Faster Canonical Forms for Primitive Coherent Configurations

(Extended Abstract)

Xiaorui Sun*
xiaoruisun@cs.columbia.edu
Department of Computer Science
Columbia University
New York, NY 10027

John Wilmes†
wilmesj@math.uchicago.edu
Department of Mathematics
University of Chicago
Chicago, IL 60637

ABSTRACT

Primitive coherent configurations (PCCs) are edge-colored digraphs that generalize strongly regular graphs (SRGs), a class perceived as difficult for Graph Isomorphism (GI). Moreover, PCCs arise naturally as obstacles to combinatorial divide-and-conquer approaches for general GI. In a natural sense, the isomorphism problem for PCCs is a stepping stone between SRGs and general GI.

In his 1981 paper in the *Annals of Math.*, Babai proposed a combinatorial approach to GI testing via an analysis of the standard individualization/refinement (I/R) technique and proved that I/R yields canonical forms of PCCs in time $\exp(\widetilde{O}(n^{1/2}))$. (The tilde hides polylogarithmic factors.) We improve this bound to $\exp(\widetilde{O}(n^{1/3}))$. This is faster than the current best bound, $\exp(\widetilde{O}(n^{1/2}))$, for general GI, and subsumes Spielman's $\exp(\widetilde{O}(n^{1/3}))$ bound for SRGs (STOC'96, only recently improved to $\exp(\widetilde{O}(n^{1/5}))$ by the present authors and their coauthors (FOCS'13)).

Our result implies an $\exp(\widetilde{O}(n^{1/3}))$ upper bound on the number of automorphisms of PCCs with certain easily described and recognized exceptions, making the first progress in 33 years on an old conjecture of Babai. The emergence of exceptions illuminates the technical difficulties: we had to separate these cases from the rest. For the analysis we develop a new combinatorial structure theory for PCCs that in particular demonstrates the presence of "asymptotically uniform clique geometries" among the constituent graphs of PCCs in a certain range of the parameters.

A corollary to Babai's 1981 result was an $\exp(\widetilde{O}(n^{1/2}))$ upper bound on the order of primitive but not doubly transitive permutation groups, solving a then 100-year old problem in group theory. An improved bound of $\exp(\widetilde{O}(n^{1/3}))$ (with known exceptions) follows from our combinatorial result. This bound was previously known (Cameron, 1981) only through the Classification of Finite Simple Groups. We note that upper bounds on the order of primitive permutation groups are central to the application of Luks's group theoretic divide-and-conquer methods to GI.

1. INTRODUCTION

The Graph Isomorphism (GI) problem has been notorious for its unresolved complexity status. GI is not believed to be NP-hard, in particular because the polynomial hierarchy would then collapse to the second level [15]. On the other hand, we have yet to see an algorithmic improvement to the 1983 worst-case time bound of $\exp(\widetilde{O}(n^{1/2}))$ [7, 8, 24] where n denotes the number of vertices. Breaking this barrier is the principal goal of current algorithmic work on the GI problem [6, 10, 13, 5].

In the present paper we break a 33-year-old $\exp(\widetilde{O}(n^{1/2}))$ barrier in the GI problem and in the related theories of primitive permutation groups and highly regular combinatorial objects, making progress for the first time in a project initiated by Babai's 1981 paper in the *Annals of Math.* [3].

Coherent configurations (CCs) are a GI-complete class of highly regular colorings of the set of pairs of vertices, definable as the stable configurations under the canonical Weisfeiler-Leman (WL) refinement [23], cf. [22, 11].

A CC is *primitive* (PCC) if the edges of each color form a strongly connected digraph that spans the set of vertices. PCCs generalize the class of non-trivial strongly regular graphs (SRGs). While imprimitive CCs provide obvious substructures for a combinatorial divide-and-conquer strategy for GI (the components of a color), PCCs don't offer such an easy handle and therefore represent a clear starting point for a combinatorial attack on the general GI problem.

This program was initiated by Babai [3] who gave a (purely combinatorial) $\exp(\widetilde{O}(n^{1/2}))$ algorithm to test isomorphism of PCCs. (The tilde hides polylog factors.) Our main result improves this bound to $\exp(\widetilde{O}(n^{1/3}))$, subsuming in particular Spielman's 1996 result [21] that gave the same bound for SRGs. We note that while Spielman's work relied on Neumaier's profound structure theory for SRGs [20], no generalization of Neumaier's theory to PCCs is known. We build our own structure theory. A notable aspect of the new theory is a clique geometry found in PCCs in a certain range of

*This work was partially supported by a grant from the Simons Foundation (#320173 to Xiaorui Sun).
†Supported by an NSF Graduate Research Fellowship under grant DGE-1144082.

STOC'15, June 14–17, 2015, Portland, Oregon, USA.

ACM 978-1-4503-3536-2/15/06 ...$15.00.
DOI: http://dx.doi.org/10.1145/2746539.2746617.

the parameters, in some analogy with the case of SRGs [18, 9] exploited in recent progress on the isomorphism problem for SRGs [5].

Before the emergence of the group-theoretic method in GI testing [1, 17], Babai proposed a combinatorial approach to GI testing via an analysis of the individualization/refinement (I/R) method. He demonstrated that individualization followed by naive vertex refinement works in time $\exp(\widetilde{O}(\sqrt{n}))$ for SRGs [2] and subsequently for PCCs [3]. Additionally, [3] solved as a by-product a then century-old problem in the theory of permutation groups, giving a nearly tight $\exp(\widetilde{O}(\sqrt{n}))$ upper bound on the orders of primitive but not doubly transitive permutation groups. In a separate 1979 paper [1], Babai also demonstrated that I/R can be combined with the group theoretic method; such combination has been particularly successful recently in reducing the complexity of SRG isomorphism to $\exp(\widetilde{O}(n^{1/5}))$ [5].

In this paper we carry the analysis of [3] further and prove that I/R yields an $\exp(\widetilde{O}(n^{1/3}))$ isomorphism test for PCCs.

This extra step involves considerable technical difficulties, highlighted by the emergence of exceptions. The line graphs of complete graphs and of complete bipartite graphs with equal parts are SRGs with too many ($\exp(\widetilde{O}(n^{1/2}))$) automorphisms to allow I/R to succeed within the time bound claimed. While these classes of graphs can be recognized in polynomial time, our structure theory has to separate them from the rest; our result implies that all other PCCs have at most $\exp(\widetilde{O}(n^{1/3}))$ automorphisms.

As a corollary to this last statement, we also make progress on the problem in the theory of permutation groups addressed by Babai [3]: it follows that primitive but not doubly transitive permutation groups have order $\exp(\widetilde{O}(n^{1/3}))$ with known exceptions. The only earlier proof of this result [12] required the Classification of Finite Simple Groups (CFSG).

We note that bounds on the orders of primitive permutation groups play a central role in the analysis of GI algorithms based on Luks's group-theoretic divide-and-conquer method [17]. In particular, any CFSG-free analysis of a Luks-based $\exp(n^{0.49})$ algorithm for GI testing will have to depend on our result (just as the current $\exp(\widetilde{O}(n^{1/2}))$ analysis depends on Babai's bound).

1.1 Coherent configurations

We say that a *configuration* $\mathfrak{X}$ on vertex set V is a partition $R_0 \cup \cdots \cup R_{r-1}$ of $V \times V$ with the following properties:

(1) the diagonal $\Delta = \{(v, v) : v \in V\}$ is the union of some of the R_i;

(2) $(\forall i)(\exists i^*)(R_i^{-1} = R_{i^*})$ (where $R_i^{-1} = \{(v, u) : (u, v) \in R_i\}$)

We think of $\mathfrak{X}$ as an edge-colored complete digraph with loops on V, with edge color classes given by the R_i. Hence, the color of a pair $(u, v) \in V \times V$ is $c(u, v) = i$ if $(u, v) \in R_i$. The *rank* r of a configuration is the number of edge color classes. We shall also speak of the colors of the vertices, defined as $c(u) := c(u, u)$. We call the digraph $\mathfrak{X}_i = (V, R_i)$ the *color-i constituent digraph.*

Given a graph $G = (V, E)$, we associate with G the configuration $\mathfrak{X}(G) = (V; \Delta, E, \overline{E})$ where $\overline{E}$ denotes the set of edges of the complement of G. (We omit E if $E = \emptyset$ and omit $\overline{E}$ if $\overline{E} = \emptyset$.) So graphs can be viewed as configurations of rank ≤ 3.

A *coherent configuration* (CC) [23, 22, 16] is a configuration which additionally satisfies the following condition:

(3) for every $0 \leq i, j, k \leq r - 1$, there is a number p_{jk}^i such that for every $(u, v) \in R_i$, there are exactly p_{jk}^i vertices $w \in V$ such that $(u, w) \in R_j$ and $(w, v) \in R_k$.

