On the Automorphism Groups of Strongly Regular Graphs I

László Babai
University of Chicago
1100 E 58th St
Chicago, IL 60637
laci@cs.uchicago.eduu

To the memory of Ákos Seress (1958–2013)

ABSTRACT

We derive structural constraints on the automorphism groups of strongly regular (s. r.) graphs, giving a surprisingly strong answer to a decades-old problem, with tantalizing implications to testing isomorphism of s. r. graphs, and raising new combinatorial challenges.

S. r. graphs, while not believed to be Graph Isomorphism (GI) complete, have long been recognized as hard cases for GI, and, in this author's view, present some of the core difficulties of the general GI problem. Progress on the complexity of testing their isomorphism has been intermittent (Babai 1980, Spielman 1996, BW & CST (STOC'13) and BCSTW (FOCS'13)), and the current best bound is $\exp(\widetilde{O}(n^{1/5}))$ (n is the number of vertices).

Our main result is that if X is a s. r. graph then, with straightforward exceptions, the degree of the largest alternating group involved in the automorphism group $\mathrm{Aut}(X)$ (as a quotient of a subgroup) is $O((\ln n)^2/\ln\ln n)$. (The exceptions admit trivial linear-time GI testing.)

The design of isomorphism tests for various classes of structures is intimately connected with the study of the automorphism groups of those structures. We include a brief survey of these connections, starting with an 1869 paper by Jordan on trees.

In particular, our result amplifies the *potential* of Luks's divide-and-conquer methods (1980) to be applicable to testing isomorphism of s. r. graphs in *quasipolynomial time.*

The challenge remains to find a hierarchy of combinatorial substructures through which this potential can be realized. We expect that the generality of our result will help in this regard; the result applies not only to s. r. graphs but to all graphs with strong spectral expansion and with a relatively small number of common neighbors for every pair of vertices. We state a purely mathematical conjecture that could bring us closer to finding the right kind of hierarchy. We also outline the broader GI context, and state conjectures in terms of "primitive coherent configurations." These are generalizations of s. r. graphs, relevant to the general GI problem.

Another consequence of the main result is the strongest argument to date against GI-completeness of s. r. graphs: we prove that no polynomial-time *categorical* reduction of GI to isomorphism of s. r. graphs is possible. All known reductions between isomorphism problems of various classes of structures fit into our notion of "categorical reduction."

The proof of the main result is elementary; it is based on known results in spectral graph theory and on a 1987 lemma on permutations by Ákos Seress and the author.

ITCS'14, January 12–14, 2014, Princeton, NJ, USA

http://dx.doi.org/10.1145/2554797.2554830 ...$15.00.

Categories and Subject Descriptors

Mathematics of computing [**Discrete mathematics**]: Graph theory; Theory of computation [**Design and analysis of algorithms**]: Graph algorithms analysis

Keywords

graphs, groups, automorphism groups, algorithms, isomorphism testing, strongly regular graphs

1. INTRODUCTION

In just a few lines and from mostly known igredients we derive a surprisingly strong and unanticipated answer to a decades-old mathematical question with implications to graph isomorphism testing, the combinatorics of highly regular configurations, and the theory of permutation groups.

Accordingly, this paper is short on proofs and long on motivation. The proofs, albeit simple, draw on diverse sources: two distinct areas of spectral graph theory (expansion, where the focus is on inequalities; and the spectral aspects of strong regularity, where identities play a central role), a lemma on permutations that initially arose in the context of parallel algorithms and the diameter of permutation groups; and a combinatorial lemma about strongly regular graphs, initially devised in the context of isomorphism testing.

We start with describing the main results, and discuss the motivation in a subsequent section. In a brief "Outlook" section (Sec. 8) we outline the broader graph isomorphism (GI) context and state relevant conjectures in terms of "primitive coherent configurations."

Nothing but the most basic group theory is required for the main results (the notion of the alternating group and of subgroups and quotient groups). Elements of the theory of permutation groups are required for the algorithmic motivation, specifically the notion of primitive permutation groups.

These concepts have been fundamental to the area of GI testing ever since Gene Luks's seminal 1980 paper [46]. We review basic permutation group concepts in the Appendix (Sec. A). The reader may understand much of the motivation by having just the vague notion that "primitive permutation groups" are those permutation groups where natural "divide and conquer" breaks down.

1.1 The main results

A graph X is *strongly regular* with parameters (n, k, λ, μ) if X 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.

A group G is said to *involve* the group H if $H \cong L/N$ for some $N \lhd L \leq G$ (quotient of a subgroup).

Next we introduce a term motivated by the asymptotic theory of primitive permutation groups (see Theorem 6) that will be convenient to use in the statement of our main results.

Definition 1. The *thickness* $\theta(G)$ of a group G is the greatest t such that the alternating group A_t is involved in G.

We note that this is not standard terminology, but Peter Cameron, one of the architects of asymptotic group theory, agreed to use this term in the future[1].

We shall say that the strongly regular graph X is *trivial* if X or its complement is disconnected. In this case, X or its complement is the disjoint union of cliques of equal size. We shall say that X is *graphic* if X or its complement is the line graph of a graph. (The vertices of the line graph $L(Y)$ of the graph Y correspond to the edges of Y; two vertices of $L(Y)$ are adjacent in $L(Y)$ if the corresponding edges of Y share a vertex.) The line graph $L(Y)$ is s. r. exactly if Y is either a complete graph K_v ($n = \binom{v}{2}$) or a complete bipartite graph $K_{v,v}$ (with equal parts; $n = v^2$).

We note that it is straightforward to recognize trivial and graphic s. r. graphs and to test their isomorphism in linear time. We also note that the automorphism groups of these families of s. r. graphs have large thickness: at least $\sqrt{n}$ in each case.

THEOREM 2. *Let X be a non-trivial and non-graphic strongly regular graph with n vertices. Then the thickness of the automorphism group of X is*

$$\theta(\mathrm{Aut}(X)) = O((\ln n)^2 / \ln \ln n).$$

This will be proved in Section 5.2.

