THE UNIVERSITY OF CHICAGO

STRUCTURE, AUTOMORPHISMS, AND ISOMORPHISMS OF REGULAR COMBINATORIAL OBJECTS

A DISSERTATION SUBMITTED TO
THE FACULTY OF THE DIVISION OF THE PHYSICAL SCIENCES
IN CANDIDACY FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY

DEPARTMENT OF MATHEMATICS

BY
JOHN WILMES

CHICAGO, ILLINOIS
AUGUST 2016

To Mom and Dad

"...muchas cosas carecían de nombre,

y para mencionarlas había que señalarlas con el dedo."

Gabriel García Márquez, *Cien Años de Soledad*

Table of Contents

List of Figures

List of Tables

ACKNOWLEDGMENTS

All the results in this thesis are joint work with some subset of László Babai, Xi Chen, Shang-Hua Teng, and Xiaorui Sun. A complete account of the proper credit for each result is given in Section 1.4.

I am particularly grateful to my adviser, Professor László Babai, for teaching me, in many long meetings, how to do and write mathematics.

My fruitful collaborations with Xi Chen, Shang-Hua Teng, and Xiaorui Sun led to much of the research in this thesis. I am grateful to Professor Xi Chen for generously hosting me at Columbia University for a semester, and for the many inspiring conversations on Graph Isomorphism we had. I am grateful to Professor Shang-Hua Teng for his encouragement and support, and for posing many intriguing questions. I thank Xiaorui Sun for the extraordinary effort he invested into our collaborations, and the keen insights he shared that proved essential to our joint results.

I am thankful to Professor Alexander Razborov and Professor George Glauberman for insightful comments and conversations throughout my time in Chicago, and for their careful reading of this thesis.

My thanks also go to my fellow graduate students Tim Black, Bobby Wilson, and Max Engelstein for many helpful conversations about group theory and analysis.

Finally, I am deeply grateful to my family for their love and support—to my parents and my wife, Madlen–and to my daughter, Tara, for putting it all in perspective.

ABSTRACT

We develop new structure theory for highly regular combinatorial objects, including Steiner designs, strongly regular graphs, and coherent configurations. As applications, we make progress on old problems in algebraic combinatorics and the theory of permutation groups, and break decades-old barriers on the complexity of the algorithmic Graph Isomorphism problem.

A central aspect of our structural contributions is the discovery of clique geometries in regular structures. A second aspect is bounds on the rate of expansion of small sets.

In the case of Steiner designs, we give a $n^{O(\log n)}$ bound on the number of automorphisms where n is the number of points. This result is nearly optimal in two ways: it essentially matches the number of automorphisms in affine or projective space, and we show that the bound does not extend to the broader class of balanced incomplete block designs. The line-graphs of Steiner designs are strongly regular graphs, and in fact are one of the cases of Neumaier's classification of strongly regular graphs. We bound the number of reconstructions of a Steiner design from its line-graph in order to apply our automorphism bound for Steiner designs to this class of strongly regular graphs, and show that this class of strongly regular graphs has at most $\exp(\widetilde{O}(v^{1/14}))$ automorphisms, where v is the number of vertices and the $\widetilde{O}$ hides polylogarithmic factors.

We give an $\exp(\widetilde{O}(1+\lambda/\mu))$ bound on the number of automorphisms of any nontrivial $\mathrm{SR}(v,\rho,\lambda,\mu)$ strongly regular graph. (Here, v is the number of vertices, ρ is the valency, and λ and μ are the number of common neighbors of a pair of adjacent and nonadjacent vertices, respectively.) As a consequence, we obtain a quasipolynomial bound on the number of automorphisms when $\rho = \Omega(v^{5/6})$.

In further study of the structure of the automorphism groups of $\mathrm{SR}(v,\rho,\lambda,\mu)$ graphs, we find a Γ_μ subgroup of index $v^{O(\log v)}$ (i.e., a subgroup of index $v^{O(\log v)}$ for which all composition factors are subgroups of S_μ) with known exceptions. In combination with our bound on the number of automorphisms and an earlier bound due to Spielman, we find a

Γ_d subgroup of the automorphism group of index v^d, where $d = \widetilde{O}(v^{1/5})$, again with known exceptions.

We classify the primitive coherent configurations with not less than $\exp(\widetilde{O}(v^{1/3}))$ automorphisms, where v is the number of vertices. As a corollary to our combinatorial classification result, we infer a classification of large primitive permutation groups, previously known only through the Classification of Finite Simple Groups.

As a consequence of the combinatorial structure underlying our bounds for the automorphism groups, we give corresponding bounds for the time-complexity of deciding isomorphism. When we bound the order of the automorphism group, our time-complexity bounds are identical to the bounds on the order. From our study of the composition factors of automorphism groups of strongly regular graphs, we obtain a $v^{\mu+O(\log v)}$ and a $\exp(\widetilde{O}(v^{1/5}))$ bound on the time-complexity of deciding isomorphism of strongly regular graphs.

Chapter 1

INTRODUCTION

1.1 Regularity versus Symmetry

A central theme of this thesis is the tension between regularity and symmetry in combinatorial structures. Norman Biggs distinguishes the two in the introduction to his classic text on algebraic graph theory:

> A symmetry property of a graph is related to the existence of automorphisms... A regularity property is defined in purely numerical terms. Consequently, symmetry properties induce regularity properties, but the converse is not necessarily true. [Big93]

In fact, paradoxically, high degrees of regularity seem to inhibit symmetry. Latin squares are typical. A Latin square is an $n \times n$ array of the symbols $1 \leq i \leq n$ such that every symbol appears exactly once in each row and column. One demonstration of the regularity of Latin squares is that they are the simplest nontrivial transversal designs, the line-graphs of which are strongly regular (see Chapter 2 for definitions). On the other hand, almost all Latin squares have trivial automorphism groups! (This result is implicit in [Bab80a], but see also [Cam15, MW05].) Furthermore, thanks to their quasigroup structure, no Latin square has more than $n^{\log_2 n}$ automorphisms.[1]

By contrast, some of the quintessential objects of algebraic combinatorics have exponentially many automorphisms. For example, the Johnson scheme $\mathfrak{J}(m,k)$ is a primitive coherent configuration on $v = \binom{m}{k}$ vertices with $m! = \exp(\Omega(v^{1/k}))$ automorphisms, and the Hamming scheme $\mathfrak{H}(m,d)$ is a primitive coherent configuration on $v = m^d$ vertices with $d!(m!)^d = \exp(\Omega(v^{1/d}))$ automorphisms.

1. Mathematicians from many disciplines might be surprised that a (superpolynomial!) $n^{\log_2 n}$ bound would be "small." Indeed, $n^{\log_2 n}$ is tiny compared the $(n!)^3$ possible permutations of the rows, columns, and symbols.

The main contribution of this thesis is to show that in fact with the exception of the Johnson and Hamming schemes, along with their close relatives, regularity imposes strong constraints on the order and structure of an automorphism group.

In particular, we make progress toward Babai's conjecture that in fact the Johnson and Hamming schemes, along with their interpolations, are the *only* primitive coherent configurations with exponentially many automorphisms. We prove that all nontrivial primitive coherent configurations, other than the Johnson scheme $\mathfrak{J}(m,2)$ and Hamming scheme $\mathfrak{H}(m,2)$, have at most $\exp(O(v^{1/3}\log^{7/3} v))$ automorphisms, where v is the number of vertices. Our classification is the first improvement to Babai's 1981 bound of $\exp(O(v^{1/2}\log^2 v))$ for the number of automorphisms of a nontrivial primitive coherent configuration.

As a corollary, we classify the largest primitive permutation groups (those of order $\exp(\Omega(v^{1/3}\log^{7/3} v))$. This permutation group classification was previously known only through the Classification of Finite Simple Groups [Cam81].

We obtain even stronger bounds in the cases of strongly regular graphs and Steiner 2-designs.

For strongly regular graphs, we give the first quasipolynomial bound on the number of automorphisms in an entire interval of the exponent of the valency parameter, improving Babai's $\exp(O(v^{1/6}\log^2 v))$ bound in this range of the parameters. This quasipolynomial bound follows from a more general $\exp(O((1+\lambda/\mu)\log^4 v))$ bound on the number of automorphisms of a strongly regular graph, where λ, resp. μ, is the number of common neighbors of a pair of adjacent, resp. nonadjacent, vertices. In addition, we give a strong structural constraint on the automoprhism group when μ is small. With the exception of Johnson and Hamming graphs, we show that the point-stablizer in the automorphism group of some $O(\log v)$ vertices has the property that all composition factors are subgroups of S_μ. Combined with a bound by Spielman on the order of the automorphism group [Spi96], we conclude that all composition factors in the point-stablizier of some d vertices lie in S_d, where $d = O(v^{1/5}\log^{2/5} v)$ (again, with Johnson and Hamming graphs as exceptions).

For nontrivial Steiner 2-designs, we give an essentially tight $n^{O(\log n)}$ bound on the number of automorphisms, where n is the number of points. The previous best bound was $\exp(\widetilde{O}(n^{1/2}))$, due to Babai and Pyber [BP94] and independently to Spielman [Spi96]. We note that the line-graphs of Steiner 2-designs are strongly regular—indeed, they form one of the cases in Neumaier's classification of strongly regular graphs—and that the line-graph of a trivial Steiner 2-design is a Johnson graph. As an application of our automorphism bound for Steiner 2-designs, we give an $\exp(O(v^{1/14}\log^{22/7} v))$ bound on the number of automorphisms of a line-graph of a Steiner 2-design where v is the number of vertices.

Our analysis extends to Steiner t-designs; however, we prove that no such generalization is possible for balanced incomplete block designs. In particular, we construct $\mathrm{S}_2(2,3,n)$ designs with $2^{\Omega(n)}$ automorphisms.

Precise statements are given in Chapter 2.

1.2 Combinatorial Structure Theory

Our bounds on the orders of automorphism groups of regular combinatorial objects are built on new structure theory we have developed. For every class of structures we consider, our bounds on the number of automorphisms rely in part on new estimates for the rate of expansion of small sets.

One of the elements of our structure theory for Steiner designs is an addressing scheme that produces a hierarchy of increasing sets of pairwise independent, uniformly distributed points. This scheme expresses the structural homogeneity of Steiner designs in a new way. Separately, we bound the number of possible reconstructions of a Steiner design (in fact, more generally, of a partial geometry) from its strongly regular line-graph, allowing us to apply our bound on the number of automorphisms of a Steiner design to this class of strongly regular graphs.

For "sub-amply regular graphs," a class generalizing distance-regular graphs (including strongly regular graphs), we bound the number λ of common neighbors of a pair of vertices.

Our work substantially improves the known bounds on λ for a wide range of parameters, even in the special case of strongly regular graphs. As a consequence, we give improved estimates of the small-scale vertex expansion in such graphs. As a corollary to our bound on λ, we expand the range of parameters of distance-regular graphs known to be "asymptotically Delsarte," i.e., graphs with a clique geometry whose order asymptotically meets Delsarte's upper bound.

We also obtain additional estimates on vertex expansion of moderately sized sets in strongly regular graphs, effective on a larger scale.

In the case of strongly regular graphs, our structural results both build on and augment Neumaier's classification of strongly regular graphs. However, no generalization of Neumaier's theory to primitive coherent configurations has been known. We provide a weak generalization, sufficient for our purposes.

One of the central elements of our structural study of coherent configurations is the discovery of clique geometries in a certain range of parameters. Clique geometries are collections of maximal cliques such that every edge belongs to a unique clique. The structure provided by a clique geometry is particularly useful to our project of classifying the primitive coherent configurations with many automorphisms, because it allows the separation of exceptional families of highly symmetrical coherent configurations from "quasirandom" coherent configurations. Except when the coherent configuration resembles a Johnson or Hamming scheme, the clique geometry ensures that there is a large family of induced claws which break symmetry and allow us to bound the number of automorphisms. When clique geometries are not present, we bound the rank of the configuration.

Our structural results are described in Chapter 2, and developed in detail in Chapter 5 and Sections 4.1, 6.3, and 7.2.

1.3 The Isomorphism Problem

The Graph Isomorphism problem is the computational problem of deciding whether a given pair of graphs is isomorphic. This problem is of great interest to complexity theory since it is one of a very small number of natural problems in NP of intermediate complexity status—it is unlikely to be NP-complete but not known to be solvable in polynomial time.

Our analyses of the orders of automorphism groups yield corresponding time-complexity bounds for deciding isomorphism. In particular, we show that the simple individualization and refinement process gives an $n^{O(\log n)}$-time algorithm for deciding isomorphism of Steiner designs with n points, a quasipolynomial-time algorithm for deciding isomorphism of strongly regular graphs in a certain range of the parameters, and an $\exp(O(v^{1/3}\log^{7/3} v))$-time algorithm for deciding isomorphism of primitive coherent configurations with v vertices. Furthermore, we show that combining individualization and refinement with Luks's group-theoretic divide-and-conquer method gives a $v^{\mu+O(\log v)}$-time algorithm, as well as an $\exp(O(v^{1/5}\log^{2/5} v))$-time algorithm for deciding isomorphism of strongly regular graphs. (Here, μ is the number of common neighbors of a pair of non-adjacent vertices.)

Meanwhile, in a major development, Babai has announced a quasipolynomial-time algorithm for deciding isomorphism of general graphs [Bab15]. This result supersedes many of our time-complexity bounds; however, none of the results of Sections 1.1 and 1.2 follow from Babai's algorithmic result. We will contrast Babai's results with our own, and explore the connections between them, in Chapter 9. We shall indicate how further work along the lines of our structural analysis of primitive coherent configurations might lead to substantial simplification of Babai's algorithm.

1.4 Acknowledgement of Collaborations

Most of the results in this thesis originally appeared in joint papers with various subsets of László Babai, Xi Chen, Xiaorui Sun, and Shang-Hua Teng. In this section we indicate the

papers where these joint results have appeared or will appear. A simultaneous thesis by Sun will include disjoint elements from these joint works. Below, we indicate which technical developments appear in each thesis.

The analysis of Steiner designs in Chapter 4 is joint work with Babai, and was originally outlined in an extended abstract in the 2013 ACM Symposium on Theory of Computing [BW13]. The reconstruction bounds for partial geometries proved in Section 5.4 appears in the journal version of the same paper [BW16]. A simultaneous, independent proof of the $n^{O(\log n)}$ bound on the number of automorphisms of a Steiner design, due to Chen, Sun, and Teng, was outlined in the same conference proceedings [CST13a], and appears in [Sun16].

The $\exp(\widetilde{O}(1+\lambda/\mu))$ bound on the number of automorphisms of a strongly regular graph in Section 6.4 was originally outlined in an extended abstract in the 2013 IEEE Symposium on Foundations of Computer Science, coauthored with Babai, Chen, Sun, and Teng [BCS$^+$13, Section 6]. A distinct proof of a consequence, an $\exp(\widetilde{O}(\sqrt{v/\rho}))$ bound on the number of automorphisms, was outlined in Section 7 of the same extended abstract, and appears in [Sun16]. The proof in Section 6.5 that the point-stabilizer of some $O(\log v)$ vertices in the automorphism group of a strongly regular graph is a Γ_μ group was also originally outlined in Section 4 of the same 2013 extended abstract [BCS$^+$13]. The journal version of the same paper includes the quasipolynomial bound on the number of automorphisms of a strongly regular graph with valency $\rho \geq v^{5/6}$, Corollary 2.4.3.

The bound on the parameter λ of a "sub-amply regular graph" proved in Section 5.1, and the analysis of clique geometries in distance-regular graphs in Section 5.2, originally appeared in joint work with Babai [BW15].

The automorphism bound for primitive coherent configurations was originally outlined in an extended abstract in the 2015 ACM Symposium on Theory of Computing, coauthored with Sun [SW15a]. The elements of its proof described in Section 5.3 and Chapter 7 appear in the journal version of the same paper [SW15b]. Separate elements of the proof of this automorphism bound appear in Sun's Ph.D. thesis [Sun16] (see Sections 2.8 and 5.3, and

Chapter 7 of the present thesis).

1.5 Organization of the Thesis

We now outline the structure of this thesis. In Chapter 2, we introduce the notation used throughout this thesis, and define the basic objects of study. We also give precise statements for our main results for the automorphism groups of these objects, as well as giving context for these results, for example by explaining Babai's conjectured classification of primitive coherent configurations. A classic tool that can be used to find a base of an automorphism group, the individualization/refinement heuristic, is briefly described in Chapter 3. Our analyses of individualization/refinement, described in Chapters 4, 6, and 7, are the basic tools we use to bound the number of automorphisms of Steiner designs, strongly regular graphs, and primitive coherent configurations, respectively. Much of our structure theory, on which these analyses are built, is developed in Chapter 5, but elements of our structural contributions also appear in Chapters 4, 6, and 7. The consequences for primitive permutation groups of our combinatorial classification of primitive coherent configurations are described in Chapter 8. In Chapter 9, we establish our results for the Graph Isomorphism problem, and explore the connection between our results and Babai's recent breakthrough on the general Graph Isomorphism problem.

Chapter 2

DEFINITIONS AND STATEMENT OF RESULTS

We now introduce the notation that will be used throughout this thesis, and define the highly regular structures we study. We give statements of our main results on the automorphism groups of regular combinatorial objects, and outline many of our contributions to the structure theory of these objects. Some of the more technical aspects of our structure theory will be stated in later sections. Discussion of the consequences of our results for the Graph Isomorphism problem will be deferred to Chapter 9.

2.1 Basic Notation and Terminology

All combinatorial structures considered in this thesis are finite.

An *incidence structure* is a triple $\mathfrak{X} = (\mathcal{P}, \mathcal{B}, \mathcal{I})$, where $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{B}$. The set $\mathcal{P}$ is the set of "points," $\mathcal{B}$ is the set of "blocks" or "lines," and $\mathcal{I}$ is the "incidence relation." We say $p \in \mathcal{P}$ is *incident on* or *with* $B \in \mathcal{B}$, and vice versa, if $(p, B) \in \mathcal{I}$. We often identify the block B with the set of points incident on B, in which case we say the block *contains* the points with which it is incident. The size of a block (equivalently, the length of a line) is the number of points it contains. We say two blocks, or lines, intersect if they contain a common point. Graphs are examples of incidence structures, with blocks given by the edges.

The *line-graph* $L(\mathfrak{X})$ of the incidence structure $\mathfrak{X}$ is the graph whose vertices are the lines of $\mathfrak{X}$, with adjacency when the lines intersect.

If G is a graph, we always denote by $V(G)$ the set of vertices of G, and by $E(G)$ the set of edges of G. If $x, y \in V(G)$, we write $x \sim y$ if x and y are adjacent.

If $x \in V(G)$, we write $G(x)$ for the set of neighbors of x (out-neighbors, if G is directed). We write $G^+(x) = G(x) \cup \{x\}$. Given a set $A \subseteq V(G)$, we write $G(A) = \bigcup_{x \in A} G(x)$.

The *complete graph* K_n is the graph on n vertices in which every pair of distinct vertices is adjacent. The *complete bipartite graph* $K_{m,n}$ is the graph on $m + n$ vertices, partitioned

into a set A of cardinality m and a set B of cardinality n, such that $a \sim b$ for every pair of vertices $a \in A$ and $b \in B$.

Given a (directed) graph G on n vertices, its *adjacency matrix* $A = A(G)$ is the $n \times n$ matrix whose (i, j)th entry is 1 if there is an edge from the ith vertex to the jth vertex, and 0 otherwise. The *eigenvalues* of G are the eigenvalues of $A(G)$. We refer the reader to [GR01] for an overview of the linear algebra of graphs.

We write $\mathbb{F}_q$ for the finite field with q elements. We write $\log n = \log_2 n$. We use the notation $[n] = \{0, \ldots, n-1\}$.

2.2 The Asymptotic Perspective

In this thesis, we are are interested primarily in the *asymptotic* behavior of combinatorial structures as they grow larger. To interpret asymptotic inequalities involving the parameters of a finite structure, we think of the structure as belonging to an infinite family in which the asymptotic inequalities hold.

For functions $f, g : \mathbb{N} \to \mathbb{R}_{>0}$, we write $f(n) = O(g(n))$ if there is some constant C such that $f(n) \leq Cg(n)$, and we write $f(n) = \Omega(g(n))$ if $g(n) = O(f(n))$. In order to simplify some expressions ,we will write $f(n) = \widetilde{O}(g(n))$ if there is a constant c such that $f(n) = O(g(n) \log^c n)$. We write $f(n) = \Theta(g(n))$ if $f(n) = O(g(n))$ and $f(n) = \Omega(g(n))$. We write $f(n) = o(g(n))$ if for every $\varepsilon > 0$, there is some N_ε such that for $n \geq N_\varepsilon$, we have $f(n) < \varepsilon g(n)$. We write $f(n) = \omega(g(n))$ if $g(n) = o(f(n))$. We use the notation $f(n) \sim g(n)$ for asymptotic equality, i.e., $\lim_{n\to\infty} f(n)/g(n) = 1$. The asymptotic inequality $f(n) \lesssim g(n)$ means $g(n) \sim \max\{f(n), g(n)\}$.

2.3 Steiner Designs

Definition 2.3.1. A *Steiner t-design* $\mathrm{S}(t, k, n)$, with $t \leq k < n$, is an incidence structure on n points, with lines of size k, such that for every t points, there is a unique line incident

with all of them.

An $\mathrm{S}(t,k,n)$ design is *trivial* if $t = k$.

A celebrated theorem of Wilson states that $\mathrm{S}(2,k,n)$ designs exist for all k, and all sufficiently large n satisfying a divisibility condition in terms of k [Wil72a, Wil72b, Wil75]. A recent breakthrough of Keevash extends this result to $\mathrm{S}(t,k,n)$ designs [Kee14].

Steiner 2-designs are the most familiar. For example, the points and lines of d-dimensional affine space over $\mathbb{F}_q$ give an $\mathrm{S}(2,q,q^d)$ design, and d-dimensional projective space over $\mathbb{F}_q$ gives an $\mathrm{S}(2,q+1,(q^{d+1}-1)/(q-1))$ design. Our main result concerning Steiner designs is the following Theorem 2.3.2. A more detailed statement appears as Theorem 4.0.1, and a corollary concerning the time-complexity of deciding isomorphism as Theorem 9.3.1.

Theorem 2.3.2. *A nontrivial* $\mathrm{S}(t,k,n)$ *has at most* $n^{t+O(\log n)}$ *automorphisms.*

The essence of the difficulty is in solving the problem for $t = 2$; our solution then extends to arbitrary t by a standard "derived design" argument.

A simultaneous, independent proof of Theorem 2.3.2 in the essential case $t = 2$, due to Chen, Sun, and Teng, appears in [CST13a], and will also appear in [Sun16].

The bound of Theorem 2.3.2 is tight up to the hidden constant, even when $t = 2$, as demonstrated by affine and projective spaces over finite fields. The best previously known bound on the order of the automorphism group for the essential case $t = 2$ was $\exp(O(n^{1/2}\log^{3/2} n))$, obtained in the 1990s independently by Babai and Pyber [BP94] and by Spielman [Spi96]. In the special case of a "Steiner triple system," or $\mathrm{S}(2,3,n)$ design, the $n^{\log n}$ bound that follows immediately from the quasigroup structure was observed by Miller in 1978 [Mil78].

It is natural to ask whether Theorem 2.3.2 generalizes to "balanced incomplete block designs." A *balanced incomplete block design* $\mathrm{S}_\lambda(t,k,n)$ is an incidence structure on n points, with blocks of size k, such that for every t points, there are exactly λ blocks incident with all of them. In particular, a $\mathrm{S}_1(t,k,n)$ design is exactly an $\mathrm{S}(t,k,n)$ Steiner t-design.

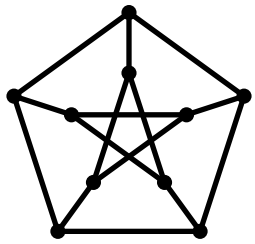

Figure 2.1: The Petersen graph, a $\mathrm{SR}(10, 3, 0, 1)$ strongly regular graph.

We show in Section 4.3 that no generalization of Theorem 2.3.2 to balanced incomplete block designs is possible by constructing a family of $\mathrm{S}_2(2, 3, n)$ designs with $2^{n/2}$ automorphisms.

Our proof of Theorem 2.3.2 makes use of a concentration inequality based on a pairwise independent addressing scheme for Steiner 2-designs. The addressing scheme provides a new expression of the structural homogeneity of Steiner 2-designs, absent in more general block designs. We describe this addressing scheme in Chapter 4, where we prove Theorem 2.3.2.

2.4 Strongly Regular Graphs

Definition 2.4.1. A *strongly regular graph* $\mathrm{SR}(v, \rho, \lambda, \mu)$ is a ρ-regular graph on v vertices such that every adjacent (resp. nonadjacent) pair of distinct vertices has exactly λ (resp. μ) common neighbors.

The *trivial* strongly regular graphs are disjoint unions of cliques of the same order, and the complements of such. Nontrivial examples include the famous Petersen graph (Fig. 2.1) and the Hoffman-Singleton graph [HS60].

Strongly regular graphs, along with their generalizations, coherent configurations (see Section 2.5), are an important class of objects studied in algebraic combinatorics [Big93, GR01, BCN89].

In Chapter 6, we shall prove the following bound on the number of automorphisms of a strongly regular graph. A more detailed statement appears as Theorem 6.4.1, and a corollary

concerning the time-complexity of deciding isomorphism as Theorem 9.3.3.

Theorem 2.4.2. *Let G be a nontrivial* $\mathrm{SR}(v, \rho, \lambda, \mu)$ *graph with $\rho \leq v/2$. Then G has at most* $\exp(O((1 + \lambda/\mu) \log^4 v))$ *automorphisms.*

We remark that the complement of a strongly regular graph is again strongly regular, so the assumption $\rho \leq v/2$ is benign.

In order to be effective, Theorem 2.4.2 requires a bound on λ. In this thesis, we will employ three different bounds, effective in different ranges of the valency parameter ρ (see Section 6.1). We remark on the utility of bounds on the parameter λ in Section 2.8.

Using in Theorem 2.4.2 a bound on λ proved by Pyber [Pyb14], we obtain the following corollary (see Section 6.2).

Corollary 2.4.3. *Let G be a nontrivial* $\mathrm{SR}(v, \rho, \lambda, \mu)$ *graph with $\rho \leq v/2$. If $\rho = \Omega(v^{5/6})$, then* $|\operatorname{Aut}(G)| \leq \exp(O(\log^4 v))$.

Using a second bound on λ, and combining Theorem 2.4.2 with an earlier automorphism bound due to Spielman [Spi96], we remove the dependence on the parameters ρ, λ, and μ, obtaining an $\exp(\widetilde{O}(v^{1/4}))$ bound on the number of automorphisms, with known exceptions. This automorphism bound, and a stronger bound due to Chen, Sun, and Teng [CST13b], are described in Section 2.4.2 below.

2.4.1 Neumaier's Classification

We briefly describe the spectra of strongly regular graphs, and some important families of strongly regular graphs. We then state Neumaier's classification of strongly regular graphs. We refer the reader to [Neu79, Neu82] for proofs.

Nontrivial strongly regular graphs have exactly three eigenvalues. Indeed, a connected regular graph is a nontrivial strongly regular graph if and only if it has three distinct eigenvalues (see [GR01] for an overview of strongly regular graph spectra). Since $\mathrm{SR}(v, \rho, \lambda, \mu)$ graphs are ρ-regular, their greatest eigenvalue is ρ. Of the remaining eigenvalues, one is

positive and the other is negative—we denote the remaining positive eigenvalue by θ, and the negative eigenvalue by τ.

A *conference graph* is a $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph with $\rho = (v-1)/2$, $\lambda = (v-5)/4$, and $\mu = (v-1)/4$. These are the only strongly regular graphs that may have noninteger eigenvalues.

The line-graphs of "partial geometries" are a particularly rich source of strongly regular graphs. A *partial geometry* $\mathrm{PG}(r, k, \alpha)$ is an incidence structure on n points, satisfying the following four axioms.

(i) Every line is incident on exactly k points.

(ii) Every point is incident on exactly r lines.

(iii) For any pair of distinct points, at most one line is incident with both.

(iv) For every nonincident point p and line ℓ, there are exactly α lines incident with p which intersect ℓ.

A Steiner $\mathrm{S}(2, k, n)$ design is exactly a $\mathrm{PG}(r, k, k)$ partial geometry, where $r = (n-1)/(k-1)$. Equally important in the study of strongly regular graphs are "transversal designs." A *transversal design* $\mathrm{TD}(r, k)$ is a $\mathrm{PG}(r, k, k-1)$. As with a Steiner design, we call a $\mathrm{TD}(r, k)$ design *trivial* when $k = 2$.

The line-graph of a $\mathrm{PG}(r, k, \alpha)$ geometry is always strongly regular (see Proposition 5.4.1). We remark that the negative eigenvalue of the line-graph of a $\mathrm{PG}(r, k, \alpha)$ is $\tau = -k$.

For any fixed integer $k \geq 2$, there are infinitely many $\mathrm{S}(2, k, n)$ designs (by Wilson's theorem [Wil75]), and infinitely many $\mathrm{TD}(r, k)$ designs.[1] Hence, there are infinitely many strongly regular graphs with least eigenvalue $-k$.

In fact, all but finitely many strongly regular graphs with least eigenvalue $-k$ an integer are line-graphs of $\mathrm{S}(2, k, n)$ designs or $\mathrm{TD}(r, k)$ designs. Neumaier gives the following classification.

1. For example, a simple construction based on finite field arithmetic gives a $\mathrm{TD}(q, q+1)$ design for every prime power q, and every $\mathrm{TD}(r, k)$ design induces a $\mathrm{TD}(r, k-1)$ design.

Theorem 2.4.4 (Neumaier's classification [Neu79]). *Let G be a nontrivial* $\mathrm{SR}(v, \rho, \lambda, \mu)$ *graph. Then at least one of the following is true:*

(a) G is a conference graph;

(b) G is the line-graph of a transversal design;

(c) G is the line-graph of a Steiner design;

(d) G satisfies an eigenvalue inequality called the claw bound *(see Theorem 6.1.5)*

We do not state the full claw bound here to avoid interrupting the narrative. In fact, we shall only use the claw bound through a simple asymptotic consequence, observed by Spielman [Spi96]: the bound $\lambda = o(\rho)$ (Theorem 6.1.7 (iii)).

2.4.2 Bounds for the Automorphism Group

In addition to the trivial strongly regular graphs, two other families provide easy examples of strongly regular graphs with an enormous number of automorphisms: the line-graphs of trivial Steiner designs and of trivial transversal designs.

The line-graph of an $\mathrm{S}(2, 2, n)$ design is called the *triangular graph* $T(n)$. It is exactly the line-graph of the complete graph K_n, and has $v = \binom{n}{2}$ vertices, with $\binom{n}{2} = \exp(\Theta(\sqrt{v}\log v))$ automorphisms. The line-graph of a $\mathrm{TD}(r, 2)$ design is called the *lattice graph* $L_2(r)$. It is exactly the line-graph of the complete bipartite graph $K_{r,r}$ with equal parts, and $v = r^2$ vertices with $2(r!)^2 = \exp(\Theta(\sqrt{v}\log v))$ automorphisms.

In 1979, Babai proved that nontrivial strongly regular graph cannot have automorphism groups of order far exceeding that of the triangular and lattice graphs. More precisely, he gave a $\exp(O(\sqrt{v}\log^2 v))$ bound on the number of automorphisms of a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph, essentially matching the number of automorphisms of the triangular and lattice graphs. In fact, Babai proved the following theorem, from which the stated bound follows, since $\rho \geq \sqrt{v-1}$ for every strongly regular graph.

Theorem 2.4.5 (Babai [Bab80b]). *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph with $\rho \leq v/2$. Then $|\operatorname{Aut}(G)| \leq \exp(O((v/\rho)\log^2 v))$.*

In fact, Babai conjectures that the triangular and lattice graphs are the *only* nontrivial strongly regular graphs with exponentially many (i.e., at least $\exp(v^{\varepsilon})$) automorphisms (see Conjecture 2.5.5 for the precise statement of an even stronger version of this conjecture). Spielman made progress toward the conjecture in 1996, showing that the triangular and lattice graphs are indeed exceptional.

Theorem 2.4.6 (Spielman [Spi96]). *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph, which is not a triangular or lattice graph. Then $|\operatorname{Aut}(G)| \leq \exp(O(v^{1/3}\log^2 v))$.*

Spielman organizes his analysis around Neumaier's classification. In particular, since $\rho = (v-1)/2$ in Theorem 2.4.4 (a), these graphs have at most at most $v^{O(\log v)}$ automorphisms by Theorem 2.4.5. Spielman furthermore observes that when G satisfies (b) or (c) of Theorem 2.4.4, either G can be uniquely reconstructed from the corresponding design $\mathfrak{X}$ and $\operatorname{Aut}(G) \cong \operatorname{Aut}(\mathfrak{X})$, or G satisfies the claw bound (d) (see Proposition 6.1.6). Hence, by applying bounds on the number of automorphisms of Steiner and transversal designs, Spielman reduces his analysis to the case of graphs satisfying the claw bound, where his estimate on the parameter λ applies.

We go beyond Spielman's analysis of the order of automorphism groups of strongly regular graphs in two ways. First, we go beyond the unique reconstruction bound for line-graphs of partial geometries. Even when unique reconstruction is impossible, we bound the number of possible reconstructions of a partial geometry from its line-graph (see Theorems 2.7.10 and 2.7.11). Combined with Theorem 2.3.2, we obtain the following overall bound on the number of automorphisms for strongly regular graphs in cases (b) or (c) of Neumaier's classification.

Theorem 2.4.7. *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph. If G is the line-graph of a nontrivial Steiner design, then $|\operatorname{Aut}(G)| \leq \exp(\widetilde{O}(v^{1/14}))$. If G is the line-graph of a nontrivial*

transversal design, then $|\operatorname{Aut}(G)| \leq \exp(\widetilde{O}(v^{1/11}))$.

Theorem 2.4.7 is proved in Section 6.2.

Furthermore, we improve the bound on the number of automorphisms of a strongly regular graph in the general case.

Theorem 2.4.8. *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph, which is not a triangular or lattice graph. Then $|\operatorname{Aut}(G)| \leq \exp(\widetilde{O}(v^{1/4}))$.*

We prove Theorem 2.4.8 in Section 6.2 by employing both Spielman's method and our Theorem 2.4.2 in different ranges of the parameters of the strongly regular graph. We also require the bound $\lambda = O(\sqrt{\rho\mu} + \sqrt{n})$, stated in Section 2.7.1 below.

Meanwhile, the following stronger bound on the number of automorphisms of a strongly regular graphs has been proved by Chen, Sun, and Teng [Sun16, CST13b].

Theorem 2.4.9 (Chen–Sun–Teng [Sun16, CST13b])**.** *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph, which is not a triangular or lattice graph. Then $|\operatorname{Aut}(G)| \leq \exp(\widetilde{O}(v^{9/37}))$.*

In addition to our bounds on the order of the automorphism group of a strongly regular graph, we establish a subtler constraint.

Following Luks [Luk82], we denote by Γ_d the class of groups all of whose composition factors are isomorphic to subgroups of S_d.

Theorem 2.4.10. *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph, which is not a triangular or lattice graph. Then $\operatorname{Aut}(G)$ has a Γ_μ subgroup of index at most $v^{O(\log v)}$.*

We prove Theorem 2.4.10 in Section 6.5.

Theorem 2.4.10 strongly constrains the automorphism group of a strongly regular graph when μ is small. Combining the theorem with the above bounds on the number of automorphisms, we obtain the following overall result, proved in Section 6.2.

Corollary 2.4.11. *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph, which is not a triangular or lattice graph. Then $\operatorname{Aut}(G)$ has a Γ_d subgroup of index at most v^d, where $d = O(v^{1/5} \log^{2/5} v)$.*

We remark that Babai has established a related constraint on the automorphism group of a strongly regular graph. The *thickness* $\theta(\Gamma)$ of a group Γ is the largest t such that there exist groups $\Psi \lhd \Phi \leq \Gamma$ with $\Phi/\Psi \cong A_t$. In particular, Γ_d groups have thickness at most d.

Theorem 2.4.12 (Babai [Bab14])**.** *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph, which is not a triangular or lattice graph. Then $\theta(\mathrm{Aut}(G)) \leq O(\log^2 n / \log\log n)$.*

Note that Theorem 2.4.12 does not imply Corollary 2.4.11—in particular, a group with thickness d need not be a Γ_d group. Indeed, by a result of Feit and Tits [FT78] (cf. [BPS09]), it follows that $\theta := \theta(\mathrm{PSL}_n(\mathbb{F}_2)) \leq n + 2$ for $n \geq 7$. On the other hand, with finitely many exceptions, the minimum degree of a (faithful) permutation representation of $\mathrm{PSL}_n(\mathbb{F}_2)$ is $2^n - 1$ [Coo78]. In particular, $\mathrm{PSL}_n(\mathbb{F}_2)$ is not a Γ_d group for any $d < 2^{\theta-2} - 1$.

2.5 Primitive Coherent Configurations

Definition 2.5.1. A *configuration* of rank r is a pair $\mathfrak{X} = (V, c)$, where V is a finite set and $c : V \times V \to [r]$ is a map such that $c(x, x) \neq c(y, z)$ for any $x, y, z \in V$ with $y \neq z$, and for all $i \in [r]$ there is $i^* \in [r]$ such that $c(x, y) = i$ if and only if $c(y, x) = i^*$.

The elements of V are called *vertices*, and c is called the *coloring*. A configuration can be viewed as a vertex- and edge-colored complete digraph such that vertex- and edge-colors never coincide, and the color of an edge determines the color of its reverse. The colors are the elements of $\{0, \ldots, r-1\}$. The diagonal colors $c(x, x)$ are the vertex-colors and the off-diagonal colors are the edge-colors.

Definition 2.5.2. A configuration is *coherent* if for all $i, j, k < r$ there is a *structure constant* p^i_{jk} such that for all vertices $x, y \in V$ with $c(x, y) = i$, there are exactly p^i_{jk} vertices z such that $c(x, z) = j$ and $c(z, y) = k$.

Our main result for coherent configurations, Theorem 2.5.4 below, is a classification of those coherent configurations with not less than $\exp(\widetilde{O}(v^{1/3}))$ automorphisms, where v is the number of vertices.

The term "coherent configuration" was coined by Donald Higman in 1969 [Hig70], but the essential objects are older. Coherent configurations effectively appeared for the first time in Schur's 1933 paper [Sch33] as a tool for understanding permutation groups. Later, independent work by statisticians such as Bose and Shimamoto [BS52] developed the concept from a combinatorial perspective in order to study partially balanced incomplete block designs. In a third line of work motivated by the Graph Isomorphism problem, Weisfeiler and Leman defined coherent configurations for the first time in their full generality [WL68]. In the intervening years, coherent configurations, and association schemes in particular, have become basic objects of study in algebraic combinatorics [BI84, BCN89, Bai04, Zie10].

Given a coherent configuration $\mathfrak{X} = (V, c)$, we denote by R_i the set of ordered pairs $(x, y) \in V \times V$ of color $c(x, y) = i$. For each edge-color i, the directed graph $\mathfrak{X}_i = (V, R_i)$ is the *color-i constituent digraph*. When $i = i^*$, we view its constituent (di)graph as an undirected graph.

Definition 2.5.3. A coherent configuration $\mathfrak{X}$ is *homogeneous* if there is only one vertex color. It is *primitive* if it is homogeneous, and each constituent digraph is strongly connected.

A *trivial* coherent configuration is a configuration of rank 2.

Given a (non-complete, non-empty) graph G with vertex set V, we define $\mathfrak{X}(G)$ as the rank 3 configuration on V whose constituent graphs are G and its complement. If G is complete or empty, $\mathfrak{X}(G)$ is the trivial configuration on V.

The configuration $\mathfrak{X}(G)$ is coherent if and only if G is strongly regular. Hence, strongly regular graphs correspond to coherent configurations of rank at most 3 with undirected constituent graphs.

The following automorphism bound, proved in Chapter 7, is our main result for coherent configurations.

Theorem 2.5.4. *Let $\mathfrak{X}$ be a nontrivial primitive coherent configuration on v vertices. Then either $\mathfrak{X} = \mathfrak{X}(G)$ for G the triangular or lattice graph, or $|\operatorname{Aut}(\mathfrak{X})| \leq \exp(O(v^{1/3} \log^{7/3} v))$.*

The primitive coherent configurations corresponding to the triangular and lattice graphs belong to a larger family of primitive coherent configurations with exponentially many automorphisms. The *Johnson scheme* $\mathfrak{J}(m,k)$, where $m > 2k$, is the primitive coherent configuration (V,c), where V is the collection of k-subsets of $[m]$, and $c(A,B) = |A \setminus B|$. The *Hamming scheme* $\mathfrak{H}(m,d)$ is the primitive coherent configuration (V,c) where V is the set of words of length m from an alphabet of size d, and $c(w_1,w_2)$ is the Hamming distance between w_1 and w_2. In particular, $\mathfrak{X}(T(m)) = \mathfrak{J}(m,2)$ and $\mathfrak{X}(L_2(m)) = \mathfrak{H}(m,d)$.

The Johnson scheme $\mathfrak{J}(m,k)$ has $v = \binom{m}{k}$ vertices and $m! = \exp(\Omega(v^{1/k}\log v))$ automorphisms. The Hamming scheme $\mathfrak{H}(m,d)$ has $v = m^d$ vertices and $d!(m!)^d = \exp(\Omega(v^{1/d}\log v))$ automorphisms.

In particular, the examples of $\mathfrak{J}(m,3)$ and $\mathfrak{H}(m,3)$ show that the bound of Theorem 2.5.4 is tight up to logarithmic factors in the exponent. Babai conjectures that $\mathfrak{J}(m,3)$ and $\mathfrak{H}(m,3)$ are in fact the only examples of primitive coherent configurations with $\exp(\omega(v^{1/4}\log v))$ automorphisms.

The Johnson and Hamming schemes are examples of a more general family of coherent configurations called "Cameron schemes" (see Definition 2.6.3), which also includes interpolations between Johnson and Hamming schemes. Babai conjectures that Cameron schemes are the only primitive coherent configurations with exponentially many automorphisms.

Conjecture 2.5.5 (Babai)**.** *For every $\varepsilon > 0$, there is some N_ε such that if $\mathfrak{X}$ is a primitive coherent configuration on $v \geq N_\varepsilon$ vertices and $|\operatorname{Aut}(\mathfrak{X})| \geq \exp(v^\varepsilon)$, then $\mathfrak{X}$ is a Cameron scheme.*

In 1981, Babai verified the conjecture for all $\varepsilon > 1/2$, proving that all nontrivial primitive coherent configurations have at most $\exp(O(v^{1/2}\log^2 v))$ automorphisms. Theorem 2.5.4 extends this verification to all $\varepsilon > 1/3$, the first improvement to Babai's automorphism bound.

Since the triangular and lattice graphs are in fact the only nontrivial strongly regular graphs corresponding to Cameron schemes, Conjecture 2.5.5 in particular implies that the

bound on the number of automorphisms of a strongly regular graph appearing in Theorem 2.4.9 could be improved to subexponential, $\exp(v^{o(1)})$.

2.6 Permutation Groups

Coherent configurations appeared for the first time in a paper of Schur on permutation groups [Sch33], and can be viewed as combinatorial relaxations of permutation groups. Given a permutation group $\Gamma \leq \mathrm{Sym}(V)$, we define the *Schurian configuration* $\mathfrak{X}(\Gamma)$ on vertex set V by taking the R_i given by the orbitals of Γ, i.e., the orbits of the induced action on $V \times V$. The configuration $\mathfrak{X}(\Gamma)$ is coherent, and clearly $\Gamma \leq \mathrm{Aut}(\mathfrak{X}(\Gamma))$. The Schurian configuration $\mathfrak{X}(\Gamma)$ is homogeneous if and only if Γ is transitive, and primitive if and only if Γ is a primitive permutation group.

By characterizing all the permutation groups whose Schurian configurations correspond to the triangular and lattice graphs, we obtain the following corollary to Theorem 2.5.4, our classification of primitive coherent configurations. We denote by $S_m^{(k)}$ and $A_m^{(k)}$ the actions of S_m and A_m, respectively, on the k-subsets of $[m]$, and $G \wr H$ denotes the wreath product of the permutation groups $G \leq S_n$ by $H \leq S_m$ in the product action on a domain of size n^m.

Corollary 2.6.1. *Let Γ be a primitive permutation group of degree n. Then either $|\Gamma| \leq \exp(O(n^{1/3}\log^{7/3} n))$, or Γ is one of the following groups:*

(a) S_n or A_n;

(b) $S_m^{(2)}$ or $A_m^{(2)}$, where $n = \binom{m}{2}$;

(c) a subgroup of $S_m \wr S_2$ containing $(A_m)^2$, where $n = m^2$.

We note that groups of Corollary 2.6.1 (a) yield trivial Schurian configurations, the groups of (b) yield $\mathfrak{J}(2, m)$, and the groups of (c) yield $\mathfrak{H}(m, 2)$.

We give the first elementary proof of Corollary 2.6.1 in Chapter 8—in particular, we do not require the Classification of Finite Simple Groups (CFSG). Previously, the only CFSG-free classification of the large primitive permutation groups was given by Babai in a pair of papers in 1981 and 1982 [Bab81, Bab82]. Babai proved that $|\Gamma| \leq \exp(O(n^{1/2}\log^2 n))$ for primitive groups Γ other than A_n and S_n [Bab81].

However, using CFSG, Cameron proves a much stronger classification [Cam81], describing all primitive permutation groups above a $n^{O(\log\log n)}$ order threshold. We state Maróti's refinement of his classification of permutation groups of order greater than $n^{1+\log n}$ [Mar02].

Theorem 2.6.2 (Cameron [Cam81], Maróti [Mar02])**.** *If Γ is a primitive permutation group of degree $n > 24$, then one of the following holds:*

(a) there are positive integers d, k, and m such that $(A_m^{(k)})^d \leq \Gamma \leq S_m^{(k)} \wr S_d$;

(b) $|\Gamma| \leq n^{1+\log_2 n}$.

We say a primitive permutation group Γ is a *Cameron group with parameters* (m, k, d) if it satisfies Theorem 2.6.2 (a).

Definition 2.6.3. A coherent configuration $\mathfrak{X}$ is a *Cameron scheme* if $\mathfrak{X} = \mathfrak{X}(\Gamma)$ for some Cameron group Γ.