The numbers p_{jk}^i are called the *structure constants* of $\mathfrak{X}$.

Remark 1. Isomorphisms of configurations preserve edge colors by definition. Since the isomorphism problem for edge-colored graphs easily reduces to GI via Frucht's gadgets [14] (cf. [19]), configurations are GI-complete. In fact, CCs are GI-complete, as a consequence of the Weisfeiler–Leman (WL) canonical refinement method [23, 22] which keeps refining the coloring until (3) is satisfied.

A CC is *primitive* (PCC) if it has the following additional properties:

(4) $\Delta = R_0$;

(5) the constituent digraphs $\mathfrak{X}_i$ are strongly connected for every $1 \leq i \leq r - 1$.

A *canonical form* on a class $\mathcal{C}$ of finite structures is a function $F : \mathcal{C} \to \mathcal{C}$ such that (i) $F(C) \cong C$ for every $C \in \mathcal{C}$, and (ii) $F(C) = F(C')$ whenever $C \cong C'$. Note that if a canonical form for a class $\mathcal{C}$ of explicit structures can be computed in time T, then isomorphism within $\mathcal{C}$ can be tested in time $O(T)$. We state our main result.

THEOREM 1. *A canonical form of primitive coherent configurations (PCCs) with n vertices can be computed in time $\exp(\widetilde{O}(n^{1/3}))$. In particular, isomorphism of PCCs can be tested within the same time bound.*

1.2 Relation to strongly regular graphs

An undirected graph $G = (V, E)$ is *strongly regular* (SRG) with parameters (n, k, λ, μ) if G has n vertices, every vertex has degree k, each pair of adjacent vertices has λ common neighbors, and each pair of non-adjacent vertices has μ common neighbors. We note that G is a SRG if and only if $\mathfrak{X}(G)$ is a CC. If a SRG G is nontrivial, i.e., it is connected and coconnected, then $\mathfrak{X}(G)$ is a PCC.

SRGs have long been identified as a hard (but probably not complete, see [4]) case for GI.

Progress has been made intermittently on testing isomorphism of SRGs. An $\exp(\widetilde{O}(n^{1/2}))$ bound was established by Babai [2] (1980), a few years before the same bound for general graphs was found. This was improved to $\exp(\widetilde{O}(n^{1/3}))$ by Spielman [21] (1996), and further to $\exp(\widetilde{O}(n^{1/5}))$ by the present authors and their coauthors [5] (2013).

PCC isomorphism can be viewed as an intermediate problem between isomorphism of SRGs and general GI. While we draw inspiration and some technical elements from recent work on SRG isomorphism, overall there is no straightforward generalization of the SRG techniques.

1.3 Individualization/refinement and the automorphism bound

Let $\mathrm{Iso}(\mathfrak{X}, \mathfrak{Y})$ denote the set of isomorphisms from $\mathfrak{X}$ to $\mathfrak{Y}$, and $\mathrm{Aut}(\mathfrak{X}) = \mathrm{Iso}(\mathfrak{X}, \mathfrak{X})$.

The *individualization/refinement* (I/R) method is a classic approach to GI. *Individualization* means the assignment

of individual colors to some vertices; then the irregularity so created propagates via some canonical color refinement process. For a class $\mathcal{C}$ of configurations, an assignment $\mathfrak{X} \mapsto \mathfrak{X}'$ is a *color refinement* if $\mathfrak{X}, \mathfrak{X}' \in \mathcal{C}$ have the same set of vertices and the coloring of $\mathfrak{X}'$ is a refinement of the coloring of $\mathfrak{X}$. Such an assignment is *canonical* if for all $\mathfrak{X}, \mathfrak{Y} \in \mathcal{C}$, we have $\mathrm{Iso}(\mathfrak{X}, \mathfrak{Y}) = \mathrm{Iso}(\mathfrak{X}', \mathfrak{Y}')$. In particular, $\mathrm{Aut}(\mathfrak{X}) = \mathrm{Aut}(\mathfrak{X}')$.

The simplest canonical color refinement process is the *naive vertex refinement*. The edge-colors do not change, only the vertex-colors are refined. The refined color of vertex u of the configuration $\mathfrak{X}$ encodes the following information: the current color of u and the number of vertices v of color i such that $c(u, v) = j$, for every pair (i, j), where i is a vertex-color and j is an edge-color. Naive vertex refinement is the only color refinement used in the present paper. We note that it can be performed in polynomial time.

Repeated application of the refinement process leads to the *stable refinement* after at most $n - 1$ rounds.

If after individualizing the elements of a set $S \subseteq V$, all vertices get different colors in the resulting stable refinement, we say that S *completely splits* $\mathfrak{X}$ (with respect to the given canonical refinement process).

The following lemma is standard (see, e.g., [5, Section 2]).

LEMMA 2. *Let $\mathcal{C}$ be a class of configurations, and suppose that for every $\mathfrak{X} \in \mathcal{C}$ there is set of α vertices that completely splits $\mathfrak{X}$ with respect to a polynomial-time canonical color refinement process. Then the following statements hold for every $\mathfrak{X} \in \mathcal{C}$:*

1. *$|\mathrm{Aut}(\mathfrak{X})| \le n^\alpha$;*
2. *a canonical form can be computed in time $n^{\alpha+O(1)}$;*
3. *for every $\mathfrak{Y} \in \mathcal{C}$, the set of isomorphisms from $\mathfrak{X}$ to $\mathfrak{Y}$ can be listed in time $n^{\alpha+O(1)}$.*

In particular, I/R can efficiently split a configuration $\mathfrak{X}$ only if $\mathfrak{X}$ has a small automorphism group. There are, however, PCCs with large automorphism groups. Next, we define such classes.

Given a graph H, the *line-graph* $L(H)$ has as vertices the edges of H, with two vertices adjacent in $L(H)$ if the corresponding edges are incident in H. The *triangular graph* $T(m)$ is the line-graph of the complete graph K_m (so $n = \binom{m}{2}$). The *lattice graph* $L_2(m)$ is the line-graph of the complete bipartite graph $K_{m,m}$ (on equal parts) (so $n = m^2$).

Definition 3. A PCC is *exceptional* if it is of the form $\mathfrak{X}(G)$, where G is isomorphic to the complete graph K_n, the triangular graph $T(m)$, or the lattice graph $L_2(m)$, or the complement of such a graph.

We remark that it is easy to recognize an exceptional PCC from its clique structure and create a canonical form in polynomial time.

The exceptional PCCs have $n^{\Omega(\sqrt{n})}$ automorphisms. Our main result implies that all the non-exceptional PCCs have far fewer automorphisms.

THEOREM 4 (MAIN). *Given a non-exceptional PCC $\mathfrak{X}$, there exists a set of $\widetilde{O}(n^{1/3})$) vertices that completely splits $\mathfrak{X}$. In particular, $|\mathrm{Aut}(\mathfrak{X})| \le \exp(\widetilde{O}(n^{1/3}))$ and we can find a canonical form for $\mathfrak{X}$ in time $\exp(\widetilde{O}(n^{1/3}))$.*

(The class $\mathcal{C}$ within which we perform individualization and refinement is the class of non-exceptional PCCs along with their vertex-refinements.)

Separating the exceptional PCCs from those PCCs which are split by a small set is a key challenge we had to overcome. As mentioned above, Spielman achieved such a separation in the context of SRGs via Neumaier's classification of SRGs [20], but no such classification is available for PCCs. Instead, we find "clique geometries" in PCCs in a certain range of the parameters (see Section 2), and use them to either recognize one of the exceptional PCCs or apply I/R to find a canonical form.

Our main result represents progress toward the following decades-old conjecture of Babai (cf. [4]).

CONJECTURE 5 (BABAI). *For all $\varepsilon > 0$, there is some N_ε such that if $\mathfrak{X}$ is a primitive coherent configuration on $n \ge N_\varepsilon$ vertices and $|\mathrm{Aut}(\mathfrak{X})| \ge \exp(n^\varepsilon)$ then $\mathrm{Aut}(\mathfrak{X})$ is a primitive permutation group.*

Babai proved the conjecture for all $\varepsilon > 1/2$, and our Theorem 4 extends it to all $\varepsilon > 1/3$.

Progress on Babai's conjecture is significant in part because the detailed classification of large primitive permutation groups due to Cameron [12] implies, as pointed out in [4], that isomorphism of CCs with primitive automorphism groups of order greater than $\exp(n^\varepsilon)$ can be tested in polynomial time. Hence, confirmation of the conjecture would raise hope that an analysis of I/R could give a subexponential-time isomorphism test for PCCs.

Acknowledgements

The authors are grateful to László Babai for sparking our interest in the problem addressed in this paper, providing insight into primitive coherent configurations and primitive groups, uncovering a faulty application of previous results in an early version of the paper, and giving invaluable assistance in framing the results in a compelling and readable manner.