[1]Peter Cameron and this author together coined the term "asymptotic group theory" while organizing the first conference specifically dedicated to this area, the European Research Conference "Group Theory: Finite to Infinite," held at Il Ciocco, Lucca, Italy, July 1996. Weeks before the meeting, the sponsoring European Science Foundation informed me that the stellar list of speakers we invited was insufficiently European and therefore this "Russian–Israeli event," as they labeled it, referring to the nationalities of a significant fraction of the speakers, would be canceled. I also received the hint that I could avert this disaster by relabeling the nationalities of visiting scholars according to the countries they visited. Thus Rostislav Grigorchuk (Steklov Inst.) became Swiss (Geneva), Ehud Hrushovski (Hebrew U.) British (Cambridge), etc., and the Europeanness scores kept by the bean counters of Brussels worked out in the end. A happy outcome for asymptotic group theory.

The best previously known bound is $\theta(\mathrm{Aut}(X)) = \widetilde{O}(n^{1/5})$, inferable from [9] (see Section B in the Appendix); prior to 2013, the best known bound was $\widetilde{O}(n^{1/3})$, inferable from Spielman [59]. (The tilde hides polylogarithmic factors.)

One more piece of terminology will come in handy.

Definition 3. Let X be a regular graph of degree k. Let $k = \xi_1 \geq \xi_2 \geq \cdots \geq \xi_n$ denote the eigenvalues of the adjacency matrix of X. Set $\xi = \xi(X) = \max\{|\xi_i| \mid 2 \leq i \leq n\}$. We call this quantity the *zero-weight spectral radius* of X. (It is the spectral radius of the adjacency operator restricted to the subspace $\sum x_i = 0$.)

We shall actually prove the following more general result.

THEOREM 4. *Let X be a regular graph of degree k with zero-weight spectral radius of ξ. Suppose every pair of vertices in X has at most q common neighbors. Assume $q + \xi < k$. Then the thickness of* $\mathrm{Aut}(X)$ *is at most*

$$\frac{(\ln n)^2}{2 \ln \ln n} \cdot \frac{1 + o(1)}{\left(1 - \frac{q+\xi}{k}\right)^2}. \tag{1}$$

(Here the $o(1)$ term goes to zero as $n \to \infty$ uniformly regardless of the other parameters.)

This will be proved in Section 4.

To infer Theorem 2 from Theorem 4, we shall need to show that for non-trivial, non-graphic s. r. graphs, $q + \xi$ is bounded away from k. Since the complement of a s. r. graph is s. r., it suffices to prove this under the assumption that our s. r. graphs have degree $k \leq (n-1)/2$. In fact, we shall need to assume $k < n/4$. For the cases $k \geq n/4$ we shall take a more direct approach.

THEOREM 5. *Let X be a non-trivial, non-graphic strongly regular graph of degree k with $n \geq 29$ vertices and zero-weight spectral radius of ξ. Suppose every pair of vertices in X has at most q common neighbors. Assume $k \leq n/4$. Then $q + \xi < 7k/8$.*

This will be proved in Section 5.1.

Theorems 2 and 4 will immediately follow from bounds we establish on the order of automorphisms (Prop. 13 and Theorem 20, respectively). Specifically, we prove that the order of any automorphism of a non-trivial, non-graphic s. r. graph is at most n^8 (Theorem 20). We also indicate that in fact a stronger, $n^{1+o(1)}$ bound holds (Theorem 21).

2. MOTIVATION: THE GRAPH ISOMORPHISM PROBLEM

2.1 Complexity status

Graph Isomorphism (GI) continues to be one of the intriguing problems of usettled complexity status. It is unlikely to be NP-complete; an early indication of this was that for GI, existence and counting are polynomial-time equivalent [3, 49]. More compelling evidence was provided by the early theory of interactive proofs which demonstrated that if GI is NP-complete then the polynomial-time hierarchy collapses to $\Sigma_2^P = \Pi_2^P = \mathrm{AM}$ [33] (based on [7, 21, 34]). (For a self-contained proof, see [16].)

On the other hand, while GI $\in$ NP $\cap$ coAM, the GI problem is not known to belong to coNP. On the algorithmic front, the best complexity bound is $\exp(\widetilde{O}(\sqrt{n}))$ [14, 63, 12] which has not been improved in three decades.

2.2 Automorphism group vs. isomorphism testing

Algorithms for testing isomorphism of a class of objects are intimately related to the order and structure of the automorphism groups of those objects. There are examples in the history of the two subjects when structural information on the automorphism groups was the basis of the design of efficient isomorphism tests; and conversely, methods developed to test isomorphism of such structures had implications on the structure of the automorphism groups. Yet in other cases the two subjects evolved separately, pursued by separate communities with different context and terminology, yet with virtually identical underlying methods.

In an 1869 paper [41], Jordan counted the automorphisms of trees. His method easily yields a description of the structure of the automorphism groups of trees in terms of iterated direct products and wreath products of symmetric groups, and just as easily yields a canonical form (and therefore isomorphism test) of trees in linear time. Independent work in the early 1970s on the isomorphism problem for planar graphs [39, 40] by Hopcroft and Tarjan, and on the description of the structure of the automorphism groups of planar graphs [2] by this author is based on the same structural principles (canonical reduction to bi-connected and triconnected components and the structure of three-connected planar graphs).

In 1938, Roberto Frucht [31] discovered that every finite group is isomorphic to the automorphism group of a finite graph. First he showed this to be the case for colored directed graphs, namely, the Cayley diagram of the group, and then applied gadgets to encode color and orientation by undirected, uncolored graphs. Decades later, Frucht's gadgets were reinvented in the context of the reduction of the isomorphism problem of directed (colored) graphs to undirected graphs [50].

Frucht's theme was further developed by the Prague category theory school in the 1960s and early 70s. In particular, Hedrlín and Pultr [35] showed in 1966 that every category of finite structures is "fully embeddable" in the category of finite graphs. (For a beautiful exposition, see [36].) A "full embedding" is a functor F that maps the set of $X \to Y$ morphisms bijectively *onto* the set of $F(X) \to F(Y)$ morphisms. In particular, F preserves the automorphism groups and the endomorphism monoids of objects, and $X \cong Y$ if and only if $F(X) \cong F(Y)$. The Hedrlín–Pultr construction is explicit and polynomial-time, thus an immediate (weak) corollary to their work is that the isomorphism problem for explicit structures reduces in polynomial time to the isomorphims problem for graphs. A decade later Miller [50] rediscovered this result and brought it to the attention of the theory community (STOC 1977).

