for any $i$ and for any $0 \leq a \leq m - 1$ and $0 \leq b \leq k - 1$, where calculations are performed modulo $k$. Thus, we must have $\beta_a(b) = b + c_a$ for some constant $c_a$ with $0 \leq c_a \leq k - 1$. So $g(a, b) = (\alpha(a), b + c_a)$ where $\alpha \in S_m$. It is clear from the definition of the wreath product of permutation groups that $g \in S_m \wr \mathbb{Z}_k$, as required. This completes the proof. \qed

Definition 3.2.3 The **complete digraph** on $n$ vertices is the digraph $\vec{K}(V, A)$, where $A$ consists of all possible ordered pairs of vertices from the set $V$. It is denoted by $K_n^2$.

**Definition 3.2.4** We say that the arc $(u, v)$ is within the set of vertices $V'$ if $u, v \in V'$.

The notion of transitivity for permutation groups can be generalised.
Definition 3.2.5 The permutation group $G$ acting on the set $V$ is $k$-transitive if given any two $k$-tuples $(v_1,\ldots,v_k)$ and $(u_1,\ldots,u_k)$ with $v_1,\ldots,v_k, u_1,\ldots,u_k \in V$, there exists some $g \in G$ such that $g(v_i) = u_i$ for $1 \leq i \leq k$.

In particular, we often say that a 2-transitive group is doubly transitive.

Definition 3.2.6 Let $g$ be a permutation from a permutation group of degree $n$.

The action of $g$ is semi-regular if there exists some $d$ such that the disjoint cycle notation for $g$ consists of $d$ cycles of length $d'$, where $dd' = n$ and $d, d' \neq 1$.

Notation 3.2.7 Let $G$ be a transitive permutation group admitting a complete block system $\mathcal{B}$ of $m$ blocks of size $k$. For $g \in G$, define $g/\mathcal{B}$ in the permutation group $S_m$ by $g/\mathcal{B}(i) = j$ if and only if $g(B_i) = B_j$, $B_i, B_j \in \mathcal{B}$.

Notation 3.2.8 In cases where the group referred to may be unclear, we denote the identity element of the group $G$ by $1_G$.

Definition 3.2.9 Let $B$ be a $G$-block. If the order of the permutation group $G$ is equal to the order of $G|_B$, then the action of $G|_B$ is said to be faithful.

Using Theorem 1.2.30, it is easy to show that $G|_B$ is faithful if and only if $\text{Stab}_G(B) = 1$. This can be used as an alternative definition of faithfulness, and is generally the criterion used to show that some action is faithful, or alternatively that the action is not faithful.

Definition 3.2.10 Let $B_1$ and $B_2$ be $G$-blocks. We say that $G|_{B_1}$ is equivalent to $G|_{B_2}$ if there is a permutation group isomorphism from $G|_{B_1}$ to $G|_{B_2}$.

Definition 3.2.11 The abstract group $G$ has $k$ representations of degree $n$ if there are precisely $k$ nonisomorphic permutation groups of degree $n$ for which the abstract group is isomorphic to $G$.

Definition 3.2.12 The abstract group $G$ is a Burnside group if every primitive permutation group containing the regular representation of $G$ as a transitive subgroup is doubly transitive.
Burnside gave the first example of such a group, hence the name. This is extremely useful in the theory of circulant graphs, due to the following theorem.

**Theorem 3.2.13 ([96], Theorem 25.3)** Every cyclic group of composite order is a Burnside group. That is, every permutation group containing the regular representation of a cyclic group of composite order as a transitive subgroup is either imprimitive or doubly transitive.

This chapter of the thesis relies more heavily on abstract group theory than the other chapters. A few of the definitions from abstract algebra that are particularly critical for understanding this chapter are included here; however, it is impractical to include the extent of background and definitions required for full understanding. For terminology and notation not explained within this thesis, the reader is referred to [38] or [89].

**Definition 3.2.14** The socle of the abstract group $G$, denoted by soc$(G)$, is the group $\langle N_1, \ldots, N_k \rangle$, where $N_1, \ldots, N_k$ are all of the minimal normal subgroups of $G$.

In the cases that arise within this chapter of the thesis, the minimal normal subgroup of $G$ is always unique, so the socle is in fact a minimal normal subgroup of $G$.

**Definition 3.2.15** The abstract group $G$ is solvable if there exists a chain of normal subgroups

$$1 = N_0 \triangleleft N_1 \triangleleft \ldots \triangleleft N_k = G$$

such that $N_i/N_{i-1}$ is a cyclic group for $1 \leq i \leq k$.

It is straightforward to show that any abelian group must be solvable.

**Definition 3.2.16** The abstract group $G$ is simple if it contains no normal subgroups other than the trivial subgroups $1$ and $G$.

So if $G$ is simple, then $N \triangleleft G$ implies that either $N = 1$ or $N = G$. 
Definition 3.2.17 A transposition is a permutation whose disjoint cycle decomposition consists of a single cycle of length 2 (where cycles of length 1 are omitted).

Definition 3.2.18 The alternating group of degree $n$, denoted by $A_n$, is the subgroup of $S_n$ consisting of all elements that can be written as a product of an even number of transpositions.

Theorem 3.2.19 ([96]. Theorem 9.7) The permutation group $A_n$ is $(n-2)$-transitive for $n \geq 3$.

Theorem 3.2.20 (Exercise 1. pg. 169, [43]) A doubly transitive solvable group of degree $n$ containing an $n$-cycle must have $n = 4$.

The following very powerful result is a cornerstone of the proof. In a number of instances, it allows us to say with certainty what the action of the automorphism group of a unit circulant digraph must be, and to exploit known properties of $A_m$, $S_m$ and $PSL(d, q)$. As a consequence of this theorem, it will be useful to consider these specific group actions in more detail later.

Theorem 3.2.21 ([33]. Theorem 1.49) If $H$ is a nonsolvable doubly transitive permutation group of degree $m$ that contains an $m$-cycle, then one of the following holds:

(i) $H \cong A_m$ or $S_m$;

(ii) $m = 11$ and $H = PSL(2, 11)$ or $M_{11}$;

(iii) $m = 23$ and $H \cong M_{23}$;

(iv) $m = (q^d - 1)/(q - 1)$ for some prime power $q$ and $H$ is isomorphic to a subgroup of $PGL(d, q)$ containing $PSL(d, q)$.

Peter Cameron gives the following list of groups that can occur as socles of doubly transitive groups of degree $n$. This list can be combined with the previous result to tell us more about the structure of the groups that arise in the context of this chapter.
Theorem 3.2.22 ([13], pp. 8-9) Let $G$ be a doubly transitive group of degree $n$. Then the socle of $G$ is one of the following:

(i) $A_n$, $n \geq 5$, acting as a permutation group of degree $n$;
(ii) $\text{PSL}(d,q)$, $d \geq 2$, acting as a permutation group of degree $(q^d - 1)/(q - 1)$;
(iii) $\text{PSU}(3,q)$, acting as a permutation group of degree $q^3 + 1$;
(iv) $^2B_2(q)$ (Suzuki), acting as a permutation group of degree $q^2 + 1$;
(v) $^2G_2(q)$ (Ree), acting as a permutation group of degree $q^3 + 1$;
(vi) $\text{PSp}(2d,2)$, acting as a permutation group of degree $2^{2d-1} + 2^{d-1}$;
(vii) $\text{PSp}(2d,2)$, acting as a permutation group of degree $2^{2d-1} - 2^{d-1}$;
(viii) $\text{PSL}(2,11)$, acting as a permutation group of degree 11;
(ix) $\text{PSL}(2,8)$, acting as a permutation group of degree 28;
(x) $A_7$, acting as a permutation group of degree 15;
(xi) $M_{11}$ (Mathieu), acting as a permutation group of degree 11 or 12;
(xii) $M_{12}$ (Mathieu), acting as a permutation group of degree 12;
(xiii) $M_{22}$ (Mathieu), acting as a permutation group of degree 22;
(xiv) $M_{23}$ (Mathieu), acting as a permutation group of degree 23;
(xv) $M_{24}$ (Mathieu), acting as a permutation group of degree 24;
(xvi) $\text{HS}$ (Higman-Sims), acting as a permutation group of degree 176;
(xvii) $\text{Co}_3$ (Conway), acting as a permutation group of degree 276;

The socle is at least doubly transitive except when it is $\text{PSL}(2,8)$ acting as a permutation group of degree 28.

Furthermore, $\text{PSL}(2,q)$ has a unique representation of degree $q + 1$; $A_n$, $n \geq 5$, $n \neq 6$ has a unique representation of degree $n$; $M_{11}$ has a unique representation of degree 11; $M_{23}$ has a unique representation of degree 23; $\text{PSL}(d,q)$ has two representations of degree $(q^d - 1)/(q - 1)$; $A_6$ has two representations of degree 6; and
none of the groups mentioned in this theorem has three or more representations of the degrees listed.

**Definition 3.2.23** The digraph $\vec{X}$ is a **circulant digraph** if it is a Cayley digraph on a cyclic group.

**Definition 3.2.24** The digraph $\vec{X}$ is a **unit circulant** if it is a circulant digraph of order $n$ whose connection set is a subset of $\mathbb{Z}_n$.

Let $x: \mathbb{Z}_n \to \mathbb{Z}_n$ by $x(i) = i + 1$. We use this conceptualisation of the $n$-cycle $x$ at times in what follows.

Now we are ready to proceed with the proof of Toida's conjecture.

### 3.3 Main Theorem

Some of the technical parts of the proof of the following theorem will be postponed to later sections.

**Theorem 3.3.1** Let $\vec{X}$ be a unit circulant digraph on $n$ vertices. Then $\vec{X}$ is a CI-digraph.

**Proof.** Let $x, y$ be $n$-cycles in $\text{Aut}(\vec{X})$. Let

$$Y = \{y' \in \text{Aut}(\vec{X}) : \text{there exists } \gamma \in \text{Aut}(\vec{X}) \text{ such that } \gamma^{-1}y\gamma = y'\}.$$ 

By Theorem 1.3.1, we need only show that $x \in Y$.

If $\text{Aut}(\vec{X})$ is doubly transitive, then $\vec{X} \in \{E_n, K_n^2\}$, $\text{Aut}(\vec{X}) = S_n$, and we are done. Since any cyclic group of degree $n$ is a Burnside group if $n$ is composite by Theorem 3.2.13, and the result of this theorem is known for $n$ prime (Theorem 3.1.1), the only remaining possibility is that $\text{Aut}(\vec{X})$ is imprimitive.

In order to enable us to use Lemma 3.5.4 (stated and proven later), the proof will proceed by induction on the number of prime factors of $n$. The base case where $n$ is prime is given by Theorem 3.1.1, so in what follows, we can assume that any
digraphs of strictly smaller order than \( n \) that are unit circulant digraphs are in fact CI-digraphs.

Choose \( y' \in Y \) in such a way that \( \langle x^a \rangle = \langle (y')^a \rangle \), where \( a \) is as small as possible \( (0 < a \leq n) \). If \( \gcd(a, n) = k \), then \( \langle (y')^k \rangle = \langle x^k \rangle \), so by the choice of \( a \), \( k = a \). Thus, we must have that \( a|n \), say \( ab = n \), and by Theorem 1.2.56, the orbits of \( x^a \) are blocks of \( \langle x, y' \rangle \), yielding a complete block system \( B \) consisting of \( a \) blocks of size \( b \).

We will deal with the case \( a = n \) later; for now we assume that the blocks are nontrivial (if \( a = 1 \), then we are done).

Suppose that \( \text{Stab}_{\langle x, y' \rangle}(B) \) is not faithful on some block \( B \) of \( B \). Since \( \langle x^a \rangle = \langle (y')^a \rangle \), every element of \( \langle x, y' \rangle \) commutes with \( x^a \). Hence Lemma 3.5.5 (stated and proven later) applies, and we have some complete block system \( F \) consisting of \( n/p \) blocks of size \( p \) for some prime \( p \) such that the action of \( \text{Stab}_{\langle x, y' \rangle}(F) \) is not faithful.

Now Lemma 3.5.1 (stated and proven later) applies (we use Corollary 1.2.55 to see that the action is primitive). Since the action of \( \text{Stab}_{\langle x, y' \rangle}(F) \) is not faithful, there are clearly at least two blocks in the block system formed in Lemma 3.5.1. Denote this block system by \( E \). If vertices of \( \tilde{X} \) are labeled \( 0, 1, \ldots, n - 1 \), according to the action of \( x \), then the vertices in the block \( E \) of \( E \) that contains the vertex 0 form the exponents of a proper subgroup of \( \langle x \rangle \), by Theorem 1.2.57. Since \( \tilde{X} \) is a unit circulant digraph, there can be no arcs within the block \( E \); and since the action of \( \langle x \rangle \) is transitive on the blocks of \( E \), there are no arcs within any block of \( E \). If there is an arc from some vertex in the block \( F \) of \( F \) to some vertex in the block \( F' \) of \( F \), where \( F \) and \( F' \) are in different blocks of \( E \), then Lemma 3.5.1 tells us that all arcs from \( F \) to \( F' \) exist (take \( \langle x^a \rangle|_E \), where \( F \in E' \)). Thus \( \tilde{X} = \tilde{X}/F \mathcal{I} \langle \tilde{X}[F] \rangle \) for \( F \in F \). Since \( \tilde{X}[E] \) contains no arcs for any \( E \in E \), we certainly have \( \tilde{X}[F] \) contains no arcs for any \( F \in F \). Thus \( \tilde{X} = \tilde{X}/F \mathcal{I} E_p \). It is not hard to see that since \( \tilde{X} \) is a unit circulant digraph, \( \tilde{X}/F \) is also a unit circulant digraph on fewer than \( n \) vertices, and hence is a CI-digraph. If \( \tilde{X}/F \) is reducible, say \( \tilde{X}/F = \tilde{X}' \mathcal{I} E_k \), then \( \tilde{X} = (\tilde{X}' \mathcal{I} E_k) \mathcal{I} E_p = \tilde{X}' \mathcal{I} E_{kp} \). We continue this reduction until we reach a digraph \( \tilde{X}' \) such that \( \tilde{X}' \) is irreducible and \( \tilde{X} = \tilde{X}' \mathcal{I} E_{kp} \) for some \( k \). Then by Lemma 3.5.4,
since \( p \geq 2 \), \( \bar{X} \) is a CI-digraph, and we are done.

Thus, in what follows, we may assume that unless \( a = n \), we have \( \text{Stab}_{\langle x, y' \rangle}(B) \) is faithful.

By Theorem 3.2.13 again, we have only four cases to consider: (1) \( a \) is prime; (2) the action of \( \langle x, y' \rangle/B \) is imprimitive; (3) the action of \( \langle x, y' \rangle/B \) is doubly transitive; and (4) \( a = n \).

**Case 1.** The number \( a \) is prime, say \( a = p \). Thus we have \( \langle x^p \rangle = \langle (y')^p \rangle \). Notice that every element of \( \langle x, y' \rangle \) must commute with \( x^p \).

Now, by Theorem 1.2.35. \( x/B \) and \( y'/B \) are both contained in (possibly distinct) Sylow \( p \)-subgroups of \( \langle x, y' \rangle/B \), and by Theorem 1.2.34, these Sylow \( p \)-subgroups are conjugate in \( \langle x, y' \rangle/B \). So there exists some \( \delta \in \langle x, y' \rangle \) such that \( \delta^{-1}y'^{\delta}/B \) is in the same Sylow \( p \)-subgroup of \( \langle x, y' \rangle/B \) as \( x/B \). Hence

\[
\delta^{-1}y'^{\delta}/B \in \langle x \rangle/B.
\]

Suppose that \( \delta^{-1}y'^{\delta}/B = x^i/B \).

(Note that since \(|\delta^{-1}y'^{\delta}| = n\), we certainly cannot have \( i = 0 \). Then

\[
x^{-i}\delta^{-1}y'^{\delta} \in \text{Stab}_{\langle x, y' \rangle}(B).
\]

Now, let the vertices of \( \bar{X} \) be labeled by the integers (modulo \( n \)) according to the action of \( x \), so that \( B_j \), the \( j \)th block of \( B \), consists of all vertices whose residue (modulo \( p \)) is \( j \). Suppose that

\[
\delta^{-1}y'^{\delta}(j) = j + i + k_j p
\]

for some \( k_j \). Recall that \( \delta^{-1}y'^{\delta} \) commutes with \( x^p \). Hence

\[
\delta^{-1}y'^{\delta}(j + k'p) = \delta^{-1}y'^{\delta}x^{k'p}(j) = x^{k'p}\delta^{-1}y'^{\delta}(j) = x^{k'p}(j + i + k_j p) = j + i + (k_j + k')p
\]
for any \( k' \). We have just shown that

\[
x^{-i}\delta^{-1}y'\delta|_B \in \langle x^p \rangle|_B
\]

for any \( B \in \mathcal{B} \).

Let \( k_0 \) be such that

\[
x^{-i}\delta^{-1}y'\delta|_{B_0} = x^{k_0p}|_{B_0}.
\]

Then \( x^{-i-k_0p}\delta^{-1}y'\delta|_{B_0} = 1 \)

Since the action of \( \text{Stab}_{(x,y')}(\mathcal{B}) \) is faithful, we have

\[
x^{-i-k_0p}\delta^{-1}y'\delta = 1.
\]

Hence \( \delta^{-1}y'\delta = x^{i+k_0p} \),

so \( \delta^{-1}y'\delta \in Y \), and \( \langle \delta^{-1}y'\delta \rangle = \langle x \rangle \), contradicting the choice of \( y' \).

Case 2. The action of \( \langle x, y' \rangle/B \) is imprimitive. Let this action admit a complete block system \( C \) of \( r \) blocks of size \( s \), where \( s \) is chosen to be as small as possible. Note that \( rs = a \), by Theorem 1.2.54.

Subcase (a). The size \( s \) of the blocks is prime, \( s = p \). This proof is very similar to the proof for Case 1.

Now, by Theorem 1.2.35, \( x^r/B \) and \( (y')^r/B \) are both contained in Sylow \( p \)-subgroups of \( \langle x, y' \rangle/B \) (which may be distinct), and by Theorem 1.2.34, these Sylow \( p \)-subgroups are conjugate in \( \langle x, y' \rangle/B \). So there exists some \( \delta \in \langle x, y' \rangle \) such that \( \delta^{-1}(y')^r\delta/B \) is in the same Sylow \( p \)-subgroup of \( \langle x, y' \rangle/B \) as \( x^r/B \). Hence

\[
\delta^{-1}(y')^r\delta/B \in \langle x^r \rangle/B.
\]

Suppose that \( \delta^{-1}(y')^r\delta/B = x^{ir}/B \).

