Identifying Cayley Graphs Among Vertex-Transitive Graphs of Prime Power Order

MICHELLE ONG SHU TIAN

Capstone Final Report for BSc (Honours) in

Mathematical, Computational and Statistical Sciences

Supervised by: Dr. Guang Rao

AY 2023/2024

Yale-NUS College Capstone Project

DECLARATION & CONSENT

1. I declare that the product of this Project, the Thesis, is the end result of my own work and that due acknowledgement has been given in the bibliography and references to ALL sources be they printed, electronic, or personal, in accordance with the academic regulations of Yale-NUS College.

2. I acknowledge that the Thesis is subject to the policies relating to Yale-NUS College Intellectual Property (Yale-NUS HR 039).

ACCESS LEVEL

3. I agree, in consultation with my supervisor(s), that the Thesis be given the access level specified below: [check one only]

✓ Unrestricted access
Make the Thesis immediately available for worldwide access.

o Access restricted to Yale-NUS College for a limited period
Make the Thesis immediately available for Yale-NUS College access only from ____________ (mm/yyyy) to ______________ (mm/yyyy), up to a maximum of 2 years for the following reason(s): (please specify; attach a separate sheet if necessary):
____.

After this period, the Thesis will be made available for worldwide access.

o Other restrictions: (please specify if any part of your thesis should be restricted)
____
____

Michelle Ong (Cendana)
Name & Residential College of Student

Signature of Student

5/4/2024
Date

Rao Guang (Cert)
Name & Signature of Supervisor

5/4/2024
Date

Acknowledgements

This thesis and my Yale-NUS journey have been shaped by a great many people, all of whom cannot possibly be listed here. Nonetheless, I would be remiss not to thank the following:

- Grant Rao, for his infinite patience, excellent supervision and teaching, and for introducing me to graph theory and finite geometry in the first place. It has truly been a pleasure to work with and learn from him as both capstone supervisee and student. I've learned more than I thought possible over the past year and a half.
- Francesca Spagnuolo, for lessons that go far beyond gradients and groups—though those too were crucial, especially the algebraic foundations which eventually led to this capstone. Her compassion, generosity, and empathetic guidance—first as lecturer, then as AD and mentor—have brought me through *so* much. I thank her for always listening, gifting me so many hours of her time (and tissues), and believing in me before I could myself.
- I couldn't have asked for better or kinder teachers than the entire mathematics faculty, of whom I have not yet mentioned Andreas Heinecke, David Smith, and Timothy Wertz. One of each of their courses got me to switch majors from chemistry, and they took me through many fun and inspiring classes. Special thanks to Dave for letting me first try out research (and Hagoromo chalk), and for habits of writing and work that have served me well ever since.
- My beloved suitemates Betty, Gen, Nicole, Ryan, and Yi Wei: for hundreds of dining hall meals, senior suite nights, buttery runs, plushies, summer video calls, too-close-to-2359 submissions, and

above all their consistent love and support over our years living together. Words cannot express how much I appreciate all of you.

- Andrew, Julene, Kevin, Neha, Nicholas, Nicole (again), Ren Yu, and Zhao, who each belong to most of the following sets: math / MCS nerds, pset defeaters, best classmates, research commiserators, Budapest gang, chaotic bridge players, foosball fanatics, gym buddies, deep conversationalists. They're all weird, wonderful friends to be with. Extra thanks to Julene for reading a draft of this thesis!
- The library staff (in particular Li-Jen and James See) and fellow student associates, past and present. Too many great faculty to name (special thanks to Emily Dalton for the semesterly coffee chats!). All the other people in the Yale-NUS community who supported me in big and small ways, and who made these four years so special—especially Joanna, for journeying with me through the better part of my time in college, and AD May-yi, for facilitating that.
- Ashy, Charlie & Gingy, Frisky, Gohan, Isabel, Kelly, Kimchi, Pedro, Plum, Putu, Sniffers, Suki, Wallace, for essential animal therapy—and their humans (for those who have them), for sharing them. (Also the neighbor's cat from Budapest—I miss you.)
- Valencia Jesudoss, for the lifelong gift of a love of reading. Timothy Ong, for being my first mathematical mentor till A Levels, cat pictures, and the mechanical keyboard(s) on which most of this thesis was composed.
- Sam Carter for the joys of my new favorite LaTeX package, which I discovered while trying to learn Ti*k*Z to draw graphs.

YALE-NUS COLLEGE

Abstract

B.Sc (Hons)

Identifying Cayley Graphs Among Vertex-Transitive Graphs of Prime Power Order

by Michelle ONG

A Cayley graph is a graph associated with a group and an inverse-closed subset of its nonidentity elements. A vertex-transitive graph is a graph whose automorphism group acts transitively on its vertex set. Any Cayley graph is vertex-transitive, but identifying non-Cayley vertex-transitive graphs is an ongoing subject of investigation. We review the methods used to answer a special case of this problem in the literature, when the graph has a prime power number p^n of vertices. We also present and prove new results related to the problem of identifying the core (minimal homomorphic image) of cubelike graphs, which are the Cayley graphs of elementary abelian groups $\mathbb{Z}_2^n$: we examine instead the Cayley graphs of $\mathbb{Z}_p^n$ for odd prime p.

Contents

List of Figures

Notation

Graphs

$V(\Gamma)$	vertex set of Γ
$E(\Gamma)$	edge set of the undirected graph Γ
$A(\Gamma)$	arc set of the directed graph Γ
$x \sim y$	x is adjacent to y
$N(x)$	neighborhood of x
$\deg(x)$	degree of x
$\deg(\Gamma)$	common degree of regular graph Γ
$\overline{\Gamma}$	complement of Γ
K_n	complete graph on n vertices
$K_{m,n}$	complete bipartite graph on $m + n$ vertices
C_n	cycle graph on n vertices
$\Sigma \leqslant \Gamma$	Σ is a subgraph of Γ
$\Gamma[S]$	subgraph induced by $S \subseteq V(\Gamma)$ in Γ
$\Gamma[\Sigma]$	lexicographic product of Γ and Σ
$\Gamma_{\mathcal{B}}$	quotient graph of Γ with respect to $\mathcal{B}$
$\omega(\Gamma)$	clique number of Γ
$\alpha(\Gamma)$	independence number of Γ
$\chi(\Gamma)$	chromatic number of Γ
$\Gamma \to \Sigma$	Γ has a homomorphism to Σ
$\Gamma \leftrightarrow \Sigma$	Γ is homomorphically equivalent to Σ
$\Gamma \cong \Sigma$	Γ is isomorphic to Σ
$\Gamma^{\bullet}$	core of Γ
$\mathrm{Aut}(\Gamma)$	automorphism group of Γ
$\mathrm{Cay}(G, S)$	Cayley graph of group G with connection set S

Groups

1	identity element or trivial subgroup
$g^{\pm}$	g, g^{-1}
$\lvert g\rvert$	order of g
$H \leqslant G$	H is a subgroup of G
$N \trianglelefteqslant G$	N is a normal subgroup of G
G/N	quotient group of G by N
Hg (resp. gH)	right (resp. left) coset of H
$[G : H]$	set of right cosets of H in G
$\lvert G : H\rvert$	index of H in G
$G \cong H$	G is isomorphic to H
$\langle S\rangle$	group generated by S
$Z(G)$	center of G
$\mathrm{Sym}(\Omega)$	symmetric group on Ω
S_n	the symmetric group $\mathrm{Sym}(\{1, 2, \ldots, n\})$
KH	the set $\{kh \mid k \in K, h \in H\}$
$K \times H$	direct product of K and H
G^n	n-fold direct product of G
$K \rtimes H$	semidirect product of K by H
$K \wr H$	(standard) wreath product
$\mathbb{Z}_n$	additive cyclic group with n elements
$\Phi(G)$	Frattini subgroup of G
$\mathrm{Core}_G(H)$	(normal) core of H in G
$\mathbb{F}_q$	finite field with q elements

Group actions

Let $g \in G$, $x \in \Omega \supseteq \Delta$. G acts on Ω.

x^g	image of point x under action of g
Δ^g	set of images of elements of Δ under action of g
x^G	orbit of x
G_x	point stabilizer of x in G
$G_{(\Delta)}$	pointwise stabilizer of Δ in G
$G_{\{\Delta\}}$	setwise stabilizer of Δ in G
$g/\mathcal{B}$	induced action of g on block system $\mathcal{B}$
$G/\mathcal{B}$	image of induced action
$G_{(\mathcal{B})}$	kernel of induced action
$\mathcal{C}/\mathcal{B}$	block system of $G/\mathcal{B}$ induced by block system $\mathcal{C}$

If Δ is an orbit of G:

g^{Δ}	restriction of action of g to Δ
G^{Δ}	transitive constituent of G on Δ

Chapter 1

Introduction

Graphs and groups are two mathematical objects that have been studied since the 18th century. Graphs can be used to model networks and are crucial in computer science. Groups, while seemingly more abstract, encode symmetries of objects and appear in music, cryptography, and physics, besides their fundamental importance in mathematics as a whole. Often in mathematics, using the tools of one area to study another can be quite productive. We will see two main ways of linking these objects.

First, we start with a graph. The symmetries of a graph that ensure adjacent vertices stay adjacent form a group, called its *automorphism group*. In many graphs, there is no way to relabel the vertices without changing the adjacency.[1] However, some graphs can be relabelled in many different ways while preserving adjacency, and these graphs have many interesting properties. While graphs can be classified into different families based on their automorphism groups, in this thesis we focus on the *vertex-transitive* graphs, for which any vertex can be sent to any other vertex by an adjacency-preserving symmetry.

[1] In fact, "almost all" finite graphs fall into this category of *asymmetric* graphs, with trivial automorphism group [5].

If we start with a group instead, we can construct a *Cayley graph* for which the vertices are all group elements, and the edges are defined by choosing a subset of the group. Cayley graphs are highly symmetric; they are a subset of vertex-transitive graphs. The converse does not hold, as there are non-Cayley vertex-transitive graphs. A natural question is: when is a vertex-transitive graph Cayley? We will study this for a specific family of graphs. But even in this case, there is no definite answer for larger graphs when there are too many edges. This motivates us to investigate properties of certain Cayley graphs in this family.

1.1 Thesis structure and contributions

Chapter 2 will present more formally the necessary background on graphs and groups. Then, chapter 3 will consider when a vertex-transitive graph of order p^k is Cayley, beginning with small powers (for which the answer is "always"), and then considering how to deal with higher powers of p. Chapter 4 considers particular Cayley graphs and whether they are closed under the operation of "taking the core", using the property of this family that they can be viewed as finite geometries. Finally, chapter 5 provides a summary and highlights further work to be done.

To our knowledge, the results and proofs in chapter 3 have not been collected in a single document before. Therefore this review is a new contribution of this thesis, rigorous yet accessible to the reader with a first course in group theory. All results and proofs in chapter 4, except section 4.1, propositions 14 and 15, and lemma 20, are original to this thesis and result from collaboration between the author and Guang Rao. The code in the appendix was written entirely by the author.

Chapter 2

Background

Section 2.1 introduces basic definitions in graph theory and graph homomorphisms, following [8] and [10]. Then, section 2.2 presents relevant material on groups, and section 2.3 shows how groups and graphs can be related in multiple ways. Some examples of graphs, in appendix B, are linked when introduced.

2.1 Graphs

graph
order
size
digraph
adjacent
neighbor
neighborhood
incident
degree

A *graph* Γ consists of a vertex set $V(\Gamma)$ and an edge set $E(\Gamma)$. The *order* of Γ is $|V(\Gamma)|$, and the *size* of Γ is $|E(\Gamma)|$. In this thesis, we will mostly consider only simple graphs (that is, undirected without loops or multiple edges), for which $E(\Gamma)$ consists of unordered pairs of distinct vertices of Γ. However, section 3.2 will use the more general setting of a *digraph* (directed graph), where $E(\Gamma)$ is replaced by the set of arcs $A(\Gamma)$, in which the pairs are ordered. If $\{x, y\} \in E(\Gamma)$, we say x is *adjacent* to y, and denote this $x \sim y$. In this case, we also call x a *neighbor* of y (x is in the *neighborhood* of y, $N(y)$), and say that x and y are *incident* to the same edge. (We also say an edge $\{x, y\}$ is incident to the vertices x and y.) The *degree*

(k-)regular
handshaking lemma
connected
cycle
complete graph
complement
empty graph

of x is $|N(x)|$, denoted $\deg(x)$. Γ is said to be *(k-)regular* if $|N(x)| = k$ for all $x \in \Gamma$. In this case, k is called the degree of Γ and denoted $\deg(\Gamma)$. The *handshaking lemma*, which is easily proved by double counting incident pairs of vertices and edges, states that $\sum_{v \in V(\Gamma)} \deg(v) = 2|E(\Gamma)|$. A graph is *connected* if there exists a path between any two vertices. The *cycle* on k vertices is a connected 2-regular graph, denoted C_k (fig. B.1). The *complete graph* on n vertices K_n is the graph where every vertex is adjacent to every other vertex (fig. B.2). K_n is $(n-1)$-regular. The *complement* of a graph Γ is denoted by $\overline{\Gamma}$, and is defined by $V(\overline{\Gamma}) = V(\Gamma)$ and $(x, y) \in E(\overline{\Gamma})$ if and only if $(x, y) \notin E(\Gamma)$. For example, $\overline{K_n}$ is the *empty graph* on n vertices (with no edges).

subgraph
induced subgraph
clique
clique number
independent set
independence number
complete bipartite graph

A *subgraph* of Γ is a graph Σ such that $V(\Sigma) \subseteq V(\Gamma)$ and $E(\Sigma) \subseteq E(\Gamma)$. We denote this $\Sigma \leqslant \Gamma$. Σ is an *induced subgraph* of Γ if for any $x, y \in V(\Sigma)$, $x \sim y$ in Σ if and only if $x \sim y$ in Γ. We may denote the induced subgraph by $\Gamma[S]$ where $S = V(\Sigma) \subseteq V(\Gamma)$. If $\Sigma \leqslant \Gamma$ and Σ is a complete graph, then Σ is called a *clique* (and Σ is necessarily an induced subgraph). The *clique number* of Γ is the order of a largest clique of Γ, denoted $\omega(\Gamma)$. An *independent set* of Γ is a subset of $V(\Gamma)$ which induces an empty graph, i.e. a set of pairwise nonadjacent vertices. The order of a largest independent set is called the *independence number* and denoted $\alpha(\Gamma)$. The *complete bipartite graph* $K_{m,n}$ is the graph with exactly two independent sets with m and n vertices respectively, and every vertex in one independent set is adjacent to every vertex in the other (fig. B.3).