In a 1963 paper, Erdős and Rényi [30] proved that almost all finite graphs have trivial automorphism group. An algorithmic version of this statement is that the naive vertex refinement method completely splits almost all graphs in linear time [11, 13].

The first result on testing isomorphism of strongly regular graphs [4] (1980) established the algorithmic time bound $\exp(\widetilde{O}(n^{1/2}))$; as a corollary, the same value is an upper bound on the number of automorphisms of non-trivial s. r. graphs. Generalizing the method of this proof, this author proved the same bounds for primitive coherent configurations [6] (certain highly regular colorings of the edges of the directed complete graph, cf. section 8), giving, as a corollary, a nearly tight upper bound on the orders of primitive but not doubly transitive groups, solving a then 150-year-old problem on permutation groups.

Motivated partly by a question of Peter Cameron on counting finite models, arising from his study of oligomorphic permutation groups (cf. [25]), Pyber and this author gave an $\exp(\widetilde{O}(n^{1/2}))$ bound on the number of automorphisms of Steiner 2-designs in a 1994 paper [17]. Independently, in 1996, Spielman [59] used the exact same method to test isomorphism of those structures. Spielman's time bound was reduced to $n^{O(\log n)}$ in 2013 [20, 27], yielding the same bound on the number of automorphisms of Steiner 2-designs.

Spielman's main result in [59] was an $\exp(\widetilde{O}(n^{1/3}))$ algorithm to test isomorphism of s. r. graphs; his proof also established this quantity as an upper bound on the number of automorphisms of non-trivial and non-graphic s. r. graphs. Both meanings of this bound (algorithmic and algebraic) were recently improved to $\exp(\widetilde{O}(n^{9/37}))$ by Chen, Sun, and Teng [27] (cf. [9]).

Godsil studied the automorphism groups of graphs with bounded eigenvalue multiplicity [32]; a closely related underlying structure was exploited in [10] to decide isomorphism of such graphs in polynomial time.

The advent of the group theory method (1979-80) brought about much closer ties between GI and automorphism group structure; we next review this connection.

2.3 The group theory method

The group theory method, first introduced into GI in [5] and developed into a profound theory by Luks [46] has been the most successful tool in GI, especially in combination with combinatorial individualization/refinement techniques (see Appendix, Sec. C for an explanation). This combination was also first explored in [5], giving a soon obsolete $\exp(\widetilde{O}(\sqrt{n}))$ isomorphism test for graphs of bounded degree, using very elementary group theory only. Luks's methods were first combined with the individualization/refinement heuristic in [14], yielding results that have not been improved upon to this day (e. g., testing isomorphism of block designs in quasipolynomial time assuming bounded-size blocks and bounded number of blocks passing through each pair of points, and testing isomorphism of tournaments in time $n^{\log n + O(1)}$). The combined method was used in [9] to test isomorphism of s. r. graphs of degrees $k \le n^{3/5}$.

For basic concepts on permutation groups needed for the rest of the discussion in this section, especially the notion of *primitive permutation groups*, see the Appendix (Sec. A). These concepts are only needed to motivate the results, not for the actual technical development.

Luks's method processes an intransitive permutation group orbit-by-orbit, and a transitive but imprimitive permutation group by the blocks of an invariant equivalence relation. We run out of such natural divide-and-conquer options when a primitive group is encountered; nothing much better than complete enumeration of G has been used in this case.

The efficiency of Luks's divide-and-conquer thus critically depends on bounds on the orders of primitive permutation groups the algorithm may encounter; these are typically permutation groups involved in the automorphism group of some subobject of the object in question.

Bounds on the order of a primitive permutation group in turn depend on the *thickness* of the group; by a result by Cameron, Pálfy, and this author [8] and its refinements ([56, 43, 44, 48], cf. [45, Sec. 3] for a survey) we have

THEOREM 6. *If G is a primitive permutation group of degree n and thickness t then $|G| = n^{O(t)}$.*

(This result heavily depends on the classification of finite simple groups [29]. We note that while the initial motivation for [8] came from the GI problem, this result found applications in group theory, including profinite groups (a class of infinite compact groups) [22].)

For example, it is easy to see that the automorphism group of a connected graph of degree $\leq k$ with an individualized edge (an edge with a unique color) has thickness $\leq k-1$; Luks's algorithm can then be analysed via Theorem 6 to imply that isomorphism of graphs of degree $\leq k$ can be tested in time $n^{O(k)}$.

Our main result, Theorem 2, provides a polylogarithmic bound on the thickness of $\mathrm{Aut}(X)$ for all interesting strongly regular graphs, thereby raising *the possibility of a quasipolynomially efficient isomorphism test for s. r. graphs* via Luks's methods.

The question addressed by this result has been in plain view for over three decades; it is significant not only to the GI problem but also to the combinatorial study of highly regular objects such as s. r. graphs, and to the theory of primitive permutation groups. The result is surprising both for its strength and for the simplicity of its proof. It was unanticipated; just a few months earlier, an $n^{o(1)}$ bound was still only a vague hope, and the possibility of its failing seemed like a potential major obstacle to the ultimate goal of the BCSTW [9] project, namely, a subexponential isomorphism test for s. r. graphs.

In addition to the algorithmic perspectives this result opens, it also provides the strongest evidence yet against GI-completeness of s. r. graphs (see Theorem 22).

A caveat: this purely mathematical result does not in itself have immediate algorithmic consequences. While it removes a major obstacle to applying Luks's method to s. r. graphs with quasipolynomial efficiency, another major obstacle to applying Luks's method remains: the apparent lack of a recursive structure in s. r. graphs. In addition to a thickness bound on the automorphism groups, the known applications of Luks's method require a *hierarchy of substructures* that satisfy the same constraint on their automorphism groups. (E. g., a connected graph of degree $\leq k$ with a uniquely colored edge can be built up layer by layer from graphs with the same defining properties.) S. r. graphs don't have such a hierarchical structure. Our result is more general, however, and applies to all graphs with strong spectral expansion and a relatively small number of common neighbors to every pair of vertices (Theorem 4).