(Note that since \( |\delta^{-1}(y')^r\delta| = bs \), we certainly cannot have \( i = 0 \).) Then

\[
x^{-ir}\delta^{-1}(y')^r\delta \in \text{Stab}_{(x,y')}(\mathcal{B}).
\]
We know that
\[ x^{-ir} \delta^{-1}(y')^r \delta \in \text{Stab}_{(x,y')}(B). \]

Let the vertices of $\tilde{X}$ be labeled with the integers (modulo $n$) according to the action of $x$, so that $B_j$, the $j$th block of $B$, consists of all vertices whose residue (modulo $a$) is $j$. Suppose that
\[ \delta^{-1}(y')^r \delta(j) = j + ir + k_j a \]
for some $k_j$. Recall that $\delta^{-1}(y')^r \delta$ commutes with $x^a$. Hence
\[
\begin{align*}
\delta^{-1}(y')^r \delta(j + k'a) &= \delta^{-1}(y')^r \delta x^{k'a}(j) \\
&= x^{k'a} \delta^{-1}(y')^r \delta(j) \\
&= x^{k'a}(j + ir + k_j a) \\
&= j + ir + (k_j + k')a
\end{align*}
\]
for any $k'$. We have just shown that
\[ x^{-ir} \delta^{-1}(y')^r \delta|_B \in (x^a)|_B \]
for any $B \in \mathcal{B}$.

Let $k_0$ be such that
\[ x^{-ir} \delta^{-1}(y')^r \delta|_{B_0} = x^{k_0 a}|_{B_0}. \]
Then $x^{-ir-k_0 a} \delta^{-1}(y')^r \delta|_{B_0} = 1$.

Since the action of $\text{Stab}_{(x,y')}(\mathcal{B})$ is faithful, we have
\[ x^{-ir-k_0 a} \delta^{-1}(y')^r \delta = 1. \]
Hence $\delta^{-1}(y')^r \delta = x^{ir+k_0 a}$,
so $\delta^{-1}y' \delta \in Y$, and $\langle (\delta^{-1}y' \delta)^r \rangle = \langle x^r \rangle$, contradicting the choice of $y'$.

Subcase (b). The size $s$ of the blocks is composite. Since $s$ is as small as possible, by Theorem 3.2.13, $\text{Stab}_{(x,y')}(\mathcal{C})|_C$ is doubly transitive. Let $N$ be the socle
of \(\text{Stab}(x,y')(C)|_C\). By the list in Theorem 3.2.22, \(N\) is certainly nonabelian and \(N\) is at least doubly transitive, unless \(N = \text{PSL}(2,8)\) and \(|C| = 28\). However, this group does not arise as the socle of any group given in Theorem 3.2.21, so \(N\) is nonabelian, doubly transitive and simple. We know that every element of \(<x,y'>\) commutes with \(x^a\). If \(h \in \text{Stab}(x,y')(B)\), let \(i\) be such that \(h(0) = ia\). Then \(x^{-ia}h \in \text{Stab}(x,y')(B)\) and \(x^{-ia}h(0) = 0\). Since we are not in the non-faithful case above, we have \(x^{-ia} = 1\), so \(h = x^{ia}\). Hence \(\text{Stab}(x,y')(B) = <x^a>\). Then Lemma 3.6.2 or Lemma 3.5.2 (stated and proven later) applies. If Lemma 3.6.2 applies, then we have some \(y'' \in Y\) for which \(<x^a> = ((y'')^a)\) and Subcase (a) above applies to \(y''\), yielding a contradiction. If Lemma 3.5.2 applies, then we reduce the nontrivial factor of the wreath product to a CI-digraph as in the argument above where the action was not faithful, until we can use Lemma 3.5.4 to reach the desired conclusion.

**Case 3.** The action of \(<x,y'/B\) is doubly transitive. By Theorem 3.2.21, this action is either solvable, or is isomorphic to \(A_5\) or \(S_5\), or \(a = \frac{q^2 - 1}{q - 1}\) for some prime power \(q\), and \(<x,y'/B\) is isomorphic to a subgroup of \(\text{PGL}(d,q)\) containing \(\text{PSL}(d,q)\).

By Corollary 3.6.9 and Lemma 3.6.11 (stated and proven later), if \(<x,y'/B\) is not solvable, then we can conjugate \(y'\) by an element \(\delta \in <x,y'>\) in such a way that \(<\delta^{-1}y',x>/B\) is imprimitive, and we replace \(y'\) by \(\delta^{-1}y'\delta\) and use the arguments of Case 2.

If \(<x,y'/B\) is solvable, then since \(a\) is not prime, we must have by Theorem 3.2.20 \(a = 4\), and since \(<x,y'/B\) is doubly transitive and contains a 4-cycle, we must have \(<x,y'/B \cong S_4\). Fix \(B_0 \in B\) and choose \(\delta \in <x,y'>\) such that \(\delta(B_0) = B_0\) and \(\delta(x^i(B_0)) = (y')^i(B_0)\), for \(1 \leq i \leq 3\). We can do this since both \(x/B\) and \(y'/B\) are 4-cycles and \(S_4\) is 4-transitive. Then clearly, we will have \(x^{-1} \delta^{-1} y' \delta \in \text{Stab}(x,y')(B)\). Since \(x^a\) commutes with everything in \(<x,y'>\), there exists some \(i\) such that \(x^{-ia-1} \delta^{-1} y' \delta |_{B_0} = 1\). Since \(\text{Stab}(x,y')(B)\) is faithful, we have \(x^{ia+1} = \delta^{-1}y'\delta\), so we must have \(<x> = \langle \delta^{-1}y'\delta\rangle\), contradicting the choice of \(y'\).

**Case 4.** \(a = n\). We do at least have that \(\text{Aut}(\bar{X})\) is imprimitive, with the complete block system \(B\) consisting of \(m\) blocks of size \(k\). We choose \(B\) in such a
way that $k$ is minimal, with as few factors as possible.

If $k$ is composite, then by Lemma 3.4.1 (stated and proven later), $\text{Stab}_{(x,y')}(B)\mid_B$ is primitive for any $B \in \mathcal{B}$. If $k$ is prime, then by Corollary 1.2.55, $\text{Stab}_{(x,y')}(B)\mid_B$ is primitive for any $B \in \mathcal{B}$.

If the action of $\text{Stab}_{(x,y')}(B)\mid_B$ is not faithful for some $B \in \mathcal{B}$, then Lemma 3.5.1 applies as before, so we can see that the digraph $\overline{X}$ is the wreath product of some irreducible unit circulant CI-digraph with a trivial graph. Using Lemma 3.5.4 completes the proof in this case.

So we may assume that the action of $\text{Stab}_{(x,y')}(B)$ is faithful.

If $k$ were prime, say $k = p$, then by Theorem 1.2.35, $x^m$ and $(y')^m$ are in Sylow $p$-subgroups of $\text{Stab}_{(x,y')}(B)$, so by Theorem 1.2.34, there is an element $\delta \in \text{Stab}_{(x,y')}(B)$ such that $\delta^{-1}(y')^m \delta$ and $x^m$ are in the same Sylow $p$-subgroup of $\text{Stab}_{(x,y')}(B)$. Hence $\delta^{-1}(y')^m \delta \mid_B = x^{im} \mid_B$ for some $i_B$ for any $B \in \mathcal{B}$. Since the action of $\text{Stab}_{(x,y')}(B)$ is faithful, this shows that $i_B$ does not in fact depend on $B$. So we have $\delta^{-1}(y')^m \delta = x^{im}$, contradicting $a = n$.

So we assume that $k$ is composite. Since $\text{Stab}_{(x,y')}(B)\mid_B$ is primitive for any $B \in \mathcal{B}$, we must have by Theorem 3.2.13 that $\text{Stab}_{(x,y')}(B)\mid_B$ is doubly transitive for any $B \in \mathcal{B}$. By Theorem 3.2.21, we have $\text{Stab}_{(x,y')}(B)\mid_B$ is either solvable, isomorphic to $A_k$ or $S_k$, or $k = \frac{q^d - 1}{q - 1}$ for some prime power $q$, and $\text{Stab}_{(x,y')}(B)\mid_B$ is isomorphic to a subgroup of $\text{PGL}(d, q)$ containing $\text{PSL}(d, q)$. By Corollary 3.6.9 and Lemma 3.6.11, if $\text{Stab}_{(x,y')}(B)\mid_B$ is not solvable, we contradict the choice of $k$.

If $\text{Stab}_{(x,y')}(B)\mid_B$ is solvable, then since $k$ is composite, we again see that by Theorem 3.2.20 we must have $k = 4$ and $\text{Stab}_{(x,y')}(B)\mid_B \cong S_4$. Fix some vertex $v \in B$, and choose $\delta \in \text{Stab}_{(x,y')}(B)$ such that $\delta(v) = v$ and $\delta(x^{im}(v)) = (y')^{im}(v)$ for $1 \leq i \leq 3$. Now, $x^{-m} \delta^{-1} y' \delta \mid_B = 1$, so (since $\text{Stab}_{(x,y')}(B)$ is faithful) we have $\delta^{-1}(y')^m \delta = x^m$, contradicting the choice of $y'$.

$\Box$
3.4 Finding Blocks

This is the one lemma that is used in both of the cases into which the proof naturally breaks down, as outlined in the next two sections, so it is cited in lemmata within each of these sections. Its simplicity makes it very useful in a wide variety of situations.

**Lemma 3.4.1** Let $G \leq S_n$ such that $\langle x \rangle \leq G$. Assume that $G$ admits a complete block system $\mathcal{B}$ of $m$ blocks of size $k$ formed by the orbits of $\langle x^m \rangle$. Furthermore, assume that $\text{Stab}_G(\mathcal{B})|_B$ admits a complete block system of $r$ blocks of size $s$ formed by the orbits of $\langle x^{ms} \rangle|_B$ for some $B \in \mathcal{B}$ ($rs = k$). Then $G$ admits a complete block system $\mathcal{C}$ of $mr$ blocks of size $s$ formed by the orbits of $\langle x^{ms} \rangle$.

**Proof.** If $\text{Stab}_G(\mathcal{B})|_B$ admits a complete block system $\mathcal{C}_B$ of $r$ blocks of size $s$ formed by the orbits of $\langle x^{ms} \rangle|_B$ for some $B \in \mathcal{B}$, then by Theorem 3.2.1, $w(\mathcal{C}_B)$ is a complete block system of $\text{Stab}_G(\mathcal{B})|_{B'}$, where $w(B) = B'$. As $\langle x^m \rangle|_{B'} \leq \text{Stab}_G(\mathcal{B})|_{B'}$, by Theorem 1.2.57, every complete block system of $\text{Stab}_G(\mathcal{B})|_{B'}$ is formed by the orbits of $\langle x^{ma} \rangle|_{B'}$ for some $a \in \mathbb{Z}_k$. As for every divisor $d$ of $k$, there is a unique subgroup of $\langle x^m \rangle|_{B'}$ of order $d$, by Theorem 1.2.19, we conclude that the blocks of $w(\mathcal{C}_B)$ are the orbits of $\langle x^{ms} \rangle|_{B'}$. Hence for every $B \in \mathcal{B}$, the orbits of $\langle x^{ms} \rangle|_B$ form a complete block system $\mathcal{C}_B$ of $\text{Stab}_G(\mathcal{B})|_B$. But then if $w \in G$, then $w(\mathcal{C}_B) = \mathcal{C}_{B'}$ for some $B'$ so that $C = \bigcup_{B \in \mathcal{B}} \mathcal{C}_B$ is a complete block system of $G$. □

3.5 Wreath Products

Much of the proof of this result falls naturally into two cases: the case in which the digraph $\bar{X}$ can be represented as the wreath product of some smaller digraph with the trivial graph, and the case where such reduction is not possible. This subsection contains the lemmata that deal with digraphs that fall into the former of these two cases.
Let \( G \) be a transitive permutation group that admits a complete block system \( \mathcal{B} \) of \( m \) blocks of size \( k \), where \( \mathcal{B} \) is formed by the orbits of some normal subgroup \( N \triangleleft G \). Furthermore, assume that \( \text{Stab}_G(\mathcal{B})|_B \) is primitive for every \( B \in \mathcal{B} \), and that \( \text{Stab}_G(\mathcal{B}) \) is not faithful. Define an equivalence relation \( \equiv \) on \( \mathcal{B} \) by \( B \equiv B' \) if and only if the subgroups of \( \text{Stab}_G(\mathcal{B}) \) that fix \( B \) and \( B' \), pointwise respectively, are equal. We denote these subgroups by \( \text{Stab}_G(B)B \) and \( \text{Stab}_G(B)B' \), respectively. Denote the equivalence classes of \( \equiv \) by \( C_0, \ldots, C_a \) and let \( E_i = \bigcup_{B \in C_i} B \). The following result was proven in [18] in the case where \( k = p \). It is straightforward to generalise this result to \( k \) being composite provided that \( \text{Stab}_G(\mathcal{B})|_B \) is primitive for every \( B \in \mathcal{B} \) and the action of \( \text{Stab}_G(\mathcal{B}) \) is not faithful.

**Lemma 3.5.1** (Dobson. [18]) Let \( \tilde{X} \) be a vertex-transitive digraph for which \( G \leq \text{Aut}(\tilde{X}) \) as above. Then \( \text{Stab}_G(\mathcal{B})|_{E_i} \leq \text{Aut}(\tilde{X}) \) for every \( 0 \leq i \leq a \) (here if \( g \in \text{Stab}_G(\mathcal{B}) \), then \( g|_{E_i}(x) = g(x) \) if \( x \in E_i \) and \( g|_{E_i}(x) = x \) if \( x \not\in E_i \)). Furthermore, \( \{ E_i : 0 \leq i \leq a \} \) is a complete block system of \( G \).

**Proof.** Suppose that \( B \) and \( B' \) are in distinct equivalence classes. We know that \( \text{Stab}_G(\mathcal{B})B \triangleleft \text{Stab}_G(\mathcal{B}) \). Since \( \text{Stab}_G(\mathcal{B})|_{B'} \) is primitive, the orbits of \( \text{Stab}_G(\mathcal{B})|_{B'} \) must be either singletons or a single orbit consisting of all vertices in \( B' \). Since \( \text{Stab}_G(\mathcal{B})B \neq \text{Stab}_G(\mathcal{B})B' \), we have the latter case, so \( \text{Stab}_G(\mathcal{B})B \) is transitive on \( B' \). This yields the first part of the result. The second part is trivial. \( \square \)

**Lemma 3.5.2** Let \( y \in S_n \) be an \( n \)-cycle such that \( (x, y) \) admits a complete block system \( \mathcal{B} \) of \( m \) blocks of size \( k \) and \( (x, y)/\mathcal{B} \) admits a complete block system \( \mathcal{C} \) of \( r \) blocks of size \( s \), where \( s \) is composite. Assume that \( \text{Stab}_{(x, y)}(\mathcal{B}) = \langle x^m \rangle \) and that \( \text{soc}(\text{Stab}_{(x, y)}/\mathcal{B}(\mathcal{C})|_{\mathcal{C}}) \) is a doubly transitive nonabelian simple group. Let \( \mathcal{D} = \{ D_C = \bigcup \{ B \in C \} : C \in \mathcal{C} \} \) be the complete block system of \( (x, y) \) of \( r \) blocks of size \( sk \). If \( \text{Stab}_{(x, y)}(\mathcal{D}) \) is not faithful, and if \( (x, y) \leq \text{Aut}(\tilde{X}) \) for some unit circulant digraph, then \( \tilde{X} \) is isomorphic to the wreath product of a unit circulant digraph of order \( n/i \) over a trivial graph of order \( i \) for some \( i > 1 \).
Define \( \pi : \text{Stab}_{(x,y)}(D) \to S_\mathcal{B} \) by \( \pi(g) = g|_D \) for some fixed \( D_0 \in D \). As \( \text{Stab}_{(x,y)}(D) \) does not act faithfully on every \( D \in \mathcal{D} \), it does not act faithfully on any \( D \in \mathcal{D} \). Hence \( \text{Ker}(\pi) \neq 1 \). As \( \text{Stab}_{(x,y)}(C) = \langle x^m \rangle \), if \( g \in \text{Ker}(\pi) \), \( g \neq 1 \), then \( g/B \neq 1 \). Let \( C \in \mathcal{C} \) be such that \( g/B|_C \neq 1 \), and let \( D_C \in \mathcal{D} \) such that \( D_C = \cup \{ B : B \in C \} \). As \( \text{Ker}(\pi) \triangleleft \text{Stab}_{(x,y)}(D) \) and \( \text{soc}(\text{Stab}_{(x,y)}(C)|C) \) is a doubly transitive nonabelian simple group, we have that \( \text{soc}(\text{Ker}(\pi)/B|_C) = \text{soc}(\text{Stab}_{(x,y)}(C)|C) \) is a doubly transitive nonabelian simple group. We now show that there exists \( N \triangleleft \text{Ker}(\pi) \) such that if \( N|_{D_C} \neq 1 \), then \( \text{soc}(N/B|_C) \) is a doubly transitive nonabelian simple group for \( D_C \in \mathcal{D} \) and \( C \in \mathcal{C} \). We will say that a group that satisfies this condition has Property 1.

Let \( C_1, \ldots, C_t \in \mathcal{C} \) be all of the blocks of \( \mathcal{C} \) such that \( \text{Ker}(\pi)/B|_{C_1} = 1 \). Let \( \bar{D} = \cup_{i=1}^t D_{C_i} \) and define \( \bar{\pi} : \text{Ker}(\pi) \to S_\mathcal{B} \) by \( \bar{\pi}(g) = g|_{B} \). As \( \langle y^m \rangle = \langle x^m \rangle \), \( \langle x^m \rangle \) is in the center of \( \langle x, y \rangle \). As the centraliser in \( S_n \) of \( \langle x^m \rangle \) is isomorphic to \( S_m \wr \mathbb{Z}_k \) by Theorem 3.2.2, we conclude that \( \text{Im}(\bar{\pi}) \leq \mathbb{Z}_k^* \) is abelian and hence solvable. Thus by Theorem 1.2.30, \( (\text{Ker}(\pi)/B|_C)/(\text{Ker}(\bar{\pi})/B|_C) \) is solvable, and \( \text{soc}(\text{Ker}(\pi)/B|_C) \) is doubly transitive, nonabelian and simple, we must certainly have \( \text{Ker}(\bar{\pi})/B|_C \neq 1 \). Thus \( \text{Ker}(\bar{\pi})/B|_{D_C} \neq 1 \). We claim that \( N = \text{Ker}(\bar{\pi}) \) has the required property. To verify this, suppose that \( N|_{D_C} \neq 1 \), that is, \( \text{Ker}(\bar{\pi})|_{D_C} \neq 1 \), so \( C \notin \{ C_1, \ldots, C_t \} \), so \( \text{Ker}(\pi)/B|_C \neq 1 \). As \( \text{Ker}(\pi) \triangleleft \text{Stab}_{(x,y)}(D) \) and \( \text{soc}(\text{Stab}_{(x,y)}(C)|C) \) is doubly transitive, nonabelian and simple, the fact that \( \text{Ker}(\pi)/B|_C \neq 1 \) forces \( \text{soc}(\text{Ker}(\pi)/B|_C) \) to be doubly transitive, nonabelian and simple. Since \( N = \text{Ker}(\bar{\pi}) \), we must have \( \text{soc}(\text{Ker}(\bar{\pi})/B|_C) \) being doubly transitive, nonabelian and simple also, since it is not 1. Thus \( N = \text{Ker}(\bar{\pi}) \) has the required property.