2. STRUCTURE THEORY OF PRIMITIVE COHERENT CONFIGURATIONS

To prove Theorem 4, we need to develop a structure theory of PCCs. The overview in this section highlights the main components of our structure theory.

Throughout the paper, $\mathfrak{X}$ will denote a PCC of rank r on vertex set V with structure constants p^i_{jk} for $0 \le i, j, k \le r - 1$. **We assume throughout that** $r > 2$, since the case $r = 2$ is the trivial case of $\mathfrak{X}(K_n)$, listed as one of our exceptional PCCs.

For any color i in a PCC, we write $n_i = n_{i^*} = p^0_{ii^*} = p^0_{i^*i}$, the out-degree of each vertex in $\mathfrak{X}_i$.

Two colors, 0 and 1, will play a special role. Recall that $R_0 = \Delta$ is the diagonal. Without loss of generality, **we assume throughout that** $n_1 = \max_i n_i$. We write $\rho = \sum_{i \ge 2} n_i = n - n_1 - 1$.

We say that color 1 is *dominant* if $n_1 \ge n/2$, i.e., $\rho < n/2$. Colors $i > 1$ are *nondominant*. We call a pair of distinct vertices dominant (nondominant) when its color is dominant (nondominant, resp.). We say color i is *symmetric* if $i^* = i$. Note that when color 1 is dominant, it is symmetric, since $n_{1^*} = n_1 \ge n/2$.

Let $G(\mathfrak{X})$ be the graph on V formed by the nondominant pairs. So $G(\mathfrak{X})$ is regular of valency ρ, and every pair of distinct nonadjacent vertices in $G(\mathfrak{X})$ has exactly μ common neighbors, where $\mu = \sum_{i,j\geq 2} p^1_{ij}$. The graph $G(\mathfrak{X})$ is not generally SR, since pairs of adjacent vertices in $G(\mathfrak{X})$ of different colors in $\mathfrak{X}$ will in general have different numbers of common neighbors. However, intuition from SRGs will prove valuable in understanding $G(\mathfrak{X})$.

For a color i and vertex u, we denote by $\mathfrak{X}_i(u)$ the set of vertices v such that $c(u,v) = i$. We write $N(u)$ for the set of neighbors of u in the graph $G(\mathfrak{X})$. For i nondominant, we define $\lambda_i = |\mathfrak{X}_i(u) \cap N(v)|$, where $c(u,v) = i$. So, the parameters λ_i are loosely analogous to the parameter λ of a SRG.

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.

We use the notation $\alpha_k \sim \beta_k$ for asymptotic equality ($\lim_{k\to\infty} \alpha_k/\beta_k = 1$). The asymptotic inequality $\alpha_k \lesssim \beta_k$ means $\beta_k \sim \max\{\alpha_k, \beta_k\}$. To interpret asymptotic inequalities involving the parameters of a PCC, we think of the PCC as belonging to an infinite family in which the asymptotic inequalities hold.

Definition 6. A **clique geometry** on a CC $\mathfrak{X}$ is a collection $\mathcal{G}$ of maximal cliques in $G(\mathfrak{X})$ such that every pair of adjacent vertices in $G(\mathfrak{X})$ belongs to a unique clique in $\mathcal{G}$. The clique geometry $\mathcal{G}$ is **asymptotically uniform** (for an infinite family of PCCs) if for every $C \in \mathcal{G}$, $u \in C$, and nondominant color i, we have either $|C \cap \mathfrak{X}_i(u)| \sim \lambda_i$ or $|C \cap \mathfrak{X}_i(u)| = 0$ (as $n \to \infty$).

We have the following sufficient condition for the existence of clique geometries in PCCs.

THEOREM 7. *Let $\mathfrak{X}$ be a PCC satisfying $\rho = o(n^{2/3})$, and fix a constant $\varepsilon > 0$. If $\lambda_i \geq \varepsilon n^{1/2}$ for every nondominant color i, then for n sufficiently large, there is a clique geometry $\mathcal{G}$ on $\mathfrak{X}$. Moreover, $\mathcal{G}$ is asymptotically uniform.*

Theorem 7 provides a powerful dichotomy for PCCs: either there is an upper bound on some parameter λ_i, or there is a clique geometry. Adapting a philosophy expressed in [5], we note that bounds on λ_i are useful because they limit the correlation between the i-neighborhoods of two random vertices. Similar bounds on the parameter λ of a SRG were used in [5].

On the other hand, Theorem 7 guarantees that if all parameters λ_i are sufficiently large, the PCC has an asymptotically uniform clique geometry. This is our weak analogue of Neumaier's geometric structure. Clique geometries offer their own dichotomy. Geometries with at most two cliques at a vertex can classified; this includes the exceptional PCCs (Theorem 8 below). A far more rigid structure emerges when there are at least three cliques at every vertex. In this case, we exploit the ubiquitous 3-claws (induced $K_{1,3}$ subgraphs) in $G(\mathfrak{X})$ in order to construct a set which completely splits $\mathfrak{X}$ (Lemma 14 (b)).

OVERVIEW OF PROOF OF THEOREM 7. The existence of a weaker clique structure follows from a result of Metsch [18]. (See Lemma 18 below and the comments in the paragraph preceding it.) Specifically, under the hypotheses of Theorem 7, for every nondominant color i and vertex u, there is a partition of $\mathfrak{X}_i(u)$ into cliques of order $\sim \lambda_i$ in $G(\mathfrak{X})$. We call such a collection of cliques a *local clique partition* (referring to the color-i neighborhood of any fixed vertex).

The challenge is to piece together these local clique partitions into a clique geometry. An obstacle is that Metsch's cliques are cliques of $G(\mathfrak{X})$, not $\mathfrak{X}_i$; that is, the edges of the cliques partitioning $\mathfrak{X}_i(u)$ have nondominant colors but not in general color i. In particular, for two vertices $u, v \in V$ with $c(u,v) = i$, the clique containing v in the partition of $\mathfrak{X}_i(u)$ may not correspond to any of the cliques in the partition of $\mathfrak{X}_i(v)$.

We first generalize these local structures. An *I-local clique partition* is a partition of $\bigcup_{i\in I} \mathfrak{X}_i(u)$ into cliques of order $\sim \sum_{i\in I} \lambda_i$. We study the maximal sets I for which such I-local clique partitions exist, and eventually prove that these maximal sets I partition the set of nondominant colors, and the corresponding cliques are maximal in $G(\mathfrak{X})$.

Finally, we prove a symmetry condition: given a nondominant pair of vertices $u, v \in V$, the maximal local clique at u containing v is equal to the maximal local clique at v containing u. This symmetry ensures the cliques form a clique geometry, and this clique geometry is asymptotically uniform by construction.

The details of the proof are given in Section 5. □

The case that $\mathfrak{X}$ has a clique geometry with some vertex belonging to at most two cliques includes the exceptional CCs corresponding to $L(K_m)$ and $L(K_{m,m})$. We give the following classification.

THEOREM 8. *Let $\mathfrak{X}$ be a PCC such that $\rho = o(n^{2/3})$. Suppose that $\mathfrak{X}$ has an asymptotically uniform clique geometry $\mathcal{G}$ and a vertex $u \in V$ belonging to at most two cliques of $\mathcal{G}$. Then for n sufficiently large, one of the following is true:*

(1) $\mathfrak{X}$ has rank three and is isomorphic to $\mathfrak{X}(L(K_m))$ or $\mathfrak{X}(L(K_{m,m}))$;

(2) $\mathfrak{X}$ has rank four, $\mathfrak{X}$ has a non-symmetric non-dominant color i, and $G(\mathfrak{X})$ is isomorphic to $L(K_m)$ for $m = n_i + 2$.

Before sketching a proof of Theorem 8, we state Lemma 9, which demonstrates some of the power of the inequality $\rho = o(n^{2/3})$.

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

LEMMA 9. *Let $\mathfrak{X}$ be a PCC with $\rho = o(n^{2/3})$. Then, for n sufficiently large, $\mathrm{dist}_i(1) = 2$ for every nondominant color i. Consequently, $n_i \geq \sqrt{n-1}$ for $i \neq 0$.*

OVERVIEW OF PROOF OF LEMMA 9. We will in fact prove that if $\mathrm{dist}_i(1) \geq 3$ for some color i, then $\rho \gtrsim n^{2/3}$. Without loss of generality, we assume $n_1 \sim n$, since otherwise we are already done.