Hence, Conjecture 2.5.5 states that Cameron's classification of primitive permutation groups of large order transfers to the combinatorial setting of primitive coherent configurations. Furthermore, as we prove in Chapter 8, the conjecture entails Cameron's theorem, above the threshold $|\Gamma| \geq \exp(n^{\varepsilon})$. Thus, confirmation of Conjecture 2.5.5 would yield a CFSG-free proof of Cameron's classification (above this threshold).

2.7 Clique Geometries

Many of our results are built upon our analysis of the combinatorial structure of cliques in graphs. A *clique* C in an undirected graph G is a set of pairwise adjacent vertices; its *order*

$|C|$ is the number of vertices in the set.

Definition 2.7.1. A *clique geometry* on a graph G is a collection $\mathcal{G}$ of maximal cliques such that every pair of adjacent vertices in G belongs to a unique clique in $\mathcal{G}$.

The line-graphs of partial geometries give the quintessential example of a clique geometry. For each point p of the partial geometry, there is a maximal clique in the line-graph given by the set of all lines incident on p. The collection of all such cliques forms a clique geometry.

Indeed, clique geometries seem to have been studied for the first time in a paper of Bose in which he also introduced partial geometries [Bos63]. (Bose considered only clique geometries with additional regularity properties corresponding to the case of a partial geometry.) Clique geometries have since appeared in the algebraic combinatorics literature under various terminology [God93, Met91], and were also essential to Neumaier's classification of strongly regular graphs [Neu82, Neu79].

We make use of clique geometries in three ways. First, by counting the intersections between cliques in a clique geometry, we bound the parameter λ of a strongly regular graph, allowing us to prove Theorem 2.4.8 from Theorem 2.4.2. In fact, we bound this parameter for a class of graphs generalizing distance-regular graphs. Second, reconstructing a partial geometry from its line-graph is equivalent to finding the clique geometry corresponding to the points. Hence, to prove Theorem 2.4.7, we bound the number of clique geometries of the line-graph of a partial geometry. Third, we give sufficient conditions of the existence of clique geometries in a union of constituent graphs of a primitive coherent configuration, showing that unless a clique geometry is present, the primitive coherent configuration exhibits strong small-scale vertex expansion. We also classify the primitive coherent configurations with clique geometries. Our analysis of clique geometries is a crucial ingredient in the proof of Theorem 2.5.4.

2.7.1 Clique Geometries in Distance-Regular Graphs

Given a graph G and vertex x, we denote by $G(x)$ the neighbors of x in G, and by $G^{(i)}(x)$ the collection of vertices at distance i from x. We denote by $d_G(x, y)$ the distance from x to y in G.

Definition 2.7.2. A connected graph G is *distance-regular* if it is regular, and for every positive integer i there are constants b_i and c_i such that for any pair of vertices x, y with $d_G(x, y) = i$, there are precisely c_i neighbors of y in $G^{(i-1)}(x)$ and b_i neighbors of y in $G^{(i+1)}(x)$. The constants b_i and c_i are called the *intersection numbers* of G.

Given a distance-regular graph G, we will always denote by ρ the valency of G, and, in analogy with strongly regular graphs, write $\lambda = \rho - b_1 - 1$ for the number of common neighbors of two adjacent vertices in G, and $\mu = c_2$ for the number of common neighbors of two vertices at distance 2 in G.

Indeed, distance-regular graphs generalize strongly regular graphs, and are generalized in turn by coherent configurations: if G is distance-regular with vertex set V, then $\mathfrak{X} = (V, d_G)$ is a coherent configuration.

We shall bound the parameter λ for another class of graphs generalizing distance-regular graphs.

Definition 2.7.3. We say a graph is *sub-amply regular* $\mathrm{SubAR}(v, \rho, \lambda, \mu)$ if it is ρ-regular on v vertices, any two adjacent vertices have exactly λ common neighbors, and any pair of vertices at distance 2 from each other have *at most* μ common neighbors.[2]

Theorem 2.7.4. *Let G be a* $\mathrm{SubAR}(v, \rho, \lambda, \mu)$ *graph which is not a disjoint union of cliques. Then*

$$\lambda + 1 < \max\left\{4\sqrt{2v}, \frac{6}{\sqrt{13}-1}\sqrt{\rho(\mu-1)}\right\}.$$

2. The term "sub-amply regular" is not standard, but this class of graphs captures the general context in which our bound on λ applies. More commonly studied are *amply regular* graphs, which are $\mathrm{SubAR}(v, \rho, \lambda, \mu)$ graphs in which every pair of vertices at distance 2 from each other have *exactly* μ common neighbors.

Even in the very special case of strongly regular graphs, this result considerably improves the previously known bounds for λ (Spielman [Spi96] and Pyber [Pyb14]) in some ranges of the parameters. (See Section 6.1) for a detailed comparison.)

We shall prove Theorem 2.7.4 in Section 5.1 as a corollary to a theorem of Metsch [Met91]. Metsch's theorem, stated below using our terminology, gives sufficient conditions of the existence of a clique geometry in a sub-amply regular graph.

Theorem 2.7.5 (Metsch [Met99, Result 2.1])**.** *Let G be a* SubAR(v, ρ, λ, μ) *graph, and let t be an integer such that*

$$\lambda > (2t-1)(\mu-1) - 1, \text{ and}$$
$$\rho < (t+1)(\lambda+1) - \frac{1}{2}t(t+1)(\mu-1).$$

Then the maximal cliques of order at least $\lambda + 2 - (t-1)(\mu-1)$ form a clique geometry, and each vertex belongs to at most t cliques of the geometry.

In Section 5.1, we shall give a quick proof of an asymptotic simplification of Theorem 2.7.5, replacing the assumptions on the parameters with the asymptotic inequality $\rho\mu = o(\lambda^2)$ in order to find a clique geometry with cliques of order $\sim \lambda$ (see Theorem 5.1.2).

In the special case of a distance-regular graph G, Delsarte gave the following bound on the order of a clique.

Lemma 2.7.6 (Delsarte [Del73])**.** *Let G be a distance-regular graph of valency ρ whose least eigenvalue is τ. Then no clique in G has order greater than $1 + \rho/|\tau|$.*

For G, ρ, and τ as in Lemma 2.7.6, we say G is *Delsarte geometric* if it has a clique geometry in which all cliques achieve order $1 + \rho/|\tau|$. For example, the line-graphs of partial geometries are Delsarte geometric: for every point p of a PG(r, k, α), there is a clique C_p in the line-graph consisting of all the $r = 1 + \rho/|\tau|$ lines through p (see Section 5.4).

The concept of a Delsarte geometric graph was introduced by Godsil [God93], who called

such graphs "geometric" and gave a sufficient condition for a distance-regular graph to be "geometric." We state this sufficient condition in Theorem 5.2.1.

We observe that a simpler condition, involving only the parameters of the graph, already guarantees that it is "asymptotically Delsarte geometric." A distance-regular graph G is *asymptotically Delsarte geometric* if it has a clique-geometry whose cliques have order $\sim 1 + \rho/|\tau|$, where ρ is the valency of G and τ is the least eigenvalue.

Theorem 2.7.7. *Let G be a distance-regular graph of valency ρ whose least eigenvalue is τ. Suppose $|\tau|\mu = o(\lambda)$. Then G is asymptotically Delsarte geometric.*

Theorem 2.7.7 is proved in Section 5.2.

2.7.2 Clique Geometries in Line-Graphs of Partial Geometries

In order to prove Theorem 2.4.7, our bound on the number of automorphisms of the line-graph of a partial geometry, we first reconstruct the partial geometry from its line-graph.

The *unique* reconstruction of a $\mathrm{PG}(r, k, \alpha)$ partial geometry from its line-graph is not always possible; in particular, there exist non-isomorphic finite projective planes of the same order, but the line-graph of every finite projective plane is the complete graph. In fact, while $k \sim n^{1/2}$ for finite projective planes with n points, unique reconstructibility already fails even for partial geometries with $k \sim n^{1/3}$. We overcome the non-uniqueness obstacle by borrowing the basic idea of "list decoding" in the theory of error-correcting codes: we show that the number of reconstructions can be controlled and produce a moderate-length list that includes all reconstructions.

First, we clarify what exactly is meant by "reconstruction."

Definition 2.7.8. Given a graph G, a (r, k, α)-*reconstruction system* is a clique geometry in G such that every clique has order r, every vertex belongs to exactly k cliques, and for every clique C and every vertex $u \notin C$, the vertex u has exactly α neighbors in C. A *reconstruction system* is a (r, k, α)-reconstruction system for some positive value of the parameters (r, k, α).

Except in the case of a complete graph, G has a (r, k, α)-reconstruction system if and only if G is the line-graph of a $\mathrm{PG}(r, k, \alpha)$ (see Proposition 5.4.2). Hence, reconstructing a partial geometry from its line-graph amounts to finding a highly regular clique geometry in the line-graph.

Up to a certain threshold in the values of the parameters, there is a *unique* clique geometry satisfying Definition 2.7.8 in the line-graph of a partial geometry. This threshold was already observed by Miller [Mil78] and Spielman [Spi96] in the case of transversal designs and Steiner designs, respectively.

Theorem 2.7.9 (Unique reconstruction (cf. [Mil78, Spi96]))**.** *If $\mathfrak{X}$ is a $\mathrm{PG}(r, k, \alpha)$ with $k < 1 + (r - \alpha)/(\alpha - 1)$, then $L(\mathfrak{X})$ has a unique reconstruction system.*

We give a proof of Theorem 2.7.9 in Section 5.4, where we also point out that the bound in the theorem is tight (Proposition 5.4.4).

Beyond the unique reconstruction threshold, we are still able to limit the number of possible reconstructions of a partial geometry from its line-graph by bounding the number of clique geometries satisfying the regularity constraints of Definition 2.7.8.

Theorem 2.7.10. *Let $\mathfrak{X}$ be a $S(2, k, n)$ design with r blocks incident on each point. Suppose $\mathfrak{X}$ is not a projective plane (i.e., suppose $k < r$). Then the number of reconstruction systems in $L(\mathfrak{X})$ is at most most $\exp(O((k^3/n) \log^4 n / \log^2(r/k)))$.*

For general partial geometries, we have the following somewhat weaker bound.

Theorem 2.7.11. *Suppose $\mathfrak{X}$ is a $\mathrm{PG}(r, k, \alpha)$ with m lines, and $r \neq \alpha$. Then there are at most $\exp(O((k\alpha/r)^2 \log^6 m / \log^3(r/\alpha)))$ reconstruction systems in $L(\mathfrak{X})$, and they can all be listed within the same time bound.*

Theorems 2.7.10 and 2.7.11 are proved in Section 5.4.

2.7.3 Clique Geometries in Primitive Coherent Configurations

Clique geometries are central to our structure theory for primitive coherent configurations. In particular, we shall give a sufficient condition for the existence of a clique geometry in a certain union of the constituent graphs of a primitive coherent configuration.

Let $\mathfrak{X}$ be a nontrivial primitive coherent configuration on v vertices with structure constants p^i_{jk}. Without loss of generality, assume 0 is the vertex color. For any color $i > 0$ in $\mathfrak{X}$, we write $\rho_i = p^0_{ii^*}$, the out-valency of a vertex in the ith constituent digraph $\mathfrak{X}_i$. We say that color i is *dominant* if $\rho_i \geq v/2$. Colors i with $\rho_i < v/2$ are *nondominant*.

When $\mathfrak{X}$ has no dominant color, it is in a sense "pseudorandom." In particular, such configurations cannot have a very large number of automorphisms (see Lemma 7.1.2). Therefore, in the proof of our bound on the number of automorphisms of a primitive coherent configuration, Theorem 2.5.4, we will be able to reduce to the case that $\mathfrak{X}$ has a dominant color.

Suppose now that $\mathfrak{X}$ has a dominant color, without loss of generality the color 1. Let $G_{\mathfrak{X}}$ be the graph on $V(\mathfrak{X})$ formed by the pairs with nondominant color. So $G_{\mathfrak{X}}$ is regular of valency $v - \rho_1 - 1$, and for every pair of distinct nonadjacent vertices in $G(\mathfrak{X})$, the number of common neighbors is exactly $\sum_{i,j\geq 2} p^1_{ij}$. In analogy with the parameters of a strongly regular graph, we will therefore write $\rho = v - \rho_1 - 1$ and $\mu = \sum_{i,j\geq 2} p^1_{ij}$.

However, the graph $G_{\mathfrak{X}}$ is not generally strongly regular, since pairs of adjacent vertices in $G_{\mathfrak{X}}$ of different colors in $\mathfrak{X}$ will in general have different numbers of common neighbors. Nevertheless, we shall find a clique geometry in $G_{\mathfrak{X}}$ under certain assumptions on the parameters of $\mathfrak{X}$.

Recall that for a graph G and a vertex x, we write $G(x)$ for the set of (out-)neighbors of x in G. For any nondominant color i of $\mathfrak{X}$, we write $\lambda_i = |\mathfrak{X}_i(x) \cap G_{\mathfrak{X}}(y)|$, where $c(x, y) = i$.

Definition 2.7.12. Let $\mathfrak{X}$ be a nontrivial primitive coherent configuration with a dominant color. A *clique geometry in the primitive coherent configuration* $\mathfrak{X}$ is a clique geometry in $G_{\mathfrak{X}}$. The clique geometry is *asymptotically uniform* if for every clique C in the geometry, every vertex $x \in C$, and every nondominant color i, we have either $|C \cap \mathfrak{X}_i(x)| \sim \lambda_i$ or

$|C \cap \mathfrak{X}_i(x)| = 0$.

In Section 5.3, we prove the following sufficient condition for the existence of clique geometries in primitive coherent configurations.

Theorem 2.7.13. *Let $\mathfrak{X}$ be nontrivial primitive coherent configuration with $\rho < o(v^{2/3})$ and $\lambda_i \geq \Omega(v^{1/2})$. Then for v sufficiently large, $\mathfrak{X}$ has an asymptotically uniform clique geometry.*

Theorem 2.7.13 provides a powerful dichotomy for primitive coherent configurations: either there is an upper bound on some parameter λ_i, or there is a clique geometry. The parameters λ_i are loosely analogous to the parameter λ of a strongly regular graph, and similarly control the small-scale vertex expansion in constituent digraphs, as described in Section 2.8.

Clique geometries offer their own dichotomy. Geometries with at least three cliques at every vertex have a rigid structure. In this case, we are able to exploit the ubiquitous 3-claws (induced $K_{1,3}$ subgraphs) in $G_{\mathfrak{X}}$ in order to bound the number of automorphisms (see Lemma 7.1.5). On the other hand, geometries with at most two cliques at a vertex can classified; this includes the cases of primitive coherent configurations corresponding to the triangular and lattice graphs. We state this classification in the following theorem.

Theorem 2.7.14. *Suppose $\mathfrak{X}$ is a primitive coherent configuration with $\rho = o(v^{2/3})$. If $\mathfrak{X}$ has an asymptotically uniform clique geometry, and some vertex w belongs to at most two cliques of the geometry, then for v sufficiently large, one of the following is true:*

(a) $\mathfrak{X}$ has rank three and is isomorphic to $\mathfrak{X}(T(\rho/2+2))$ or $\mathfrak{X}(L_2(\rho/2+1))$;

(b) $\mathfrak{X}$ has rank four, $\mathfrak{X}$ has a non-symmetric non-dominant color i, and $G(\mathfrak{X})$ is isomorphic to $T(\rho_i+2)$.

We prove Theorem 2.7.14 in Section 7.2.

2.8 Vertex Expansion

Estimates on the rate of vertex expansion in graphs are essential to many of our arguments, particularly in our analyses of strongly regular graphs and primitive coherent configurations.

Of particular importance are bounds on the parameter λ in a strongly regular graph. Let G be a $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph, and set $\nu = \max\{\lambda, \mu\}$. A set A of vertices of size $o(\rho/\nu)$ has optimal vertex expansion—its neighborhood $G(A)$ has size $\sim \rho|A|$ (see Lemma 6.4.7.) As observed in Corollary 6.1.4, relatively straightforward, asymptotically tight bounds for the parameter μ are available under mild assumptions. Hence, upper bounds on λ yield upper bounds on ν, and hence on the small-scale vertex expansion of a strongly regular graph.

In a similar fashion, the parameters λ_i control the small-scale vertex expansion of constituent graphs of primitive coherent configurations.

We also rely on estimates of the rate of vertex expansion at larger scales, via the following to lemmas.

Lemma 2.8.1. *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph. Let $x \in V(G)$ and $A \subseteq G(x)$. Then $|G(A) \setminus G^+(x)| \geq (\rho - \lambda - 1)|A|/\mu$.*

The second vertex expansion lemma, though only improving on Lemma 2.8.1 by a factor of 2 at best, requires a considerably more delicate argument. However, this this extra factor of 2 will be essential in the proof of Theorem 2.4.10 in Section 6.5 (see the note following Lemma 6.5.10).

Lemma 2.8.2. *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph, and let $x \in V(G)$. Let $0 < \varepsilon \leq 1/3$ and $A \subseteq G(x)$. Suppose $|A| + \lambda < \varepsilon\rho$, and let $\alpha = 2(1 - \varepsilon)((\mu - 4)/\mu)$. Then $|G(A) \setminus G^+(x)| \geq \alpha(\rho/\mu)|A|$.*

We also state a different sort of vertex expansion estimate for constituent graphs of primitive coherent configurations, Lemma 2.8.3 below, used in the proof of Theorem 2.5.4.

Let $\mathfrak{X}$ be a primitive coherent configuration. Given a color i, integer δ, and vertex x, the

δ-sphere $\mathfrak{X}_i^{(\delta)}(x)$ in $\mathfrak{X}_i$ centered at x is the set of vertices y such that the directed distance from x to y in $\mathfrak{X}_i$ is δ.

Lemma 2.8.3 is proved in [Sun16] (cf. [SW15b]).

Lemma 2.8.3 (Growth of Spheres)**.** *Let $\mathfrak{X}$ be a primitive coherent configuration, let $i, j \geq 1$ be nondiagonal colors, let $\delta = \mathrm{dist}_i(j)$, and $x \in V(\mathfrak{X})$. Then for any integer $1 \leq \alpha \leq \delta - 2$, we have*

$$|\mathfrak{X}_i^{(\alpha+1)}(x)||\mathfrak{X}_i^{(\delta-\alpha)}(x)| \geq n_i n_j.$$

We note that Lemma 2.8.3 is straightforward when $\mathfrak{X}_i$ is distance-regular. Indeed, a significant portion of the difficulty of the lemma was in finding the correct generalization.

Chapter 3

INDIVIDUALIZATION AND REFINEMENT

In order to bound the order of the automorphism group of a combinatorial structure, we analyze the "individualization/refinement" procedure. This technique was introduced as "deep stabilization" in [Wei76] in the context of Graph Isomorphism problem. The connection with Graph Isomorphism is explained in Section 9.1. We shall use individualization and refinement to find bases of automorphism groups.

A *base* for a group Γ acting on a set V is a subset $S \subseteq V$ such that the pointwise stabilizer $\Gamma_{(S)}$ of S in Γ is trivial. If S is a base, then clearly $|\Gamma| \leq |V|^{|S|}$.

In order to bound the order of the automorphism group of a regular combinatorial object, we will find a "small" base. We do so by first selecting a candidate base S ("individualizing" some set of points or vertices), and then attempting via "canonical color refinement" to find a combinatorial proof that fixing S pointwise kills the automorphism group.

We now give a complete description of the individualization/refinement procedure.

3.1 Color Refinement

We shall apply individualization/refinement to colored versions of the combinatorial structures we study. A coloring of a set S is simply a map $\gamma : S \to C$ for some finite set C, whose elements are called the *colors*. For example, as we have explained, a coherent configuration can be viewed as a complete directed graph along with colorings of its edges and vertices, satisfying certain regularity properties.

Let $\mathcal{C}$ be a class of colored combinatorial structures, i.e., a collection of pairs (X, γ) where X is a combinatorial structure and γ is a coloring of substructures of X. For example, in this thesis we will study the class of vertex-colored graphs and vertex-colored primitive coherent configurations, i.e., to graphs and primitive coherent configurations equipped with additional

colorings of their vertices.[1] We also apply individualization/refinement to colored incidence structures, i.e., incidence structures with colorings of the points and colorings of the blocks. By definition, an automorphism of a colored combinatorial structure or an isomorphism between colored structures preserves the coloring.

Given a coloring $\gamma : S \to C$, the preimage of a color $i \in C$ under γ is called a *color class*. A subset of S is *closed* (with respect to γ) if it is a union of γ-color classes. A coloring $\gamma' : S \to C'$ *refines* the coloring $\gamma : S \to C$ if every γ-color class is closed with respect to γ'.

A *color refinement operator* over a class $\mathcal{C}$ of colored combinatorial structures is a map $\mathcal{R} : \mathcal{C} \to \mathcal{C}$ that assigns to element of $\mathcal{C}$ a new element with the same underlying combinatorial structure and a refined coloring. The color refinement operator $\mathcal{R}$ is *canonical* if for every $X, Y \in \mathcal{C}$, we have $\mathrm{Iso}(X, Y) = \mathrm{Iso}(\mathcal{R}(X), \mathcal{R}(Y))$. A coloring is $\mathcal{R}$-*stable* if its color classes are invariant under $\mathcal{R}$. Iteratively applying a color refinement operator $\mathcal{R}$ to a finite structure with initial coloring γ eventually yields a $\mathcal{R}$-stable coloring γ'; we call γ' the $\mathcal{R}$-*stable refinement* of γ.

3.1.1 Naive Refinement

The only refinement operator we consider for Steiner designs is *naive refinement*. Let $\mathfrak{X}$ be a partial geometry with point set $\mathcal{P}$ and block set $\mathcal{B}$, and let $\gamma : \mathcal{P} \cup \mathcal{B} \to C$ be a coloring of the points and blocks such that $\gamma(p) \neq \gamma(B)$ for any $p \in \mathcal{P}$ and $B \in \mathcal{B}$. Given an element $x \in \mathcal{P} \cup \mathcal{B}$, we define the map $m_x : C \to \mathbb{Z}$ by setting $m_x(i)$ to be the number of elements of $\mathcal{P} \cup \mathcal{B}$ incident to x of color i. (So $m_x(i)$ counts blocks of color i if x is a point, and $m_x(i)$ counts points if x is a block.) The *naive color refinement operator* for Steiner designs is the map $(\mathfrak{X}, \gamma) \mapsto (\mathfrak{X}, \gamma')$, where $\gamma'(x)$ is the pair $(\gamma(x), m_x)$ for $x \in \mathcal{P} \cup \mathcal{B}$.

We also define naive refinement for configurations. Let $\mathfrak{X} = (V, c)$ be a configuration of

1. Primitive coherent configurations are already equipped with a trivial (homogeneous) vertex coloring. When we speak of a vertex coloring a primitive coherent configuration in the context of individualization refinement, we usually refer to an additional, auxiliary vertex coloring. To avoid confusion, we will use c to denote the coloring defining a configuration, and γ for the auxiliary colorings used in the individualization/refinement process.

rank r, and let $\gamma : V \to C$ be a coloring of the vertices. Given $u \in V$, we define the map $m_u : [r] \times C \to \mathbb{Z}$ by setting $m_u(i, j)$ to be the number of vertices $v \in V$ such that $c(u, v) = i$ and $\gamma(v) = j$. The *naive refinement operator for configurations* is the map $(\mathfrak{X}, \gamma) \mapsto (\mathfrak{X}, \gamma')$, where $\gamma'(u)$ is the pair $(\gamma(u), m_u)$ for $u \in V$.

We define naive refinement for the graph G as naive refinement for the configuration $\mathfrak{X}(G)$.

3.1.2 Weisfeiler-Leman Refinement

In 1968, Weisfeiler and Leman defined a natural canonical refinement operator for configurations, in the context of the Graph Isomorphism problem [WL68, Wei76]. Let $\mathfrak{X} = (V, c)$ be a configuration of rank r. Given $u, v \in V$, we define the map $m_{(u,v)} : [r] \times [r] \to \mathbb{Z}$ by setting $m_{(u,v)}(i, j)$ to be the number of vertices w such that $c(u, w) = i$ and $c(w, v) = j$. We define $\hat{c}(u, v)$ to be the pair $(c(u, v), m_{(u,v)})$. Let r' be the cardinality of the image of $\hat{c}$, and let $c' : V \times V \to [r']$ be defined by setting $c'(u, v) < c'(x, y)$ if and only if $\hat{c}(u, v)$ precedes $\hat{c}(x, y)$ in the lexicographic order. The *WL refinement operator* is the map $(V, c) \mapsto (V, c')$.

We note that a configuration is coherent if and only if it is stable under WL refinement.

3.2 Permutation Group Bases via Individualization and Refinement

A coloring is *discrete* if every color class has cardinality 1, and a coloring is *trivial* if there is only one color class. Since isomorphisms preserve colors by definition, a vertex-colored graph with a discrete coloring has no automorphisms. Furthermore, if the stable refinement of a vertex-colored graph is discrete, then the original vertex-colored graph had no automorphisms. On the other hand, if G is a graph, and γ is a trivial vertex coloring of G, then $\mathrm{Aut}(G) = \mathrm{Aut}(G, \gamma)$.

We say an element is *uniquely colored* if no other element has the same color.

Individualization of an element of a colored combinatorial structure means the assignment of a unique color to that element, and individualization of a set of elements means the assignment of unique colors to each element in the set. For example, if a graph has the trivial coloring, then after individualizing the set of vertices $\{u, v\}$, we obtain a new coloring in which u and v each belong to color classes of cardinality 1, and all other vertices belong to a third color class. In particular, given a graph X and a set of vertices S, we have $\mathrm{Aut}(X)_{(S)} = \mathrm{Aut}((X, \gamma_S))$, where γ_S is a coloring given by individualizing S, starting from a trivial coloring.

Hence, if after individualizing S, the stable coloring under a canonical color refinement operator is discrete, then S is a base for the automorphism group. This is the procedure we use in order to find bases for automorphism groups, and thereby bound their order.

Definition 3.2.1. Let X be a combinatorial structure, and suppose $\mathrm{Aut}(X) \leq \mathrm{Sym}(V)$ for some set V. We say a canonical color refinement operator $\mathcal{R}$ is *d-effective* for X if after individualizing d elements of V from a trivial coloring of V, the $\mathcal{R}$-stable refinement is discrete.

The following proposition summarizes the standard facts about individualization and refinement we shall use in order to prove our automorphism bounds.

Proposition 3.2.2. *Let X be a combinatorial structure, and suppose* $\mathrm{Aut}(X) \leq \mathrm{Sym}(V)$ *for some set V. If there exists a d-effective canonical color refinement operator for X, then* $|\mathrm{Aut}(X)| \leq |V|^d$.

3.3 Color-Boundedness

Even when we cannot achieve a discrete coloring, a relatively fine coloring can still constrain the automorphism group.

Given a graph G, a set $A \subseteq V(G)$, and vertices $x, y \in V(G)$, we say that x and y are *A-twins* if they have the exact same set of neighbors in A, i. e., if for each $z \in A$, the vertex

z is adjacent to x if and only if z is adjacent to y.

Let G be a vertex-colored graph with color classes $C_1, \ldots, C_m$ (in this order). Let $B_k = \bigcup_{i=1}^{k} C_i$. We say that G *is color-d-bounded* if for $k = 1, \ldots, m$, every equivalence class of B_{k-1}-twins in C_k has at most d vertices. (Note that $B_0 = \emptyset$, so for $k = 1$ this condition means $|C_1| \leq d$.)

Color-d-boundedness imposes a strong constraint on the automorphism group when d is small.

Proposition 3.3.1. *Let G be a vertex-colored graph on v vertices. Suppose that after individualizing some set of ℓ vertices in G, the stable refinement with respect to a canonical color refinement operator is color-d-bounded. Then $\mathrm{Aut}(G)$ has a Γ_d subgroup of index at most v^ℓ.*

Proof. The point-stabilizer of ℓ vertices in $\mathrm{Aut}(G)$ is a subgroup of index at most v^ℓ. Hence, it suffices to show that the automorphism group of a color-d-bounded graph is a Γ_d group.

Suppose G is color-d-bounded, and let $C_1, \ldots C_m$ and $B_0, \ldots, B_m$ be as in the definition of color-d-boundedness above. Let G_k be the graph induced by G on B_k, so $G_m = G$ and G_0 is the empty graph. We have a homomorphism $\pi_k : \mathrm{Aut}(G_k) \to \mathrm{Aut}(G_{k-1})$ for all $1 \leq k \leq m$ given by restricting each permutation $\phi \in \mathrm{Aut}(G_k)$ to the (necessarily ϕ-invariant) set B_{k-1}. Note that $\phi \in \ker(\pi_k)$ only if ϕ stabilizes setwise each equivalence class of B_{k-1}-twins in C_k. Hence, if $A_1 \cup \cdots \cup A_r$ is the partition of C_k into equivalence classes of B_{k-1}-twins, then $\ker(\pi_k)$ is isomorphic to a subgroup of $\mathrm{Sym}(A_1) \times \cdots \times \mathrm{Sym}(A_r)$. In particular, $\ker(pi_k)$ is a Γ_d group. But by construction $\mathrm{Aut}(G)$ has normal series $1 = \Gamma_0 \lhd \Gamma_1 \lhd \cdots \lhd \Gamma_m = \mathrm{Aut}(G)$ with $\Gamma_k \leq \ker(\pi_k)$, so $\mathrm{Aut}(G)$ is a Γ_d group. □

We will use Proposition 3.3.1 to prove Theorem 2.4.10.

Chapter 4

STEINER DESIGNS

In this chapter, we prove Theorem 2.3.2, our essentially tight bound on the number of automorphisms of a Steiner design. The following Theorem 4.0.1 is the main technical result of this chapter. Theorem 2.3.2 follows from it immediately, in view of Proposition 3.2.2.

Theorem 4.0.1. *Naive refinement is* $(t + O(\log n))$*-effective for any* $\mathrm{S}(2, k, n)$ *design with* $k > t$.

Before proving Theorem 4.0.1, we describe in Section 4.1 the structural observations about Steiner designs that we employ to prove the automorphism bound. Then, in Section 4.2, we apply this structure theory to prove Theorem 2.3.2 by analyzing individualization and refinement in Steiner designs. We also show that our automorphism bound cannot be generalized to balanced incomplete block designs in Section 4.3, by constructing a family of $S_2(2, 3, n)$ designs with $2^{n/2}$ automorphisms.

4.1 Cones and Towers

We first describe our structural contributions for Steiner 2-designs, the essential estimates we use to prove Theorem 2.3.2. The main element of our structural results is a pairwise independent addressing scheme arising out of "towers of cones."

Let $\mathfrak{X}$ be a $\mathrm{S}(2, k, n)$ design with point set $\mathcal{P}$ and block set $\mathcal{B}$. For distinct $p, q \in \mathcal{P}$, we denote the unique block containing p and q by $\overline{pq} \in \mathcal{B}$. For an ordered pair (p, q) of distinct points, we define the *truncated block* $B(p, q) = \overline{pq} \setminus \{p\}$; so $|B(p, q)| = k - 1$. We also define the (degenerate) truncated block $B(p, p)$ to be the singleton set $\{p\}$.

For $p \in \mathcal{P}$ and $A \subseteq \mathcal{P}$, define the *cone with base* A *and apex* p as $C_p(A) = \bigcup_{a \in A} B(p, a)$. Note that if A is a fixed closed set (with respect to a point-coloring), then $|C_p(A)|$ is determined by the color of p in the stable refinement. Furthermore, if A is closed, then $C_p(A)$ is closed in the stable refinement after individualizing p.

Our analysis of Steiner designs builds on a stochastic process that produces a growing family of pairwise independent random points from an iterated tower of random cones. First, we describe some basic properties of cones themselves.

4.1.1 Estimates for Cones

Our first lemma controls the size of our cones.

Lemma 4.1.1. *Let $A \subseteq \mathcal{P}$ be nonempty and choose a point $p \in \mathcal{P}$ at random. Then*

$$\mathbb{E}_p(|C_p(A)|) \geq (k-1)\left(1 - \frac{(k-2)|A|}{n}\right)|A|.$$

Proof. From the definition of $C_p(A)$, we have

$$\begin{aligned}
\mathbb{E}_p(|C_p(A)|) &= \frac{1}{n}\sum_{p\in\mathcal{P}} |C_p(A)| \\
&\geq \frac{k-1}{n}\sum_{p\in\mathcal{P}} |\{B \in \mathcal{B} : p \in B \text{ and } B \cap A \setminus \{p\} \neq \emptyset\}| \\
&\geq \frac{k-1}{n}\sum_{p\in\mathcal{P}\setminus A} |\{B \in \mathcal{B} : p \in B \text{ and } |B \cap A| = 1\}|.
\end{aligned}$$

Rearranging the sum, we obtain

$$\mathbb{E}_p(|C_p(A)|) \geq \frac{k-1}{n}\sum_{a\in A} |\{p \in \mathcal{P} \setminus A : \overline{ap} \cap A = \{a\}\}|.$$

Now for every pair of distinct points $a, a' \in A$, there are at most $(k-2)$ points in $\overline{aa'} \setminus A$. Hence, for any $a \in A$, we have

$$|\{p \in \mathcal{P} \setminus A : \overline{ap} \cap A = \{a\}\}| \geq (n - |A|(k-2)).$$

Hence,

$$\mathbb{E}_p(|C_p(A)|) \geq \frac{k-1}{n} \sum_{a \in A} (n - |A|(k-2)) = (k-1)\left(1 - \frac{(k-2)|A|}{n}\right)|A|$$

as claimed. □

We now observe a duality between the apex and the members of a cone. Its consequence that the apex of a large cone belongs to many cones over the same set will be used in Lemma 4.2.10.

Lemma 4.1.2. *Let $A \subseteq \mathcal{P}$ and fix $q \in \mathcal{P}$. If $p \in \mathcal{P}$ is chosen at random, then*

$$P_p[q \in C_p(A)] \geq \left(\frac{k-2}{k-1}\right) \cdot P_p[p \in C_q(A)] \tag{4.1}$$

Furthermore, if $q \notin A$, then

$$P_p[q \in C_p(A)] \leq P_p[p \in C_q(A)]. \tag{4.2}$$

Proof. Clearly if $q \in A$ then $P[q \in C_p(A)] = 1$, so suppose $q \notin A$. Let $A' \subseteq A$ be such that for every $a \in A$, there is a unique point $a' \in \overline{qa} \cap A'$. Thus, $C_q(A') = C_q(A)$ and $|A'| = |C_q(A)|/(k-1)$. Furthermore, for any $x \in C_q(A) \setminus A'$ we have $q \in C_x(A)$. It follows that

$$\begin{aligned} P_p[q \in C_p(A)] &\geq P_p[p \in C_q(A) \setminus A'] \\ &= \frac{1}{n}\left(|C_q(A)| - \frac{|C_q(A)|}{(k-1)}\right) \\ &= \left(\frac{k-2}{k-1}\right) \cdot P_p[p \in C_q(A)]. \end{aligned}$$

Inequality (4.2) holds since $p \in B(q,a)$ when $q \in B(p,a) \setminus A$, for any $a \in A$. □

In the next lemma, we bound the expected intersection of a fixed set of points with a

random cone over a fixed base.

Lemma 4.1.3. *Let $A, S \subset \mathcal{P}$. Then if $p \in \mathcal{P}$ is chosen at random, we have*

$$\mathbb{E}(|C_p(A) \cap S \setminus A|) \leq \frac{(k-1)|A||S|}{n}.$$

Proof. By Eq. (4.2) of Lemma 4.1.2, we have $P_p[q \in C_p(A)] \leq P_p[p \in C_q(A)]$ for any $q \notin A$. Furthermore, $|C_q(A)| \leq (k-1)|A|$ for any point q. Hence,

$$\begin{aligned}
\mathbb{E}_p(|C_p(A) \cap S \setminus A|) &= \sum_{q \in S \setminus A} P_p[q \in C_p(A)] \\
&\leq \sum_{q \in S \setminus A} P[p \in C_q(A)] \\
&\leq \sum_{q \in S \setminus A} \frac{(k-1)|A|}{n}.
\end{aligned}$$

□

4.1.2 Labeling Points in Towers

By a *numbering* of the truncated block $B(p, q)$ we mean a bijection from $[k-1]$ to $B(p, q)$ if $p \neq q$, and the constant map $[k-1] \to \{p\}$ if $p = q$.

Let $(p_0, \ldots, p_d)$ be a sequence of points, not necessarily distinct. A *d-dimensional tower* generated by $(p_0, \ldots, p_d)$ is a sequence $f = (f_0, \ldots, f_d)$ of maps $f_j : [k-1]^j \to \mathcal{P}$ such that $f_0 = p_0$ and for every $(x_1, \ldots, x_{j-1}) \in [k-1]^{j-1}$ the map $f_{(x_1,\ldots,x_{j-1})}(y) = f_j(x_1, \ldots, x_{j-1}, y)$ is a numbering of $B(p_j, f_{j-1}(x_1, \ldots, x_{j-1}))$. Note that $\mathrm{im}(f_{j+1}) = C_{p_j}(\mathrm{im}(f_j))$. In particular, $\mathrm{im}(f_j) \subseteq \mathrm{im}(f_{j+1})$ and $\mathrm{im}(f_j)$ does not depend on the particular numberings chosen along the way. Furthermore, $\mathrm{im}(f_j)$ is closed in the stable refinement after individualization of $\{p_0, \ldots, p_j\}$.

We call the elements of $[k-1]^d$ *labels*, and say that x is a *label of* p if $f_d(x) = p$, the value of d being clear from the context. A point $p \in \mathcal{P}$ may have multiple labels or no labels at all. For a label $x = (x_1, \ldots, x_d) \in [k-1]^d$, let $x^j = (x_1, \ldots, x_j) \in [k-1]^j$ denote the prefix of x in $[k-1]^j$; so $x = x^d$.

A *random tower* over $(p_0, \ldots, p_d)$ is defined by choosing the numbering $f_{(x_1,\ldots,x_j)}$ at random for every $0 \leq j \leq d$ and $(x_1, \ldots, x_j) \in [k-1]^j$.

The rest of this section refers to a d-dimensional random tower f over a random sequence $(p_0, \ldots, p_d)$ of points in $\mathcal{P}$.

Lemma 4.1.4. *For any $x \in [k-1]^d$, the point $f_d(x)$ is uniformly distributed over $\mathcal{P}$.*

Proof. The claim is trivial for $d = 0$, so suppose for induction on d that $f_{d-1}(x)$ is uniformly distributed over $\mathcal{P}$. For any $p \in \mathcal{P}$, it is clear under either of the conditions $p_d = p$ and $p_d \neq p$ that $P[f_d(x) = p] = 1/n$, so it is true overall. □

Now we establish the key pairwise independence property.

Lemma 4.1.5. *For any distinct $x, y \in [k-1]^d$ with $d \geq 1$, the points $f_d(x), f_d(y)$ are independent random variables.*

Proof. Let $x = (x_1, \ldots, x_d)$ and $y = (y_1, \ldots, y_d)$ be distinct, and let j be the length of the longest common prefix $x^j = y^j$ of x and y. Define a $(d-j)$-dimensional tower g over $(f_j(x), p_{j+1}, \ldots, p_d)$ by $g_k(z) = f_k((x^j, z))$. Then letting $x' = (x_{j+1}, \ldots, x_d)$ and $y' = (y_{j+1}, \ldots, y_d)$, we have $g_k(x') = f_{k+j}(x')$ and $g_k(y') = f_{k+j}(y')$ for all $0 \leq k \leq d-j$. But by Lemma 4.1.4, we have $f_j(x)$ uniformly distributed over $\mathcal{P}$, and clearly $f_j(x)$ is independent of $p_{j+1}, \ldots, p_d$, so g is a random $(d-j)$-dimensional tower over a random sequence of points. Thus, without loss of generality, we may assume $j = 0$.

Fix $p, q \in \mathcal{P}$ and let E denote the event that $f_d(x) = p$ and $f_d(y) = q$. Since $f_d(x)$ and $f_d(y)$ are uniformly distributed over $\mathcal{P}$ by Lemma 4.1.4, we need to show that $P[E] = 1/n^2$. We proceed by induction on d. First suppose $d = 1$. If $p = q$, then E occurs if and only if $p_0 = p_1 = p$, so $P[E] = 1/n^2$. So suppose $p \neq q$, and let E' be the event that $p, q \in B(p_1, p_0)$. Note that E' is a necessary condition for E, and given E', the probability of E is $1/((k-1)(k-2))$. For E' to occur, we must first have $p_0 \neq p_1$, since otherwise $B(p_1, p_0)$ is a single point. Furthermore, we must $p_1 \neq p, q$, since $p_1 \notin B(p_1, p_0)$. Finally, we must have $p_0, p_1 \in \overline{pq}$. In fact, having $p_0, p_1 \in \overline{pq}$, with $p_1 \neq p_1, p, q$, is both necessary

and sufficient for E' to occur. Thus, assuming $p_0 \in \overline{pq}$, if $p_0 \neq p, q$ then there are $k-3$ possibilities for p_1, and otherwise there are $k-2$ possibilities for p_1. Altogether, we have

$$\begin{aligned} P[E] &= P[E|E']P[E'] \\ &= P[E|E'] \left(P[E' \text{ and } p_0 \neq p, q] + P[E' \text{ and } p_0 \in \{p, q\}] \right) \\ &= \frac{1}{(k-1)(k-2)} \left(\frac{k-3}{n} \cdot \frac{k-2}{n} + \frac{k-2}{n} \cdot \frac{2}{n} \right) = \frac{1}{n^2}. \end{aligned}$$

Now for $d > 1$, the inductive hypothesis says that $f_{d-1}(x)$ and $f_{d-1}(y)$ are independent. Fix p_d. The random, independent points $f_{d-1}(x)$ and $f_{d-1}(y)$ determine two random, independent truncated blocks containing p_d, and the points $f_d(x)$ and $f_d(y)$ are random points from these truncated blocks. Thus, after fixing p_d, we have $f_d(x)$ and $f_d(y)$ independent, and so they are independent overall. □

We now estimate the number of points that get a label from a random tower. We will subsequently estimate the number of labels a point gets.

Corollary 4.1.6. *Let f_d be a random d-dimensional tower over a random sequence of points. The expected number of points which get at least one label from f_d is*

$$\mathbb{E}(|\operatorname{im}(f_d)|) \geq (k-1)^d - \frac{(k-1)^{2d}}{2n}.$$

Proof. Fix a point p. By the inclusion-exclusion principle and Lemmas 4.1.4 and 4.1.5,

$$\begin{aligned} P[p \in \operatorname{im}(f_d)] &\geq \sum_{x \in [k-1]^d} P[f_d(x) = p] - \sum_{x \neq y \in [k-1]^d} P[f_d(x) = f_d(y) = p] \\ &= \frac{(k-1)^d}{n} - \binom{(k-1)^d}{2} \frac{1}{n^2}. \end{aligned}$$

The estimate for $\mathbb{E}(|\operatorname{im}(f_d)|)$ then follows by the linearity of expectation. □

Since labels are distributed uniformly over points, the expected number of labels from

a random d-dimensional tower received by any fixed points $(k-1)^d/n$. From the pairwise independence of the labels, it follows that every point receives nearly the expected number with high probability.

Corollary 4.1.7. *Let f_d be a random d-dimensional tower over a random sequence of points. For each $p \in \mathcal{P}$, let X_p be the number of labels f_d gives to p. Then for all $\beta > 0$,*

$$P\left[(\exists p \in \mathcal{P})\left(\left|X_p - \frac{(k-1)^d}{n}\right| \geq \beta(k-1)^{d/2}\right)\right] < 1/\beta^2.$$

Proof. For any $p \in \mathcal{P}$ and $x \in [k-1]^d$, let $\vartheta_p(x)$ be the indicator variable for the event $f_d(x) = p$. Hence,

$$X_p = \sum_{x \in [k-1]^d} \vartheta_p(x).$$

Hence, by Lemma 4.1.5 and the fact that the $\vartheta_p(x)$ are Bernoulli random variables, we have

$$\mathrm{Var}(X_p) = \sum_{x \in [k-1]^d} \mathrm{Var}(\vartheta_p(x)) = \sum_{x \in [k-1]^d} \mathbb{E}(\vartheta_p(x)) < \mathbb{E}(X_p).$$

Hence, by Chebyshev's inequality, we have

$$P\left(\left|X_p - \frac{(k-1)^d}{n}\right| \geq \beta\sqrt{n}\sqrt{\frac{(k-1)^d}{n}}\right) < \frac{1}{n\beta^2}.$$

Applying the union bound to sum over all $p \in \mathcal{P}$ completes the proof. □

4.2 Individualization and Refinement in Steiner Designs

We prove Theorem 4.0.1 by reducing to the case of a Steiner 2-design.

Theorem 4.2.1. *Naive refinement is $O(\log n)$-effective for any $\mathrm{S}(2, k, n)$ design with $k > t$.*

Theorem 4.0.1 follows from Theorem 4.0.1 by a standard "derived design" argument.

Let $\mathfrak{X}$ be an $\mathrm{S}(t,k,n)$ design with point set $\mathcal{P}$ and block set $\mathcal{B}$. Let $A \subset \mathcal{P}$ such that $|A| \leq t-2$. The *derived design* $\mathfrak{X}_A$ at A is the $\mathrm{S}(t-|A|, k-|A|, n-|A|)$ design whose point set is $\mathcal{P} \setminus A$, and whose block set is $\{B \setminus A : B \in \mathcal{B}\}$.

Proof of Theorem 4.0.1 from Theorem 4.2.1. Let $\mathfrak{X}$ be a $\mathrm{S}(t,k,n)$ design. Fix any set A of $t-2$ points, and consider the derived design $\mathfrak{X}_A$. By Theorem 4.2.1, there exists a set S of size $O(\log n)$ such that after individualizing S in $\mathfrak{X}_A$, the stable naive-refinement is discrete. Let $T = S \cup A$. Then after individualizing T in $\mathfrak{X}$, the stable naive-refinement is discrete. □

We now prove Theorem 4.2.1. We first give a brief outline of our analysis. We will denote by $\mathfrak{X}$ a nontrivial $\mathrm{S}(2,k,n)$ design.

Along the way to proving Theorem 4.2.1, we first achieve the following four targets. Each target is achieved after $O(\log n)$ individualizations, followed by naive refinement.