Choose \( N \triangleleft \text{Ker}(\pi) \) such that \( N \neq 1 \), \( N \) has Property 1 and \( \text{soc}(N/B|_C) \) is a doubly transitive nonabelian simple group for the fewest possible number of blocks of \( \mathcal{C} \). Suppose that there exists \( \gamma \in N \) and \( C_1, C_2 \in \mathcal{C} \) such that \( \gamma/B|_{C_1} = 1 \), \( \gamma|_{D_{C_1}} \neq 1 \) and \( \gamma/B|_{C_2} \neq 1 \). Let

\[
N' = \langle g^{-1}\gamma g : g \in \text{Ker}(\pi) \rangle.
\]

Then \( N' \triangleleft \text{Ker}(\pi) \). As \( \langle x, y \rangle \leq S_m \wr \mathbb{Z}_k \), we have that \( N'/B|_{C_1} = \langle \gamma/B|_{C_1} \rangle \). Fur-
thermore, if $\gamma/\mathcal{B}|_C \neq 1$, then \text{soc}(N'/\mathcal{B}|_C)$ is a doubly transitive nonabelian simple group as \text{soc}(\text{Ker}(\pi)/\mathcal{B}|_C)$ is a doubly transitive nonabelian simple group. Redefine $l, C_1, \ldots, C_l$ so that $C_1, \ldots, C_l \in \mathcal{C}$ are all of the blocks of $\mathcal{C}$ such that $N'/\mathcal{B}|_C, = 1$. Redefine $\tilde{D} = \cup_{i=1}^l D_{C_i}$, and define $\pi': N' \to S_{\tilde{D}}$ by $\pi'(g) = g|_{\tilde{D}}$. As $(x, y) \leq S_m \times \mathbb{Z}_k$, we have $\text{Im}(\pi') \leq \mathbb{Z}^k_\mathbb{Z}$ is abelian and hence solvable. Since

$$(N'/\mathcal{B}|_C)/(\text{Ker}(\pi')/\mathcal{B}|_C)$$

is solvable by Theorem 1.2.30, we have whenever $\gamma/\mathcal{B}|_C \neq 1$, $\text{Ker}(\pi')/\mathcal{B}|_C \neq 1$, so certainly

$$\text{Ker}(\pi')|_{D_{C_i}} \neq 1.$$ 

We claim that $N'' = \text{Ker}(\pi')$ has Property 1, that $N'' \triangleleft \text{Ker}(\pi)$ and that \text{soc}(N''/\mathcal{B}|_C)$ is doubly transitive, nonabelian and simple on fewer blocks $C \in \mathcal{C}$ than \text{soc}(N/\mathcal{B}|_C)$, but is still not 1.

First, if $N''|_{D_{C_i}} \neq 1$, then $D_{C_i} \subseteq \tilde{D}$, so $N'/\mathcal{B}|_C \neq 1$. Similar to earlier arguments, we can show from this that \text{soc}(N'/\mathcal{B}|_C)$ is doubly transitive, nonabelian and simple, and that $N''/\mathcal{B}|_C \neq 1$. However, $N''/\mathcal{B}|_C \triangleleft N'/\mathcal{B}|_C$, so \text{soc}(N''/\mathcal{B}|_C)$ is doubly transitive, nonabelian and simple. Thus $N''$ has Property 1. Now, if $g \in \text{Ker}(\pi)$ and $n' \in N''$, certainly $g^{-1}n'g \in N'$ since $N'' \leq N'$ and $N' \triangleleft \text{Ker}(\pi)$. We need only show that $g^{-1}n'g|_{\tilde{D}} = 1$. But since $g \in \text{Stab}_{x,y}(\mathcal{D})$ and $n'|_{\tilde{D}} = 1$, this is clear. Hence $N'' \triangleleft \text{Ker}(\pi)$. It is not hard to see from the constructions of $N$ and $N''$ above, that we will not have $N'' = 1$, since $N''|_{C_2} \neq 1$. Finally, $N'/\mathcal{B}|_{C_1} = 1$ since $\gamma/\mathcal{B}|_{C_1} = 1$. So $D_{C_1} \subseteq \tilde{D}$, so since $N'' = \text{Ker}(\pi')$, we have $N''|_{D_{C_1}} = 1$. So $C_1$ is a block on which \text{soc}(N/\mathcal{B}|_{C_1})$ is doubly transitive, nonabelian and simple (since $N|_{D_{C_1}} \neq 1$), but $N''/\mathcal{B}|_{C_1}$ is not. Also, if $C$ is any block on which \text{soc}(N/\mathcal{B}|_C)$ is not doubly transitive, nonabelian and simple, then $N|_{D_{C}} = 1$, so $\gamma|_{D_{C}} = 1$, so $g^{-1}g/\mathcal{B}|_C = 1$ for any $g \in \text{Ker}(\pi)$, so $N'/\mathcal{B}|_C = 1$, whence $D_{C} \subset \tilde{D}$ so $N''|_{D_{C}} = 1|_{D_{C}}$, and \text{soc}(N''/\mathcal{B}|_C)$ is not doubly transitive, nonabelian and simple. This proves our claim, and our claim contradicts the choice of $N$. Thus, if $\gamma \in N$ such that $\gamma/\mathcal{B}|_C = 1$, then $\gamma|_{D_{C}} = 1$. As $\text{Stab}_{x,y}(\mathcal{B}) = (x^m)$, we have that if $\gamma \neq 1, \gamma \in N$, then $\gamma|_{D} \notin (x^m)|_{D}$ for any $D \in \mathcal{D}$. 
As $N \triangleleft \text{Ker}(\pi)$, the orbits of $N|_D$ form a complete block system of $\text{Ker}(\pi)|_D$ for every $D \in \mathcal{D}$. If $N/\mathcal{B}|_C \neq 1$, then $N|_{D_C} \neq 1$, so $\text{soc}(N/\mathcal{B}|_C)$ is doubly transitive, nonabelian, and simple. This certainly means that each orbit of $N/\mathcal{B}|_C$ contains at least one vertex from each block of $\mathcal{B}$ in $C$.

Furthermore, we claim that the cardinality of the intersection of each orbit of $N|_{D_C}$ with each block of $\mathcal{B}$ in $C$ is some constant, $j_C$. We now prove this claim. Let $O_1$ and $O_2$ be orbits of $N|_{D_C}$, and $B_1$ and $B_2$ be blocks of $\mathcal{B}$ in $C$. Suppose that the cardinality of the intersection of $B_1$ with $O_1$ is $j_C$. Then since $O_1$ is an orbit of $N$, there exists some $n' \in N$ such that

$$n'(B_1 \cap O_1) = B_2 \cap O_1.$$  

So clearly, the cardinality of the intersection of $B_2$ with $O_1$ is also $j_C$. Now, since both $B_2 \cap O_1$ and $B_2 \cap O_2$ are nonempty, let $v_1 \in B_2 \cap O_1$ and $v_2 \in B_2 \cap O_2$. Let $i$ be such that $x^{im}(v_1) = v_2$. Then since $x^{im}$ commutes with every element of $N$, and $O_1$ and $O_2$ are orbits of $N$, we must have

$$x^{im}(B_2 \cap O_1) = B_2 \cap O_2.$$  

This completes the proof of the claim.

Hence, $N|_{D_C}$ has $k/j_C$ orbits of length $sj_C$.

We now demonstrate that each orbit of $N$ is a block of $(x, y)$. If $j_C > 1$, then consider the intersection of some orbit of $N$ with some block of $\mathcal{B}$ in $C$. This is a set $Y$ of cardinality $j_C$. Let $v_1, v_2 \in Y$. Then $v_2 = x^{im}(v_1)$ for some $i$. Also, there exists some $n' \in N$ such that $n'(v_1) = v_2$, since these vertices are in the same orbit of $N$. Since $x^{im}$ commutes with $n'$, we have

$$n'(v_2) = x^{im}n'x^{-im}(v_2)$$

$$= x^{im}n'x^{-im}x^{im}(v_1)$$

$$= x^{im}(v_2),$$

so $x^{im}(v_2)$ must also be in $Y$. Using this argument repeatedly, we see that $Y$ must in fact be an orbit of $x^{n/j_C}$. Thus, it is clear that $Y$ is a block of $\text{Stab}_{(x,y)}(\mathcal{B})$, and
by Lemma 3.4.1, $Y$ is a block of $\langle x, y \rangle$. So we will actually demonstrate that each orbit of $\mathcal{V}/\mathcal{Y}$, where $\mathcal{Y}$ is the complete block system of $\langle x, y \rangle$ generated from $Y$, is a block of $\langle x, y \rangle/\mathcal{Y}$. This will certainly be sufficient to prove the claim that began this paragraph. In what follows, let $\mathcal{D}'$ denote the block system of $\langle x, y \rangle/\mathcal{Y}$ that corresponds to $\mathcal{D}$, and let $D'$ be the block of $\mathcal{D}'$ corresponding to the block $D_C$; also, let $B'$ denote the block system of $\langle x, y \rangle/\mathcal{Y}$ that corresponds to $B$. If $j_C = 1$, then $\mathcal{Y}$ is the complete trivial block system whose blocks have size 1.

The orbits of $\mathcal{N}/\mathcal{Y}|_{D'}$ are certainly blocks of $\text{Ker}(\pi)/\mathcal{Y}$, since $N \lhd \text{Ker}(\pi)$. Denote the block system of $\text{Ker}(\pi)/\mathcal{Y}$ formed by these orbits, by $\mathcal{F}_{D'}$. Notice that these blocks have size $s$, and they are minimal nontrivial blocks of $\text{Ker}(\pi)/\mathcal{Y}$ since the action of $\mathcal{N}/\mathcal{Y}|_{D'}$ is doubly transitive and hence primitive within each block of $\mathcal{F}_{D'}$.

Now, let $g \in \text{Stab}_{\langle x, y \rangle/\mathcal{Y}}(\mathcal{D}')$. Let $F \in \mathcal{F}_{D'}$. By Theorem 3.2.1, $g(F)$ is a block of $g\text{Ker}(\pi)g^{-1} = \text{Ker}(\pi)$. Suppose that $g(F) \cap F \neq \emptyset$. Since $F$ meets every block of $B'$ in $\mathcal{D}'$ in a unique point, so must $g(F)$ since $B'$ is a block system of $\langle x, y \rangle/\mathcal{Y}$. Since $F$ is a minimal nontrivial block of $\text{Ker}(\pi)/\mathcal{Y}$, we must either have $g(F) = F$, or $|g(F) \cap F| = 1$. We have $|F| = s$ is composite, so there are at least four points in $F$. Suppose that $|g(F) \cap F| = 1$, and let $Y_1, Y_2, Y_3 \in F$. Let $n' \in N$ be such that $n'(Y_1) = Y_1$ and $n'(Y_2) = Y_3$ (we can do this since $\mathcal{N}/\mathcal{Y}|_{D'}$ is doubly transitive within each of its orbits). Since every element of $N$ commutes with $x^m$, and $F$ is an orbit of $\mathcal{N}/\mathcal{Y}$, it is clear that the other orbits of $\mathcal{N}/\mathcal{Y}$ in $\mathcal{D}'$, which are the same as the other blocks of $\mathcal{F}_{D'}$, must all be contained within the set

$$\{x^{im}(F) : 0 \leq i \leq k/j_C - 1\};$$

and in fact, since each orbit of $N$ meets each block of $B$ in a unique block of $\mathcal{Y}$, the blocks of $\mathcal{F}_{D'}$ are precisely the set

$$\{x^{im}(F) : 0 \leq i \leq k/j_C - 1\}.$$

Similarly, since $x^m$ commutes with $g$, the block system of $\text{Ker}(\pi)/\mathcal{Y}$ in $\mathcal{D}'$ generated from the block $g(F)$ is precisely the set

$$\{x^{im}g(F) : 0 \leq i \leq k/j_C - 1\}.$$
Now, since $n'$ commutes with $x^m$, $n'$ must fix every block of $\mathcal{Y}$ in the block $B$ of $B$ that contains $Y_1$. Since each block of both $\mathcal{F}_{D'}$ and $g(\mathcal{F}_{D'})$ meets $B$ in a single block of $\mathcal{Y}$, and each of these blocks of $\mathcal{Y}$ is fixed setwise by $n$, each block of both $\mathcal{F}_{D'}$ and $g(\mathcal{F}_{D'})$ must be fixed setwise by $n'$. But each block of $\mathcal{Y}$ in $D'$ is in some block of $\mathcal{F}_{D'}$ and some block of $g(\mathcal{F}_{D'})$, and our assumption implies that no intersection of a block of $\mathcal{F}_{D'}$ with a block of $g(\mathcal{F}_{D'})$ contains more than one block of $\mathcal{Y}$. So this means that we must have $n'/\mathcal{Y} = 1$, contradicting the choice of $n'$. So we must have $g(F) = F$. This shows that $F$ is in fact a block of $\text{Stab}(x,y)/\mathcal{Y}(D')$.

Furthermore, since $x' \in \text{Stab}(x,y)(D)$, we have

$$x'/\mathcal{Y} \in \text{Stab}(x,y)/\mathcal{Y}(D').$$

So it is easy to see that the blocks of $\mathcal{F}_{D'}$ must be orbits of $(x^{rk})/\mathcal{Y}$. Thus, by Lemma 3.4.1, $\mathcal{F}_{D'}$ generates a complete block system $\mathcal{F}'$ of $(x,y)/\mathcal{Y}$. This completes the demonstration.

Thus, $(x,y)$ admits blocks of size $sj_C$ for each $j_C$, and there are $rk/jC$ of these blocks. Each of these blocks is an orbit of $(x^{rk}/jC)$. Furthermore, the intersection of any two blocks from distinct block systems among these, if nonempty, is also a block of $(x,y)$ that is an orbit of $x^{rk}/j$ for some $j$. Let $\mathcal{F}$ be the smallest block system of $(x,y)$ whose blocks are orbits of $x^{rk}/j$ for some $j$, so the blocks of $\mathcal{F}$ have size $js$. Then the preceding arguments have shown that every nontrivial orbit of $N$ is a union of blocks of $\mathcal{F}$.

Suppose that for some $C$, the orbits of $N|_{D_C}$ have length $j'$s, where $j' > j$ (so $j|j'$). Consider the subgroup $N'$ of $N$ such that $N'$ fixes each of the blocks of $\mathcal{F}$ in $D_C$ setwise. Clearly, $N' \triangleleft N$. Also, $N' \triangleleft \text{Ker}(\pi)$. For if $g \in \text{Ker}(\pi)$ and $n' \in N'$, then $gn'g^{-1} \in N$ since $N \triangleleft \text{Ker}(\pi)$. Since $n'$ fixes each of the blocks of $\mathcal{F}$ in $D_C$ setwise, and $g$ fixes $D_C$ setwise, $gn'g^{-1}$ certainly fixes each of the blocks of $\mathcal{F}$ in $D_C$ setwise, so $gn'g^{-1} \in N'$. Also, $N' \neq 1$. This is true because $N$ is transitive on $F \in \mathcal{F}$, where $F \subseteq D_C$. So we can choose $n' \neq 1$, $n' \in N$ such that $n'(F) = F$. Then since the blocks of $\mathcal{F}$ in $D_C$ are contained in the set

$$\{x^m(F) : 0 \leq i \leq k - 1\},$$
the fact that $n'(F) = F$ forces

$$n'(x^i(F)) = x^i n'(F) = x^i(F)$$

for any $i$, so all blocks of $\mathcal{F}$ are fixed setwise by $n'$, meaning $n' \in N'$.

Furthermore, $N'$ has Property 1. For if $N'|_{C} \neq 1$, then $N|_{C} \neq 1$, so $\text{soc}(N/\mathcal{B}|_{C})$ is doubly transitive, nonabelian and simple. Since $N' \triangleleft N$, we either have that $\text{soc}(N'/\mathcal{B}|_{C})$ is doubly transitive, nonabelian and simple, yielding Property 1, or $N'/\mathcal{B}|_{C} = 1$. But if $N'/\mathcal{B}|_{C} = 1$, then there exists some $\gamma \in N' \leq N$ such that $\gamma/\mathcal{B}|_{C} = 1$ but $\gamma|_{C} \neq 1$, contradicting the choice of $N$ as shown earlier. So $N'$ must have Property 1.

Continuing in this fashion, we can reduce $N$ to some subgroup $N'' \neq 1$ such that $N'' \triangleleft \text{Ker}(\pi)$, $N''$ has Property 1, and the nontrivial orbits of $N''$ are blocks of $\mathcal{F}$. Hence $N'' \leq \text{Stab}_{\mathcal{F}}(\mathcal{F})$, showing that $\text{Stab}_{\mathcal{F}}(\mathcal{F})$ is not faithful. Let $\mathcal{Y}$ denote the complete block system formed by taking all possible intersections of blocks in $\mathcal{B}$ with blocks in $\mathcal{F}$. Denote the complete block system of $(x,y)/\mathcal{Y}$ corresponding to $\mathcal{F}$ by $\mathcal{W}$. Then the presence of $N''$ also shows that $\text{soc}(\text{Stab}_{\mathcal{Y}}(\mathcal{W})|_{\mathcal{W}})$ is doubly transitive, nonabelian and simple, so $\text{Stab}_{\mathcal{Y}}(\mathcal{W})|_{\mathcal{W}}$ is doubly transitive and hence primitive for every $W \in \mathcal{W}$. Define an equivalence relation $\equiv$ on $\mathcal{F}$ as follows. Let $F,F' \in \mathcal{F}$ and let $W,W' \in \mathcal{W}$ be the blocks of $\mathcal{W}$ corresponding to $F$ and $F'$. Then $F \equiv F'$ if and only if the subgroup of $\text{Stab}_{\mathcal{Y}}(\mathcal{W})$ that fixes every point in $W$ is the same as the subgroup that fixes every point in $W'$. By the presence of $N''$ in $\text{Stab}_{\mathcal{F}}(\mathcal{F})$, there is clearly more than one equivalence class.

If $j = 1$, then $\mathcal{W} = \mathcal{F}$ and Lemma 3.5.1 applies.