Fixing an arbitrary vertex u, we consider the bipartite graph B between $\mathfrak{X}_i^{(\delta-1)}(u)$ and $\mathfrak{X}_1(u)$, with an edge from $x \in \mathfrak{X}_i^{(\delta-1)}(u)$ to $y \in \mathfrak{X}_1(u)$ when $c(x,y) = i$. By the coherence of $\mathfrak{X}$, the bipartite graph is regular on $\mathfrak{X}_1(u)$; call its degree γ. An obstacle to our analysis is that the graph need

not be biregular. Nevertheless, we estimate the maximum degree β of a vertex in $\mathfrak{X}_i^{(\delta-1)}(u)$ in B. We first note that $n_1\gamma \le \beta\rho$.

Let w be a vertex satisfying $c(u,w) = i$. We pass to the subgraph B' induced on $(\mathfrak{X}_i^{(\delta-2)}(w), \mathfrak{X}_i^{(\delta-1)}(w))$, and observe that the degree of vertices in $\mathfrak{X}_i^{(\delta-1)}(u) \cap \mathfrak{X}_i^{(\delta-2)}(w)$ is preserved, while the degree of vertices in $\mathfrak{X}_1(u) \cap \mathfrak{X}_i^{(\delta-1)}(w)$ does not increase. Let v be a vertex of degree β in B', and let $j = c(w,v)$. We finally consider the bipartite graph B'' on $(\mathfrak{X}_j(w), X_w)$, where X_w is the set of vertices $x \in \mathfrak{X}_i^{(\delta-1)}(w)$ with at most γ in-neighbors in $\mathfrak{X}_i$ lying in the set $\mathfrak{X}_j(w)$. In particular, $\mathfrak{X}_1(u) \cap \mathfrak{X}_i^{(\delta-1)}(w) \subseteq X_w$. This graph B'' is now regular (of degree $\ge \beta$) on $\mathfrak{X}_j(w)$. Since $X_w \subseteq \mathfrak{X}_i^{(\delta-1)}(w)$, we have $|X_w| \le \rho$, which eventually gives the bound $\beta \le \gamma\rho^2/n_1$. Combining this with our earlier estimate $\beta\rho \ge n_1\gamma$ proves the lemma.

The details of the proof are deferred to the full paper. □

Overview of proof of Theorem 8. We first use the coherence of $\mathfrak{X}$ to show that every vertex $u \in V$ belongs to exactly two cliques of $\mathcal{G}$, and these cliques have order $\sim \rho/2$. By counting vertex-clique incidences, we then obtain the estimate $\rho \lesssim 2\sqrt{2n}$. On the other hand, by Lemma 9, every nondominant color i satisfies $n_i \gtrsim \sqrt{n}$. Hence, there are at most 2 nondominant colors.

Since every vertex belongs to exactly two cliques, the graph $G(\mathfrak{X})$ is the line-graph of a graph. If there is only one nondominant color, then $G(\mathfrak{X})$ is strongly regular, and therefore, for n sufficiently large, $G(\mathfrak{X})$ is isomorphic to $L(K_m)$ or $L(K_{m,m})$. On the other hand, if there are two nondominant colors, by counting paths of length 2 we show that $G(\mathfrak{X})$ must again be isomorphic to $L(K_m)$. By studying the edge-colors at the intersection of the cliques containing two distinct vertices and exploiting the coherence of $\mathfrak{X}$, we finally eliminate the case that the two nondominant colors are symmetric.

The details of the proof are deferred to the full paper. □

For a nondominant color i and vertex u, the *δ-sphere* $\mathfrak{X}_i^{(\delta)}(u)$ in $\mathfrak{X}_i$ centered at u is the set of vertices v with $\mathrm{dist}_i(u,v) = \delta$.

Our last main structural result for PCCs is the following lower bound on the growth of spheres.

Lemma 10 (Growth of spheres). *Let $\mathfrak{X}$ be a PCC, let $i,j \ge 1$ be nondiagonal colors, let $\delta = \mathrm{dist}_i(j)$, and $u \in V$. Then for any integer $1 \le \alpha \le \delta - 2$, we have*

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

We note that Lemma 10 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.

We will use Lemma 10 to prove Lemma 11 below, which shows that a modest number of individualizations suffice to completely split $\mathfrak{X}$ when ρ is sufficiently large. We thereby reduce to the case that $\rho = o(n^{2/3})$, and so are able to take advantage of the previous structural results of this section.

Overview of proof of Lemma 10. The bipartite subgraphs of $\mathfrak{X}_i$ induced on pairs of the form $(\mathfrak{X}_j(u), \mathfrak{X}_k(u))$, where j,k are colors and u is a vertex, are biregular by the coherence of $\mathfrak{X}_i$. We exploit this biregularity to count shortest paths in $\mathfrak{X}_i$ between a carefully chosen subset of $\mathfrak{X}_i^{(\delta-\alpha)}(u)$ and $\mathfrak{X}_j(u)$, for an arbitrary vertex u.

The details of the proof are deferred to the full paper. □

3. OVERVIEW OF ANALYSIS OF ALGORITHM

We now give a high-level overview of how we apply our structure theory of PCCs to prove Theorem 4.

The structural results highlighted in Section 2 usually assumed that $\rho = o(n^{2/3})$. Hence, the first step is to reduce to this case, which we accomplish via the following lemma.

Lemma 11. *Let $\mathfrak{X}$ be a PCC. If $\rho \ge n^{2/3}(\log n)^{-1/3}$, then there is a set of size $O(n^{1/3}(\log n)^{4/3})$ which completely splits $\mathfrak{X}$.*

We remark that in the case that the rank r of $\mathfrak{X}$ is bounded, our Lemma 11 follows from a theorem of Babai [3, Theorem 2.4]. Following Babai [3], we analyze the distinguishing number.

Definition 12. Let $u,v \in V$. We say $w \in V$ **distinguishes** u and v if $c(w,u) \ne c(w,v)$. We write $D(u,v)$ for the set of vertices w distinguishing u and v, and $D(i) = |D(u,v)|$ where $c(u,v) = i$. We call $D(i)$ the **distinguishing number** of i.

Hence, $D(i) = \sum_{j \ne k} p^i_{jk^*}$. If $w \in D(u,v)$, then after individualizing w and refining, u and v get different colors.

Babai observed that in order to completely split a PCC $\mathfrak{X}$, it suffices to individualize some set of $O(n \log n / D_{\min})$ vertices, where $D_{\min} = \min_{i \ne 0}\{D(i)\}$ [3, Lemma 5.4]. Thus, to prove Lemma 11, we show that if $\rho \ge n^{2/3}(\log n)^{-1/3}$ then for every color $i \ne 0$, we have $D(i) = \Omega(n^{2/3}(\log n)^{-1/3})$.

The following bound on the number of large colors in a PCC becomes powerful when $D(i)$ is small.

Lemma 13. *Let $\mathfrak{X}$ be a PCC. For any nondiagonal color i, the number of colors j such that $n_j > n_i/2$ is at most $O((\log n + n/\rho)D(i)/n_i)$.*

Overview of proof of Lemma 13. Let I_α denote the set of colors i such that $D(i) \le \alpha$, and let J_β denote the set of colors j such that $n_j \le \beta$. For a set I of colors, let $n_I = \sum_{i \in I} n_i$ be the total degree of the colors in I.

First, we prove that $\lfloor \alpha/(3D(i)) \rfloor n_i \le n_{I_\alpha}$, a lower bound on the total degree of colors with distinguishing number $\le \alpha$. Next, we prove a lemma that allows us to transfer estimates for the total degree of colors with small distinguishing number into estimates for the total degree of colors with low degree. Specifically, we prove that $n_{J_\beta} \le 2\alpha$, where $\beta = n_{I_{\alpha/2}}$. Together, these two results allow us to transfer estimates on total degree between the sets I_α and J_β, as α and β increase.

The details of the proof are deferred to the full paper. □

Overview of proof of Lemma 11. Fix a color $i \ge 1$. We wish to give a lower bound on $D(i)$. Babai observed that for any color $j \ge 1$, we have $D(i) \ge D(j)/\mathrm{dist}_i(j)$ [3, Proposition 6.4 and Theorem 6.1]). Hence, we wish to give an upper bound on $\mathrm{dist}_i(j)$ for some color j with $D(j)$ large.

We analyze two cases: $n^{2/3}(\log n)^{-1/3} \le \rho < n/3$ and $\rho \ge n/3$.

In the former case, when $n^{2/3}(\log n)^{-1/3} \le \rho < n/3$, we first observe that $D(1) = \Omega(\rho)$. Hence, the problem is reduced to bounding the quantity $\mathrm{dist}_i(1)$ for every color i.

Our bound in Lemma 10 on the size of spheres suffices for this task since n_1 is large.