We denote by $r = (n-1)/(k-1)$ the number of blocks incident on a point. Sets of points of size r form an important threshold in our argument. A random line will not intersect sets that are much smaller, but will intersect larger sets in many points, and so some of our methods only work for sets on one side of this threshold. Sets of size $\approx r$ can be thought of as "hyperplane-like;" in the case of affine or projective space, our argument will produce many actual hyperplanes.

The first target is to produce a closed set S of cr points such that every color class in S has size at most εr, where c and ε are constants with ε much smaller than c. This is possible thanks to the following lemma.

Lemma 4.2.2. *There exists a constant c such that for every $\varepsilon > 0$, after individualizing some set of $O(\log(k/\varepsilon)(1/\varepsilon + \log n/\log k))$ points, the naive-stable refinement has a closed set of size at least cr in which every color class has size at most εr.*

To prove Lemma 4.2.2, we iteratively individualize points in stages. We measure the progress toward achieving our target by estimating the "granularity" of a portion of the Steiner design.

Given a closed set A, the *granularity* of A (with respect to the coloring) is the quantity $|A|/m(A)$, where $m(A)$ is the size of the largest color class in A.

Once we obtain a closed set S of size $\Omega(r)$ and granularity $\Omega(k/\varepsilon)$, we have achieved our first target: since $|S| \leq n$, and $r = (n-1)/(k-1)$, it will follow that every color class in S has size $\leq \varepsilon r$. To construct such a closed set S, we prove two lemmas. The first, Lemma 4.2.7, will produce from a set with granularity g another (potentially much smaller) set with granularity $8g$. The second, Lemma 4.2.8, will produce from a set with granularity g another set with granularity $\geq g/4$ and size $\Omega(r)$. Hence, by combining the two lemmas, we eventually obtain a large set with sufficient granularity.

Lemma 4.2.2 is proved in Section 4.2.1.

Our second target is to produce extend the fine coloring of the hyperplane-sized set obtained from Lemma 4.2.2 to cover the entire Steiner design. This second target is achieved with the following lemma.

Lemma 4.2.3. *Let $c, \varepsilon > 0$, and assume $9216\varepsilon \leq c \leq 1/2$. Let S be a closed set with $|S| \geq cr$ in which every point-color class has size at most εr. Then after individualizing some $O((1/c)^2 \log(k/\varepsilon))$ points, every point-color class in the naive-stable refinement has size less than $64\varepsilon r$.*

We prove Lemma 4.2.3 in Section 4.2.2. The idea is the following. Assume the set S satisfies the hypotheses of the lemma, and suppose A is a large color class. Given a random point p, since A and S are both large, many of the blocks containing both p and a point of S will intersect A. If p is individualized, then these blocks will inherit colors from their intersection with S. Hence, A will be split into smaller color classes according to its intersection with these blocks. Lemma 4.2.10 below will estimate just how likely it is that A is split favorably by such an individualization.

Our third target is to improve the second target by a polylogarithmic factor: we will ensure that every color class has size at most $\varepsilon(\log(k-1)/\log n)^2 r$ for some small constant $\varepsilon > 0$. To that end, we prove the following lemma in Section 4.2.3.

Lemma 4.2.4. *For every $\varepsilon > 0$, there is a $\delta > 0$ such that if every color class has size at most δr, then after individualizing some set of $O(\log n)$ points, every color class in the naive-stable refinement has size at most $\varepsilon(\log(k-1)/\log n)^2 r$.*

We prove Lemma 4.2.4 by observing that when the Steiner design is already relatively finely colored, the point-color classes within a tower grow more slowly than the tower itself. Thus, we obtain a closed set with improved granularity, and extend it to the entire design by again using Lemma 4.2.3.

Our final target is a discrete coloring of the entire design, achieved using the following lemma.

Lemma 4.2.5. *There is a constant $\varepsilon > 0$ such that if every color class has size at most $\varepsilon(\log(k-1)/\log n)^2 r$, then naive refinement is $O(\log n/\log k)$-effective.*

Lemma 4.2.5 is proved using an enhanced version of the same technique used to prove Lemma 4.2.4. The stronger assumption that every color class has size at most $\delta(\log(k-1)/\log n)^2 r$ means that now almost every label in the tower corresponds to a point which receives a unique color after individualizing the apexes of the tower. On the other hand, by Corollary 4.1.7, the labels are nearly uniformly distributed over the points of the design, so *almost* every point receives a unique color in the stable refinement. It is then a simple matter to ensure that every point receives a unique color.

Proof of Theorem 4.2.1. Let c be the constant given by Lemma 4.2.2. Let ε_0 be the constant ε given by Lemma 4.2.5. Let δ_0 be the constant δ given by Lemma 4.2.4 when $\varepsilon = \varepsilon_0$. Let $\varepsilon = \min\{c/9216, \delta_0/64\}$.

By Lemma 4.2.2, after $O(\log n)$ individualizations, we obtain a closed set of size at least cr in which every color class has size at most εr. Then, by Lemma 4.2.3, after individualizing an additional $O(\log k)$ points, we ensure that every point-color class in the entire design has size at most $64\varepsilon r \leq \delta_0 r$. By Lemma 4.2.4, an additional $O(\log n)$ individualizations ensure that every point-color class has size at most $\varepsilon_0(\log(k-1)/\log n)^2 r$. Hence, by Lemma 4.2.5,

a final individualization of $O(\log n/\log k)$ points suffices to ensure that the Steiner design is discretely colored in the stable refinement. □

4.2.1 Increasing the Granularity

The following estimate will ensure that if A is a large closed set, then after individualizing a random block B, some subset of B is likely to have comparable granularity to A.

Lemma 4.2.6. *Let $A \subseteq \mathcal{P}$ be a closed set in which every color class has size at most m, and let $\alpha > 1$. Let B be a random block. Then after individualizing B, the expected number of points in $A \cap B$ belonging to a color class of size at most $1+\alpha m/r$ is at least $(k/n)(1-1/\alpha)|A|$.*

Proof. For $p \in A$, let $s(p)$ denote the size of the color class containing p. Of the r blocks incident with p, at most $(s(p)-1)r/(\alpha m)$ blocks intersect this color class in more than $\alpha m/r$ other points. Now let $\vartheta(p)$ be the indicator variable for the event that $p \in B$ and at most $\alpha m/r$ other points with the same color are in B. Thus, since $|\mathcal{B}| = (n/k)r$, the expected number of points in B for which at most $\alpha m/r$ other points of the same color lie in B, is

$$\begin{aligned}
\mathbb{E}_B\left(\sum_{p\in A}\vartheta(p)\right) &\geq \sum_{p\in A}\frac{1}{|\mathcal{B}|}\left(r-\frac{(s(p)-1)}{\alpha m}r\right)\\
&= \frac{k}{n}\left(\sum_{p\in A}1-\frac{s(p)-1}{\alpha m}\right)\\
&\geq \frac{k|A|}{n}\left(1-\frac{m-1}{\alpha m}\right)\\
&> \frac{k|A|}{n}\left(1-\frac{1}{\alpha}\right).
\end{aligned}$$

□

Lemma 4.2.7. *Let $0 < \varepsilon \leq 1/2$, and let $A \subseteq \mathcal{P}$ be a closed set with granularity g. Let $0 < \varepsilon \leq 1/2$ and suppose some color class in A has size greater than εr. Then (for n sufficiently large) after individualizing some set of $O(1/\varepsilon)$ points, the naive-stable refinement has a closed set S of granularity at least $8g$.*

Proof. Let A be a closed set with granularity g. Let m be the size of the largest color class in A, and suppose $m > \varepsilon r$. We assume n is sufficiently large that $r > 8/\varepsilon$.

We claim that after individualizing at most $O(1/\varepsilon)$ points, the stable refinement has a closed set S of size $|S| > 16|A|/(\varepsilon r)$ in which every color class has size at most $2m/(\varepsilon r)$. Hence, S will have granularity $> 8g$. We define S iteratively: at each step, we individualize a block (by individualizing two points on the block), and augment S by points belonging to color classes of size at most $2m/(\varepsilon r)$ in the stable refinement. We stop when $|S| > 16|A|/(\varepsilon r)$.

Suppose $S \subseteq A$ has size less than $16|A|/(\varepsilon r) < |A|/2$. We apply Lemma 4.2.6 with $A \setminus S$ in place of A, and $\alpha = 2$. Hence, there exists a block B such that at least $(1/2)(k/n)|A \setminus S| > |A|/(4r)$ points in $(A \setminus S) \cap B$ belong to a color class intersecting B in at most $1 + 2m/r < 2m/(\varepsilon r)$ points. Thus, by individualizing B (or rather, two points on B) and adding its small point-color classes to S, we augment the size of S by at least $|A|/(4r)$. Hence, repeating this process at most $64/\varepsilon$ times, we guarantee that $|S| > (64/\varepsilon)(|A|/(4r)) = 16|A|/(\varepsilon r)$, as desired. □

Lemma 4.2.8. *Suppose $A \subseteq \mathcal{P}$ is a closed set with granularity g. Then after individualizing some $O(\log n/\log k)$ points, the naive-stable refinement has a closed set S of size $|S| = \Omega(r)$ and granularity at least $g/4$.*

Proof. Let m_0 be the size of the largest color class in $A_0 = A$. We define recursively a sequence $p_1, \ldots, p_d$ of points in $\mathcal{P}$ as follows. When A_i is defined and $|A_i| \leq (\log(k-1)/\log n)r$, by Lemma 4.1.1 let p_{i+1} be such that

$$|C_{p_{i+1}}(A_i)| \geq (k-1)\left(1 - \frac{(k-2)|A_i|}{n}\right)|A| > (k-1)\left(1 - \frac{\log(k-1)}{\log n}\right)|A_i|\,,$$

and define $A_{i+1} = C_{p_{i+1}}(A_i)$. Hence, $|A_i| > (k-1)^i(1 - \log(k-1)/\log n)^i|A_0|$. For $s = \log n/\log(k-1)$, we have

$$(k-1)^s\left(1 - \frac{\log(k-1)}{\log n}\right)^s \sim \frac{n}{\mathrm{e}} \gtrsim \left(\frac{\log(k-1)}{\log n}\right)r.$$

Thus for some $d \lesssim s$, we have that $|A_d| > (\log(k-1)/\log n)r$.

Note that after individualizing $p_1, \ldots, p_i$, the set A_i is closed in the stable refinement. Let m_i denote the size of the largest color class in the stable refinement of A_i. Observe that $m_i \leq (k-1)m_{i-1}$, so $m_i \leq (k-1)^i m_0$. Hence, the granularity of A_d is

$$\frac{|A_d|}{m_d} \geq \left(1 - \frac{\log(k-1)}{\log n}\right)^d \cdot \frac{|A_0|}{m_0} \gtrsim \frac{|A_0|}{\mathrm{e}m_0}.$$

Thus, for n sufficiently large, the granularity of A_d is at least $1/3$ the granularity of A.

If $|A_d| > r/4$, we are done. Otherwise, suppose $S \subset \mathcal{P}$ is such that $A_d \subseteq S$ and $|S| \leq r/4$. Let $p \in \mathcal{P}$ be a random point. By Lemma 4.1.1, we have $\mathbb{E}(|C_p(A_d)|) \geq (3/4)(k-1)|A_d|$. By Lemma 4.1.3, we have $\mathbb{E}(|C_p(A_d) \cap S \setminus A_d|) < (1/4)|A_d|$. Hence, since $k \geq 3$,

$$\begin{aligned}
\mathbb{E}(|C_p(A_d) \setminus S|) &= \mathbb{E}(|C_p(A_d)| - |A_d| - |C_p(A_d) \cap S \setminus A_d|) \\
&> \frac{3}{4}(k-1)|A_d| - |A_d| - \frac{1}{4}|A_d| \\
&\geq \frac{1}{8}(k-1)|A_d|.
\end{aligned}$$

Let $S_0 = A_d$, and while $|S_i| < r/4$, define $S_{i+1} = S_i \cup C_p(A_d)$, where $p = p_{i+1}$ is such that $|C_p(A_d) \setminus S| > (1/8)(k-1)|A_d|$. Since $|A_d| = \Omega(r \log k/\log n)$, there is some $d' = O(1 + \log n/(k \log k))$ such that $|S| \geq r/4$, where $S = S_{d'}$. After individualizing $p_1, \ldots, p_{d'}$, the set S is closed in the stable refinement. Furthermore, every color class in S has size at most $(k-1)m_d$, while by Lemma 4.1.1 we may ensure that $|S| \geq (3/4)(k-1)|A_d|$. Hence, the granularity of S is at least $1/4$ the granularity of A. □

Proof of Lemma 4.2.2. Fix $\varepsilon > 0$. Suppose A is a closed set of size $|A| = \Omega(r)$ and granularity g. If some color class in A has size greater than εr, then by applying Lemma 4.2.7 followed by Lemma 4.2.8, we obtain a new set $|A'|$ of size $\Omega(r)$ and granularity $\geq 2g$, at a cost of $O(1/\varepsilon + \log n/\log k)$ individualizations. Hence, starting from the set $A_0 = \mathcal{P}$, we obtain a sequence of sets A_i, each of which has size $|A_i| = |\Omega(r)|$, and with A_i having granularity

at least twice that of A_{i-1}. We can recursively define such sets A_i until we can no longer apply Lemma 4.2.7, i.e., when some set A_d is such that every color class has size at most εr. This is guaranteed to be the case if the granularity of A is $\Omega(k/\varepsilon)$. In particular, it suffices to double the granularity at most $O(\log(k/\varepsilon))$ times. Hence, we obtain the desired closed set after at most $O(\log(k/\varepsilon)(1/\varepsilon + \log n/\log k))$ individualizations. □

4.2.2 Extending the Fine Coloring of a Hyperplane

In this section, we prove Lemma 4.2.3, which lets us extend a fine coloring of a large subset of the space to the entire space at the cost of a logarithmic number of individualizations.

We use the following notion of a ζ-*split* to quantify progress in extending a fine coloring in the proof of Lemma 4.2.3.

Definition 4.2.9. Let $0 < \zeta < 1$, $p \in \mathcal{P}$, and $A \subseteq \mathcal{P}$ a color class. Then A is ζ-*split* by p if after individualizing p, every point-color class in the naive-stable refinement has size at most $(1-\zeta)|B|$.

In particular, if by individualizing a random point, we have a positive probability of obtaining a ζ-split of any large color class for some ζ not too small, then by individualizing a logarithmic number of points, we can eliminate all large color classes. The following lemma shows that we indeed have a positive probability of obtaining a ζ-split under appropriate conditions.

Lemma 4.2.10. *Let $c, \varepsilon > 0$, and assume $\varepsilon \leq c/256$. Let S be a closed set such every color class in S has size less than εr. Let let $A \subseteq \mathcal{P}$ be a color class with $|C_q(S)| \geq cn$ for some (hence, every) $q \in A$. Then there exists a $\zeta = \Omega(c)$, with $\zeta \leq 1/2$, such that if $|A| \geq 8\varepsilon r$ and $p \in \mathcal{P}$ is chosen at random, then*

$$P[A \text{ is } \zeta\text{-split by } p] = \Omega(c)$$

Proof. By Lemma 4.1.2, for any $q \in A$ we have $P[q \notin C_p(S)] < 1 - c(k-2)/(k-1)$. Thus, $\mathbb{E}(|A \setminus C_p(S)|) < (1 - c(k-2)/(k-1))|A|$, and so for any $0 < \zeta < 1$, Markov's inequality gives

$$\begin{aligned} P[|A \cap C_p(S)| < \zeta|A|] &= P[|A \setminus C_p(S)| \geq (1-\zeta)|A|] \\ &< \frac{1 - c(k-2)/(k-1)}{1-\zeta} \end{aligned}$$

which is at most $1 - c/4$ for some $c/4 < \zeta \leq 1/2$.

Let $\mathcal{S}$ denote the collection of point-color classes in S, and for a random point $p \in \mathcal{P}$, let

$$\sigma = P[\exists T \in \mathcal{S} \text{ such that } |C_p(T) \cap A| \geq (1-\zeta)|A|].$$

We will show that $\sigma < 32\varepsilon$. The lemma then follows, since with probability at least $1 - (1 - c/4) - \sigma = \Omega(c)$, at least a ζ-fraction of A is covered by $C_p(S)$, but there is no $T \in \mathcal{S}$ such that $C_p(T)$ covers a $(1-\zeta)$-fraction of A.

Suppose $p \in \mathcal{P}$ and $T \in \mathcal{S}$ are such that $|C_p(T) \cap A| \geq (1-\zeta)|A|$. Let $D = C_p(T) \cap A \setminus \{p\}$. For $q \in T$, let $D_q = \overline{pq} \cap D$, so the D_q partition D. Let $\mathcal{D}$ denote the collection of the nonempty sets D_q for $q \in T$, and let $m = |\mathcal{D}| \leq |T| \leq \varepsilon r$. The average size of a set in $\mathcal{D}$ is $|D|/m$, so at least half the points $x \in D$ belong to a set D_q with $|D_q| \geq |D|/(2m)$. Note that $\overline{px} = \overline{pq}$ if $x \in D_q$. Hence, by the choice of p and T, at least a $(1-\zeta)/2$-fraction of the points $x \in A \setminus \{p\}$ satisfy

$$|\overline{px} \cap A| > \frac{(1-\zeta)|A|}{2m} \geq \frac{(1-\zeta)|A|}{2\varepsilon r} \tag{4.3}$$

Hence, since $|C_p(T) \cap A| \geq (1-\zeta)|A|$ with probability σ over the choice of p, it follows that for a random pair $(p, x) \in \mathcal{P} \times A$ of distinct points, the probability that Eq. (4.3) holds is at least $\sigma(1-\zeta)/2$. Hence, there exists some point $x \in A$ such that for at least $\sigma(1-\zeta)(n-1)/2$ points $p \in \mathcal{P}/ \setminus \{x\}$, Eq. (4.3) holds. Hence, at least $\sigma(1-\zeta)(r/2)$ lines

containing x intersect A in more than $(1-\zeta)|A|/(2\varepsilon r)$ points. Since $|A| \geq 8\varepsilon r \geq 4\varepsilon r/(1-\zeta)$, we have

$$|A| > 1 + \frac{\sigma(1-\zeta)r}{2}\left(\frac{(1-\zeta)|A|}{2\varepsilon r} - 1\right) > \frac{\sigma(1-\zeta)^2|A|}{8\varepsilon}.$$

Thus $\sigma < 32\varepsilon$, completing the proof. □

The following elementary fact about bounded random variables will be used in the proof of Lemma 4.2.3.

Fact 4.2.11. *Let X be a random variable such that $0 \leq X \leq M$ and $\mathbb{E}(X) = m$. Then for every $\varepsilon > 0$, we have $P(X > (1-\varepsilon)m) \geq \varepsilon/((M/m) - 1 + \varepsilon)$. In particular, $P(X > m/2) \geq 1/(2(M/m) - 1)$.*

Proof. Let $p = P(X > (1-\varepsilon)m)$. We have $m \leq MP(X > (1-\varepsilon)m) + (1-\varepsilon)mP(X \leq (1-\varepsilon)m) = Mp + (1-\varepsilon)m(1-p) = p(M - (1-\varepsilon)m) + (1-\varepsilon)m$. □

We conclude this section with the proof of Lemma 4.2.3.

Proof of Lemma 4.2.3. By Lemma 4.1.1, we have $\mathbb{E}(|C_p(S)|) \geq (1/2)cn$. Since $|C_p(S)| \leq n$ for all $p \in \mathcal{P}$, by Fact 4.2.11 we have $P(|C_p(S)| > (1/4)cn) > 1/(4/c + 1) \geq (2/9)c$. Let $U \subseteq \mathcal{P}$ be the collection of points p such that $|C_p(A)| > (1/4)cn$, so $|U| \geq (2/9)cn$. Note that U is a closed set.

We will first guarantee that no point-color class in U has size greater than $8\varepsilon r$, at a cost of $O((1/c^2)\log(k/\varepsilon))$ individualizations. We define a potential function ϕ on colorings of U, with the property that when ϕ is small, every point-color class in U is also small. We then show that there is always a point whose individualization decreases the value of ϕ by a factor of $(1 - \Omega(c^2))$.

In particular, given a collection $\mathcal{T}$ of subsets of U, let $\phi(\mathcal{T}) = \sum_{T in \mathcal{T}} |T|^2$. Let $\mathcal{C}$ be the collection of point-color classes of size at least $8\varepsilon r$ in U, and note that $\phi(\mathcal{C}) \leq n^2$. Choose $p \in \mathcal{P}$ at random, and let $\mathcal{C}_p$ be the collection of color classes in U of size at least $8\varepsilon r$ in the stable refinement after individualizing p. For $C \in \mathcal{C}$, let X_C be the collection of subsets

of C in $\mathcal{C}_p$. By Lemma 4.2.10, the set C is ζ-split by p with probability at least σ, where $\zeta, \sigma = \Omega(c)$ and $\zeta \leq 1/2$. Thus,

$$\begin{aligned}\mathbb{E}_p(\phi(X_C)) &\leq (1-\sigma)|C|^2 + \sigma(\zeta^2 + (1-\zeta)^2)|C|^2 \\ &< (1-\sigma\zeta)|C|^2.\end{aligned}$$

Hence, $\mathbb{E}_p(\mathcal{C}_p) \leq (1-\Omega(c^2))\phi(\mathcal{C})$, so some point $p \in \mathcal{P}$ achieves this expectation. Hence, by individualizing at most $O((1/c^2)\log(k/\varepsilon))$ points, we guarantee that $\phi(\mathcal{C})$ is reduced by a factor of at least $k^2/(64\varepsilon^2)$, i.e., $\phi(\mathcal{C}) < 64\varepsilon^2(n^2/k^2)$. Hence, we guarantee that every point-color class in U has size at most $8\varepsilon(n/k) < 8\varepsilon r$.

Now since $|U| \geq (2/9)cn$, we have $|C_p(U)| \geq (2/9)cn$ for every point p. Thus, the lemma follows by the repeating the argument of the previous paragraph with the set $\mathcal{P}$ in place of U, the set U in place of S, and the threshold $8\varepsilon r$ replaced with the threshold $64\varepsilon r$. The assumption $9216\varepsilon < c$ guarantees we can apply Lemma 4.2.10. □

4.2.3 Simple Points

Let B be a (possibly truncated) block. We say that $x \in B$ is a *simple point* of B with respect to a coloring γ if x is the only point of its color on B. Note in particular that the single point of a degenerate truncated block is always simple. We note that if a block has a unique color, the next refinement step assigns unique colors to each of the simple points of the block.

We claim that if the size of each color class is much smaller than r then most points of most blocks are simple. Here is a formal statement.

Proposition 4.2.12. *Let $\delta > 0$ and suppose each color class has size at most $1 + \delta r$. Then for a random block B the expected number of non-simple points of B is $\leq \delta k$. Hence, for a random block B, the probability that B has more than $\sqrt{\delta}k$ non-simple points is less than $\sqrt{\delta}$.*

Proof. Let m be the maximum size of a point-color class. For a point p, the number of lines of which p is a non-simple point is at most $m-1$. So the total number of pairs (p, B) such that p is a multiple point of B is at most $n(m-1)$. These incidences are distributed among the $(n/k)r$ blocks, so the average number of multiple points per block is at most $(m-1)k/r \leq \delta k$.

The last statement of the proposition follows by Markov's inequality. □

Corollary 4.2.13. *Let f_d be a random d-dimensional tower over a random sequence of points $(p_0, \ldots, p_d)$. Fix $x \in [k-1]^d$. For $1 \leq j \leq d$, the probability that $f_j(x)$ is not a simple point of $B(p_j, f_{j-1}(k))$ is at most $2\sqrt{\delta}$.*

Proof. If $f_{j-1}(x) = p_j$, then $f_j(x)$ is a simple point of $B(p_j, f_{j-1}(x))$. Otherwise, since $f_{j-1}(x)$ and p_j are independent, random points by Lemma 4.1.4, they determine a random block $B = \overline{f_{j-1}(x)q}$. By Proposition 4.2.12, the probability that B has at least $\sqrt{\delta}k$ non-simple points is at most $\sqrt{\delta}$. If ℓ has fewer than $\sqrt{\delta}k$ non-simple points, then since p_j and $f_{j-1}(x)$ are random points of ℓ, so is $f_j(x)$, so the probability that $f_j(x)$ is a non-simple point of $\ell(f_{j-1}(x), p_j)$ is at most $\sqrt{\delta}$. Thus, the overall probability that $f_j(x)$ is not a simple point is at most $2\sqrt{\delta}$. □

Proposition 4.2.14. *Let f_d be a random d-dimensional tower over a random sequence of points $(p_0, \ldots, p_d)$. Let $x \in [k-1]^d$, let $s(x)$ be the number of indices $1 \leq j \leq d$ such that $f_j(x)$ is a simple point of $B(p_j, f_{j-1}(x))$. Then after individualizing the points $p_0, \ldots, p_d$, the color class containing $f_d(x)$ in the naive-stable refinement has at most $(k-1)^{d-s(x)}$ points.*

Proof. By induction on d, with the base case $d = 0$ clear since p_0 is individualized. Let A_1 be the color class containing $f_{d-1}(x)$ and A_2 the color class containing $f_d(x)$ in the naive-stable refinement after individualizing $p_1, \ldots, p_{d-1}$ (but before individualizing p_d).

If $f_d(x) = p_d$, then $f_d(x)$ gets a unique color after individualizing p_d. More generally, if $f_d(x)$ is a simple point of $B(p_d, f_{d-1}(x))$, then after individualizing p_d and refining to

a stable coloring, a point p gets the same color as $f_d(x)$ only if (i) $p \in B(p_d, q)$ for some $q \in A_1$; (ii) p is a simple point of $B(p_d, q)$; and (iii) $p \in A_2$. Thus, each of the at most $|A_1|$ truncated blocks $B(p_d, q)$ with $q \in A_1$ contributes at most one point to the color class containing $f_d(x)$ in the stable refinement, so the number of points in that class is at most

$$|A_1| \leq (k-1)^{d-1-s(x^{d-1})} = (k-1)^{d-s(x)}\,.$$

On the other hand, if $f_d(x)$ is not a simple point of the truncated block $B(p_d, f_{d-1}(x))$, then since $f_d(x) \in C_{p_d}(A)$ and $C_{p_d}(A)$ is a closed set with $|C_{p_d}(A)| \leq (k-1)|A|$, it follows that the color class containing $f_d(x)$ in the stable refinement has size at most $(k-1)^{d-s(x)}$, as desired. □

Lemma 4.2.15. *For every $\varepsilon > 0$, there is a $\delta > 0$ such that the following holds. Suppose $(k-1) < n^{\delta}$ and every point-color class has size at most $1 + \delta r$. Then after individualizing some set of size $O(\log n)$, every point-color class has size at most $O(n^{\varepsilon})$ in the naive-stable refinement.*

Proof. Let $\varepsilon > 0$, and assume without loss of generality that $\varepsilon < 1/2$. Let $\delta = (\varepsilon/65)^2$. Let d be the integer such that

$$\frac{n}{k-1} < (k-1)^d \leq n,$$

and let f_d be a random d-dimensional tower over a random sequence π of points $p_0, \ldots, p_d$. Let $T = \mathrm{im}(f_d)$. By Corollary 4.1.6, we have $\mathbb{E}(|T|) > (k-1)^d/2$. Since $|T| \leq (k-1)^d$ for any d-dimensional tower, by Markov's inequality we have

$$P\left[|T| \leq \frac{(k-1)^d}{4}\right] \leq P\left[(k-1)^d - |T| \geq \frac{3(k-1)^d}{4}\right] \leq \frac{2}{3}\,.$$

Fix $x \in [k-1]^d$, and let $s(x)$ be as in the statement of Proposition 4.2.14. By Corollary 4.2.13, we have $\mathbb{E}_{\pi, f_d}(s(x)) \geq d(1 - 2\sqrt{\delta})$. Thus, since $s(x) \leq d$, by Markov's inequality the probability over π that $\mathbb{E}_{f_d}(d - s(x)) \geq 8\sqrt{\delta}d$ is at most $1/4$. Therefore, with probability

at least $1 - 2/3 - 1/4 > 0$, for a random sequence π of d points, a random tower over π has $|T| > (1/4)(k-1)^d$ and $\mathbb{E}_{f_d}(d - s(x)) < 8\sqrt{\delta}$. Let π be such a sequence. Individualize the points of π and refine to the naive-stable coloring.

Again by Markov's inequality, with probability at least $7/8$ over the choice of f_d, we have $d - s(x) < 64\sqrt{\delta}d$. Hence, for fixed f_d and random $x \in [k-1]^d$, we have $d - s(x) < 64\sqrt{\delta}d$ with it follows that $7/8$ of the labels $x \in [k-1]^d$ have $d - s(x) < 64\sqrt{\delta}d$. Now for a point $p \in T$, by Proposition 4.2.14, there are at most $(k-1)^{d-s}$ points in the color class containing p, where $s = \max\{s(x) : f_d(x) = p\}$. Thus, if p belongs to a color class of size more than $(k-1)^{64\sqrt{\delta}d}$, then p has a label $x \in [k-1]^d$ with $d - s(x) \geq 64\sqrt{\delta}$; hence, at most $(1/8)(k-1)^d$ points $p \in T$ belong to color classes of size more than $(k-1)^{64\sqrt{\delta}d}$ in the stable refinement. Therefore, there is a closed subset A of T with $|A| \geq |T| - (1/8)(k-1)^d \geq (1/8)(k-1)^d$ in which the maximum size of a color class is $m \leq (k-1)^{64\sqrt{\delta}d}$. It follows that

$$\begin{aligned}\frac{|A|}{m} &\geq \frac{1}{8}(k-1)^{(1-64\sqrt{\delta})d} \geq \frac{1}{8}\left(\frac{n}{k-1}\right)^{1-64\sqrt{\delta}} \\ &\geq \frac{1}{8}n^{(1-\delta)(1-64\sqrt{\delta})}.\end{aligned}$$

Now by Lemma 4.2.8, by individualizing $O(\log n / \log k)$ additional points and refining to a stable coloring, we obtain a closed set S of size $\Omega(r)$ whose granularity is at least $1/4$ that of A. Hence, since $|S| \leq n$, every color class in S has size at most m', where

$$\begin{aligned}m' &\leq 32n^{1-(1-\delta)(1-64\sqrt{\delta}} \\ &= O(n^{\delta+64\sqrt{delta}}) = O(n^{\varepsilon})\end{aligned}$$

Now $n^{\varepsilon} = o(r)$ since $\varepsilon < 1/2$ and $r = (n-1)/(k-1) = \Omega(\sqrt{n})$. Hence, by Lemma 4.2.3, by individualizing some $O(\log(kr)) = O(\log n)$ points, we guarantee that every color class has size $O(n^{\varepsilon})$ in the stable refinement. □

Proof of Lemma 4.2.4. Let δ_0 be the constant δ given by Lemma 4.2.15 when $\varepsilon = 1/4$.

Now fix any $0 < \varepsilon < 1$, and let $\delta = \varepsilon\delta_0^2$. Suppose every color class has size at most δr. If $(k-1) \geq n^{\delta_0}$, we have $(\log(k-1)/\log n)^2 \geq \delta_0^2$, so every color class has size at most $\varepsilon(\log(k-1)/\log n)^2 r$ and we are already done. Otherwise, $(k-1) < n^{\delta_0}$. In this case, by Lemma 4.2.15, individualizing some $O(\log n)$ points, we guarantee that every color class has size at most $O(n^{1/4}) = o((\log(k-1)/\log n)^2 r)$. □

4.2.4 Discrete Coloring

Given a d-dimensional tower f over a sequence $(p_0, \ldots, p_d)$ of points, we say a label $x \in [k-1]^d$ is *simple* if $f_j(x^j)$ is a simple point of $B(p_j, f_{j-1}(x))$ for every j. The following two observations follow immediately from Proposition 4.2.14 and Corollary 4.2.13, respectively.

Observation 4.2.16. *All points with at least one simple label from f receive unique colors after individualizing $p_0, \ldots, p_d$ and a refining to a stable coloring.*

Observation 4.2.17. *Let f_d be a random d-dimensional tower over a random sequence of points $(p_0, \ldots, p_d)$, and fix $x \in [k-1]^d$. Assume each point-color class has size at most $1 + \delta r$. Then the probability that x is a simple label is at least $1 - 2\sqrt{\delta}d$.*

Lemma 4.2.18. *Suppose more than $(k-3)+r$ points of a Steiner design have unique colors. Then the naive-stable refinement is discrete.*

Proof. Let U be the set of points with unique colors and let $p \in \mathcal{P} \setminus U$. If a block B is such that $|B \cap U| \geq 2$ then B has a unique color in the stable refinement. If two such blocks B both contain p, then p has a unique color in the stable refinement. So if p does not have a unique color in the stable refinement, then at most one block B containing p has more than one point in U. Furthermore, this block B has at most $k-2$ points in U, since if every point in $B \setminus \{p\}$ has a unique color, then p will also receive a unique color in the stable refinement. Hence, $|U| \leq (k-2) + (r-1)$, where the first term counts the points in $B \cap U$; the number of remaining blocks containing p is $r-1$. □

Proof of Lemma 4.2.5. Let $\varepsilon = 2^{-12}$, and assume each point-color class has size at most $\varepsilon(\log(k-1)/\log n)^2 r$. Let d be minimal such that $(k-1)^{d/2} \geq 4n$, so in particular $d < 4\log n/\log(k-1)$. Let f be a random d-dimensional tower over a random sequence of points $(p_0, \ldots, p_d)$.

By Observation 4.2.17, the expected proportion of labels that are not simple is at most $2^{-6}(\log(k-1)/\log n)d < 1/16$, so by Markov's inequality, with probability at least $1/2$, the actual proportion is at most $1/8$.

Setting $\beta = 2$ in Corollary 4.1.7, we see that with probability at least $3/4$, the labels are distributed nearly uniformly over $\mathcal{P}$ in the sense that each point has at least half its expected number $(k-1)^d/n$ of labels, since $2(k-1)^{d/2} \leq (k-1)^d/(2n)$.

Thus, with probability at least $1/4$, both of the above events occur, i.e., at most $1/8$ of the labels are not simple, and every point in $\mathcal{P}$ gets at least $(k-1)^d/(2n)$ labels. Let $(p_0, \ldots, p_d)$ be a sequence of points such that these two events occur. Then the number of points which do not get simple labels is at most $(1/8)(k-1)^d/((k-1)^d/(2n)) < n/4$. Since at least $3/4$ of the points get at least one simple point, at least this number get unique colors after individualizing $p_0, \ldots, p_d$ and refining to a stable coloring. Thus, by Lemma 4.2.18, stable refinement is discrete. □

4.3 Balanced Incomplete Block Designs

We now construct an infinite family of $S_2(n, 3, 2)$ balanced incomplete block designs with $\exp(\Omega(n))$ automorphisms.

Let $\mathfrak{X}$ be a $S(2, 3, n)$ design, a Steiner triple system on n points. We construct from $\mathfrak{X}$ a $S_2(2, 3, 4n)$ design $D(\mathfrak{X})$ as follows. For every point x of $\mathfrak{X}$ and every $0 \leq i, j \leq 1$, we define a point x_{ij} of $D(\mathfrak{X})$. We define two types of blocks.

1. For every point x of $\mathfrak{X}$, let $S_x = \{x_{ij} : 0 \leq i, j \leq 1\}$, and include as a block of $D(\mathfrak{X})$ every triple in S_x.

2. For every line $\{x, y, z\}$ of $\mathfrak{X}$, include as a block of $D(\mathfrak{X})$ every triple of the form $\{x_{ij}, y_{k\ell}, z_{st}\}$ where $0 \leq i, j, k, \ell, s, t \leq 1$ and $s \equiv i + k \mod 2$.

Proposition 4.3.1. *Let $\mathfrak{X}$ be a $S(2, 3, n)$ design. Then the incidence structure $D(\mathfrak{X})$ is a $S_2(2, 3, 4n)$ design, and $|\operatorname{Aut}(D(\mathfrak{X}))| \geq 2^{2n}$.*

Proof. We first observe that every pair of distinct points in $D(\mathfrak{X})$ is contained in exactly two blocks. Indeed, let x_{ij} and $y_{k\ell}$ be distinct points of $D(\mathfrak{X})$. If $x = y$, then there are exactly two triples in case 1 above which contain both x_{ij} and $x_{k\ell}$, and no block from case 2 contains both, and if $x \neq y$ the opposite is true. Hence, $D(\mathfrak{X})$ is a $S_2(2, 3, 4n)$.

Now for any point x of $\mathfrak{X}$ and $0 \leq i \leq 1$, there is an automorphism $\phi_{x,i}$ of $D(\mathfrak{X})$ which transposes x_{i0} and x_{i1} while fixing all other points. Since the automorphisms $\phi_{x,i}$ have disjoint support, $|\operatorname{Aut}(D(\mathfrak{X}))| \geq 2^{2n}$ as claimed. □

Chapter 5

CLIQUE GEOMETRIES

In this chapter we develop sufficient conditions for the existence of clique geometries in sub-amply regular graphs and in primitive coherent configurations. We study the implications of clique geometries for distance-regular graphs, and the line-graphs of partial geometries.

5.1 Sub-Amply Regular Graphs

5.1.1 Metsch's Sufficient Condition

Metsch's Theorem 2.7.5, a sufficient condition for the existence of clique geometries in sub-amply regular graphs, was stated in Section 2.7.1. We have the following, simpler statement as a corollary to Metsch's theorem.

Corollary 5.1.1. *Let G be a* SubAR(v, ρ, λ, μ) *graph such that*

$$(\lambda+1)^2 > (3\rho+\lambda+1)(\mu-1). \tag{5.1}$$

Then the maximal cliques of order at least $\lambda+2-(\lceil(3/2)\rho/(\lambda+1)\rceil-1)(\mu-1)$ *form a clique geometry.*

Proof. Suppose $(\lambda+1)^2 > (3\rho+\lambda+1)(\mu-1)$, and set $t = \lceil 3\rho/(2(\lambda+1))\rceil$. We then have

$$\begin{aligned}(2t-1)(\mu-1) &< \left(2\left(\frac{3\rho}{2(\lambda+1)}+1\right)-1\right)(\mu-1)\\ &= \frac{1}{\lambda+1}(3\rho+\lambda+1)(\mu-1) < \lambda+1.\end{aligned}$$

Furthermore,

$$\begin{aligned}(t+1)\left((\lambda+1)-\frac{1}{2}t(\mu-1)\right) &> \left(\frac{3}{2}\rho+\lambda+1\right)\left(1-\frac{1}{2(\lambda+1)^2}\left(\frac{3}{2}\rho+\lambda+1\right)(\mu-1)\right)\\ &= \frac{((3/2)\rho+\lambda+1)^2}{3\rho+\lambda+1}\left(\frac{3\rho+\lambda+1}{(3/2)\rho+\lambda+1}-\frac{1}{2}\right)\\ &> \frac{1}{4}\left(\frac{9}{2}\rho+\lambda+1\right) > \rho\,.\end{aligned}$$

The corollary then follows from Theorem 2.7.5. □

We now prove the following asymptotic simplification of Corollary 5.1.1.

Theorem 5.1.2. *Let G be a* SubAR(v,ρ,λ,μ) *graph such that that $\rho\mu = o(\lambda^2)$. Then G has a clique geometry with cliques of order $\sim\lambda$, and all maximal cliques not in the geometry have order $o(\lambda)$.*

The core of the proof is Lemma 5.1.4 below, a consequence of Metsch's [Met91, Theorem 1.2]. The simplification in our proof results from our use of the following lemma, implicit in Spielman [Spi96, Lemma 17].

Lemma 5.1.3 (Spielman)**.** *Let G be a graph on ρ vertices which is regular of degree λ and such that any pair of nonadjacent vertices has at most $\mu-1$ common neighbors. Then for any vertex x, there are at most $(\rho-\lambda-1)(\mu-1)$ ordered pairs of nonadjacent vertices in $G(x)$.*

Proof. Let X be the number of ordered pairs of nonadjacent vertices in $G(x)$, and let K be the number of ordered pairs of adjacent vertices in $G(x)$, so $K+X=\lambda(\lambda-1)$. Let P be the number of ordered pairs (a,b) of vertices such that (x,a,b) induces a path of length 2 (x and b are not adjacent, and a is adjacent to both). For every neighbor a of x, and every neighbor $b\neq x$ of a, the pair (a,b) is counted in either K or P, so $K+P=\lambda(\lambda-1)$ and so $P=X$. On the other hand, there are $\rho-\lambda-1$ vertices not adjacent to x, each of which has at most $\mu-1$ common neighbors with x, and so $X=P\leq(\rho-\lambda-1)(\mu-1)$. □

Lemma 5.1.4 (Clique Partition Lemma (Metsch))**.** *Let G be a graph on ρ vertices which is regular of degree λ and such that any pair of nonadjacent vertices has at most $\mu - 1$ common neighbors. Suppose that $\rho\mu = o(\lambda^2)$. Then there is a partition of $V(G)$ into maximal cliques of order $\sim \lambda$, and all other maximal cliques of G have order $o(\lambda)$.*

Proof. Fix a vertex x and consider the induced subgraph H of G on $G^+(x)$. Suppose a and b are distinct non-adjacent vertices of H. They have at most $\mu - 1$ common neighbors in H, so there are at least $\lambda - \mu$ vertices in $H \setminus \{a, b\}$ which are not common neighbors of a and b. Hence, at least one of a and b has codegree at least $\kappa := (\lambda - \mu)/2$ in H (i. e., degree at most $\lambda - \kappa$). Let D be the set of vertices in H of codegree at least κ, and let $C = H \setminus D$. It follows that C is a clique, and clearly $x \in C$.

Now by Lemma 5.1.3, we have $|D|\kappa < (\rho - \lambda - 1)(\mu - 1) = o(\lambda^2)$, and so $|D| = o(\lambda)$. In particular, $C \sim \lambda$, and every element of D has at least one non-neighbor in C. Hence, C is a maximal clique, and every element not in C, having at least one non-neighbor in C, has at most μ neighbors in C. Thus, any maximal clique which contains x as well as a vertex not in C has order at most $|D| + \mu = o(\lambda)$. □

Theorem 5.1.2 then follows immediately by applying Lemma 5.1.4 to the graphs induced by G on $G(x)$ for $x \in V$. □

5.1.2 Bounding λ

We now derive our bound on λ in sub-amply regular graphs, Theorem 2.7.4, from Corollary 5.1.1.

Lemma 5.1.5. *Let $\mathcal{G}$ be a clique geometry in a graph G on v vertices. Suppose every vertex is in at least $r \geq 2$ and at most R cliques of $\mathcal{G}$, and each clique of $\mathcal{G}$ has order at least ℓ. Then*

$$\ell \leq \frac{R}{\sqrt{r(r-1)}}\sqrt{v}.$$

Proof. Let $m = |\mathcal{G}|$ and let N be the number of vertex–clique incidences. Then $\ell m \leq N \leq vR$. Let T be the number of triples (x, C_1, C_2) where $C_1, C_2 \in \mathcal{C}$ and $x \in C_1 \cap C_2$. Then $T = \sum_{x \in V(G)} \deg(x)(\deg(x) - 1) \geq vr(r-1)$. On the other hand, by the intersection assumption, $T \leq m(m-1) < m^2$. Comparing,

$$vr(r-1) < m^2 \leq \left(\frac{nR}{\ell}\right)^2. \qquad \square$$

Proof of Theorem 2.7.4. Case 1. Suppose $(3\rho + \lambda + 1)(\mu - 1) < (\lambda + 1)^2$. Then by Corollary 5.1.1, every edge lies in a clique of the geometry of order at least $\ell := \lambda + 2 - (3/2)\rho(\mu - 1)/(\lambda + 1) > (1/2)(\lambda + 1)$. The number of cliques in the geometry containing a given vertex is at most $R := 2\rho/(\lambda + 1)$, and at least $\rho/(\lambda + 1)$. Let $r = \lceil \rho/(\lambda + 1) \rceil$. Since G is not a disjoint union of cliques, $\lambda + 1 < \rho$, so $r \geq 2$. Applying Lemma 5.1.5 gives $\ell \leq (R/\sqrt{r(r-1)})\sqrt{v} \leq (R/r)\sqrt{2v}$. Hence, $\lambda + 1 < 4\sqrt{2v}$.

Case 2. Otherwise, $(\lambda + 1)^2 \leq (3\rho + \lambda + 1)(\mu - 1)$. Set $\delta = (\sqrt{13} - 1)/6$.

Case 2a. Suppose $\mu - 1 \geq \delta(\lambda + 1)$. Then

$$\lambda + 1 \leq (1/\delta)(\mu - 1) < (1/\delta)\sqrt{\rho(\mu - 1)}. \tag{5.2}$$

Case 2b. Otherwise, $\mu - 1 < \delta(\lambda + 1)$, and we have

$$(1 - \delta)(\lambda + 1)^2 < 3\rho(\mu - 1),$$

which is equivalent to Eq. (5.2) by our choice of δ. The theorem follows by combining Eq. (5.2) with Case 1. $\square$

5.2 Asymptotically Delsarte Distance-Regular Graphs

Godsil [God93] gave the following sufficient condition for a distance-regular graph to be Delsarte geometric.

An *m-claw* in a graph is an induced $K_{1,m}$ subgraph.

Theorem 5.2.1 (Godsil [God93])**.** *Let G be a distance-regular graph with least eigenvalue τ. If there are no m-claws in G with $m > |\tau|$ and*

$$\lambda + 1 > (2|\tau| - 1)(\mu - 1) \tag{5.3}$$

then G is Delsarte-geometric.

It would seem desirable to replace the structural assumption (bound on claw size) in Godsil's theorem by a reasonable assumption involving the parameters of the graph only since this would allow broader applicability of the result. Bang and Koolen make a step in this direction, removing the structural assumption but strengthening the constraint on the parameters.

Theorem 5.2.2 (Bang, Koolen [KB10])**.** *If $\lambda > \lfloor\tau\rfloor^2\mu$ for a distance-regular graph G with least eigenvalue τ then G is Delsarte geometric.*

Note that for large $|\tau|$, the Bang–Koolen constraint $\tau^2\mu \lesssim \lambda$ requires essentially a factor of $|\tau|/2$ larger λ than does Godsil's constraint (5.3) which for large $|\tau|$ and μ requires $2|\tau|\mu \lesssim \lambda$.

On the other hand, Theorem 2.7.7 shows that already an increase by a factor that goes to infinity arbitrarily slowly compared to Godsil's constraint, $|\tau|\mu = o(\lambda)$, suffices for an *asymptotic* Delsarte geometry, i. e., a clique geometry where the order of the cliques is $\sim \rho/|\tau|$.