Now we show that if $j > 1$, the conclusion of Lemma 3.5.1 can still be drawn. The equivalence classes defined above certainly form a complete block system $\mathcal{J}$ of $(x,y)$; we need only show that

$$\text{Stab}_{\mathcal{F}}(\mathcal{F})|_{\mathcal{J}} \leq \text{Aut}(\bar{X})$$

for every $J \in \mathcal{J}$. To do this, we will show that whenever $F \neq F'$, the subgroup of $\text{Stab}_{\mathcal{F}}(\mathcal{F})$ that fixes $F$ pointwise is transitive on $F'$. This will clearly be sufficient.
So, suppose that $F \neq F'$. Then the subgroup of $\text{Stab}_{(x,y)}(\mathcal{W})$ that fixes every point in $W$ is not the same as the subgroup that fixes every point in $W'$. Define $\tau : \text{Stab}_{(x,y)}(\mathcal{F}) \to S_y$ by $\tau(g) = g|_{F}$. Then we have the subgroup of $\text{Stab}_{(x,y)}(\mathcal{W})$ that fixes every point in $W$ being the same as $\text{Ker}(\tau)$, so since the subgroup of $\text{Stab}_{(x,y)}(\mathcal{W})$ that fixes every point in $W$ is not the same as the subgroup that fixes every point in $W'$, we must have $\text{Ker}(\tau)|_{\mathcal{W}'} \neq 1$. Since

\[ \text{Ker}(\tau)|_{\mathcal{W}'} \prec \text{Stab}_{(x,y)}(\mathcal{W})|_{W'}, \]

$\text{Ker}(\tau)|_{\mathcal{W}'} \neq 1$, and $\text{soc}(\text{Stab}_{(x,y)}(\mathcal{W})|_{W'})$ is doubly transitive, nonabelian and simple, we must have $\text{soc}(\text{Ker}(\tau)|_{\mathcal{W}'})$ also being doubly transitive, nonabelian and simple.

Now we define $\tau' : \text{Ker}(\tau) \to S_{s,j}$ by $\tau'(g) = g|_{F}$. $\text{Im}(\tau')$ must be abelian since $\text{Ker}(\tau)|_{F}$ is abelian, so $(\text{Ker}(\tau)|_{\mathcal{W}'})/(\text{Ker}(\tau')|_{\mathcal{W}'})$ is abelian by Theorem 1.2.30. Hence we ceratinly have $\text{Ker}(\tau')|_{\mathcal{W}'} \neq 1$, so $\text{Ker}(\tau')|_{\mathcal{W}'}$ is doubly transitive and nonabelian.

Notice also that $\text{Ker}(\tau') \trianglelefteq \text{Stab}_{(x,y)}(\mathcal{F})$. For if $g \in \text{Stab}_{(x,y)}(\mathcal{F})$ and $k \in \text{Ker}(\tau')$, then certainly $gkg^{-1} \in \text{Ker}(\tau)$, and since $k$ fixes $F$ pointwise and $g$ fixes $G$ setwise, $gkg^{-1}$ must fix $F$ pointwise. So the orbits of $\text{Ker}(\tau')$ are blocks of $\text{Stab}_{(x,y)}(\mathcal{F})$, and since $x^{r} \in \text{Stab}_{(x,y)}(\mathcal{F})$, it is not hard to see that the orbits of $\text{Ker}(\tau')$ must be orbits of $x^{r(j')}j'$ for some $j' \leq j$. But by Lemma 3.4.1, these orbits are blocks of $(x,y)$, and by the choice of $j$, we must have $j' = j$. So the orbit of $\text{Ker}(\tau')|_{F}$ is precisely the block $F'$. This completes the proof that when $j > 1$, we can still arrive at the conclusion of Lemma 3.5.1.

So we see that the equivalence classes form a complete block system $\mathcal{J}$ of $(x,y)$ and

\[ \text{Stab}_{(x,y)}(\mathcal{F})|_{J} \leq \text{Aut}(\bar{X}) \]

for every $J \in \mathcal{J}$. As $\mathcal{J}$ is a complete block system of $(x,y)$ and every complete block system of $(x,y)$ is formed by the orbits of a normal subgroup of $(x)$, and since we noted that there is more than one block in $\mathcal{J}$, we conclude that some block $J \in \mathcal{J}$ is a nontrivial proper subgroup of $\mathbb{Z}_{n}$. Then $J$ consists entirely of nonunits of $\mathbb{Z}_{n}$,
so that the digraph $\tilde{X}[J]$ has no arcs. Finally, observe that $J$ is a union of blocks of $\mathcal{F}$. Now, suppose that there is an arc from some vertex of $F_1 \in \mathcal{F}$ to some vertex of $F_2 \in \mathcal{F}$. Then $F_1 \neq F_2$. As $F_1 \neq F_2$, there is an arc from every vertex of $F_1$ is to every vertex of $F_2$. We conclude that $\tilde{X} = \tilde{X}/\mathcal{F} \cup (\tilde{X}[F])$ for $F \in \mathcal{F}$ and as $\tilde{X}[J]$ has no arcs for every $J \in \mathcal{F}$, $\tilde{X}[F]$ has no arcs for every $F \in \mathcal{F}$. Thus $\tilde{X} = \tilde{X}/\mathcal{F} \cup E_{sJ}$. Observe that as $\langle x \rangle/\mathcal{F} \leq \text{Aut}(\tilde{X})/\mathcal{F}$, we have that $\tilde{X}/\mathcal{F}$ is a circulant digraph. Finally, the units in $\mathbb{Z}_n$ are precisely those elements $a \in \mathbb{Z}_n$ such that $\gcd(a, n) = 1$. Let $S'$ be the connection set of $\tilde{X}/\mathcal{F}$. If $a \in S$, then $a + \mathbb{Z}_{sj} \subseteq S$ and $a(\text{mod } n/sj) \in S$. As $\gcd(a, n) = 1$, we then have that $\gcd(a(\text{mod } n/sj), n) = 1$ and $\tilde{X}/\mathcal{F}$ is a unit circulant digraph.

The following lemma is a nice little result in the field of number theory that is used in the lemma that follows it.

**Lemma 3.5.3** Let $m, k$ and $s$ be integers, with $\gcd(m, s) = 1$. Then there exists some integer $i \equiv s \pmod{m}$ such that $\gcd(i, mk) = 1$.

**Proof.** Let $j = \gcd(m, k)$. Then $\gcd(m, k/j) = 1$, so there exists some $t$ such that $tm \equiv 1 \pmod{k/j}$. Now, $(1-s)tm \equiv 1-s \pmod{k/j}$, so $s+(1-s)tm \equiv 1 \pmod{k/j}$. Then clearly, $\gcd(s+(1-s)tm, k/j) = 1$. But since $j|m$, and $\gcd(m, s) = 1$, we have $\gcd(s+(1-s)tm, j) = 1$, so $\gcd(s+(1-s)tm, k) = 1$. Equally, since $\gcd(s, m) = 1$, $\gcd(s+(1-s)tm, m) = 1$, so $\gcd(s+(1-s)tm, mk) = 1$. So $i = s+(1-s)tm$ and we are done. 

**Lemma 3.5.4** Let $\tilde{X}_1$ be an irreducible CI-digraph of $\mathbb{Z}_m$ and $k \geq 2$. Then $\tilde{X} = \tilde{X}_1 \cup E_k$ is a CI-digraph of $\mathbb{Z}_{mk}$.

**Proof.** As $\tilde{X}_1$ is irreducible, it follows by Corollary 1.2.72 that

$$\text{Aut}(\tilde{X}) = \text{Aut}(\tilde{X}_1) \cup S_k.$$ 

As $\mathbb{Z}_m \cup \mathbb{Z}_k \leq \text{Aut}(\tilde{X})$, $\tilde{X}$ is a Cayley digraph of $\mathbb{Z}_{mk}$. Furthermore, $\text{Aut}(\tilde{X})$ admits a complete block system $\mathcal{B}$ of $m$ blocks of size $k$, formed by the orbits of $\langle x^m \rangle$. 

Let \( \delta \in S_n \) such that \( \delta^{-1}x\delta \leq \text{Aut}(\bar{X}) \) and \( y = \delta^{-1}x\delta \). As \( \bar{X}_1 \) is a CI-digraph of \( \mathbb{Z}_m \), any two regular cyclic subgroups of \( \text{Aut}(\bar{X}_1) \) are conjugate. Hence there exists \( \gamma \in \text{Aut}(\bar{X}) \) such that \( \gamma^{-1}y\gamma/B \in \langle x \rangle/B \). For convenience, we replace \( \gamma^{-1}y\gamma \) with \( y \) and assume that \( y/B \in \langle x \rangle/B \). As

\[
\text{Stab}_{\text{Aut}(\bar{X})}(B) = 1_{S_m} \wr S_k,
\]

there exists \( \gamma \in \text{Stab}_{\text{Aut}(\bar{X})}(B) \) such that \( \gamma^{-1}y^m\gamma = x^m \). Again, we replace \( \gamma^{-1}y\gamma \) with \( y \) and thus assume that \( y^m = x^m \).

Fix \( v_0 \in B_0 \), and define \( s \) such that \( x(v_0) = y^s(v_0) \). Since \( x/B \) and \( y/B \) are \( m \)-cycles and \( y/B \in x/B \), we must have \( \gcd(s, m) = 1 \). By Lemma 3.5.3, there exists some \( i \) such that \( |(y^{s+m})| = mk \). Furthermore, it is clear that \( y^{s+m}/B = x/B \). Replace \( y^{s+m} \) with \( y \). Observe \( \langle x, y \rangle \leq \mathbb{Z}_m \wr \mathbb{Z}_k \), and of course, \( \mathbb{Z}_m \wr \mathbb{Z}_k \leq \text{Aut}(\bar{X}) \).

We identify \( \mathbb{Z}_{mk} \) with \( \mathbb{Z}_m \times \mathbb{Z}_k \) so that

\[
x(i, j) = (i + 1, j + \sigma_i(j)),
\]

where \( \sigma_i(j) = 0 \) if \( i \neq m - 1 \) and \( \sigma_{m-1}(j) = 1 \). Then

\[
y(i, j) = (i + 1, j + b_i),
\]

where \( b_i \in \mathbb{Z}_k \). As \( |y| = mk \), we have that \( \sum_{i=0}^{m-1} b_i \equiv b \pmod{k} \) and \( b \in \mathbb{Z}_k^* \). Let \( \beta \in \text{Aut}(\bar{X}) \) such that \( \beta(i, j) = (i, b^{-1}j) \). We replace \( y \) with \( \beta y \beta^{-1} \) and thus assume that \( \sum_{i=0}^{m-1} b_i \equiv 1 \pmod{k} \). Let \( x^m = z_0 z_1 \cdots z_{m-1} \) where each \( z_i \) is a \( k \)-cycle that contains \( (i, 0) \). Let

\[
\gamma = z_1^{-\gamma_{i-1} b_i} z_2^{-\gamma_{i+2} b_i} \cdots z_{m-1}^{b_{m-1} - 1}.
\]

It is then straightforward to verify that \( \gamma^{-1}y\gamma = x \) and \( \gamma \in 1_{S_m} \wr \mathbb{Z}_k \leq \text{Aut}(\bar{X}) \).

Lemma 3.5.5 Let \( x, y \) be \( n \)-cycles acting on a set of \( n \) elements. Assume that every element of \( \langle x, y \rangle \) commutes with \( x^a \) for some \( 0 < a < n \). Let \( ab = n \), so that \( \langle x, y \rangle \) admits a complete block system \( B \) of \( b \)-blocks of size \( b \). Assume that the action of \( \text{Stab}_{\langle x, y \rangle}(B)\vert_B \) is not faithful for some \( B \in \mathcal{B} \). Then \( \langle x, y \rangle \) admits a complete block system \( \mathcal{C}_b \) consisting of \( ab/b' \) blocks of size \( b' \) for every \( b'/b \); furthermore, there is some prime \( p \mid b \) such that the action of \( \text{Stab}_{\langle x, y \rangle}(C_p) \) is not faithful.
PROOF. Notice that
\[ \text{Stab}_{(x,y)}(B)|_B = \langle x^a \rangle |_B \]
for any \( B \in \mathcal{B} \), since \( x^a \) commutes with every element of \( \langle x, y' \rangle \). Hence \( \text{Stab}_{(x,y')}(B)|_B \) admits blocks of every possible size \( b' \) for which \( b'|b \). By Lemma 3.4.1, \( \langle x, y' \rangle \) admits a complete block system with blocks of size \( b' \) for any \( b'|b \).

Suppose that \( b = rs \). We choose \( r, s \) in such a way that \( r \) is as large as possible so that \( \text{Stab}_{(x,y)}(C_r)|_C \) is faithful for every \( C \in C_r \). (Notice that the transitivity of \( \langle x, y \rangle \) means that if \( \text{Stab}_{(x,y)}(C_r)|_C \) were not faithful for some \( C \in C_r \), then it would not be faithful for any \( C \in C_r \).) We have \( 1 \leq r < b \), and \( 2 \leq s \leq b \), since \( \text{Stab}_{(x,y)}(B)|_B \) is not faithful.

Let \( h \in \text{Stab}_{(x,y)}(B) \) be such that \( h|_B = 1_B \) but \( h \neq 1 \). Since \( \text{Stab}_{(x,y)}(C_r)|_C \) is faithful for every \( C \in C_r \), and for any \( C \subset B \) we have \( h|_C = 1 \), but \( h \neq 1 \), we must have \( h \notin \text{Stab}_{(x,y)}(C_r) \). So if \( B' \in \mathcal{B} \) is such that \( h|_{B'} \neq 1 \), then there exists some \( C \subset B' \) such that \( h(C) \neq C \). Now, \( h|_{B'} = x^{bs'|a}|_{B'} \) for some \( i_{B'} \). Since there are \( s \) blocks of \( C_r \) in \( B' \), formed by the orbits of \( \langle x^a \rangle \), we have \( h^s = 1 \), so \( x^{bs'|a} = 1 \). Hence \( b|_{i_{B'}s}, \) say \( k_{B'}b = i_{B'}s \). But \( b = rs \), so \( k_{B'}rs = i_{B'}s \), meaning that \( k_{B'}r = i_{B'} \) for any \( B' \). Thus \( h \in \text{Stab}_{(x,y)}(C_s) \). Since \( x^{bs'|a}|_{B'} \) is nontrivial, this has shown that \( \text{Stab}_{(x,y')}(C_s) \) is not faithful. Now, suppose that \( \gcd(r,s) = t \neq 1 \). Let \( r' \) be such that \( r't = r \) and let \( s' \) be such that \( s't = s \). Then for any \( B' \),
\[ i_{B'} = k_{B'}r = k_{B'}tr', \]
and so
\[ h^s|_{B'} = x^{bs'|a'}|_{B'} = x^{k_{B'}ts'r'a} = x^{k_{B'}r'a}. \]
Since \( C_r \) is formed by the orbits of \( x^a \), we have \( h^s \in \text{Stab}_{(x,y)}(C_r) \), so \( h^s = 1 \). It is not difficult to calculate that \( i_{B'} = k_{B'}r't \), and since \( \gcd(r't, s/t) = 1 \), to see that in fact \( \text{Stab}_{(x,y')}(C_{rt}) \) is faithful, contradicting the choice of \( r \). So we see that \( \gcd(r, s) = 1 \).

Let \( p \) be any prime such that \( p|s \). We claim that the action of \( \text{Stab}_{(x,y')}(C_p) \) is not faithful.
Towards a contradiction, suppose that the action of $\text{Stab}_{(x,y)}(C_p)$ were faithful. We will show that this supposition forces the action of $\text{Stab}_{(x,y')}((C_{rp})$ to be faithful, contradicting the choice of $r$.

Let $D$ be a block of $C_{rp}$ and let $h \in \text{Stab}_{(x,y')}((C_{rp})$ be such that $h|_D = 1$. If every such $h$ is an element of the group $\text{Stab}_{(x,y)}((C_r)$, then every such $h = 1$ and we are done. So we suppose that there is some such $h$ that is not an element of the group $\text{Stab}_{(x,y')}((C_r)$. As before, we can calculate that $h|_{B'} = x^{i_{B'}},$ and that $i_{B'} = k_{B'}r$; and, similarly, $i_{B'} = k'_{B'}p$. Since $\gcd(s,r) = 1,$ we have $p \nmid r,$ so $i_{B'} = k''_{B'}rp$. Now, the intersection of the orbit of $h$ containing the vertex $v$ in $B'$ with the block $D'$ of $C_{rp}$ that contains the vertex $v$ is clearly the singleton $\{v\}$, since the block $D'$ is an orbit of $x^{as/p}$. This shows that when $h$ fixes the block $D'$ setwise, it in fact fixes this block pointwise, so that $h \in \text{Stab}_{(x,y)}((C_{rp})$ with $h|_D = 1$ in fact forces $h = 1$, as required. This proves our claim.

Thus, $C_p$ is a collection of blocks of prime size of $(x,y')$, formed by the orbits of $x^{n/p}$, upon which $\text{Stab}_{(x,y)}((C_p)$ is not faithful. \hfill \Box

### 3.6 Not Wreath Products

**3.6.1 General Results**

**Lemma 3.6.1** Let $G \leq S_{mk}$ admit a complete block system $B$ of $m$ blocks of size $k$, $k$ composite. Assume that $\text{Stab}_G(B)$ acts faithfully on $B \in B$ and that $\text{Stab}_G(B)|_B$ is doubly transitive and nonsolvable for every $B \in B$. If $G$ contains an $mk$-cycle, then $\text{Stab}_G(B)|_B$ is equivalent to $\text{Stab}_B(B)|_B$ for every $B, B' \in B$.

**Proof.** As $G$ contains an $mk$-cycle, we assume without loss of generality that $x \in G$. Let $H = \langle \text{Stab}_G(B), x \rangle$. Then $\text{Stab}_H(B) = \text{Stab}_G(B)$. Let $B \in B$. Perusing the list of doubly transitive groups given in Theorem 3.2.22, we have (assuming towards a contradiction that there exist $B_1, B_2$ such that $\text{Stab}_G(B)|_{B_1}$ is not equivalent to $\text{Stab}_G(B)|_{B_2}$) that since $\text{Stab}_H(B)|_B$ has more than one representation, it has exactly two representations. Define an equivalence relation $\equiv$ on the elements permuted
by \( S_{m,k} \) by \( i \equiv j \) if and only if \( \text{Stab}_{\text{Stab}(B)}(i) = \text{Stab}_{\text{Stab}(B)}(j) \). As \( \text{Stab}_H(B)|_B \) has two representations, there are \( m/2 \) elements in each equivalence class of \( \equiv \) and these equivalence classes of \( \equiv \) form a complete block system \( C \) of \( 2k \) blocks of size \( m/2 \) formed by the orbits of \( \langle x^{2k} \rangle \). Then \( H/C \) admits a complete block system \( D \) of \( 2 \) blocks of size \( k \) formed by the orbits of \( \langle x^2 \rangle/C \). Let \( D = \{ D_1, D_2 \} \).

Furthermore, \( \text{Stab}_H(C)|_D \) is doubly transitive and nonsolvable and \( \text{Stab}_H(C)|_{D_1} \) is not equivalent to \( \text{Stab}_H(C)|_{D_2} \).