2.1.1 Colorings and graph homomorphisms

vertex coloring

A (proper) *vertex coloring* of Γ is a map from $V(\Gamma)$ into a finite set of colors such that no two adjacent vertices are assigned the same color. We often use $\{1, 2, \ldots, n\}$ as the set of colors. Γ is said to be *properly k-colorable* if Γ can be properly colored using k colors, and the least such k is known as the *chromatic number* of Γ, denoted $\chi(\Gamma)$.

properly k-colorable

chromatic number

isomorphic

Two graphs Γ and Σ are said to be *isomorphic* if there is a bijection $\varphi : V(\Gamma) \to V(\Sigma)$ such that $x \sim y$ if and only if $\varphi(x) \sim \varphi(y)$. In this case, we write $\Gamma \cong \Sigma$, and call φ an *isomorphism*. An isomorphism from a graph to itself is called an *automorphism*. These terms may be familiar from studying other (algebraic) structures; here the essential property being preserved is adjacency.

isomorphism

automorphism

A map $f : V(\Gamma) \to V(\Sigma)$ between two graphs Γ and Σ is a *(graph) homomorphism* if $x \sim y$ in Γ implies $f(x) \sim f(y)$ in Σ. For graphs without loops, this implies that $f(x) \neq f(y)$ whenever $x \sim y$. We denote this by $\Gamma \to \Sigma$. The arrow can be read as "has a homomorphism to". For $x \in V(\Sigma)$, the preimage $f^{-1}(x)$ is called a *fiber* of f. If $\Gamma \leqslant \Sigma$, then the homomorphism which maps each vertex of Γ to itself in Σ is called the *inclusion homomorphism*. Examples of homomorphisms include all graph isomorphisms (in particular automorphisms) and all vertex colorings. An *endomorphism* is a homomorphism from a graph to itself.

(graph) homomorphism

fiber

inclusion homomorphism

endomorphism

retraction

A *retraction* is a homomorphism f from a graph Γ to a subgraph $\Sigma \leqslant \Gamma$ such that the restriction of f to $V(\Sigma)$ is the identity map. If a retraction from Γ to Σ exists, then Σ is called a *retract* of Γ. An alternative, equivalent definition is as follows: Σ is a *retract* of Γ if there are homomorphisms $f : \Gamma \to \Sigma$ and $g : \Sigma \to \Gamma$ such that $f \circ g = id_\Sigma$. Then f is called a *retraction* and g is called a *co-retraction*. If Γ has a clique of order $\chi(\Gamma)$, then any $\chi(\Gamma)$-coloring of Γ determines a retraction onto the clique.

retract

co-retraction

2.1.2 Cores and the homomorphic equivalence relation

core

A graph Γ is called a *core* if any homomorphism from Γ to itself is a bijection. The complete graphs K_n and the Petersen graph are examples of cores (fig. B.4; although the Petersen graph is 3-colorable, K_3 cannot be the core since it is not a subgraph). We also call a subgraph $\Sigma \leqslant \Gamma$ a *core of* Γ if Σ is a core and $\Gamma \to \Sigma$. Any core of a graph Γ is a retract of Γ. It can be shown that every graph has a core, and that all the cores of a graph are isomorphic, which justifies talking about "the" core of a graph. The core of Γ is denoted by $\Gamma^\bullet$. Note that $\Gamma^\bullet$ is an induced subgraph of Γ. A graph is called *core-complete* if it is a core or its core is complete.

core of Γ

core-complete

We can use homomorphisms to define a relation on graphs. If $\Gamma \to \Sigma$ and $\Sigma \to \Gamma$, the graphs are said to be *homomorphically equivalent*, and we write $\Gamma \leftrightarrow \Sigma$. For example, if Γ is a retract of Σ, then it follows immediately from the definition that $\Gamma \leftrightarrow \Sigma$. In particular, $\Gamma \leftrightarrow \Sigma$ implies that $\Gamma^\bullet \leftrightarrow \Sigma^\bullet$. Clearly $\leftrightarrow$ is an equivalence relation, justifying the name. As $\Gamma^\bullet$ is the minimal (smallest order) homomorphic image of Γ, and since any subgraph has a homomorphism to the graph, it follows that $\Gamma^\bullet$ is the smallest graph which is homomorphically equivalent to Γ. More strongly, it can be shown that up to isomorphism, $\Gamma^\bullet$ is the unique graph of smallest order in the equivalence class of Γ.

homomorphically equivalent

A graph Σ is properly r-colorable if and only if there is a homomorphism from Σ to K_r (and $\chi(\Sigma)$ is the least such r). Therefore, if there is a homomorphism from Γ to Σ, we have $\Gamma \to \Sigma \to K_r$, so that $\chi(\Gamma) \leqslant \chi(\Sigma)$. In particular, if $\Gamma \leftrightarrow \Sigma$, then $\chi(\Gamma) = \chi(\Sigma)$. Hence for any graph Γ, we have $\chi(\Gamma) = \chi(\Gamma^\bullet)$.

2.2 Permutation groups

We will establish the group-theoretic notation and introduce some definitions and results in this section. We assume the reader is familiar with the following concepts from a first course on group theory: group, abelian group, subgroup, coset, group action, group homomorphism, Cayley's theorem, Cauchy's theorem, Sylow p-subgroup, the Sylow theorems, isomorphism theorems for groups. As a result of Cayley's theorem, we will freely use the language of abstract or permutation groups as context demands. We use multiplicative notation throughout, and denote by 1 both the identity element and the trivial subgroup with one element. For permutation groups, [3] is a good reference and the source for most of this section.

Let Ω be a nonempty set. A bijection of Ω to itself is called a permutation of Ω. The set of all permutations of Ω forms a group under composition, called the *symmetric group* on Ω, and denoted $\mathrm{Sym}(\Omega)$. A *permutation group* is a subgroup of a symmetric group. If $\Omega = \{1, 2, \ldots, n\}$ for $n \in \mathbb{N}$, the group is denoted by S_n. If Ω is finite, then $|\,\mathrm{Sym}(\Omega)| = |\Omega|!$.

symmetric group

permutation group

Consider the set of all automorphisms of a graph Γ, which can be viewed as permutations of $V(\Gamma)$ that preserve edges. The identity permutation is an automorphism, and the inverse of any automorphism or the composition of two automorphisms is again an automorphism. So the set of all automorphisms of Γ form its *automorphism group*, denoted $\mathrm{Aut}(\Gamma)$. Note that $\mathrm{Aut}(\Gamma) \leqslant \mathrm{Sym}(V(\Gamma))$.

automorphism group

2.2.1 Permutation group actions

Let G be a group acting on a set Ω. We will denote the image of the action of $g \in G$ on $x \in \Omega$ by x^g. If G is a permutation group on Ω, then G naturally acts on Ω where x^g is the image of $x \in \Omega$ under the permutation $g \in G$. The *degree* of an action is $|\Omega|$. The *orbit* of $x \in \Omega$ is defined as $x^G := \{x^g \mid g \in G\}$, the set of images of x under the action. The orbits of any action partition the set. The *(point) stabilizer* of $x \in \Omega$ is defined by $G_x := \{g \in G \mid x^g = x\}$, i.e. the set of group elements which fix x. It can be shown that $G_x \leqslant G$, and that for $x, y \in \Omega$ where $x = y^g$, $G_x = x^{-1}G_y x$. The *orbit-stabilizer lemma* states that $|x^G| = |G : G_x|$, the index of G_x in G. In particular, if G is finite, then $|G| = |x^G||G_x|$.

degree

orbit

(point) stabilizer

orbit-stabilizer lemma

The action of G on Ω is said to be *transitive* if for any $x \in \Omega$, $x^G = \Omega$, or in other words it has only one orbit. Equivalently, the action is transitive if for any $x, y \in \Omega$, there exists $g \in G$ such that $x^g = y$. The action is called *faithful* if the kernel of its permutation representation ρ is trivial, $\ker \rho = 1$. The action is called *semiregular* or *(fixed point) free* if the stabilizer $G_x = 1$ for any $x \in \Omega$. If an action is both transitive and semiregular, then it is called *regular*. There are several equivalent definitions of a regular group, gathered here:

transitive

faithful

semiregular

(fixed point) free

regular

Lemma 1. *Let $G \leqslant \mathrm{Sym}(\Omega)$ be transitive on finite Ω. The following are equivalent:*

1. *the action is semiregular,*
2. $|G| = |\Omega|$,
3. *for any $x, y \in \Omega$, there is a unique element $g \in G$ such that $x^g = y$.*

Proof. ($1 \Leftrightarrow 2$) By the orbit-stabilizer lemma, $|G| = |\Omega||G_x|$ if and only if $|G_x| = 1$, and the stabilizer subgroup always contains the identity.

($1 \Rightarrow 3$) By transitivity, such an element exists. Let $g, h \in G$ such that $x^g = y$ and $x^h = y$. As $x^g = x^h$, we have $(x^g)^{h^{-1}} = x$, i.e. gh^{-1} is the unique element in G_x so $gh^{-1} = 1$, hence $g = h$.

($3 \Rightarrow 1$) Let $g \in G$ such that $x^g = x$. This must be the identity, and no other element stabilizes x by uniqueness. $\square$

The following lemma has the important consequence that a transitive abelian group is regular, as the center of an abelian group is itself.

Lemma 2. *The center $Z(G)$ of a transitive group G is semiregular.*

Proof. Let $h \in Z(G)$ and $x \in \Omega$ such that $x^h = x$. As G is transitive, for any $y \in \Omega$ there exists $g \in G$ such that $x^g = y$. So $y = x^g = (x^h)^g = x^{hg} = x^{gh} = (x^g)^h = y^h$. That is, h is the identity, and so $Z(G)_x = 1$. $\square$

Let G be a group acting transitively on Ω. A nonempty subset $\Delta \subseteq \Omega$ is a *block* for G if for any $g \in G$ either $\{\delta^g \mid \delta \in \Delta\} =: \Delta^g = \Delta$, or $\Delta^g \cap \Delta = \emptyset$. Any transitive group on Ω has the singletons and Ω as blocks; these are called the *trivial blocks*. The nonempty intersection of blocks for G is again a block for G.

block

trivial blocks

Suppose G acts transitively on Ω and Δ is a block for G. The *system of blocks* containing Δ is $\Sigma := \{\Delta^g \mid g \in G\}$. The elements of Σ partition Ω and each element of Σ is a block for G. It can be seen that G acts transitively on Σ. G is called *primitive* if G has no nontrivial blocks on Ω, and *imprimitive* otherwise.

system of blocks

primitive

imprimitive

Let G act on $\Omega \supseteq \Delta$. The *pointwise stabilizer* of Δ in G is $G_{(\Delta)} := \{g \in G \mid \delta^g = \delta \text{ for all } \delta \in \Delta\}$, the elements which fix Δ pointwise. The *setwise stabilizer* of Δ in G is $G_{\{\Delta\}} := \{g \in G \mid \Delta^g = \Delta\}$, the elements which fix Δ setwise. Note that $G_{(\Delta)} \leqslant G_{\{\Delta\}} \leqslant G$, and that for any $x \in \Omega$, we have

pointwise stabilizer

setwise stabilizer

$G_{\{x\}} = G_{(\{x\})} = G_x$. If G is transitive on Ω and Δ is a block for G, then $G_{\{\Delta\}}$ is transitive on Δ.

(G)-invariant

Let G act on Ω. A subset $\Delta \subseteq \Omega$ is *(G)-invariant* if $\Delta^g = \Delta$ for all $g \in G$. Δ is G-invariant if and only if Δ is a union of orbits of G. When Δ is G-invariant, the restriction to Δ of the action of G on Ω is an action of G on Δ. Two permutation groups $G \leqslant \mathrm{Sym}(\Omega)$ and $H \leqslant \mathrm{Sym}(\Omega')$ are called *permutation isomorphic* if there exists a group isomorphism $\psi : G \to H$ and a bijection $\lambda : \Omega \to \Omega'$ such that $\lambda(x^g) = \lambda(x)^{\psi(g)}$ for all $x \in \Omega$ and $g \in G$. If $\Omega = \Omega'$, then G and H are permutation isomorphic if and only if they are conjugate in $\mathrm{Sym}(\Omega)$.

permutation isomorphic

The following result will be useful when investigating the automorphism groups of graphs of prime power order.

Proposition 3. *Let G act transitively on Ω where $|\Omega| = p^n$. Let P be a Sylow p-subgroup of G. Then P acts transitively on Ω.*

Proof. Let $x \in \Omega$ and $|P| = p^m$. By the orbit-stabilizer lemma, $|G_x| = |G|/|x^G| = p^{m-n}k$ for some k coprime to p. As the stabilizer P_x is a subgroup of P, $|P_x|$ divides p^m, and as $P_x \leqslant G_x$, we have $|P_x| \leqslant p^{m-n}k$. So $|P_x| \leqslant p^{m-n}$ which, using the orbit-stabilizer lemma again, implies

$$|x^P| \geqslant \frac{|P|}{p^{m-n}} = p^n = |\Omega|.$$

Hence $|x^P| = |\Omega|$. □

normal series

A *normal series* of a group G is a sequence of subgroups $1 = A_0 \trianglelefteq A_1 \trianglelefteq \cdots \trianglelefteq A_n = G$, with each A_i normal not only in A_{i+1} but also in G. A consequence of the previous proposition is that for a group P of prime power order, there is a normal series $1 = P_0 \leqslant P_1 \leqslant \cdots \leqslant P_n = P$ where $|P_i : P_{i-1}| = p$ for all i.

2.2.2 Semidirect and wreath products of groups

The definitions in this subsection are important to understand the proofs in chapter 3, but less so in chapter 4.

Let H and K be groups with H acting on K so that for each $x \in H$ the map $u \mapsto u^x$ is an automorphism of K, i.e. the action of H preserves the group structure of K. Define $G := \{(u, x) \mid u \in K, x \in H\}$ and an operation on G by $(u, x) \cdot (v, y) := (uv^{x^{-1}}, xy)$. Then $(G, \cdot)$ is a group with inverse element $(u, x)^{-1} = ((u^x)^{-1}, x^{-1})$. G is called the *semidirect product* of K by H, denoted by $K \rtimes H$. Semidirect products generalize direct products: choosing the identity automorphism gives the direct product.

semidirect product

Let Δ be a finite nonempty set of size m and K a group, and denote the set of all functions from Δ into K by F. Defining an operation by pointwise multiplication, $(fg)(\delta) := f(\delta)g(\delta)$ for $f, g \in F$ and $\delta \in \Delta$, turns F into a group, which is isomorphic to K^m. Now let a group H act on Δ. The *wreath product* of K by H with respect to this action of H is defined as $F \rtimes H$, where H acts on F by $f^x(\delta) := f(\delta^{x^{-1}})$ for $f \in F, \delta \in \Delta, x \in H$. The wreath product is denoted $K \wr_\Delta H$. The subgroup $B := \{(f, 1) \mid f \in F\} \cong F \cong K^m$ is called the *base group* of the wreath product. The action of H on B corresponds to permuting the components: $(u_1, \ldots, u_m)^x = (u_{1'}, \ldots, u_{m'})$ where x is the permutation that sends i to i'. Clearly, $|K \wr_\Delta H| = |K|^m |H|$. If $\Delta = H$ so that H acts regularly on itself by left multiplication, this is called the *standard wreath product* (sometimes also simply the wreath product)

wreath product

base group

standard wreath product

and we denote this by $K \wr H$.