We now prove Theorem 2.7.7.

Lemma 5.2.3. *Let G be a distance-regular graph with least eigenvalue τ. Then*

$$\lambda + \frac{\rho}{\lambda} > \frac{\rho}{|\tau|}.$$

Proof. Let $\{u_0, u_1, \ldots, u_d\}$ be the standard sequence of polynomials for G (see, e.g., [BCN89,

Section 4.1B]). It is well known that $u_0(x) = 1$, $u_1(x) = x/k$, and

$$c_1 u_0(x) + a_1 u_1(x) + b_1 u_2(x) = x u_1(x) \tag{5.4}$$

(cf. Eq. (13) in [BCN89, Section 4.1B]). Furthermore, if θ_i is the ith greatest eigenvalue of G, then the sequence $\{u_0(\theta_i), u_1(\theta_i), \ldots, u_d(\theta_i)\}$ has exactly i sign changes [BCN89, Corollary 4.1.2]. In particular, the sequence $\{u_0(\tau), u_1(\tau), \ldots, u_d(\tau)\}$ is alternating, and so $u_2(\tau) > 0$. Hence, from Eq. (5.4),

$$\lambda - \tau = \frac{\rho}{-\tau} + \frac{\rho^2}{-\tau} u_2(\tau) > \frac{\rho}{-\tau}.$$

So, if $\lambda \leq \rho/|\tau|$, then $\lambda + \rho/\lambda > \lambda - \tau > k/|\tau|$. Thus, in any case, $\lambda + \rho/\lambda > \rho/|\tau|$. □

We note that Lemma 5.2.3 is a slight improvement over Lemma 3.2 of [KB10] which states $\lambda + |\tau| > k/|\tau|$. The method of proof is virtually identical.

Proof of Theorem 2.7.7. Since $|\tau|\mu = o(\lambda)$, by Lemma 5.2.3, we have

$$\rho\mu < |\tau|\mu \left(\lambda + \frac{\rho}{\lambda}\right) = o(\lambda^2 + \rho).$$

We therefore have $\rho\mu = o(\lambda^2)$, so by Theorem 5.1.2, G has a clique geometry $\mathcal{G}$ with cliques of order $\sim \lambda$. By Lemma 2.7.6, we have $\lambda \lesssim 1 + \rho/|\tau|$. But since $\lambda \gtrsim \rho/|\tau|$ by Lemma 5.2.3, it follows that $\rho/|\tau|$ is unbounded and the cliques of the geometry have order $\sim \rho/|\tau|$. □

5.3 Primitive Coherent Configurations

We now prove Theorem 2.7.13, which gives a sufficient condition for the presence of a clique geometry in a primitive coherent configuration.

We recall our notation. Given a primitive coherent configuration $\mathfrak{X}$ of rank r, we write p^i_{jk} for the structure constants of $\mathfrak{X}$, where $i, j, k \in [r]$ are colors. We write v for the number

of vertices in $\mathfrak{X}$. We assume 0 is the vertex color, and write $\rho_i = p^0_{ii^*}$ for the out-valency of a vertex in $\mathfrak{X}_i$, the ith constituent digraph. For a set I of edge-colors, we write $\mathfrak{X}_I$ for the union $\bigcup_{i\in I} \mathfrak{X}_i$, i.e., the graph on $V(\mathfrak{X})$ with a directed edge (x, y) whenever $c(x, y) \in I$. If $i^* \in I$ whenever $i \in I$, we view $\mathfrak{X}_I$ as an undirected graph.

When $\mathfrak{X}$ has a dominant color, we assume without loss of generality that color 1 is dominant. We write $G_{\mathfrak{X}}$ for the graph $\mathfrak{X}_{\{2,\dots,r-1\}}$. We write ρ for the valency of $G_{\mathfrak{X}}$, and μ for the number of common neighbors of a pair of nonadjacent vertices in $G_{\mathfrak{X}}$. We write $\lambda_i = |\mathfrak{X}_i(x) \cap G_{\mathfrak{X}}(y)|$, where $x, y \in V(\mathfrak{X})$ are any pair of vertices such that $c(x, y) = i$.

We require some preliminary facts concerning primitive coherent configurations. The following proposition is standard, see e.g., [Zie10, Lemma 1.1.1, 1.1.2, 1.1.3].

Proposition 5.3.1. *Let $\mathfrak{X}$ be a coherent configuration. Then for all colors i, j, k, the following relations hold:*

(i) $\rho_i = \rho_{i^*}$

(ii) $p^i_{jk} = p^{i^*}_{k^*j^*}$

(iii) $\rho_i p^i_{jk} = \rho_j p^j_{ik^*}$

(iv) $\sum_{j=0}^{r-1} p^i_{jk} = \sum_{j=0}^{r-1} p^i_{kj} = \rho_k$

We also have the following estimate for μ when there is a dominant color.

Lemma 5.3.2. *Let $\mathfrak{X}$ be a primitive coherent configuration with $\rho_1 \geq v/2$. Then $\mu \leq \rho^2/\rho_1$.*

Proof. Fix a vertex x. There are at most ρ^2 paths of length two from x along edges of nondominant color, and exactly ρ_1 vertices y such that $c(x, y) = 1$. For any such vertex y, there are exactly μ paths of length two from x to y along edges of nondominant color. Hence, $\mu \leq \rho^2/\rho_1$. □

For the rest of the section, color 1 will in fact be dominant. In fact, in much of the rest of this section, we will assume that $\rho = o(v^{2/3})$. Lemma 5.3.3 below demonstrates some of the power of this supposition.

We denote by $\mathrm{dist}_i(x,y)$ the directed distance from x to y in the color-i constituent digraph $\mathfrak{X}_i$, and we write $\mathrm{dist}_i(j) = \mathrm{dist}_i(x,y)$ for any vertices x, y with $c(x,y) = j$. (This latter quantity is well-defined by the coherence of $\mathfrak{X}$.)

Lemma 5.3.3. *Let $\mathfrak{X}$ be a primitive coherent configuration with $\rho = o(v^{2/3})$. Then, for v sufficiently large, $\mathrm{dist}_i(1) = 2$ for every nondominant color i. Consequently, $\rho_i \geq \sqrt{v-1}$ for $i \neq 0$.*

For a proof of Lemma 5.3.3, see [Sun16] (cf. [SW15b]).

We shall make use of the Metsch's Clique Partition Lemma (Lemma 5.1.4) to find collections of cliques in $G(\mathfrak{X})$ that locally resemble an asymptotically uniform clique geometry. The cliques guaranteed by Lemma 5.1.4 will satisfy the following definition for a set $I = \{i\}$ containing a single edge-color (see Corollary 5.3.5 below).

Definition 5.3.4. Let $\mathfrak{X}$ be a primitive coherent configuration with a dominant color, and let I be a set of nondominant colors. An *I-local clique partition* at a vertex x is a collection $\mathcal{P}$ of subsets of $\mathfrak{X}_I(x)$ satisfying the following properties:

(i) $\mathcal{P}$ is a partition of $\mathfrak{X}_I(x)$ into maximal cliques in the subgraph of $G(\mathfrak{X})$ induced on $\mathfrak{X}_I(x)$;

(ii) for every $C \in \mathcal{P}_u$ and $i \in I$, we have $|C \cap \mathfrak{X}_i(x)| \sim \lambda_i$.

We say $\mathfrak{X}$ *has I-local clique partitions* if there is an I-local clique partition at every vertex $x \in V(\mathfrak{X})$.

A local clique partition provides only weak structure. Indeed, let C be a clique belonging to an I-local clique partition at x, for some vertex x and some set I of nondominant colors. We emphasize that while $c(x,y) \in I$ for every $y \in C$, the only guarantee for edges in C not involving x is that they are nondominant—i.e., it may be that $c(y,z) \notin I$ for a pair of vertices $y, z \in C$, though at least $c(y,z)$ is nondominant.

To prove Theorem 2.7.13, we will stitch local clique partitions together into clique geometries.

Note that from the definition, if $\mathcal{P}$ is an I-local clique partition (at some vertex) and $i \in I$, then $|\mathcal{P}| \sim \rho_i/\lambda_i$.

Corollary 5.3.5. *Let $\mathfrak{X}$ be a primitive coherent configuration, and let i be a nondominant color such that $\rho_i\mu = o(\lambda_i^2)$. Then $\mathfrak{X}$ has $\{i\}$-local clique partitions.*

Proof. Fix a vertex x, and apply Lemma 5.1.4 to the graph G induced by $G_{\mathfrak{X}}$ on $\mathfrak{X}_i(x)$. The Lemma gives a collection of cliques satisfying Definition 5.3.4. □

The following simple observation is essential for the proofs of this section.

Observation 5.3.6. *Let $\mathfrak{X}$ be a primitive coherent configuration, let C be a clique in $G_{\mathfrak{X}}$, and suppose $x \in V(\mathfrak{X}) \setminus C$ is such that $|G_{\mathfrak{X}}(x) \cap C| > \mu$. Then $C \subseteq G_{\mathfrak{X}}(x)$.*

Proof. Suppose there exists a vertex $y \in C \setminus G_{\mathfrak{X}}(x)$, so $c(x, y) = 1$. Then $|G_{\mathfrak{X}}(x) \cap G_{\mathfrak{X}}(y)| = \mu$ by the definition of the parameter μ in a primitive coherent configuration. But

$$\begin{aligned} |G_{\mathfrak{X}}(x) \cap G_{\mathfrak{X}}(y)| &\geq |G_{\mathfrak{X}}(x) \cap C \cap G_{\mathfrak{X}}(y)| = |G_{\mathfrak{X}}(x) \cap (C \setminus \{y\})| \\ &= |G_{\mathfrak{X}}(x) \cap C| > \mu, \end{aligned}$$

a contradiction. □

Under modest assumptions, if local clique partitions exist, they are unique.

Lemma 5.3.7. *Let $\mathfrak{X}$ be a primitive coherent configuration, let i be a nondominant color such that $\rho_i\mu = o(\lambda_i^2)$, and let I be a set of nondominant colors such that $i \in I$. Suppose $\mathfrak{X}$ has I-local clique partitions. Then for every vertex $x \in V$, there is a unique I-local clique partition $\mathcal{P}$ at x.*

Proof. Let $x \in V$ and let $\mathcal{P}$ be an I-local clique partition at x. Let C and C' be two distinct maximal cliques in the subgraph of $G(\mathfrak{X})$ induced on $\mathfrak{X}_I(x)$. We show that $|C \cap C'| <$

μ. Suppose for the contradiction that $|C \cap C'| \geq \mu$. For a vertex $y \in C \setminus C'$, we have $|G_{\mathfrak{X}}(y) \cap (C' \cup \{x\})| > \mu$, and so $C' \subseteq G_{\mathfrak{X}}(y)$ by Observation 5.3.6. But since $y \notin C'$, this contradicts the maximality of C'. So in fact $|C \cap C'| < \mu$.

Now let $C \notin \mathcal{P}$ be a maximal clique in the subgraph of $G(\mathfrak{X})$ induced on $\mathfrak{X}_I(x)$. Since $\mathcal{P}$ is an I-local clique partition, it follows that

$$|C| = \sum_{C' \in \mathcal{P}} |C' \cap C| < \mu|\mathcal{P}| \sim \rho_i \mu / \lambda_i = o(\lambda_i).$$

Then C does not belong to an I-local clique partition, since it fails to satisfy Property (ii) of Definition 5.3.4. □

5.3.1 Local Cliques and Symmetry

Suppose $\mathfrak{X}$ has I-local clique partitions, and $c(x, y) \in I$ for some $x, y \in V$. We remark that in general, the clique containing y in the I-local clique partition at x will not be in any way related to any clique in the I-local clique partition at y. In particular, we need not have $c(y, x) \in I$. However, even when $c(y, x) \in I$ as well, there is no guarantee that the clique at x containing y will have any particular relation to the clique at y containing x. This lack of symmetry is a fundamental obstacle that we must overcome to prove Theorem 2.7.13.

Lemma 5.3.9 below is the main result of this subsection. It gives sufficient conditions on the parameters of a primitive coherent configuration for finding the desired symmetry in local clique partitions satisfying the following additional condition.

Definition 5.3.8. Let $\mathfrak{X}$ be a primitive coherent configuration with a dominant color. Let I be a set of nondominant colors in $\mathfrak{X}$, let $x \in V(\mathfrak{X})$, and let $\mathcal{P}$ be an I-local clique partition at x. We say $\mathcal{P}$ is *strong* if for every $C \in \mathcal{P}$, the clique $C \cup \{x\}$ is maximal in $G(\mathfrak{X})$. We say $\mathfrak{X}$ has *strong* I-local clique partitions if there is a strong I-local clique partition at every vertex $x \in V$.

We introduce additional notation. Suppose I is a set of nondominant colors, and $i \in I$

satisfies $\rho_i\mu = o(\lambda_i)^2$. If $\mathfrak{X}$ has I-local clique partitions, then for every $x, y \in V$ with $c(x,y) \in I$, we denote by $K_I(x,y)$ the set $C \cup \{x\}$, where C is the clique in the partition of $\mathfrak{X}_I(x)$ containing y (noting that by Lemma 5.3.7, this clique is uniquely determined).

Lemma 5.3.9. *Let $\mathfrak{X}$ be a primitive coherent configuration with $\rho = o(v^{2/3})$, let i be a nondominant color, and let I and J be sets of nondominant colors such that $i \in I$, $i^* \in J$, and $\mathfrak{X}$ has strong I-local and J-local clique partitions. Suppose $\lambda_i\lambda_{i^*} = \Omega(v)$. Then for every $x, y \in V$ with $c(x,y) = i$, we have $K_I(x,y) = K_J(y,x)$.*

We first prove two easy preliminary statements.

Proposition 5.3.10. *Suppose $\rho = o(v^{2/3})$. Then $\mu = o(v^{1/3})$ and $\mu\rho = o(v)$. Furthermore, for every nondominant color i, we have $\mu = o(\rho_i)$.*

Proof. By Lemma 5.3.2, $\mu \leq \rho^2/\rho_1 = o(v^{1/3})$, and then $\mu\rho = o(v)$. The last inequality follows by Lemma 5.3.3. □

Lemma 5.3.11. *Let $\mathfrak{X}$ be a primitive coherent configuration and let I and J be sets of nondominant colors such that $\mathfrak{X}$ has strong I-local and J-local clique partitions. Suppose that for some vertices $x, y, z, w \in V$ we have $|K_I(x,y) \cap K_J(z,w)| > \mu$. Then $K_I(x,y) = K_J(z,w)$.*

Proof. Suppose there exists a vertex $u \in K_J(z,w) \setminus K_I(x,y)$. We have $|G_{\mathfrak{X}}(u) \cap K_I(x,y)| \geq |K_J(z,w) \cap K_I(x,y)| > \mu$. Then $K_I(x,y) \subseteq G_{\mathfrak{X}}(u)$ by Observation 5.3.6, contradicting the maximality of $K_I(x,y)$. Thus, $K_J(z,w) \subseteq K_I(x,y)$. Similarly, $K_I(x,y) \subseteq K_J(z,w)$. □

Proof of Lemma 5.3.9. Without loss of generality, assume $\lambda_i \leq \lambda_{i^*}$.

Suppose for contradiction that there exists a vertex $x \in V$ such that for *every* $y \in \mathfrak{X}_i(x)$, we have $K_I(x,y) \neq K_J(y,x)$. Then $|K_I(x,y) \cap K_J(y,x)| \leq \mu$ by Lemma 5.3.11. Fix $y \in \mathfrak{X}_i(x)$, so for every $w \in K_I(x,y) \cap \mathfrak{X}_i(x)$, we have $|K_J(w,x) \cap K_I(x,y)| \leq \mu$. Hence, there exists some sequence $w_1, \ldots, w_\ell$ of $\ell = \lceil \lambda_i/(2\mu) \rceil$ vertices $w_\alpha \in K_I(x,y) \cap \mathfrak{X}_i(x)$

such that $K_J(w_\alpha, x) \neq K_J(w_\beta, x)$ for $\alpha \neq \beta$. But by Lemma 5.3.11, for $\alpha \neq \beta$ we have $|K_J(w_\alpha, x) \cap K_J(w_\beta, x)| \leq \mu$. Hence, for any $1 \leq \alpha \leq \ell$ we have

$$\left| K_J(w_\alpha, x) \setminus \bigcup_{\beta \neq \alpha} K_J(w_\beta, x) \right| \gtrsim \lambda_{i^*} - \mu\lambda_i/(2\mu) \geq \lambda_{i^*}/2.$$

But $K_J(w_\alpha, x) \subseteq G_{\mathfrak{X}}(x)$, so

$$|G_{\mathfrak{X}}(x)| \geq \left| \bigcup_{\alpha=1}^{\ell} K_J(w_\alpha, x) \right| \gtrsim \frac{\lambda_i \lambda_{i^*}}{4\mu} = \omega(\rho)$$

by Proposition 5.3.10. This contradicts the definition of ρ.

Hence, for any vertex x, there is some $y \in \mathfrak{X}_i(x)$ such that $K_I(x, y) = K_J(y, x)$. Then, in particular, $|\mathfrak{X}_{i^*}(y) \cap \mathfrak{X}_I(x)| \gtrsim \lambda_{i^*}$ by the definition of a J-local clique partition. By the coherence of $\mathfrak{X}$, for every $y \in \mathfrak{X}_i(x)$, we have $|\mathfrak{X}_{i^*}(y) \cap \mathfrak{X}_I(x)| \gtrsim \lambda_{i^*}$. Recall that $\mathfrak{X}_I(x)$ is partitioned into $\sim \rho_i/\lambda_i$ maximal cliques, and for each of these cliques C other than $K_I(x, y)$, we have $|G_{\mathfrak{X}}(y) \cap C| \leq \mu$. Hence,

$$|\mathfrak{X}_{i^*}(y) \cap K_I(x, y)| \gtrsim \lambda_{i^*} - O\left(\frac{\mu\rho_i}{\lambda_i}\right) = \lambda_{i^*} - o\left(\frac{v}{\lambda_i}\right) \sim \lambda_{i^*}$$

by Proposition 5.3.10. Since the J-local clique partition at y partitions $\mathfrak{X}_{i^*}(y)$ into $\sim \rho_i/\lambda_{i^*}$ cliques, at least one of these intersects $K_I(x, y)$ in at least $\sim \lambda_{i^*}^2/\rho_i = \omega(\mu)$ vertices. In other words, there is some $z \in \mathfrak{X}_{i^*}(y)$ such that $|K_J(y, z) \cap K_I(x, y)| = \omega(\mu)$. But then $K_J(y, z) = K_I(x, y)$ by Lemma 5.3.11. In particular, $x \in K_J(y, z)$, so $K_J(y, z) = K_J(y, x)$. Hence, $K_J(y, x) = K_J(y, z) = K_I(x, y)$, as desired. □

5.3.2 Existence of Strong Local Clique Partitions

Our next step in proving Theorem 2.7.13 is showing the existence of strong local clique partitions. We accomplish this via the following lemma.

Lemma 5.3.12. *Let $\mathfrak{X}$ be a primitive coherent configuration such that $\rho = o(v^{2/3})$, and let i be a nondominant color such that $\rho_i \mu = o(\lambda_i^2)$. Suppose that for every color j with $\rho_j < \rho_i$, we have $\lambda_j = \Omega(\sqrt{v})$. Then for v sufficiently large, there is a set I of nondominant colors with $i \in I$ such that $\mathfrak{X}$ has strong I-local clique partitions.*

We will prove Lemma 5.3.12 via a sequence of lemmas which gradually improve our guarantees about the number of edges between cliques of the I-local clique partition at a vertex x and the various neighborhoods $\mathfrak{X}_j(x)$ for $j \notin I$.

Lemma 5.3.13. *Let $\mathfrak{X}$ be a primitive coherent configuration, and let i and j be nondominant colors. Then for any $0 < \varepsilon < 1$ and any $x, y \in V$ with $c(x, y) = j$, we have*

$$|\mathfrak{X}_i(x) \cap G_{\mathfrak{X}}(y)| \leq \max\left\{\frac{\lambda_i + 1}{1 - \varepsilon}, \rho_i \sqrt{\frac{\mu}{\varepsilon \rho_j}}\right\}$$

Proof. Fix $x, y \in V$ with $c(x, y) = j$ and let $\alpha = |\mathfrak{X}_i(x) \cap G_{\mathfrak{X}}(y)|$. We count the number of triples (a, b, z) of vertices such that $a, b \in \mathfrak{X}_i(x) \cap G_{\mathfrak{X}}(z)$, with $c(x, z) = j$ and $c(a, b) = 1$. There are at most ρ_i^2 pairs $a, b \in \mathfrak{X}_i(x)$, and if $c(a, b) = 1$ then there are at most μ vertices z such that $a, b \in G_{\mathfrak{X}}(z)$. Hence, the number of such triples is at most $\rho_i^2 \mu$. On the other hand, by the coherence of $\mathfrak{X}$, for every z with $c(x, z) = j$, we have at least $\alpha(\alpha - \lambda_i - 1)$ pairs $a, b \in \mathfrak{X}_i(x) \cap G_{\mathfrak{X}}(z)$ with $c(a, b) = 1$. Hence, there are at least $\rho_j \alpha(\alpha - \lambda_i - 1)$ total such triples. Thus,

$$\rho_j \alpha(\alpha - \lambda_i - 1) \leq \rho_i^2 \mu.$$

Hence, if $\alpha \leq (\lambda_i + 1)/(1 - \varepsilon)$, then we are done. Otherwise, $\alpha > (\lambda_i + 1)/(1 - \varepsilon)$, and then $\lambda_i + 1 < (1 - \varepsilon)\alpha$. So, we have

$$\rho_i^2 \mu \geq \rho_j \alpha(\alpha - \lambda_i - 1) > \varepsilon \rho_j \alpha^2,$$

and then $\alpha < \rho_i \sqrt{\mu/(\varepsilon \rho_j)}$. □

Lemma 5.3.14. *Let $\mathfrak{X}$ be a primitive coherent configuration, and let i be a nondominant color such that $\rho_i\mu = o(\lambda_i^2)$. Let I be a set of nondominant colors with $i \in I$ such that $\mathfrak{X}$ has I-local clique partitions. Let j be a nondominant color such that $\rho_i\sqrt{\mu/\rho_j} < (\sqrt{3}/2)\lambda_i$. Let $x \in V$, let $\mathcal{P}_u$ be the I-local clique partition at x, and let $y \in \mathfrak{X}_j(x)$. Suppose some clique $C \in \mathcal{P}_x$ is such that $c(x,y) = j$ and $|G_{\mathfrak{X}}(y) \cap C| \geq \mu$. Then for every pair of vertices $w, z \in V$ with $c(w,z) = j$, letting $\mathcal{P}_w$ be the I-local clique partition at w, the following statements hold:*

(i) there is a unique clique $C \in \mathcal{P}_w$ such that $C \subseteq G_{\mathfrak{X}}(z)$;

(ii) $|G_{\mathfrak{X}}(z) \cap \mathfrak{X}_i(w)| \sim \lambda_i$.

Proof. Letting $\widehat{C} = C \cup \{x\}$, we have $|\widehat{C} \cap G_{\mathfrak{X}}(y)| \geq \mu + 1 > \mu$. Therefore, by Observation 5.3.6, we have $C \subseteq G_{\mathfrak{X}}(y)$. In particular, $|G_{\mathfrak{X}}(y) \cap \mathfrak{X}_i(x)| \gtrsim \lambda_i$, and so by the coherence of $\mathfrak{X}$, $|G_{\mathfrak{X}}(z) \cap \mathfrak{X}_i(w)| \gtrsim \lambda_i$ for every pair $w, z \in V$ with $c(w,z) = j$.

Now fix $w \in V$, and let $\mathcal{P}_w$ be the I-local clique partition at w. By the definition of an I-local clique partition, we have $|\mathcal{P}_w| \sim \rho_i/\lambda_i$. For every $z \in \mathfrak{X}_j(w)$, by assumption we have

$$|G_{\mathfrak{X}}(z) \cap \mathfrak{X}_i(w)| \gtrsim \lambda_i = \omega(\mu\rho_i/\lambda_i). \tag{5.5}$$

Then it follows from the pigeonhole principle that for v sufficiently large, there is some clique $C \in \mathcal{P}_w$ such that $|G_{\mathfrak{X}}(z) \cap C| > \mu$, and then $C \subseteq G_{\mathfrak{X}}(z)$ by Observation 5.3.6.

Now suppose for contradiction that there is some clique $C' \in \mathcal{P}_w$ with $C' \neq C$, such that $C' \subseteq G_{\mathfrak{X}}(z)$.

$$|G_{\mathfrak{X}}(z) \cap \mathfrak{X}_i(w)| \geq |C \cup C'| \gtrsim 2\lambda_i \sim 2(\lambda_i + 1) \tag{5.6}$$

(with the last relation holding since $\lambda_i = \omega(\sqrt{\rho_i\mu}) = \omega(1)$.) However, by Lemma 5.3.13 with $\varepsilon = 1/3$, we have

$$|\mathfrak{X}_i(w) \cap G_{\mathfrak{X}}(z)| \leq \max\left\{\frac{3}{2}(\lambda_i + 1), \rho_i\sqrt{\frac{3\mu}{\rho_j}}\right\} = \frac{3}{2}(\lambda_i + 1),$$

with the last equality holding by assumption. This contradicts Eq. (5.6), so we conclude that C is the unique clique in $\mathcal{P}_w$ satisfying $C \subseteq G_{\mathfrak{X}}(z)$. In particular, by Observation 5.3.6, we have $|G_{\mathfrak{X}}(z) \cap C'| \leq \mu$ for every $C' \in \mathcal{P}_w$ with $C' \neq C$.

Finally, we estimate $|G_{\mathfrak{X}}(z) \cap \mathfrak{X}_i(w)|$ by

$$\begin{aligned} &|G_{\mathfrak{X}}(z) \cap \mathfrak{X}_i(w) \cap C| + \sum_{C' \neq C} |G_{\mathfrak{X}}(z) \cap \mathfrak{X}_i(w) \cap C'| \\ &\lesssim \lambda_i + \mu\rho_i/\lambda_i \sim \lambda_i, \end{aligned}$$

which, combined with Eq. (5.5), gives $|G_{\mathfrak{X}}(z) \cap \mathfrak{X}_i(w)| \sim \lambda_i$. □

Lemma 5.3.15. *Let $\mathfrak{X}$ be a primitive coherent configuration, and let i be a nondominant color such that $\rho_i\mu = o(\lambda_i^2)$. There exists a set I of nondominant colors with $i \in I$ such that $\mathfrak{X}$ has I-local clique partitions and the following statement holds. Suppose j is a nondominant color such that $\rho_i\sqrt{\mu/\rho_j} = o(\lambda_i)$, let $x \in V$, and let $\mathcal{P}$ be the I-local clique partition at x. Then for any $C \in \mathcal{P}$ and any vertex $y \in \mathfrak{X}_j(x) \setminus C$, we have $|G_{\mathfrak{X}}(y) \cap C| < \mu$.*

Proof. By Corollary 5.3.5, $\mathfrak{X}$ has $\{i\}$-local clique partitions. Let I be a maximal subset of of the nondominant colors such that $i \in I$ and $\mathfrak{X}$ has I-local clique partitions. We claim that I has the desired property.

Indeed, suppose there exists some color $j \notin I$ satisfying $\rho_i\sqrt{\mu/\rho_j} = o(\lambda_i)$, some vertices x, y with $c(x, y) = j$, and some $C \in \mathcal{P}$ with $|G_{\mathfrak{X}}(y) \cap C| \geq \mu$, where $\mathcal{P}$ is the I-local clique partition at x. By Lemma 5.3.14, for n sufficiently large, for every vertex $x, y \in V$ with $c(x, y) = j$, and I-local clique partition $\mathcal{P}$ at x, (i) there is a unique clique $C \in \mathcal{P}$ such that $C \subseteq G_{\mathfrak{X}}(y)$, and (ii) we have

$$|G_{\mathfrak{X}}(y) \cap \mathfrak{X}_i(x)| \sim \lambda_i. \tag{5.7}$$

Now fix $x \in V$ and let $\mathcal{P}$ be the I-local clique partition at x. Let $\mathcal{P}'$ be the collection of sets C' of the form

$$C' = C \cup \{y \in \mathfrak{X}_j(x) : C \subseteq G_{\mathfrak{X}}(y)\}$$

for every $C \in \mathcal{P}$. Let $J = I \cup \{j\}$. We claim that $\mathcal{P}'$ satisfies Properties (i) and (ii) of Definition 5.3.4, so $\mathfrak{X}$ has local clique partitions on J. This contradicts the maximality of I, and the lemma then follows.

First we verify Property (i) of Definition 5.3.4. By properties (i) and (ii) above, $\mathcal{P}'$ partitions $\mathfrak{X}_J(x)$. Furthermore, the sets $C \in \mathcal{P}'$ are cliques in $G(\mathfrak{X})$, since for any $C \in \mathcal{P}'$ and any distinct $y, w \in C \cap \mathfrak{X}_j(x)$, we have

$$|G_{\mathfrak{X}}(y) \cap G_{\mathfrak{X}}(w)| \geq |C \cap \mathfrak{X}_I(x)| \gtrsim \lambda_i = \omega(\mu)$$

and so $c(y, w)$ is nondominant by the definition of μ. Furthermore, the cliques $C \in \mathcal{P}'$ are maximal in the subgraph of G($\mathfrak{X}$) induced on $\mathfrak{X}_J(x)$, since by property (ii) above, for any clique $C \in \mathcal{P}'$ and $y \in \mathfrak{X}_J(x) \setminus C$, we have $|G_{\mathfrak{X}}(y) \cap C \cap \mathfrak{X}_I(x)| < \mu$.

We now verify Property (ii) of Definition 5.3.4. By the pigeonhole principle, there is some $C \in \mathcal{P}'$ with

$$|C \cap \mathfrak{X}_j(x)| \gtrsim \frac{\rho_j}{|\mathcal{P}'|} = \frac{\rho_j}{|\mathcal{P}|} \sim \frac{\lambda_i \rho_j}{\rho_i}.$$

But since C is a clique in $G(\mathfrak{X})$, we have $|C \cap \mathfrak{X}_j(x)| \leq \lambda_j + 1$. So, from the defining property of j,

$$\lambda_j + 1 \gtrsim \frac{\lambda_i \rho_j}{\rho_i} = \omega(\sqrt{\mu \rho_j})$$

Since ρ_j and μ are positive integers, we have in particular $\lambda_j = \omega(1)$, and thus

$$\lambda_j \gtrsim \frac{\lambda_i \rho_j}{\rho_i} = \omega(\sqrt{\mu \rho_j}). \tag{5.8}$$

Hence, $\rho_j \mu = o(\lambda_j^2)$, and so by Corollary 5.3.5, $\mathfrak{X}$ has $\{j\}$-local clique partitions.

Let $C' \subseteq \mathfrak{X}_j(x)$ be a maximal clique in $G(\mathfrak{X})$ of order $\sim \lambda_j$. By Eq. (5.7) there are $\sim \lambda_j \lambda_i$ nondominant edges between C' and $\mathfrak{X}_i(x)$, so some $z \in \mathfrak{X}_i(x)$ satisfies

$$|G_{\mathfrak{X}}(z) \cap C'| \gtrsim \lambda_j \lambda_i / \rho_i = \omega(\lambda_j \sqrt{\mu / \rho_j}) = \omega(\mu).$$

(The last equality uses Eq. (5.8).) Furthermore, by Eq. (5.8), we have

$$\rho_j \lesssim (\rho_i/\lambda_i)\lambda_j = o(\sqrt{\rho_i/\mu}\lambda_j),$$

where the last inequality comes from the assumption that $\sqrt{\rho_i\mu} = o(\lambda_i)$. So by applying Lemma 5.3.14 with $\{j\}$ in place of I, it follows that for every $z \in \mathfrak{X}_i(x)$, we have $|G_{\mathfrak{X}}(z) \cap \mathfrak{X}_j(x)| \sim \lambda_j$.

We count the nondominant edges between $\mathfrak{X}_i(x)$ and $\mathfrak{X}_j(x)$ in two ways: there are $\sim \lambda_j$ such edges at each of the ρ_i vertices in $\mathfrak{X}_i(x)$, and (by Eq. (5.7)) there are $\sim \lambda_i$ such edges at each of the ρ_j vertices in $\mathfrak{X}_j(x)$. Hence, $\rho_i\lambda_j \sim \rho_j\lambda_i$.

Now, using Eq. (5.8), $\mu|\mathcal{P}'| \sim \mu\rho_i/\lambda_i \sim \mu\rho_j/\lambda_j = o(\lambda_j)$. By the maximality of the cliques $C \in \mathcal{P}'$ in the subgraph of $G(\mathfrak{X})$ induced on $\mathfrak{X}_J(x)$, for every distinct $C, C' \in \mathcal{P}'$ and $y \in C$, we have $|G_{\mathfrak{X}}(y) \cap C'| \leq \mu$. Therefore, for $y \in C \cap \mathfrak{X}_j(x)$, we have

$$\begin{aligned}
\lambda_j - |\mathfrak{X}_j(x) \cap C| &= |\mathfrak{X}_j(x) \cap G_{\mathfrak{X}}(y)| - |\mathfrak{X}_j(x) \cap C| \\
&\leq \left|\left(G_{\mathfrak{X}}(y) \cap \mathfrak{X}_j(x)\right) \setminus C\right| \\
&\leq \mu|\mathcal{P}'| = o(\lambda_j),
\end{aligned}$$

so that $|\mathfrak{X}_j(x) \cap C| \sim \lambda_j$, as desired.

Now $\mathcal{P}'$ satisfies Definition 5.3.4, giving the desired contradiction. □

Proof of Lemma 5.3.12. Suppose for contradiction that no set I of nondominant colors with $i \in I$ is such that $\mathfrak{X}$ has strong I-local clique partitions. Without loss of generality, we may assume that ρ_i is minimal for this property, i.e., for every nondominant color j with $\rho_j < \rho_i$, there is a set J of nondominant colors with $j \in J$ such that $\mathfrak{X}$ has strong I-local clique partitions.

Let I be the set of nondominant colors containing i guaranteed by Lemma 5.3.15.

Let $x \in V$ be such that some clique C in the I-local clique partition at x is not maximal

in $G(\mathfrak{X})$. In particular, let $y \in V \setminus C$ be such that $C \subseteq G_{\mathfrak{X}}(y)$, and let $j = c(x, y)$. Then j is a nondominant color, and $j \notin I$. Furthermore, by the defining property of I (the guarantee of Lemma 5.3.15), it is not the case that $\rho_i\sqrt{\mu/\rho_j} = o(\lambda_i)$. In particular we may take $\rho_j < \rho_i$, since otherwise, if $\rho_j \geq \rho_i$, then $\rho_i\sqrt{\mu/\rho_j} \leq \sqrt{\rho_i\mu} = o(\lambda_i)$ by assumption. Now since $\rho_j < \rho_i$, also $\lambda_j = \Omega(\sqrt{v})$ by assumption. Furthermore, by the minimality of ρ_i, there is a set J of nondominant colors with $j \in J$ such that $\mathfrak{X}$ has strong J-local clique partitions on J. In particular, $i \notin J$.

By the definition of I-local clique partitions,

$$|G_{\mathfrak{X}}(y) \cap \mathfrak{X}_i(x)| \geq |G_{\mathfrak{X}}(y) \cap \mathfrak{X}_i(x) \cap C| \gtrsim \lambda_i.$$

Now let D be the clique containing y in the J-local clique partition at x. By the coherence of $\mathfrak{X}$, for every $w \in \mathfrak{X}_j(x) \cap D$, we have $|G_{\mathfrak{X}}(w) \cap \mathfrak{X}_i(x)| \gtrsim \lambda_i$. Hence, there are $\gtrsim \lambda_j\lambda_i$ nondominant edges between $\mathfrak{X}_j(x) \cap D$ and $\mathfrak{X}_i(x)$. So, by the pigeonhole principle, some vertex $z \in \mathfrak{X}_i(x)$ satisfies

$$\begin{aligned}|G_{\mathfrak{X}}(z) \cap D \cap \mathfrak{X}_j(x)| &\gtrsim \frac{\lambda_i\lambda_j}{\rho_i} = \omega\left(\sqrt{\frac{\mu}{\rho_i}}\lambda_j\right) \\ &= \omega\left(\sqrt{\frac{\mu v}{\rho_i}}\right) = \omega(\mu).\end{aligned}$$

(The second inequality uses the assumption that $\sqrt{\rho_i\mu} = o(\lambda_i)$. The last inequality uses Proposition 5.3.10.) But then $D \setminus \{z\} \subseteq G_{\mathfrak{X}}(z)$ by Observation 5.3.6. Then $z \in D$ by the definition of a strong local clique partition, and so $i \in J$, a contradiction.

We conclude that in fact $\mathfrak{X}$ has strong local clique partitions on I. □

We finally complete the proof of Theorem 2.7.13.

Proof of Theorem 2.7.13. By Lemma 5.3.12, for every nondominant color i there is a set I such that $\mathfrak{X}$ has strong local clique partitions on I. We claim that these sets I partition the collection of nondominant colors. Indeed, suppose that there are two sets I and J of

nondominant colors such that $i \in I \cap J$ and $\mathfrak{X}$ has strong I-local and J-local clique partitions. Let $x, y \in V$ be such that $c(x,y) = i$. By the uniqueness of the induced $\{i\}$-local clique partition at x (Lemma 5.3.7), we have

$$|K_I(x,y) \cap K_J(x,y)| \gtrsim \lambda_i = \omega(\mu),$$

so $K_I(x,y) = K_J(x,y)$, and $I = J$. In particular, for every nondominant color i, there exists a unique set I of nondominant colors such that $\mathfrak{X}$ has strong I-local clique partitions.

We simplify our notation and write $K(x,y) = K_I(x,y)$ whenever $c(x,y) \in I$ and $\mathfrak{X}$ has strong I-local clique partitions. By Lemma 5.3.9, we have $K(x,y) = K(y,x)$ for all $x, y \in V$ with $c(x,y)$ nondominant. Let $\mathcal{G}$ be the collection of cliques of the form $K(x,y)$ for $c(x,y)$ nondominant. Then $\mathcal{G}$ is an asymptotically uniform clique geometry. □

5.3.3 Consequences of Local Clique Partitions for the Parameters λ_i

We conclude this section by analyzing some consequences for the parameters λ_i of our results on strong local clique partitions.

Lemma 5.3.16. *Let $\mathfrak{X}$ be a primitive coherent configuration with $\rho = o(v^{2/3})$. For every nondominant color i, we have $\lambda_i < \rho_i - 1$.*

Proof. Suppose for contradiction that $\lambda_i = \rho_i - 1$ for some nondominant color i. For every nondominant color j, by Proposition 5.3.10, we have $\rho_i \sqrt{\mu/\rho_j} = o(\rho_i) = o(\lambda_i)$. Furthermore, $\rho_i \mu = o(\lambda_i^2)$. Let I be the set of nondominant colors with $i \in I$ guaranteed by Lemma 5.3.15. In particular, $\mathfrak{X}$ has I-local clique partitions. In fact, since $\lambda_i = \rho_i - 1$, for every vertex x and every clique C in the I-local clique partition at x, we have $C \cap \mathfrak{X}_i(x) \sim \rho_i$. Hence, there is only one clique in the I-local clique partition at x, and so $\mathfrak{X}_I(x)$ is a clique in $G(\mathfrak{X})$. For every vertex x, let $K_I(x) = \mathfrak{X}_I(x) \cup \{x\}$. Then for every vertex $y \notin \mathfrak{X}_I(x)$, we have $|G_{\mathfrak{X}}(y) \cap K_I(x)| \leq \mu$. In particular, $K_I(x)$ is a maximal clique in $G(\mathfrak{X})$, and $\mathfrak{X}$ has strong I-local clique partitions.

Let $x, y \in V$ with $y \in \mathfrak{X}_I(x)$, let $j = c(x,y) \in I$, and suppose $|K_I(y) \cap K_I(x)| > \mu$. Then $K_I(y) = K_I(x)$ by Lemma 5.3.11. Hence, by the coherence of $\mathfrak{X}$, for any $w, z \in V$ with $z \in \mathfrak{X}_j(w)$, $K_I(w) = K_I(z)$. By applying this fact iteratively, we find that for any two vertices $w, z \in V$ such that there exists a path from w to z in $\mathfrak{X}_j$, we have $z \in K_I(w)$, contradicting the primitivity of $\mathfrak{X}$. We conclude that $|K_I(y) \cap K_I(x)| \leq \mu$ if $c(x,y) \in I$. Hence, if we fix a vertex x and count pairs of vertices $(y,z) \in \mathfrak{X}_i(x) \times \mathfrak{X}_I(x)$ with $c(z,y) = i$, we have

$$\rho_i \sum_{j \in I} p_{ji}^i \leq \rho_I \mu,$$

where $\rho_I = \sum_{i \in I} \rho_i$. In particular, for any vertex x and $y \in \mathfrak{X}_i(x)$, we have $|\mathfrak{X}_{i^*}(y) \cap \mathfrak{X}_I(x)| \leq \mu\rho_I/\rho_i$.

Fix a vertex $y \in V$. For some integer ℓ, we fix distinct vertices $x_1, \ldots, x_\ell$ in $\mathfrak{X}_{i^*}(y)$ such that for all $1 \leq \alpha, \beta \leq \ell$, we have $x_\alpha \notin \mathfrak{X}_I(x_\beta)$. Since $|\mathfrak{X}_{i^*}(y) \cap \mathfrak{X}_I(x_\alpha)| \leq \mu\rho_I/\rho_i$, we may take $\ell = \lfloor \rho_i/(2\mu) \rfloor$. As $\mu = o(\rho_i)$ by Proposition 5.3.10, we therefore have $\ell = \Omega(\rho_i/\mu)$.

By Lemma 5.3.11, for $\alpha \neq \beta$, we have $|\mathfrak{X}_I(x_\alpha) \cap \mathfrak{X}_I(x_\beta)| \leq \mu$. Hence, for any $1 \leq \alpha \leq \ell$, we have

$$\left| \mathfrak{X}_I(x_\alpha) \setminus \bigcup_{\beta \neq \alpha} \mathfrak{X}_I(x_\beta) \right| \gtrsim \rho_I - \left\lfloor \frac{\rho_i}{2\mu} \right\rfloor \mu \geq \frac{\rho_I}{2}.$$

But $c(x_\alpha, y) = i$, so $y \in K_I(x_\alpha)$, and so $\mathfrak{X}_I(x_\alpha) \setminus \{y\} \subseteq K_I(x_\alpha) \subseteq \{y\} \subseteq G_{\mathfrak{X}}(y)$. Then

$$|G_{\mathfrak{X}}(y)| \geq \left| \bigcup_{\alpha=1}^{\ell} \mathfrak{X}_I(x_\alpha, y) \setminus \{y\} \right| \gtrsim \frac{\rho_I \ell}{2} = \Omega(\frac{\rho_i^2}{\mu}) = \omega(\rho)$$

by Proposition 5.3.10. But this contradicts the definition of ρ. We conclude that $\lambda_i < \rho_i - 1$. □

Lemma 5.3.17. *Let $\mathfrak{X}$ be a primitive coherent configuration. Suppose for some nondominant color i we have $\lambda_i < \rho_i - 1$. Then $\lambda_i \leq (1/2)(\rho_i + \mu)$.*

Proof. Fix a vertex x, and suppose $\lambda_i < \rho_i - 1$. Then there exist vertices $y, z \in \mathfrak{X}_i(x)$ such

that $c(y,z)$ is dominant. Then $|G_{\mathfrak{X}}(y) \cap G_{\mathfrak{X}}(z)| = \mu$. Therefore,

$$2\lambda_i - \mu \leq |(G_{\mathfrak{X}}(x) \cup G_{\mathfrak{X}}(y)) \cap \mathfrak{X}_i(x)| \leq \rho_i.$$

□

Corollary 5.3.18. *Suppose $\mathfrak{X}$ is a primitive coherent configuration with $\rho = o(v^{2/3})$. Then for every nondominant color i, we have $\lambda_i \lesssim \rho_i/2$.*

Proof. For every nondominant color i we have $\lambda_i < \rho_i - 1$ by Lemma 5.3.16. Then by Lemma 5.3.17 and Proposition 5.3.10, we have $\lambda_i \leq (1/2)(\rho_i + \mu) \sim \rho_i/2$. □

Corollary 5.3.19. *Let $\mathfrak{X}$ be a primitive coherent configuration with $\rho = o(v^{2/3})$ with an asymptotically uniform clique geometry $\mathcal{G}$. Then for every nondominant color i there is an integer $m_i \geq 2$ such that $\lambda_i \sim \rho_i/m_i$.*

Proof. Fix a nondominant color i and a vertex x, and let m_i be the number of cliques $C \in \mathcal{G}$ such that $x \in C$ and $\mathfrak{X}_i(x) \cap C \neq \emptyset$. So $\rho_i/m_i \sim \lambda_i$. But by Corollary 5.3.18, we have $\lambda_i \lesssim \rho_i/2$, so $m_i \geq 2$. □

5.4 Reconstruction of Partial Geometries

We now prove Theorems 2.7.10 and 2.7.11, our bounds on the number of possible reconstructions of a partial geometry from its line-graph. From these, we prove Theorem 2.4.7.

First, we observe the correspondence between the parameters of a partial geometry and the parameters of its (strongly regular) line-graph.

Proposition 5.4.1. *Let $\mathfrak{X}$ be a $\mathrm{PG}(r,k,\alpha)$ geometry. Then $L(\mathfrak{X})$ is a $\mathrm{SR}(v,\rho,\lambda,\mu)$ graph,*

where

$$v = r\left(\frac{(r-1)(k-1)+\alpha}{\alpha}\right),$$
$$\rho = (r-1)k,$$
$$\lambda = (r-2)+(k-1)(\alpha-1), \text{ and}$$
$$\mu = k\alpha.$$

Furthermore, if $\theta > \tau$ are the nonprincipal eigenvalues, then

$$\theta = r-\alpha-1, \text{ and}$$
$$\tau = -k.$$

We recall that reconstructing a $\mathrm{PG}(r,k,\alpha)$ geometry from its line-graph is equivalent to finding a reconstruction system (see Definition 2.7.8), a clique geometry in which every clique has order r, every vertex belongs to exactly k cliques, and for every clique C and every vertex $u \notin C$, the vertex u ahs exactly α neighbors in C.