As \( x \in H \), \( \text{Stab}_H(C)|_{D_1} \) contains a \( k \)-cycle. Hence \( \text{Stab}_H(C)|_{D_1} \) contains a \( k \)-cycle and has two representations. By Theorem 3.2.21 and Theorem 3.2.22, together with \( k \) composite, we need only consider the cases where \( \text{soc}(\text{Stab}_H(C)|_{D_1}) = A_6 \) \( (k = 6) \), or \( \text{PSL}(d, q) \) \( (k = (q^d - 1)/(q - 1) \) and \( d \geq 2) \). If \( k = 6 \) and \( \text{soc}(\text{Stab}_H(C)|_{D_1}) = A_6 \) or \( S_6 \), then as \( \text{Stab}_H(C)|_{D_1} \) contains a \( 6 \)-cycle,

\[
\text{Stab}_H(C)|_{D_1} = S_6,
\]

contradicting Lemma 3.6.10 (stated and proven later). If \( k = (q^d - 1)/(q - 1) \) and \( \text{soc}(\text{Stab}_H(C)|_{D_1}) = \text{PSL}(d, q) \), then by Corollary 3.6.7 (stated and proven later) \( K \) does not contain a \( 2k \)-cycle, a contradiction. \( \square \)

**Lemma 3.6.2** Let \( y \in S_n \) be an \( n \)-cycle such that \( \langle x, y \rangle \) admits a complete block system \( B \) of \( m \) blocks of size \( k \) and \( \langle x, y \rangle/B \) admits a complete block system \( C \) of \( r \) blocks of size \( s \), where \( s \) is composite. Assume that \( \text{Stab}_{\langle x, y \rangle}(B) = \langle x^m \rangle \) and that \( \text{soc}(\text{Stab}_{\langle x, y \rangle/B}(C)|_C) \) is a doubly transitive nonabelian simple group. Let

\[
D = \{ D_C = \cup \{ B \in C : C \in C \} \}
\]

be the complete block system of \( \langle x, y \rangle \) of \( r \) blocks of size \( sk \). If \( \text{Stab}_{\langle x, y \rangle}(D) \) is faithful, then there exists \( y' \in \langle x, y \rangle \) such that \( \langle y' \rangle \) is conjugate to \( \langle y \rangle \) in \( \langle x, y \rangle \) and \( \langle x, y' \rangle \) admits a complete block system \( E \) of \( m/p \) blocks of size \( pk \) for some prime \( p|m \), and \( \langle (y')^m \rangle = \langle x^m \rangle \).

**Proof.** As \( \langle x, y \rangle \) admits a complete block system \( B \) of \( m \) blocks of size \( k \), the blocks of \( B \) are formed by the orbits of \( \langle x^m \rangle \) and \( \langle y^m \rangle \). As \( \text{Stab}_{\langle x, y \rangle}(B) = \langle x^m \rangle \), we have that \( \langle y^m \rangle = \langle x^m \rangle \). Hence if \( \delta \in \langle x, y \rangle \), then \( \delta^{-1} y^m \delta = y^m \).
Since \( \text{Stab}_{(x,y)}(D) \) acts faithfully on each block of \( D \), it suffices to show that there exists \( y' \in (x,y) \) such that \( \langle y' \rangle \) is conjugate to \( \langle y \rangle \) in \( (x,y) \) and \( \langle x,y' \rangle \) admits a complete block system \( E \) of \( m/p \) blocks of size \( pk \), for some \( p \mid m \). It thus suffices to show that there exists \( y' \in (x,y) \) such that \( \langle y' \rangle \) is conjugate to \( \langle y \rangle \) in \( (x,y) \) and \( \langle x,y' \rangle / B \) admits a complete block system \( F \) of \( m/p \) blocks of size \( p \) for some \( p \mid m \).

As \( \text{Stab}_{(x,y)}(D) \) acts faithfully on each \( D \in D \) and \( \text{soc}(\text{Stab}_{(x,y)}/G(C)|_C) \) is a doubly transitive nonabelian simple group, it is nonsolvable. It follows by Lemma 3.6.1 that the actions of \( \text{Stab}_{(x,y)}/G(C)|_C \) and \( \text{Stab}_{(x,y)}/G(C)|_{C'} \) are equivalent for every \( C, C' \in C \). As \( s \) is composite, it follows from Theorem 3.2.21 that the group \( \text{soc}(\text{Stab}_{(x,y)}/G(C)|_C) \) is either \( A_s \) or \( PSL(d,q) \). Hence \( \text{Stab}_{(x,y)}/G(C)|_C \) is \( A_s \), \( S_s \) or is contained in \( PGL(d,q) \) and contains \( PSL(d,q) \). By Corollary 3.6.9 and Lemma 3.6.11 there exists \( g \in (x,y) \) such that \( \langle x^r, g^{-1}y^rg \rangle / B|_C \) admits \( s/p \) blocks of size \( p \). By Lemma 3.4.1, \( (x,g^{-1}yg)/B \) admits a complete block system of \( m/p \) blocks of size \( p \), and we are done. \( \square \)

### 3.6.2 Results Dealing with \( PSL(d,q) \)

The next two lemmata and the proposition that follow them were proven by Dr. Dave Witte, to assist Dr. Dobson and myself with this result. Since they have not appeared elsewhere, the proofs of the results are included here.

**Notation 3.6.3** In this subsection, if \( V \) is a vector space, then \( P(V) \) is used to denote the set of all points of the vector space.

**Lemma 3.6.4** Let \( m = (q^d - 1)/(q - 1) \), with \( n \geq 3 \), write \( q = p^r \) with \( p \) prime, and let \( m' = m/\gcd(r,m) \). Let \( x \) be an element of order \( m' \) in \( PGL(d,q) \) that acts semi-regularly on \( P((F_q)^d) \). Then \( x \) is not conjugate to \( x^{-1} \) in \( PGL(d,q) \).

**Proof.** Let \( \hat{x} \) be any lift of \( x \) to \( GL(d,q) \). The cardinality of the linear span of any \( \hat{x} \)-orbit is at least \( (q - 1)m' \), which is greater than \( q^{d-1} \), so we see that \( \hat{x} \) is irreducible. Thus, by Schur's Lemma, the centraliser of \( \hat{x} \) in \( \text{Mat}(d,q) \) is a finite field. From the cardinality, we conclude that the centraliser is isomorphic to \( F_{q^d} \).
Abusing notation, we may assume that this centraliser is actually $\mathbb{F}_{q^d}$ itself. Thus, we may assume that $\hat{x} \in \mathbb{F}_{q^d}^*$ and that the centraliser of $\hat{x}$ in $\text{GL}(d, q)$ is $\mathbb{F}_{q^d}^*$.

Suppose $g \in \text{PGL}(d, q)$ with $g^{-1}xg = x^{-1}$. Because $g$ inverts $x$, it must normalise $\mathbb{F}_{q^d}^*$, the centraliser of $x$ in $\text{GL}(d, q)$. Therefore, the map $\mathbb{F}_{q^d}^* \to \mathbb{F}_{q^d}^*$ defined by $t \mapsto g^{-1}tg$ is clearly a field automorphism (i.e., it is bijective and respects addition and multiplication). So there is a natural number $k$, such that $g^{-1}tg = t^k$ for all $t \in \mathbb{F}_{q^d}^*$. (Because $t^{p^rd} = t^q = t$ for all $t \in \mathbb{F}_{q^d}^*$, we may and do assume $k \leq rd/2$.)

Because $g^{-1}xg = x^{-1}$, we must have $p^k \equiv 1 \pmod{m'}$, so

\[ p^k + 1 \geq m' \geq \frac{p^{rd} - 1}{(p^r - 1)} = \frac{p^{rd}}{r} + \frac{p^{rd-2}}{r} + \cdots + \frac{p^{rd-1}}{r} > \frac{p^{rd}}{r} + 1. \]

It therefore suffices to show $\frac{p^{rd}}{r} \geq p^{rd/2}$, for this implies $k > rd/2$, a contradiction.

Case 1. Assume $(p, r) \neq (2, 3)$. We have $r \leq \frac{p^r}{2} \leq \frac{p^{rd/2}}{r}$, so

\[ \frac{p^{rd}}{r} \geq \frac{p^{rd/2}}{\frac{p^{rd/2}}{r}} = p^{rd/2}. \]

Therefore, $k > rd/2$, a contradiction.

Case 2. Assume $(p, r) = (2, 3)$ and $d \geq 4$. We have

\[ \frac{p^{rd-1}}{r} = \frac{8^{d-1}}{3} > 8^{d-2} \geq 8^{d/2} = p^{rd/2}, \]

so $k > rd/2$, a contradiction.

Case 3. Assume $(p, r, d) = (2, 3, 3)$. We have

\[
\begin{align*}
p^k + 1 &> \frac{p^{rd-1}}{r} + \frac{p^{rd-2}}{r} = \frac{2^{3(3-1)}}{3} + \frac{2^{3(3-2)}}{3} \\
&= 24 > 16\sqrt{2} + 1 = 2^{9/2} + 1 = p^{rd/2} + 1.
\end{align*}
\]

Therefore, $k > rd/2$, a contradiction. \qed
Lemma 3.6.5 Let \( m = (q^d - 1)/(q - 1) \), with \( d \geq 3 \), write \( q = p^r \) with \( p \) prime, let \( m' = m / \gcd(r,m) \), and let \( V \) be an \( d \)-dimensional vector space over \( \mathbb{F}_q \). Let \( x \) be an element of order \( m' \) in \( \text{PGL}(V) \) that acts semi-regularly on \( \mathbb{P}(V) \), and let \( \mathcal{H}(V) \) be the set of all \((d-1)\)-dimensional subspaces of \( V \). There is a bijection \( f: \mathbb{P}(V) \to \mathcal{H}(V) \) and an automorphism \( \rho \) of \( \text{PGL}(V) \), such that \( \rho(x) = x^{-1} \) and, for all \( v \in \mathbb{P}(V) \) and all \( g \in \text{PGL}(V) \), we have \( f(gv) = \rho(g)f(v) \).

**Proof.** Let \( \hat{x} \) be a representative of \( x \) in \( \text{GL}(V) \). From the beginning of the proof of the preceding lemma, we see that we may assume \( V = F_{q^d} \) and that \( \hat{x} \in F_{q^d}^* \).

Define \( \text{tr}: F_{q^d} \to F_q \) by \( \text{tr}(t) = t + t^q + \cdots + t^{q^d-1} \) (so \( \text{tr} \) is the “trace map” from \( F_{q^d} \) to \( F_q \)), and define an \( F_q \)-bilinear form on \( F_{q^d} \) by \( (s \mid t) = \text{tr}(st) \). Because \( F_{q^d} \) is a separable extension of \( F_q \), this bilinear form is nondegenerate (i.e., for every nonzero \( s \in F_{q^d} \), there is some \( t \in F_{q^d} \) with \( (s \mid t) \neq 0 \)). For each one-dimensional \( F_q \)-subspace \( W \) of \( F_{q^d} \), define
\[
 f(W) = \{ v \in F_{q^d} \mid (v \mid W) = 0 \}.
\]
Because the bilinear form is nondegenerate, \( f \) is a bijection from the set of one-dimensional subspaces of \( F_{q^d} \) onto the set of \((d-1)\)-dimensional subspaces.

For each \( g \in \text{PGL}(V) \), let \( g^T \) be the transpose of \( g \) with respect to the bilinear form (that is, \( (v \mid gw) = (g^Tv \mid w) \)), and let \( \rho(g) = (g^T)^{-1} \).

Because \( (\rho(g)v, gW) = ((g^T)^{-1}v, gW) = (g^T(g^T)^{-1}v, W) = (v, W) \), it is clear that \( f(gW) = \rho(g)f(W) \).

Furthermore, for every \( v, w \in F_{q^d} \), we have \( \langle \hat{x}^{-1}v, \hat{x}w \rangle = \text{tr}((\hat{x}^{-1}v)(\hat{x}w)) = \text{tr}(vw) \), so it is clear that \( f(\hat{x}W) = \hat{x}^{-1}f(W) \), so \( \rho(\hat{x}) = \hat{x}^{-1} \).

**Proposition 3.6.6** Let \( m = (q^d - 1)/(q - 1) \), with \( d \geq 3 \). Suppose \( \text{PSL}(d,q) \leq G \leq \text{PGL}(d,q) \) with \( d \geq 3 \), and let \( H \) be a group that contains \( G \) as a normal subgroup. Suppose \( H \) acts imprimitively on a set \( \Omega \), with a complete block system \( \{B_1, B_2\} \) consisting of 2 blocks of cardinality \( m \). Assume \( G = \{ h \in H \mid h(B_1) = B_1, h(B_2) = B_2 \} \). Assume \( G \) acts doubly transitively on \( B_i \) for each \( i = 1,2 \), and
that the action of $G$ on $B_1$ is not equivalent to the action of $G$ on $B_2$. Then $H$ does not contain a transitive, cyclic subgroup.

**Proof.** Suppose $H$ does contain a transitive, cyclic subgroup $\langle y \rangle$. Then $G$ contains a cyclic subgroup $\langle x \rangle$ that is transitive on each of $B_1$ and $B_2$ (and we may assume that $x \in \langle y \rangle$). Write $q = p^r$ with $p$ prime, and let $m' = m/\gcd(r, m)$, so $x^r$ is an element of order $m'$ in $\text{PGL}(d, q)$ that acts semi-regularly.

Because the action of $G$ on $B_1$ is not equivalent to the action of $G$ on $B_2$, one of the actions (say, the action on $B_1$), must be isomorphic to the action of $G$ on $\mathbb{P}(k \mathbb{F}_q^d)$; and the other action must be isomorphic to the action of $G$ on $\mathbb{H}(k \mathbb{F}_q^d)$.

Let $G' = \langle x^r \rangle \text{PSL}(d, q) \subset G$. By combining the conclusion of the preceding paragraph with Lemma 3.6.5, we see that there is a bijection $f: B_1 \to B_2$ and an automorphism $\rho$ of $\text{PGL}(d, q)$, such that $\rho(x^r) = x^{-r}$ and, for all $v \in B_1$ and all $g \in G'$, we have $f(gv) = \rho(g)f(v)$.

Note that $\rho(G') = G'$, because $\rho(x^r) = x^{-r}$ and because every automorphism of $\text{PGL}(d, q)$ normalises $\text{PSL}(d, q)$. Also note that $y$ normalises $G'$, because $y$ centralises $x$ (recall that $x \in \langle y \rangle$) and because $\text{PSL}(d, q)$ is normal in $H$ (since $\text{PSL}(d, q)$ is characteristic in $G$, and $G$ has index two in $H$). Therefore, we may define an automorphism $\rho'$ of $G'$ by $\rho'(g) = y\rho(g)y^{-1}$.

Because $\langle y \rangle$ is transitive, we know that $y(B_2) = B_1$, so we may define a permutation $f'$ of $B_1$ by $f'(v) = yf(v)$. Then, for all $v \in B_1$ and all $g \in G'$, we have

$$f'(gv) = yf(gv) = (y\rho(g)y^{-1})yf(v) = \rho'(g)f'(v) = \rho'(g)f(v).$$

Thus, the permutation $f'$ normalises $G'|_{B_1}$, so $f'$ normalises $\text{PSL}(d, q)$, from which we conclude that $f' \in \text{PGL}(d, q)$.

Because $x \in \langle y \rangle$, we know that $y$ centralises $x^r$, so

$$\rho'(x^r) = y\rho(x^r)y^{-1} = yx^{-r}y^{-1} = x^{-r}.$$ 

Therefore, from (3.1), we conclude that $f'$ conjugates $x^r|_{B_1}$ to $x^{-r}|_{B_1}$. This contradicts the conclusion of Lemma 3.6.4. \hfill $\Box$
Corollary 3.6.7 Let $G \leq S_{2m}$ admit a complete block system $\mathcal{B}$ of 2 blocks of size $m$. Assume that $\text{Stab}_G(\mathcal{B})$ acts faithfully on $B \in \mathcal{B}$ and $\text{soc}(\text{Stab}_G(\mathcal{B})) \cong \text{PSL}(d, q)$, where $d$ is an integer, $q$ is a prime power, and $m = (q^d - 1)/(q - 1)$. Let $\mathcal{B} = \{B_1, B_2\}$. If $\text{Stab}_G(\mathcal{B})|_{B_1}$ is not equivalent to $\text{Stab}_G(\mathcal{B})|_{B_2}$, then $G$ does not contain a $2m$-cycle.

**Proof.** Most of this result is trivial from Proposition 3.6.6. When $d = 2$, we have $\text{PSL}(2, q)$, and this group has only one transitive representation acting on $(q^d - 1)/(q - 1) = q + 1$ points. This is because the stabiliser of a point in such a representation is the normaliser of a Sylow $p$-subgroup (where $p$ is the prime dividing $q$), and so by Theorem 1.2.34, they are all conjugate. Thus, when $d = 2$, the hypotheses of this lemma cannot arise. 

Lemma 3.6.8 Let $C_1$ and $C_2$ be cyclic subgroups of $\text{PGL}(d, q)$ (with $n \geq 2$) that act transitively on $\mathbb{P}(\mathbb{F}_q^d)$. Then there is some $g \in \text{PSL}(d, q)$ such that $C_1 \cap (g^{-1}C_2g)$ is nontrivial.

**Proof.** Let $c$ generate $C_1$, write $q = p^r$, with $p$ prime, and let $m = (q^d - 1)/(q - 1)$. Because $|\text{PGL}(d, q) : \text{PGL}(d, q)| = r$, we know $c^r \in \text{PGL}(d, q)$. The cardinality of each orbit of $c^r$ is

$$\frac{m}{\gcd(r, m)} \geq \frac{m}{r} > \frac{m}{p^r} = \frac{q^d - 1}{q(q - 1)} > \frac{q^d - q}{q - 1} = \frac{q^d - 1}{q - 1} = |\mathbb{P}(\mathbb{F}_q^d)|.$$

So no orbit of $c^r$ is contained in any proper subspace of $\mathbb{P}(\mathbb{F}_q^d)$. Therefore, letting $c'$ be a representative of $c^r$ in $\text{GL}(d, q)$, we see that $c'$ acts irreducibly on $(\mathbb{F}_q^d)$. So there is some element $\alpha$ of $\mathbb{F}_q^\times$ such that the action of $c'$ on $(\mathbb{F}_q^d$ is $\mathbb{F}_q$-linearly isomorphic to the action of $\alpha$ by multiplication on $\mathbb{F}_q^d$. So the action of $(c')\mathbb{F}_q^\times$ is $\mathbb{F}_q$-linearly isomorphic to the action of a subgroup of $\mathbb{F}_q^d$ by multiplication on $\mathbb{F}_q^d$.