In the case that $\rho \geq n/3$, Babai observed that the color j maximizing $D(j)$ satisfies $D(j) = \Omega(n)$. We partition the colors of $\mathfrak{X}$ according to their distinguishing number, by first partitioning the positive integers less than $D(j)$ into cells of length $3D(i)$. (Specifically, we partition the colors of $\mathfrak{X}$ so that the α-th cell contains the colors k satisfying $3D(i)\alpha \leq D(k) < 3D(i)(\alpha+1)$, and there are $O(D(j)/D(i))$ cells.) Each cell of this partition $\mathcal{P}$ is nonempty. In fact, we show that the sum of the degrees of the colors in each cell is at least n_i.

On the other hand, Lemma 13 says that there are few colors k satisfying $n_k > n_i/2$, and we show that the total degree of the colors k with $n_k \leq n_i/2$ is also small. Since each cell of the partition has degrees summing to at least n_i, these together give an upper bound on the number of cells, and hence a lower bound on $D(i)$.

The details of the proof are deferred to the full paper. □

We have now reduced to the case that $\rho = o(n^{2/3})$. Our analysis of this case is inspired by Spielman's analysis of SRGs [21].

LEMMA 14. *There exists a constant $\varepsilon > 0$ such that the following holds. Let $\mathfrak{X}$ be a PCC with $\rho = o(n^{2/3})$. If $\mathfrak{X}$ satisfies either of the following conditions, then there is a set of $O(n^{1/4}(\log n)^{1/2})$ vertices which completely splits $\mathfrak{X}$.*

(a) There is a nondominant color i such that $\lambda_i < \varepsilon n^{1/2}$.

(b) For every nondominant color i, we have $\lambda_i \geq \varepsilon n^{1/2}$. Furthermore, $\mathfrak{X}$ has an asymptotically uniform clique geometry $\mathcal{C}$ such that every vertex belongs to at least three cliques of $\mathcal{C}$.

OVERVIEW OF PROOF OF LEMMA 14. We will show that if we individualize a random set of $O(n^{1/4}(\log n)^{1/2})$ vertices, then with positive probability, every pair of distinct vertices gets different colors in the stable refinement.

Let $u, v \in C$, and fix two colors i and j. Generalizing a pattern studied by Spielman, we say a triple (w, x, y) is good for u and v if $c(u, x) = c(u, y) = c(x, y) = 1$, $c(u, w) = i$, and $c(w, x) = c(w, y) = j$, but there exists no vertex z such that $c(v, z) = i$ and $c(z, x) = c(z, y) = j$. To ensure that u and v get different colors in the stable refinement, it suffices to individualize two vertices $x, y \in V$ for which there exists a vertex w such that (w, x, y) is good for u and v. We show that if there are many good triples for u and v, then individualizing a random set of $O(n^{1/4}(\log n)^{1/2})$ vertices is overwhelming likely to result in the individualization of such a pair $x, y \in V$.

Condition (a) of the lemma is analogous to the asymptotic consequences of Neumaier's claw bound used by Spielman [21] (cf. [9, Section 2.2]), except that the bound on λ_i does not imply a similar bound on λ_{i^*}. We show that a relatively weak bound on λ_{i^*} already suffices for Spielman's argument to essentially go through. However, if even this weaker assumption fails, then we turn to our local clique structure for the analysis (as described in the overview of Theorem 7).

When condition (b) holds, we cannot argue along Spielman's lines, and instead analyze the structural properties of our clique geometries to estimate the number of good triples.

The details of the proof are deferred to the full paper. □

By Theorem 7, either the hypotheses of of Lemma 14 are satisfied, or $\mathfrak{X}$ has an asymptotically uniform clique geometry $\mathcal{C}$, and some vertex belongs to at most two cliques of $\mathcal{C}$. Theorem 8 gives a characterization PCCs $\mathfrak{X}$ with the latter property: $\mathfrak{X}$ is one of the exceptional PCCs, or $\mathfrak{X}$ has rank four with a non-symmetric non-dominant color i and $G(\mathfrak{X})$ is isomorphic to $L(K_m)$ for $m = n_i + 2$. We handle this final case via the following lemma. The proof is deferred to the full paper.

LEMMA 15. *Let $\mathfrak{X}$ be a PCC satisfying Theorem 8 (2). Then some set of size $O(\log n)$ completely splits $\mathfrak{X}$.*

We conclude this overview by observing that Theorem 4 follows from the above results.

PROOF OF THEOREM 4. Let $\mathfrak{X}$ be a PCC. Suppose first that $\rho \geq n^{2/3}(\log n)^{-1/3}$. Then by Lemma 11, there is a set of size $O(n^{1/3}(\log n)^{4/3})$ which completely splits $\mathfrak{X}$.

Otherwise, $\rho < n^{2/3}(\log n)^{-1/3} = o(n^{2/3})$. By Theorem 7, either the hypotheses of Lemma 14 are satisfied, or the hypotheses of Theorem 8 are satisfied. In the former case, some set of $O(n^{1/4}(\log n)^{1/2})$ vertices completely splits $\mathfrak{X}$. In the latter case, either $\mathfrak{X}$ is exceptional, or, by Lemma 15, some set of $O(\log n)$ vertices completely splits $\mathfrak{X}$. □

4. PRELIMINARY OBSERVATIONS

In this section, we give some basic observations about PCCs that will be useful in the following technical sections.

We recall that when color 1 is dominant, it is symmetric. In this case, we recall our notation $\mu = |N(x) \cap N(y)|$, where $x, y \in V$ are any pair of vertices with $c(x, y) = 1$ and $N(x)$ is the nondominant neighborhood of x. Hence, $\mu = \sum_{i,j>1} p^1_{ij}$.

LEMMA 16. *Let $\mathfrak{X}$ be a PCC with $n_1 \geq n/2$. Then $\mu \leq \rho^2/n_1$.*

PROOF. Fix a vertex u. There are at most ρ^2 paths of length two from u along edges of nondominant color, and exactly n_1 vertices v such that $c(u, v) = 1$. For any such vertex y, there are exactly μ paths of length two from u to v along edges of nondominant color. Hence, $\mu \leq \rho^2/n_1$. □

PROPOSITION 17. *Let $\mathfrak{X}$ be a PCC with $\rho = o(n^{2/3})$. Then $\mu = o(n^{1/3})$ and $\mu\rho = o(n)$.*

PROOF. By Lemma 16, $\mu \leq \rho^2/n_1 = o(n^{1/3})$, and then $\mu\rho = o(n)$. □

5. CLIQUE GEOMETRIES

In this section, we prove Theorem 7, giving sufficient conditions for the existence of an asymptotically uniform clique geometry in a PCC.

We use the word "geometry" in Definition 6 because the cliques resemble lines in a geometry: two distinct cliques intersect in at most one vertex. Indeed, a regular graph G has a clique geometry $\mathcal{G}$ with cliques of uniform order only if it is the point-graph of a geometric 1-design with lines corresponding to cliques of $\mathcal{G}$.

Theorem 7 builds on earlier work of Metsch [18] on the existence of similar clique structures in "sub-amply regular graphs" (cf. [9]) via the following lemma. The lemma can be derived from [18, Theorem 1.2], but see [9, Lemma 4] for a self-contained proof.

LEMMA 18. *Let H be a graph on k vertices which is regular of degree λ and such that any pair of nonadjacent vertices have at most μ common neighbors. Suppose that $k\mu = o(\lambda^2)$. Then there is a partition of $V(H)$ into maximal cliques of order $\sim \lambda$, and all other maximal cliques of H have order $o(\lambda)$.*

Metsch's result, applied to the graphs induced by $G(\mathfrak{X})$ on sets of the form $\mathfrak{X}_i(u)$, gives collections of cliques which locally resemble asymptotically uniform clique geometries. These collections satisfy the following definition for a set $I = \{i\}$ containing a single color.

Definition 19. Let I be a set of nondominant colors. An **I-local clique partition** at a vertex u is a collection $\mathcal{P}$ of subsets of $\mathfrak{X}_I(u)$ satisfying the following properties:

1. $\mathcal{P}$ is a partition of $\mathfrak{X}_I(u)$ into maximal cliques in the subgraph of $G(\mathfrak{X})$ induced on $\mathfrak{X}_I(u)$;
2. for every $C \in \mathcal{P}_u$ and $i \in I$, we have $|C \cap \mathfrak{X}_i(u)| \sim \lambda_i$.

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

To prove Theorem 7, we will stitch local clique partitions together into geometric clique structures.