2.3 Cayley graphs and vertex-transitive graphs

We now introduce the main objects studied in this thesis.

Cayley graph

connection set

Let G be a group and $S \subseteq G$ be closed under taking inverses and not containing the identity. A *Cayley graph* $\Gamma = \mathrm{Cay}(G, S)$ is the graph defined by setting $V(\Gamma) := G$ and $E(\Gamma) := \{\{x, y\} \mid xy^{-1} \in S\}$. In other words, $x \sim y$ if and only if $xy^{-1} \in S$. The set S is called the *connection set* of the Cayley graph. The condition that S be inverse-closed is to ensure that adjacency is symmetric, so that the graph is undirected. However, the more general *Cayley digraph* relaxes this condition. Also, the identity element is always excluded from S for the graph to be simple (without loops). This causes no loss of generality, as including the identity element adds exactly one loop to every vertex. A Cayley graph is $|S|$-regular. Note that a Cayley graph is connected if and only if S generates G. If $S = \emptyset$, then Γ is the empty graph on $|G|$ vertices. We will omit this trivial case in what follows by assuming that S is nonempty.

Cayley digraph

vertex-transitive

A graph Γ is called *vertex-transitive* if its automorphism group $\mathrm{Aut}(\Gamma)$ acts transitively on $V(\Gamma)$. Note that a vertex-transitive graph is regular (i.e., every vertex has the same degree). All Cayley graphs are vertex-transitive (see the proof of theorem 5 below), but there are vertex-transitive graphs which are not Cayley, such as the Petersen graph. Because Cayley graphs are vertex-transitive, we will assume in many proofs in this thesis that a certain subgraph contains the identity without loss of generality. We may wonder if there is anything inherently interesting about Cayley graphs as graphs, rather than just being nice representations of groups. The following theorem tells us there is:

Theorem 4. *Any vertex-transitive graph* Γ *is a retract of some Cayley graph.*

Proof. Let $S := \{\sigma \in \mathrm{Aut}(\Gamma) \mid (u, \sigma(u)) \in E(\Gamma)\}$ for some fixed $u \in V(\Gamma)$. S is the union of left cosets of the stabilizer $\mathrm{Aut}(\Gamma)_u$. As S is inverse-closed and does not contain the identity, we may define $\mathrm{Cay}(\mathrm{Aut}(\Gamma), S)$.

We show that $\mathrm{Cay}(\mathrm{Aut}(\Gamma), S) \leftrightarrow \Gamma$. Let $\rho : \mathrm{Cay}(\mathrm{Aut}(\Gamma), S) \to \Gamma$ defined by $\varphi \mapsto \varphi(u)$ and $\gamma : \Gamma \to \mathrm{Cay}(\mathrm{Aut}(\Gamma), S)$ defined by selecting $\gamma(v) = \varphi_v$ such that $\varphi_v(u) = v$ for all $v \in V(\Gamma)$. Both ρ and γ are homomorphisms, as (by definition) $\varphi_1 \sim \varphi_2$ if and only if $\varphi_1(u) \sim \varphi_2(u)$ in the original graph Γ, for $\varphi_1, \varphi_2 \in \mathrm{Aut}(\Gamma)$. So $\mathrm{Cay}(\mathrm{Aut}(\Gamma), S)$ is homomorphically equivalent to Γ.

Note that ρ is a retraction as for any $u \in V(\Gamma)$, $\rho \circ \gamma(u) = u$. □

So Cayley graphs represent all equivalence classes of vertex-transitive graphs under the homomorphic equivalence relation. The next theorem is the basis of essentially all work done on establishing whether specific graphs are Cayley, and in particular whether a given vertex-transitive graph is Cayley [1].

Theorem 5 (Sabidussi)**.** *A graph* Γ *is a Cayley graph if and only if* $\mathrm{Aut}(\Gamma)$ *contains a regular subgroup.*

Proof. First assume $\Gamma = \mathrm{Cay}(G, S)$. Consider the bijections $T_a : \Gamma \to \Gamma$ defined by $T_a(x) = ax$, which are automorphisms of Γ. The set $H := \{T_a \mid a \in G\}$ is a group, hence a subgroup of $\mathrm{Aut}(\Gamma)$. Furthermore, H is transitive ($T_{gh^{-1}}$ sends g to h) and semiregular (no nonidentity element fixes a given element by left multiplication), so H is regular.

For the converse, let u, v be vertices of Γ. Then there is a unique element $g_v \in G$ such that $u^{g_v} = v$. Define $S := \{g_v \mid v \sim u\}$. Now for vertices x, y of Γ, since $g_x \in \mathrm{Aut}(\Gamma)$, we have $x \sim y$ if and only if $u = x^{g_x^{-1}} \sim y^{g_x^{-1}} = u^{g_y g_x^{-1}}$. Then identifying x with g_x gives $\Gamma = \mathrm{Cay}(G, S)$. Since Γ is undirected and has no loops, S is an inversed-closed subset of nonidentity elements of G. □

We will see this theorem used many times over in chapter 3. The next results on cores of vertex-transitive graphs will be useful in chapter 4:

Theorem 6 (Welzl). *If a graph Γ is vertex-transitive, then $\Gamma^\bullet$ is vertex-transitive.*

Proof. Let $f : \Gamma \to \Gamma^\bullet$ be a retraction with co-retraction g. For any $u, v \in V(\Gamma^\bullet)$, there is an automorphism φ of Γ mapping $g(u)$ to $g(v)$. Then $f \circ \varphi \circ g(u) = f \circ g(v) = v$, since $f \circ g$ is the identity map on $\Gamma^\bullet$. The map $f \circ \varphi \circ g$ is an endomorphism of $\Gamma^\bullet$, hence an automorphism. Thus $\mathrm{Aut}(\Gamma^\bullet)$ acts transitively on $\Gamma^\bullet$. □

Theorem 7. *If a graph Γ is vertex-transitive, then $|V(\Gamma^\bullet)|$ divides $|V(\Gamma)|$.*

Proof. Consider a homomorphism $f : \Gamma \to \Gamma^\bullet = \Sigma$. Let $g \in \mathrm{Aut}(\Gamma)$. Then $f(\Sigma^g) = \Sigma$, so in every fiber of f there is one vertex of Σ^g. Let $v \in V(\Gamma)$. By vertex-transitivity, for any v we have the same number of automorphisms such that $v \in \Sigma^g$, call it n. Hence $n \cdot |f^{-1}(v)| = |\mathrm{Aut}(\Gamma)|$, and n is independent of choice of v. So any fiber $f^{-1}(v)$ has size $|\mathrm{Aut}(\Gamma)|/n$. As fibers form a partition of the domain, the result follows. □

2.3.1 Cubelike graphs

finite elementary abelian group

A *finite elementary abelian group* is a group of the form $\mathbb{Z}_p^n$, the n-fold direct product of the cyclic group of order p, where p is a prime number. Every nonidentity element of $\mathbb{Z}_p^n$ has order p. A *p-group* is a group in which the order of every element is a power of some prime p. Clearly, $\mathbb{Z}_p^n$ is a p-group. $\mathbb{Z}_p^n$ is a vector space over the finite field of p elements $\mathbb{F}_p$. This view of the group will be especially useful in the proofs of chapter 4, in light of section 4.1. A minimal generating set of $\mathbb{Z}_p^n$ has n elements, and one example of a generating set is the set of standard basis vectors with entries in $\mathbb{F}_p$. So if $\mathrm{Cay}(\mathbb{Z}_p^n, S)$ is connected, then $|S| \geqslant n$.

p-group

A *cubelike graph* (sometimes called a binary Cayley graph) is a graph $\mathrm{Cay}(\mathbb{Z}_2^n, S)$ for some S. For example, the n-dimensional hypercube graph Q_n can be viewed as a cubelike graph with S taken to be the standard basis vectors (fig. B.5). Cubelike graphs have been conjectured to have cubelike cores in [13], and the authors show that the conjecture holds for small cubelike graphs (up to order 32). The same paper concludes that even if the conjecture turns out to be untrue, the cores of cubelike graphs have many features that make them very similar to cubelike graphs, gathered in their Theorem 9.1. However, the techniques used in that paper to rule out all non-cubelike vertex-transitive graphs on up to 32 vertices would not be helpful in general, as even computational methods cannot handle the very large number of groups and graphs to consider without a stronger theoretical framework.

cubelike graph

In chapter 4 we will consider the same conjecture, but study $\mathrm{Cay}(\mathbb{Z}_p^n, S)$ for $p \geqslant 3$ instead of $p = 2$. We call this a *generalized cubelike graph* and ask whether this family is closed under the operation of "taking the core".

generalized cubelike graph

Chapter 3

Recognizing Cayley graphs from vertex-transitive graphs

This chapter aims to provide a survey of the methods used to determine whether a given vertex-transitive graph is a Cayley graph. As mentioned in chapter 2, theorem 5 is crucial to this question. The O'Nan-Scott theorem completely classifies the finite primitive (permutation) groups, so when $\mathrm{Aut}(\Gamma)$ is primitive, it is relatively straightforward to know whether or not $\mathrm{Aut}(\Gamma)$ contains a regular subgroup. However, when $\mathrm{Aut}(\Gamma)$ is imprimitive, there is not yet a systematic way to do so. Alspach in [1] summarized the work done up to the time of publication in 2004.

We focus only on those graphs of order p^n for prime p, as these are most relevant to the cubelike problem. For $n \in \{1, 2, 3\}$, a vertex-transitive graph is always a Cayley graph. This does not hold for $n \geqslant 4$, as a construction by McKay and Praeger in [15] shows. However, Feng in [6] showed that for odd prime p and any $n \in \mathbb{N}$, if the common degree of the vertices is less than $2p + 2$, then the graph is Cayley.

3.1 Graphs of order p and p^2

Consider a vertex-transitive graph of prime order p. Together with theorem 5, the following shows that such a graph is always Cayley:

Proposition 8. *If $G \leqslant \mathrm{Sym}(\Omega)$ is a transitive group of prime degree p, then G contains a p-cycle which generates a regular subgroup of G.*

Proof. Let $x \in \Omega$. As G is transitive, $|x^G| = |\Omega| = p$ divides $|G|$, so by Cauchy's theorem there exists $g \in G$ with $|g| = p$. Then the cycle decomposition of g is a product of disjoint p-cycles, but as $G \leqslant S_p$, no two p-cycles are disjoint. So g is itself a p-cycle. Then $\langle g \rangle$ is clearly transitive and abelian, hence regular. □

A classic paper [14] by Marušič first showed that any vertex-transitive graph of order p^2 or p^3 is Cayley. For a proof of the p^2 case following [21], we introduce two key definitions.

Frattini subgroup

The *Frattini subgroup* of G, denoted $\Phi(G)$, is defined as the intersection of all maximal subgroups of G. $\Phi(G)$ is the set of all non-generators of G, i.e., all the elements g for which whenever $\langle X, g \rangle = G$ then $\langle X \rangle = G$. We always have $\Phi(G) \trianglelefteq G$. If P is a finite p-group, then $P/\Phi(P) \cong \mathbb{Z}_p^n$, where k is the size of a minimal generating set for P [12].

core

The *core* of a subgroup (unrelated to the core of a graph) is defined as follows. Let H be a subgroup of G. Then G acts on the set of right cosets $[G : H]$ by right multiplication. This induces a permutation representation $\varphi : G \to \mathrm{Sym}([G : H])$. Then $\mathrm{Core}_G(H) := \ker \varphi = \bigcap_{g \in G} g^{-1}Hg$. Note that $\mathrm{Core}_G(H) \trianglelefteq G$. A subgroup $H \leqslant G$ is called *core-free* if $\mathrm{Core}_G(H)$ is the trivial subgroup. H is core-free if and only if the action φ on $[G : H]$ above is faithful.

core-free

Theorem 9. *A transitive group $G \leqslant \mathrm{Sym}(\Omega)$ of degree p^2, where p is prime, has a regular subgroup.*

Proof. Let P be a minimal transitive subgroup of G. Then since taking a Sylow p-subgroup of P also gives a transitive subgroup, P must be itself a p-group. Further, every maximal subgroup M of P is intransitive by choice of P. For any $\alpha \in \Omega$, we have $|P_\alpha| = |P|/p^2$ by the orbit-stabilizer lemma. Now $|M| = |M_\alpha||\alpha^M| \leqslant |M_\alpha| \cdot p$, since M is intransitive (so the orbit cannot have size p^2). Then

$$\frac{|P|}{p^2} = |P_\alpha| \geqslant |M_\alpha| \geqslant \frac{|M|}{p} = \frac{|P|}{p^2},$$

so we have equality everywhere, and as $M_\alpha \leqslant P_\alpha$, $M_\alpha = P_\alpha$. So $P_\alpha \leqslant M$. Then since M was an arbitrary maximal subgroup, $P_\alpha \leqslant \Phi(P)$. Now $p \leqslant |P : \Phi(P)| \leqslant |P : P_\alpha| = p^2$, so there are only two possible values of $|P : \Phi(P)|$. If $|P : \Phi(P)| = p$, then P is cyclic (since $P/\Phi(P)$ is elementary abelian of order p), therefore abelian (and transitive by definition), hence regular. If instead $|P : \Phi(P)| = p^2$, then $P_\alpha = \Phi(P)$. Consider

$$\mathrm{Core}_P(P_\alpha) = \bigcap_{g \in P} P_\alpha^g = \bigcap_{g \in P} P_{\alpha^g} = \bigcap_{x \in \Omega} P_x = 1,$$

where the second equality is because all point stabilizers are conjugate to each other, and the third because P is transitive. Since P_α is core-free and $\Phi(P) \trianglelefteq P$, we have $P_\alpha = 1$. Hence $P \cong \mathbb{Z}_p^2$ is regular. □

Theorem 5 again implies any vertex-transitive graph on p^2 vertices is Cayley.