Before proving our bounds on the number of reconstruction systems, we describe the extent to which *unique* reconstruction of a partial geometry is possible.

5.4.1 Unique Reconstruction of Partial Geometries

We first observe that the *parameters* of a partial geometry are always uniquely determined by its line-graph.

Proposition 5.4.2 (Uniqueness of parameters)**.** *The regular graph G is the line-graph of a partial geometry if and only if there exists a reconstruction system in G. In particular, if a reconstruction system in G exists then G is strongly regular and the parameters (r,k,α) are determined by the parameters of the strongly regular graph.*

Proof. If G is the line-graph of a partial geometry, then k is the absolute value of the negative eigenvalue of G [Neu79]. Since $\rho = k(r-1)$ and $\mu = \alpha k$, the other parameters of the partial geometry are also uniquely determined by the graph parameters. □

We now prove Theorem 2.7.9, the unique reconstruction criterion for partial geometries.

Proof of Theorem 2.7.9. Let $\mathfrak{X}$ be a $\mathrm{PG}(r,k,\alpha)$ with $k < (1+(r-\alpha)/(\alpha-1)$. Fix two adjacent vertices of $L(\mathfrak{X})$, i. e., two intersecting lines ℓ_1, ℓ_2 of $\mathfrak{X}$, and let p be the unique point of $\mathfrak{X}$ contained in both. Note that ℓ_1 and ℓ_2 have $r-2+(\alpha-1)(k-1)$ common neighbors in $L(\mathfrak{X})$, and $r-2$ of these contain p. These $r-2$ neighbors are all adjacent. On the other hand, each of the $(\alpha-1)(k-1)$ common neighbors not containing p is adjacent to at most $(\alpha-2)$ of the common neighbors containing p. Thus, if

$$r-3 > (\alpha-1)(k-1)-1+(\alpha-2),$$

or, equivalently, if

$$k < 1+\frac{r-\alpha}{\alpha-1},$$

then the lines which contain p are distinguished from whose which do not by their valency in the subgraph induced on the common neighbors of ℓ_1 and ℓ_2.

For any pair of adjacent vertices x, y in $L(\mathfrak{X})$, let $C_{x,y}$ denote the set containing x, y, and every common neighbor of x and y with at least $r-3$ neighbors in common with both x and y. Then $C_{x,y}$ is a clique, and the collection of all such cliques $C_{x,y}$ is the unique reconstruction system in $L(\mathfrak{X})$. □

Corollary 5.4.3. *If $\mathfrak{X}$ is a $S(2,k,n)$ design with $k(k^2-2k+2) < n$, then $L(\mathfrak{X})$ has a unique reconstruction system, and it can be recovered from $L(\mathfrak{X})$ in polynomial time.*

The unique reconstruction inequality of Corollary 5.4.3 for Steiner designs is equivalent to the inequality $\rho < f(v)$ for a certain function $f(v) \sim v^{3/4}$, where v is the number of vertices of $L(\mathfrak{X})$.

Now we show that this unique reconstructibility bound is optimal.

Proposition 5.4.4. *There exists an infinite family of $S(2,k,n)$ designs $\mathfrak{X}$ with $n = k(k^2 - 2k + 2)$ such that $L(\mathfrak{X})$ has more than one reconstruction system.*

Proof. Let $\mathfrak{X}$ consist of the set of points and lines of the 3-dimensional projective space over $GF(q)$. We have $k = q + 1$ and $v = q^3 + q^2 + q + 1 = k(k^2 - 2k + 2)$ for such designs. This system has an anti-automorphism that swaps points and hyperplanes; so the system $\mathcal{R} = \{X_h : h \text{ a hyperplane}\}$ where X_h denotes the set of lines in h constitutes a second reconstruction system. □

5.4.2 Feasible Cliques

We now turn our attention to proving Theorems 2.7.10 and 2.7.11. In the rest of this section, G will be the line-graph of a PG(r,k,α) with n points and $m = v$ lines (G has v vertices).

We say a clique C is *feasible* if $C \in \mathcal{R}$ for some reconstruction system $\mathcal{R}$ of G.

Theorem 5.4.5. *Assume G is not complete, and let $s = \lfloor 1 + \log m / \log(r/\alpha) \rfloor$. Then the number of feasible cliques is at most $\binom{m}{s}$.*

We say a set of vertices A is a *seed* of a clique C if C consists of A and all the common neighbors of the set A.

Lemma 5.4.6 (Small seeds)**.** *If G is not complete, then each feasible clique has a seed of size $s = \lfloor 1 + \log m / \log(r/\alpha) \rfloor$.*

Proof. Any feasible clique is the collection of lines through some point p in a partial geometry whose line-graph is isomorphic to G, so for each point p, it suffices to find a collection S of s lines in $\mathfrak{X}$ with the property that any line intersecting each element of S must contain p.

Fix a point p and a line ℓ such that $p \notin \ell$. Let $t \geq 1$. Let $S = \{\ell_1, \ldots, \ell_t\}$ be a collection of lines through p chosen independently at random. Since $p \notin \ell$, there are exactly α lines

containing p which intersect ℓ. Hence, the probability that ℓ intersects each ℓ_i is $(\alpha/r)^t$. Then, by the union bound,

$$P[(\exists \ell)(\forall i)(\ell \cap \ell_i \neq \emptyset)] \leq \left(\frac{\alpha}{r}\right)^t m\,.$$

□

Theorem 5.4.5 follows immediately from Lemma 5.4.6: every feasible clique can be generated from a set of vertices of size $\lfloor 1 + \log m / \log(r/\alpha) \rfloor$. □

Given a reconstruction system $\mathcal{R}$ of G, a *point-clique* is an element of $\mathcal{R}$; all other maximal cliques of G are *nonpoint-cliques*.

Lemma 5.4.7. *Let $\mathcal{R}$ be a reconstruction system of G. Let C be a nonpoint-clique and let P be a point-clique. Then $|P \cap C| \leq \alpha$.*

Proof. Since C is a nonpoint-clique, there is some line $\ell \in C \setminus P$. Since P contains exactly α lines which meet ℓ, and every line in C meets ℓ, we have $|P \cap C| \leq \alpha$. □

5.4.3 Reconstruction of Steiner Designs

We say a clique C is *regular* if (i) $|C| = r$, and (ii) every vertex $\ell \notin C$ has exactly α neighbors $\ell' \in C$. Clearly point-cliques are regular, and therefore so are all feasible cliques of G. We say two cliques C_1, C_2 are *adjacent* if they intersect in exactly one vertex of G, i.e., in exactly one line.

To prove our reconstruction bound for Steiner designs, we first show that for every nonpoint-clique C, there are many point-cliques which are not adjacent to C. In order to reconstruct the design, it therefore suffices to sample a small, random collection $\mathcal{K}$ of point-cliques: point-cliques will always be adjacent to the cliques in $\mathcal{K}$, but with good probability, every nonpoint-clique will be non-adjacent to at least one clique in $\mathcal{K}$.

Lemma 5.4.8. *Suppose $\mathfrak{X}$ is a Steiner $S(2,k,n)$ design, and let C be a regular nonpoint-clique. Then at least $\Omega(n^2/k^3)$ point-cliques are not adjacent to C.*

Proof. For a point-clique $P \in \mathcal{R}$, let $d_P = |P \cap C|$. By Lemma 5.4.7, since $\alpha = k$ for a Steiner design, we have $d_P \leq k$ for every $P \in \mathcal{R}$. Let $D = \max\{d_P : P \in \mathcal{R}\}$.

Fix a line $\ell \in C$. Since $d_P \leq D$ for each of the k point-cliques P containing ℓ, and every line in C intersects ℓ, we have $1 + (D-1)k \geq |C| = r$. Hence,

$$D \geq 1 + \frac{r-1}{k}.$$

Let $P \in \mathcal{R}$ be such that $d_P = D$. By the regularity of C, if $\ell \in P \setminus C$, there are exactly $k - D$ lines of C which intersect ℓ away from P. Hence, there are at least $(k-1)-(k-D) = D-1$ points on ℓ which do not lie on any line in C. Hence, summing over all lines $\ell \in P \setminus C$, the number m_C of point-cliques which do not lie on any line of C is at least

$$m_C \geq (r-D)(D-1) = -D^2 + (r+1)D - r. \tag{5.9}$$

We have $1 + (r-1)/k \leq D \leq k$, so the right side of Eq. (5.9) is minimized either when $D = k$ or when $D = 1 + (r-1)/k$.

Suppose first that $D = k$, so $m_C \geq (r-k)(k-1)$. If $k \geq r/2$, since $k < r$, we have $m_C \geq (r/2 - 1) = \Omega(r^2/k)$. Otherwise $k < r/2$. Since always $D - 1 \geq (r-1)/k$, we have

$$m_C \geq \frac{(r-k)(r-1)}{k} > \frac{r(r-1)}{2k} = \Omega\left(\frac{r^2}{k}\right).$$

Otherwise, suppose $D = 1 + (r-1)/k$. Then by Eq. 5.9, we have

$$m_C \geq \frac{(rk - r - k + 1)(r-1)}{k^2} > \frac{r(k-2)(r-1)}{k^2} = \Omega\left(\frac{r^2}{k}\right).$$

Hence, in any case, $m_C = \Omega(r^2/k) = \Omega(n^2/k^3)$, as desired. □

For the remainder of this section, we write $s = \lfloor 1 + \log m / \log(r/\alpha) \rfloor$.

Corollary 5.4.9. *Suppose $\mathfrak{X}$ is a Steiner $S(2, k, n)$ design. There is a collection $\mathcal{K}$ of $O(k^3 s \log n/n)$ point-cliques such that every nonpoint-clique is nonadjacent with at least one element of $\mathcal{K}$.*

Proof. By Lemma 5.4.8, if C is a nonpoint-clique and P is a random point-clique, the probability that P is nonadjacent with C is at least $\Omega(n/k^3)$. By Theorem 5.4.5, there are at most $m^s = n^{O(s)}$ nonpoint-cliques. By the union bound, if d point-cliques are chosen at random, the probability that there is a nonpoint-clique adjacent to all d point-cliques is at most

$$\left(1 - \Omega\left(\frac{n}{k^3}\right)\right)^d n^{O(s)}$$

For some $d = O(k^3 s \log n/n)$, this probability is less than 1. Therefore, some choice of $O(k^3 s \log n/n)$ point-cliques has the desired property. □

Proof of Theorem 2.7.10. Let $\mathcal{F}$ be the collection of all feasible cliques. By Theorem 5.4.5, we have $|\mathcal{F}| \leq \binom{m}{s} = n^{O(s)}$.

Fix a reconstruction system $\mathcal{R}$. By Corollary 5.4.9, some collection $\mathcal{K}$ of $O(kns \log n/r^2)$ point-cliques has the property that every nonpoint-clique in $\mathcal{F}$ is nonadjacent with at least one element of $\mathcal{K}$. On the other hand, every point-clique in $\mathcal{R} \setminus \mathcal{K}$ is adjacent to every element of $\mathcal{K}$. Hence, $\mathcal{R}$ is completely determined by the choice of $\mathcal{R}$. Thus, there are at most $\exp(O(k^3(s \log n)^2/n))$ reconstruction systems. □

5.4.4 Reconstruction for General α

We now prove the weaker reconstruction bound of Theorem 2.7.11, which applies more generally to $\mathrm{PG}(r, k, \alpha)$ partial geometries. The approach of Theorem 2.7.10 fails badly when α is much smaller than k: with high probability, two random point-cliques are nonadjacent, so we no longer distinguish nonpoint-cliques from point-cliques by adjacency with a small set of chosen point-cliques. However, it is still the case that for any pair of distinct point-cliques

P_1, P_2 we have $|P_1 \cap P_2| \leq 1$. So, we identify nonpoint-cliques C by choosing point-cliques P for which $|P \cap C| \geq 2$.

We say a point-clique $P \in \mathcal{R}$ is a *concentration point* for the nonpoint-clique C if $|P \cap C| \geq 2$.

Lemma 5.4.10. *Let C be a regular nonpoint-clique. The number of lines with a concentration point for C is at least*

$$\frac{r(r-1)(r-\alpha)}{\alpha(\alpha-1)}.$$

Proof. For a point-clique $P \in \mathcal{R}$, let $d_P = |P \cap C|$. By Lemma 5.4.7, we have $d_P \leq \alpha$ for every $P \in \mathcal{R}$.

Let $\mathcal{C}$ be the set of concentration points for C. Since $|C| = r$ and every pair of lines in C meets at exactly one concentration point, we have

$$\sum_{P \in \mathcal{C}} \binom{d_P}{2} = \binom{r}{2}.$$

On the other hand, if $\ell \notin C$, then by the regularity of C, at most α lines of C meet in concentration points of ℓ, so

$$\sum_{\substack{P \in \mathcal{C}, \\ P \ni \ell}} \binom{d_P}{2} \leq \binom{\alpha}{2}$$

Let L be the collection of lines not in C with a concentration point for C. Then

$$\begin{aligned}(r-\alpha)\binom{r}{2} &\leq \sum_{P \in \mathcal{C}} (r - d_P)\binom{d_P}{2} = \sum_{P \in \mathcal{C}} \sum_{\ell \in P \setminus C} \binom{d_P}{2} \\ &= \sum_{\ell \in L} \sum_{\substack{P \in \mathcal{C}, \\ P \ni \ell}} \binom{d_P}{2} \leq |L| \binom{\alpha}{2}.\end{aligned}$$

Hence, $|L| \geq r(r-1)(r-\alpha)/(\alpha(\alpha-1))$ as claimed. □

For the remainder of this section, we write $s = \lfloor 1 + \log m / \log(r/\alpha) \rfloor$.

Corollary 5.4.11. *There is a collection L of $O(sk\alpha \log m/r)$ lines such that every nonpoint-clique has a concentration point on at least one of the lines in L.*

The proof is identical to the proof of Corollary 5.4.9 from Lemma 5.4.8. □

Lemma 5.4.12. *Let ℓ be a line. There is a collection $\mathcal{K}$ of $O(sk\alpha \log m/r)$ point-cliques containing ℓ such that a regular clique $C \notin \mathcal{K}$ containing ℓ is a point-clique if and only if it is adjacent to every clique in $\mathcal{K}$.*

Proof. Again, the proof is very similar to the proof of Corollary 5.4.9. We choose point-cliques $P_1, \ldots, P_d$ containing ℓ at random, and let C be a regular clique containing ℓ. Clearly, if C is a point-clique, then either $C = P_i$ for some i, or C is adjacent to every P_i. On the other hand, if C is a nonpoint-clique, then by Lemma 5.4.7, $|P \cap C \setminus \{\ell\}| \leq \alpha - 1$ for every point-clique P containing ℓ. But the $r-1$ lines in $C \setminus \{\ell\}$ all intersect ℓ, so there are at least $(r-1)/(\alpha-1)$ concentration points for C containing ℓ. None of these concentration points is adjacent to C. In particular, the probability that every point-clique P_i is adjacent to C is at most $(1 - (r-1)/(k(\alpha-1)))^d$.

By Theorem 5.4.5, there are at most m^s nonpoint-cliques, so by the union bound, the probability that there exists a nonpoint-clique adjacent to each P_i is at most

$$\left(1 - \Omega\left(\frac{r}{k\alpha}\right)\right)^d m^s.$$

For some $d = O(sk\alpha \log m/r)$, this probability is less than 1, hence some choice of point-cliques has the desired property. □

Proof of Theorem 2.7.11. Let $\mathcal{F}$ be the collection of all feasible cliques. By Theorem 5.4.5, we have $|\mathcal{F}| \leq \binom{m}{s}$.

Fix a reconstruction system $\mathcal{R}$. By Corollary 5.4.11, some collection L of $O(sk\alpha \log m/r)$ lines has the property that every nonpoint-clique has a concentration point on at least one line of L. By Lemma 5.4.12, for each line $\ell \in L$, there is a set $\mathcal{K}_\ell$ of $O(sk\alpha \log m/r)$ point-cliques containing ℓ such that for any clique $C \in \mathcal{F}$ containing ℓ, we have $C \in \mathcal{R}$ if and

only if $C \in \mathcal{K}_\ell$ or C is adjacent to every clique in $\mathcal{K}_\ell$. Let $\mathcal{R}_\ell$ denote the cliques in $\mathcal{R}$ containing ℓ. We may therefore recover $\mathcal{R}$ from $\mathcal{K}_\ell$.Let $\mathcal{R}' = \bigcup_{\ell \in L} \mathcal{R}_\ell$. By the definition of L, a clique $C \in \mathcal{F} \setminus \mathcal{R}'$ is a point-clique if and only if there is no $P \in \mathcal{R}'$ such that $|P \cap C| \geq 2$. Hence, from $\mathcal{R}'$, we can recover $\mathcal{R}$.Thus, the choice of $\bigcup_{\ell \in L} \mathcal{K}_\ell$, a collection of $O(sk\alpha \log m/r)^2$ cliques in $\mathcal{F}$, completely determines $\mathcal{R}$. In particular, there are at most $\exp(O((k\alpha/r)^2(s \log m)^3))$ reconstruction systems. $\square$

Chapter 6

STRONGLY REGULAR GRAPHS

In this chapter, we prove our automorphism bounds for strongly regular graphs. We begin by collecting various estimates for the parameters of strongly regular graphs in Section 6.1. In Section 6.2, we prove several of our automorphism bounds for strongly regular graphs. Section 6.3 gives two vertex expansion lemmas that will be useful in later proofs. Finally, in Section 6.4, we prove Theorem 2.4.2, on which many of our other automorphism bounds depend.

Since the complement of a strongly regular graph is again strongly regular, we will assume throughout that $\rho \leq (v-1)/2$.

6.1 Bounds on the Parameters

We now summarize the bounds we have available for the parameters of strongly regular graphs. We begin with a summary of standard facts (see, e.g., [GR01, Chapter 10]).

Proposition 6.1.1. *Let G be a nontrivial* $\mathrm{SR}(v, \rho, \lambda, \mu)$ *graph with nonprincipal eigenvalues $\theta > \tau$. Then the following statements are all true:*

(i) $\rho(\rho - \lambda - 1) = (v - \rho - 1)\mu$

(ii) $\theta\tau = \mu - \rho$

(iii) $\theta + \tau = \lambda - \mu$

Using Proposition 6.1.1, we have the following simple corollary to Theorem 2.7.4 in the case of a strongly regular graph.

Corollary 6.1.2. *Let G be a nontrivial* $\mathrm{SR}(v, \rho, \lambda, \mu)$ *graph with nonprincipal eigenvalues $\theta > \tau$. Then*

$$\theta < \max\left\{4\sqrt{2v}, \frac{6}{\sqrt{13}-1}\sqrt{\rho(\mu-1)}\right\} + \sqrt{\rho}.$$

Proof. By Proposition 6.1.1 (ii), we have $\theta < \rho/(-\tau)$, so if $-\tau \geq \sqrt{\rho}$, the inequality is immediate. Otherwise, $-\tau \leq \sqrt{\rho}$, and so the inequality follows from Proposition 6.1.1 (iii) and Theorem 2.7.4. □

The following bound is implicit in [Bab80b] and is given explicitly in [Bab14, Lemma 17].

Proposition 6.1.3. *Let G be a nontrivial* $\mathrm{SR}(v, \rho, \lambda, \mu)$ *graph. Then* $\max(\lambda, \mu) < (3/4)\rho$.

The following is an easy consequence of Proposition 6.1.3.

Corollary 6.1.4. *Let G be a nontrivial* $\mathrm{SR}(v, \rho, \lambda, \mu)$ *graph. Then*

(i) $\mu = \Theta(\rho^2/v)$.

Specifically,

(ii) $\rho^2/(4v) < \mu < 2\rho^2/v$.

Furthermore, if $\rho = o(v)$ *and* $\lambda = o(\rho)$, *then*

(iii) $\mu \sim \rho^2/v$.

Proof. From Proposition 6.1.1 (i) and our convention $\rho \leq (v-1)/2$ we have that $\mu(v-1)/2 < \rho(\rho - 1)$ and therefore $\mu v/2 < \rho^2$. From Proposition 6.1.1 (i) and Proposition 6.1.3, we obtain $\mu n > k^2/4$, proving parts (i) and (ii). Part (iii) of the corollary is immediate from part (ii). □

We point out the philosophical significance of Corollary 6.1.4. Written as $\mu/n \sim (k/n)^2$, Corollary 6.1.4 (iii) can be interpreted as saying that the neighborhoods of nonadjacent pairs of vertices are "asymptotically independent." Since most pairs of vertices are not adjacent, this is the typical behavior.

While the neighborhoods of adjacent vertices can be heavily positively correlated, bounds on λ limit this correlation.

We now state the full version of Neumaier's classification, from which one such bound on λ will follow.

Theorem 6.1.5 (Neumaier's classification [Neu79])**.** *Let G be a nontrivial* $\mathrm{SR}(v, \rho, \lambda, \mu)$ *graph with nonprincipal eigenvalues $\theta > \tau$. Then at least one of the following is true:*

(a) G is a conference graph;

(b) G is the line-graph of a transversal design;

(c) G is the line-graph of a Steiner design;

(d) G satisfies the claw bound*:*

$$\theta \leq \max\left\{2(-\tau-1)(\mu+\tau+1)+\tau, \frac{\tau(\tau+1)(\mu+1)}{2}-1\right\}. \tag{6.1}$$

Inequality (6.1) is called the "claw bound."

We demonstrated in Section 5.4 that in general a transversal or Steiner design cannot be uniquely reconstructed from its line-graph. However, in cases (b) and (c) of Neumaier's classification, we can without loss of generality assume that the design can be uniquely reconstructed from its line-graph, since otherwise the line-graph satisfies the claw bound and falls under case (d). Indeed, recalling that a transversal design is a $\mathrm{PG}(r, k, k-1)$ geometry, and a Steiner design is a $\mathrm{PG}(r, k, k)$ geometry, we have the following more general proposition.

Proposition 6.1.6. *Let $\mathfrak{X}$ be a* $\mathrm{PG}(r, k, \alpha)$ *geometry. Then either $L(\mathfrak{X})$ has a unique reconstruction system (in the sense of Definition 2.7.8), or $L(\mathfrak{X})$ satisfies the claw bound, inequality* (6.1)*.*

Proof. Let G be the line-graph of a Steiner or transversal design, i.e., the line-graph of a $\mathrm{PG}(r, k, \alpha)$ with $\alpha = k$ or $\alpha = k-1$. Suppose G does not have a unique reconstruction system. By Theorem 2.7.9, we have $k \geq 1 + (r-\alpha)/(\alpha-1)$, so $r - \alpha - 1 \leq k(\alpha-1) - \alpha$.

Hence, assuming $k, \alpha \geq 1$, we have

$$\begin{aligned} r - \alpha - 1 &\leq (k\alpha - k) - \alpha \\ &\leq 2(k-1)(k\alpha - k) + k - 2 \\ &= 2(k-1)(k\alpha - k + 1) - k. \end{aligned}$$

By Proposition 5.4.1, we have $\mu = k\alpha$, and if $\theta > \tau$ are the nonprincipal eigenvalues, then $\theta = r - \alpha - 1$ and $\tau >= -k$. Hence, we have $\theta \leq 2(-\tau - 1)(\mu + \tau + 1) + \tau$, proving inequality (6.1). □

The following consequences of Neumaier's classification for the parameters of a strongly regular graph are implicit in Spielman's paper on the Strongly Regular Graph Isomorphism problem [Spi96].

Theorem 6.1.7 (Spielman [Spi96])**.** *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph with nonprincipal eigenvalues $\theta > \tau$. If G satisfies inequality* (6.1) *(the claw bound), then*

(i) $\theta < \rho^{2/3}(\mu + 1)^{1/3}$*;*

(ii) $\lambda < \rho^{2/3}(\mu + 1)^{1/3}$*;*

Assume furthermore that $\rho = o(v)$. Then

(iii) $\lambda = o(\rho)$*;*

Spielman explicitly states (iii). For the reader's convenience, we now give an organized presentation of a proof of the full statement of Theorem 6.1.7.

Proof of Theorem 6.1.7. For any strongly regular graph, $\tau \leq -1$ (see, e.g., [BCN89, Corollary 3.5.4]). Therefore $2(-\tau - 1)(\mu + 1 + \tau) + \tau \leq \tau^2(\mu + 1)$, and so, assuming the claw bound, we have

$$\theta \leq \tau^2(\mu + 1). \tag{6.2}$$

Combining this with $\rho - \mu = -\theta\tau$ from Proposition 6.1.1 (ii) gives

$$\theta \leq \left(\frac{\rho-\mu}{\theta}\right)^2 (\mu+1),$$

and hence, multiply both sides by θ^2 and taking the $1/3$ power,

$$\theta \leq (\rho-\mu)^{2/3}(\mu+1)^{1/3},$$

proving part (i) of the theorem. But then combining the bound on θ above with Proposition 6.1.1 (iii) we have

$$\lambda < \theta + \mu < \rho^{2/3}(\mu+1)^{1/3},$$

proving part (ii) of the theorem.

Now if $\rho = o(n)$, then $\mu = o(k)$ from Corollary 6.1.4. Then $\lambda = o(k)$ from part (ii) of the theorem, giving part (iii). □

The following elementary inequalities appear in a recent paper by Pyber [Pyb14].

Theorem 6.1.8 (Pyber [Pyb14])**.** *Let G be a nontrivial* $\mathrm{SR}(v,\rho,\lambda,\mu)$ *graph with nonprincipal eigenvalues $\theta > \tau$. Then*

(i) $\theta < v^{1/4}\rho^{1/2}$;

(ii) $\lambda < v^{1/4}\rho^{1/2} + \mu$.

We now summarize the combination of the bounds on θ from Corollary 6.1.2, Theorem 6.1.7, and Theorem 6.1.8, and state the best bound for each possible value of the valency ρ.

Corollary 6.1.9. *Let*

$$g(v,\rho) = \min\left\{\left(\frac{\rho}{v}\right)^{4/3},\ \frac{\rho^{1/2}}{v^{3/4}},\ \max\left\{\left(\frac{\rho}{v}\right)^{3/2},\ \left(\frac{1}{v}\right)^{1/2}\right\}\right\}.$$

Table 6.1: Piecewise description of the function $g(v, \rho)$ giving the best known bounds on θ/v

Value	Parameter range	Source
$(\rho/v)^{4/3}$	$\rho \leq v^{5/8}$	Spielman [Spi96]
$v^{-1/2}$	$v^{5/8} \leq \rho \leq v^{2/3}$	Corollary 6.1.2
$(\rho/v)^{3/2}$	$v^{2/3} \leq \rho \leq v^{3/4}$	Corollary 6.1.2
$\rho^{1/2}v^{-3/4}$	$\rho \geq v^{3/4}$	Pyber [Pyb14]

Then for any nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ *graph* G *with nonprincipal eigenvalues* $\theta > \tau$*, if* G *satisfies inequality* (6.1) *(the claw bound), we have*

$$\frac{\theta}{v} = O(g(v, \rho)).$$

Note that the function $g(v, \rho)$ is continuous, so up to constant factors the transition is continuous around the boundaries of the intervals in Table 6.1.

We now summarize the combination of the bounds on λ from Theorem 2.7.4, Theorem 6.1.7, and Theorem 6.1.8, and state the best bound for each possible value of the valency ρ.

Corollary 6.1.10. *Let*

$$h(v, \rho) = \min\left\{\left(\frac{\rho}{v}\right)^{4/3},\ \max\left\{\frac{\rho^{1/2}}{v^{3/4}},\ \left(\frac{\rho}{v}\right)^{2}\right\},\ \max\left\{\left(\frac{\rho}{v}\right)^{3/2},\ \left(\frac{1}{v}\right)^{1/2}\right\}\right\}.$$

Then for any nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ *graph* G *with nonprincipal eigenvalues* $\theta > \tau$*, if* G *satisfies inequality* (6.1) *(the claw bound), we have*

$$\frac{\lambda}{v} = O(h(v, \rho)).$$

Table 6.2: Piecewise description of the function $h(v, \rho)$ giving the best known bounds on λ/v

Value	Parameter range	Source
$(\rho/v)^{4/3}$	$\rho \leq v^{5/8}$	Spielman [Spi96]
$v^{-1/2}$	$v^{5/8} \leq \rho \leq v^{2/3}$	Theorem 2.7.4
$(\rho/v)^{3/2}$	$v^{2/3} \leq \rho \leq v^{3/4}$	Theorem 2.7.4
$\rho^{1/2}v^{-3/4}$	$v^{3/4} \leq \rho \leq v^{5/6}$	Pyber [Pyb14]
$(\rho/v)^2$	$\rho \geq v^{5/6}$	Pyber [Pyb14]

6.2 Bounds on Automorphism Group

We now use the parameter estimates of the previous section to derive four of our results for the automorphism groups of strongly regular graphs, Corollary 2.4.3, Theorem 2.4.7, Theorem 2.4.8, and Corollary 2.4.11.

Proof of Corollary 2.4.3. Let G be a $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph with $\rho = \Omega(v^{5/6})$. Corollary 6.1.10 and Corollary 6.1.4, we have $\lambda/\mu = O(1)$. Hence, by Theorem 2.4.2, we have $|\operatorname{Aut}(G)| \leq \exp(O(\log^4 v))$. □

For the proof of Theorem 2.4.7, we require the following result of Miller, a $n^{O(\log n)}$ bound for the number of automorphisms of a transversal design. The bound follows directly from the quasigroup structure of a transversal design.

Theorem 6.2.1 (Miller [Mil78])**.** *Let $\mathfrak{X}$ be a nontrivial $\mathrm{TD}(r, k)$ design with n points. Then naive refinement is $O(\log n)$-effective for $\mathfrak{X}$, and $\mathfrak{X}$ has at most $n^{O(\log n)}$ automorphisms.*

Proof of Theorem 2.4.7. Let G be a $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph, and assume G is the line-graph of a Steiner $\mathrm{S}(2, k, n)$ design. If $\rho > v^{11/14} \log^{4/7} v$, then by Corollary 6.1.10 and Corollary 6.1.4 we have $\lambda/\mu = O(v^{5/4}\rho^{-3/2})$. Hence G has at most $\exp(O(v^{1/14} \log^{22/7} v))$ automorphisms by Theorem 2.4.2. Otherwise, $\rho \leq v^{11/14} \log^{4/7} v$. By Proposition 5.4.1, we have $v = \Theta(r^2)$ and $\rho = \Theta(rk)$. Furthermore, the number of lines v in a Steiner 2-design is rn/k. Hence, $k^3/n = \Theta(\rho^2/v^{3/2})$, and $\log(r/k) = \Theta(\log(v/\rho)) = \Omega(\log n)$. Hence, by Theorem 2.7.10 there are at most $\exp(O(v^{1/14} \log^{22/7} v))$ reconstruction systems in G. By Theorem 2.3.2,

each reconstructed Steiner design has at most $n^{O(\log n)} = v^{O(\log v)}$ automorphisms. Hence, G has at most $\exp(O(v^{1/14} \log^{22/7} v))$ automorphisms.

The proof when G is the line-graph of a transversal design is similar, using instead the threshold $\rho > v^{17/22} \log^{2/11} v$, Theorem 6.2.1 in place of Theorem 2.3.2, and Theorem 2.7.11 in place of Theorem 2.7.10. □

To prove Theorem 2.4.8, we require the following more detailed statement of Spielman's Theorem 2.4.6.

Theorem 6.2.2 (Spielman [Spi96])**.** *Let $\mathcal{C}_\varepsilon$ be the class of* $\mathrm{SR}(v, \rho, \lambda, \mu)$ *graphs with $\rho < \varepsilon v^{2/3}$ and $\lambda < \varepsilon\rho$. There is an $\varepsilon > 0$ such that naive refinement is $O(\sqrt{v \log v/\rho})$-effective for $\mathcal{C}_\varepsilon$.*

The proof of Theorem 2.4.8 is essentially identical to Spielman's proof of Theorem 2.4.6, except that we use our Theorem 2.4.2 instead of Babai's Theorem 2.4.5 for large valencies.

Proof of Theorem 2.4.8. Let G be a $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph. We divide our analysis according to Neumaier's classification of strongly regular graphs, Theorem 6.1.5. If G is a conference graph, then $\mu = \Omega(\lambda)$, and so has at most $\exp(\widetilde{O}(1))$ automorphisms by Theorem 2.4.2. If G is the line-graph of a $\mathrm{TD}(r, k)$ design or $\mathrm{S}(2, k, n)$ design, and does not satisfy Neumaier's claw bound, then the design can be uniquely reconstructed from G by Theorem 2.7.9. The design has at most $n^{O(\log n)}$ automorphisms, where n is the number of points, by Theorems 2.3.2 and 6.2.1. Hence, if G is the line-graph of a design and does not satisfy Neumaier's claw bound, it has at most $v^{O(\log v)}$ automorphisms.

Hence, we may assume G satisfies Neumaier's claw bound. Furthermore, if $\rho = \Omega(v^{2/3})$, then $\lambda/\mu = O(\sqrt{v/\rho}) = O(v^{1/6})$ by Corollary 6.1.10, so G has at most $\exp(\widetilde{O}(v^{1/6}))$ automorphisms by Theorem 2.4.2. Otherwise, if $\rho = o(v^{2/3})$, then also $\lambda = o(\rho)$ by Corollary 6.1.10, so G has $\exp(\widetilde{O}(v^{1/4}))$ automorphisms by Theorem 6.2.2. □

Proof of Corollary 2.4.11. Let G be a $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph which is not a triangular or lattice graph. We divide our analysis according to Neumaier's classification of strongly regular

graphs, Theorem 6.1.5. If G is a conference graph, then $\mu = \Omega(\lambda)$, and so we have the stronger result that $|\operatorname{Aut}(G)| \leq \exp(\widetilde{O}(1))$ by Theorem 2.4.2. If G is the line-graph of a $\mathrm{TD}(r,k)$ design or $\mathrm{S}(2,k,n)$ design, and does not satisfy Neumaier's claw bound, then the design can be uniquely reconstructed from G. Suppose G is the line-graph of a $\mathrm{S}(2,k,n)$ design and G does not satisfy Neumaier's claw bound. Since G is not a triangular graph, the Steiner design is nontrivial, and so the design (and hence G) has at most $n^{O(\log n)} = v^{O(\log v)}$ automorphisms by Theorem 2.3.2. Similarly, if G is the line-graph of a $\mathrm{TD}(r,k)$ design and G does not satisfy Neumaier's claw bound, it has at most $v^{O(\log v)}$ automorphisms by Theorem 6.2.1.

Hence, we may assume G satisfies Neumaier's claw bound. Furthermore, if $\rho = \Omega(v)$, then $\mu = \Omega(\rho) = \Omega(\lambda)$ by Corollary 6.1.4. Hence, by Theorem 2.4.2, we have $|\operatorname{Aut}(G)| \leq \exp(\widetilde{O}(1))$. So, we may additionally assume $\rho = o(v)$. By Corollary 6.1.10, we therefore have $\lambda = o(\rho)$. Now if $\rho < v^{3/5}\log^{1/5} v$, then $\mu = O(v^{1/5}\log^{2/5} v)$ by Corollary 6.1.4, so the result follows from Theorem 2.4.10. If $v^{3/5}\log^{1/5} v \leq \rho = o(v^{2/3})$, then Theorem 6.2.2 gives the stronger result that $|\operatorname{Aut}(G)| \leq \exp(O(v^{1/5}\log^{2/5} v))$. And otherwise, by Corollary 6.1.10 and Corollary 6.1.4, we have $\lambda/\mu = O(\sqrt{v/\rho}) = O(v^{1/6})$, so Theorem 2.4.2 gives that $|\operatorname{Aut}(G)| \leq \exp(\widetilde{O}(v^{1/6}))$. □

6.3 Two Vertex Expansion Lemmas

We now prove the two vertex expansion lemmas for strongly regular graphs stated in Section 2.8. The first is easy, and will suffice for the proof of the $\exp(\widetilde{O}(\lambda/\mu))$ bound on the number of automorphisms proved in the next section.

Proof of Lemma 2.8.1. Every vertex $y \in G(A)\setminus G^+(x)$ satisfies $|G(y)\cap A| \leq |G(y)\cap G(x)| \leq \mu$. On the other hand, every vertex $z \in A$ has exactly $\rho - \lambda - 1$ neighbors $y \in G(A)$ such that $y \notin G^+(x)$. Therefore, by counting the edges between A and $|G(A) \setminus G^+(x)|$, we have $|G(A) \setminus G^+(x)| \geq (\rho - \lambda - 1)|A|/\mu$. □

Proof of Lemma 2.8.2. Define T as the set of triples (a, y, b) of vertices satisfying $a \in A, b \in G(x) \setminus A$, and $y \in G(a) \cap G(b)$. Let $X = \{(a, y, b) \in T : y \notin G^+(x)\}$. We claim that

$$|X| \geq \left(\frac{1-\varepsilon}{2}\right)|A|\rho(\mu-4). \tag{6.3}$$

The lemma then follows. Indeed, suppose $y \in G(A) \setminus G^+(x)$. So

$$\mu = |G(y) \cap G(x)| = |G(y) \cap G(x) \cap A| + |G(y) \cap G(x) \setminus A|$$

Note that if $a, b \in V(G)$ are such that $(a, y, b) \in T$, then $a \in G(y) \cap G(x) \cap A$, and $b \in G(y) \cap G(x) \setminus A$. Thus, the number of pairs $a, b \in V(G)$ such that $(a, y, b) \in X$ is at most

$$|G(y) \cap G(x) \cap A| \cdot |G(y) \cap G(x) \setminus A| = |G(y) \cap G(x) \cap A|(\mu - |G(y) \cap G(x) \cap A|) \leq \frac{\mu^2}{4}.$$

Therefore,

$$|G(A) \setminus G^+(x)| \geq \frac{4|X|}{\mu^2} \geq 2(1-\varepsilon)\frac{|A|\rho(\mu-4)}{\mu^2} = \alpha\left(\frac{\rho}{\mu}\right)|A|.$$

We now prove inequality (6.3).

Let $Z = \{(a, y, b) \in T : a \not\sim b \text{ and } y \neq x\}$. For every vertex $a \in A$, there are $\geq \rho - \lambda - |A|$ vertices $b \in G(x) \setminus A$ with $a \not\sim b$. For every such pair (a, b), there are $\mu - 1$ vertices y such that $(a, y, b) \in Z$. Thus, $|Z| \geq |A|(\rho - \lambda - |A|)(\mu - 1) > |A|(1-\varepsilon)\rho(\mu-1)$. We will estimate $|X|$ in terms of $|Z|$.

Let $X' = \{(a, y, b) \in T : y \notin G(x)\}$. Thus, $X \subset X'$, and $X' \setminus X$ is the set of triples of the form (a, x, b) where $a \in A$ and $b \in G(x) \setminus A$. In particular, $|X'| = |X| + |A|(\rho - |A|)$. The set $Z \setminus X'$ is the collection of triples (a, y, b) of distinct vertices in $G(x)$ such that $a \in A$, $b \notin A$, and (a, y, b) induces a path (i. e., $a \sim y \sim b$ and $a \not\sim b$).

Let F be the set of edges $\{a, b\}$ such that $a \in A$ and $b \in G(x) \setminus A$. For any $(a, y, b) \in Z \setminus X'$, exactly one of the edges $\{a, y\}$ and $\{y, b\}$ is in F. Fix $\{a, b\} \in F$ and define $K = K(a, b) =$

$G(a) \cap G(b) \cap G(x)$. For any vertex $z \in V$, if $(z, a, b) \in Z \setminus X'$ then $z \in G(a) \cap G(x) \setminus K$, so there are at most $|G(a) \cap G(x) \setminus K| = \lambda - |K|$ such vertices z. Similarly, the number of vertices z such that $(a, b, z) \in Z \setminus X'$ is at most $|G(b) \cap G(x) \setminus K| = \lambda - |K|$. Thus,

$$|Z \setminus X'| \leq \sum_{\{a,b\} \in F} 2(\lambda - |K(a, b)|)$$

On the other hand, $X' \setminus Z$ contains all triples (a, y, b) such that $\{a, b\} \in F$ with $a \in A$ and $y \in G(a) \cap G(b) \setminus G(x)$. Thus, for fixed $\{a, b\} \in F$, there are exactly $|G(a) \cap G(b) \setminus K| = \lambda - |K|$ vertices y such that $(a, y, b) \in X' \setminus Z$. Thus,

$$|X' \setminus Z| \geq \sum_{\{a,b\} \in F} (\lambda - |K(a, b)|)$$

so that $|X' \setminus Z| \geq |Z \setminus X'|/2$. It follows that

$$\begin{aligned} |X'| &= |X' \cap Z| + |X' \setminus Z| \\ &\geq |X' \cap Z| + |Z \setminus X'|/2 \qquad\qquad \geq |Z|/2 \geq (1/2)|A|(1 - \varepsilon)\rho(\mu - 1)\,. \end{aligned}$$

Since $|X| = |X'| - |A|(\rho - |A|) \geq |X'| - |A|\rho$ and $\varepsilon \leq 1/3$, we have $|X| \geq (1/2)|A|(1 - \varepsilon)\rho(\mu - 4)$, completing the proof of inequality (6.3). □

6.4 The $\exp(\widetilde{O}(1 + \lambda/\mu))$ Bound

In this section, we will prove Theorem 2.4.2. More precisely, we prove the following result.

Theorem 6.4.1. *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph with $\rho \leq v/2$. Naive refinement is $O((1 + \lambda/\mu) \log^3 v)$-effective for G.*

Theorem 2.4.2 follows immediately in light of Proposition 3.2.2. □

We continue to assume $\rho \leq v/2$.

We set $\nu = \max\{\lambda, \mu\}$. Recall that $\mu = \Theta(\rho^2/v)$ (Corollary 6.1.4). Therefore $1 + \lambda/\mu = \Theta(\nu v/\rho^2)$. Hence, to prove Theorem 6.4.1, we shall prove that naive-refinement is $O((\nu v/\rho^2)\log^3 v)$-effective.

For non-trivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graphs with $\nu = \Omega(\rho)$, the following more detailed statement of Theorem 2.4.5 already gives the a stronger result.

Theorem 6.4.2 (Babai [Bab80b])**.** *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph with $\rho \leq v/2$. Then naive refinement is $O((v/\rho)\log v)$-effective.*

Hence, for the rest of Section 6.4, G will be a $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph with $\nu = o(\rho)$. In particular, $\mu = o(\rho)$ and so $\rho = o(v)$ by Corollary 6.1.4.

6.4.1 Overview of Proof

The proof of Theorem 6.4.1 is in some ways similar to the argument in Section 4.2. By individualizing vertices in stages, we gradually refine the overall coloring of G. There are three intermediate targets on the way to our ultimate target of discretely coloring G, outlined below. Each target is achieved from the previous target after at most $O((\nu/\mu)\log^3 v)$ individualizations.

The first goal is to ensure that there are $\Omega(\rho/\nu)$ uniquely colored vertices. This is the most technically demanding stage of the proof. We achieve the goal by iteratively applying Lemma 6.4.10, which guarantees that unless we already have enough uniquely colored vertices, we can individualize a single vertex to increase the total number of vertex colors in G by a multiplicative factor of $(1 + \Omega(\rho^2/(\nu v \log v)))$. Then $O((\nu v \log^2 v)/\rho^2)$ applications of the Lemma guarantee that there are enough uniquely colored vertices.

To prove Lemma 6.4.10, we find a collection $\mathcal{C}$ of color classes and a number $r \geq 2$ such that $r \leq |C| \leq 2r$ for every $C \in \mathcal{C}$ and $|\mathcal{C}| = \Omega(m/\log v)$, where m is the total number of colors in G. Such a collection exists, as long as we do not yet have enough uniquely colored vertices.

Suppose first that the color classes in $\mathcal{C}$ are large ($r = \Omega(\rho/\nu)$). Let $x \in V$ be a random vertex. For every color class $C \in \mathcal{C}$, we have $x \in G(C)$ with probability $\Omega((\rho/v)|C|) = \Omega(\rho^2/(\nu v))$. Furthermore, the probability that $C \subseteq G(x)$ is very small. Thus, with probability $\Omega(\rho^2/(\nu v))$, we have $G(x) \cap C$ a nonempty strict subset of C, so individualizing x splits C into two closed sets, $G(x) \cap C$ and $C \setminus G(x)$. So in the case that we have many large color classes, we can increase the total number of colors in G by the desired amount. The details are given in Lemma 6.4.12.

A more subtle argument is required in the event that the color classes in $\mathcal{C}$ are small ($r < \varepsilon\rho/\nu$). In this case, for every $C \in \mathcal{C}$, most vertices in $G(C)$ have a *unique* neighbor in C. So, a random vertex x will have a single neighbor y in C, for each of several color classes $C \in \mathcal{C}$. Then after individualizing x and refining to the stable coloring, each of these vertices y will become uniquely colored—the effect is the same as if we had individualized each such vertex y, but we only "pay" for the individualization of x. Some delicate analysis lets us show that $G(y)$ in turn intersects many color classes for each such vertex y. The details are given in Lemma 6.4.13

We have now obtained $\Omega(k/\nu)$ uniquely colored vertices. For the next two targets, our principal tool is Lemma 6.4.6. The lemma guarantees that a pair of vertices $x, y \in V$ will get different colors from each other after a moderate number of individualizations and refinement, assuming that the symmetric difference $G(x) \triangle G(y)$ already intersects many color classes. The idea of the proof is as follows. Consider two distinct vertices $x, y \in V(G)$ for which many color classes intersect the symmetric difference $G(x) \triangle G(y)$ of their neighborhoods. Our goal is to ensure that (after individualization and refinement) $G(x) \triangle G(y)$ intersects some color class C in exactly one vertex. Then either $G(x)$ intersects C or $G(y)$ intersects C, but not both, and so x and y get different colors in the stable refinement. If a color class C has large intersection with $G(x) \triangle G(y)$, then the neighborhood of a random vertex z has a good chance of intersecting $C \cap (G(x) \triangle G(y))$. So by individualizing such a vertex z, the set $C \cap G(z)$ is a smaller closed set which intersects $G(x) \triangle G(y)$. By iteratively

individualizing such random vertices z, we eventually ensure that there are many *small* color classes intersecting $G(x) \triangle G(y)$. But now if we take a random vertex z, there is a good chance that z has a *unique* neighbor in one of these small color classes C. Then after individualizing z, the steady set $N(z) \cap C$ will intersect $G(x) \triangle G(y)$ in exactly one vertex, giving the desired result.