This observation presents the **combinatorial challenge** to find such a hierarchical structure in s. r. graphs (after individualization of a moderate number of vertices), possibly capitalizing on the generality of our result as well as on the simplicity of its proof: the proof should be easy to adapt to a variety of circumstances.

There are encouraging initial results in the direction of building a hierarchy with a thickness bound; the paper [9] (FOCS'13) builds such a hierarchical structure after individualizing $O(\log n)$ vertices, where the automorphism group of every member of the hierarchy has thickness $\leq \mu$, the number of common neighbors of a pair of non-adjacent vertices. Using Luks's method via [14] and a result of Miller [52], we then infer that isomorphism of s. r. graphs can be tested in time $n^{O(\mu+\log n)}$. This is one of the key results in [9]. In the cases of interest, we have $\mu \sim k^2/n$ [53, 54, 59], so this gives a strong bound when k is not much larger than its minimum possible value, $\sqrt{n-1}$.

Tournaments illustrate the difficulty of the combinatorial challenge. Their automorphism groups have odd order and therefore have thickness ≤ 2. It follows that the primitive permutation groups involved in them have polynomially bounded order. (This was first proved by Pálfy [55] and Wolf [62]. Pálfy's proof served as a model for [8].) Yet the best known bound on the complexity of testing isomorphism of tournaments is $n^{\log n+O(1)}$ [14] because the natural divide-and-conquer strategy for tournaments leads to a recursion of the form $T(n) = nT(n/2) + n^{O(1)}$, not as strong as would be hoped based on the group theory. Overcoming this combinatorial difficulty is a three-decades-old challenge.

We state a purely mathematical conjecture that could bring us closer to the possibility of a subexponential (or even quasipolynomial) application of Luks's method to s. r. graphs. Following Luks [46], we say that a group G belongs to the class Γ_d if every composition factor of G is a subgroup of the symmetric group S_d.

CONJECTURE 7. *Let X be a non-trivial and non-graphic strongly regular graph with n vertices. Then X has a set S of $O(\log n)$ vertices such that the stabilizer of S in $\mathrm{Aut}(X)$ belongs to the class $\Gamma_{m(n)}$ for some function $m(n) = n^{o(1)}$.*

The conclusion may hold even with a polylogarithmic bound on $m(n)$. If the goal is a subexponential isomorphism test, it may suffice to require that $|S| = n^{o(1)}$.

Most known applications of Luks's method are tied to Γ_d-groups for bounded or slowly growing d, resulting from a hierarchical structure called "color-d-bounded graphs" in [9, Sec. III]. One of the main results of [9] alluded to above establishes a "color-μ-bounded" structure for s. r. graphs after individualizing $O(\log n)$ vertices; this proves the Conjecture with $m(n) = O(\mu + \log n)$. – Tournaments are a notable exception; their automorphism groups do not fit in a Γ_d class with small d. Yet a quasi-polynomial-time isomorphism test for tournaments is based on the solvability of their automorphism groups [14].

2.4 Further motivation

We note that considerable added motivation for our results comes from outside the theory of computing: combinatorics and group theory. The relevant subarea of the former is the the study of the symmetries of highly regular objects; one of the relevant subareas of the latter is the study of primitive permutation groups. We mention a further result of interest to these fields which can be proved by our methods combined with group theory.

THEOREM 8. *Let X be a non-trivial and non-graphic strongly regular graph with n vertices. Assume $\mathrm{Aut}(X)$ is primitive. Then $|\mathrm{Aut}(X)| \leq n^{(1+o(1))\log n}$.*

This answers, in a very strong sense, another question the author has considered for three decades, motivated by the seminal paper by Cameron [24].

It would be of great algorithmic interest if in Theorem 8 the assumption of primitivity could be dropped. In fact, motivated by [24] and [6], it has been this author's belief for more than three decades that non-trivial and non-graphic s. r. graphs have very small automorphism groups.

CONJECTURE 9. *Let X be a non-trivial and non-graphic strongly regular graph with n vertices. Then* $\mathrm{Aut}(X)$ *has subexponential order, i. e.,* $|\mathrm{Aut}(X)| < \exp(n^{o(1)})$.

The best result to date in this direction [28] (cf. [9]) is that

$$|\mathrm{Aut}(X)| < \exp(\widetilde{O}(n^{9/37})). \tag{2}$$

The significance of the conjecture is that it would give purely combinatorial individualization/refinement techniques a chance to achieve a subexponential-time isomorphism test for s. r. graphs; it is no coincidence that the $\exp(\widetilde{O}(n^{9/37}))$ bound was obtained in this context (as were all previous bounds: $\exp(\widetilde{O}(n^{1/2}))$ [4] and $\exp(\widetilde{O}(n^{1/3}))$ [59]). On the other hand, if this conjecture is false, this would virtually rule out that individualization/refinement methods alone could succeed. The difficulties encountered in trying to reduce the $\exp(\widetilde{O}(n^{9/37}))$ bound may suggest that perhaps the conjecture is in fact false.

I note that a similar feeling of possible futility may arise from the considerable difficulties we had to overcome just to reduce Spielman's $\exp(\widetilde{O}(n^{1/3}))$ bound to $\exp(\widetilde{O}(n^{1/5}))$. The good news is that Theorem 2 removes the possibility of a similar obstacle to the group theory approach.

3. TWO LEMMAS

We shall need a variant of the "Expander Mixing Lemma" of Alon and Chung [1] which we state here.

LEMMA 10 (EXPANDER MIXING LEMMA). *Let $X = (V, E)$ be a regular graph of degree k with zero-weight spectral radius ξ. Let $d(S)$ denote the average degree of the subgraph induced by $S \subseteq V$. Then*

$$|d(S) - (|S|/n)k| \le \xi. \tag{3}$$

For the reader's convenience, we include the very short proof of this lemma in the Appendix, Sec. E.

The following lemma by Ákos Seress and the author is one of our main tools.