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

COROLLARY 20. *Let $\mathfrak{X}$ be a PCC and let i be a nondominant color such that $n_i\mu = o(\lambda_i^2)$. Then $\mathfrak{X}$ has $\{i\}$-local clique partitions.*

PROOF. Fix a vertex u, and apply Lemma 18 to the graph H induced by $G(\mathfrak{X})$ on $\mathfrak{X}_i(u)$. The Lemma gives a collection of cliques satisfying Definition 19. □

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

LEMMA 21. *Let $\mathfrak{X}$ be a PCC, let i be a nondominant color such that $n_i\mu = o(\lambda_i^2)$, 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 $u \in V$, there is a unique I-local clique partition $\mathcal{P}$ at u.*

PROOF. Let $u \in V$ and let $\mathcal{P}$ be an I-local clique partition at u. Let C and C' be two distinct maximal cliques in the subgraph of $G(\mathfrak{X})$ induced on $\mathfrak{X}_I(u)$. We show that $|C \cap C'| < \mu$. Suppose for the contradiction that $|C \cap C'| \geq \mu$. For a vertex $v \in C \setminus C'$, we have $|N(v) \cap (C' \cup \{u\})| > \mu$, and so $C' \subseteq N(v)$ by Observation 24. But since $v \notin C'$, 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 $\mathfrak{X}_I(u)$. Since $\mathcal{P}$ is an I-local clique partition, it follows that

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

Then C does not belong to an I-local clique partition, since it fails to satisfy Property 2 of Definition 19. □

5.1 Local cliques and symmetry

Suppose $\mathfrak{X}$ has I-local clique partitions, and $c(u,v) \in I$ for some $u, v \in V$. We remark that in general, the clique containing v in the I-local clique partition at u will not be in any way related to any clique in the I-local clique partition at v. In particular, we need not have $c(v,u) \in I$. However, even when $c(v,u) \in I$ as well, there is no guarantee that the clique at u containing v will have any particular relation to the clique at v containing u. This lack of symmetry is a fundamental obstacle that we must overcome to prove Theorem 7.

Lemma 23 below is the main result of this subsection. It gives sufficient conditions on the parameters of a PCC for finding the desired symmetry in local clique partitions satisfying the following additional condition.

Definition 22. Let I be a set of nondominant colors, let $u \in V$, and let $\mathcal{P}$ be an I-local clique partition at u. We say $\mathcal{P}$ is **strong** if for every $C \in \mathcal{P}$, the clique $C \cup \{u\}$ 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 $u \in V$.

We introduce additional notation. Suppose I is a set of nondominant colors, and $i \in I$ satisfies $n_i\mu = o(\lambda_i)^2$. If $\mathfrak{X}$ has I-local clique partitions, then for every $u, v \in V$ with $c(u,v) \in I$, we denote by $K_I(u,v)$ the set $C \cup \{u\}$, where C is the clique in the partition of $\mathfrak{X}_I(u)$ containing v (noting that by Lemma 21, this clique is uniquely determined).

LEMMA 23. *Let $\mathfrak{X}$ be a PCC with $\rho = o(n^{2/3})$, 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 $\lambda_i\lambda_{i^*} = \Omega(n)$. Then for every $u, v \in V$ with $c(u,v) = i$, we have $K_I(u,v) = K_J(v,u)$.*

The following simple observation is essential for what follows.

OBSERVATION 24. *Let $\mathfrak{X}$ be a PCC, let C be a clique in $G(\mathfrak{X})$, and suppose $u \in V \setminus C$ is such that $|N(u) \cap C| > \mu$. Then $C \subseteq N(u)$.*

PROOF. Suppose there exists a vertex $v \in C \setminus N(u)$, so $c(u,v) = 1$. Then $|N(u) \cap N(v)| = \mu$ by the definition of μ in a PCC. But

$$\begin{aligned}|N(u) \cap N(v)| &\geq |N(u) \cap C \cap N(v)| = |N(u) \cap (C \setminus \{v\})| \\ &= |N(u) \cap C| > \mu,\end{aligned}$$

a contradiction. □

COROLLARY 25. *Let $\mathfrak{X}$ be a PCC 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 $u, v, x, y \in V$ we have $|K_I(u,v) \cap K_J(x,y)| > \mu$. Then $K_I(u,v) = K_J(x,y)$.*

PROOF. Suppose there exists $z \in K_J(x,y) \setminus K_I(u,v)$. We have $|N(z) \cap K_I(u,v)| \geq |K_J(x,y) \cap K_I(u,v)| > \mu$. Then $K_I(u,v) \subseteq N(z)$ by Observation 24, contradicting the maximality of $K_I(u,v)$. Thus, $K_J(x,y) \subseteq K_I(u,v)$. Similarly, $K_I(u,v) \subseteq K_J(x,y)$. □

PROOF OF LEMMA 23. Without loss of generality, assume $\lambda_i \leq \lambda_{i^*}$.

Suppose for contradiction that there exists a vertex $u \in V$ such that for *every* $v \in \mathfrak{X}_i(u)$, we have $K_I(u,v) \neq K_J(v,u)$. Then $|K_I(u,v) \cap K_J(v,u)| \leq \mu$ by Corollary 25. Fix $v \in$

$\mathfrak{X}_i(u)$, so for every $w \in K_I(u,v) \cap \mathfrak{X}_i(u)$, we have $|K_J(w,u) \cap K_I(u,v)| \le \mu$. Hence, there exists some sequence $w_1, \dots, w_\ell$ of $\ell = \lceil \lambda_i/(2\mu) \rceil$ vertices $w_\alpha \in K_I(u,v) \cap \mathfrak{X}_i(u)$ such that $K_J(w_\alpha, u) \neq K_J(w_\beta, u)$ for $\alpha \neq \beta$. But by Corollary 25, for $\alpha \neq \beta$ we have $|K_J(w_\alpha, u) \cap K_J(w_\beta, u)| \le \mu$. Hence, for any $1 \le \alpha \le \ell$ we have

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

But $K_J(w_\alpha, u) \subseteq N(u)$, so

$$|N(u)| \ge \left| \bigcup_{\alpha=1}^{\ell} K_J(w_\alpha, u) \right| \gtrsim \frac{\lambda_i \lambda_{i^*}}{4\mu} = \omega(\rho)$$

by Proposition 17. This contradicts the definition of ρ.

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

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

by Proposition 17. Since the J-local clique partition at v partitions $\mathfrak{X}_{i^*}(v)$ into $\sim n_i/\lambda_{i^*}$ cliques, at least one of these intersects $K_I(u,v)$ in at least $\sim \lambda_{i^*}^2/n_i = \omega(\mu)$ vertices. In other words, there is some $x \in \mathfrak{X}_{i^*}(v)$ such that $|K_J(v,x) \cap K_I(u,v)| = \omega(\mu)$. But then $K_J(v,x) = K_I(u,v)$ by Corollary 25. In particular, $u \in K_J(v,x)$, so $K_J(v,x) = K_J(v,u)$. Hence, $K_J(v,u) = K_J(v,x) = K_I(u,v)$, as desired. □

5.2 Existence of strong local clique partitions

Our next step in proving Theorem 7 is showing the existence of strong local clique partitions. We accomplish this via the following lemma.

LEMMA 26. *Let $\mathfrak{X}$ be a PCC such that $\rho = o(n^{2/3})$, and let i be a nondominant color such that $n_i\mu = o(\lambda_i^2)$. Suppose that for every color j with $n_j < n_i$, we have $\lambda_j = \Omega(\sqrt{n})$. Then for n 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 26 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 u and the various neighborhoods $\mathfrak{X}_j(u)$ for $j \notin I$.

LEMMA 27. *Let $\mathfrak{X}$ be a PCC, and let i and j be nondominant colors. Then for any $0 < \varepsilon < 1$ and any $u, v \in V$ with $c(u,v) = j$, we have*

$$|\mathfrak{X}_i(u) \cap N(v)| \le \max\left\{ \frac{\lambda_i + 1}{1-\varepsilon}, n_i\sqrt{\frac{\mu}{\varepsilon n_j}} \right\}$$

PROOF. Fix $u, v \in V$ with $c(u,v) = j$ and let $\alpha = |\mathfrak{X}_i(u) \cap N(v)|$. We count the number of triples (x,y,z) of vertices such that $x, y \in \mathfrak{X}_i(u) \cap N(z)$, with $c(u,z) = j$ and $c(x,y) = 1$. There are at most n_i^2 pairs $x, y \in \mathfrak{X}_i(u)$, and if $c(x,y) = 1$ then there are at most μ vertices z such that $x, y \in N(z)$. Hence, the number of such triples is at most $n_i^2\mu$. On the other hand, by the coherence of $\mathfrak{X}$, for every z with $c(u,z) = j$, we have at least $\alpha(\alpha - \lambda_i - 1)$ pairs $x, y \in \mathfrak{X}_i(u) \cap N(z)$ with $c(x,y) = 1$. Hence, there are at least $n_j\alpha(\alpha - \lambda_i - 1)$ total such triples. Thus, $n_j\alpha(\alpha - \lambda_i - 1) \le n_i^2\mu$.Hence, if $\alpha \le (\lambda_i + 1)/(1-\varepsilon)$, then we are done. Otherwise, $\alpha > (\lambda_i+1)/(1-\varepsilon)$, and then $\lambda_i + 1 < (1-\varepsilon)\alpha$. So, we have $n_i^2\mu \ge n_j\alpha(\alpha - \lambda_i - 1) > \varepsilon n_j \alpha^2$, and then $\alpha < n_i\sqrt{\mu/(\varepsilon n_j)}$. □

LEMMA 28. *Let $\mathfrak{X}$ be a PCC, and let i be a nondominant color such that $n_i\mu = o(\lambda_i^2)$. 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 $n_i\sqrt{\mu/n_j} < (\sqrt{3}/2)\lambda_i$. Let $u \in V$, let $\mathcal{P}_u$ be the I-local clique partition at u, and let $v \in \mathfrak{X}_j(u)$. Suppose some clique $C \in \mathcal{P}_u$ is such that $c(u,v) = j$ and $|N(v) \cap C| \ge \mu$. Then for every vertex $x, y \in V$ with $c(x,y) = j$, letting $\mathcal{P}_x$ be the I-local clique partition at x, the following statements hold:*

(i) there is a unique clique $C \in \mathcal{P}_x$ such that $C \subseteq N(y)$;

(ii) $|N(y) \cap \mathfrak{X}_i(x)| \sim \lambda_i$.