We apply Lemma 6.4.6 to obtain a closed set of vertices in which every color class contains at most 3ν vertices. Let $\{x_1, \ldots, x_t\}$ be a collection of $\Theta(\rho/\nu)$ uniquely colored vertices. For $1 \leq i \leq t$, let A_i be the set of vertices in $G(x_i)$ which are not adjacent to any of the vertex x_j for $j \neq i$, so $A_i = G(x) \setminus \bigcup_{j \neq i} G(x_j)$. We observe that each set A_i is closed and has size $\Omega(\rho)$. Then by a vertex expansion lemma of the previous section, it follows that $|G(A_i)| = \Omega(v)$, so a random vertex has a neighbor in A_i with positive probability. Hence, there are $\Omega(v)$ vertices with neighbors in $\Omega(\rho/\nu)$ of the sets A_i. Let B be the set of such vertices. We observe that for every $x \in B$, there are at most 3ν vertices y such that $G(x) \triangle G(y)$ fails to intersect $\Omega(\rho/\nu)$ of the sets A_i (Lemma 6.4.16). Hence, by applying Lemma 6.4.6, we ensure that each $x \in B$ gets a different color from all but 3ν other vertices. In particular, we achieve our second goal, a closed set of vertices in which every color class contains at most 3ν vertices.

Completing the proof is now relatively simple. Our next goal is to obtain $\Omega(v)$ uniquely colored vertices. Let C be the set of vertices with $\Omega(\rho)$ in the set B of the previous paragraph. Then $|C| = \Omega(v)$, and every pair of distinct vertices $x, y \in C$ has $|(G(x) \triangle G(y)) \cap B| = \Omega(\rho)$. Since we have ensured that color classes in B have size $O(\nu)$, it follows that $G(x) \triangle G(y)$ intersects $\Omega(\rho/\nu)$ color classes, and hence, by applying Lemma 6.4.6, we give different colors to every pair of vertices in C.

Having obtained $\Omega(v)$ uniquely colored vertices via the previous two stages is then enough to give every vertex a unique color without additional individualization.

Throughout this section, we crucially rely on the vertex expansion of strongly regular graphs. In particular, we frequently rely on the fact that sets A of size $o(\rho/\nu)$ have neighbor-

hoods of size $\sim \rho|A|$, and most vertices in $G(A)$ have a unique neighbor in A (Lemma 6.4.7).

6.4.2 Pairwise Subregular Graphs

Most of our lemmas apply to a class of graphs broader than strongly regular graphs. In particular, every result in the present section applies more generally to graphs satisfying the following condition.

Definition 6.4.3. Given integers v, ν, ρ with $\nu < \rho$, a *pairwise subregular graph* $\mathrm{SR}(v, \rho, \nu)$ is a ρ-regular graph on v vertices such no two vertices have more than ν common neighbors.

In particular, by Proposition 6.1.3, every $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph is a $\mathrm{SR}(v, \rho, (3/4)\rho)$ graph. The following observation is implicit in [Bab80b].

Observation 6.4.4. *Naive refinement is $O(v \log v/(\rho - \nu))$-effective for $\mathrm{SR}(v, \rho, \nu)$ graphs.*

One of the main results of this section, Lemma 6.4.5, shows that by individualizing ν/ρ-times fewer vertices and naively refining, we already obtain a large number of uniquely colored vertices.

Lemma 6.4.5. *Let G be a $\mathrm{SR}(v, \rho, \nu)$ graph. Then there is a set of $O\left(\dfrac{\nu v \log^2 v}{\rho(\rho - \nu)}\right)$ vertices such that after individualizing these, there are $\Omega(\rho/\nu)$ uniquely colored vertices in the stable refinement.*

We will prove Lemma 6.4.5 in Section 6.4.2.

We say that the set $W \subseteq V$ *distinguishes* the vertices x and y with respect to the canonical refinement operator $\mathcal{R}$ if after individualization of all vertices in W, x and y receive different colors in the $\mathcal{R}$-stable refinement.

Lemma 6.4.6 below guarantees the existence of a moderately sized set W that distinguishes all pairs $x, y \in V(G)$ for which $G(x) \triangle G(y)$, the symmetric difference of their neighborhoods, intersects many color classes.

Lemma 6.4.6. *Let G be a $\mathrm{SR}(v, \rho, \nu)$ graph. Let $1 \leq m = O(\rho/\nu)$, let A be a closed set of vertices, and let P be the set of pairs (x, y) of vertices such that $(G(x) \triangle G(y)) \cap A$ intersects at least m color classes. Then there is a set of $O(|G(A)| \log^3 v/(m(\rho - \nu)))$ vertices that distinguishes every pair in P.*

We will prove Lemma 6.4.6 in Section 6.4.2.

Preliminary Estimates for Pairwise Subregular Graphs

Lemma 6.4.7. *Let G be a $\mathrm{SR}(v, \rho, \nu)$ graph. Let $0 < \delta < 1$. Suppose $A \subset V(G)$ has size $|A| \leq \delta\rho/\nu$. Then there are more than $(1-\delta)\rho|A|$ vertices $x \in G(A)$ such that $|G(x) \cap A| = 1$. In particular, $|G(A)| > (1 - \delta)\rho|A|$.*

Proof. The number of edges between A and the set of vertices with at least two neighbors in A is at most $\nu|A|(|A|-1)$. The number of edges between A and $G(A)$ is $\rho|A|$. So the number of neighbors $x \in G(A)$ such that $|G(x) \cap A| = 1$ is at least $\rho|A| - \nu|A|(|A|-1) > (1-\delta)\rho|A|$. □

Lemma 6.4.8. *Let G be a $\mathrm{SR}(v, \rho, \nu)$ graph. Let $0 < \delta < 1$. Suppose $A_1 \cup \cdots \cup A_m = A$ is a partition of a set $A \subseteq V(G)$ into sets A_i of size at most $\delta\rho/\nu$. Let B be a set such that $G(A) \subseteq B \subseteq V(G)$. Choose $x \in B$ at random. Let M be the number of sets A_i such that $|G(x) \cap A_i| = 1$. Then $\mathbb{E}(M) > (1 - \delta)\rho|A|/|B|$.*

Proof. By Lemma 6.4.7,

$$\mathbb{E}_{x \in B}(M) > \sum_{i=1}^{m} \frac{(1-\delta)\rho|A_i|}{|B|} = \frac{(1-\delta)\rho|A|}{|B|}\,. \qquad \square$$

Lemma 6.4.9. *Let G be a $\mathrm{SR}(v, \rho, \nu)$ graph. If $A \subseteq V(G)$ has size $|A| = \Omega(\rho/\nu)$, then $|G(A)| = \Omega(\rho^2/\nu)$. If furthermore $|A| \geq 2$, then $|B| = \Omega(\rho(\rho - \nu)/\nu)$, where $B \subseteq G(A)$ is the set of vertices x such that $G(x) \cap A \subsetneq A$.*

Proof. Indeed, let $r = \min\{\lfloor \rho/\nu \rfloor, |A|\}$, so $r \leq \rho/\nu$ and $r = \Omega(\rho/\nu)$. Then

$$|G(A)| \geq \sum_{i=0}^{r-1} \rho - i\nu > \rho r - \nu r^2/2 \geq \rho r/2 = \Omega(\rho^2/\nu).$$

Furthermore, since $|A| \geq 2$, there are at most ν vertices x such that $G(x) \cap A = A$, so $|B| \geq |G(A)| - \nu$. If $r \leq 2$, then $\rho/\nu = O(r) = O(1)$. Since clearly $|G(A)| \geq \rho$, then $|B| \geq \rho - \nu = \Omega(\rho(\rho - \nu)/\nu)$. Otherwise, $r \geq 3$, and

$$|B| \geq |G(A)| - \nu \geq \rho r/2 - \rho \geq \rho(r/2 - r/3) = \rho r/6 = \Omega(\rho^2/\nu)\,. \qquad \square$$

Obtaining Many Uniquely Colored Vertices

We now prove Lemma 6.4.5. Indeed, Lemma 6.4.5 is immediate from $O((\nu v \log^2 v)/(\rho(\rho-\nu)))$ applications of the following lemma. $\square$

Lemma 6.4.10. *Let G be a $\mathrm{SR}(v, \rho, \nu)$ graph. Let m be the total number of vertex colors in G. There is a vertex such that after individualizing this vertex, one of the following situations occurs:*

(a) the stable refinement has at least $\Omega(\rho(\rho - \nu)m/(\nu v \log v))$ more vertex colors;

(b) there are $\Omega(\rho/\nu)$ uniquely colored vertices in the stable refinement.

We first reduce Lemma 6.4.10 to the problem of adding $\Omega(\rho(\rho-\nu)/(\nu v)) \cdot |\mathcal{C}|$ to the total number of colors after a single individualization, where $\mathcal{C}$ is a collection of nearly uniformly-sized color classes.

Lemma 6.4.11. *Let G be a $\mathrm{SR}(v, \rho, \nu)$ graph. Let $A \subseteq V(G)$ be a closed set, let $\mathcal{C}$ be the collection of color classes in A, and suppose $r \geq 2$ is such that $r \leq |C| \leq 2r$ for each $C \in \mathcal{C}$. There is a vertex such that after individualizing this vertex, one of the following situations occurs:*

(a) the stable refinement has at least $\Omega(\rho(\rho-\nu)|\mathcal{C}|/(\nu v))$ *more vertex colors;*

(b) there are $\Omega(\rho/\nu)$ *uniquely colored vertices in the refinement.*

Proof of Lemma 6.4.10 from Lemma 6.4.11. Let G by a $\mathrm{SR}(v,\rho,\nu)$ graph and let m be the total number of vertex colors in G. Let s be the number of uniquely colored vertices in G. Let c be the constant hidden by the Ω in situation (b) of Lemma 6.4.11; so in situation (b) of Lemma 6.4.11, we are guaranteed $\geq c\rho/\nu$ uniquely colored vertices. Without loss of generality, assume $c \leq 1/2$.

We must show that unless $s \geq c\rho/\nu$, there is some set $\mathcal{C}$ of color classes and some number $r \geq 2$ such that $r \leq |C| \leq 2r$ for each $C \in \mathcal{C}$, and $|\mathcal{C}| = \Omega(m/\log v)$. There are $m-s$ color classes of size ≥ 2, so by the pigeonhole principle there is some $r \geq 2$ such that $r \leq |C| \leq 2r$ for at least $(m-s)/\log v$ color classes C. In particular, it suffices to show that either $s \geq c\rho/\nu$ or $s \leq m/2$.

Let U be the collection of uniquely colored vertices, so $s = |U|$, and suppose $s < c\rho/\nu$. For $x \in U$, let N_x be the set of neighbors of x which are neither in U nor adjacent to any vertex in $U \setminus \{x\}$, i.e., $N_x = G(x) \setminus (U \cup G(U \setminus \{x\}))$. Since every pair of distinct vertices $x, y \in U$ has at most ν common neighbors, for every $x \in U$ we have

$$|N_x| \geq \rho - |U| - \nu(|U|-1) \geq \rho - c\rho \geq (1/2)\rho.$$

In particular, N_x is nonempty. Since $G(y)$ is a closed set for every $y \in U$ and since U is a closed set, also N_x is a closed set. Moreover, by definition, N_x contains no uniquely colored vertices. So each set N_x contains at least one color class not in U, and since the sets N_x are disjoint, there exist at least s color classes other than those in U. So $s \leq m/2$, as claimed. □

The following two lemmas each cover a distinct case in the proof of Lemma 6.4.11.

Lemma 6.4.12. *Let G be a $\mathrm{SR}(v,\rho,\nu)$ graph. Let $A \subseteq V(G)$ be a closed set that does not*

contain a uniquely colored vertex. Suppose A is partitioned into closed sets $A_1, \dots, A_m$ of size $|A_i| \geq \Omega(\rho/\nu)$ for all $1 \leq i \leq m$. Then there is a vertex $x \in G(A)$ such that after individualizing x, the stable refinement has at least $\Omega(\rho(\rho-\nu)m/(\nu|G(A)|))$ more vertex color classes in A.

Proof. Let x be a random vertex in $G(A)$. For $1 \leq i \leq m$ let M_i be the number of color classes $C \subseteq A_i$ such that $G(x) \cap C$ is a nonempty strict subset of C. Fix $1 \leq i \leq m$. We claim that $\mathbb{E}(M_i) = \Omega(\rho(\rho-\nu)/(\nu|G(A)|))$. We consider two cases.

Case 1: There is a color class $C \subseteq A_i$ of size at least $(1/2)\rho/\nu$. By Lemma 6.4.9, the set B of vertices $y \in G(C)$ satisfying $G(y) \cap C \subsetneq C$ has size $|B| = \Omega(\rho(\rho-\nu)/\nu)$. Hence, $x \in B$ with probability $\Omega(\rho(\rho-\nu)/(\nu|G(A)|))$, and whenever $x \in B$ the set $G(x) \cap C$ is a nonempty strict subset of C.

Case 2: Every color class $C \subseteq A_i$ has size less than $(1/2)\rho/\nu$. If $|G(x) \cap C| = 1$ for some color class $C \subseteq A_i$, then $G(x) \cap C$ is a nonempty strict subset of C, since $|C| \geq 2$ by hypothesis. By applying Lemma 6.4.8 to the partition of A_i into color classes (with $B = G(A) \supseteq G(A_i)$), we therefore estimate $\mathbb{E}(M_i) \geq (1/2)\rho|A_i|/|G(A)| = \Omega(\rho^2/(\nu|G(A)|))$.

In both cases, $\mathbb{E}(M_i) = \Omega(\rho(\rho-\nu)/(\nu|G(A)|))$.

Now let M be the number of color classes $C \subseteq A$ such that $G(x) \cap C$ is a nonempty strict subset of C, where again x is a random vertex in $G(A)$. So, $M = \sum_{i=1}^{m} M_i$, and hence $\mathbb{E}(M) = \Omega(\rho(\rho-\nu)m/(\nu|G(A)|))$. Thus, there is some vertex $x \in G(A)$ such that for $\Omega(\rho(\rho-\nu)m/(\nu|G(A)|))$ color classes $C \subseteq A$, the set $G(x) \cap C$ is a nonempty strict subset of C. After individualizing x, each such color class C is split into two disjoint closed sets in the stable refinement, namely $C \cap G(x)$ and $C \setminus G(x)$, giving the desired result. □

Lemma 6.4.13. *Let G be a $\mathrm{SR}(v, \rho, \nu)$ graph. Let $0 < \varepsilon, \delta < 1$ and $m > 0$. Let $A \subseteq V(G)$ be a closed set. Suppose that for every color class $C \subseteq A$, we have*

(1) $2 \leq |C| \leq \varepsilon(\rho/\nu)$

and furthermore, there exists a closed subset $S_C \subseteq G(C)$ satisfying the following:

(2) if $y \in S_C$ then $|G(y) \cap C| = 1$;

(3) $|S_C| \geq \delta\rho|C|$;

(4) every color class in S_C has size $\leq m|C|$.

Then there is a vertex x such that individualizing x, either

(a) the stable refinement has at least $(\delta/2)(\rho/\nu)$ uniquely colored vertices in total, or

(b) the stable refinement has at least $(\delta/4)(1-\varepsilon)\rho^2|A|/(m|G(A)|)$ more vertex colors.

Proof. Let $\mathcal{C}$ be the collection of color classes in A. Using assumption (1), we apply Lemma 6.4.8 to the partition of A into color classes (with $B = G(A)$). It follows that there is a vertex $x \in G(A)$ and color classes $C_1, \ldots, C_t \in \mathcal{C}$ with $t > (1-\varepsilon)\rho|A|/|G(A)|$ such that $|G(x) \cap C_i| = 1$ for all $1 \leq i \leq t$. Let x_i denote the unique vertex in $G(x) \cap C_i$ and let $S_i = S_{C_i}$ for all $1 \leq i \leq t$. Note that each x_i becomes uniquely colored if we individualize x and refine. Hence, if $t > (\delta/2)(\rho/\nu)$, we have already achieved outcome (a).

Otherwise, when $t \leq (\delta/2)(\rho/\nu)$, we continue to analyze the original coloring. Fix $1 \leq i \leq t$ and a color class $D \subseteq S_i$. Consider the bipartite graph induced between C_i and D. Since C_i and D are color classes, the graph is biregular, and by assumption (2), every vertex $y \in D$ has exactly one neighbor in C_i. Hence, $|G(x_i) \cap D| = |D|/|C_i|$, and since $|C_i| \geq 2$, in particular $G(x_i) \cap D$ is a nonempty strict subset of D. It follows that if we individualize x and refine then $D \cap G(x_i)$ and $D \setminus G(x_i)$ become nonempty closed sets.

Let $T_i = (S_i \cap G(x_i)) \setminus \bigcup_{j \neq i} G(x_j)$. Note that since each of the sets $G(x_j)$ for $1 \leq j \leq t$ become closed sets after individualizing x and refining, then also T_i becomes a closed set after individualizing x and refining. We estimate the number of color classes D in the original coloring which intersect T_i. We have

$$|S_i \cap G(x_i)| = \sum_{D \subseteq S_i} |G(x_i) \cap D| = \sum_{D \subseteq S_i} |D|/|C_i| = |S_i|/|C_i| \geq \delta\rho,$$

where the sums are over color classes, and the last inequality comes from assumption (3). Furthermore, since $G(x_i) \cap G(x_j) \leq \nu$ for all $j \neq i$, we have

$$\left| \bigcup_{j \neq i} G(x_i) \cap G(x_j) \right| \leq (t-1)\nu < (\delta/2)\rho$$

Hence, $|T_i| \geq \delta\rho - (\delta/2)\rho = (\delta/2)\rho$. Furthermore, for every color class $D \subseteq S_i$, we have $|G(x_i) \cap D| = |D|/|C_i| \leq m$ by assumption (4). So, there are at least $(\delta/2)(\rho/m)$ color classes D such that $D \cap T_i \neq \emptyset$.

The number M of pairs (i, D) such that $1 \leq i \leq t$ and such that D is a color class which intersects T_i is therefore at least $(\delta/2)(t\rho/m)$. We compare M to the number of additional color classes added after individualizing x and refining to the stable coloring. For $1 \leq \ell \leq t$, let $\mathcal{D}_\ell$ be the collection of color classes D which intersect exactly ℓ of the sets T_i. So, $M = \sum_{\ell=1}^{t} \ell|\mathcal{D}_\ell|$. Observe that if a color class D intersects some set T_i, then $T_i \cap D$ is a nonempty closed set in the stable refinement, as is $D \setminus T_i$, since $T_i \subseteq G(x_i)$ is a closed set in the stable refinement. In particular, every $D \in \mathcal{D}_1$ is split into at least two color classes in the stable refinement. Furthermore, since the sets T_i are disjoint, every $D \in \mathcal{D}_\ell$ is split into at least ℓ color classes. In particular, the number of *additional* color classes is at least

$$|\mathcal{D}_1| + \sum_{\ell \geq 2} (\ell - 1)|\mathcal{D}_\ell| \geq M/2 = (\delta/4)(t\rho/m) \geq (\delta/4)(1-\varepsilon)\rho^2|A|/(m|G(A)|). \qquad \square$$

Finally, we complete the proof of Lemma 6.4.11.

Proof of Lemma 6.4.11. Case 1: $r \geq (1/4)(\rho/\nu)$. By applying Lemma 6.4.12 to the partition of A into color classes, and using the trivial bound $|G(A)| \leq n$, it follows that we can individualize a single vertex so that the total number of colors in the refinement increases by at least $\Omega(\rho(\rho - \nu)|\mathcal{C}|/(\nu v))$.

Case 2: $r < (1/4)(\rho/\nu)$. For each $C \in \mathcal{C}$, define U_C to be the set of neighbors of C which are not neighbors of any other $C' \in \mathcal{C}$, i.e., $U_C = G(C) \setminus \bigcup_{C \neq C' \in \mathcal{C}} G(C')$. Since every $C' \in \mathcal{C}$

is a color class, every set $G(C')$ for $C' \in \mathcal{C}$ is a closed set, and so U_C is a closed set. We consider two subcases.

Case 2a: There is a subset $\mathcal{D} \subseteq \mathcal{C}$ with $|\mathcal{D}| \geq |\mathcal{C}|/2$, and $|U_D| \geq |G(D)|/4$ for all $D \in \mathcal{D}$. For every $D \in \mathcal{D}$, since $|D| \leq 2r \leq (1/2)(\rho/\nu)$ by assumption, it follows by Lemma 6.4.7 that $|G(D)| \geq (1/2)\rho|D|$. For every $D \in \mathcal{D}$, we have $|U_D| \geq (1/4)|G(D)| \geq (1/8)\rho|D|$. Since $|\mathcal{D}| \geq |\mathcal{C} \setminus \mathcal{D}|$ and every $C \in \mathcal{C}$ satisfies $r \leq |C| \leq 2r$, we have $\sum_{D\in\mathcal{D}} 2|D| \geq \sum_{C\in\mathcal{C}\setminus\mathcal{D}} |C|$. Therefore,

$$3\sum_{D\in\mathcal{D}} |D| \geq \sum_{C\in\mathcal{D}} |C| + \sum_{C\in\mathcal{C}\setminus\mathcal{D}} |C| = |A|.$$

Let $U = \bigcup_{D\in\mathcal{D}} U_D$. Since the sets U_D are disjoint by construction, then

$$|U| \geq \left|\bigcup_{D\in\mathcal{D}} U_D\right| \geq \sum_{D\in\mathcal{D}} (1/8)\rho|D| \geq (1/24)\rho|A| = \Omega(\rho r|\mathcal{D}|).$$

Now if $\geq (1/48)\rho|A| = \Omega(\rho/\nu)$ vertices in G are uniquely colored, then we have already achieved outcome (b). So, we may assume that $< (1/48)\rho|A|$ vertices in G are uniquely colored. In particular, at most $|U|/2$ vertices are uniquely colored. For $D \in \mathcal{D}$, let $W_D \subseteq U_D$ be the set of vertices in U_D which are not uniquely colored, so $\sum_{D\in\mathcal{D}} |W_D| \geq |U|/2$. Hence, for random $D \in \mathcal{D}$, we have $\mathbb{E}(|W_D|) \geq |U|/(2|\mathcal{D}|) = \Omega(\rho r)$. Furthermore, for every $D \in \mathcal{D}$, we have $|W_D| \leq |G(D)| \leq \rho|D| = O(\rho r)$. Hence, by Fact 4.2.11, for a constant fraction of the sets $D \in \mathcal{D}$, we have $|W_D| = \Omega(\rho r)$.

We apply Lemma 6.4.12 to the union of those sets W_D having size $\Omega(\rho r) = \Omega(\rho/\nu)$; so again we can individualize a single vertex so that the total number of colors in the stable refinement increases by at least $\Omega(\rho(\rho-\nu)|\mathcal{D}|/(\nu v)) = \Omega(\rho(\rho-\nu)|\mathcal{C}|/(\nu v))$.

Case 2b: There is a subset $\mathcal{D} \subseteq \mathcal{C}$ with $|\mathcal{D}| > |\mathcal{C}|/2$, and $|U_D| < |G(D)|/4$ for all $D \in \mathcal{D}$.

For $D \in \mathcal{D}$, we have $|U_D| < |G(D)|/4 \leq \rho|D|/4$. Let S_D be the set of vertices $x \in G(D) \setminus U_D$ such that $|G(x) \cap D| = 1$. Again, for every $D \in \mathcal{D}$, since $|D| \leq 2r \leq (1/2)(\rho/\nu)$ by assumption, it follows by Lemma 6.4.7 that $|S_D| \geq (1/2)\rho|D| - |U_D| > (1/4)\rho|D|$. Let

$x \in S_D \subseteq G(D) \setminus U_D$. By the definition of U_D, there is some $C \in \mathcal{C}$ with $C \neq D$ such that $x \in G(C)$. Since C and D are color classes, then every vertex y with the same color as x also has a neighbor in C and in D. Counting the triples (a, b, y) with $a \in C$, $b \in D$ and $y \in G(u) \cap G(v)$, it follows that there are $\leq |C||D|\nu \leq 2r\nu|D|$ such vertices $y \in G(C) \cap G(D)$, so the color class containing x has size $\leq 2r\nu|D|$. Now consider the set $A' = \bigcup_{D \in \mathcal{D}} |D|$. So A', along with the closed subsets $S_D \subseteq G(D)$ for color classes $D \subseteq A'$, satisfies the conditions of Lemma 6.4.13, with values $\varepsilon = 1/2$, $\delta = 1/4$, and $m = 2r\nu$. Therefore, by Lemma 6.4.13, after individualizing a single vertex, either the stable refinement has $\Omega(\rho/\nu)$ uniquely colored vertices, or refinement adds at least $\Omega(\rho^2|A'|/(r\nu|G(A')|))$ to the total number of colors. This proves the lemma, since $|A'|/r = \Omega(|\mathcal{C}|)$ and $|G(A')| \leq v$. □

Distinguishing Pairs of Vertices

We prove Lemma 6.4.6 via the following two lemmas.

Lemma 6.4.14. *Let G be a $\mathrm{SR}(v, \rho, \nu)$ graph. Let $A_1, \ldots, A_m$ be disjoint subsets of a set $A \subseteq V(G)$ such that $|A_i| = \Omega(\rho/\nu)$ and $|A_i| \geq 2$ for all $1 \leq i \leq m$. Let B be a set such that $G(A) \subseteq B \subseteq V(G)$. For any $\delta > 0$, there is some $t = O(|B|\nu \log(m/\delta)/(\rho(\rho - \nu)))$ such that if $x_1, \ldots, x_t$ is a random sequence of vertices in B then*

$$P\left[(\forall i)(\exists j)\left(1 \leq |A_i \cap G(x_j)| < |A_i|\right)\right] \geq 1 - \delta\,.$$

Proof. Fix $1 \leq i \leq m$. Let B_i be the collection of vertices $x \in G(A_i)$ such that $G(x) \cap A_i \subsetneq A_i$. By Lemma 6.4.9, we have $|B_i| \geq \Omega(\rho(\rho - \nu)/\nu)$. So if x is a random vertex in B, we have $x \in B_i$ with probability $\Omega(\rho(\rho - \nu)/(\nu|B|))$.

Thus, if $x_1, \ldots, x_t \in B$ is a random sequence of vertices, then we have

$$P\left[(\forall j)\left(x_j \notin B_i\right)\right] \leq (1 - \Omega(\rho(\rho - \nu)/(\nu|B|)))^t\,.$$

Then by the union bound,

$$P\left[(\exists i)(\forall j)\left(x_j \notin B_i\right)\right] \leq m\left(1-\Omega(\rho(\rho-\nu)/(\nu|B|))\right)^t.$$

For some $t = O(|B|\nu\log(m/\delta)/(\rho(\rho-\nu)))$, this probability is at most δ. □

Lemma 6.4.15. *Let G be a $\mathrm{SR}(v,\rho,\nu)$ graph. Let $A \subseteq V(G)$ be a closed set. Suppose $x, y \in V(G)$ are such that $G(x) \setminus G(y)$ intersects A in at least m different color classes. Let B be a set such that $G(A) \subseteq B \subseteq V(G)$. Then a set of $O(|B|\log^2 v/((\rho-\nu)\min\{m,\rho/\nu\}))$ random vertices in B distinguish x and y with probability $\Omega(1)$.*

Proof. By possibly passing to a subset of A, excluding some of its color classes, we may assume $m \leq \rho/\nu$. Let $A_1 \cup \cdots \cup A_m$ be the partition of $G(x)\triangle G(y)$ induced by the coloring. Suppose z is a vertex such that $1 \leq |G(z)\cap A_i| < |A_i|$ for some $1 \leq i \leq m$. Then either $1 \leq |G(z)\cap A_i| \leq |A_i|/2$ or $1 \leq |A_i \setminus G(z)| \leq |A_i|/2$. Hence, after individualizing z and refining, there is a non-empty subset A_i' of A_i of size $\leq |A_i|/2$ such that A_i' is the intersection of $G(x)\triangle G(y)$ with a color class.

We apply Lemma 6.4.14 with $\delta = 1-(1/2)^{1/\log v}$ to those sets A_i such that $|A_i| \geq (1/4)\rho/\nu$. It follows that if we select $s = O(|B|\nu\log v/(\rho(\rho-\nu))) = O(|B|\log v/((\rho-\nu)m))$ random vertices $z_1,\ldots,z_s \in B$, then with probability at least $(1/2)^{1/\log v}$, for every $1 \leq i \leq m$ either $|A_i| < (1/4)\rho/\nu$, or after individualizing each vertex z_i and refining, there is some nonempty subset A_i' of A_i of size $\leq |A_i|/2$ such that A_i' is the intersection of $G(x)\triangle G(y)$ with a color class. Hence, by applying Lemma 6.4.14 at most $O(\log n)$ times, we see that after individualizing a set Z of $O(|B|\log^2 v/((\rho-\nu)m))$ random vertices and refining, then with probability $\Omega(1)$, for every $1 \leq i \leq m$ there is a nonempty subset A_i' of A_i of size $< (1/4)\rho/\nu$ such that A_i' is the intersection of $G(x)\triangle G(y)$ with a color class. Suppose now that this event occurs.

Let $A' = \bigcup_{i=1}^m A_i'$ and note that $|A'| \geq m$. While $|A'| > (1/2)\rho/\nu$, we pass to a smaller subset of A' by excluding, arbitrarily, a set A_i'. Since each excluded set A_i' has size

$< (1/4)\rho/\nu$, we ensure that if any sets A'_i are excluded, we still have $|A'| > (1/4)\rho/\nu$, in which case $4|A'| > m$ by supposition. In any case, by excluding sets A'_i if necessary, we may assume $m = O(|A'|)$ and $|A'| \leq (1/2)\rho/\nu$. Then by Lemma 6.4.7, there are $\Omega(\rho|A'|) = \Omega(\rho m)$ neighbors z of A' such that $|G(z) \cap A'| = 1$. Therefore, if $z \in B$ is a random vertex, then with probability $\Omega(\rho m/|G(A)|)$, there is some $1 \leq i \leq m$ such that $|G(z) \cap A'_i| = 1$. Hence, if Z' is a set of $O(|B|/(\rho m))$ random vertices in B, then with probability $\Omega(1)$, there is some $z \in Z'$ and some $1 \leq i \leq m$ such that $|G(z) \cap A'_i| = 1$. After individualizing each vertex in Z' and refining, $G(z) \cap A'_i$ is the intersection of $G(x) \triangle G(y)$ with a closed set. But since $G(z) \cap A'_i$ contains only a single vertex, it is either a subset of $G(x) \setminus G(y)$ or of $G(y) \setminus G(x)$; in either case, x and y are distinguished. □

Proof of Lemma 6.4.6. Fix $(x, y) \in P$. Let $t = |G(A)| \log^2 v/((\rho - \nu)m)$. By Lemma 6.4.15, $O(t)$ random vertices distinguish x and y with probability $\Omega(1)$. Therefore, individualizing $O(t \log v)$ random vertices distinguishes *every* such pair in P with positive probability. □

We conclude this section with the following lemma, which will allow us to show that many pairs of vertices satisfy the hypotheses of Lemma 6.4.6.

Lemma 6.4.16. *Let G be a $\mathrm{SR}(v, \rho, \nu)$ graph. Let $x \in V(G)$ and let $C_1, \ldots, C_t$ be a collection of color classes which each intersect $G(x)$. Suppose further that $|G(x) \cap \bigcup_i C_i| \geq 2$. Then there are $\leq 3\nu$ vertices y such that $G(x) \triangle G(y)$ intersects $\leq (1/3)t$ of the color classes C_i.*

Proof. Suppose first that $t = 1$. Since $|G(x) \cap C_1| \geq 2$, let $w, z \in G(x) \cap C_1$ be distinct vertices. There are at most ν vertices y such that $y \in G(w) \cap G(z)$, so there are at most ν vertices y such that $C_1 \subseteq G(x) \cap G(y)$.

Now suppose $t \geq 1$. Choose vertices $z_1, \ldots, z_t$ with $z_i \in G(x) \cap C_i$ for all $1 \leq i \leq t$. If $t = 2$, there are at most ν vertices y such that $z_1, z_2 \in G(x) \cap G(y)$, so there are at most ν vertices y such that $G(x) \triangle G(y)$ contains neither z_1 nor z_2. So suppose $t \geq 3$.

There are $\leq t(t-1)\nu$ ordered triples (i, j, y) such that $i \neq j$ and y is a vertex such that $z_i, z_j \in G(y)$. On the other hand, suppose y is such that $G(x) \triangle G(y)$ intersects at most

$(1/3)t$ of the sets C_i. Then there are at least $(2/3)t((2/3)t-1)$ ordered pairs i, j with $i \neq j$ such $z_i, z_j \in G(y)$. Hence, there are at most

$$\frac{t(t-1)\nu}{(2/3)t((2/3)t-1)} \leq 3\nu$$

such vertices y. □

6.4.3 Discretely Coloring a Strongly Regular Graph

We again require that G be strongly regular; for the proofs in this section, it no longer suffices that G is pairwise subregular. Recall, however, our notation $\nu = \max\{\lambda, \mu\}$, so $\mathrm{SR}(v, \rho, \lambda, \mu)$ graphs are still $\mathrm{SR}(v, \rho, \nu)$.

Lemma 6.4.17. *Let G be a $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph satisfying $\nu = o(\rho)$. If there are $\Omega(\rho/\nu)$ uniquely-colored vertices in G, then after individualizing some $O(\nu v \log^3 v/\rho^2)$ vertices, in the stable refinement there is a closed set $A \subseteq V(G)$ of size $|A| = \Omega(v)$ such that every color class $C \subseteq A$ satisfies $|C| \leq 3\nu + 1$.*

Proof. Let $x_1, \ldots, x_m$ be distinct uniquely colored vertices with $m = \Omega(\rho/\nu)$ and $m \leq (1/2)\rho/\nu$. Define $N_i = G(x_i) \setminus \bigcup_{j \leq i} G(x_j)$ for $1 \leq i \leq m$, so the N_i are pairwise-disjoint closed sets. Furthermore, since $|G(x_i) \cap G(x_j)| \leq \nu$ for $i \neq j$, we have $|N_i| \geq \rho - \nu(m-1) > (1/2)\rho$ for $1 \leq i \leq m$. Therefore, by Lemma 2.8.1, $|G(N_i)| \gtrsim (\rho/\mu)|N_i| \gtrsim (1/2)v$.

For $x \in V$ a random vertex, let $S(x)$ denote the number of sets N_i such that $x \in G(N_i)$ for $1 \leq i \leq m$. We have

$$\mathbb{E}_{x \in V}(S(x)) \geq \sum_{i=1}^{m} P[x \in G(N_i)] \gtrsim (1/2)m.$$

Since $S(x) \leq m$, it follows by Fact 4.2.11 that if A is the collection of vertices x with $S(x) \geq (1/4)m$, then $|A| = \Omega(v)$. We observe that A is a closed set, since the sets N_i are closed sets, and so the set of vertices with any given number of neighbors in any subcollection

of the N_i is again a closed set.

By Lemma 6.4.16, for every $x \in A$, there are at most 3ν vertices y such that $G(x) \triangle G(y)$ intersects fewer than $(1/12)m$ of the sets N_i. By Lemma 6.4.6 there is a set of $O(\nu v \log^3 v/\rho^2)$ vertices such that after individualizing these and refining, no set of more than $3\nu+1$ vertices in A have the same color. In other words, after individualizing these and refining, every color class in A contains $\leq 3\nu + 1$ vertices. □

Lemma 6.4.18. *Let G be a $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph satisfying $\nu = o(\rho)$. If there is a closed set $A \subseteq V(G)$ with $|A| = \Omega(v)$, and every color class $C \subseteq A$ satisfies $|C| \leq 3\nu + 1$, then after individualizing some $O(\nu v \log^3 v/\rho^2)$ vertices, the stable refinement has $\Omega(v)$ uniquely colored vertices.*

Proof. Since $|A| = \Omega(v)$, for a random vertex $x \in V$ we have $\mathbb{E}(|G(x) \cap A|) = \Omega(\rho)$. Let B be the collection of vertices x such that $|G(x) \cap A| = \Omega(\rho)$, so by Fact 4.2.11 we have $|B| = \Omega(v)$. Again, repeating the argument in the proof of Lemma 6.4.17, the set B is closed. Now for any distinct $x, y \in B$, we have $|(G(x) \setminus G(y)) \cap A| \geq \Omega(\rho) - \nu = \Omega(\rho)$. Since every color class in A has size $O(\nu)$, at least $\Omega(\rho/\nu)$ distinct color classes intersect $G(x) \triangle G(y)$. So by Lemma 6.4.6, with B in place of the set A in the Lemma, there is a set of $O(\nu v \log^3 v/\rho^2)$ vertices such that after individualizing these, every pair of distinct vertices in B gets different colors in the refinement. In other words, since B is a closed set, every vertex in B becomes uniquely colored. □

Finally, we ensure G has a discrete coloring.

Lemma 6.4.19. *Let G be a $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph satisfying $\nu = o(\rho)$. If there are $\Omega(v)$ uniquely colored vertices, then for v sufficiently large, the stable refinement is discrete.*

Proof. Let A be the set of vertices with unique colors, and let B be the set of vertices with at least $\nu+1$ neighbors in A. Hence, no two vertices in B have the same set of uniquely colored neighbors, so every vertex in B will get a unique color in the stable refinement. Similarly,

every vertex with at least $\nu + 1$ neighbors in $A \cup B$ will get a unique color in the stable refinement.

Thus, it suffices to show that every vertex $x \notin A \cup B$ has at least $\nu + 2$ neighbors in $A \cup B$ for v sufficiently large. Indeed, if $x \notin B$, then $|A \setminus G(x)| \geq \Omega(n) - \nu = \Omega(n)$. Every vertex in $A \setminus G(x)$ has μ neighbors in $G(x)$, so the number of edges between $G(x)$ and $A \setminus G(x)$ is $\Omega(\mu n) = \Omega(\rho^2)$ by Corollary 6.1.4. Thus, $\mathbb{E}_{y \in G(x)}(|G(y) \cap A|) = \Omega(\rho)$, and since each vertex in $G(x)$ has at most ρ neighbors in A, it follows by Fact 4.2.11 that at least $\Omega(\rho)$ neighbors y of x each have at least $\Omega(\rho)$ neighbors in A. Since $\nu = o(\rho)$, for v sufficiently large, each of these vertices y is in B, and x has more than $\nu + 1$ neighbors in B. □

Proof of Theorem 6.4.1. We have already seen in the discussion following the statement of Theorem 6.4.1 that we may assume $\nu = o(\rho)$. Apply Lemmas 6.4.5, 6.4.17, 6.4.18, and 6.4.19, in that order. □

This completes the proof of Theorem 2.4.2.

6.5 Color-μ-Boundedness of Strongly Regular Graphs

We now prove Theorem 2.4.10.

Theorem 6.5.1. *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph, not isomorphic to $T(n)$ or $L_2(n)$ for any n. After individualizing some $O(\log v)$ vertices, the WL-stable refinement is color-μ-bounded.*

Theorem 2.4.10 follows immediately, in view of Proposition 3.3.1. □

6.5.1 Reduction to the Case $\rho = o(v)$

For nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graphs with $\rho = \Omega(v)$, Theorem 6.4.2 gives the stronger result that naive refinement is $O(\log v)$-effective.

We now show that even if $\rho/v \to 0$ slowly, after individualizing some $O(\log v)$ vertices, the naive-stable refinement is color-μ-bounded. This is a corollary to the main technical result of [Bab80b] which we now state.

Lemma 6.5.2 ([Bab80b])**.** *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph. For vertices x, y, let $D(x, y)$ be the set of those vertices z that are adjacent to exactly one of x and y. Then, for all $x \neq y$,*

$$|D(x, y)| \geq \rho/2. \tag{6.4}$$

Corollary 6.5.3. *If G is a non-trivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph, then after the individualization of some $O((v/\rho)\log(v/\rho))$ vertices all color classes in the naive-stable refinement will have size $\leq \mu$.*

Note that the conclusion is much stronger than color-μ-boundedness.

Proof of Corollary 6.5.3. Following [Bab80b], we say that vertex z *distinguishes* vertices x and y if $z \in D(x, y)$. If this is the case and we individualize z then after naive refinement, x and y get different colors. Let us individualize a random sequence $z_1, \ldots, z_t$ of vertices. By Lemma 6.5.2, the probability that vertices x and y are not distinguished by any of the z_i is $\leq (1 - \rho/(2v))^t < \exp(-\rho t/(2v))$. Let N denote the number of pairs of vertices that are not distinguished. Then $E(N) \leq \binom{v}{2} \exp(-\rho t/(2v))$. It follows that there is a choice of the z_i for which $N \leq \binom{v}{2} \exp(-\rho t/(2v))$. If this number is less than $\binom{\mu+1}{2}$ then after naive refinement, each vertex color occurs at most μ times. Setting $t \geq (4v/\rho)\ln(v/\mu)$ suffices for this. In view of Corollary 6.1.4 we have $v/\mu < ((2v/\rho)^2)$, so $t \geq (8v/\rho)(\ln(2v/\rho))$ suffices. □

6.5.2 Generating a Graph μ Vertices at a Time

Let S be a set of vertices. We define $N_2(S)$ to be the set of common neighbors of non-adjacent pairs in S, i.e.,

$$N_2(S) = \{z \in V(G) : \ \exists x, y \in S \text{ s. t. } x \neq y,\ x \not\sim y, \text{ and } z \in G(x) \cap G(y)\}$$

We define $\widehat{S} = S \cup N_2(S)$, and we define $\overline{S}$ to be the smallest set A containing S such that $\widehat{A} = A$. In other words,

$$\overline{S} = \bigcap_{\substack{A \supseteq S \\ \widehat{A} = A}} A\,.$$

We say S *generates* the set A if $A \subseteq \overline{S}$.

We show that there exists a small set S of vertices such that S generates all of V.

Lemma 6.5.4. *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph such that $\lambda = o(\rho)$ and $\rho = o(v)$. There exists a set $S \subseteq V(G)$ with $|S| = O(\log v)$ such that $\overline{S} = V(G)$.*

We will show how Theorem 6.5.1 follows from Lemma 6.5.4 after we prove the following elementary observation.

Proposition 6.5.5. *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph. Let S be a closed set in the WL-stable refinement. Then $N_2(S)$ is also a closed set.*

Proof. Let $x \in V(G)$. Because of the WL-stability, encoded in the color of x is the number of triples (x, y, z) of vertices such that $y \not\sim z$ and $x \sim y$ and $x \sim z$ where $y, z \in S$. Note that $x \in N_2(S)$ if and only if this count is positive. Therefore $N_2(S)$ is a closed set in the WL-stable refinement. □

Proof of Theorem 6.5.1 from Lemma 6.5.4. By Corollary 6.5.3, if $\rho \geq v/\sqrt{\log v}$, then after individualizing $O(\sqrt{\log v} \log\log v)$ vertices, every color class in the naive-stable refinement will have size at most μ. Hence, we may assume $\rho = o(v)$. Now if G is the line-graph of a nontrivial Steiner design or nontrivial transversal design, then the combination of Proposition 6.1.6 with Theorems 4.2.1 and 6.2.1 shows that unless G satisfies Neumaier's claw bound, naive refinement is $O(\log v)$-effective. (The case of a trivial Steiner or transversal design corresponds to a triangular or lattice graph.) Hence, by Theorem 6.1.5, we may assume G satisfies Neumaier's claw bound. Therefore, by Corollary 6.1.10, we have $\lambda = o(\rho)$.

Observe that by construction, for any set $T \subseteq V(G)$, each vertex in $N_2(T)$ has a pair of nonadjacent neighbors in T. Therefore, no set of $\mu + 1$ vertices in $N_2(T)$ can have the same

set of neighbors in T. Furthermore, if T is a closed set in the vertex-colored graph G, then so is $N_2(T)$ by Proposition 6.5.5.

By Lemma 6.5.4, there is some set $S \subseteq V(G)$ with $|S| = O(\log v)$ such that $\overline{S} = V(G)$. After individualizing S, we order the color classes of the WL-stable refinement as follows. The first color classes are all the uniquely colored vertices, including all the vertices of S. Then, when the color classes in a set T have all been added to the ordering, we add all the color classes in $N_2(T) \setminus T$ in any order. The graph is thus color-μ-bounded. □

We outline the proof of Lemma 6.5.4 before proceeding. We will analyze sets of the form

$$A + y := G(A \setminus G^+(y)) \cap G(y) \tag{6.5}$$

where $A \subseteq V(G)$ and $y \in V(G)$. Note that $A + y \subseteq \widehat{A \cup \{y\}}$, since if $x \in A + y$ then $x \sim y$ and $x \sim a$ for some $a \in A \setminus G^+(y)$. Furthermore, $A + y \subseteq G(y)$.

We will prove Lemma 6.5.4 in three stages.

In the first and most complex stage we iteratively construct sets S_i so that $\overline{S_i}$ grows larger and larger. At the i-th step, we define S_{i+1} by adding a few carefully chosen vertices to S_i. To measure the growth of $\overline{S_i}$, we find a sequence of vertices $z_1, z_2, \ldots$ and a constant $c > 0$ so that $|\overline{S_{i+1}} \cap G(z_{i+1})| \geq (1+c)|\overline{S_i} \cap G(z_i)|$. We finish this first stage after $O(\log v)$ iterations, when we have found a set S of size $O(\log v)$ and a vertex x so that $|\overline{S} \cap G(x)| = \Omega(\rho)$.

The key to our analysis of this first stage is the pair of vertex expansion lemmas proved in Section 6.3, which we use to estimate the size of $G(A)$, where $A = \overline{S_i}) \cap G(z_i)$.

In particular, Lemma 2.8.2 entails that $|G(A)| \gtrsim 2(\rho/\mu)|A|$, assuming $|A| = o(\rho)$ and $\mu = \omega(1)$. We further estimate that for a random vertex $y \in V(G)$, we have $\mathbb{E}_y(|A + y|) \gtrsim (\mu/\rho)|N(A)|$ (Lemma 6.5.10). Putting these two estimates together, we find that $\mathbb{E}_y(|A + y|) \gtrsim 2|A|$, and so for some vertex $y \in V(G)$, we have

$$|\overline{S_i \cup \{y\}} \cap G(y)| \gtrsim 2|\overline{S_i} \cap G(z_i)|$$

We then set $S_{i+1} = S_i \cup \{y\}$ and $z_{i+1} = y$. Iterating this process completes the first stage of the proof in the case that μ is unbounded.