Similarly, if $f$ is a generator of $C_2$, then $f^r$ lifts to an element $f'$ of $\text{GL}(d, q)$ such that the action of $(f')\mathbb{F}_q^\times$ is $\mathbb{F}_q$-linearly isomorphic to the action of a subgroup of $\mathbb{F}_q^d$ by multiplication on $\mathbb{F}_q^d$. Because $\mathbb{F}_q^d$ is cyclic, it has only one subgroup of any given order, so we conclude that the action of $(c')\mathbb{F}_q^\times$ is $\mathbb{F}_q$-linearly isomorphic to the action of $(f')\mathbb{F}_q^\times$; in other words, $(c')\mathbb{F}_q^\times$ is conjugate to $(f')\mathbb{F}_q^\times$ in $\text{GL}(d, q)$. 

\[\square\]
Because the centraliser of \( c' \) in \( \text{GL}(d, q) \) contains elements of every possible nonzero determinant (cf. [43] proof of Satz 7.3(b), pp. 187–189), we conclude that \( \langle c' \rangle \mathbb{F}_q^\times \) is conjugate to \( \langle f' \rangle \mathbb{F}_q^\times \) via an element of \( \text{SL}(d, q) \). Therefore, replacing \( C_1 \) by a conjugate under \( \text{SL}(d, q) \), we may assume \( \langle c' \rangle \mathbb{F}_q^\times = \langle f' \rangle \mathbb{F}_q^\times \). So \( c' = f' \).

\[ \square \]

**Corollary 3.6.9** Suppose \( \text{PSL}(d, q) \leq G \leq \text{PGL}(d, q) \) (with \( d \geq 2 \)). Let \( C_1 \) and \( C_2 \) be cyclic subgroups of \( G \) that act transitively on \( \mathbb{P}((\mathbb{F}_q)^d) \). Then there is some \( g \in G \) such that \( \langle C_1, (g^{-1}C_2g) \rangle \) acts imprimitively on \( \mathbb{P}((\mathbb{F}_q)^d) \). Furthermore, the blocks can be chosen to have prime size.

**Proof.** Most of this result is trivial from Lemma 3.6.8. For the “furthermore,” let \( C_1 = \langle x \rangle \) and \( C_2 = \langle y \rangle \). Then since \( \langle x \rangle \cap \langle g^{-1}yg \rangle \neq \emptyset \), we have \( \langle x \rangle \cap \langle g^{-1}yg \rangle = \langle x^m \rangle \) for some \( m \). Since \( \langle x^m \rangle \leq \langle g^{-1}yg \rangle \), we have \( \langle g^{-1}yg \rangle = \langle x^m \rangle \). Thus the center of \( \langle x, g^{-1}yg \rangle \) contains \( \langle x^m \rangle \), so the orbits of every subgroup of \( \langle x^m \rangle \) form a complete block system. We choose a subgroup of prime order to yield the desired result.

\[ \square \]

### 3.6.3 Results dealing with \( A_n \) and \( S_n \)

**Lemma 3.6.10** Let \( G \leq S_{12} \) admit a complete block system \( B \) of 2 blocks of size 6. Let \( B = \{B_1, B_2\} \). Assume that \( \text{Stab}_G(B) \) acts faithfully on \( B \in B \) and that \( \text{Stab}_G(B) \cong S_6 \) but \( \text{Stab}_G(B)|_{B_1} \) is not equivalent to \( \text{Stab}_G(B)|_{B_2} \). Then \( G \) does not contain a 12-cycle.

**Proof.** Assume that \( G \) contains a 12-cycle. Without loss of generality, we assume that \( x \in G \). Then \( B \) is formed by the orbits of \( \langle x^2 \rangle \) and \( x^2 \in \text{Stab}_G(B) \). Then conjugation by \( x \) induces an automorphism \( \alpha \) from \( \text{Stab}_G(B)|_{B_1} \) to \( \text{Stab}_G(B)|_{B_2} \). As \( \text{Stab}_G(B)|_{B_1} \) is not equivalent to \( \text{Stab}_G(B)|_{B_2} \), \( \alpha \) is an outer automorphism of \( S_6 \).

The group \( S_6 \) has two kinds of elements of order 3: (a) 3-cycles, and (b) the product of two disjoint 3-cycles. Any element of type (b) is the square of a 6-cycle, but no element of type (a) is the square of a 6-cycle. It is well-known that there is an outer automorphism of \( S_6 \) that interchanges type (a) and type (b) (cf. [89],
11.4.3, pp. 310-311). Thus, this outer automorphism cannot take any 6-cycle to another 6-cycle.

However, modulo inner automorphisms, there is only one outer automorphism of $S_6$. Hence, as $\alpha$ is an outer automorphism of $S_6$, $\alpha(x^2|B_i)$ is not a 6-cycle so that $x^{-1}x^2x \notin \langle x \rangle$, a contradiction. □

**Lemma 3.6.11** Let $x, y$ be $n$-cycles in $A_n$, $n$ composite, acting on the set $X$ with $|X| = n$. Then for any prime $p|n$ there exists $\delta \in A_n$ such that $\langle x, \delta^{-1}y\delta \rangle$ admits $n/p$ blocks of size $p$.

**Proof.** Since $n$ is composite and $A_n$ contains an $n$-cycle, we must have $n \geq 8$, so $A_n$ is $(n-2)$-transitive by Theorem 3.2.19. Label the elements of $X$ by $\{(i, j) : i \in \mathbb{Z}_p, j \in \mathbb{Z}_{n/p}\}$, such that $x^{n/p}(i, j) = (i+1, j)$. Let $(c_0, k_0), (c_1, k_1), \ldots, (c_{n/p-1}, k_{n/p-1})$ be in distinct orbits of $y^{n/p}$. Then we can choose $\delta \in A_n$ such that

$$\delta(y^{an/p}(c_j, k_j)) = x^{an/p}(0, j) = (a, j),$$

for all $j \geq 1$. Clearly $\delta(y^{an/p}(c_0, k_0))$ must be in the set $\{(i, 0) : i \in \mathbb{Z}_p\}$, so the sets $\{(i, j) : i \in \mathbb{Z}_p\}$, must be blocks of $\langle x, \delta^{-1}y^{n/p}\delta \rangle$ for each $j \in \mathbb{Z}_{n/p}$. Since they are in fact orbits of both $x^{n/p}$ and $\delta^{-1}y^{n/p}\delta$, they are actually blocks of both $\langle x \rangle$ and $\langle \delta^{-1}y\delta \rangle$, so are blocks of $\langle x, \delta^{-1}y\delta \rangle$. □
Chapter 4

Isomorphic Cayley Graphs on Nonisomorphic Groups

4.1 Preliminaries

This chapter examines the question of when two Cayley digraphs on different abelian groups of prime power order can be isomorphic. This is a natural extension of the Cayley Isomorphism problem that asks when two Cayley digraphs on the same group can be isomorphic.

Anne Joseph [45] had previously determined the answer to this question when the groups have order $p^2$ ($p$ prime). Her results are extended. The results in this chapter have appeared in the *Journal of Graph Theory* [77]. Andrew Mauer independently proved the extension of her result to the prime-cubed case [71]. The only other result along these lines is by J. Dixon [16], who enumerated the Cayley graphs isomorphic to small hypercubes.

For many of the results in this chapter, the lemmata and proofs used are direct extensions of those in Joseph's paper [45].

We define a partial order on the set of abelian groups of order $p^n$ as follows.

**Definition 4.1.1** We say $G \leq_{po} H$ if there is a chain

$$H_1 < H_2 < \ldots < H_m = H$$
Figure: The partial order for abelian groups of order $p^5$.

of subgroups of $H$ such that $H_1, \frac{H_2}{H_1}, \ldots, \frac{H_m}{H_{m-1}}$ are all cyclic, and

$$G \cong H_1 \times H_2 \times \ldots \times H_m.$$  

There is an equivalent definition for this partial order that is less group-theoretic but perhaps more intuitive.

**Definition 4.1.2** We say that a string of integers $i_1, \ldots, i_m$ is a **subdivision** of the string of integers $j_1, \ldots, j_m'$ if there is some permutation $\delta$ of $\{1, \ldots, m\}$ and some strictly increasing sequence of integers $0 = k_0, \ldots, k_t = m$ such that $i_{\delta(k_s+1)} + \ldots + i_{\delta(k_{s+1})} = j_{s+1}, 0 \leq s \leq m' - 1$.

Now, $G \leq_{p\Omega} H$ precisely if $G \cong \mathbb{Z}_{p^{i_1}} \times \mathbb{Z}_{p^{i_2}} \times \ldots \times \mathbb{Z}_{p^{i_m}}$ and $H \cong \mathbb{Z}_{p^{j_1}} \times \mathbb{Z}_{p^{j_2}} \times \ldots \times \mathbb{Z}_{p^{j_{m'}}}$, where $i_1, \ldots, i_m$ is a subdivision of $j_1, \ldots, j_{m'}$. 
The figure on the previous page illustrates this partial order on abelian groups of order \( p^5 \).

The following are a few results by other mathematicians that are used in this chapter of the thesis.

**Theorem 4.1.3** (Sabidussi, [86], Lemma 4) Let \( \bar{X} \) be a digraph and \( G \) be a group. The automorphism group \( \text{Aut}(\bar{X}) \) has a subgroup isomorphic to \( G \) that acts regularly on \( V(\bar{X}) \) if and only if \( \bar{X} \) is isomorphic to a Cayley digraph \( \bar{X}(G; S) \) for some subset \( S \) of \( G \).

Although the proof in Sabidussi's paper is given for graphs rather than digraphs, it works for both structures, as well as for colour digraphs.

**Lemma 4.1.4** (Joseph, [45], Lemma 3.11) Let \( \bar{X} \) and \( \bar{X}' \) be digraphs. Let \( \phi : V(\bar{X}) \rightarrow V(\bar{X}') \) be a surjective map. Assume the following conditions are satisfied:

1. For every \( v \) and \( w \) in \( V(\bar{X}') \), the induced subdigraph \( \bar{X}[\phi^{-1}(v)] \) is isomorphic to the induced subdigraph \( \bar{X}[\phi^{-1}(w)] \).

2. For every \( x \) and \( y \) in \( V(\bar{X}) \) with \( \phi(x) \neq \phi(y) \), the vertex \( x \) is adjacent to the vertex \( y \) in \( \bar{X} \) if and only if \( \phi(x) \) is adjacent to \( \phi(y) \) in \( \bar{X}' \).

Then \( \bar{X} \cong \bar{X}' \downarrow \bar{X}[\phi^{-1}(v_0)] \) for every \( v_0 \in V(\bar{X}') \).

The proof of this result is a simple matter of defining an isomorphism together with induction.

The following are two well-known results about \( p \)-groups, and the proofs are straightforward.

**Theorem 4.1.5** Any nontrivial \( p \)-group has an element of order \( p \).

**Theorem 4.1.6** A nontrivial \( p \)-group has a nontrivial center.

**Theorem 4.1.7** ([95], Proposition 3.1) If the permutation group \( G \) is transitive on the set \( V \) and \( x, y \in V \), then \( G_x \) and \( G_y \) are conjugate in \( G \).
We are now ready to give the main result, which will be proven in the succeeding sections.

**Theorem 4.1.8** Let $\tilde{X} = \tilde{X}(G; S)$ be a Cayley digraph on an abelian group $G$ of order $p^n$, where $p$ is an odd prime. Then the following are equivalent:

1. The digraph $\tilde{X}$ is isomorphic to a Cayley digraph on both $\mathbb{Z}_{p^n}$ and $H$, where $H$ is an abelian group with $|H| = p^n$, say
   
   $H = \mathbb{Z}_{p^{k_1}} \times \mathbb{Z}_{p^{k_2}} \times \ldots \times \mathbb{Z}_{p^{k_m}}$,
   
   where $k_1 + \ldots + k_m = n$.

2. There exist a chain of subgroups $G_1 < \ldots < G_{m-1}$ in $G$ such that
   
   (a) $G_1, G_2/G_1, \ldots, G_{m-1}/G_{m-1}$ are cyclic groups;
   
   (b) $G_1 \times G_2/G_1 \times \ldots \times G_{m-1}/G_{m-1} \leq_{po} H$;
   
   (c) For all $s \in S \setminus G_i$, we have $sG_i \subseteq S$, for $i = 1, \ldots, m-1$. (That is, $S \setminus G_i$ is a union of cosets of $G_i$.)

3. There exist Cayley digraphs $\tilde{U}_1, \ldots, \tilde{U}_m$ on cyclic $p$-groups $H_1, \ldots, H_m$ such that $H_1 \times \ldots \times H_m \leq_{po} H$ and $\tilde{X} \cong \tilde{U}_m \mid \ldots \mid \tilde{U}_1$.

   These in turn imply:

4. $\tilde{X}$ is isomorphic to Cayley digraphs on every abelian group of order $p^n$ that is greater than $H$ in the partial order.

This theorem provides several conditions for determining whether or not a given Cayley digraph on an abelian group can be represented as a Cayley digraph on other abelian groups of the same odd prime power order.

Let us look at some simple examples of the use of this theorem. Let

$G = \mathbb{Z}_9 \times \mathbb{Z}_3 \times \mathbb{Z}_3$. 

Let
\[ S = \{(2, i, j), (5, i, j), (8, i, j), (0, i, 2), (0, 1, 0) : 0 \leq i, j \leq 2\}. \]
Then \( G \) and \( S \) satisfy condition (2) with \( G_1 = \langle (0, 1, 0) \rangle, G_2 = \langle G_1, (0, 0, 1) \rangle, G_3 = \langle G_2, (3, 0, 0) \rangle, \) and \( H = \mathbb{Z}_3 \). So (due to condition (4)) \( \bar{X}(G; S) \) can be represented as a Cayley digraph on any abelian group of order 81.

Alternatively, consider the same group \( G \) with
\[ S = \{(2, i, j), (5, i, j), (8, i, j), (0, 1, 1), (0, 1, 2) : 0 \leq i, j \leq 2\}. \]
There is no cyclic subgroup \( G_1 \) of \( G \) that will satisfy condition (2c), so the digraph \( \bar{X}(G; S) \) cannot be represented as a Cayley digraph on the cyclic group of order 81.

Condition (3) is more of a visual condition, stating that the digraph \( \bar{X} \) is a Cayley digraph on both the cyclic group and some other abelian group of order \( p^n \), if and only if it can be drawn as the wreath product of a sequence of Cayley digraphs on smaller cyclic groups.

The next two sections, which prove \( 3 \Rightarrow 1, 4 \) and \( 2 \Rightarrow 3 \), are based very closely on Joseph's paper. In section 4.4, which proves that \( 1 \Rightarrow 2 \), the proof follows the same outline as Joseph's (although some of the methods required are slightly different), through Lemma 4.4.4. From that point on, the lemmata and proofs diverge significantly from those in her paper. These three sections complete the proof of Theorem 4.1.8. Section 4.5 deals with the case where \( p = 2 \), and section 4.6 gives a slightly weaker result following from the same proof for the case where \( G \) is not abelian. Section 4.7 considers the possibility of further extensions of these results.

### 4.2 Proof of \( 3 \Rightarrow 1, 4 \)

Throughout the proof of the main result, we will generally be using induction. The base case is \( n = 1 \), and is trivially true.

Once we have noted that the wreath product of permutation groups is associative, we are ready to proceed with our proof.
Let us define \( v_j (1 \leq j \leq m) \) to be the number of vertices in \( \tilde{U}_j \) (which is a power of \( p \)). We may assume that the digraph \( \tilde{U}_j \) has vertices labeled with \( 0, 1, \ldots, v_j - 1 \) in such a way that the permutation \( \sigma \) defined by \( \sigma(x) = x + 1 \) modulo \( v_j \) is an automorphism of the digraph. It is sufficient, by Theorem 4.1.3 above, to find a regular subgroup of \( \text{Aut}(\tilde{X}) \) that is isomorphic to the group

\[
\mathbb{Z}_{v_j} \times H_1 \times \ldots \times H_{i-1} \times H_{i+1} \times \ldots \times H_{j-1} \times H_{j+1} \times \ldots \times H_m,
\]

for each pair \((i, j)\) satisfying \(1 \leq i < j \leq m\). This is because every abelian group of order \( p^n \) that is greater than \( H_1 \times H_2 \times \ldots \times H_m \) in the partial order can be obtained by repeating the step of combining two elements in the direct product, with appropriate choices of \( i \) and \( j \). Since \( H \) is greater than or equal to \( H_1 \times H_2 \times \ldots \times H_m \), the result will be achieved if such regular subgroups of \( \text{Aut}(\tilde{X}) \) are shown to exist.

By repeated use of Theorem 1.2.71, we see that

\[
\text{Aut}(\tilde{U}_1) \lhd \text{Aut}(\tilde{U}_2) \lhd \ldots \lhd \text{Aut}(\tilde{U}_m) \leq \text{Aut}(\tilde{U}_1 \lhd \tilde{U}_2 \lhd \ldots \lhd \tilde{U}_m) = \text{Aut}(\tilde{X}),
\]

so if we can find the required regular subgroups in

\[
\text{Aut}(\tilde{U}_1) \lhd \text{Aut}(\tilde{U}_2) \lhd \ldots \lhd \text{Aut}(\tilde{U}_m),
\]

we will be done. We will do this by finding independent cycles (recall Definition 1.2.43) of lengths

\[
v_i v_j, v_1, \ldots, v_{i-1}, v_{i+1}, \ldots, v_{j-1}, v_{j+1}, \ldots, v_m.
\]

The cycle of length \( v_k \) will affect only the vertices of \( \tilde{U}_k \) \((1 \leq k \leq m, k \neq i, j)\). The cycle is defined as follows. It is not hard to see that the map

\[
f_k((u_1, \ldots, u_k, \ldots, u_m)) = (u_1, \ldots, u_k + 1, \ldots, u_m)
\]

(where addition is done modulo \( v_j \)) is in the group

\[
\text{Aut}(\tilde{U}_1) \lhd \text{Aut}(\tilde{U}_2) \lhd \ldots \lhd \text{Aut}(\tilde{U}_m).
\]
These are clearly independent cycles. Now we will replace the cycles \( f_i \) and \( f_j \) by a single cycle \( g_{i,j} \) of length \( v_i v_j \) which is also in \( \text{Aut}(X) \). Let \( f'_i \) be the restriction of \( f_i \) to \( \bar{U}_1 \ldots \bar{U}_{i-1} \), and \( f''_j \) be the restriction of \( f_j \) to \( \bar{U}_j \ldots \bar{U}_m \). Define \( f'_{j,u} \) to be equal to \( f''_j \) if the given value \( u_i \) is equal to \( v_i - 1 \), and to be the identity otherwise. Then define

\[
g_{i,j}(u_1, \ldots, u_m) = (f'_i(u_1, \ldots, u_{j-1}), f'_{j,u}(u_j, \ldots, u_m)).
\]

It is clear from the definition of wreath products of groups that this will be in \( \text{Aut}(\bar{X}) \), and it is not hard to see that it is indeed a cycle of the required length which is independent of the other cycles we have created.