3.2 Graphs of order p^3

The following proof of the p^3 case appears in [4] in less detail, and with somewhat different notation. We remark that it is *not* true that every transitive group of degree p^3 contains a regular subgroup, which partly accounts for the much more technical and difficult proof for this case compared to the p and p^2 cases.

Let G be a permutation group with orbit Δ and $g \in G$. Then restricting the domain of g to Δ induces a permutation on Δ. The resulting permutation is denoted g^Δ. The group $G^\Delta := \{g^\Delta \mid g \in G\}$ is called the *transitive constituent* of G on Δ, and G^Δ is indeed transitive on Δ. For a transitive group $G \leqslant \mathrm{Sym}(\Omega)$, a *G-congruence* is an equivalence relation $\sim$ on Ω such that $x \sim y$ if and only if $x^g \sim y^g$ for every $g \in G$. In this case, the set of equivalence classes of $\sim$ forms a block system for G. A *normal block system* is a block system of a transitive group G that is the set of orbits of a normal subgroup of G.

transitive constituent

G-congruence

normal block system

Suppose G is a transitive permutation group with a block system $\mathcal{B}$. Then G has an *induced action* $g/\mathcal{B}$ on $\mathcal{B}$, defined for $g \in G$ by $g/\mathcal{B} : B \mapsto B'$ if and only if $B^g = B'$. Define also $G/\mathcal{B} := \{g/\mathcal{B} \mid g \in G\}$ and denote the subgroup that fixes each block of $\mathcal{B}$ setwise by $G_{(\mathcal{B})} := \{g \in G \mid g/\mathcal{B} = 1\}$ (here the "points" of the action are the blocks of $\mathcal{B}$). That is, $G_{(\mathcal{B})}$ is the kernel of the induced homomorphism $G \to \mathrm{Sym}(\mathcal{B})$, and so by the first isomorphism theorem $|G| = |G/\mathcal{B}| \cdot |G_{(\mathcal{B})}|$. If $N \trianglelefteqslant G$ and $\mathcal{B}$ is the set of orbits of N (a normal block system), then $N \leqslant G_{(\mathcal{B})}$.

induced action

Let G be transitive with block systems $\mathcal{B}$ and $\mathcal{C}$. We write $\mathcal{B} \preceq \mathcal{C}$ if every block of $\mathcal{B}$ is contained in a block of $\mathcal{C}$. In this case the set of all blocks of $\mathcal{B}$ whose union is a block $C \in \mathcal{C}$ is a block of G/C, denoted by

$C/\mathcal{B}$. The set $\mathcal{C}/\mathcal{B} := \{C/\mathcal{B} \mid C \in \mathcal{C}\}$ is a block system of $G/\mathcal{B}$, called the block system *induced by* $\mathcal{C}$.

Let G be a transitive group with a normal block system $\mathcal{B}$ with blocks of prime size p. For any $B \in \mathcal{B}$, the transitive constituent of the stabilizer $G^B_{(\mathcal{B})}$ is a transitive group on p points, so contains a p-cycle by theorem 8. Let $\sim$ be a relation on $\mathcal{B}$ defined as follows: $B \sim B'$ if and only if (for any $\gamma \in G_{(\mathcal{B})}$, γ^B is a p-cycle if and only if $\gamma^{B'}$ is also a p-cycle). Then $\sim$ is an equivalence relation, where each equivalence class consists of blocks of $\mathcal{B}$. Define $\mathcal{E} := \{\cup_{B \in C} B \mid C \text{ is an equivalence class of } \sim\}$. Also, for $g \in G_{(\mathcal{B})}$, denote by $g|_B$ the element of $S_n \geqslant G$ which permutes the points in B as g (restricted to B) does, and fixes every point not in B.

Lemma 10 ([4] Lemma 5.3.11)**.** *Let* Γ *be a digraph. Let* $G \leqslant \mathrm{Aut}(\Gamma)$ *have a normal block system* $\mathcal{B}$ *with blocks of prime size* p*. Then* G *has another block system* $\mathcal{E}$ *defined above, and* $\gamma|_E \in \mathrm{Aut}(\Gamma)$ *for any* $\gamma \in G_{(\mathcal{B})}$ *and any* $E \in \mathcal{E}$*.*

Proof. First we will show that $\sim$ is a $G/\mathcal{B}$-congruence, that is, $B \sim B'$ if and only if $B^g \sim B'^g$ for every $g \in G$. Suppose for some $g \in G$, $B \sim B'$ but $B^g \not\sim B'^g$. Then there exists $\gamma \in G_{(\mathcal{B})}$ such that γ^{B^g} is a p-cycle but $\gamma^{B'^g}$ is not a p-cycle, so has order k coprime to p. Raising γ to power k, we may assume without loss of generality that $\gamma^{B^g} = (x_0\ x_i\ \dots\ x_{p-1})$ and $\gamma^{B'^g} = 1$. Then since $x_i^{g^{-1}(g\gamma g^{-1})} = x_i^{\gamma g^{-1}} = x_{i+1}^{g^{-1}}$, we have

$$(g^{-1}\gamma g)^B = (x_0^{g^{-1}}\ x_1^{g^{-1}} \dots x_{p-1}^{g^{-1}}).$$

So $(g^{-1}\gamma g)^B$ is a p-cycle, and similarly we have $(g^{-1}\gamma g)^{B'} = 1$. This contradicts that $B \sim B'$. Reversing this argument, we also conclude that if

$B^g \sim B'^g$, then $B \sim B'$. So $\sim$ is a $G/\mathcal{B}$-congruence. Then $\mathcal{E}/\mathcal{B}$ is a block system of $G/\mathcal{B}$. Hence $\mathcal{E}$ is a block system of G.

We claim that if $(x_0, y_0) \in A(\Gamma)$ for some $x_0 \in B, y_0 \in B' \not\sim B$, then $(x, y) \in A(\Gamma)$ for every $x \in B, y \in B'$. Since $B' \not\sim B$, γ^B is a p-cycle but $\gamma^{B'}$ is not a p-cycle for some $\gamma \in G_{(\mathcal{B})}$. By taking γ^k with k coprime to p, we may again assume that $\gamma^{B'} = 1$ and $\gamma^B = (x_0\ x_1\ \ldots\ x_{p-1})$. Then the image of the arc (x_0, y_0) under application of γ^r is (x_r, y_0). So for every $x \in B$, $(x, y_0) \in A(\Gamma)$. Now, there is some $\delta \in G_{(\mathcal{B})}$ such that $\delta^{B'}$ is a p-cycle. As above, applying δ to each arc (x, y_0) $p-1$ times gives us the arcs (x, y) for every $x \in B, y \in B'$.

Let $\gamma \in G_{(\mathcal{B})}$ and consider for $E \in \mathcal{E}$ the map $\gamma|_E$. Let $a := (x_0, y_0) \in A(\Gamma)$. If both $x_0, y_0 \in E$, then $a^{\gamma|_E} = a^\gamma \in A(\Gamma)$. Similarly, if both $x_0, y_0 \notin E$, then $a^{\gamma|_E} = a \in A(\Gamma)$. Now if $x_0 \in E, y_0 \notin E$, let $B, B' \in \mathcal{B}$ such that $x_0 \in B$ and $y_0 \in B'$. As $\gamma|_E$ fixes each block of $\mathcal{B}$ setwise, $\gamma|_E(x_0) \in B$, and $\gamma|_E(y_0) = y_0 \in B'$. By the previous paragraph, $(x, y) \in A(\Gamma)$ for every $x \in B, y \in B'$. So $\gamma|_E(x_0, y_0) \in A(\Gamma)$. On the other hand, if $x_0 \notin E, y_0 \in E$, then analogously $\gamma|_E(x_0) = x_0 \in B$, and $\gamma|_E(y_0) \in B'$, so that $\gamma|_E(x_0, y_0) \in A(\Gamma)$ again. This exhausts all possibilities for a, so $\gamma|_E \in \mathrm{Aut}(\Gamma)$. $\square$

lexicographic product

We introduce one type of graph product: The *lexicographic product* $\Gamma[\Sigma]$[1] of graphs Γ, Σ is the graph where $V(\Gamma[\Sigma]) = V(\Gamma) \times V(\Sigma)$ and any two vertices $(u, v), (x, y) \in \Gamma[\Sigma]$ are adjacent if and only if either $u \sim x$ in Γ, or $u = x$ and $v \sim y$ in Σ. Note that these adjacency conditions are mutually exclusive for simple graphs. The lexicographic product is sometimes also called the *wreath product* and denoted $\Gamma \wr \Sigma$, because it is

[1] Do not confuse this notation with that of the induced subgraph: here the object contained in brackets is another graph, not a subset of vertices.

closely related to the group wreath product [4].[2] The lexicographic product is not commutative in general, but is associative [11]. The resulting graph looks like substituting a copy of Σ for every vertex of Γ, and adding every possible edge between the copies of Σ. The lexicographic product of two Cayley (di)graphs is again a Cayley (di)graph.

Now we finally come to the main theorem of this section.

Theorem 11. *Every vertex-transitive digraph of order p^3, for prime p, is isomorphic to a Cayley digraph.*

Proof. Let Γ be a vertex-transitive digraph of order p^3, and P be a Sylow p-subgroup of $\mathrm{Aut}(\Gamma)$. By proposition 3, P is transitive. Additionally, P (being a p-group) has nontrivial center, so there exists $\alpha \in Z(P)$ such that $|\alpha| = p$. Then $\langle \alpha \rangle \trianglelefteqslant P$, and so the set of orbits of $\langle \alpha \rangle$ is a block system $\mathcal{B}$ of P with blocks of size p. So $P/\mathcal{B}$ is a transitive group of degree p^2, hence contains a regular subgroup. We pick a largest subgroup $P' \leqslant P$ such that $P'/\mathcal{B}$ is a regular group. Since the center of a transitive group is semiregular, by choice of P' we have $\alpha \in P'$, and so $P' \geqslant \langle \alpha \rangle$ is transitive.

Define an equivalence relation $\sim$ on $\mathcal{B}$ by $B \sim B'$ if and only if for any $\gamma \in P'_{(\mathcal{B})}$, γ^B is a p-cycle if and only if $\gamma^{B'}$ is a p-cycle. Then lemma 10 says P' admits a block system $\mathcal{E}$ consisting of the equivalence classes of $\sim$, and for any $\gamma \in P'_{(\mathcal{B})}$, $E \in \mathcal{E}$, we have $\gamma|_E \in \mathrm{Aut}(\Gamma)$. By maximality of P', we have for any $\gamma \in P'_{(\mathcal{B})}$ and $E \in \mathcal{E}$ that $\gamma|_E \in P'$ (otherwise, $\gamma \notin P'$, but $P'_{(\mathcal{B})} \leqslant P'$, a contradiction). We now consider that there are three possibilities for the number of equivalence classes of $\sim$: $1, p, p^2$. If there is one equivalence class ($\mathcal{E}$ has one block), then $P'_{(\mathcal{B})} = \langle \alpha \rangle$, and

[2] In [4], the notation for the group wreath product is swapped so that the base group is on the right.

as $|P'/\mathcal{B}| = p^2$, by the orbit-stabilizer lemma $|P'| = |P'/\mathcal{B}| \cdot |P'_{(\mathcal{B})}| = p^3$. Since P' is regular, Γ is isomorphic to a Cayley digraph of P'. If there are p^2 equivalence classes of $\sim$ ($\mathcal{E}$ has p^2 blocks and in fact $\mathcal{E} = \mathcal{B}$), then Γ is isomorphic to the lexicographic product $\Gamma_1[\Gamma_2]$, where Γ_1 is a vertex-transitive digraph of order p^2 and Γ_2 is a vertex-transitive digraph of order p. Since Γ_1 and Γ_2 are both Cayley digraphs, $\Gamma \cong \Gamma_1[\Gamma_2]$ is again a Cayley digraph.

If there are p equivalence classes of $\sim$, then $\mathcal{E}$ has p blocks of size p^2. Then $P'_{(\mathcal{B})} = \langle \alpha|_E \mid E \in \mathcal{E}\rangle$, which has order p^p, since there are p cycle-disjoint elements of order p in $\{\alpha|_E \mid E \in \mathcal{E}\}$. As $P'/\mathcal{B}$ is regular, $|P'| = |P'_{(\mathcal{B})}| \cdot |(P')^{\mathcal{B}}| = p^p \cdot p^2 = p^{p+2}$. As $P'/\mathcal{E}$ is of degree p, there exists $\tau_1 \in P'$ such that $\tau_1/\mathcal{E}$ has order p. If $\tau_1/\mathcal{B}$ has order p^2, then since $|P'/\mathcal{B}| = p^2$, we have $P'/\mathcal{B} = \langle \tau_1/\mathcal{B}\rangle$. As $\alpha \in Z(P')$, $\langle \tau_1, \alpha\rangle$ is an abelian subgroup, which is regular. So we assume that $\tau_1/\mathcal{B}$ has order p instead.

We claim that $(P'_E)^E$, the transitive constituent of the "point" stabilizer of E in P', is regular for every $E \in \mathcal{E}$. Indeed, as $P'/\mathcal{B}$ is regular, any element of P'_E that fixes a point (block of $\mathcal{B}$) must fix every block of $\mathcal{B}$, and hence lies in $P'_{(\mathcal{B})}$. As $P'_{(\mathcal{B})} = \langle \alpha|_E \mid E \in \mathcal{E}\rangle$ is semiregular in its action on $E \in \mathcal{E}$, the only element of P'_E fixing a point is the identity.

Now since $(P'_E)^E$ is regular for every $E \in \mathcal{E}$, it has p^2 elements. So by the embedding theorem ([4] theorem 4.3.1, first proven by Krasner and Kalužnin), P' is permutation isomorphic to a subgroup of $(P'_E)^E \wr (P'/\mathcal{E})$, which is either $\mathbb{Z}_p^2 \wr \mathbb{Z}_p$ or $\mathbb{Z}_{p^2} \wr \mathbb{Z}_p$. Let $\tau_2 \in P'$ such that $\langle \tau_2\rangle/\mathcal{B}$ has order p and is not contained in $\langle \tau_1\rangle/\mathcal{B}$.