PROOF. Letting $\widehat{C} = C \cup \{u\}$, we have $|\widehat{C} \cap N(v)| \ge \mu + 1 > \mu$. Therefore, by Observation 24, we have $C \subseteq N(v)$. In particular, $|N(v) \cap \mathfrak{X}_i(u)| \gtrsim \lambda_i$, and so by the coherence of $\mathfrak{X}$, $|N(y) \cap \mathfrak{X}_i(x)| \gtrsim \lambda_i$ for every pair $x, y \in V$ with $c(x,y) = j$.

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

$$|N(y) \cap \mathfrak{X}_i(x)| \gtrsim \lambda_i = \omega(\mu n_i/\lambda_i). \tag{1}$$

Then it follows from the pigeonhole principle that for n sufficiently large, there is some clique $C \in \mathcal{P}_x$ such that $|N(y) \cap C| > \mu$, and then $C \subseteq N(y)$ by Observation 24.

Now suppose for contradiction that there is some clique $C' \in \mathcal{P}_x$ with $C' \neq C$, such that $C' \subseteq N(y)$.

$$|N(y) \cap \mathfrak{X}_i(x)| \ge |C \cup C'| \gtrsim 2\lambda_i \sim 2(\lambda_i + 1) \tag{2}$$

(with the last relation holding since $\lambda_i = \omega(\sqrt{n_i\mu}) = \omega(1)$.) However, by Lemma 27 with $\varepsilon = 1/3$, we have

$$|\mathfrak{X}_i(x) \cap N(y)| \le \max\left\{ \frac{3}{2}(\lambda_i + 1), n_i\sqrt{\frac{3\mu}{n_j}} \right\} = \frac{3}{2}(\lambda_i + 1),$$

with the last equality holding by assumption. This contradicts Eq. (2), so we conclude that C is the unique clique in $\mathcal{P}_x$ satisfying $C \subseteq N(y)$. In particular, by Observation 24, we have $|N(y) \cap C'| \le \mu$ for every $C' \in \mathcal{P}_x$ with $C' \neq C$.

Finally, we estimate $|N(y) \cap \mathfrak{X}_i(x)|$ by

$$|N(y) \cap \mathfrak{X}_i(x) \cap C| + \sum_{C' \neq C} |N(y) \cap \mathfrak{X}_i(x) \cap C'| \lesssim \lambda_i + \mu n_i/\lambda_i \sim \lambda_i,$$

which, combined with Eq. (1), gives $|N(y) \cap \mathfrak{X}_i(x)| \sim \lambda_i$. □

LEMMA 29. *Let $\mathfrak{X}$ be a PCC, and let i be a nondominant color such that $n_i\mu = o(\lambda_i^2)$. 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 $n_i\sqrt{\mu/n_j} = o(\lambda_i)$, let $u \in V$, and let $\mathcal{P}$ be the I-local clique partition at u. Then for any $C \in \mathcal{P}$ and any vertex $v \in \mathfrak{X}_j(u) \setminus C$, we have $|N(v) \cap C| < \mu$.*

PROOF. By Corollary 20, $\mathfrak{X}$ 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 $n_i\sqrt{\mu/n_j} = o(\lambda_i)$, some vertices u, v with $c(u,v) = j$, and some $C \in \mathcal{P}$ with $|N(v) \cap C| \geq \mu$, where $\mathcal{P}$ is the I-local clique partition at u. By Lemma 28, for n sufficiently large, for every vertex $u, v \in V$ with $c(u,v) = j$, and I-local clique partition $\mathcal{P}$ at u, (i) there is a unique clique $C \in \mathcal{P}$ such that $C \subseteq N(v)$, and (ii) we have

$$|N(v) \cap \mathfrak{X}_i(u)| \sim \lambda_i. \tag{3}$$

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

$$C' = C \cup \{v \in \mathfrak{X}_j(u) : C \subseteq N(v)\}$$

for every $C \in \mathcal{P}$. Let $J = I \cup \{j\}$. We claim that $\mathcal{P}'$ satisfies Properties 1 and 2 of Definition 19, so $\mathfrak{X}$ has local clique partitions on J. This contradicts the maximality of I, and the lemma then follows.

First we verify Property 1 of Definition 19. By properties (i) and (ii) above, $\mathcal{P}'$ partitions $\mathfrak{X}_J(u)$. Furthermore, the sets $C \in \mathcal{P}'$ are cliques in $G(\mathfrak{X})$, since for any $C \in \mathcal{P}'$ and any distinct $v, w \in C \cap \mathfrak{X}_j(u)$, we have

$$|N(v) \cap N(w)| \geq |C \cap \mathfrak{X}_I(u)| \gtrsim \lambda_i = \omega(\mu)$$

and so $c(v,w)$ 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 $\mathfrak{X}_J(u)$, since by property (ii) above, for any clique $C \in \mathcal{P}'$ and $v \in \mathfrak{X}_J(u) \setminus C$, we have $|N(v) \cap C \cap \mathfrak{X}_I(u)| < \mu$.

We now verify Property 2 of Definition 19. By the pigeonhole principle, there is some $C \in \mathcal{P}'$ with

$$|C \cap \mathfrak{X}_j(u)| \gtrsim \frac{n_j}{|\mathcal{P}'|} = \frac{n_j}{|\mathcal{P}|} \sim \frac{\lambda_i n_j}{n_i}.$$

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

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

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

$$\lambda_j \gtrsim \frac{\lambda_i n_j}{n_i} = \omega(\sqrt{\mu n_j}). \tag{4}$$

Hence, $n_j\mu = o(\lambda_j^2)$, and so by Corollary 20, $\mathfrak{X}$ has $\{j\}$-local clique partitions.

Let $C' \subseteq \mathfrak{X}_j(u)$ be a maximal clique in $G(\mathfrak{X})$ of order $\sim \lambda_j$. By Eq. (3) there are $\sim \lambda_j\lambda_i$ nondominant edges between C' and $\mathfrak{X}_i(u)$, so some $x \in \mathfrak{X}_i(u)$ satisfies

$$|N(x) \cap C'| \gtrsim \lambda_j\lambda_i/n_i = \omega(\lambda_j\sqrt{\mu/n_j}) = \omega(\mu).$$

(The last equality uses Eq. (4).) Furthermore, by Eq. (4), we have

$$n_j \lesssim (n_i/\lambda_i)\lambda_j = o(\sqrt{n_i/\mu}\lambda_j),$$

where the last inequality comes from the assumption that $\sqrt{n_i\mu} = o(\lambda_i)$. So by applying Lemma 28 with $\{j\}$ in place of I, it follows that for every $x \in \mathfrak{X}_i(u)$, we have $|N(x) \cap \mathfrak{X}_j(u)| \sim \lambda_j$.

We count the nondominant edges between $\mathfrak{X}_i(u)$ and $\mathfrak{X}_j(u)$ in two ways: there are $\sim \lambda_j$ such edges at each of the n_i vertices in $\mathfrak{X}_i(u)$, and (by Eq. (3)) there are $\sim \lambda_i$ such edges at each of the n_j vertices in $\mathfrak{X}_j(u)$. Hence, $n_i\lambda_j \sim n_j\lambda_i$.