The group generated by these cycles is certainly regular on the digraph \( \bar{X} \), so the result follows. \( \square \)

### 4.3 Proof of \( 2 \Rightarrow 3 \)

**Proof.** (\( 2 \Rightarrow 3 \).) Define a digraph \( \bar{X}' \) on the cosets of \( G_{m-1} \) by

\[
V(\bar{X}') = \{G_{m-1}x : x \in G\}
\]

and the arcs of the digraph are

\[
A(\bar{X}) = \{[G_{m-1}x, G_{m-1}y] : x^{-1}y \in S \setminus G_{m-1}\}.
\]

Since \( S \setminus G_{m-1} \) is a union of cosets of \( G_{m-1} \), these arcs are well-defined. It is not hard to see from this definition that \( \bar{X}' \) (which we will call \( \bar{U}_m \)) is a Cayley digraph on \( G_{m-1} \).

Now define the map \( \phi : V(\bar{X}) \to V(\bar{X}') \) by \( \phi(x) = G_{m-1}x \). The conditions in Lemma 4.1.4 above are satisfied, so we have \( \bar{X} \cong \bar{X}' \) \( \bar{X}[G_{m-1}] \). Now the induced subdigraph \( \bar{X}[G_{m-1}] \) is just the Cayley digraph \( \bar{X}(G_{m-1}; S \cap G_{m-1}) \). With the subgroups \( G_1, \ldots, G_{m-2} \), this second Cayley digraph satisfies condition (2) of Theorem 4.1.8, but has \( |G_{m-1}| \) vertices. By induction, we can assume that this
digraph $\hat{X}[G_{m-1}]$ is the wreath product of Cayley digraphs $\hat{U}_{m-1}, \ldots, \hat{U}_1$ on the groups $G_{m-1}, \ldots, G_1$, respectively.

Now

$$\hat{X} \cong \hat{X}' \wr \hat{X}[G_{m-1}] \cong \hat{U}_m \wr \hat{U}_{m-1} \wr \cdots \wr \hat{U}_1$$

is as required. \qed

4.4 Proof of $1 \Rightarrow 2$

We are now assuming that condition (1) of the main result holds.

Lemma 4.4.1 The Sylow $p$-subgroups of $\text{Aut}(\hat{X})$ contain regular subgroups $Q$ and $R$ that are isomorphic to $\mathbb{Z}_{p^n}$ and $H$, respectively. Thus the Sylow $p$-subgroups have order at least $p^{n+1}$.

Proof. Since $\hat{X}$ is a Cayley digraph on both $\mathbb{Z}_{p^n}$ and $H$, the group $\text{Aut}(\hat{X})$ contains regular subgroups that are isomorphic to $\mathbb{Z}_{p^n}$, and others isomorphic to $H$. These are certainly contained in Sylow $p$-subgroups by Theorem 1.2.35, and since all Sylow $p$-subgroups are conjugate by Theorem 1.2.34, each Sylow $p$-subgroup must contain at least one subgroup isomorphic to each of $\mathbb{Z}_{p^n}$ and $H$. We call these $Q$ and $R$.

Since both of these groups are in a Sylow $p$-subgroup, and they are nonisomorphic, the Sylow $p$-subgroup must have order at least $p^{n+1}$. \qed

The Sylow $p$-subgroup under examination, which contains subgroups $Q \cong \mathbb{Z}_{p^n}$ and $R \cong H$, will be denoted by $P$.

Notice that by Theorems 1.2.19, 1.2.56 and 1.2.57, the action of $Q$ on $\hat{X}$ produces unique complete block systems of $\hat{X}$ of any size $p^m, 1 \leq m \leq n - 1$. If the vertices of $\hat{X}$ are labeled with $0, 1, \ldots, p^n - 1$ in such a way that addition modulo $p^n$ has the same action on $\hat{X}$ as $Q$ has, then the blocks of size $p^m$ are precisely the congruence classes modulo $p^{n-m}$. 

Lemma 4.4.2 Every Q-block is a P-block, and vice versa.

Proof. Since \( Q \leq P \), every P-block is a Q-block. We will use induction, and show that if \( P \) has blocks of size \( p^{i-1} \) that are the orbits of a normal subgroup of order \( p^{i-1} \) in \( P \), then \( P \) has blocks of size \( p^i \) that are orbits of a normal subgroup of order \( p^i \) in \( P \), where \( i < n \). Then since there are \( P \)-blocks of every possible size, and since these \( P \)-blocks are also \( Q \)-blocks, and since the \( Q \) blocks of any given size are unique, every \( Q \)-block must be a \( P \)-block.

We will be using Theorem 1.2.56 heavily, so it is useful to point out that \( P \) is indeed transitive, and due to size alone, the normal subgroups we will consider must be intransitive. In the base case \( i = 1 \), this is straightforward: \( P \) itself is a non-trivial \( p \)-group, so has a non-trivial center by Theorem 4.1.6, which is itself a \( p \)-group and so must have an element of order \( p \) by Theorem 4.1.5. This element generates a subgroup of order \( p \) within the center of \( P \), which is certainly normal in \( P \). By Theorem 1.2.56, the orbits of this group are \( P \)-blocks.

We will denote the normal subgroup of order \( p^{i-1} \) by \( P^{(i-1)} \). We look at the group \( P/P^{(i-1)} \). This is a non-trivial \( p \)-group since \( i < n \), and by Theorem 4.1.6 it has a non-trivial center. The center is a \( p \)-group, so by Theorem 4.1.5 has an element \( g \) of order \( p \). Now look at \( (P^{(i-1)}, g) \). First, this is normal in \( P \) since if

\[
h \in aP^{(i-1)} \subseteq G,
\]

then

\[
h^{-1}gh \in P^{(i-1)}a^{-1}gaP^{(i-1)}
\]

and since \( g \) is in the center of \( P/P^{(i-1)} \), this means

\[
h^{-1}gh \in gP^{(i-1)} \subseteq (P^{(i-1)}, g).
\]

Also, the orbits have length \( p^i \) since the action of \( g \) combines sets of \( p \) orbits of \( P^{(i-1)} \), each of which had length \( p^{i-1} \) by assumption. Hence \( (P^{(i-1)}, g) \) is an intransitive, normal, non-trivial subgroup of \( P \), whence by Theorem 1.2.56, each of its orbits is a \( P \)-block.
As these are $P$-blocks of size $p^i$, they must also be $Q$-blocks, and hence be the unique $Q$-blocks of size $p^i$ already described. Since this has shown that $P$ has blocks of every order $p^i$ ($1 \leq i \leq n - 1$), every $Q$-block is indeed a $P$-block. 

**Notation 4.4.3** We will denote the $P$-block of size $p^i$ that contains the vertex $x$ by $B_{x,i}$.

**Lemma 4.4.4** If $x$ and $y$ are two vertices in the same $P$-block of size $p$ (that is, $y \in B_{x,1}$), then $P_x = P_y$.

**Proof.** Since the group $P_x$ fixes the vertex $x$, it must fix the block $B_{x,1}$ setwise. Since $P_x$ is a $p$-group, all orbits must have length a power of $p$, so each of the other $p - 1$ elements of $B_{x,1}$, including $y$, must be fixed pointwise by $P_x$. Hence, $P_x \leq P_y$. But since $P$ is transitive, by Theorem 4.1.7, the groups $P_x$ and $P_y$ are conjugate, so they must be equal. 

The following rather nice lemma was pointed out to me by Dr. David Witte of Oklahoma State University when he was trying to understand my original proof.

**Lemma 4.4.5** If a group $G$ acts on a set $X$, and $x \in X$, then

$$B = \{y \in X : G_x = G_y\}$$

is a $G$-block.

**Proof.** Suppose $y \in B \cap g(B)$, for some $g \in G$. Since $y \in g(B)$, there exists $v \in B$ such that $y = g(v)$, and so

$$G_y = gG_vg^{-1} = gG_xg^{-1}.$$  

Because $y \in B$, this means that $G_x = gG_xg^{-1}$. Suppose $z \in g(B)$. Then, as was true for $y$,

$$G_z = gG_xg^{-1} = G_x.$$  

Hence $z \in B$, and since $z$ was arbitrary, $g(B) \subseteq B$. Therefore $g(B) = B$, and $B$ is a $G$-block. 

\[\square\]
Definition 4.4.6 Let $K$ be a permutation group on a set $X$ with complete block systems based on blocks of two different sizes $j$ and $j'$, $j' < j$. Let $X'$ be the set of blocks of size $j'$ within a fixed block of size $j$. We examine those elements of $K$ which fix each block of size $j'$ setwise. If the permutation group formed by the action of these elements on the set $X'$ is isomorphic to the group $L$, then we say that $K$ acts as $L$ on the blocks of size $j'$ within the blocks of size $j$.

Lemma 4.4.7 Suppose $x$ and $y$ are elements of the set $V(\bar{X})$ that are in different $P$-blocks of size $p^i$, and $R$ acts as $\mathbb{Z}_p \times \mathbb{Z}_p$ on the blocks of size $p^{i-1}$ within the blocks of size $p^{i+1}$, where $i \geq 1$. Then the $P_\infty$-orbit of $y$ is not a subset of $B_{y,i-1}$.

Proof. We examine the group $P_{B_{x,i-1}}$, consisting of all automorphisms in $P$ that fix $B_{x,i-1}$ setwise. (In particular, this contains $P_\infty$.) Now, suppose there is an element $\beta$ of this group that moves $y$ from $B_{y,i-1}$; that is, $\beta \in P_{B_{x,i-1}}$ and $\beta(y) \notin B_{y,i-1}$. Because $\beta(x) \in B_{x,i-1}$, there is some $\sigma \in Q_{B_{x,i-1}}$, such that $\sigma(\beta(x)) = x$; that is, $\sigma \beta \in P_\infty$. Because $Q_{B_{x,i-1}}$ fixes every block of size $p^{i-1}$ setwise, we see that $\sigma \beta(y) \notin B_{y,i-1}$, which yields the result. So we may assume that every element of $P_{B_{x,i-1}}$ fixes $B_{y,i-1}$ setwise.

Let $\mathcal{B}$ be the set of blocks of size $p^{i-1}$ that are contained in $B_{x,i+1}$. The preceding paragraph implies that $P_{B_{y,i-1}} = P_{B_{x,i-1}}$. Now by Lemma 4.4.5, the union of all blocks of size $p^{i-1}$ which have the same setwise stabilisers is a $P$-block $B$ containing both $B_{y,i-1}$ and $B_{x,i-1}$. But we know precisely what the $P$-blocks are, and since $x$ and $y$ are not in the same block of size $p^i$, $B$ must contain $B_{x,i+1}$ at the very least. Hence every point in $\mathcal{B}$ has the same (setwise) stabiliser (namely $P_{B_{x,i-1}}$), so $P_{B_{x,i+1}} / P_{B_{x,i-1}}$ is a regular permutation group on the set $\mathcal{B}$.

Note, however, that the image of $Q_{B_{x,i+1}}$ in $P_{B_{x,i+1}} / P_{B_{x,i-1}}$ is cyclic, whereas the image of $R_{B_{x,i+1}}$ is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$, by assumption. This means that $P_{B_{x,i+1}} / P_{B_{x,i-1}}$ contains two nonisomorphic transitive subgroups, which contradicts the regularity.

The proof of the next lemma is intricate, but not particularly deep. It is the only part of the proof of Theorem 4.1.8 that requires the assumption that $p$ be odd.
Lemma 4.4.8 Suppose \( x \) and \( y \) are elements of the set \( V(\bar{X}) \) that are in different \( P \)-blocks of size \( p^j \). Then if the length of the \( P_x \)-orbit of \( y \) is at least \( p^j \), then the entire block \( B_{y,j} \) must be contained in this orbit.

**Proof.** The proof is by induction on \( j \). The base case, \( j = 0 \), is trivial.

Now we suppose that the orbit has length at least \( p^j \), where \( 1 \leq j \). By the induction hypothesis, the orbit must contain \( B_{y,j-1} \). Since \( P_x \) is a \( p \)-group, and \( B_{y,j} \) is a block of \( P \) and therefore of \( P_x \), the intersection of the \( P_x \)-orbit of \( y \) with \( B_{y,j} \) must have length a power of \( p \), so the length is either \( p^{j-1} \) or \( p^j \). If it is \( p^j \) then we are done, so we assume that it is \( p^{j-1} \). Now, the rest of this orbit (which by assumption has length at least \( p^j \)) must consist of at least \( p - 1 \) other blocks of size \( p^{j-1} \) within distinct blocks of size \( p^j \). Since these are in the orbit of \( y \), there is a \( \beta \in P_x \) that takes \( y \) into one of these other blocks. Choose \( \beta \) in such a way that the size of the smallest block containing both \( y \) and \( \beta(y) \) is minimised, while still being larger that \( p^j \).

Let \( B_{y,l} \) be the smallest \( P \)-block that contains both \( y \) and \( \beta(y) \). Note that

\[
l \geq j + 1.
\]  

(4.1)

Let \( \sigma \in Q \) be such that \( \langle \sigma \rangle = Q \). Now, there exists a number \( a \) such that

\[
\sigma^a(x) = y.
\]  

(4.2)

Also, since \( \beta(y) \in B_{y,l} \), there must be some number \( b \) such that

\[
\sigma^b \in Q_{B_{y,l}}
\]  

and

\[
\sigma^b(y) = \beta(y).
\]  

(4.3)  

Hence,

\[
\sigma^{-a-b} \beta \sigma^a \in P_x.
\]  

(4.4)  

(Recall also that \( Q_{B_{y,l}} \) fixes every \( P \)-block of size \( p^l \) setwise.)

We will show (through long calculation) that

\[
\beta^p(y) \in B_{\sigma^b(y),l-2} \subseteq B_{y,l-1}.
\]
Then the choice of $\beta$ to minimise $l$ will force

$$\beta^p(y) \in B_{y,i-1},$$

so we must have

$$B_{y,j-1} \subseteq B_{\sigma^p(y),i-2}$$

since the intersection of these sets is nonempty and by (4.1). But this tells us that $\sigma^p$ fixes $B_{y,i-2}$ setwise, so $\sigma^p \in Q_{B_{y,i-2}}$. Clearly then, $\sigma^b \in Q_{B_{x,i-1}}$. But this means that

$$\sigma^b(y) = \beta(y) \in B_{y,i-1},$$

contradicting the definition of $l$.

The only possibility remaining will be the truth of this lemma. Now to the calculations.

The smallest $P$-block containing both $x = \sigma^{-a}(y)$ and

$$\sigma^b(x) = \sigma^{b-a}(y) \quad \text{(by (4.2))}$$

$$= \sigma^{-a} \beta(y) \quad \text{(by (4.4))}$$

must be

$$\sigma^{-a}(B_{y,i}) = B_{x,i} \quad \text{(by (4.2))}$$

so the $P_x$-orbit of $\sigma^b(x)$ is contained in $B_{\sigma^b(x),i-1}$. Thus there exist numbers $c$ and $d$ such that

$$\sigma^c, \sigma^d \in Q_{B_{x,i-1}} \quad \text{and} \quad (4.6)$$

$$\beta(\sigma^b(x)) = \sigma^c(\sigma^b(x)) \quad \text{and} \quad (4.7)$$

$$\sigma^{-a-b} \beta \sigma^a(\sigma^b(x)) = \sigma^d(\sigma^b(x)) \quad \text{(using (4.5)). Let} \quad (4.8)$$

$$\gamma = \sigma^{-b-c} \beta \sigma^b; \quad \text{then} \quad (4.9)$$

$$\gamma \in P_x \quad \text{(using (4.7)).}$$
By (4.2) and (4.4), we have

\[ \beta^2(y) = \beta \sigma^{a+b}(x) \]
\[ = \sigma^{a+b}(\sigma^{a-b} \beta \sigma^a) \sigma^b(x) \]
\[ = \sigma^{a+b+d+b}(x) \quad \text{(using (4.8))}. \quad (4.10) \]

Hence,

\[ \gamma(y) = \sigma^{b-c} \beta \sigma^b(y) \quad \text{(by (4.9))} \]
\[ = \sigma^{b-c} \beta^2(y) \quad \text{(by (4.4))} \]
\[ = \sigma^{b-c} \sigma^{a+2b+d}(x) \quad \text{(by (4.10))} \]
\[ = \sigma^{a+b-c+d}(x). \quad (4.11) \]

Now, by (4.6) and (4.11), we have that

\[ \gamma(y) \in B_{\sigma^{a+b}(x),j-1} = B_{\beta(y),j-1} \quad \text{(by (4.2), (4.4))}. \]

Hence \( B_{\gamma(y),j-1} = B_{\beta(y),j-1} \), so \( \gamma^{-1} \beta(y) \) is in the block \( B_{y,j-1} \). Our choice of \( \beta \) to minimise \( l \) forces \( \gamma^{-1} \beta(y) \in B_{y,j-1} \). Hence we must have

\[ \gamma(y) \in B_{\beta(y),j-1} \quad \text{and so} \quad (4.12) \]
\[ \sigma^{a+b-c+d}(x) \in B_{\sigma^{a+b}(x),j-1} \quad \text{(by (4.11), (4.2), (4.4))}, \text{ so} \]
\[ \sigma^{d-c} \in Q_{B_{x,j-1}}, \quad \text{whence} \quad (4.13) \]
\[ \beta^2(y) = \sigma^{a+2b+d}(x) \quad \text{(by (4.10))} \]
\[ \in B_{\sigma^{a+2b+d}(x),j-1} \quad \text{(by (4.13))}. \quad (4.14) \]

By induction on \( k \), we will now show that

\[ \gamma^k(y) \in B_{\beta^k(y),j-1} \quad \text{(4.15)} \]  
and \( \beta^{k+1}(y) \in B_{\sigma^{a+(k+1)b+\frac{b(k+1)}{2}}(x),j-2}. \quad (4.16) \)

The base case for (4.15) is (4.12). We require two base cases for (4.16); the case for \( k = 0 \) is clear from (4.2) and (4.4), and the case \( k = 1 \) is clear from (4.14) and (4.1).
Since $\sigma^b$ and $\sigma^c \in Q_{B_{x,l}}$ ((4.3), (4.5)) and $\sigma^{-a-b}\beta\sigma^a \in P_x$ (4.6), we must have some number $e$ such that

$$\sigma^e \in Q_{B_{x,l-1}}$$

and

$$\sigma^{-a-b}\beta\sigma^a\sigma^{k_b+\frac{k(k-1)}{2}}(x) = \sigma^c\sigma^{k_b+\frac{k(k-1)}{2}}c(x).$$

Now, by induction,

$$\beta^{k+1}(y) \in B_{\beta^\sigma^{a+b}+\frac{k(k-1)}{2}}(x), l-2$$

(by (4.16)),

$$= B_{\beta^\sigma^{a+b+c}+\frac{k(k-1)}{2}}(x), l-2$$

(by (4.18))

$$= B_{\beta^\sigma^{(k+1)b}+\frac{k(k-1)}{2}}c(x), l-2.$$ (4.19)

Also, since $\sigma^c \in Q_{B_{x,l-1}}$ (4.6) and since $\beta \in P_x$, there must exist some number $f$ such that

$$\sigma^f \in Q_{B_{x,l-2}}$$

and

$$\sigma^f\beta\sigma^{(1-k)}c(x) = \sigma^{(1-k)}c(x).$$

Let

$$\psi = \sigma^{(k-1)c+f}\beta\sigma^{(1-k)c},$$

so $\psi \in P_x$.