If P' is permutation isomorphic to a subgroup of $\mathbb{Z}_p^2 \wr \mathbb{Z}_p$, then we label the set permuted by P' with elements of $\mathbb{Z}_p^3$ so that

$$\tau_1 : (i,j,k) \mapsto (i + a_i, j, k+1)$$
$$\tau_2 : (i,j,k) \mapsto (i + b_i, j+1, k)$$
$$\alpha : (i,j,k) \mapsto (i+1, j, k)$$

where $a_i, b_i \in \mathbb{Z}_p$. As $\mathcal{E} = \{\{(i,j,k) \mid (i,j) \in \mathbb{Z}_p^2\} \mid k \in \mathbb{Z}_p\}$, the maps $(i,j,k) \mapsto (i+a_i,j,k)$ and $(i,j,k) \mapsto (i+b_i,j,k)$ belong to $P'_{(\mathcal{B})} = \langle \alpha|_E \mid E \in \mathcal{E}\rangle$, since they fix every block of $\mathcal{B}$ setwise. We may thus assume without loss of generality that $a_i = b_i = 0$ for every $i \in \mathbb{Z}_p$, in which case $\langle \tau_1, \tau_2, \alpha\rangle \cong \mathbb{Z}_p^3$. As $\langle \tau_1, \tau_2, \alpha\rangle$ is transitive and abelian, it is a regular subgroup of $\mathrm{Aut}(\Gamma)$, so Γ is isomorphic to a Cayley digraph of $\mathbb{Z}_p^3$.

If instead P' is permutation isomorphic to a subgroup of $\mathbb{Z}_{p^2} \wr \mathbb{Z}_p$, then we label the set permuted by P' by elements of $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ so that $\tau_1 : (i,j) \mapsto (i+b_i, j+1)$ and $\tau_2 : (i,j) \mapsto (i+c_i, j)$, where $b_i, c_i \in \mathbb{Z}_{p^2}$. As $\langle \tau_1, \tau_2\rangle/\mathcal{B} \leqslant P'/\mathcal{B} \cong \mathbb{Z}_p \times \mathbb{Z}_p$, we may assume that $b_i \equiv 0 \bmod p$ and $c_i \equiv 1 \bmod p$ for every $i \in \mathbb{Z}_p$ (think of $\mathbb{Z}_{p^2}$ as $\{xp + y \mid x, y \in \mathbb{Z}_p\}$). Then $\tau_2^p(i,j) = (i + p^2 e_i + p, j) = (i+p, j) \neq 1$, and $\tau_2^p \in P'_{(\mathcal{B})}$. So $\tau_1^p|_E \in P'$ for all $E \in \mathcal{E}$. Then $(\tau_2^p)^{d_i} : (i,j) \mapsto (i + pd_i, j)$ and $(\tau_2^p)^{e_i}$ are both in P'. Hence $\tau_1' = \tau_1 \circ (\tau_2^{pd_i})^{-1}$ and $\tau_2' = \tau_2 \circ (\tau_2^{pe_i})^{-1}$ are also contained in P', and we see that $\tau_1' : (i,j) \mapsto (i, j+1)$, $\tau_2' : (i,j) \mapsto (i+1, j)$. So $\langle \tau_1', \tau_2'\rangle$ is regular and isomorphic to $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$, and therefore Γ is isomorphic to a Cayley digraph of $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$. $\square$

3.3 Graphs of order p^n for $n \geqslant 4$

Unfortunately, the nice pattern established in the previous sections does not hold for powers of p greater than 3. For $p = 2$, a vertex-transitive non-Cayley graph of order 16 exists [15]. As a vertex-transitive graph Γ is Cayley if and only if the union of finitely many copies of Γ is Cayley, we have that a vertex-transitive non-Cayley graph 2^n exists for all $n \geqslant 4$. For $p \geqslant 3$, a construction of a vertex-transitive non-Cayley graph of order p^n for all $n \geqslant 4$ can be found in [15]. So other sufficient conditions must be found for a vertex-transitive graph on p^n vertices to be Cayley.

Feng in [6] provides one such condition for odd primes. We introduce one definition for the proof: Let $\mathcal{B} = \{B_1, \ldots, B_m\}$ be a partition of vertices of a graph Γ into m blocks (not necessarily of equal size). A *quotient graph* of Γ is a graph $\Gamma_{\mathcal{B}}$ defined by $V(\Gamma_{\mathcal{B}}) = \mathcal{B}$ and edges defined by $B_i \sim B_j$ if and only if $v_i \sim v_j$ for some $v_i \in B_i, v_j \in B_j$.

quotient graph

Theorem 12. *A vertex-transitive graph Γ of order p^n for prime $p \geqslant 3$ and $n \in \mathbb{N}$, with $\deg(\Gamma) < 2p + 2$, is a Cayley graph.*

Proof. As a disconnected vertex-transitive graph is Cayley if and only if one of its components is Cayley, we assume without loss of generality that Γ is connected. By proposition 3, a Sylow p-subgroup $P \leqslant \mathrm{Aut}(\Gamma)$ is transitive on $V(\Gamma)$. Since Γ has odd order and is regular, by the handshaking lemma $\deg(\Gamma) \cdot |V(\Gamma)| = 2|E(\Gamma)|$, so $\deg(\Gamma)$ is even. Hence either $\deg(\Gamma) = 2p$ or $\deg(\Gamma) \leqslant 2p - 2$.

If $\deg(\Gamma) \leqslant 2p - 2$, we claim that P is regular. Let $u \in V(\Gamma)$. Since $\deg(\Gamma) < 2p$ is even, P_u fixes at least one vertex in $N(u)$. So P_u has either one orbit of length p (call this a *p-orbit*) on $N(u)$, or none. Suppose for a

p-orbit

contradiction P_u has a p-orbit Δ on $N(u)$. Let $v \in \Delta$. As P is transitive, $v^\alpha = u$ for some $\alpha \in P$. If $u^\alpha \in \Delta$, then $(u^\alpha)^\beta = v$ for some $\beta \in P_u$. On the other hand, $v^{\alpha\beta} = u^\beta = u$. This implies $|\alpha\beta| = 2$, but Lagrange's theorem says this is impossible since $|P|$ is odd. Hence $u^\alpha \notin \Delta$, and as P_u only has one p-orbit on $N(u)$, P_u fixes u^α. So $P_u = P_{u^\alpha}$. But since $\alpha^{-1} \in P_u$, conjugating both sides by α^{-1} gives $P_u = P_{u^{\alpha^{-1}}} = P_v$, contradicting that Δ is an orbit of P_u. Hence P_u fixes $N(u)$ pointwise. By transitivity of P and connectedness of Γ, this implies $P_u = 1$, so P is regular on $V(\Gamma)$.

If $\deg(\Gamma) = 2p$, we claim that P has a regular subgroup. It suffices to show that any transitive p-subgroup $P \leqslant \mathrm{Aut}(\Gamma)$ has a regular subgroup. We proceed by induction on k. Proposition 8 proves it for $k = 1$.

Let $u \in V(\Gamma)$. If P_u fixes a vertex in $N(u)$, then it has at most one p-orbit on $N(u)$, so P is regular by previous arguments. So assume P_u has two p-orbits. Let $N \leqslant Z(P)$ with $|N| = p$, which exists as P has nontrivial center. As $N \trianglelefteq P$, the set of orbits of N forms a normal imprimitive block system $\mathcal{B} = \{B_0, B_1, \ldots, B_{p^{n-1}-1}\}$ of P. Since $N \leqslant P_{(\mathcal{B})}$, the kernel of the induced action of P on $\mathcal{B}$, we have $\deg(\Gamma_\mathcal{B}) \leqslant 2p$.

If $\deg(\Gamma_\mathcal{B}) = 2p = \deg(\Gamma)$, then every element of $N(u)$ must belong to a different block. Thus $(P_{(\mathcal{B})})_u$ fixes $N(u)$ pointwise, and since Γ is connected, $(P_{(\mathcal{B})})_u = 1$. Then $P_{(\mathcal{B})} = (P_{(\mathcal{B})})_u N = N$, implying that P/N acts faithfully on $V(\Gamma_\mathcal{B})$. As P/N is transitive on $V(\Gamma_\mathcal{B})$, P/N contains a regular subgroup of $\mathrm{Aut}(\Gamma_\mathcal{B})$ by the inductive hypothesis, say P'/N. Then P' acts transitively on $V(\Gamma)$, and as $|P'| = |N| \cdot |P'/N| = p \cdot |V(\Gamma_\mathcal{B})| = |V(\Gamma)|$, P' is a regular subgroup of P.

So we assume $\deg(\Gamma_\mathcal{B}) < 2p$. For any $u \in V(\Gamma)$, P_u has two p-orbits on $N(u)$. Let $u_0 \in B_0$. Since $\deg(\Gamma) = 2p > \deg(\Gamma_\mathcal{B})$, there is a block, say

B_1, such that B_1 contains at least two vertices u_1, v_1 adjacent to u_0. We claim that u_1 and v_1 are in the same p-orbit of P_{u_0} on $N(u_0)$: otherwise, as B_1 is a block of P and $|B_1| = p$, u_0 is adjacent to exactly two vertices in B_1, which must be u_1 and v_1. But this implies that $\Gamma_{\mathcal{B}}$ has degree p, contradicting that $|V(\Gamma_{\mathcal{B}})|$ is odd (by handshaking again). Since u_0 was arbitrary, the induced subgraph $\Gamma[B_i] = \overline{K_p}$ for each i.

Observe that $\Gamma[B_0 \cup B_1] \cong K_{p,p}$. As P is transitive, there exists α such that $u_0^\alpha \in B_1$. Then B_0 is a p-orbit of $P_{u_0^\alpha}$ on $N(u_0^\alpha)$. If $u_0^{\alpha^2} \in B_0$, then for some $\beta \in P_{u_0^\alpha}$ we have $(u_0^{\alpha^2})^\beta = (u_0^\alpha)^{\alpha\beta} = u_0$. But since $u_0^{\alpha\beta} = (u_0^\alpha)^\beta = u_0^\alpha$, we have that $|\alpha\beta|$ is even, contradicting that $|P|$ is odd. So $u_0^{\alpha^2} \notin B_0$ and without loss of generality $u_0^{\alpha^2} \in B_2$. Hence $\Gamma[B_1 \cup B_2] \cong K_{p,p}$ also. If we repeat this argument for all powers of α and blocks of $\mathcal{B}$, we see that (up to relabeling) $B_i^\alpha = B_{i+1}$, so $\Gamma[B_i \cup B_{i+1}] \cong K_{p,p}$, for $0 \leqslant i \leqslant p^{n-1} - 1$ (with $B_{p^{n-1}} = B_0$). Further, $\Gamma[B_i \cup B_j] \cong \overline{K_{2p}}$ for $j - i \neq \pm 1$, as every vertex in B_i is already adjacent to all the $2p$ vertices in $B_{i-1} \cup B_{i+1}$. So Γ is the lexicographic product $C_{p^{n-1}}[\overline{K_p}]$. Clearly $\langle N, \alpha \rangle$ acts transitively on $V(\Gamma)$. Since $N \leqslant Z(P)$, we also know $\langle N, \alpha \rangle$ is abelian. Hence $\langle N, \alpha \rangle$ is a regular subgroup of P. $\square$

This degree bound does not hold for $p = 2$, as a vertex-transitive non-Cayley graph of order 16 and degree 4 was found with a computer [6].

This theorem imposes a rather strict condition; as the bound does not depend on n, the proportion of graphs of order p^n satisfying the bound is relatively small when n is large. Hence we would like to continue studying graphs in this family, which we will do in chapter 4.

Chapter 4

Cores of generalized cubelike graphs

The problem of finding the cores of cubelike graphs is a well-known unsolved problem, for which the most recent results were published in [13]. In light of the general results on vertex-transitive graphs of prime power order reviewed in chapter 3, it is worth seeing to what extent we can apply these techniques to specific situations. The generalized cubelike graphs are a good concrete example of such graphs, and studying them could also lead to insights on the original cubelike problem, which motivates this chapter. We will investigate several special cases of conjecture 13, using the tools and language of finite geometry introduced in section 4.1.

4.1 Finite geometries

For more on incidence geometry, we refer the reader to [20].

geometry

A *geometry* is a triple $\Gamma = (X, \sim, T)$ over a *type set* I satisfying:

- The *type function* $T : X \to I$ is surjective.

- The *incidence relation* $\sim$ on the elements of the set X is reflexive, symmetric, and satisfies ($x \sim y$ and $T(x) = T(y)$) implies $x = y$.
- Every *flag* (set of pairwise incident elements) of Γ is contained in a *chamber* (flag containing every type in I).

projective space

A *projective space* is a geometry over the type set $\{$point, line$\}$ satisfying:

1. Any two points determine a unique line.
2. If lines PQ, RS intersect at a point O, then PR intersects QS.
3. There are three noncollinear points.
4. Each line has at least three points.

affine space

An *affine space* is a geometry over the type set $\{$point, line$\}$ satisfying:

1. Any two points determine a unique line.
2. Every line is incident with at least two points.
3. There are at least two lines.
4. There is an equivalence relation $\|$ on the set of lines such that for any point $P \not\sim \ell$ a line, there is a unique line $m \sim P$ with $m \parallel \ell$.

subspace

A set of points K in a projective or affine space is called a *subspace* if for any $P, Q \in K$, all the points on the line PQ are also in K.

Let V be a $(d+1)$-dimensional vector space over $\mathbb{F}_q$, where $q = p^k$ for prime p. The geometry defined by taking the one-dimensional vector subspaces of V as points, two-dimensional subspaces as lines, and incidence relation induced by containment in V is a projective space. This geometry is denoted $PG(d,q)$. If a hyperplane (maximal proper subspace) is removed from $PG(d,q)$, then the geometry defined by letting vectors $x \in \mathbb{F}_q^d$ be points, additive cosets $y + \langle x \rangle$ with $x, y \in \mathbb{F}_q^d$ be lines, and incidence induced by containment is an affine space. This geometry is denoted $AG(d,q)$.

$PG(d,q)$

$AG(d,q)$

4.2 The conjecture

Recall that a generalized cubelike graph is defined as a graph $\mathrm{Cay}(\mathbb{Z}_p^n, S)$ for $p \geqslant 3$, $n \in \mathbb{N}$. Inspired by the problem studied in [13], we have:

Conjecture 13. *The core of a generalized cubelike graph is a generalized cubelike graph.*

When $n = 1$, a generalized cubelike graph is itself a core. Indeed, since such a graph $\Gamma = \mathrm{Cay}(\mathbb{Z}_p, S)$ has prime order, by theorem 7 the order of $\Gamma^\bullet$ is 1 or p. Recall that any element in $\mathbb{Z}_p$ generates the entire group, so that if S is nonempty as we require, Γ is connected. Hence $1 < \chi(\Gamma) \leqslant |V(\Gamma^\bullet)|$, so $\Gamma^\bullet$ has p vertices (and the core is an induced subgraph). So for the remainder of the exposition, we assume $n \geqslant 2$.

normal

A Cayley graph is called *normal* if $g^{-1}Sg = S$ for all $g \in G$, i.e. its connection set is closed under conjugation.[1] As $\mathbb{Z}_p^n$ is abelian, any generalized cubelike graph is normal. Roberson [16] showed the following result, which hints at a product structure for normal Cayley graphs:

Proposition 14. *Let X be a normal Cayley graph and Y be a core of X. Then there exists a partition $\{V_1, \ldots, V_k\}$ of $V(X)$ such that each V_i induces a copy of Y.*

We will see that for certain choices of the connection set S, a generalized cubelike graph is indeed a (lexicographic) product of graphs.