LEMMA 11 ([18]). *Let σ be a permutation of n elements. Assume σ has order n^α for some $\alpha > 0$. Then some non-identity power of σ has at least $(1 - 1/\alpha)n$ fixed points.*

The original statement of this lemma included an unnecessary condition, so for completeness, we include the short proof of this lemma as well in the Appendix, Sec. D.

This lemma played a key role in the proof that basic questions about permutation groups (membership, order, etc.) are in NC [15]. It was also central to the first non-trivial bound ($\exp(\sqrt{n \ln n}(1 + o(1)))$) on the (worst-case) diameter of the symmetric group [19]. In a recent breakthrough by Helfgott and Seress [37], this bound was reduced to quasi-polynomial, and this lemma was again one of the igredients.

Ákos Seress (1958–2013) was my #1 collaborator, with 15 joint papers over a period of 25 years, several of which I count among the highlights of my career. This collaboration began in summer 1986 at a conference in Szeged, Hungary, where, by a stroke of serendipity, both of us missed the sightseeing boat. This lemma was a fruit of the first hours of our collaboration, conceived at the banks of the river Tisza even before the return of the boat.

4. FIXED-POINTS OF AUTOMORPHISMS

PROPOSITION 12. *Let X be a regular graph of degree k with zero-weight spectral radius of ξ. Suppose every pair of vertices in X has at most q common neighbors. Then every nonidentity automorphism of X has at most $n(q+\xi)/k$ fixed points.*

PROOF. Let σ be a nonidentity automorphism. Let $S = \mathrm{supp}(\sigma) = \{x \in V \mid x^\sigma \neq x\}$ be the support of σ. Let $N(x)$ denote the set of neighbors of x outside S. Then, by the Expander Mixing Lemma (Lemma 10), there exists $x \in S$ such that $|N(x)| \ge (1 - |S|/n)k - \xi$. On the other hand, $N(x) = N(x^\sigma)$, therefore $|N(x)| \le q$. We infer that $q \ge (1 - |S|/n)k - \xi$, and therefore the number of points fixed by x is $n - |S| \le n(q + \xi)/k$. □

PROPOSITION 13. *Let X be a regular graph of degree k with zero-weight spectral radius of ξ. Suppose every pair of vertices in X has at most q common neighbors. Assume $q + \xi < k$. Then the order of any automorphism of X is at most $n^{k/(k-q-\xi)}$.*

PROOF. Combine Prop. 12 and the Lemma 11. □

PROOF OF THEOREM 4. Let $z(t)$ denote the largest among the orders of elements of A_t. It is known that $z(t) = \exp(\sqrt{t \ln t}(1 + o(1)))$ [42]. In fact all we need is $z(t) \ge \exp(\sqrt{t \ln t}(1 + o(1)))$ which easily follows from the Prime Number Theorem, taking the product of cycles of small odd prime lengths.

Suppose A_t is involved in $\mathrm{Aut}(X)$. Then $\mathrm{Aut}(X)$ has an element of order $\ge z(t)$. Therefore

$$n^{k/(k-q-\xi)} \ge z(t). \tag{4}$$

Let us replace t by the greatest value t' for which inequality (4) holds. Then the statement follows with a $o(1)$ term that goes to zero as $t' \to \infty$. But $n \to \infty$ implies $t' \to \infty$ since $n^{k/(k-q-\xi)} \ge n$. □

5. STRONGLY REGULAR GRAPHS

Throughout this section, X will be a s. r. graph with parameters (n, k, λ, μ).

A *conference graph* is a strongly regular graph with parameters $k = (n-1)/2$, $\mu = (n-1)/4$, $\lambda = \mu - 1$.

5.1 Preparatory inequalities

The following well-known facts easily follow from the definition, cf. [23, Lemma 1.1.1 and Theorem 1.3.1].

PROPOSITION 14. *Let X be a nontrivial s. r. graph.*

(i) $\mu(n - k - 1) = k(k - \lambda - 1)$

(ii) X has three distinct eigenvalues, $k > r > -s$; here $r \ge 1$ and $s \ge 2$.

(iii) The eigenvalues of a conference graph are $r = (-1 + \sqrt{n})/2$ and $-s = (-1 - \sqrt{n})/2$.

(iv) Unless X is a conference graph, all eigenvalues are integers.

(v) $r - s = \lambda - \mu$ and $rs = k - \mu$.

The case $s = 2$ was characterized in the 1980s by Hoffman and Ray-Chaudhuri [38] and Seidel [57]. For a particularly elegant treatment, see [26].

THEOREM 15 (SEIDEL [57], CF. [26, THEOREM 4.13]). *If X is a nontrivial s. r. graph with $n \geq 29$ vertices and least eigenvalue $-s = -2$ then X is graphic (the line graph of K_v or $K_{v,v}$).*

Since the complement of a s. r. graph is s. r., we may assume $k \leq (n-1)/2$.

Notation. $\vartheta_1 = \max\{\lambda, \mu\}$ and $\vartheta_2 = \min\{\lambda, \mu\}$.

The following was proved by the author in a paper that appeared in 1980.

LEMMA 16 ([4]). *Let X be a non-trivial s. r. graph of degree $k \leq (n-1)/2$. Then*

(a) $k - \vartheta_2 \leq 2(k - \vartheta_1)$;

(b) $k^2 > n \cdot \vartheta_2$.

We derive further inequalities from Prop. 14 and Lemma 16.

LEMMA 17. *If X is non-trivial and $k \leq (n-1)/2$ then*

(A) $\vartheta_2 < k/2$ and $\vartheta_1 < 3k/4$.

(B) If in addition $s \geq 3$ and $k \leq n/4$ then $\vartheta_1 + r < 7k/8$.

PROOF. For part (A) we note that it follows from part (b) of Lemma 16 that $\vartheta_2 < k^2/n < k/2$; then from part (a) we infer that $\vartheta_1 < 3k/4$.

For part (B), assume first that $\lambda \geq \mu$. From part (v) of Proposition 14 we see that $rs - r + s = k - \lambda$ and therefore $(s-1)r + \lambda < k$. It follows that $(s-1)(\lambda + r) < (s-2)\lambda + k < (3(s-2)/4+1)k = (3s-2)k/4 < 7(s-1)k/8$, so $\lambda + r < 7k/8$.