When μ is bounded, the vertex expansion estimate of Lemma 2.8.2 becomes ineffective, and we instead rely on Lemma 2.8.1, which entails that $|G(A)| \gtrsim (\rho/\mu)|A|$. So, again using Lemma 6.5.10, we find a vertex y such that $|A + y| \gtrsim |A|$. By carefully estimating the edge density between A and $A + y$, we are then able to estimate the size of $G(B)$, where $B = A \cup (A + y)$. Our estimate for $|G(B)|$ allows us to again apply Lemma 6.5.10 to find a vertex z such that $|B + z| \gtrsim (1 + c)|B|$ for some constant c. Now we set $S_{i+1} = S_i \cup \{y, z\}$ and $z_{i+1} = z$. Iterating this process completes the first stage of the proof in the case that μ is bounded.

So, by applying the entire first stage twice, we find a set S of size $|S| = O(\log v)$ and two distinct vertices $x, x' \in V(G)$ such that $|\overline{S} \cap G(x)| = \Omega(\rho)$ and $|\overline{S} \cap G(x')| = \Omega(\rho)$. Letting $A = \overline{S}$, we show in the next two stages that that already $A = V(G)$. In Lemma 6.5.12, we count the number of triples $a, b, c \in V$ with $a \in A \cap G(x)$, $b \in A \cap G(x')$, $a \not\sim b$, and $c \in G(a) \cap G(b)$ to show that $\widehat{A} = A$ contains a constant fraction of the vertices in $V(G)$. Finally in Lemma 6.5.13 we complete the proof by showing that any constant fraction of the graph generates the entire graph when v is large enough. These last two lemmas are proved in Section 6.5.4.

6.5.3 The Growth Lemma

Of the three stages, the first is the most difficult and the most interesting. We give a precise statement.

Lemma 6.5.6. *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph such that $\lambda = o(\rho)$ and $\rho = o(v)$. There exists a pair of distinct vertices $x, x' \in V$ and a set $S \subseteq V$ with $|S| = O(\log v)$ such that $|\overline{S} \cap G(x)| = \Omega(\rho)$ and $|\overline{S} \cap G(x')| = \Omega(\rho)$.*

We prove the lemma inductively; in the inductive step, Lemma 6.5.7 below, we show

that a subset of a neighborhood of a vertex will generate a significantly larger subset of a neighborhood of a vertex after adding two additional vertices. Here is the precise statement.

Lemma 6.5.7 (Growth Lemma)**.** *There exists $\varepsilon > 0$ such that the following holds. Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph such that $\lambda = o(\rho)$ and $\rho = o(v)$. Let $x \in V(G)$ and $A \subseteq G(x)$. Suppose $|A| < \varepsilon\rho$. Then there is a vertex y and $\omega(1)$ vertices z such that $|\overline{A'} \cap G(z)| \gtrsim (1+\varepsilon)|A|$ where $A' = A \cup \{y, z\}$.*

Lemma 6.5.6 will then follow by induction.

Proof of Lemma 6.5.6 from Lemma 6.5.7. Let ε be as in Lemma 6.5.7. Fix two adjacent vertices y_0 and z_0, and let $S_0 = \{y_0, z_0\}$. When S_i, y_i, and z_i have been defined, consider the set $A_i = \overline{S_i} \cap G(z_i)$.

If $|A_i| < \varepsilon\rho$, then by Lemma 6.5.7 there is a pair y_{i+1}, z_{i+1} of vertices such that $|\overline{A_i'} \cap G(z_{i+1})| \gtrsim (1+\varepsilon)|A_i|$, where $A_i' = A_i \cup \{y_{i+1}, z_{i+1}\}$. Let $S_{i+1} = S_i \cup \{y_{i+1}, z_{i+1}\}$, and observe that $\overline{S_{i+1}} \supseteq \overline{A_i'}$. Hence,

$$|\overline{S_{i+1}} \cap G(z_{i+1})| \gtrsim (1+\varepsilon)|\overline{S_i} \cap G(z_i)|. \tag{6.6}$$

On the other hand, if $|A_i| \geq \varepsilon\rho$, we set $S = S_i$ and $x = z_i$, so that $|\overline{S} \cap G(x)| = |A_i| = \Omega(\rho)$. Observe that Eq. (6.6) guarantees that we will indeed have $|A_i| \geq \varepsilon\rho$ for some $i = O(\log v)$, and hence we will have $|S| = 2(i+1) = O(\log v)$.

We next define a set S' and a vertex x' by repeating the recursive construction of S and x exactly as in the previous paragraphs, except that whenever we would define a vertex z_{i+1}, we guarantee that $z_{i+1} \neq x$. Since Lemma 6.5.7 ensures that we have $\omega(1) > 2$ choices for each vertex z_{i+1}, this additional guarantee is possible. In particular, we obtain a set S' and a vertex $x' \neq x$ such that $|\overline{S'} \cap G(x')| = \Omega(\rho)$ and $|S'| = O(\log v)$.

So the vertices x and x' and the set $S \cup S'$ together satisfy the statement of Lemma 6.5.6, as desired. □

We prove Lemma 6.5.7 via the following two lemmas: the first is used for unbounded μ, the other for bounded μ.

Lemma 6.5.8. *Let G be a nontrivial $\mathrm{SR}(v,\rho,\lambda,\mu)$ graph such that $\lambda = o(\rho)$ and $\rho = o(v)$. For any $0 < \varepsilon \leq 1/3$, let $A \subseteq G(x)$ and suppose $|A| < \varepsilon\rho$. Let $\alpha = 2(1-\varepsilon)((\mu-4)/\mu)$. If $\alpha > 0$ then there are $\omega(1)$ vertices $z \in V$ such that $|\overline{A'} \cap G(z)| \gtrsim \alpha|A|$ where $A' = A \cup \{z\}$.*

Lemma 6.5.9. *Let G be a nontrivial $\mathrm{SR}(v,\rho,\lambda,\mu)$ graph such that $\lambda = o(\rho)$ and $\rho = o(v)$. Let $A \subseteq G(x)$ and suppose $|A| \leq \rho/(2\mu^2) - \lambda$. Then there exists a vertex y and $\omega(1)$ vertices z such that $|\overline{A'} \cap G(z)| \gtrsim (5/4)|A|$ where $A' = A \cup \{y,z\}$.*

A preliminary estimate is required. Recall our notation (from Eq. (6.5)) $A + y = G(A \setminus G^+(y)) \cap G(y)$. Recall that $A + y \subseteq \widehat{A \cup \{y\}} \cap G(y)$, and note that $|A+y| \leq \mu|A|$.

Lemma 6.5.10. *Let G be a nontrivial $\mathrm{SR}(v,\rho,\lambda,\mu)$ graph such that $\lambda = o(\rho)$ and $\rho = o(v)$. Let $A \subseteq V(G)$ and $X \subseteq G(A)$. Then, for $y \in V(G)$ chosen at random,*

$$\mathbb{E}_y(|(A+y) \cap X|) \geq |X|(\rho - \lambda - 1)/n \sim |X|(\mu/\rho).$$

Proof. For each $x \in X$, designate a neighbor $x' \in A$. For random $y \in V(G)$, let $\vartheta_x(y)$ denote the indicator of the event that $y \in G(x) \setminus G^+(x')$. Since $|G(x) \cap G^+(x')| = \lambda + 1$, we have $\mathbb{E}_y(\vartheta_x(y)) = (\rho - \lambda - 1)/v$.

Now, if $x \in X$ and $\vartheta_x(y) = 1$, then $y \sim x$ but $y \not\sim x'$, and so $x \in (A+y) \cap X$. So $|(A+y)\cap X| \geq \sum_{x\in X} \vartheta_x(y)$ and $\mathbb{E}_y(|(A+y)\cap X|) \geq \sum_{x\in X} \mathbb{E}_y(\vartheta_x(y)) = |X|(\rho-\lambda-1)/v$. □

We can now see the importance of the extra factor of 2 in the expansion afforded by Lemma 2.8.2 in comparison to Lemma 2.8.1. If $A \subseteq G(x)$ for some vertex x, then Lemma 2.8.1 along with Lemma 6.5.10 applied to the set $X = G(A)$ gives $\mathbb{E}_y(|A+y|) \gtrsim |A|$—so the operation $\cdot + y$ doesn't grow the set A at all. By contrast, if we use Lemma 2.8.2 instead, we get $\mathbb{E}_y(|A+y|) \gtrsim 2|A|$ (assuming A is sufficiently small and μ is sufficiently large). This argument suffices for the proof of Lemma 6.5.8 below.

Proof of Lemma 6.5.8. From Lemma 2.8.2, we have $|G(A)| \gtrsim \alpha(\rho/\mu)|A|$. By Lemma 6.5.10, $\mathbb{E}_z(|A+z|) \gtrsim \alpha|A|$. Since always $|A+z| \leq \mu|A|$, Fact 4.2.11 gives for any $\delta > 0$ that

$$P(|A+z| > (1-\delta)\alpha|A|) \gtrsim \frac{\delta\alpha}{\mu - (1-\delta)\alpha}.$$

Thus, there are $\Omega(\delta v/\mu)$ vertices z with $|A+z| > (1-\delta)\alpha|A|$. Letting $\delta = \sqrt{\mu/v}$ proves the lemma. □

We now prove Lemma 6.5.9, using the following additional estimate.

Lemma 6.5.11. *Let G be a nontrivial* $\mathrm{SR}(v,\rho,\lambda,\mu)$ *graph such that $\lambda = o(\rho)$ and $\rho = o(v)$. Let $x \in V(G)$ and $A \subseteq G(x)$. Then for $y \in V(G)$ chosen at random,*

$$\mathbb{E}_y(|(A+y) \setminus G^+(x)|) \geq \frac{(\rho-\lambda-1)^2}{v\mu}|A| \sim |A|.$$

Proof. Set $X = G(A) \setminus G^+(x)$, so $|X| \geq (\rho-\lambda-1)|A|/\mu$ by Lemma 2.8.1. Then the inequality follows immediate from Lemma 6.5.10, using $\mu \sim \rho^2/v$ from Corollary 6.1.4. □

Proof of Lemma 6.5.9. Let $y \in V(G)$ be a random vertex, and consider the random variable $X = |(A+y) \setminus G^+(x)|$. We have $0 \leq X \leq \mu|A|$, and $\mathbb{E}_y(X) \gtrsim |A|$ by Lemma 6.5.11. Hence, by Fact 4.2.11 there are $\gtrsim v/(2\mu-1)$ vertices y such that $|(A+y) \setminus G^+(x)| \gtrsim |A|/2$. If for at least half of these vertices y we have $|(A+y) \setminus G^+(x)| \geq (5/4)|A|$ then we are done: letting $z = y$, we have $\overline{A'} \cap G(z) \supseteq A + z$ sufficiently large sufficiently often.

Assume now the opposite; so there are $\gtrsim v/(4\mu-2)$ vertices y such that $|A|/2 \lesssim |(A+y) \setminus G^+(x)| \leq (5/4)|A|$.

Fix such a vertex y. Let $B = (A+y) \setminus G(x)$, so $|A|/2 \lesssim |B| \leq (5/4)|A|$. Every vertex $b \in B$ has at most μ neighbors $a \in A \subseteq G(x)$, and b has λ common neighbors with each such neighbor a. On the other hand, whenever $b \in B$ and $a \in A$ are nonadjacent, they have

μ common neighbors. Hence,

$$|G(A) \cap G(B)| \leq |B|\mu\lambda + |B||A|\mu = |B|\mu(|A| + \lambda) \leq \frac{\rho}{2\mu}|B|,$$

where the last inequality comes from the hypothesis that $|A| \leq \rho/(2\mu^2) - \lambda$. Since $A \subseteq G(x)$ and $B \subseteq G(y)$, we may use Lemma 2.8.1 to estimate $|G(A)| \geq (\rho - \lambda - 1)|A|/\mu$ and $|G(B)| \geq (\rho - \lambda - 1)|B|/\mu$. Therefore,

$$\begin{aligned}
|G(A \cup B)| &= |G(A)| + |G(B)| - |G(A) \cap G(B)| \\
&\geq \frac{\rho - \lambda - 1}{\mu}(|A| + |B|) - \frac{\rho}{2\mu}|B| \\
&= \frac{\rho - \lambda - 1}{\mu}|A| + \frac{\rho/2 - \lambda - 1}{\mu}|B| \\
&\gtrsim \frac{\rho}{\mu}|A| + \frac{\rho/2}{\mu}\frac{|A|}{2} \\
&= \frac{5}{4}\frac{\rho}{\mu}|A|.
\end{aligned}$$

Applying Lemma 6.5.10 to $A \cup B$ in the role of A and $G(A \cup B)$ in the role of X we obtain, for random $z \in V(G)$,

$$\mathbb{E}_z(|(A \cup B) + z|) \gtrsim |G(A \cup B)|\mu/\rho \gtrsim (5/4)|A|.$$

On the other hand, for all z we have $|(A \cup B) + z| \leq \mu|A \cup B| \leq (9/4)\mu|A|$. Consider the random variable $Z = |(A \cup B) + z|$; for any $\delta > 0$, applying Fact 4.2.11 gives

$$P(Z > (1 - \delta)(5/4)|A|) \gtrsim \frac{5\delta}{9\mu - 5(1 - \delta)}.$$

Thus, there are $\Omega(\delta v/\mu)$ vertices z with $|(A \cup B) + z| > (1 - \delta)(5/4)|A|$. Letting $\delta = \sqrt{\mu/v} = o(1)$ proves the lemma. □

Proof of the Lemma 6.5.7. Let $\varepsilon = 1/73$, and suppose $|A| < \varepsilon\rho$. For $\mu \leq 6$, we apply

Lemma 6.5.9. Since $\lambda = o(\rho)$, for n sufficiently large we have $|A| < \varepsilon\rho < \rho/(2\mu^2) - \lambda$, and so there is a vertex y and $\omega(1)$ vertices z such that $|A' \cap G(z)| \gtrsim (5/4)|A| > (1+\varepsilon)|A|$ where $A' = A \cup \{y, z\}$. For $\mu \geq 7$, we apply Lemma 6.5.8. Here, we do not need the extra vertex y: there are $\omega(1)$ vertices z such that $|A' \cap G(z)| \gtrsim (8/7)(1-\varepsilon)|A| > (1+\varepsilon)|A|$, where $A' = A \cup \{z\}$. □

6.5.4 The Final Stage

Lemma 6.5.12. *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph such that $\lambda = o(\rho)$ and $\rho = o(v)$. Let $A \subseteq V(G)$. Suppose there exist distinct vertices x, y such that $|A \cap G(x)| \geq \varepsilon\rho$ and $|A \cap G(y)| \geq \varepsilon\rho$ for some constant $\varepsilon > 0$. Then $|\widehat{A}| \gtrsim \varepsilon^2 v$.*

Proof. Let $X = A \cap G(x) \setminus G(y)$ and $Y = A \cap G(y) \setminus G(x)$. Without loss of generality, assume $|Y| \leq |X|$. We have $|G(x) \cap G(y)| \leq \lambda$ and therefore $|Y| \geq \varepsilon\rho - \lambda \sim \varepsilon\rho$.

Define $T = \{(a, b, z) : a \in X, b \in Y, a \not\sim b, z \in G(a) \cap G(b)\}$. Note that if $(a, b, z) \in T$ then $z \in \widehat{A}$.

Since no vertex in X is adjacent to y, each vertex in $a \in X$ has at most μ neighbors in Y, and so there are at least $|Y| - \mu$ vertices $b \in Y$ such that $a \not\sim b$. Therefore,

$$|T| \geq |X|(|Y| - \mu)\mu \sim \varepsilon^2\rho^2\mu.$$

For every $a \in X$, there are at most μ neighbors of a in $G(y)$, and for each such neighbor z, there are at most λ vertices $b \in Y \cap G(z)$. Hence, there are at most $|X|\mu\lambda$ triples $(a, b, z) \in T$ with $z \in G(y)$. Similarly, there are $\leq |Y|\mu\lambda$ triples $(a, b, z) \in T$ such that $z \in G(x)$. For every other vertex z appearing in T, we have $|G(z) \cap X| \leq \mu$ and $|G(z) \cap Y| \leq \mu$, so there are $\leq \mu^2$ pairs a, b such that $(a, b, z) \in T$. Thus, the number of distinct vertices $z \in V(G) \setminus (X \cup Y)$ such that $(a, b, z) \in T$ for some a, b is at least

$$\frac{|T| - \mu\lambda|X| - \mu\lambda|Y|}{\mu^2} \gtrsim \frac{\varepsilon^2\rho^2}{\mu} \sim \varepsilon^2 v\,.$$

In particular, $|\widehat{A}| \gtrsim \varepsilon^2 v$. □

The final stage in the proof of Lemma 6.5.4 is following Lemma 6.5.13, which states that any constant fraction of a strongly regular graph generates the entire graph. It's proof is essentially identical to that of Lemma 6.4.19.

Lemma 6.5.13. *Let G be a nontrivial $\mathrm{SR}(v, \rho, \lambda, \mu)$ graph such that $\lambda = o(\rho)$ and $\rho = o(v)$. Let $A \subseteq V(G)$ is such that $|A| = \Omega(v)$. Then for v sufficiently large, $\overline{A} = V(G)$.*

Proof. Let B be the set of vertices with at least $\lambda + 2$ neighbors in A. Since among any collection of $\lambda + 2$ vertices, there is a pair of non-adjacent vertices, then $B \subseteq N_2(A) \subseteq \overline{A}$. Similarly, if a vertex x has at least $\lambda + 2$ neighbors in $A \cup B$, then $x \in N_2(A \cup B) \subseteq \overline{A}$.

Thus, it suffices to show that every vertex $x \notin A \cup B$ has at least $\lambda + 2$ neighbors in $A \cup B$, for v sufficiently large. Indeed, if $x \notin A \cup B$, then $|A \setminus G(x)| \geq \Omega(v - \lambda - 1) = \Omega(v)$. Every vertex in $A \setminus G(x)$ has μ neighbors in $G(x)$, so the number of edges between $G(x)$ and $A \setminus G(x)$ is $\Omega(\mu v) = \Omega(\rho^2)$ by Corollary 6.1.4. Thus, $\mathbb{E}_{y \in G(x)}(|G(y) \cap A|) = \Omega(\rho)$, and since each vertex in $G(x)$ has at most ρ neighbors in A, it follows by Fact 4.2.11 that at least $\Omega(\rho)$ neighbors y of x each have at least $\Omega(\rho)$ neighbors in A. Since $\lambda = o(\rho)$, for v sufficiently large, each of these vertices y is in B, and x has more than $\lambda + 2$ neighbors in B. □

Finally, we complete the proof of Lemma 6.5.4 by using Lemmas 6.5.6, 6.5.12, and 6.5.13 in this order.

Proof of Lemma 6.5.4. By Lemma 6.5.6, there exists a constant $\varepsilon > 0$, a set A of $O(\log v)$ vertices, and a pair of distinct vertices x, y which satisfy the conditions of Lemma 6.5.12. Now, by the conclusion of that lemma, $\widehat{\overline{A}} = \overline{A}$ satisfies the condition of Lemma 6.5.13 and therefore, for all sufficiently large n we have $\overline{A} = V(G)$. □

Chapter 7

PRIMITIVE COHERENT CONFIGURATIONS

In this section, we give an overview of Theorem 2.5.4, our classification of primitive coherent configurations with large automorphism groups. In Section 7.1, we describe how we divide our analysis into cases, depending on the magnitude of ρ relative to v, and on the parameters λ_i. In Section 7.2, we prove Theorem 2.7.14, our classification of primitive coherent configurations having clique geometries with just two cliques at some vertex. Finally, in Section 7.3, we give some of the details of our analysis of the individualization/refinement heuristic in a range of the parameters. Other details of the analysis can be found in [Sun16] (cf. [SW15b]); we briefly summarize the omitted portions of the analysis below.

7.1 Overview of Analysis

As with our automorphism bounds for Steiner designs and strongly regular graphs, we prove Theorem 2.5.4 by analyzing the individualization/refinement heuristic. We prove the following main result, from which Theorem 2.5.4 immediately follows.

Theorem 7.1.1. *Let $\mathfrak{X}$ be a nontrivial primitive coherent configuration on v vertices. Then either $\mathfrak{X} = \mathfrak{X}(G)$ for G the triangular or lattice graph, or naive refinement is $O(v^{1/3}\log^{4/3} v)$-effective for $\mathfrak{X}$.*

Using Theorem 2.7.13, we divide our analysis into three cases. In the first case, either there is no dominant color, or $\rho > v^{2/3}(\log v)^{-1/3}$. In the second and third cases, we will assume $\rho = o(v^{2/3})$. Then by Theorem 2.7.13, either $\mathfrak{X}$ has an asymptotically uniform clique geometry (the second case), or there is some color k with $\lambda_k =< \varepsilon v^{1/2})$ (the third case).

We address the first case with the following lemma.

Lemma 7.1.2. *Let $\mathfrak{X}$ be a primitive coherent configuration. If $\rho \geq v^{2/3}(\log v)^{-1/3}$, then naive refinement is $O(v^{1/3}(\log v)^{4/3})$-effective for $\mathfrak{X}$.*

We remark that in the case that the rank r of $\mathfrak{X}$ is bounded, Lemma 7.1.2 follows from the following theorem of Babai.

Theorem 7.1.3 (Babai [Bab81, Theorem 2.4])**.** *Let $\mathfrak{X}$ be a nontrivial primitive coherent configuration of rank r. Then naive refinement is $O(r(v/\rho)\log v)$-effective.*

Lemma 7.1.2 is proved in [Sun16] (cf. [SW15b]). The "Growth of Spheres" estimate, Lemma 2.8.3, is a crucial component of the proof.

In the second case of our analysis, when $\mathfrak{X}$ has an asymptotically uniform clique geometry, we use Theorem 2.7.14 to classify the primitive coherent configurations in which some vertex belongs to only two cliques of the geometry. Theorem 2.7.14 helpfully separates the primitive coherent configurations with exceptionally large automorphisms from those to which individualization and refinement can be efficiently applied. However, case (b) of the classification provided by Theorem 2.7.14 is a rank four primitive coherent configuration that is not included among our list of exceptions in Theorem 2.7.14. Hence, this rank four configuration must be dealt with separately. We address this case with the following lemma.

Lemma 7.1.4. *Let $\mathfrak{X}$ be a primitive coherent configuration satisfying Theorem 2.7.14 (b). Then naive refinement is $O(\log v)$-effective for $\mathfrak{X}$.*

Thus, by combining Theorem 2.7.14 with Lemma 7.1.4, we conclude that when $\mathfrak{X}$ has an asymptotically uniform clique geometry, either the configuration is one of our exceptions, corresponding to a triangular or lattice graph, or every vertex belongs to at least three cliques in the geometry. In this latter case, there are many induced $K_{1,3}$ subgraphs in $G_{\mathfrak{X}}$. Similarly, in the third case of our overall analysis, when $\lambda_k < \varepsilon v^{1/2}$ for some color k, we again find many induced 3-claws in a union of constituent graphs. These ubiquitous 3-claws are essential for proving the following lemma.

Lemma 7.1.5. *There exists a constant $\varepsilon > 0$ such that the following holds. Let $\mathfrak{X}$ be a primitive coherent configuration with $\rho = o(v^{2/3})$. If $\mathfrak{X}$ satisfies either of the following conditions, then naive refinement is $O(v^{1/4}(\log v)^{1/2})$-effective for $\mathfrak{X}$.*

(a) For every nondominant color k, we have $\lambda_k \geq \varepsilon v^{1/2}$. Furthermore, $\mathfrak{X}$ has an asymptotically uniform clique geometry $\mathcal{G}$ such that every vertex belongs to at least three cliques of $\mathcal{G}$.

(b) There is a nondominant color k such that $\lambda_k < \varepsilon v^{1/2}$.

We describe the proof of Lemma 7.1.5 in Section 7.3.

We now prove Theorem 7.1.1 from the above lemmas.

Proof of Theorem 7.1.1. Let $\mathfrak{X}$ be a primitive coherent configuration. Suppose first that $\rho \geq v^{2/3}(\log v)^{-1/3}$. Then by Lemma 7.1.2, naive refinement is $O(v^{1/3}(\log v)^{4/3})$-effective for $\mathfrak{X}$.

Otherwise, $\rho < n^{2/3}(\log n)^{-1/3} = o(n^{2/3})$. By Theorem 2.7.13, either the hypotheses of Lemma 7.1.5 are satisfied, or the hypotheses of Theorem 2.7.14 are satisfied. In the former case, naive refinement is $O(v^{1/4}(\log v)^{1/2})$-effective for $\mathfrak{X}$. In the latter case, either $\mathfrak{X}$ is given by the triangular or lattice graph, or, by Lemma 7.1.4, naive refinement is $O(\log v)$-effective for $\mathfrak{X}$. □

7.2 A Combinatorial Classification of Primitive Coherent Configurations

In this section we will classify primitive coherent configurations $\mathfrak{X}$ having a clique geometry $\mathcal{G}$ and a vertex belonging to at most two cliques of $\mathcal{G}$. In particular, we prove Theorem 2.7.14.

We will assume the hypotheses of Theorem 2.7.14. So, $\mathfrak{X}$ will be a primitive coherent configuration such that $\rho = o(v^{2/3})$, with an asymptotically uniform clique geometry $\mathcal{G}$ and a vertex $x \in V$ belonging to at most two cliques of $\mathcal{G}$.

Lemma 7.2.1. *Under the hypotheses of Theorem 2.7.14, for v sufficiently large, every vertex $x \in V$ belongs to exactly two cliques of $\mathcal{G}$, each of order $\sim \rho/2$.*

Proof. Recall that by the definition of a clique geometry, for every vertex $x \in V$, every nondominant color i, and every clique C in the geometry containing x, we have $|C \cap \mathfrak{X}_i(x)| \lesssim \lambda_i$. Thus, by Corollary 5.3.18, every vertex belongs to at least two cliques. In particular, u belongs to exactly two cliques of $\mathcal{G}$, and (by Corollary 5.3.18) it follows that $\lambda_i \sim \rho_i/2$ for every nondominant color i. Hence, by the definition of a clique geometry, for every vertex x and every nondominant color i, there are exactly two cliques $C \in \mathcal{G}$ such that $x \in C$ and $\mathfrak{X}_i(x) \cap C \neq \emptyset$.

Let i and j be nondominant colors, and let $y \in \mathfrak{X}_j(w)$, and let $C \in \mathcal{G}$ be the clique containing u and v. Since $|\mathfrak{X}_i(w) \cap C| \sim \lambda_i \sim \rho_i/2$, we have

$$|G_{\mathfrak{X}}(y) \cap \mathfrak{X}_i(w)| \gtrsim \rho_i/2. \tag{7.1}$$

Now suppose for contradiction that some $x \in V$ belongs to at least three cliques of $\mathcal{G}$. Then there is some $C \in \mathcal{G}$ and nondominant color i such that $x \in C$ but $\mathfrak{X}_i(x) \cap C = \emptyset$. Let j be a nondominant color such that $\mathfrak{X}_j(x) \cap C \neq \emptyset$, and let $y \in \mathfrak{X}_j(x) \cap C$. By the coherence of $\mathfrak{X}$ and Eq. (7.1), we have $|G_{\mathfrak{X}}(y) \cap \mathfrak{X}_i(x)| \gtrsim \rho_i/2$.

But since there are exactly two cliques $C' \in \mathcal{G}$ such that $x \in C'$ and $\mathfrak{X}_i(x) \cap C' \neq \emptyset$, then one of these cliques C' is such that $|G_{\mathfrak{X}}(y) \cap \mathfrak{X}_i(x) \cap C'| \gtrsim \rho_i/4$. By Proposition 5.3.10, $\rho_i/4 = \omega(\mu)$ for n sufficiently large. But then $C' \subseteq G_{\mathfrak{X}}(y)$, and $y \notin C'$, contradicting the maximality of C'.

So every vertex $x \in V$ belongs to exactly two cliques of $\mathcal{G}$, and for each clique $C \in \mathcal{G}$ containing x and each nondominant color i, we have $|\mathfrak{X}_i(x) \cap C| \sim \rho_i/2$. It follows that $|C| \sim \rho/2$ for each $C \in \mathcal{G}$. □

Lemma 7.2.2. *Under the hypotheses of Theorem 2.7.14, for v sufficiently large, $\mathfrak{X}$ has rank at most four.*

Proof. Counting the number of vertex–clique incidences in $G(\mathfrak{X})$, we have $2v \sim |\mathcal{G}|(\rho/2+1) \sim |\mathcal{G}|\rho/2$ by Lemma 7.2.1. On the other hand, every pair of distinct cliques $C, C' \in \mathcal{G}$ intersects

in at most one vertex in $G(\mathfrak{X})$ by Property 2 of Definition 2.7.1, and so $|\mathcal{G}|^2/2 \gtrsim v$. It follows that $\rho \lesssim \sqrt{8v}$. On the other hand, by Lemma 5.3.3, we have $\rho_i \gtrsim \sqrt{v}$ for every $i > 1$. Since $\rho = \sum_{i>1} \rho_i$, for v sufficiently large there are at most two nondominant colors. □

Lemma 7.2.3. *Under the hypotheses of Theorem 2.7.14, let x be a vertex, and $C_1, C_2 \in \mathcal{G}$ be the two cliques containing x. Then for any $y \neq x$ in C_1, we have $|G_{\mathfrak{X}}(y) \cap (C_2 \setminus \{x\})| \leq 1$.*

Proof. We first note that by Lemma 7.2.1, there are indeed exactly two cliques containing x. Note that $y \notin C_2$, since otherwise there are two cliques in $\mathcal{G}$ containing both x and y. Suppose y has two distinct neighbors a, b in $C_2 \setminus \{x\}$, so $a, b \notin C_1$ for the same reason. Let $C_3 \in \mathcal{G} \setminus \{C_1\}$ be the unique clique containing y other than C_1. We have $a, b \in C_3$, but then $|C_2 \cap C_3| \geq 2$, a contradiction. So y has at most one neighbor in $C_2 \setminus \{x\}$. □

The following result is folklore, although we could not find an explicit statement in the literature. A short elementary proof can be found inside the proof of [CGSS76, Lemma 4.13].

Lemma 7.2.4. *Let G be a connected and co-connected strongly regular graph. If G is the line-graph of a graph, then G is isomorphic to $T(m)$, $L_2(m)$, or C_5.*

Proof of Theorem 2.7.14. Let H be the graph with vertex set $\mathcal{G}$, and an edge $\{C, C'\}$ whenever $|C \cap C'| \neq 0$. Then $G(\mathfrak{X})$ is isomorphic to the line-graph $L(H)$.

By Lemma 7.2.2, $\mathfrak{X}$ has rank at most four. By assumption, $\mathfrak{X}$ has rank at least three.

Consider first the case that $\mathfrak{X}$ has rank three. The nondiagonal colors i, j of a rank three primitive coherent configuration $\mathfrak{X}$ satisfy either $i^* = i$ and $j^* = j$, in which case $\mathfrak{X}$ is a strongly regular graph, or $i^* = j$, in which case $\mathfrak{X}$ is a "strongly regular tournament," and $\rho = (n-1)/2$. We have assumed $\rho = o(n^{2/3})$, so $\mathfrak{X}$ is a strongly regular graph. But $G(\mathfrak{X})$ is the line-graph of the graph H, so by Lemma 7.2.4, for $n > 5$, $\mathfrak{X}$ is isomorphic to either $\mathfrak{X}(T(m))$ or $\mathfrak{X}(L_2(m))$.

Suppose now that $\mathfrak{X}$ has rank four, and let $I = \{2, 3\}$ be the nondominant colors. Fix $x \in V$, and let $C_1, C_2 \in \mathcal{G}$ be the cliques containing x by Lemma 7.2.1. By Corollary 5.3.18 and Lemma 7.2.3, for any $i, j \in I$, not necessarily distinct, there exist $y \in C_1$ and $z \in C_2$

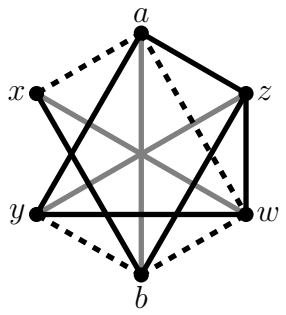

Figure 7.1: Two nonadjacent vertices a and b in $G_{\mathfrak{X}}$, and their common neighbors w, x, y, z. The gray lines represents the dominant color 1 in $\mathfrak{X}$, the dashed lines color 2, and the black lines color 3. The pairs of color 1, and the colors involving a and b are chosen without loss of generality, and these determine the remaining colors involving w.

with $c(y,z) = 1$, $c(y,x) = i$, and $c(x,z) = j$. Therefore, $p^1_{ij} \geq 1$, and so $\mu \sum_{i,j>1} p^1_{ij} \geq 4$. Now let $w \in V$ be such that $c(x,w) = 1$, and let $D_1, D_2 \in \mathcal{G}$ be the cliques containing w. For any $\alpha, \beta \in \{1,2\}$, we have $|C_\alpha \cap D_\beta| \leq 1$, and so $\mu \leq 4$. Hence, $\mu = 4$, and $|C_\alpha \cap D_\beta| = 1$ for every $\alpha, \beta \in \{1,2\}$. Therefore, for any pair of distinct cliques $C, C' \in \mathcal{G}$ we have $|C \cap C'| = 1$, and so H is isomorphic to K_m, where $m = |\mathcal{G}|$.

In particular, every clique $C \in \mathcal{G}$ has order $m-1$, and so $\rho_2 + \rho_3 = 2(m-2)$.

Now we prove $2^* = 3$ and $3^* = 2$. Suppose for contradiction that colors 2 and 3 are symmetric. Fix two vertices a and b with $c(a,b) = 1$. (See Figure 7.1.) Then $G_{\mathfrak{X}}(a) \cap G_{\mathfrak{X}}(b) = \{w,x,y,z\}$ for some vertices $w,x,y,z \in V$, and there are four distinct cliques $C_1, C_2, C_3, C_4 \in \mathcal{G}$ such that every vertex in $A = \{a,b,w,x,y,z\}$ lies in the intersection of two of these cliques. Without loss of generality, assume $c(w,x)$ and $c(y,z)$ are dominant, and all other distinct pairs in A except (a,b) have nondominant color. Since for any $i,j \in I$ we have $p^1_{ij} = 1$, then without loss of generality, by considering the paths of length two from a to b in $G(\mathfrak{X})$, we have $c(a,w) = c(a,x) = 2$, $c(a,y) = c(a,z) = 3$, $c(b,w) = c(b,y) = 2$, and $c(b,x) = c(b,z) = 3$. Now $c(w,a) = c(w,b) = 2$, and so $c(w,y) = c(w,z) = 3$ since $p^1_{ij} = 1$ for all $i,j \in I$ and $c(w,x) = 1$. But now $c(a,z) = c(b,z) = c(w,z) = 3$, which contradicts the fact that $p^1_{23} = p^1_{33} = 1$ for $c(z,y) = 1$. We conclude that $2^* = 3$ and $3^* = 2$. $\square$

Proof of Lemma 7.1.4. Let $\mathfrak{X}$ be a rank four primitive coherent configuration with a non-symmetric nondominant color i, and $G_{\mathfrak{X}}$ is isomorphic to $T(m)$ for $m = \rho_i + 2$. (The other nondominant color is i^*.) In particular, every clique in $\mathcal{G}$ has order $\rho_i + 1$.

Note that $p^i_{ii^*} = p^i_{ii} = p^i_{i^*i}$ by Proposition 5.3.1. For any edge $\{x, y\}$ in $T(m)$, there are exactly $m - 2 = \rho_i$ vertices z adjacent to both x and y. Hence, considering all the possible of colorings of these edges in $\mathfrak{X}$, we have

$$\rho_i = p^i_{ii} + p^i_{ii^*} + p^i_{i^*i} + p^i_{i^*i^*} = 3p^i_{ii} + p^i_{i^*i^*}.$$

Therefore, $p^i_{ii} + p^i_{i^*i^*} \geq \rho_i/3$, and

$$p^i_{ii^*} + p^i_{i^*i} \leq 2\rho_i/3. \tag{7.2}$$

Fix an arbitrary clique $C \in \mathcal{G}$ and any pair of distinct vertices $x, y \in C$. (By possibly exchanging x and y, we have $c(x, y) = i$.) Of the $\rho_i - 1$ vertices z in $C \setminus \{x, y\}$, at most $2\rho_i/3$ of these have $c(z, x) = c(z, y)$, by Eq. (7.2). So, including x and y themselves, there are at least $\rho_i/3 - 1 + 2 = \rho_i/3 + 1$ vertices $z \in C$ such that $c(z, x) \neq c(z, y)$. Thus, if we individualize a random vertex $z \in C$, then $\Pr[c(z, x) \neq c(z, y)] > 1/3$. If this event occurs, then x and y get different colors in the stable refinement. Hence, if we individualize each vertex of C independently at random with probability $6\ln(\rho_i^2)/\rho_i$, then x and y get the same color in the stable refinement with probability $\leq 1/\rho_i^4$. The union bound then gives a positive probability to every pair of vertices getting a different color, so there is a set A of size $O(\log \rho_i)$ such that after individualizing each vertex in A and refining to the stable coloring, every vertex in C has a unique color. We repeat this process for another clique C', giving every vertex in C' a unique color at the cost of another $O(\log \rho_i)$ individualizations.

On the other hand, every other clique $C'' \in \mathcal{G}$ intersects $C \cup C'$ in two uniquely determined vertices, since $G_{\mathfrak{X}}$ is isomorphic to $T(m)$. So, if $x \in C''$ and $y \notin C''$, then x and y get different colors in the stable refinement. Since every vertex lies in two uniquely determined cliques by

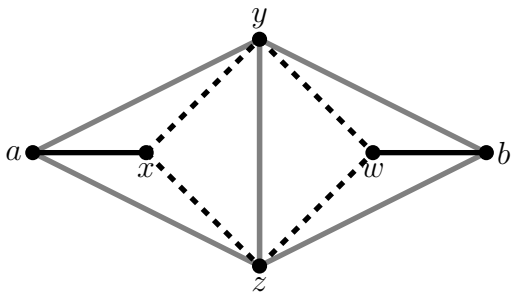

Figure 7.2: A quadruple (a, x, y, z) with property $Q(i, j)$ and a triple (x, y, z) that is good for a and b. The gray lines represent the dominant color 1, the black lines color i, and the dashed lines color j.

Lemma 7.2.1, it follows that every vertex gets a different color in the stable refinement. □

7.3 Good Triples

We now describe the proof of Lemma 7.1.5.

For given nondominant colors i and j, we will be interested in quadruples of vertices (w, x, y, z) with the following property:

Property $Q(i, j)$*:* $c(y, z) = c(w, y) = c(w, z) = 1$, $c(w, x) = i$, and $c(x, y) = c(x, z) = j$ (See Figure 7.2)

Definition 7.3.1 (Good triple of vertices)**.** For fixed nondominant colors i, j and vertices a, b, we say a triple of vertices (x, y, z) is *good* for a and b if (a, x, y, z) has Property $Q(i, j)$, but there is no vertex w such that (b, w, y, z) has Property $Q(i, j)$.

We observe that if (x, y, z) is good for vertices a and b, and both y and z are individualized, then a and b receive different colors after two refinement steps.

In the case of a strongly regular graph, there is only one choice of nondominant color, and Property $Q(i, j)$ and Definition 7.3.1 can be simplified: a triple (x, y, z) is good for a and b if the graph induced on $\{x, y, z, a\}$ by the nondominant color is isomorphic to $K_{1,3}$, with x the vertex of valency 3, but there is no vertex w such that the graph induced on $\{w, y, z, b\}$

is isomorphic to $K_{1,3}$. Careful counting of induced $K_{1,3}$ subgraphs formed a major part of Spielman's proof of Theorem 2.4.6. Spielman's ideas inspired the following lemma, which generalizes Lemmas 14 and 15 of [Spi96].

Lemma 7.3.2. *Let $\mathfrak{X}$ be a primitive coherent configuration with $\rho = o(v^{2/3})$. Suppose that for every distinct $a, b \in V$ there are nondominant colors i and j such that there are $\alpha = \Omega(\rho_i \rho_j^2)$ good triples (x, y, z) of vertices for (a, b). Then naive refinement is $O(v^{1/4}(\log v)^{1/2})$-effective.*

Proof. Let S be a random set of vertices given by including each vertex in V independently with probability p, for some p we will specify later. Fix distinct $a, b \in V$. We estimate the probability that there is a good triple (x, y, z) for a and b such that $y, z \in S$.

Let T denote the set of good triples (x, y, z) of vertices for (a, b). Observe that any vertex $x \in \mathfrak{X}_i(a)$ appears in at most ρ_j^2 good triples (x, y, z) in T. On the other hand, if $x \in \mathfrak{X}_i(a)$ is a random vertex, and N is the number of pairs y, z such that $(x, y, z) \in T$, then $\mathbb{E}[N] \geq \alpha/\rho_i$. Therefore, we have

$$\rho_j^2 \Pr[N \geq \alpha/(2\rho_i)] + (1 - \Pr[N \geq \alpha/(2\rho_i)])\alpha/(2\rho_i) \geq \mathbb{E}[N] \geq \alpha/\rho_i,$$

and so, since $\alpha = \Omega(\rho_i \rho_j^2)$ and $\alpha < \rho_i \rho_j^2$ by definition,

$$\Pr[N \geq \alpha/(2\rho_i)] \geq \frac{1}{2\rho_j^2 \rho_i/\alpha - 1} = \Omega(1).$$

Let X_0 be the set of vertices $x \in \mathfrak{X}_i(a)$ appearing in at least $\alpha/(2\rho_i)$ triples (x, y, z) in T, so $|X_0| = \Omega(\rho_i)$. Now let $X \subseteq X_0$ be a random set given by including each vertex $x \in X_0$ independently with probability $v/(3\rho_i\rho_j)$.

Fix a vertex $x \in X$ and a triple $(x, y, z) \in T$. Note that there are at most $p_{ij}^1 \lesssim \rho_i \rho_j / v$ vertices $x' \in X_0$ such that $c(x', y) = j$. Therefore, by the union bound, the probability that there is some $x' \neq x$ with $x' \in \mathfrak{X}_{j^*}(y) \cap X$ is $\leq 1/3$. Similarly, the probability that there is

some $x' \in \mathfrak{X}_{j*}(z) \cap X$ with $x' \neq x$ is at most 1/3. Hence, the probability that

$$\mathfrak{X}_{j*}(y) \cap X = \mathfrak{X}_{j^*}(z) \cap X = \{x\} \tag{7.3}$$

is at least 1/3.

Now for any $x \in X$, let T_x denote the set of pairs $y, z \in V$ such that $(x, y, z) \in T$ and Eq. (7.3) holds. We have $\mathbb{E}[|T_x|] \geq \alpha/(6\rho_i) = \Omega(\rho_j^2)$. But in any case, $|T_x| \leq \rho_j^2$. Therefore, for any $x \in X$, we have $|T_x| = \Omega(\rho_j^2)$ with probability $\Omega(1)$. Let $X' \subseteq X$ be the set of vertices x with $|T_x| = \Omega(\rho_j^2)$. Since $\mathbb{E}[|X'|] = \Omega(|X|)$, we have $|X'| = \Omega(|X|)$ with probability $\Omega(1)$. Furthermore, $|X| = \Omega(v/\rho_j)$ with high probability by the Chernoff bound.

Thus, there exists a set $X' \subseteq \mathfrak{X}_i(a)$ of size $|X'| = \Omega(v/\rho_j)$ such that $|T_x| = \Omega(\rho_j^2)$ for every $x \in X'$.

Now fix a $x \in X'$. The probability that there are at least two vertices in $\mathfrak{X}_j(x) \cap S$ is at least

$$1 - (1-p)^{\rho_j} - p\rho_j(1-p)^{\rho_j - 1} > 1 - e^{-p\rho_j} - p\rho_j e^{-p\rho_j} = \Omega(p^2\rho_j^2)$$

if $p\rho_j < 1$, using the Taylor expansion of the exponential function. Since $|T_x| = \Omega(\rho_j^2)$, the probability that there is a pair $(y, z) \in T_x$ with $y, z \in S$ is $\Omega(p^2\rho_j^2)$.

Therefore, the probability that there is no $x \in X'$ with a pair $(y, z) \in T_x$ such that $y, z \in S$ is at most

$$(1 - \Omega(p^2\rho_j^2))^{|X'|} \leq (1 - \Omega(p^2\rho_j^2))^{\varepsilon v/\rho_j},$$

for some constant $0 < \varepsilon < 1$. For $p = \beta\sqrt{\log v/(v\rho_j)}$ with a sufficiently large constant β, this probability is at most $1/(2v^2)$. Since $\rho_j \gtrsim \sqrt{v}$ for all j by Lemma 5.3.3, we may take $p = \beta\sqrt{\log v/v^{3/2}}$ with a sufficiently large constant β. Then, for any pair $a, b \in V$ of distinct vertices, the probability no good triple (x, y, z) for a and b has $y, z \in S$ is at most $1/(2v^2)$. By the union bound, the probability that there is some pair $a, b \in V(\mathfrak{X})$

of distinct vertices such that no triple (x, y, z) has the desired property is at most $1/2$. Therefore, after individualizing every vertex in S, every vertex in $V(\mathfrak{X})$ gets a unique color with probability at least $1/2$. By the Chernoff bound, we may furthermore assume that $|S| = O(v^{1/4}(\log v)^{1/2})$. □

Hence, to prove Lemma 7.1.5, it suffices to show that there are many good triples for every pair of vertices.

Lemma 7.1.5 presents two cases. In case (a), there is an asymptotically uniform clique geometry such that every vertex belongs to at least three cliques. It is easy to see that in this case the graph $G_{\mathfrak{X}}$ induces many $K_{1,3}$ subgraphs, and so it is reasonable to expect that there will be many good triples in $\mathfrak{X}$. The details of this argument are presented in [Sun16].

Case (b) of Lemma 7.1.5 is more subtle. In principle, the inequality $\lambda_k < \varepsilon v^{1/2}$ guaranteed in case (b) is analogous to the inequality $\lambda = o(\rho)$ used by Spielman to prove his automorphism bound for $\mathrm{SR}(v, \rho, \lambda, \mu)$ graphs [Spi96] (see Theorem 6.1.7). Indeed, $\rho = \Omega(v^{1/2})$ for $\mathrm{SR}(v, \rho, \lambda, \mu)$ graphs, and the inequality $\lambda < \varepsilon v^{1/2}$ would have sufficed for Spielman's argument, for some sufficiently small constant ε. However, for a primitive coherent configuration, a bound on λ_k does not in general imply any bound on λ_{k^*}. As we have seen in Section 5.3, this lack of symmetry between the parameters λ_k and λ_{k^*} is a major obstacle to generalizing arguments for strongly regular graphs to the context of primitive coherent configurations.