Now, using Eq. (4), $\mu|\mathcal{P}'| \sim \mu n_i/\lambda_i \sim \mu n_j/\lambda_j = o(\lambda_j)$. By the maximality of the cliques $C \in \mathcal{P}'$ in the subgraph of $G(\mathfrak{X})$ induced on $\mathfrak{X}_J(u)$, for every distinct $C, C' \in \mathcal{P}'$ and $v \in C$, we have $|N(v) \cap C'| \leq \mu$. Therefore, for $v \in C \cap \mathfrak{X}_j(u)$, we have

$$\begin{aligned}\lambda_j - |\mathfrak{X}_j(u) \cap C| &= |\mathfrak{X}_j(u) \cap N(v)| - |\mathfrak{X}_j(u) \cap C| \\ &\leq |(N(v) \cap \mathfrak{X}_j(u)) \setminus C| \\ &\leq \mu|\mathcal{P}'| = o(\lambda_j),\end{aligned}$$

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

Now $\mathcal{P}'$ satisfies Definition 19, giving the desired contradiction. □

PROOF OF LEMMA 26. 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 n_i is minimal for this property, i.e., for every nondominant color j with $n_j < n_i$, 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 29.

Let $u \in V$ be such that some clique C in the I-local clique partition at u is not maximal in $G(\mathfrak{X})$. In particular, let $v \in V \setminus C$ be such that $C \subseteq N(v)$, and let $j = c(u,v)$. Then j is a nondominant color, and $j \notin I$. Furthermore, by the defining property of I (the guarantee of Lemma 29), it is not the case that $n_i\sqrt{\mu/n_j} = o(\lambda_i)$. In particular we may take $n_j < n_i$, since otherwise, if $n_j \geq n_i$, then $n_i\sqrt{\mu/n_j} \leq \sqrt{n_i\mu} = o(\lambda_i)$ by assumption. Now since $n_j < n_i$, also $\lambda_j = \Omega(\sqrt{n})$ by assumption. Furthermore, by the minimality of n_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,

$$|N(v) \cap \mathfrak{X}_i(u)| \geq |N(v) \cap \mathfrak{X}_i(u) \cap C| \gtrsim \lambda_i.$$

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

$$\begin{aligned}|N(y) \cap D \cap \mathfrak{X}_j(u)| &\gtrsim \frac{\lambda_i\lambda_j}{n_i} = \omega\left(\sqrt{\frac{\mu}{n_i}}\lambda_j\right) \\ &= \omega\left(\sqrt{\frac{\mu n}{n_i}}\right) = \omega(\mu).\end{aligned}$$

(The second inequality uses the assumption that $\sqrt{n_i\mu} = o(\lambda_i)$. The last inequality uses Proposition 17.) But then $D \setminus \{y\} \subseteq N(y)$ by Observation 24. Then $y \in D$ 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 7.

PROOF OF THEOREM 7. By Lemma 26, 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 $u, v \in V$ be such that $c(u,v) = i$. By the uniqueness of the induced $\{i\}$-local clique partition at u (Lemma 21), we have

$$|K_I(u,v) \cap K_J(u,v)| \gtrsim \lambda_i = \omega(\mu),$$

so $K_I(u,v) = K_J(u,v)$, 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 $K(u,v) = K_I(u,v)$ whenever $c(u,v) \in I$ and $\mathfrak{X}$ has strong I-local clique partitions. By Lemma 23, we have $K(u,v) = K(v,u)$ for all $u, v \in V$ with $c(u,v)$ nondominant. Let $\mathcal{G}$ be the collection of cliques of the form $K(u,v)$ for $c(u,v)$ nondominant. Then $\mathcal{G}$ is an asymptotically uniform clique geometry. □

6. CONCLUSION

We have given an algorithm for deciding isomorphism of primitive coherent configurations in time $\exp(\widetilde{O}(n^{1/3}))$. In fact, we have proved that except for the readily identified exceptions of K_n, $L(K_n)$, and $L(K_{n,n})$, a PCC is completely split after individualizing $\widetilde{O}(n^{1/3})$ vertices and applying naive color refinement.

Further progress on the isomorphism problem for PCCs may be possible, but a more powerful structure theory for PCCs will be required. For example, we anticipate that a strengthening of Theorem 7 will be helpful. Loosely speaking, it would be desirable to find a broader range of parameters under which PCCs are guaranteed to have some "geometric structure" (which should generalize our clique geometries), as seems the case with the PCCs corresponding to large primitive groups (see Conjecture 5). (The most familiar of these are the Johnson schemes $J(m,k)$ and Hamming schemes $H(k,q)$ for bounded k.)

QUESTION 1. *Is there a range of parameters, including the known PCCs with exponentially many automorphisms, in which a PCC is guaranteed to have "geometric structure?"*

The PCCs with large automorphism groups appearing in Babai's conjecture are all in fact association schemes, i.e., they satisfy $i^* = i$ for every color i. Intuitively, the presence of asymmetric colors should reduce the number of automorphisms. On the other hand, the possibility of asymmetric colors greatly complicates our analysis. Hence, a reduction to the case of assocation schemes would be desirable.

QUESTION 2. *Is it the case that every sufficiently large PCC with at least* $\exp(n^{\Omega(1)})$ *automorphisms is an association scheme?*

7. REFERENCES

[1] L. Babai. Monte Carlo algorithms in graph isomorphism testing. Tech. Report 79–10, Dép. Math. et Stat., Univ. de Montréal, 1979. Available at: `http://people.cs.uchicago.edu/~laci/lasvegas79.pdf`.

[2] L. Babai. On the complexity of canonical labeling of strongly regular graphs. *SIAM J. Comput.*, 9(1):212–216, 1980.

[3] L. Babai. On the order of uniprimitive permutation groups. *Ann. of Math.*, 113(3):553–568, 1981.

[4] L. Babai. On the automorphism groups of strongly regular graphs I. In *Proc. 5th ITCS*, pages 359–368, 2014.

[5] L. Babai, X. Chen, X. Sun, S.-H. Teng, and J. Wilmes. Faster canonical forms for strongly regular graphs. In *Proc. 54th FOCS*, pages 157–166, 2013.

[6] L. Babai and P. Codenotti. Isomorphism of hypergraphs of low rank in moderately exponential time. In *Proc. 49th FOCS*, pages 667–676, 2008.

[7] L. Babai, W. M. Kantor, and E. M. Luks. Computational complexity and the classification of finite simple groups. In *Proc. 24th FOCS*, pages 162–171, 1983.

[8] L. Babai and E. M. Luks. Canonical labeling of graphs. In *Proc. 15th STOC*, pages 171–183, 1983.

[9] L. Babai and J. Wilmes. Asymptotic Delsarte cliques in distance-regular graphs. 2013. To appear: *J. Algebr. Comb.*

[10] L. Babai and J. Wilmes. Quasipolynomial-time canonical form for Steiner designs. In *Proc. 45th STOC*, pages 261–270, 2013.

[11] J.-Y. Cai, M. Fürer, and N. Immerman. An optimal lower bound on the number of variables for graph identification. *Combinatorica*, 12(4):389–410, 1992.

[12] P. J. Cameron. Finite permutation groups and finite simple groups. *Bull. London Math Soc.*, 13:1–22, 1981.

[13] X. Chen, X. Sun, and S.-H. Teng. Multi-stage design for quasipolynomial-time isomorphism testing of Steiner 2-systems. In *Proc. 45th STOC*, pages 271–280, 2013.

[14] R. Frucht. Herstellung von Graphen mit vorgegebener abstrakter Gruppe. *Composition Math.*, 6:239–250, 1938.

[15] O. Goldreich, S. Micali, and A. Wigderson. Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof system. *J. ACM*, 38(1):691–729, 1991.

[16] D. G. Higman. Coherent configurations I. *Geometriae Dedicata*, 4:1–32, 1975.

[17] E. M. Luks. Isomorphism of graphs of bounded valence can be tested in polynomial time. *J. Comput. System Sci.*, 25(1):42–65, 1982.

[18] K. Metsch. On a characterization of bilinear forms graphs. *European Journal of Combinatorics*, 20:293–306, 1999.

[19] G. L. Miller. Graph isomorphism, general remarks. In *Proc. 9th STOC*, pages 143–150, 1977.

[20] A. Neumaier. Strongly regular graphs with smallest eigenvalue $-m$. *Arch. Math.*, 33(4):392–400, 1979.

[21] D. A. Spielman. Faster isomorphism testing of strongly regular graphs. In *Proc. 28th STOC*, pages 576–584, 1996.

[22] B. Weisfeiler, editor. *On Construction and Identification of Graphs*, volume 558 of *Lecture Notes in Mathematics*. Springer-Verlag, 1976.

[23] B. Weisfeiler and A. A. Leman. A reduction of a graph to a canonical form and an algebra arising during this reduction. *Nauchno-Tech. Info.*, 9:12–16, 1968.

[24] V. N. Zemlyachenko, N. M. Korneenko, and R. I. Tyshkevich. Graph isomorphism problem. *Zap. Nauchn. Sem. (LOMI)*, 118:83–158, 215, 1982.