By (4.9), we have

$$\gamma_k(y) = \sigma^{-b-c}\beta\sigma^b\gamma_{k-1}(y)$$

$$\in B_{\sigma^{-b-c}\beta\sigma^{a+b}+\frac{k(k-1)}{2}}(x), l-2$$

(by (4.15), (4.16) and (4.1))

$$= B_{\sigma^{-b-c}\beta\sigma^{(1-k)c}+\frac{k(k-1)}{2}}c(x), l-2$$

(by induction (4.16).)

$$= B_{\sigma^{-b-c}\beta\sigma^{(1-k)c}\beta^k(y), l-2}$$

(by (4.21))

$$= B_{\sigma^{-b-c}\psi\beta^k(y), l-2}$$

(by (4.20)). (4.22)

Now we use (4.21) and the fact that $\sigma^c$ and $\sigma^f$ are in $Q_{B_{x,l-1}}$ ((4.6) and (4.20)) to note that

$$\psi\beta^k(y) \in B_{\beta^{k+1}(y), l-1}.$$
So the choice of \( \beta \) minimizing \( l \) again intervenes to force

\[
\psi \beta^k(y) \in B_{\beta^{k+1}(y), j-1}.
\] (4.23)

Using (4.1), (4.22) and (4.23), we see that

\[
\gamma^k(y) \in B_{\sigma^{-k}\epsilon \hat{c} \beta^{k+1}(y), l-2} = B_{\sigma^{-k}\epsilon \hat{c} \beta^{k+1}(y), l-2}^{(4.19)}
\]

\[
= B_{\sigma^{-k}\epsilon \hat{c} \beta^{k+1}(y), l-2}^{(4.24)}.
\]

Since \( \sigma^c \) and \( \sigma^e \) are in \( Q_{B_x, l-1} \) ((4.6) and (4.17)), we see that the vertex

\[
\sigma^{-k}\epsilon \hat{c} \beta^{k+1}(y) \in B_{\sigma^{-k}\epsilon \hat{c} \beta^{k+1}(y), l-1} = B_{\beta^k(y), l-1}^{(4.16)}
\]

so

\[
\gamma^k(y) \in B_{\beta^k(y), l-1}.
\]

The choice of \( \beta \) to minimise \( l \) forces

\[
\gamma^k(y) \in B_{\beta^k(y), j-1}^{(4.25)}
\]

the first of the desired inductive conclusions (4.15).

Combining (4.25), (4.24) and (4.1) with the inductive assumption from (4.16) that

\[
\beta^k(y) \in B_{\sigma^{-k}\epsilon \hat{c} \beta^{k+1}(y), l-2}^{(4.26)}
\]

we see that

\[
\sigma^{-k}\epsilon \hat{c} \beta^{k+1}(y) \in Q_{B_x, l-2}.
\]

Hence

\[
\beta^{k+1}(y) \in B_{\sigma^{-k}\epsilon \hat{c} \beta^{k+1}(y), l-2}^{(4.19)}
\]

\[
= B_{\sigma^{-k}\epsilon \hat{c} \beta^{k+1}(y), l-2}^{(4.26)},
\]

which concludes the induction on \( k \).
In particular, for $k = p - 1$, we now have that

$$\beta^p(y) \in B_{\sigma^{p+1} + \frac{p(p-1)}{2} c(y),l-2} \quad \text{(by (4.16))}$$

$$= B_{\sigma p + \frac{p(p-1)}{2}c(y),l-2} \quad \text{(by (4.2))}.$$

Because $\sigma^b \in Q_{B_x,i}$ (4.3) and $\sigma^c \in Q_{B_x,i-1}$ (4.6) and $p$ divides $\frac{p(p-1)}{2}$ (this is the only place where the assumption of $p$ being odd is necessary), we have

$$\sigma^{rb} \in Q_{B_x,i-1}$$

and

$$\sigma^{\frac{p(p-1)}{2}c} \in Q_{B_x,i-1}.$$

Hence,

$$\beta^p(y) \in B_{\sigma^{rb}(y),l-2} \subseteq B_{y,l-1},$$

and as mentioned earlier, this completes the proof. \qed

Lemma 4.4.9 Suppose $x$ and $y$ are elements of the set $V(\bar{X})$ that are in different $P$-blocks of size $p^i$, and $R$ acts as $\mathbb{Z}_p \times \mathbb{Z}_p$ on the blocks of size $p^{i-1}$ within the blocks of size $p^{i+1}$. Then the orbit of $P_x$ containing $y$ also contains all of $B_{y,j}$, for $0 \leq j \leq i$; in particular, $B_{y,i}$ is contained in the orbit.

PROOF. The result is by induction on $j$. The base case of $j = 0$ is trivial.

In the induction hypothesis, we assume that $B_{y,j-1}$ is contained in the orbit. Since $j - 1 < i$, Lemma 4.4.7 tells us that the orbit is not contained within $B_{y,j-1}$, so there are other vertices in the orbit. Thus, the length of the orbit (being a power of $p$) must be at least $p^i$. Now Lemma 4.4.8 tells us that $B_{y,j}$ is contained in the orbit, as desired. \qed

Corollary 4.4.10 Suppose $R$ does not act as $\mathbb{Z}_p$ on the blocks of size $p^i$ within the blocks of size $p^j$, where $1 \leq i < j \leq n$. Then $B_{x,k}$ is a wreathed block, for some $k$ such that $i < k < j$. 
PROOF. Since the action of $R$ is not cyclic, there must be some $i'$ and $j'$ with $i \le i' < j' \le j$ such that $j' - i' = 2$, and $R$ acts as $\mathbb{Z}_p \times \mathbb{Z}_p$ on the blocks of size $p'$ within the blocks of size $p'$. By Lemma 4.4.9 with $i = i' + 1$, if $x$ is adjacent to a vertex $y \not\in B_{x,i'+1}$, then $x$ is adjacent to every vertex in $B_{y,i'+1}$. Hence $B_{x,k}$ is a wreathed block, where $k = i' + 1$.

Notice that since $\tilde{X}$ is Cayley on the group $G$, the Sylow $p$-subgroup $P$ must contain a subgroup $R'$ which is conjugate to $G$ in $\text{Aut}(\tilde{X})$. In Lemmata 4.4.7, 4.4.8 and 4.4.9 and Corollary 4.4.10, no special properties of $R$ were employed; in fact, these lemmata continue to hold if $R$ is replaced by $R'$.

**Lemma 4.4.11** There exists a chain of subgroups $G_1 < \ldots < G_{m-1}$ in $G$ such that

1. $G_1, G_2/G_1, \ldots, G/G_{m-1}$ are cyclic groups;
2. $G_1 \times G_2/G_1 \times \ldots \times G/G_{m-1} \leq p_0 H$;
3. For any vertices $x$ and $y$ in $V(\tilde{X})$ with $y \not\in G_i x$, if there is an arc from $x$ to $y$ in $\tilde{X}$, then there is an arc from $x$ to $v$ for all vertices $v \in G_i y$.

**Proof.** Fix a vertex $x \in \tilde{X}$. List the wreathed $P$-blocks containing $x$ in order:

$$\{x\} = B_0 \subset B_1 \subset \ldots \subset B_m = \tilde{X}.$$

For each $i$, there is a unique subgroup $G_i$ of $G$ with $B_i = G_i x$. Also, there is a unique subgroup $H_i$ of $H$ with $B_i = H_i x$.

By the definition of a wreathed block, condition (3) of this lemma is immediate. By Corollary 4.4.10 and the remark that followed it, the fact that there are no wreathed blocks between $B_{i-1}$ and $B_i$ implies that both $G_i/H_{i-1}$ and $H_i/H_{i-1}$ must be cyclic ($1 \leq i \leq m$), fulfilling condition (1).

Finally, since $G_i/H_{i-1}$ and $H_i/H_{i-1}$ have the same order $|B_i|/|B_{i-1}|$, they must be isomorphic groups. Since $G_0 = H_0$ is the identity, $G_m = G$ and $H_m = H$, we get

$$G_1 \times G_2/G_1 \times \ldots \times G/G_{m-1} \cong H_1 \times H_2/H_1 \times \ldots \times H/H_{m-1} \leq p_0 H.$$
Taking the case where \( x \) is the identity element of \( G \), it is easy to see that this result is exactly condition (2) of the main result. This completes the proof of \( 1 \Rightarrow 2 \).

\[ \square \]

### 4.5 What happens if \( p = 2? \)

As was noted earlier, only one lemma toward the proof of the main theorem required the assumption that \( p \) be odd. When \( p \) is even, I have not managed to prove a corresponding lemma, but neither have I found any counterexamples. Indeed, the following version of Theorem 4.1.8 is true when \( p = 2 \).

**Theorem 4.5.1** Let \( \tilde{X} = \tilde{X}(G; S) \) be a Cayley digraph on an abelian group \( G \) of order \( 2^n \). Then the following are equivalent:

1. The digraph \( \tilde{X} \) is isomorphic to a Cayley digraph on both \( \mathbb{Z}_{2^n} \) and \( H = \mathbb{Z}_2 \).

2. There exist a chain of subgroups \( G_1 < \ldots < G_{m-1} \) in \( G \) such that
   
   (a) \( G_1, \frac{G}{G_{i+1}}, \ldots, \frac{G}{G_m} \) are cyclic groups;
   
   (b) \( G_1 \times \frac{G}{G_1} \times \ldots \times \frac{G}{G_m} \leq_p H \);
   
   (c) For all \( s \in S \setminus G_i \), we have \( sG_i \subseteq S \), for \( i = 1, \ldots, m-1 \). (That is, \( S \setminus G_i \) is a union of cosets of \( G_i \).)

3. There exist Cayley digraphs \( \tilde{U}_1, \ldots, \tilde{U}_m \) on cyclic 2-groups \( H_1, \ldots, H_m \) such that \( H_1 \times \ldots \times H_m \leq_p H \) and \( \tilde{X} \cong \tilde{U}_m \ldots \tilde{U}_1 \).

   These in turn imply:

4. \( \tilde{X} \) is isomorphic to Cayley digraphs on every abelian group of order \( 2^n \).

The following lemma immediately gives us \( (1 \Rightarrow 2) \) of Theorem 4.5.1.
Lemma 4.5.2 Under the assumptions of (1) of Theorem 4.5.1, there are subgroups

\[ H_1 < \ldots < H_{n-1} \]

in \( G \) such that \( |H_i| = p^i \) (1 \( \leq i \leq n-1 \)) and for any vertices \( x \) and \( y \) in \( \tilde{X} \) with \( y \notin H_i x \), if \( x \) and \( y \) are adjacent in \( \tilde{X} \) then \( x \) is adjacent to \( v \) for all vertices \( v \in H_i y \).

Proof. Label the digraph \( \tilde{X} \) according to the group \( G \). Then the \( P \)-block of size \( p^i \) containing the identity element of \( G \) is a subgroup of order \( p^i \). This is true since adding any element of \( G \) in this block to every vertex is an automorphism of \( \tilde{X} \) that takes the identity element of \( G \) to another element in this same block, and hence fixes the block setwise. This means that the elements in this block form a closed set under addition, so are a subgroup. We call this subgroup \( H_i \).

We will use induction. With trivial base case \( n = 1 \). Since the definitions of the subgroups \( H_i \) do not change in the inductive step, we can use the induction to assume that the result holds within the block \( B_{x,n-1} \). Now we have two blocks of size \( 2^{n-1} \), with \( x \) in one and \( y \) in the other. We will show that if \( x \) and \( y \) are adjacent in \( \tilde{X} \), then every arc from \( B_{x,n-1} \) to \( B_{y,n-1} \) exists.

First, notice that since \( \tilde{X} \) is a Cayley digraph on \( \mathbb{Z}_2^n \), a group of characteristic 2, the definition of a Cayley digraph tells us that for every arc from \( a \) to \( b \) coming from the element \( b - a = b + a \) of \( S \), there must be a corresponding arc from \( b \) to \( a \) coming from the element \( a - b = a + b \) of \( S \). So we really have a Cayley graph here. Notice also that any two vertices \( a \) and \( b \) in \( B_{y,n-1} \) have an even number of mutual neighbours in \( B_{x,n-1} \). This is because for every vertex \( c \) in \( B_{x,n-1} \) that is adjacent to \( a \) and \( b \), the vertex \( a + b - c = a + b + c \) is also adjacent to both \( a \) and \( b \), and \( a + b + c = c \) would imply \( a + b = 0 \) and hence \( a = b \).

Consider \( \tilde{X} \) now as a Cayley graph on \( \mathbb{Z}_2^n \), and label it accordingly. Since the graph is vertex-transitive, we may assume that 0 and \( x \) are the same vertex. If there are no edges from 0 to \( B_{y,n-1} \), then it is not difficult to see that there are no edges between \( B_{x,n-1} \) and \( B_{y,n-1} \), and we are done. So we may assume that there is an edge between 0 and \( y = m \equiv 1 \) (mod 2) without any loss of generality. Since \( \tilde{X} \) is a Cayley graph, the element \( 2^n - m \) is also in the connection set \( S \). Now as mentioned
in the last paragraph, the vertices \( m \) and \(-m\) must have an even number of mutual neighbours in \( B_{x,n-1} \). Suppose \( a \in B_{x,n-1} \) is adjacent to both \( m \) and \(-m\). Then \(-a\) is also adjacent to both \( m \) and \(-m\). So the only way in which we can have an even number of mutual neighbours for \( m \) and \(-m\), is if the vertex \( 2^{n-1} \) is adjacent to both \( m \) and \(-m\). Thus, every vertex that is adjacent to \( 0 \) is also adjacent to \( 2^{n-1} \).

Now, \( 2^{n-1} \) is the only other element in \( B_{0,1} \), and we already know by our induction hypothesis that \( 0 \) and \( 2^{n-1} \) have precisely the same adjacencies within \( B_{x,n-1} \). Since this is true for \( B_{0,1} \), and the graph is vertex-transitive, the same must be true for each \( P \)-block of size 2. Hence we can form a new graph on \( p^{n-1} \) vertices, one corresponding to each of the \( P \)-blocks of size 2 in \( \tilde{X} \), with an edge between two vertices if and only if all possible edges existed between the corresponding blocks in \( \tilde{X} \). Now we use our induction hypothesis on this graph and carry the conclusion back to the original graph \( \tilde{X} \), yielding the desired result.

Again, taking the case where \( x \) is the identity element of \( G \) in this lemma, yields condition (2) of Theorem 4.5.1.

### 4.6 Non-abelian groups

It is worthy of note that the only way in which the condition that \( G \) be abelian is used in this paper is to work with the richness of the structure of the poset (short for partially-ordered set) defined on abelian groups and to achieve condition (4) of the main theorem. So (using \( H = G \) in the proof) we have the following theorem.

**Theorem 4.6.1** Let \( \tilde{X} = \tilde{X}(G; S) \) be a Cayley digraph on a group \( G \) of order \( p^n \), where \( p \) is an odd prime. Then the following are equivalent:

1. The digraph \( \tilde{X} \) is isomorphic to a Cayley digraph on \( \mathbb{Z}_{p^n} \).
2. There exist a chain of subgroups \( G_1 < \ldots < G_{m-1} \) in \( G \) such that
   
   (a) \( G_1, G_2, \ldots, G_{m-1} \) are cyclic groups;
(b) for all \( s \in S \setminus G_i \), we have \( sG_i \subseteq S \), for \( i = 1, \ldots, m - 1 \). (That is, \( S \setminus G_i \) is a union of cosets of \( G_i \).)

3. There exist Cayley digraphs \( \bar{U}_1, \ldots, \bar{U}_m \) on cyclic p-groups \( H_1, \ldots, H_m \) such that there is some chain of subgroups \( G_1 < \cdots < G_{m-1} \) in \( G \) with

\[
G_1 = H_1, \quad \frac{G_2}{G_1} = H_2, \ldots, \quad \frac{G}{G_{m-1}} = H_m
\]

and \( \bar{X} \cong \bar{U}_m \cdots \bar{U}_1 \).

That is, a Cayley digraph on any group of prime power order can be represented as a Cayley digraph on the cyclic group of the same order if and only if the digraph is the wreath product of a sequence of Cayley digraphs on smaller cyclic groups.

### 4.7 Further extensions

In the general case where the digraph is on a number of vertices \( n \) that is not a prime power, less can be said immediately. First of all, if \( n \) is a product of distinct primes \( p_1, \ldots, p_m \), then \( \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_m} \) is actually cyclic, and hence isomorphic to \( \mathbb{Z}_n \). So any digraph which is a Cayley digraph on one group is necessarily Cayley on the other group.

Moreover, this is true if \( n = n_1n_2\ldots n_m \) where \( n_i \) and \( n_j \) are coprime for every \( i \) and \( j \) with \( 1 \leq i < j \leq m \), and the groups under consideration are \( \mathbb{Z}_n \) and \( \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m} \).

If, on the other hand, \( p \) divides both \( n_i \) and \( n_j \), and the digraph \( \bar{X} \) is Cayley on both \( \mathbb{Z}_n \) and \( \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m} \), then we examine the Cayley digraph \( \bar{X}' \) on those vertices of \( \bar{X} \) that correspond to a Sylow \( p \)-subgroup of \( \mathbb{Z}_n \). Due to the conjugacy of all Sylow \( p \)-subgroups of \( \text{Aut}(\bar{X}) \), it is not hard to show that \( \bar{X}' \) is also Cayley on a Sylow \( p \)-subgroup of \( \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_m} \). We can therefore use Theorem 4.1.8 of this paper to determine its form as a wreath product of smaller digraphs. The remainder of the structure of the digraph \( \bar{X} \) is not so easy to determine in this case, and remains an interesting problem.
Another question that has been suggested is what happens in the case of digraphs that can be represented on two different abelian groups, neither of which is cyclic. The results in this paper rely heavily on properties of the cyclic group, and I have not been able to make any significant progress toward answering this question.
This, therefore, is mathematics: she gives life to her own discoveries; she awakens the mind and purifies the intellect; she brings light to our intrinsic ideas; she abolishes the oblivion and ignorance which are ours by birth.

Proclus

It is my hope that the work in this thesis has in some small way enhanced and refined the beauty that is mathematics. In the course of working on it, I have found great satisfaction in the purity and truth of my chosen discipline; the same qualities that have always been singular about mathematics, and that were described so well by the 5th century Greek, Proclus.
Bibliography