Rotheram proved conjecture 13 for some generalized cubelike graphs:

[1] In the literature, a normal Cayley graph may instead refer to $\Gamma = \mathrm{Cay}(G, S)$ where the regular subgroup of $\mathrm{Aut}(\Gamma)$ corresponding to right multiplication by elements of G is a normal subgroup of $\mathrm{Aut}(\Gamma)$.

Proposition 15 ([18] Corollary 7.2.8). *Let $\Gamma = \mathrm{Cay}(G, S)$ be a connected, undirected graph with $G \cong \mathbb{Z}_p^n$ where $p \neq 3$ is prime, and $\mathrm{Aut}(\Gamma^\bullet)$ primitive in its action on $V(\Gamma^\bullet)$. Then $\Gamma^\bullet$ is a Cayley graph of $\mathbb{Z}_p^m$, where $1 \leqslant m \leqslant n$.*

However, requiring $\mathrm{Aut}(\Gamma^\bullet)$ to act primitively on $V(\Gamma^\bullet)$ is a strong condition, so the question remains open for most generalized cubelike graphs.

4.3 Removing one element from S

If a generalized cubelike graph has order p^n and connection set $S = \mathbb{Z}_p^n \setminus 1$ (which is necessarily the complete graph K_{p^n}), then removing an element g and its inverse from S will remove the edges of exactly p^{n-1} edge-disjoint p-cycles from K_{p^n}. We may wonder whether this removal will produce a graph which is still a core. Intuitively, this would make sense as there are "too many" edges remaining in the graph for there to be a homomorphism to a smaller subgraph. We first consider the case where $p = 3, n = 2$ (fig. B.6). We will write $g^\pm$ for g, g^{-1} from now.

Theorem 16. *A graph $\Gamma = \mathrm{Cay}(\mathbb{Z}_3^2, S)$ where $S = \mathbb{Z}_3^2 \setminus \{1, g^\pm\}$ for any $g \in \mathbb{Z}_3^2 \setminus 1$ is a core.*

Proof. Let $x \in V(\Gamma)$. We note that in $\mathbb{Z}_3^2$ viewed as $AG(1,3)$, the one-dimensional affine subspaces (lines) are 3-cycles. So asking how many lines pass through a point is the same as asking how many 3-cycles pass through a vertex. There are a total of $3^2 - 1$ nonzero vectors, or nonidentity elements, and $3 - 1$ distinct nonzero vertices in each 3-cycle. So the number of 3-cycles passing through x is $\frac{8}{2} = 4$.

Suppose for a contradiction that Γ is not a core. Since the core is an induced subgraph, by theorem 7 we have that $|V(\Gamma^\bullet)| = 3$. Because Γ

is 6-regular, there is at least one edge in the induced subgraph created by any three vertices. As Γ is vertex-transitive, theorem 6 then implies that $\Gamma^\bullet = C_3$. There are $\frac{|S|}{2} = 3$ pairwise edge-disjoint 3-cycles passing through x, since each cycle contributes 2 to the degree. We also note that these cycles are automatically vertex-disjoint because they are 3-cycles.

Now there are two vertices $a, b \in V(\Gamma)$ not adjacent to x. As the homomorphic image of an odd cycle is an odd cycle of no greater length, every 3-cycle in Γ must be identifiable with each other, which can be thought of as 3-coloring the graph. Label x with 1, and the two vertices in each of the three disjoint 3-cycles containing x with 2 and 3 respectively. Let one of the vertices labeled 2, contained in one of these 3-cycles, be called z. As $\deg(z) = 6$ and z can only be additionally adjacent to the two vertices labeled 3, but not the other vertices labeled 2, it follows that $z \sim a$ and $z \sim b$. Further, $\{a, b\} \in E(\Gamma)$: using the fact that z must be contained in 4 3-cycles and checking all possible 3-cycles forces a, b, z to form a 3-cycle. Hence (without loss of generality) b is labeled 2 and a is labeled 3. But a can only be adjacent to 3 additional vertices for the coloring to be proper, which means that $\deg(a) \leqslant 5$, a contradiction. $\square$

The next theorem shows that for $n > 2$, no generalized cubelike graph with $p = 3$ and connection set $\mathbb{Z}_3^n \setminus \{1, g^\pm\}$ is a core. However, the cores of such graphs are still generalized cubelike graphs (fig. 4.1).

Theorem 17. *Let $n > 2$ and $\Gamma = \mathrm{Cay}(G, S)$ where $G = \mathbb{Z}_3^n$ and $S = G \setminus \{1, g^\pm\}$ for any $g \in \mathbb{Z}_3^n \setminus 1$. Then $\Gamma^\bullet \cong \mathrm{Cay}(\mathbb{Z}_3^{n-1}, \mathbb{Z}_3^{n-1} \setminus 1)$.*

Proof. Removing $g^\pm$ from the connection set removes the edges of 3^{n-1} 3-cycles from K_{p^n}. Now these 3-cycles are mutually vertex-disjoint: for any $x \in V(\Gamma)$, we have $\{x, xg, xg^2\} = x\langle g \rangle$, i.e., the cycles generated by right

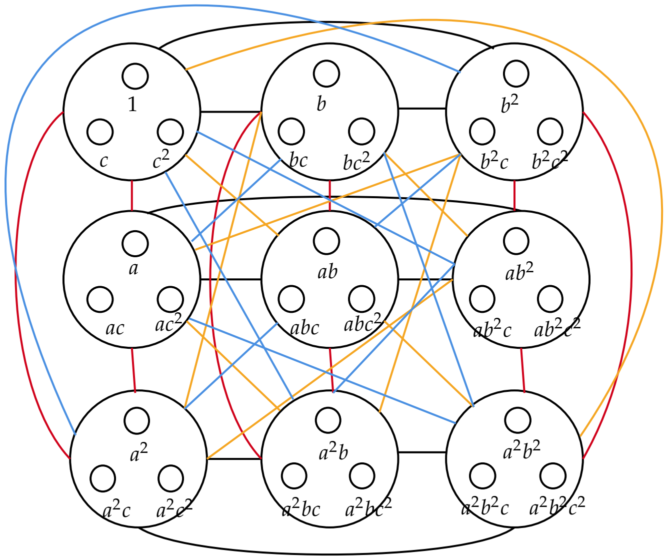

FIGURE 4.1: $\mathrm{Cay}(\mathbb{Z}_3^3, \mathbb{Z}_3^3 \setminus \{1, c^{\pm}\})$ where $\mathbb{Z}_3^3 = \langle a, b, c\rangle$. Lines between independent sets mean "every vertex in one set has an edge to every vertex in the other set". Different colors correspond to edges induced by different cosets in S: red $a^{\pm}\langle c\rangle$, black $b^{\pm}\langle c\rangle$, yellow $(ab)^{\pm}\langle c\rangle$, blue $(ab^2)^{\pm}\langle c\rangle$.

multiplication by g are precisely the left cosets of the cyclic subgroup $\langle g\rangle$. As left cosets of a subgroup partition the group, any two cycles are either the same or disjoint. So after removal, we have 3^{n-1} independent sets of size 3 in the graph, the vertices of which remain adjacent to every other vertex in Γ. Picking one vertex from each independent set produces $K_{3^{n-1}}$ as a subgraph of Γ. Then we have a homomorphism to a proper subgraph of Γ: sending the three vertices of each independent set to one vertex in $K_{3^{n-1}}$ suffices. So Γ is not a core. Further, as any complete graph is a core, $\Gamma^{\bullet}$ cannot be smaller than $K_{3^{n-1}}$, and as $|V(\Gamma^{\bullet})|$ divides $|V(\Gamma)|$, the core cannot be larger than $K_{3^{n-1}}$ which has order 3^{n-1}. So $\Gamma^{\bullet} = K_{3^{n-1}}$. This is the Cayley graph of $\mathbb{Z}_3^{n-1}$ with all nonidentity elements in the connection set. $\square$

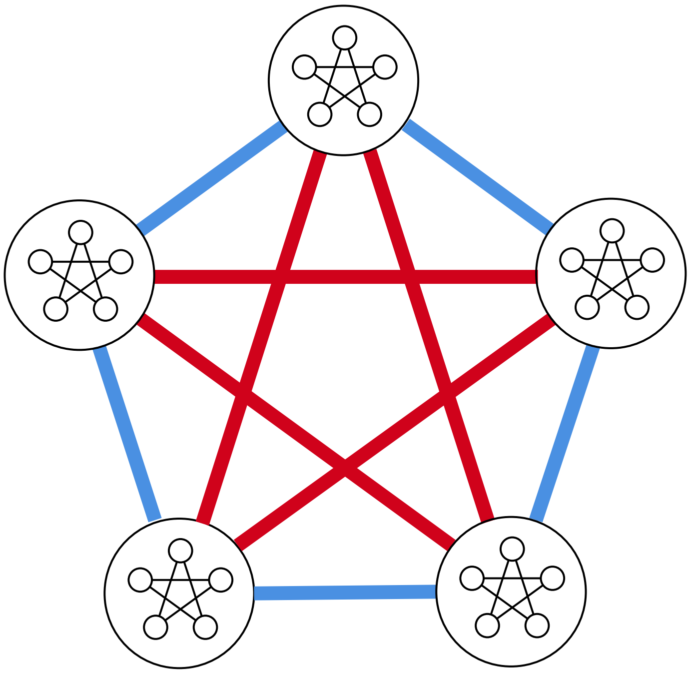

FIGURE 4.2: $\mathrm{Cay}(\mathbb{Z}_5^2, \mathbb{Z}_5^2 \setminus \{1, b^{\pm}\})$, where $\mathbb{Z}_5^2 = \langle a, b\rangle$. Thick lines: "every vertex in one set has an edge to every vertex in the other set". Different colors correspond to edges induced by different cosets of $\langle b\rangle$ in S: blue $a^{\pm}\langle b\rangle$, red $(a^2)^{\pm}\langle b\rangle$, black $(b^2)^{\pm} = \langle b\rangle \setminus \{1, b^{\pm}\}$.

Recall that the lexicographic product of graphs was defined in chapter 3. The Γ of theorem 17 is the lexicographic product $K_{3^{n-1}}[\overline{K_3}]$. There are at least two obvious ways we may try to generalize this result: by considering $p > 3$, or by considering $S = \mathbb{Z}_3^n \setminus \{1, g_1^{\pm}, g_2^{\pm}, \ldots\}$ (removing more elements).

We consider the former generalization first. For $p > 3$, removing a p-cycle no longer produces an independent set on p vertices, and so the same homomorphism as for $p = 3$ will not work. However, the resulting graph is still a lexicographic product $K_{p^{n-1}}[K_p - C_p]$, where $K_p - C_p$ means the edges of a p-cycle have been removed from K_p (fig. 4.2). Using this view of the graph, we immediately have the following result:

Theorem 18. *Let $p \geqslant 5$ be a prime and $n \in \mathbb{N}$. Then $\Gamma := \mathrm{Cay}(G, S)$ where $G = \mathbb{Z}_p^n$ and $S = G \setminus \{1, g^{\pm}\}$ for any $g \in \mathbb{Z}_p^n \setminus 1$ is a core.*

Proof. We consider a proper vertex coloring of Γ. Let $B_0, B_1, \ldots, B_{p^{n-1}}$ be the "$K_p - C_p$" sets in the lexicographic product. Pick one vertex u_i from each B_i. The induced subgraph $\Sigma = \Gamma[\{u_0, u_1, \ldots, u_{p^{n-1}}\}]$ is $K_{p^{n-1}}$, so at least p^{n-1} colors are needed to color the graph. Now any u_i must be adjacent to at least one other vertex $y_i \in B_i$. But since y_i is also adjacent to every other vertex in Σ, it must have a different color to all the vertices in Σ. Hence at least $p^{n-1} + 1$ colors are needed to color the graph. As the chromatic number of any graph is a lower bound on the order of its core (since $\chi(\Gamma) = \chi(\Gamma^\bullet) \leqslant |V(\Gamma^\bullet)|$), we have $|V(\Gamma^\bullet)| \geqslant \chi(\Gamma) \geqslant p^{n-1} + 1$. As $|V(\Gamma^\bullet)|$ divides $|V(\Gamma)|$, we have $|V(\Gamma^\bullet)| = p^n$. □

4.4 Removing more elements from S

Now we turn to the other generalization, removing more elements from the connection set S. Again, we first work on the case where $p = 3$ and $n = 3$. Consider the case when a subgroup generated by two elements (and one is not a power of the other) is contained in S.

Theorem 19. *Let $\Gamma := \mathrm{Cay}(G, S)$ where $G = \mathbb{Z}_3^3 = \langle a, b, c \rangle$ and $S \subseteq G \setminus 1$, with $\langle a, b \rangle \subseteq S \cup 1 (\neq G)$. Then $\Gamma^\bullet = K_9$.*

Proof. We assume for this proof that at least two nonidentity elements are missing from S, since the one-element case was covered in theorem 17. Γ is the graph obtained by removing additional 3-cycles from the lexicographic product $K_{3^{3-1}}[\overline{K_3}]$. So $|V(\Gamma^\bullet)| \leqslant 3^2$, as we have seen in theorem 17 that the core of this lexicographic product has order 3^2. Now $\langle a, b \rangle$ remains in $S \cup 1$, which induces precisely a subgraph isomorphic to K_9. Hence $\Gamma^\bullet = K_9$. $\square$

The other case, when $S \cup 1$ contains no subgroup $\langle x, y \rangle$, requires some setup. The following (known) lemma states that a group homomorphism always gives rise to a graph homomorphism between Cayley graphs.

Lemma 20. *Let* $\Gamma = \mathrm{Cay}(G, S)$ *and* $\varphi : G \to H$ *a group homomorphism. Then* $\Gamma \to \Sigma = \mathrm{Cay}(H, \varphi(S))$ *where* $\varphi(S) := \{\varphi(v) \mid v \in S\}$.