Assume now that $\lambda < \mu$. From part (i) of Prop. 14 we see that $3\mu n/4 \leq \mu(n-k) \leq k^2$ and therefore $\mu \leq 4k^2/(3n) < k/3$. Moreover, by Part (v) of Prop. 14, we have $r < k/s \leq k/3$. Therefore $\mu + r < 2k/3$. □

We are essentially done proving one of our main auxiliary results, Theorem 5.

PROOF OF THEOREM 5. Modulo the change of notation ($q = \vartheta_1$ and $\xi = r$), the conclusion of Theorem 5 is the same as the conclusion of part (B) of Lemma 17. We only need to justify the assumption $s \geq 3$ made in Lemma 17, part (B). We have $s \geq 2$ by item (ii) of Prop. 14 since X is nontrivial. If X is a conference graph then $s \geq (1 + \sqrt{29})/2 > 3$ by item (iii) of Prop. 14 since $n \geq 29$. If X is not a conference graph then s is an integer by item (iv) of Prop. 14. So we only need to rule out the case $s = 2$; this is done by Seidel's theorem (Theorem 15). □

These preparations will suffice for the proof of our main result in the case $k < n/4$. For the cases when k is large, we use a different tool.

LEMMA 18. *Let X be a nontrivial s. r. graph of degree $k \leq (n-1)/2$. Then any nontrivial automorphism of X fixes fewer than $n - k/2$ vertices.*

For the proof of this lemma, we shall use the following result. Following [4], we say that vertex x *distinguishes* vertices y and z if x is adjacent to exactly one of y and z.

LEMMA 19 ([4]). *Let X be a nontrivial s. r. graph of degree $k \leq (n-1)/2$. Then every pair of distinct vertices is distinguished by at least $k - \vartheta_2$ vertices.*

PROOF OF LEMMA 18. According to part (A) of Lemma 17, we have $\vartheta_2 < k/2$ and therefore by Lemma 19, every pair of distinct vertices is distinguished by more than $k/2$ vertices.

Let now σ be a nontrivial automorphism that fixes the set F. Let $x \in V \setminus F$, so $x^\sigma \neq x$. Let D denote the set of vertices that distinguish x and x^σ. Clearly, $D \cap F = \emptyset$. Since $|D| > k/2$, it follows that $|F| < n - k/2$. □

5.2 Fixed points of automorphisms

Our main result will follow from the following inequalities.

THEOREM 20. *Let X be a non-trivial and non-graphic strongly regular graph with n vertices. Let σ be a non-identity automorphism of X. Then*

(i) σ has at most $7n/8$ fixed points; and

(ii) σ has order $\leq n^8$.

PROOF. Item (ii) follows from item (i) by Lemma 11. To prove item (i), we consider two cases.

I. If $k < n/4$ then by Theorem 5 we have $q + \xi < 7k/8$ and therefore, by Prop. 12, σ fixes fewer than $7n/8$ points.

II. Let us now assume $n/4 \leq k \leq (n-1)/2$. Then, by Lemma 18, σ fixes fewer than $n - k/2 \leq 7n/8$ points. □

Our main result, Theorem 2, follows from Theorem 20 by the same argument as the proof of Theorem 4 at the end of Section 4.

6. IMPROVED BOUNDS VIA NEUMAIER'S CLASSIFICATION OF S. R. GRAPHS

In this section we state a stronger version of Theorem 20.

THEOREM 21. *Let X be a non-trivial, non-graphic strongly regular graph with n vertices. Let σ be a non-identity automorphism of X. Then σ has order $\leq n^{1+o(1)}$.*

Moreover, either $|\operatorname{Aut}(X)| = n^{O(\log n)}$, or σ has $o(n)$ fixed points.

The proof of this result is based on a more substantial body of work. Neumaier [53, 54] classified s. r. graphs into several classes, one of which, following [9], we call *geometric*. These are the line graphs of certain "linear spaces" (transversal designs and Steiner 2-designs with lines of length at least 3 and at most $\approx v^{1/3}$ where v is the number of points in the geometry). These have been shown in [51, 20, 27] to satisfy the bound $|\operatorname{Aut}(X)| = n^{O(\log n)}$. Moreover, in these cases one can show that the order of σ is $O(n)$. Spielman [59] observed that in the remaining cases one can infer from Neumaier's results that both ξ and q are $o(k)$ and therefore Proposition 13 gives the bounds stated.

The details will be given elsewhere; [9] provides a good overview of the facts cited.

7. GI-COMPLETENESS

All known reductions between the isomorphism problems for various classes of structures are *functorial* in the following sense. Let $\mathrm{Iso}(X_1, X_2)$ denote the set of isomorphisms from object X_1 to object X_2.

Let $\mathcal{X}$ and $\mathcal{Y}$ be two classes of objects. A *functorial reduction* of the isomorphism problem for class $\mathcal{X}$ to the isomorphism problem of $\mathcal{Y}$ is a pair of maps (f, F) such that $f : \mathcal{X} \to \mathcal{Y}$, and F is a functor from the category of isomorphisms in $f(\mathcal{X})$ to the category of isomorphisms in $\mathcal{X}$ such that $F(\mathrm{Iso}(f(X_1), f(X_2)) = \mathrm{Iso}(X_1, X_2)$ (F is surjective).

We say that this reduction is *polynomial time* if f is computable in polynomial time.

This concept was introduced by the author in [3]. The main result of that paper regarding this concept was that there is no polynomial-time functorial reduction from degree-$(k+1)$ graphs to degree-k graphs when k is a prime number. This was motivated by Miller's result that for $k \neq 4$ no degree-$(k+1)$ to degree-k reduction can be constructed via a certain type of gadgets [50].

Our main result has the following consequence.

THEOREM 22. *There is no polynomial-time functorial reduction from GI to the isomorphism problem for s. r. graphs.*

For the proof, we need the following observation [3]. Let $\mathrm{maxord}(G)$ denote the maximum order of elements in the group G.