Hence, the analysis of case (b) of Lemma 7.1.5 in [SW15b] is divided into two subcases. In the first subcase, we additionally assume that $\lambda_{k^*} \lesssim \rho_k/3$, and the argument proceeds similarly to that of Spielman in the case of a strongly regular graph [Spi96]. A detailed argument in this first subcase can be found in [Sun16]. In the second subcase, when $\lambda_{k^*} \gtrsim \rho_k/3$, we instead make use of the local clique partitions guaranteed by Lemma 5.3.15. We now present a detailed analysis of this second subcase.

Lemma 7.3.3. *Let τ be an arbitrary fixed positive integer. Let $\mathfrak{X}$ be a primitive coherent configuration with $\rho = o(v^{2/3})$ and a nondominant color k such that $\lambda_k < v^{1/2}/(\tau + 1)$ and*

$\lambda_{k^*} \gtrsim n_k/\tau$. *Then for every pair of distinct vertices* $a, b \in V(\mathfrak{X})$, *there are* $\Omega(\rho_k^3)$ *good triples of vertices for* a *and* b *with respect to the colors* $i = k^*$ *and* $j = k^*$.

Lemma 7.3.4. *Let* $\mathfrak{X}$ *be a primitive coherent configuration with* $\rho = o(v^{2/3})$ *and strong* I*-local clique partitions for some set* I *of nondominant colors. Let* $j \in I$ *be a color such that* $\lambda_j = \Omega(\rho_j)$. *Let* x *and* b *be vertices such that* $c(x, b) = 1$. *Then for any nondominant color* i *with* $\rho_i \leq \rho_j$, *there are* $o(\rho_j^2)$ *triples* (w, y, z) *of vertices such that* $y, z \in \mathfrak{X}_j(x)$, $c(y, z) = 1$ *and* (b, w, y, z) *has Property* $Q(i, j)$.

Proof. Fix a nondominant color i, and let T be the set of triples (w, y, z) such that $y, z \in \mathfrak{X}_j(x)$, $c(y, z) = 1$ and (b, w, y, z) has Property $Q(i, j)$.

If $c(w, x) = 1$, then $|\mathfrak{X}_j(w) \cap \mathfrak{X}_j(x)| = p^1_{jj^*}$, and so there are at most $(p^1_{jj^*})^2$ pairs $y, z \in \mathfrak{X}_j(x)$ with $c(y, z) = 1$ such that $(w, y, z) \in T$. Then since $c(b, w) = i$ whenever $(w, y, z) \in T$, the total number of triples $(w, y, z) \in T$ such that $c(w, x) = 1$ is at most

$$(p^1_{jj^*})^2 \rho_i \lesssim (\rho_j^2/n)^2 \rho_i \leq \rho_j^2(\rho^3/v^2) = o(\rho_j^2),$$

where the first inequality follows from Proposition 5.3.1 (iii) and (4), and the relation $\rho_1 \sim v$.

Since $c(x, b) = 1$, there are $\leq \rho\rho_i/v$ vertices $w \in \mathfrak{X}_i(b) \cap G_{\mathfrak{X}}(x)$. Suppose $w \in \mathfrak{X}_i(b) \cap G_{\mathfrak{X}}(x)$. Let $\mathcal{G}$ denote the collection of maximal cliques partitioning $\mathfrak{X}_I(x)$. If some clique in $\mathcal{G}$ contains w, let C be that clique; otherwise, let $C = \emptyset$. Since $\mathcal{G}$ partitions $\mathfrak{X}_j(x)$ into $\sim \rho_j/\lambda_j = O(1)$ cliques for each $x \in V(\mathfrak{X})$, and since $|\mathfrak{X}_j(w) \cap C'| \leq \mu$ for every clique $C' \in \mathcal{G}$ with $C \neq C'$, we therefore have $|(\mathfrak{X}_j(x) \cap \mathfrak{X}_j(w)) \setminus C| \lesssim \mu\rho_j/\lambda_j = O(\mu)$. But then there are at most

$$|\mathfrak{X}_j(x) \cap \mathfrak{X}_j(w)| \cdot |(\mathfrak{X}_j(x) \cap \mathfrak{X}_j(w)) \setminus C| = O(\rho_j\mu)$$

pairs $y, z \in \mathfrak{X}_j(x)$ with $c(y, z) = 1$ such that $(b, w, y, z) \in T$, for a total of at most $O(\rho_j\mu(\rho\rho_i)/v) = o(\rho_j^2)$ triples $(w, y, z) \in T$ with $c(w, x) \neq 1$. □

Proof of Lemma 7.3.3. Let ℓ be a nondominant color. Then by Proposition 5.3.10, we have $\rho_k\sqrt{\mu/\rho_\ell} = o(\rho_k) = o(\lambda_{k^*})$. Similarly, $\rho_k\mu = o(\lambda_{k^*}^2)$. Hence, by Lemma 5.3.15 and Definition 5.3.8, there is a set I of nondominant colors with $k^* \in I$ such that $\mathfrak{X}$ has strong I-local clique partitions. Since $\lambda_k < v^{1/2}/(\tau+1) \lesssim \rho_k/(\tau+1)$ by Lemma 5.3.3, and since $\lambda_{k^*} \gtrsim \rho_k/\tau$, the by the definition of an I-local clique partition, $k \notin I$. Hence, by the definition of a strong I-local clique partition and Observation 5.3.6, for a vertex x and a vertex $y \in \mathfrak{X}_k(x)$, $|G_{\mathfrak{X}}(y) \cap \mathfrak{X}_{k^*}(x)| \le \tau\mu = o(\rho_k)$.

On the other hand, by Corollary 5.3.18, we have $\lambda_{k^*} \lesssim \rho_k/2$, and hence $\lambda_k \le v^{1/2}/3 \lesssim \rho_k/3$ by Lemma 5.3.3.

Fix $a, b \in V(\mathfrak{X})$, and let $j = c(a,b)$, and let $\varepsilon = 2\mu/\rho_j$, so $\varepsilon = o(1)$ by Proposition 5.3.10. By Lemma 5.3.13, we have

$$|\mathfrak{X}_{k^*}(u) \cap G_{\mathfrak{X}}(v)| \le \max\left\{\frac{\lambda_{k^*}+1}{1-\varepsilon}, \rho_{k^*}\frac{\mu}{\varepsilon\rho_j}\right\} \lesssim \rho_{k^*}/2.$$

Let $x \in \mathfrak{X}_{k^*}(a) \setminus G_{\mathfrak{X}}(b)$. We have $c(x,a) = k$ and so $|\mathfrak{X}_{k^*}(x) \cap G_{\mathfrak{X}}(a)| = o(\rho_k)$. We count the number of pairs of non-adjacent vertices (y,z) such that (a,x,y,z) has Property $Q(k^*,k^*)$.

For every vertex $y \in \mathfrak{X}_{k^*}(x) \setminus G_{\mathfrak{X}}(a)$, there are at least $\rho_{k^*} - |\mathfrak{X}_{k^*}(x) \cap G_{\mathfrak{X}}(a)| - \lambda_{k^*} \gtrsim \rho_{k^*}/2$ vertices $z \in \mathfrak{X}_{k^*}(x) \setminus G_{\mathfrak{X}}(a)$ such that (a,x,y,z) has Property $Q(k^*,k^*)$. Since $|\mathfrak{X}_{k^*}(x) \cap G_{\mathfrak{X}}(a)| \lesssim \rho_{k^*}/3$, the number of pairs (y,z) with $c(y,z) = 1$ such that (a,x,y,z) has Property $Q(i,j)$ is $\gtrsim (2\rho_{k^*}/3)(\rho_{k^*}/2) = (1/3)\rho_{k^*}^2$.

But by Lemma 7.3.4, there are $o(\rho_k^2)$ triples (y,z,w) of vertices such that $y,z \in \mathfrak{X}_{k^*}(x)$, $c(y,z) = 1$ and (b,w,y,z) has Property $Q(k^*,k^*)$. So there are $\Omega(\rho_k^2)$ pairs (y,z) of vertices such that (x,y,z) is good for a and b with respect to colors $i = k^*$ and $j = k^*$. Since we have $\Omega(\rho_k)$ choices for vertex x, there are in total $\Omega(\rho_k^3)$ good triples, as desired. □

Chapter 8

PRIMITIVE PERMUTATION GROUPS

We now use Theorem 2.5.4 to prove Corollary 2.6.1, our CFSG-free classification of large primitive permutation groups. More generally, we show that verification of Conjecture 2.5.5 to an order threshold of $\exp(n^{\varepsilon})$ entails Cameron's classification of primitive permutation groups, up to the same order threshold. These permutation group classifications follow from Theorem 8.2.1, the main result of this section.

8.1 Johnson, Hamming, and Cameron Graphs

Before stating Theorem 8.2.1, we define Cameron graphs and compute their automorphism groups. We start with the special case of a Johnson graph.

The *Johnson graph* $J(m,k)$ with $m > 2k$ is the graph whose vertex set V is the collection of k-subsets of $[m]$, with $A \sim B$ whenever $|A \setminus B| = 1$. So $J(m,k)$ is a constituent graph of the coherent configuration $\mathfrak{J}(m,k)$.

Proposition 8.1.1. *Suppose $m > 2k$. Then* $\mathrm{Aut}(J(m,k)) = S_m^{(k)}$.

Proof. Clearly $S_m^{(k)} \leq \mathrm{Aut}(J(m,k))$. We show that $\mathrm{Aut}(J(m,k)) \leq S_m^{(k)}$ by observing that the set $[m]$ can be reconstructed from $J(m,k)$, modulo S_m.

For $i \in [m]$, let $A_i = \{A \in V(J(m,k)) : i \in A\}$. Note that every pair of vertices in A_i is at distance at most $k-1$ in $J(m,k)$, and $|A_i| = \binom{m-1}{k-1}$. Now suppose $X \subseteq V(J(m,k))$ has the property that every pair of vertices in X is at distance at most $k-1$. Then every pair $A, B \in X$ has nonempty intersection. By the Erdős–Ko–Rado Theorem, we have $|X| \leq \binom{m-1}{k-1}$ [EKR61]. But furthermore, Hilton and Milner observe that either the inequality is strict, or we have $\bigcap_{A \in X} A \neq \emptyset$ [HM67]. Hence, if $|X| = \binom{m-1}{k-1}$, then $X = A_i$ for some $i \in [m]$. Therefore, the collection $\mathcal{A} = \{A_i : i \in [m]\}$ can be reconstructed from $J(m,k)$. Furthermore, every vertex in $J(m,k)$ is uniquely determined by the k sets in $\mathcal{A}$ to which

it belongs. Therefore, any automorphism of $J(m,k)$ is determined by its action on $\mathcal{A}$, and $\mathrm{Aut}(J(m,k)) \leq S_m$ as claimed. $\square$

Given graphs G and H, the *Cartesian product* $G\square H$ has vertex set $V(G) \times V(H)$ with $(x,y) \sim (x',y')$ if $x = x'$ and $y \sim y'$ in H, or if $x \sim x'$ in G and $y = y'$. Since $(F\square G)\square H$ and $F\square(G\square H)$ are isomorphic, we define the *dth Cartesian power* $\square^d G$ as the d-fold Cartesian product of G with itself.

We remark that $\square^d K_m$ is usually called the *Hamming graph* $H(m,d)$; it is a constituent graph of the Hamming scheme $\mathfrak{H}(m,d)$.

Definition 8.1.2. The *Cameron graph* $C(m,k,d)$, with $m > 2k$, is the graph $\square^d J(m,k)$.

Let $G = C(m,k,d)$ be a Cameron graph. If $x \in V(G)$, then $x = (x_1, \ldots, x_d)$, where $x_i \subseteq [m]$ with $|x_i| = k$ for all $1 \leq i \leq d$.

Cameron graphs are to Cameron schemes as Johnson and Hamming graphs are to Johnson and Hamming schemes; in particular, Cameron graphs are constituent graphs of Cameron schemes.

Proposition 8.1.3. *Let $\mathfrak{X}$ be a Cameron scheme. Then for some integers m, k, and d, with $m > 2k$, there is a constituent graph of $\mathfrak{X}$ isomorphic to $C(m,k,d)$.*

Proof. We have $\mathfrak{X} = \mathfrak{X}(\Gamma)$ for some Cameron group Γ. In particular, we have integers m, k, and d such that $(A_m^{(k)})^d \leq \Gamma \leq S_m^{(k)} \wr S_d$. Hence, we may identify $V = V(\mathfrak{X})$ with $V(C(m,k,d))$. Let $x_1, \ldots, x_d$ be k-subsets of $[m]$, and let x_1' be a k-subset of $[m]$ such that $|x_1 \setminus x_1'| = 1$. The orbit of the pair $((x_1, x_2, \ldots, x_d), (x_1', x_2, \ldots, x_d))$ in the induced action of Γ on $V \times V$ is exactly the set of ordered pairs of adjacent vertices in $C(m,k,d)$. $\square$

We have the following characterization of the automorphism groups of Cameron graphs.

Lemma 8.1.4. *Suppose $m > 2k$. Then* $\mathrm{Aut}(C(m,k,d)) = S_m^{(k)} \wr S_d$

Lemma 8.1.4 will follow from a classical theorem of Sabidussi, which states that connected graphs have unique "prime factorizations." A graph G is *prime* if, whenever $G = K\square H$,

either K or H is the trivial graph on a single vertex, and the other is G. We denote by $G \sqcup H$ the disjoint union of the graphs G and H.

Theorem 8.1.5 (Sabidussi [Sab59])**.** *Let G be a connected graph. Then there is a unique (up to isomorphism) collection $\{G_1, \ldots, G_d\}$ of prime graphs G_i such that $G = G_1 \Box \cdots \Box G_d$. Furthermore,* $\mathrm{Aut}(G) \cong \mathrm{Aut}(G_1 \sqcup \cdots \sqcup G_d)$.

Proposition 8.1.6. *Suppose $m > 2k$. Then $J(m,k)$ is prime.*

Proof. S_m is not a nontrivial product of groups. Therefore, by Theorem 8.1.5, supposing that $J(m,k)$ is not prime, one of the graphs in its Cartesian product decomposition must have trivial automorphism group, contradicting that $\mathrm{Aut}(J(m,k))$ is transitive. Hence, $J(m,k)$ is prime. □

Proof of Lemma 8.1.4. By Theorem 8.1.5 and Proposition 8.1.6, we have $\mathrm{Aut}(\Box^d J(m,k)) = \mathrm{Aut}(J(m,k)) \wr S_d$. Thus, by Proposition 8.1.1, $\mathrm{Aut}(\Box^d J(m,k)) = S_m^{(k)} \wr S_d$. □

8.2 Schurian Configurations

Our main result of Chapter 8 is the following weak converse to Proposition 8.1.3, which characterizes the large groups whose Schurian configurations have Cameron constituent graphs.

Theorem 8.2.1. *There exists an absolute constant $c > 0$ such that the following holds. Let Γ be a primitive permutation group of degree n and order $|\Gamma| \geq \exp(c \log^3 n)$. Suppose some constituent graph of $\mathfrak{X}(\Gamma)$ is isomorphic to $C(m,k,d)$, for some $m,k,d \in \mathbb{N}$ with $m > 2k$. Then Γ is a Cameron group with parameters (m,k,d) (and $\mathfrak{X}(\Gamma)$ is a Cameron scheme).*

Corollary 2.6.1 follows from from Theorems 2.5.4 and 8.2.1.

Proof of Corollary 2.6.1. Let Γ be a primitive permutation group of degree n, and order greater than $\exp(cv^{1/3} \log^{7/3} v)$, where c is the constant hidden by the O-notation in Theorem 2.5.4. Let $\mathfrak{X} = \mathfrak{X}(\Gamma)$. Since $\Gamma \leq \mathrm{Aut}(\mathfrak{X})$, by Theorem 2.5.4 we have that either $\mathfrak{X}$ is the

trivial primitive coherent configuration, or $\mathfrak{X} = \mathfrak{X}(G)$ for G the triangular or lattice graph. In other words, either $\mathfrak{X}$ is isomorphic to $\mathfrak{J}(m,k)$, where $k \in \{1,2\}$, or $\mathfrak{X}$ is isomorphic to $\mathfrak{H}(d,m)$, where $d = 2$.

So $\mathfrak{X}$ has a constituent graph isomorphic to a Cameron graph $C(m,k,d)$, where $(k,d) \in \{(1,1),(2,1),(1,2)\}$. Hence, by Theorem 8.2.1, we have that Γ is a Cameron group with parameters (m,k,d), where $(k,d) \in \{(1,1),(2,1),(1,2)\}$. If $(k,d) = (1,1)$, then $A_m \leq \Gamma \leq S_m$, so we are in situation (a) of Corollary 2.6.1. If $(k,d) = (2,1)$, then $A_m^{(2)} \leq \Gamma \leq S_m^{(2)}$, so we are in situation (b) of Corollary 2.6.1. Otherwise, $(k,d) = (1,2)$, and so $(A_m)^2 \leq \Gamma \leq S_m \wr S_2$, and we are in situation (c) of Corollary 2.6.1. □

In fact, from Theorem 8.2.1, it follows that Babai's conjectured classification of primitive coherent configurations, Conjecture 2.5.5, implies Cameron's classification of primitive permutation groups up to an order threshold of $\exp(n^{\varepsilon})$.

We note that a similar guarantee as Theorem 8.2.1 is already possible using CFSG, via Cameron's classification of large primitive groups. In particular, without requiring the structural assumption that $C(m,k,d)$ is a constituent graph of $\mathfrak{X}(\Gamma)$, and with the order threshold relaxed to $|\Gamma| > n^{1+\log_2 n}$, Theorem 2.6.2 guarantees that Γ is a Cameron group.

The two key ingredients to our CFSG-free proof of Theorem 8.2.1 are the following theorem of Livingstone and Wagner [LW65, Theorem 2] (cf. [Wie67]), and Pyber's elementary bound on the order of a doubly-transitive permutation group [Pyb93].

Theorem 8.2.2 (Livingstone–Wagner [LW65])**.** *Suppose $\Gamma \leq S_n$ acts transitively on k-subsets of $[n]$, where $k \geq 2$ and $n \geq 2k$. Then Γ is $(k-1)$-transitive on $[n]$.*

Theorem 8.2.3 (Pyber [Pyb93])**.** *Suppose $\Gamma \leq S_n$ is doubly transitive, and $A_n \not\leq \Gamma$. Then $|\Gamma| \leq \exp(O(\log^3 n))$.*

We now prove Theorem 8.2.1. Given a permutation group Γ and a subset X of its domain, we denote by $\Gamma_{\{X\}}$ the *setwise stabilizer* of X in Γ.

Proof of Theorem 8.2.1. Let $m, k, d \in \mathbb{N}$, with $m > 2k$, and suppose $C(m,k,d)$ is a constituent graph of $\mathfrak{X} = \mathfrak{X}(\Gamma)$. By Lemma 8.1.4, we have $\Gamma \leq S_m^{(k)} \wr S_d$. We must show that $(A_m^{(k)})^d \leq \Gamma$. We will show that $\Phi \leq \Gamma$, where $\Phi = \{(\phi, 1, \ldots, 1) \in (A_m^{(k)})^d : \phi \in A_m^{(k)}\}$; the theorem then follow by symmetry.

We have $n = \binom{m}{k}^d$, so $k, d < \log_2 n$, and clearly $m \leq n$. Hence, $d! m^k \leq \exp(O(\log^2 n))$. Thus, we may assume $|\Gamma| \geq d! m^{kd} \exp(c \log^3 n)$, some some constant c to be specified later.

We identify $V(\mathfrak{X}_1)$ with the collection of d-tuples $(x_1, \ldots, x_d)$ of k-subsets x_i of $[m]$.

Let $x_2, \ldots, x_d$ be arbitrary fixed k-subsets of $[m]$. Let

$$X = \{(x_1, x_2, \ldots, x_d) \in V(\mathfrak{X}_1) : x_1 \text{ a } k\text{-subset of } [m]\}$$

Hence, the subgraph of the constituent graph $C(m,k,d)$ induced on X is isomorphic to $J(m,k)$.

By Theorem 8.1.5, since the prime factorization of $C(m,k,d)$ into a product of $J(m,k)$ is unique, any $\gamma \in \Gamma$ that maps some pair in X to another pair in X, in fact stabilizes X setwise. In particular, $\Gamma_{\{X\}}$ is transitive on ordered pairs of adjacent vertices in X.

Clearly $(S_m^{(k)} \wr S_d)_{\{X\}} \geq S_m^{(k)} \times (S_{m-k}^{(k)})^{d-1}$. Hence, we have

$$|\Gamma : \Gamma_{\{X\}}| = |\Gamma \cap (S_m^{(k)} \wr S_d) : \Gamma \cap (S_m^{(k)} \wr S_d)_{\{X\}}| \leq \left(\frac{m!}{(m-k)!}\right)^{d-1} d! < d! m^{kd}.$$

In particular, $|\Gamma_{\{X\}}| > \exp(c \log^3 m)$.

Now $\Gamma_{\{X\}} \leq S_m^{(k)}$, and the action of $\Gamma_{\{X\}}$ on k-subsets of $[m]$ is transitive.

Suppose $k = 1$. Then $J(m,k) = K_m$, and since $\Gamma_{\{X\}}$ is transitive on ordered pairs of adjacent vertices in X, it is doubly transitive on $[m]$. Hence, by Theorem 8.2.3, we have $A_m \leq \Gamma_{\{X\}}$, for c a sufficiently large constant.

Suppose $k = 2$, and suppose for contradiction that $\Gamma_{\{X\}}$ is not doubly transitive on $[m]$. Then $\mathfrak{X}(\Gamma)$ is a strongly regular tournament, having rank 3 and two edge-colors each of valency $(v-1)/2$. Then by Theorem 7.1.3 and Proposition 3.2.2, $|\Gamma| \leq \exp(O(\log^2 m))$, a

contradiction for c sufficiently large. Hence, again $\Gamma_{\{X\}}$ is doubly transitive on $[m]$, and we have $A_m \leq \Gamma_{\{X\}}$ by Theorem 8.2.3.

Finally, suppose $k \geq 3$. By Theorem 8.2.2, $\Gamma_{\{X\}}$ is doubly transitive on $[m]$. Hence, by Theorem 8.2.3, we have $A_m \leq \Gamma_{\{X\}}$, again for c sufficiently large. $\square$

Chapter 9

THE ISOMORPHISM PROBLEM

The Graph Isomorphism has long been one of the only natural problems in NP eluding classification. Early work on interactive proofs gave evidence that Graph Isomorphism is not NP-complete: if it is NP-complete, then the polynomial hierarchy collapses [GMW91]. Yet, for over three decades, the best known upper bound on the worst-case time-complexity of deciding Graph Isomorphism was $\exp(\widetilde{O}(\sqrt{v}))$, where v is the number of vertices [ZKT82, BL83, BKL83].

In a recent breakthrough, Babai has improved the time-complexity bound to quasipolynomial [Bab15].

In this chapter, we present our time-complexity bounds for deciding isomorphism of regular combinatorial objects. We compare these results with Babai's recent quasipolynomial-time algorithm for general graph isomorphism [Bab15]. First, we review the two most essential algorithmic techniques for provable Graph Isomorphism time-complexity bounds. We have already used the first, individualization and refinement, in order to establish our bounds in the previous chapters on the number of automorphisms of highly regular structures. We describe its application to the Graph Isomorphism problem in Section 9.1. The second algorithmic technique, Luks's group-theoretic divide-and-conquer method, is described in Section 9.2. Then, in Section 9.3, we give our time-complexity bounds for deciding isomorphism of highly regular combinatorial objects. As we explain, our algorithmic results follow immediately from the combinatorial theorems proved in the previous chapters.

9.1 Canonical Forms via Individualization and Refinement

The individualization/refinement heuristic we have analyzed in the previous chapters has its origin in the study of the Graph Isomorphism problem. Weisfeiler and Leman defined their canonical color refinement process in this context.

Canonical color refinement can give short proofs of non-isomorphism—unless two graphs have the same list of colors in the stable refinement, with color classes of the same size, they are not isomorphic. (The converse need not be true. For example, WL refinement on its own cannot distinguish pairs of strongly regular graphs with the same parameters.)

A more powerful approach combines refinement with individualization to produce canonical forms. A *canonical form* on a class $\mathcal{C}$ of finite structures is a function $F : \mathcal{C} \to \mathcal{C}$ such that (i) $F(X) \cong X$ for every $X \in \mathcal{C}$, and (ii) $F(X) = F(Y)$ whenever $X \cong Y$. Note that if a canonical form for a class $\mathcal{C}$ of explicit structures can be computed in time T, then isomorphism of any $X, Y \in \mathcal{C}$ can be decided in time $O(T)$ by checking whether $F(X)$ and $F(Y)$ are equal.

Let $\mathcal{R}$ be a canonical color refinement operator, and suppose that after d individualizations in a vertex-colored graph G, the $\mathcal{R}$-stable refinement is discrete (i.e., $\mathcal{R}$ is d-effective for G). Hence, the choice of d individualizations determines an ordering of $V(G)$ according to the vertex colors in the stable refinement, and hence determines an explicit adjacency matrix for G. A canonical form can then by computed by taking the lexicographically least adjacency matrix over all possible choices of d individualizations in G. We have the following proposition.

Proposition 9.1.1. *Suppose the canonical color refinement operator $\mathcal{R}$ is d-effective for a class $\mathcal{C}$ of graphs. Then a canonical form for $\mathcal{C}$ can be computed in time $O(v^d T(\mathcal{R}))$, where v is the number of vertices and $T(\mathcal{R})$ is the time required to compute the $\mathcal{R}$-stable refinement.*

Analogous statements hold for other combinatorial structures, such as Steiner designs. Note that the naive-stable refinement and the WL-stable refinement can both be computed in polynomial time.

We note that since canonical color refinement can only be d-effective for graphs with $\leq v^d$ automorphisms, Proposition 9.1.1 does not provide an efficient algorithm for computing canonical forms of any class of graphs including graphs with large automorphism groups. Hence, graphs with large automorphism groups pose a mathematical obstacle to the efficient

application of individualization and refinement for Graph Isomorphism.

9.2 The Group Theory Method

The first Graph Isomorphism algorithm that made use of permutation group machinery in a significant way was Babai's 1979 polynomial-time Las Vegas algorithm for deciding isomorphism of vertex-colored graphs with bounded color class size [Bab]. Algorithms based on even more substantial group theory soon followed, in particular Luks's polynomial-time algorithm for deciding isomorphism of graphs of bounded valency [Luk82]. The combination of Luks's divide-and-conquer algorithm with Zemlyachenko's combinatorial valency reduction lemma led to the $\exp(\widetilde{O}(v^{1/2}))$-time algorithm for general Graph Isomorphism that remained the state of the art for over 30 years [ZKT82, BL83, BKL83]. The basic divide-and-conquer approach pioneered by Luks also underlies Babai's quaspolynomial-time Graph Isomorphism algorithm.

We will only use Luks's group-theoretic method via the following easily-stated Theorem 9.2.1, based on the Babai–Luks string isomorphism framework [BL83] combined with Miller's trick for avoiding dependence of the timing on valency [Mil83] (see Theorem 3.8 and Proposition 3.9 of [BCS+13]).

We again use the "color-d-boundedness" concept, defined in Section 3.3.

Theorem 9.2.1. *Let $\mathcal{C}$ be a class of vertex-colored graphs, closed under isomorphisms. Let $\mathcal{R}$ be a canonical refinement operator over $\mathcal{C}$. Let $G \in \mathcal{C}$ have v vertices. Suppose that after individualizing some set of ℓ vertices, the $\mathcal{R}$-stable refinement is color-d-bounded. Then we can compute a canonical form of G in time $T(\mathcal{R})v^{\ell+O(d)}$, where $T(\mathcal{R})$ denotes the cost computing the $\mathcal{R}$-stable refinement of a graph on v vertices.*

Theorem 9.2.1 offers a way around the obstacle that graphs with large automorphism groups pose for individualization refinement. For example, let G be the disjoint union of m copies of K_2, each belonging to its own vertex color class. Thus, $|\operatorname{Aut}(G)| = 2^m$, but the

graph is already color-2 bounded, and so Theorem 9.2.1 gives a polynomial-time canonical form.

On the other hand, Theorem 9.2.1 presents a mathematical obstacle of its own, since Proposition 3.3.1 states that Theorem 9.2.1 is only applicable to graphs whose automorphism groups have Γ_d subgroups of index at most v^ℓ.

9.3 Time-Complexity Bounds for Deciding Isomorphism

We now summarize our results for deciding isomorphism, starting with Steiner designs.

9.3.1 Steiner Designs

Theorem 9.3.1. *Canonical forms for Steiner $S(t, k, n)$ designs can be computed, and isomorphism decided, in time $n^{t+O(\log n)}$.*

The previous best was $n^{t+O(k \log k+\log n)}$, due to Huber [Hub11], based on the Babai–Luks $n^{O(k \log k+\log n)}$ time-complexity bound for $S(2, k, n)$ designs [BL83]. In contrast to our own analysis, the time-complexity bounds of Huber and Babai–Luks generalize to balanced incomplete block designs, giving a $n^{t+O(\lambda \log \lambda+k \log k+\log n)}$ time-complexity bound for deciding isomorphism of $S_\lambda(t, k, n)$ designs.

Theorem 9.3.1 is immediate from Theorem 4.0.1 and Proposition 9.1.1. □

9.3.2 Strongly Regular Graphs

Strongly regular graphs were long perceived as a difficult case for Graph Isomorphism. In 1979, Babai gave an $\exp(\widetilde{O}(v^{1/2}))$-time algorithm for $\mathrm{SR}(v, \rho, \lambda, \mu)$ graphs [Bab80b]. His time-complexity bound was not improved until 1996, when Spielman gave an $\exp(\widetilde{O}(v^{1/3}))$-time algorithm. Spielman's result, in turn, stood until the 2013, when the present author and his collaborators established the following time-complexity bound.

Theorem 9.3.2. *Canonical forms for* $\mathrm{SR}(v, \rho, \lambda, \mu)$ *graphs can be computed, and isomorphism decided, in time* $\exp(\widetilde{O}(v^{1/5}))$.

Theorem 9.3.2 follows by combining the following, more detailed time-complexity bounds.

Theorem 9.3.3. *Canonical forms for* $\mathrm{SR}(v, \rho, \lambda, \mu)$ *graphs can be computed, and isomorphism decided in time* $\exp(\widetilde{O}(1 + \lambda/\mu))$.

Theorem 9.3.3 is immediate from Theorem 6.4.1 and Proposition 9.1.1. □

Theorem 9.3.4. *Canonical forms for* $\mathrm{SR}(v, \rho, \lambda, \mu)$ *graphs can be computed, and isomorphism decided in time* $v^{\mu+O(\log v)}$.

Theorem 9.3.4 is immediate from Theorems 6.5.1 and 9.2.1, in view of the fact that canonical forms for triangular and lattice graphs can be easily computed in polynomial time. □

The combination of Theorems 9.3.3, 9.3.4, and 6.2.2 with the bounds on the parameters of strongly regular graph given in Section 6.1 give Theorem 9.3.2. The proof is analogous to the proof of Corollary 2.4.11, with the caveat that we must also use the fact that the unique reconstruction of a partial geometry from its line-graph given by Theorem 2.7.9 can be found in polynomial time. □

Furthermore, we can find *all* reconstructions of a partial geometry from its line-graph in time polynomial in the bounds on the number of reconstructions given by Theorems 2.7.10 and 2.7.11. Hence, combining Theorem 2.7.10 with Theorem 9.3.1 gives the following time-complexity bound for deciding isomorphism of a line-graph of a Steiner design.

Theorem 9.3.5. *Canonical forms for* $\mathrm{SR}(v, \rho, \lambda, \mu)$ *graphs that are line-graphs of Steiner designs can be computed in time* $\exp(\widetilde{O}(v^{1/14}))$.

The proof is identical to that of Theorem 2.4.7.

9.3.3 Primitive Coherent Configurations

The general Graph Isomorphism problem is easily reduced to the problem of deciding isomorphism of coherent configurations, by Weisfeiler–Leman refinement. While inhomogeneous coherent configurations and imprimitive coherent configurations provide obvious substructures for a combinatorial partitioning strategy for Graph Isomorphism (the partition of the diagonal, and the components of a constituent graph, respectively), primitive coherent configurations do not offer such an easy handle and therefore represent a clear starting point for a combinatorial attack on the general Graph Isomorphism problem. This program was initiated by Babai [Bab81], who gave an $\exp(\widetilde{O}(v^{1/2}))$-time algorithm to decide isomorphism of primitive coherent configurations with v vertices. We give the following improvement.

Theorem 9.3.6. *Canonical forms for primitive coherent configurations can be computed, and isomorphism decided, in time* $\exp(\widetilde{O}(v^{1/3}))$*, where* v *is the number of vertices.*

Proof. Trivial coherent configurations, triangular graphs, and lattice graphs can all be recognized, and canonical forms computed, in polynomial time. (For example, the trivial Steiner design corresponding to the triangular graph can be recognized using Theorem 2.7.9.) For all other primitive coherent configurations, a canonical form can be computed in time $\exp(\widetilde{O}(v^{1/3}))$ using Theorem 7.1.1 and Proposition 9.1.1. □

9.3.4 Comparison with Babai's Quasipolynomial-Time Algorithm

Babai's quasipolynomial-time algorithm for general Graph Isomorphism supersedes many of the results in this section. In particular, his result is both more general, and provides better time-complexity, than Theorems 9.3.2, 9.3.5, and 9.3.6.

On the other hand, our results always produce canonical forms, which Babai does not currently claim. In some cases, our results give better time-complexity bounds. While Babai estimates his time-complexity bound as $\exp(O(\log v)^7)$, we obtain $\exp(O(\log n)^2)$ for Steiner $\mathrm{S}(2,k,n)$ designs, $\exp(O(\log n)^{c+1})$ for $\mathrm{SR}(v,\rho,\lambda,\mu)$ graph with $\mu = O(\log n)^c$ by Theo-

rem 9.3.4, and $\exp(O(\log v)^4)$ for $\mathrm{SR}(v, \rho, \lambda, \mu)$ graphs with $\rho = \Omega(v^{5/6})$ by Theorem 9.3.3 and Corollary 6.1.10. Finally, our algorithms are much simpler: with the exception of Theorems 9.3.4 and 9.3.2, we only make use of individualization and refinement.

We note that our Theorem 9.3.6 has direct relevance to the general Graph Isomorphism problem. Indeed, primitive coherent configurations appear in Babai's quasipolynomial-time analysis as a combinatorial obstacle that he overcomes. By substituting Theorem 9.3.6 for the recursive "Split-or-Johnson" procedure in Babai's algorithm, it is possible to obtain an $\exp(\widetilde{O}(v^{1/3}))$-time algorithm for general Graph Isomorphism [Bab15, Remark 6.1.3]. Although this does not come close to Babai's quasipolynomial time-complexity, it does break the decades-old $\exp(\widetilde{O}(v^{1/2}))$ time-complexity barrier for general Graph Isomorphism. Moreover, this $\exp(\widetilde{O}(n^{1/3}))$ algorithm is considerably simpler than the algorithm that includes the "Split-or-Johnson" routine. Further progress along the lines of Theorem 9.3.6 would offer the possibility of a substantially simpler subexponential-time (or even possibly quasipolynomial-time) algorithm for general Graph Isomorphism.

References

[Bab] László Babai. Monte Carlo algorithms in graph isomorphism testing. Tech. Report 79–10, Dép. Math. et Stat., Univ. de Montréal, 1979.

[Bab80a] László Babai. Almost all Steiner triple systems are asymmetric. *Topics in Steiner Systems*, pages 37–39, 1980.

[Bab80b] László Babai. On the complexity of canonical labeling of strongly regular graphs. *SIAM Journal on Computing*, 9(1):212–216, 1980.

[Bab81] László Babai. On the order of uniprimitive permutation groups. *Annals of Mathematics*, 113(3):553–568, 1981.

[Bab82] László Babai. On the order of doubly transitive permutation groups. *Inventiones Mathematicae*, 65(3):473–484, 1982.

[Bab14] László Babai. On the automorphism groups of strongly regular graphs I. In *Proc. 5th Innovations in Theoretical Computer Science (ITCS'14)*, pages 359–368, 2014.

[Bab15] László Babai. Graph isomorphism in quasipolynomial time. *arXiv*, 1512.03547, 2015.

[Bai04] R. A. Bailey. *Association Schemes: Designed Experiments, Algebra and Combinatorics*. Cambridge University Press, Cambridge, 2004.

[BCN89] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-Regular Graphs*. Springer-Verlag, Berlin, 1989.

[BCS+13] László Babai, Xi Chen, Xiaorui Sun, Shang-Hua Teng, and John Wilmes. Faster canonical forms for strongly regular graphs. In *Proc. 54th IEEE Symp. on Foundations of Computer Science (FOCS'13)*, pages 157–166, 2013.

[BI84] Eiichi Bannai and Tatsuro Ito. *Algebraic Combinatorics I: Association Schemes*. The Benjamin/Cummings Publishing Co., Inc., Menlo Park, CA, 1984.

[Big93] Norman Biggs. *Algebraic Graph Theory*. Cambridge University Press, 1993.

[BKL83] László Babai, William M. Kantor, and Eugene M. Luks. Computational complexity and the classification of finite simple groups. In *Proc. 24th IEEE Symp. on Foundations of Computer Science (FOCS'83)*, pages 162–171, 1983.

[BL83] László Babai and Eugene M. Luks. Canonical labeling of graphs. In *Proc. 15th ACM Symp. on Theory of Computing (STOC'83)*, pages 171–183, 1983.

[Bos63] R. C. Bose. Strongly regular graphs, partial geometries and partially balanced designs. *Pacific Journal of Mathematics*, 13:389–419, 1963.

[BP94] László Babai and László Pyber. Permutation groups without exponentially many orbits on the power set. *Journal of Combinatorial Theory, Series A*, 66(1):160–168, 1994.

[BPS09] László Babai, Péter Pálfy, and Jan Saxl. On the number of p-regular elements in finite simple groups. *LMS Journal of Computation and Mathematics*, 12:82–119, 2009.

[BS52] R. C. Bose and T. Shimamoto. Classification and analysis of partially balanced incomplete block designs with two associate classes. *Journal of the American Statistical Association*, 47(258):151–184, 1952.

[BW13] László Babai and John Wilmes. Quasipolynomial-time canonical form for Steiner designs. In *Proc. 45th ACM Symp. on Theory of Computing (STOC'13)*, pages 261–270, 2013.

[BW15] László Babai and John Wilmes. Asymptotic Delsarte cliques in distance-regular graphs. *Journal of Algebraic Combinatorics*, 2015.

[BW16] László Babai and John Wilmes. Steiner designs have few automorphisms. pages 1–29, 2016. In preparation.

[Cam81] Peter J. Cameron. Finite permutation groups and finite simple groups. *Bulletin of the London Mathematical Society*, 13:1–22, 1981.

[Cam15] Peter Cameron. Asymmetric Latin squares, Steiner triple systems, and edge-parallelisms. *arXiv*, 1507.02190, 2015.

[CFI92] Jin-Yi Cai, Martin Fürer, and Neil Immerman. An optimal lower bound on the number of variables for graph identification. *Combinatorica*, 12(4):389–410, 1992.

[CGSS76] Peter J. Cameron, Jean-Marie Goethals, Johan J. Seidel, and Ernest E. Shult. Line graphs, root systems and elliptic geometry. *Journal of Algebra*, 43:305–327, 1976.

[Coo78] Bruce N Cooperstein. Minimal degree for a permutation representation of a classical group. *Israel Journal of Mathematics*, 30(3):213–235, 1978.

[CST13a] Xi Chen, Xiaorui Sun, and Shang-Hua Teng. Multi-stage design for quasipolynomial-time isomorphism testing of Steiner 2-systems. In *Proc. 45th ACM Symp. on Theory of Computing (STOC'13)*, pages 271–280, 2013.

[CST13b] Xi Chen, Xiaorui Sun, and Shang-Hua Teng. A new bound on the order of the automorphism groups of strongly regular graphs. 2013. Manuscript.

[Del73] Philippe Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Journal of Research*, (10):vi+97, 1973.

[EKR61] Paul Erdős, Chao Ko, and Richard Rado. Intersection theorems for systems of finite sets. *The Quarterly Journal of Mathematics*, 12(1):313–320, 1961.

[FT78] Walter Feit and Jacques Tits. Projective representations of minimum degree of group extensions. *Canadian Journal of Mathematics*, 30(5):1092–1102, 1978.

[GMW91] Oded Goldreich, Silvio Micali, and Avi Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof system. *Journal of the ACM*, 38(1):691–729, 1991.

[God93] Christopher D. Godsil. Geometric distance-regular covers. *New Zealand Journal of Mathematics*, 22(2):3138, 1993.

[GR01] Christopher David Godsil and Gordon Royle. *Algebraic Graph Theory*, volume 207. Springer New York, 2001.

[Hig70] D. G. Higman. Coherent configurations I. *Rendiconti del Seminario Matematico della Università di Padova*, 44:1–25, 1970.

[HM67] Anthony Hilton and Eric Milner. Some intersection theorems for systems of finite sets. *The Quarterly Journal of Mathematics*, 18(1):369–384, 1967.

[HS60] Alan Hoffman and Robert Singleton. On Moore graphs with diameters 2 and 3. *IBM Journal of Research and Development*, 4(5):497–504, 1960.

[Hub11] Michael Huber. Computational complexity of reconstruction and isomorphism testing for designs and line graphs. *J. Combin. Theory Ser. A*, 118(2):341–349, 2011.

[KB10] Jack H Koolen and Sejeong Bang. On distance-regular graphs with smallest eigenvalue at least $-m$. *Journal of Combinatorial Theory, Series B*, 100(6):573–584, 2010.

[Kee14] Peter Keevash. The existence of designs. *arXiv*, 1401.3665, 2014.

[Luk82] Eugene M. Luks. Isomorphism of graphs of bounded valence can be tested in polynomial time. *Journal of Computer and System Sciences*, 25(1):42–65, 1982.

[LW65] Donald Livingstone and Ascher Wagner. Transitivity of finite permutation groups on unordered sets. *Mathematische Zeitschrift*, 90(5):393–403, 1965.

[Mar02] Attila Maróti. On the orders of primitive groups. *Journal of Algebra*, 258(2):631–640, 2002.

[Met91] Klaus Metsch. Improvement of Bruck's completion theorem. *Designs, Codes and Cryptography*, 1(2):99–116, 1991.

[Met99] Klaus Metsch. On a characterization of bilinear forms graphs. *European Journal of Combinatorics*, 20(4):293–306, 1999.

[Mil78] Gary L. Miller. On the $n^{\log n}$ isomorphism technique: A preliminary report. In *Proc. 10th ACM Symp. on Theory of Computing (STOC'78)*, pages 51–58, 1978.

[Mil83] Gary L. Miller. Isomorphism of graphs which are pairwise k-separable. *Information and Control*, 56(1-2):21–33, 1983.

[MW05] Brendan McKay and Ian Wanless. On the number of Latin squares. *Annals of Combinatorics*, 9(3):335–344, 2005.

[Neu79] Arnold Neumaier. Strongly regular graphs with smallest eigenvalue $-m$. *Archiv der Mathematik*, 33(4):392–400, 1979.

[Neu82] Arnold Neumaier. Quasiresidual 2-designs, $1\frac{1}{2}$-designs, and strongly regular multigraphs. *Geometriae Dedicata*, 12(4):351–366, 1982.

[Pyb93] László Pyber. On the orders of doubly transitive permutation groups, elementary estimates. *Journal of Combinatorial Theory, Series A*, 62(2):361–366, 1993.

[Pyb14] László Pyber. Large connected strongly regular graphs are Hamiltonian. *arXiv*, 1409.3041, 2014.

[Sab59] Gert Sabidussi. Graph multiplication. *Mathematische Zeitschrift*, 72(1):446–457, 1959.

[Sch33] I. Schur. Zur Theorie der einfach transitiven Permutationsgruppen. *Sitzungsberichte der Preussischen Akademie der Wissenschaften*, pages 598–623, 1933.

[Spi96] Daniel A. Spielman. Faster isomorphism testing of strongly regular graphs. In *Proc. 28th ACM Symp. on Theory of Computing (STOC'96)*, pages 576–584, 1996.

[Sun16] Xiaorui Sun. *On the structure and isomorphism of graphs*. PhD thesis, Columbia University, 2016.

[SW15a] Xiaorui Sun and John Wilmes. Faster canonical forms for primitive coherent configurations. In *Proc. 47th ACM Symp. on Theory of Computing (STOC'15)*, pages 693–702, 2015.

[SW15b] Xiaorui Sun and John Wilmes. Structure and automorphisms of primitive coherent configurations. *arXiv*, 1510.02195, 2015.

[Wei76] Boris Weisfeiler, editor. *On Construction and Identification of Graphs*, volume 558 of *Lecture Notes in Mathematics*. Springer-Verlag, 1976.

[Wie67] Helmut Wielandt. Endliche k-homogene Permutationsgruppen. *Mathematische Zeitschrift*, 101(2):142–142, 1967.

[Wil72a] Richard M Wilson. An existence theory for pairwise balanced designs I. Composition theorems and morphisms. *Journal of Combinatorial Theory, Series A*, 13(2):220–245, 1972.

[Wil72b] Richard M Wilson. An existence theory for pairwise balanced designs II. the structure of PBD-closed sets and the existence conjectures. *Journal of Combinatorial Theory, Series A*, 13(2):246–273, 1972.

[Wil75] Richard M Wilson. An existence theory for pairwise balanced designs, III: Proof of the existence conjectures. *Journal of Combinatorial Theory, Series A*, 18(1):71–79, 1975.

[WL68] B. Weisfeiler and A. A. Leman. A reduction of a graph to a canonical form and an algebra arising during this reduction. *Nauchno-Technicheskaya Informatsiya*, 9:12–16, 1968.

[Zie10] Paul-Hermann Zieschang. *Theory of Association Schemes*. Springer, 2010.

[ZKT82] Victor N. Zemlyachenko, N. M. Korneenko, and Regina I. Tyshkevich. Graph isomorphism problem. *Zapiski Nauchnykh Seminov (LOMI)*, 118:83–158, 215, 1982.