Proof. By definition, $x \sim y$ if and only if $xy^{-1} \in S$ for any $x, y \in G$. Now since φ is a group homomorphism, $xy^{-1} \in S$ implies $\varphi(x)\varphi(y)^{-1} = \varphi(xy^{-1}) \in \varphi(S)$, which is true if and only if $\varphi(x) \sim \varphi(y)$ in Σ. Hence $x \sim y$ implies $\varphi(x) \sim \varphi(y)$, which means φ is a graph homomorphism. $\square$

Lemma 21. *Let* $\mathbb{Z}_3^3 = \langle a, b, c \rangle$. *If* $K_9 \cong \Sigma' \leqslant \Gamma = \mathrm{Cay}(\mathbb{Z}_3^3, S)$, *then* $S \cup 1$ *contains* $\langle x, y \rangle$ *for some* $x, y \in \mathbb{Z}_3^3$, $x \notin \langle y \rangle$.

Proof. The proof is given as GAP code in appendix A.1, which checks all possible connection sets S for which $\mathrm{Cay}(\mathbb{Z}_3^3, S)$ contains a clique of order 9. For every such S, we check whether any $\langle x, y \rangle$ is contained in S (and the answer is always yes). $\square$

Remark 22. We initially attempted a different proof of lemma 21 by viewing the subgraph as $AG(2, 3)$. Observe that if $1 \in K_9 \leqslant \Gamma$, then 1 has two types of neighbors in K_9, elements in $\langle a, b \rangle$ or not in $\langle a, b \rangle$. As K_9 is 8-regular, by the pigeonhole principle there are 4 vertices of at least one type. Then it suffices to show that Σ' contains 4 directions in $AG(2, 3)$, as there are precisely 4 directions through every point and S is inverse-closed. While the case when there are four elements in $\langle a, b \rangle$ in $N(1) \cap \Sigma'$ was fairly straightforward, the other case was extremely tedious to calculate by hand, and we did not have time to complete it.

natural map

Recall the definition of a quotient graph from section 3.3. If each $B_i \in \mathcal{B}$ is an independent set in Γ, then $\Gamma \to \Gamma_{\mathcal{B}}$. Indeed, the *natural map* $\pi_{\mathcal{B}}$ which sends each vertex or edge to the equivalence class to which it belongs (for the equivalence relation induced by $\mathcal{B}$) is a homomorphism [10].

Now let $\Gamma = \mathrm{Cay}(G, S)$, where $G = \mathbb{Z}_3^3$. Consider the quotient graph $\Gamma_{\mathcal{B}}$ formed by identifying 9 independent sets of 3 vertices each, which exist in Γ when at least one element g of G is not in S. These independent sets correspond to cosets of $\langle g \rangle$, and since $\langle g \rangle \trianglelefteq G$ (as G is abelian), the partition $\mathcal{B}$ is the quotient group $G/\langle g \rangle$. (In fig. 4.1, picking $g = c$, we have $\Gamma_{\mathcal{B}} = K_9$.) Then $\pi_{\mathcal{B}} : \Gamma \to \Gamma_{\mathcal{B}}$ is a homomorphism, and $V(\Gamma_{\mathcal{B}}) = 9$. There are two possibilities: first, $\Gamma_{\mathcal{B}}$ is isomorphic to a subgraph of Γ.

Theorem 23. *Let* $\Gamma = \mathrm{Cay}(G, S)$ *where* $G = \mathbb{Z}_3^3 = \langle a, b, c \rangle$ *and* $S \subseteq G \setminus 1$ *such that* $\langle x, y \rangle \nsubseteq S \cup 1$ *for any* $x, y \in G$. *Let* $\mathcal{B} = G/\langle c \rangle$. *Suppose* $\Gamma_{\mathcal{B}}$ *is isomorphic to a subgraph of* Γ. *Then* $\Gamma^\bullet = K_3$.

Proof. Note that S is a proper subset of $G \setminus 1$, because of the condition that $\langle x, y \rangle \nsubseteq S \cup 1$ for any $x, y \in G$.

Suppose for a contradiction $\Gamma^\bullet \neq K_3$. Note that since Γ is vertex-transitive, $\Gamma_{\mathcal{B}}$ is vertex-transitive. If $\Gamma_{\mathcal{B}}$ is not a core, then there is a homomorphism $f : \Gamma_{\mathcal{B}} \to \Sigma = (\Gamma_{\mathcal{B}})^\bullet$ with $|\Sigma| = 3$ by theorem 7. But then $\Sigma = K_3$, a contradiction. So $\Gamma_{\mathcal{B}}$ is a core. Now if $\Gamma_{\mathcal{B}} \neq K_9$, then $\alpha(\Gamma_{\mathcal{B}}) \geqslant 3$, which implies that $\chi(\Gamma_{\mathcal{B}}) \leqslant 3$. Hence $\chi(\Gamma_{\mathcal{B}}) = 3$, i.e. $\Gamma_{\mathcal{B}} \to K_3$, contradicting that $\Gamma_{\mathcal{B}}$ is a core. So $\Gamma_{\mathcal{B}} = K_9$.

We will show that $S \cup 1$ contains a subgroup generated by two elements. $\Gamma_{\mathcal{B}}$ is a vertex-transitive graph on 3^2 vertices, hence a Cayley graph by theorem 9. Let $N := \langle c \rangle$ and consider $\varphi : G \to H := G/N$ defined by $g \mapsto gN$. Now φ is a surjective group homomorphism, and by lemma 20 also a graph homomorphism from Γ to $\Sigma := \mathrm{Cay}(H, \varphi(S))$. Since G is elementary abelian, H is also elementary abelian and therefore isomorphic to a subgroup of G, so Σ is isomorphic to a subgraph of Γ. We denote this subgraph by Σ'. Without loss of generality, we may assume that both vertices $a, b \in S$, so we have $aN, bN \in SN := \{sN \mid s \in S\} = \varphi(S)$. Further, since there must be two elements $x, y \in V(\Sigma')$ such that $x \notin \langle y \rangle$, by relabeling the vertices of Γ we may assume that $a, b \in V(\Sigma')$. By lemma 21, $S \cup 1 \supseteq \langle x, y \rangle$ for some $x \notin y$, a contradiction. $\square$

For the other case, when the quotient graph is not a subgraph, Γ is a core. Indeed, suppose $K_3 \neq \Gamma^\bullet$ for $\Gamma = \mathrm{Cay}(\mathbb{Z}_3^3, S)$ and $\langle x, y \rangle \not\subseteq S \cup 1$ for all $x, y \in \mathbb{Z}_3^3$. Then $\Gamma_\mathcal{B} \not\leqslant \Gamma$ by the contrapositive of theorem 23. The GAP code in appendix A.2 shows for any choice of S with such conditions, Γ has chromatic number 7 or 8. Suppose $|V(\Gamma^\bullet)| = 9$, then $\Gamma^\bullet$ is a Cayley graph. Since $\Gamma^\bullet \neq K_9$ (otherwise some $\langle x, y \rangle$ is contained in $S \cup 1$, by arguments in the previous proof), by vertex-transitivity and the condition that S is inverse-closed we have $\deg(\Gamma^\bullet) \leqslant 6$. But Brooks' theorem gives $\chi(\Gamma) = \chi(\Gamma^\bullet) \leqslant \deg(\Gamma^\bullet)$, a contradiction. Hence $|V(\Gamma^\bullet)| > 9$, so Γ must be itself a core. However, we have not been able to come up with a neater proof which does not require exhaustive computation to determine $\chi(\Gamma)$ for all possible choices of S.

Chapter 5

Conclusion

In chapter 3, we reviewed existing results on identifying Cayley graphs from vertex-transitive graphs of order p^n. These results only hold for small n, or else for graphs with relatively few edges, if $\mathrm{Aut}(\Gamma)$ is not known to be primitive. We then turned to studying generalized cubelike graphs, as they are a concrete example of vertex-transitive graphs on p^n vertices. In particular, we considered conjecture 13, which is analogous to the previously studied cubelike problem from [13]. None of our results in chapter 4 contradict conjecture 13, but so far only prove it for very specific choices of generalized cubelike graphs, summarized here:

p	n	S	$\mathrm{Cay}(\mathbb{Z}_p^n, S)^\bullet$
any	1	any	$\mathrm{Cay}(\mathbb{Z}_p^n, S)$
any	any	$\mathbb{Z}_p^n \setminus 1$	$\mathrm{Cay}(\mathbb{Z}_p^n, S) \cong K_{p^n}$
3	2	$\mathbb{Z}_p^n \setminus \{1, g^\pm\}$	$\mathrm{Cay}(\mathbb{Z}_p^n, S) \cong K_3[K_3 - C_3]$
3	$\geqslant 3$	$\mathbb{Z}_p^n \setminus \{1, g^\pm\}$	$\mathrm{Cay}(\mathbb{Z}_p^{n-1}, \mathbb{Z}_p^{n-1} \setminus 1) \cong K_{3^{n-1}}$
$\geqslant 5$	any	$\mathbb{Z}_p^n \setminus \{1, g^\pm\}$	$\mathrm{Cay}(\mathbb{Z}_p^n, S) \cong K_{p^{n-1}}[K_p - C_p]$
3	3	contains $\langle x, y\rangle$ for $x \notin \langle y \rangle$	$\mathrm{Cay}(\mathbb{Z}_3^2, \mathbb{Z}_3^2 \setminus 1) \cong K_9$
3	3	does not contain any $\langle x, y\rangle$	K_3 if $\Gamma_{\mathcal{B}} \leqslant \Gamma$; else $\mathrm{Cay}(\mathbb{Z}_p^n, S)$

5.1 Further work

The immediate next step towards proving (or disproving) conjecture 13 would be to come up with a more insightful proof for $\mathbb{Z}_3^3$ where S does not contain any two-dimensional subspace, and the quotient graph $\Gamma_{\mathcal{B}}$ is not isomorphic to a subgraph of Γ. This is especially important as even for graphs of order 27, the code in appendix A.2 takes nearly 30 days to run, so computational methods would not be practical for even slightly larger orders. A better proof of lemma 21 would also be desirable. In both cases, a proof by hand would likely give us a better idea about the structure of the problem and the graphs at hand.

Following this, we hope that some of the proof ideas from chapter 4 could be generalized to proving results for all n or different values of p, such as considering the quotient subgraph by a certain subgroup, or viewing the graph as a type of graph product (lexicographic products are only one possible graph product; see [11] for much more).

For generalizations to all n, inductive proofs could be attempted for some of the graphs, as we have already established a base case for certain choices of S. It is also possible that some of the ideas could be used to make progress on the original cubelike problem, i.e. when $p = 2$.

Another observation is that the graphs we studied so far are core-complete. Core-complete graphs have been of interest to many researchers, and many families of graphs have been shown to be core-complete, including distance-transitive graphs [9], nonedge-transitive graphs [2], and strongly regular graphs [17]. Core-completeness of generalized cubelike graphs is stronger than conjecture 13. So if generalized cubelike graphs could be shown to be core-complete, this would imply conjecture 13.

Bibliography

[1] Brian Alspach. "Cayley Graphs". In: *Topics in Algebraic Graph Theory*. Ed. by Lowell W Beineke and Robin J Wilson, pp. 156–176.

[2] Peter J. Cameron and Priscila A. Kazanidis. "CORES OF SYMMETRIC GRAPHS". In: *Journal of the Australian Mathematical Society* 85.2 (Oct. 2008), pp. 145–154. ISSN: 1446-7887, 1446-8107. DOI: 10.1017/S1446788708000815. URL: https://www.cambridge.org/core/product/identifier/S1446788708000815/type/journal_article (visited on 11/12/2023).

[3] John D. Dixon and Brian Mortimer. *Permutation Groups*. Vol. 163. Graduate Texts in Mathematics. New York, NY: Springer New York, 1996. ISBN: 978-1-4612-6885-7 978-1-4612-0731-3. DOI: 10.1007/978-1-4612-0731-3. URL: http://link.springer.com/10.1007/978-1-4612-0731-3 (visited on 12/22/2023).

[4] Ted Dobson, Aleksander Malni, and D. Marui. *Symmetry in Graphs*. Cambridge, United Kingdom: Cambridge University Press, 2022. ISBN: 978-1-108-55399-5.

[5] Paul Erds and Alfréd Rényi. "Asymmetric Graphs". In: *Acta Mathematica Academiae Scientiarum Hungaricae* 14.3-4 (Sept. 1963), pp. 295–315. ISSN: 0001-5954, 1588-2632. DOI: 10.1007/BF01895716. URL:

http://link.springer.com/10.1007/BF01895716 (visited on 04/01/2024).

[6] Yan-Quan Feng. "On Vertex-Transitive Graphs of Odd Prime-Power Order". In: *Discrete Mathematics* 248.1-3 (Apr. 2002), pp. 265–269. ISSN: 0012365X. DOI: 10.1016/S0012-365X(01)00348-X. URL: https://linkinghub.elsevier.com/retrieve/pii/S0012365X0100348X (visited on 03/01/2024).

[7] *GAP – Groups, Algorithms and Programming, Version 4.12.2*. The GAP Group. URL: gap-system.org.

[8] Chris Godsil and Gordon Royle. *Algebraic Graph Theory*. Graduate Texts in Mathematics 207. New York: Springer, 2001. 439 pp. ISBN: 978-0-387-95220-8.

[9] Chris Godsil and Gordon F. Royle. "Cores of Geometric Graphs". In: *Annals of Combinatorics* 15.2 (June 2011), pp. 267–276. ISSN: 0218-0006, 0219-3094. DOI: 10.1007/s00026-011-0094-5. URL: http://link.springer.com/10.1007/s00026-011-0094-5 (visited on 11/12/2023).

[10] Gea Hahn and Claude Tardif. "Graph Homomorphisms: Structure and Symmetry". In: *Graph Symmetry: Algebraic Methods and Applications*. Ed. by Gea Hahn and Gert Sabidussi. Dordrecht: Springer Netherlands, 1997, pp. 107–166. ISBN: 978-94-015-8937-6. DOI: 10.1007/978-94-015-8937-6_4. URL: http://link.springer.com/10.1007/978-94-015-8937-6_4 (visited on 08/17/2023).

[11] Richard Hammack, Wilfried Imrich, and Sandi Klavžar. *Handbook of Product Graphs*. Second edition, first issued in paperback. Discrete

Mathematics and Its Applications. Boca Raton London New York: CRC Press, Taylor & Francis Group, 2016. 518 pp. ISBN: 978-1-138-19908-8.

[12] I. Martin Isaacs. *Finite Group Theory*. Graduate Studies in Mathematics v. 92. Providence, R.I: American Mathematical Society, 2008. 350 pp. ISBN: 978-0-8218-4344-4.