LEMMA 23. *Let (f, F) be a functorial reduction as above. Then for any object $X \in \mathcal{X}$, the group $\mathrm{Aut}(X)$ is a quotient of the group $\mathrm{Aut}(f(X))$. In particular, $\theta(\mathrm{Aut}(X)) \leq \theta(\mathrm{Aut}(f(X)))$ and $\mathrm{maxord}(\mathrm{Aut}(X)) \leq \mathrm{maxord}(\mathrm{Aut}(f(X)))$.*

PROOF. Indeed, $\mathrm{Aut}(X) = \mathrm{Iso}(X, X)$, so F gives a map from $\mathrm{Aut}(f(X))$ onto $\mathrm{Aut}(X)$. This map is a homomorphism, given that F is a functor. □

PROOF OF THEOREM 22. Suppose (f, F) is a functorial reduction from GI to the isomorphism problem for s. r. graphs. Let us consider 5 copies of the graph $K_{1,k}$ ($k+1$ vertices with one vertex of degree k (the "root") and k vertices of degree 1); and let us join the five roots in a 5-cycle to obtain the graph X. So X has $n = 5(k+1)$ vertices. Assume $k \geq 5$. Now $\mathrm{Aut}(X) = S_k \wr D_5$ (the wreath product of S_k by the dihedral group D_5). It is easy to see that the automorphism groups of the trivial and the graphic s. r. graphs do not map onto this group because they do not map onto D_5. Let now $f(X) = Y$; so Y is non-trivial and non-graphic. Let m be the number of vertices of Y. We claim that m is large. We could argue from Theorem 2, using the fact that $k = \theta(\mathrm{Aut}(X)) \leq \theta(\mathrm{Aut}(Y))$. Let us use Theorem 20 (ii) directly instead, using the inequality $\mathrm{maxord}(\mathrm{Aut}(X)) \leq \mathrm{maxord}(\mathrm{Aut}(f(X)))$. Now X has an automorphism of order $\exp(\sqrt{k \ln k}(1 + o(1))) = \exp(\sqrt{n \ln n}(1/\sqrt{5} + o(1)))$, so $\mathrm{Aut}(f(X))$ must have an element of this order; so by item (ii) in Theorem 20 we have $\exp(\sqrt{n \ln n}(1/\sqrt{5} + o(1)) \leq m^8$ and therefore $m \geq \exp(\sqrt{n \ln n}(1/(8\sqrt{5} + o(1)))$, growing exponentially. □

8. OUTLOOK

We outline the broader context of this work. Consider the colored directed complete graph $\mathcal{X} = (V, c)$ where V is the set of vertices and the coloring $c : V \times V \to \{0, \ldots, r-1\}$ of the ordered pairs pairs satisfies the following conditions: (i) if $c(x, x) = c(y, z)$ then $y = z$; and (ii) $c(x, y)$ determines $c(y, x)$. We call $\mathcal{X}$ a "configuration." If c is onto, we say that $\mathrm{rank}(\mathcal{X}) = r$.

For $i, j < r$ and $x, y \in V$ let $p(x, y; i, j)$ denote the number of those $z \in V$ satisfying $c(x, z) = i$ and $c(z, y) = j$. The *Weisfeiler-Leman refinement* [61, 60] defines a refined coloring c' by making $c'(x, y) = c'(u, v)$ if and only if $c(x, y) = c(u, v)$ and for all $j, k < r$ we have $p(x, y; i, j) = p(u, v; i, j)$. The stable colorings (that do not get further refined) are called *coherent configurations*; these are characterized by the property that $p(x, y; i, j)$ is determined by i, j, and $c(x, y)$. (See [6] for more background on coherent configurations.)

It is clear that isomorphism of coherent configurations is GI-complete: given a graph $G = (V, E)$, view it as a rank-3 configuration by setting $c(x, y) = 0$ if $x = y$, $c(x, y) = 1$ if $\{x, y\} \in E$, and $c(x, y) = 2$ if $x \neq y$ and $\{x, y\} \notin E$; then refine this to stable coloring.

We say that the coherent configuration $\mathcal{X}$ is *homogeneous* if all diagonal pairs (x, x) have the same color; call this color 0. We say that the coherent configuration $\mathcal{X}$ is *primitive* if $\mathcal{X}$ is homogeneous and $(\forall i \geq 1)$ the digraph (V, R_i) is connected, where $R_i = \{(x, y) \mid c(x, y) = i\}$. We note that the rank-3 primitive coherent configurations are the s. r. graphs and the analogously defined s. r. tournaments.

The results of this paper represent progress in the context of the following problem, motivated by [24] and [6] and considered by the author for over three decades.

CONJECTURE 24. *Let $\mathcal{X}$ be a primitive coherent configuration with n vertices. For all $\epsilon > 0$ there exists $n_0(\epsilon)$ such that if $n \geq n_0(\epsilon)$ and $|\mathrm{Aut}(\mathcal{X})| \geq \exp(n^\epsilon)$ then $\mathrm{Aut}(\mathcal{X})$ is a primitive permutation group.*

This would be significant because of the detailed description of large primitive permutation groups by Cameron [24]. Since primitive coherent configurations are in a way the combinatorial building blocks of all coherent configurations, this problem would amplify the potential of combinatorial individualization/refinement methods to contribute to progress on the GI problem. We note that [6] confirms this conjecture for $\epsilon = 1/2 + o(1)$. In the rank-3 case, [27] (cf. [9]), combined with [6], confirms the conjecture for $\epsilon = 9/37 + o(1)$.

A weaker version of this conjecture in terms of the thickness of $\mathrm{Aut}(\mathcal{X})$, made plausible by the results of this paper, is the following.

CONJECTURE 25. *Let $\mathcal{X}$ be a primitive coherent configuration with n vertices. For all $\epsilon > 0$ there exists $n_0(\epsilon)$ such that if $n \geq n_0(\epsilon)$ and $\theta(\mathrm{Aut}(\mathcal{X})) \geq n^\epsilon$ then $\mathrm{Aut}(\mathcal{X})$ is a primitive permutation group.*

This version would amplify the potential of Luks's group theoretic divide-and-conquer methods, in conjunction with individualization/refinement, to achieve a subexponential upper bound on the complexity of the GI problem. Again, [6] confirms this conjecture for $\epsilon = 1/2 + o(1)$. In the rank-3 case, [9] confirms the conjecture for $\epsilon = 1/5 + o(1)$.