[13] Laura Mančinska et al. "Cores of Cubelike Graphs". In: *European Journal of Combinatorics* 87 (June 2020), p. 103092. ISSN: 01956698. DOI: 10.1016/j.ejc.2020.103092. URL: https://linkinghub.elsevier.com/retrieve/pii/S0195669820300135 (visited on 05/17/2023).

[14] Dragan Marušič. "Vertex Transitive Graphs and Digraphs of Order p^k". In: *Annals of Discrete Mathematics* 27 (1985), pp. 115–128.

[15] Brendan D. McKay and Cheryl E. Praeger. "Vertex-Transitive Graphs Which Are Not Cayley Graphs, I". In: *Journal of the Australian Mathematical Society. Series A. Pure Mathematics and Statistics* 56.1 (Feb. 1994), pp. 53–63. ISSN: 0263-6115. DOI: 10.1017/S144678870003473X. URL: https://www.cambridge.org/core/product/identifier/S144678870003473X/type/journal_article (visited on 01/11/2024).

[16] David Roberson. *Cores of Vertex Transitive Graphs*. Feb. 18, 2013. arXiv: 1302.4470 [math]. URL: http://arxiv.org/abs/1302.4470 (visited on 11/11/2023). preprint.

[17] David E. Roberson. "Homomorphisms of Strongly Regular Graphs". In: *Algebraic Combinatorics* 2.4 (2019), pp. 481–497. ISSN: 2589-5486. DOI: 10.5802/alco.50. URL: https://alco.centre-mersenne.org/item/ALCO_2019__2_4_481_0 (visited on 04/05/2024).

[18] Ricky Rotheram. "Cores of Vertex-Transitive Graphs". University of Melbourne, Oct. 2013. 128 pp. URL: https://rest.neptune-prod.its.unimelb.edu.au/server/api/core/bitstreams/f449cc91-6380-5783-afc5-e74856486a5b/content (visited on 11/12/2023).

[19] L. H. Soicher. *GRAPE, GRaph Algorithms using PErmutation groups, Version 4.9.0*. Refereed GAP package. Dec. 2022. URL: https://gap-packages.github.io/grape/.

[20] Johannes Ueberberg. *Foundations of Incidence Geometry: Projective and Polar Spaces*. Springer Monographs in Mathematics. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg Springer e-books, 2011. ISBN: 978-3-642-20972-7.

[21] Ming-Yao Xu. "A NOTE ON PERMUTATION GROUPS AND THEIR REGULAR SUBGROUPS". In: *Journal of the Australian Mathematical Society* 85.2 (Oct. 2008), pp. 283–287. ISSN: 1446-7887, 1446-8107. DOI: 10.1017/S1446788708000967. URL: https://www.cambridge.org/core/product/identifier/S1446788708000967/type/journal_article (visited on 01/31/2024).

Appendix A

GAP code

What follows is the GAP language [7] code used to prove lemma 21 and the last result of chapter 4. The code uses the GRAPE package [19].

A.1 Proof of lemma 21

```
LoadPackage("grape");;

G := ElementaryAbelianGroup(3^3);;
no_inverse := List(Elements(G));;
id := Remove(no_inverse, 1);;
for x in no_inverse do
    Remove(no_inverse,
      Position(no_inverse, Inverse(x))
      );;
od;

unique2D := Set([]);;

# Find all 2D subspaces:
for i in [2..13] do # <g,g> is not 2D
    for j in [1..i-1] do # group is abelian
        AddSet(unique2D,
          Group(no_inverse[i], no_inverse[j])
          );;
    od;
od;

# WTS: if K9 is subgraph, then some 2D subspace in S.
```

```
# |S| at least 8. But function definition allows
# taking half the elements and a minimum size of 4.

for k in [4..13] do
    for S in Combinations(no_inverse, k) do
        if CliqueNumber(CayleyGraph(G,S))<9
        then continue;
        fi;
        S_with_id := Union(S, List(S,Inverse), [id]);
        any_subspace_contained := false;
        for unique in unique2D do
            if IsSubset(S_with_id, unique)
            then any_subspace_contained := true;
            break;
            fi;
        od;
        if not any_subspace_contained then
        Print(S);
        Print(CliqueNumber(CayleyGraph(G,S)),"\n");
        fi;
    od;
od;
```

A.2 Last result

In practice, this code would take too long to run on an ordinary computer. I made use of the NUS high performance computing resources[1], slightly modifying the code to run on several clusters simultaneously and to write some relevant output to a file. The code could probably be optimized further to take advantage of symmetries in the group, but time constraints prevented this.

```
LoadPackage("grape");;

G := ElementaryAbelianGroup(3^3);;
gens := GeneratorsOfGroup(G);;
```

[1] https://nusit.nus.edu.sg/hpc/. GAP is now installed on clusters atlas8/ parallel24 and atlas9/ parallel20; thanks to Miguel Costa for help with the setup.

```
# Build the set of unique 2D subspaces of the group
no_inverse := List(Elements(G));;
id := Remove(no_inverse, 1);;

for x in no_inverse do
    Remove(no_inverse,
      Position(no_inverse, Inverse(x))
      );;
od;

unique2D := Set([]);;

# Find all 2D subspaces:
for i in [2..Size(no_inverse)] do # <g,g> is not 2D
    for j in [1..i-1] do # group is abelian
        AddSet(unique2D,
          Group(no_inverse[i], no_inverse[j])
          );;
    od;
od;

a:=gens[1]; b:=gens[2]; c:=gens[3];

# WLOG exclude <a> and <b>
exclude_two_gens := ShallowCopy(unique2D);
for unique in exclude_two_gens do
    if IsSubset(unique, GroupByGenerators([a])) or
    IsSubset(unique, GroupByGenerators([b])) then
    Unbind(exclude_two_gens[
      Position(exclude_two_gens,unique)
      ]);
    fi;
od;
exclude_two_gens := Set(exclude_two_gens);
etg_list := [];
for unique in exclude_two_gens do
    temp := [];
    for x in unique do
        if (not x in temp)
        and (not Inverse(x) in temp)
        and (not x=id) then
            Add(temp, x);
        fi;
    od;
    Add(etg_list, temp);
```

```
od;

# Function to construct complements of S sets
optimized_T := function(subspaces)
    local T_temp, unique2D_copy, x, y, x_prime;
    T_temp := Set([a,Inverse(a),b,Inverse(b)]);
    unique2D_copy := ShallowCopy(subspaces);

    while Size(unique2D_copy) > 0 do
        x := unique2D_copy[1];
        # Add a non-identity element not yet in T
        for y in x do
            if (not y=id) and (not y in T_temp) then
                AddSet(T_temp, y);
                AddSet(T_temp, Inverse(y));
                break;
            fi;
        od;
        # Remove other 2D subspaces containing element
        for x_prime in unique2D_copy do
            if y in x_prime then
                Unbind(unique2D_copy[
                  Position(unique2D_copy, x_prime)
                  ]);
            fi;
        od;
        # Remove holes in the list
        unique2D_copy := Compacted(unique2D_copy);
    od;
    return Union(T_temp,[id]);
end;

S_sets := Set([]);
other_S_sets := Set([]);
chromatic_nums := Set([]);

# Permute order of subspaces and each subspace
for p1 in PermutationsList(etg_list[1]) do
for p2 in PermutationsList(etg_list[2]) do
for p3 in PermutationsList(etg_list[3]) do
for p4 in PermutationsList(etg_list[4]) do
for p5 in PermutationsList(etg_list[5]) do
for p6 in PermutationsList(etg_list[6]) do
for permutation in
  PermutationsList([p1, p2, p3, p4, p5, p6])
```

```
  do
    T := optimized_T(permutation);;
    S := Difference(Elements(G),T);;
    if (not S in S_sets)
    and (not S in other_S_sets) then
        chi := ChromaticNumber(CayleyGraph(G,S));;
        if not chi=3 then
            AddSet(other_S_sets, S);
            AddSet(chromatic_nums, [Size(S),chi]);;
            break;
        else
            AddSet(S_sets, S);
        fi;
    fi;
od; od; od; od; od; od; od;
```

Appendix B

Graph examples

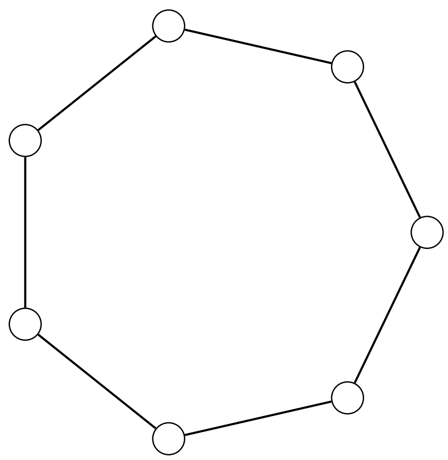

FIGURE B.1: Cycle graph on 7 vertices, C_7.

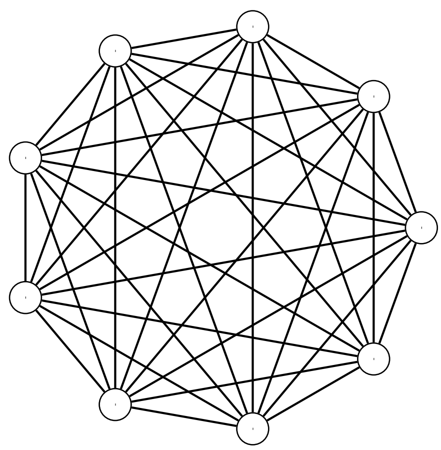

FIGURE B.2: Complete graph on 9 vertices, K_9, or $\mathrm{Cay}(\mathbb{Z}_3^2, \mathbb{Z}_3^2 \setminus 1)$.

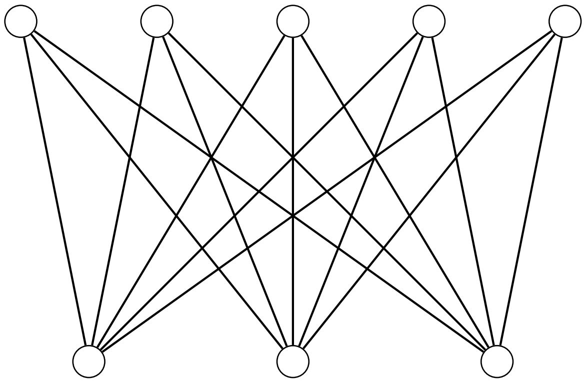

FIGURE B.3: Complete bipartite graph $K_{3,5}$.

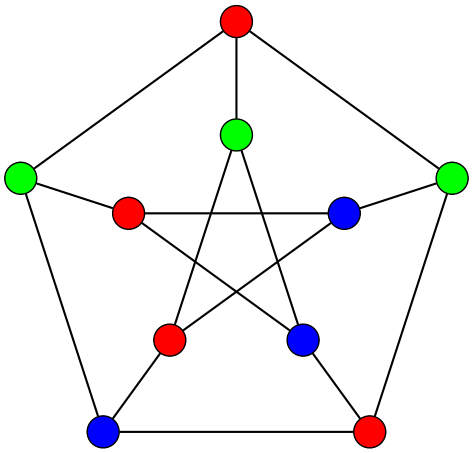

FIGURE B.4: 3-coloring of Petersen graph.

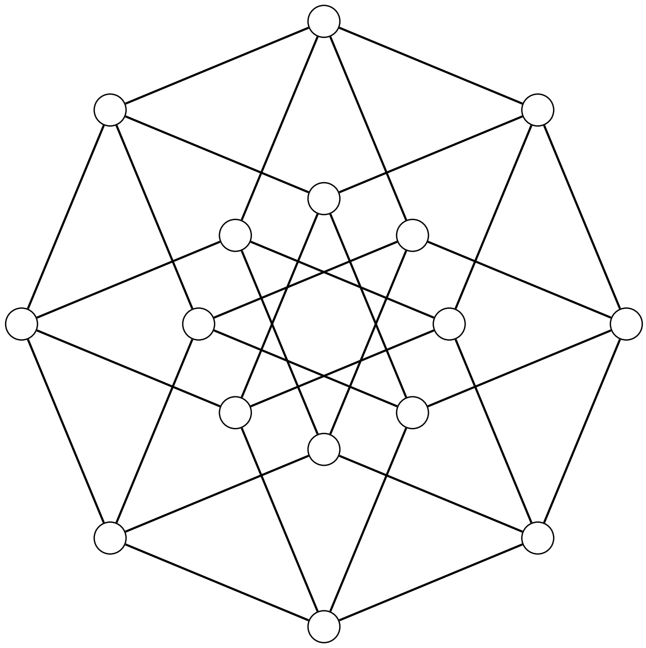

FIGURE B.5: Hypercube Q_4, or $\mathrm{Cay}(\mathbb{Z}_2^4, \{\mathbf{e}_i \mid 1 \leqslant i \leqslant 4\})$.

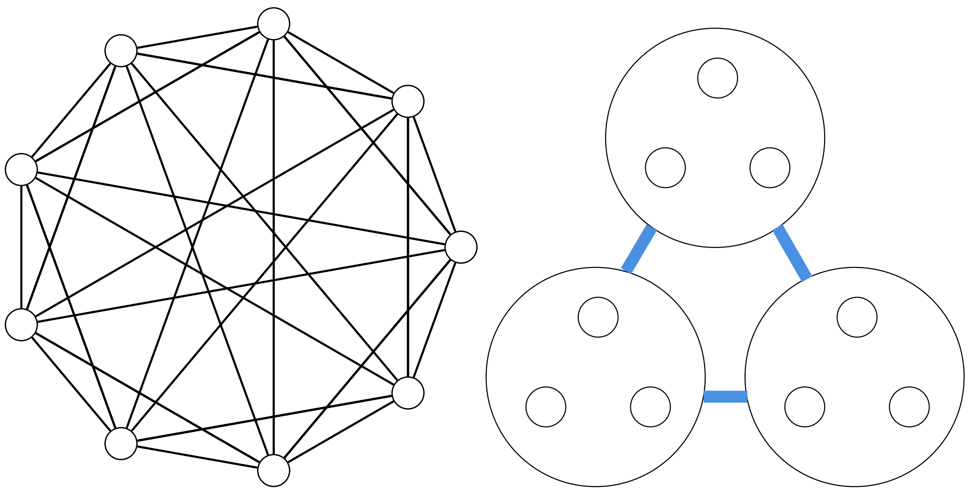

FIGURE B.6: Two views of $\mathrm{Cay}(\mathbb{Z}_3^2, \mathbb{Z}_3^2 \setminus \{1, g^{\pm}\})$. Note the three missing 3-cycles when compared to figure B.2. Thick blue lines mean "every vertex in one set has an edge to every vertex in the other set".