9. ACKNOWLEDGMENTS

I gratefully acknowledge the inspiration gained from two sources: the collaboration with my student John Wilmes and with Xi Chen, Xiaorui Sun, and Shang-Hua Teng on the isomorphism problem for strongly regular graphs [20,

27, 9]; and a conversation with Ian Wanless about the order of automorphisms of quasigroups, the subject of a paper by McKay, Wanless, and Zhang [47]. The latter discussion took place at the conference "Combinatorics, Algebra and More," celebrating Peter Cameron's 65th birthday at Queen Mary, University of London in July 2013. I thank the organizers, David Ellis and Leonard Soicher, for the opportunity to attend the meeting.

This research was supported in part by NSF Grant CCF-1017781.

10. REFERENCES

[1] Noga Alon, Fan R. K. Chung: Explicit construction of linear sized tolerant networks. *Discrete Math.* **72** (1988) 15–19

[2] László Babai: Automorphism groups of planar graphs II. In: *Infinite and Finite Sets* (Proc. Conf. Keszthely, Hungary, 1973, A. Hajnal et al eds.) Bolyai Society – North-Holland, 1975, pp. 29–84

[3] László Babai: On the isomorphism problem. Preprint, 1977 (10pp.) (cited in [49])

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

[5] László Babai: Monte Carlo algorithms in graph isomorphism testing. Tech. Rep. 79–10, Dép. Math. et Stat., Univ. de Montréal, 1979.

[6] László Babai: On the order of uniprimitive permutation groups. *Annals of Math.* **113(3)** (1981) 553–568.

[7] László Babai: Trading group theory for randomness. *In: 17th STOC*, pp. 421–429, 1985.

[8] László Babai, Peter J. Cameron, Péter Pál Pálfy: On the orders of primitive groups with restricted nonabelian composition factors. *J. Algebra* **79** (1982), 161–168.

[9] László Babai, Xi Chen, Xiaorui Sun, Shang-Hua Teng, John Wilmes: Faster Canonical Forms For Strongly Regular Graphs. *In: 54th IEEE FOCS*, pp. 157–166, 2013.

[10] László Babai, Dmitry Yu. Grigor'ev, David M. Mount: Isomorphism of graphs with bounded eigenvalue multiplicity. In: *Proc. 14th ACM STOC*, 1982, pp. 310–324.

[11] László Babai, Paul Erdős, Stanley M. Selkow: Random graphs isomorphism, *SIAM J. on Computing* **9** (1980), 628-635.

[12] László Babai, William M. Kantor, Eugene M. Luks: Computational complexity and the classification of finite simple groups. *In: 24th IEEE FOCS*, pp. 162–171, 1983.

[13] László Babai, Luděk Kučera: Canonical labeling of graphs in linear average time. *In Proc. 20th FOCS.*, pp. 39–46, 1979.

[14] László Babai, Eugene M. Luks: Canonical labeling of graphs. *In: 15th ACM STOC*, pp. 171–183, 1983.

[15] László Babai, Eugene M. Luks, Ákos Seress: Permutation groups in NC. *In: Proc. 19th ACM STOC*, 1987, pp. 409–420

[16] László Babai, Shlomo Moran: Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes. *J. Comput. Systems Science* **36** (1988), 254–276

[17] László Babai, László Pyber: Permutation groups without exponentially many orbits on the power set. *J. Combinat. Theory, Ser. A*, **66** (1994), 160–168.

[18] László Babai, Ákos Seress: On the degree of transitivity of permutation groups: a short proof. *J. Combinatorial Theory-A* **45** (1987), 310–315

[19] László Babai, Ákos Seress: On the diameter of Cayley graphs of the symmetric group. *J. Combinatorial Theory-A* **49** (1988), 175–179

[20] László Babai, John Wilmes: Quasipolynomial-time canonical form for Steiner designs. *In: 45th ACM STOC*, pp. 261-270, 2013.

[21] Ravi B. Boppana, Johan Håstad, Stathis Zachos: Does co-NP have short interactive proofs? *Information Processing Letters*, **25(2)** (1987), 127–132

[22] Alexandre V. Borovik, László Pyber, Aner Shalev: Maximal subgroups in finite and profinite groups. Trans. Amer. Math. Soc. **348(9)** (1996), 3745–3761.

[23] Andries E. Brouwer, Arjeh M. Cohen, Arnold Neumaier: *Distance-Regular Graphs.* Springer 1989.

[24] Peter J. Cameron: Finite permutation groups and finite simple groups. *Bull. London Math Soc.* **13** (1981) 1–22.

[25] Peter J. Cameron: *Oligomorphic Permutation Groups.* London Math. Soc. Lecture Notes 152. Cambridge Univ. Press, 1990.

[26] Peter J. Cameron, Jean-Marie Goethals, Johan Jacob Seidel, Ernest E. Shult: Line Graphs, Root Systems, and Elliptic Geometry. *J. Algebra* **43** (1976) 305-327

[27] Xi Chen, Xiaorui Sun, Shang-Hua Teng: Multi-stage design for quasipolynomial-time isomorphism testing of Steiner 2-systems. *In: 45th STOC*, pp. 271–280, 2013

[28] Xi Chen, Xiaorui Sun, Shang-Hua Teng: On the order of the automorphism groups of strongly regular graphs. In preparation.

[29] John H. Conway, Robert T. Curtis, Simon P. Norton, Richard A. Parker, Robert A. Wilson: *ATLAS of finite groups.* Oxford Univ. Press 1985, 2003.

[30] Paul Erdős, Alfréd Rényi: Asymmetric graphs. *Acta Math. Acad. Sci. Hung.* **14** (1963) 295–315

[31] Roberto Frucht: Herstellung von Graphen mit vorgegebener abstrakter Gruppe. *Composition Math.* **6** (1938) 239–250

[32] Chris D. Godsil: Graphs, groups, and polytopes. In: *Combinatorial Mathematics*, Springer LNM Vol. 686, 1978, pp. 157–164

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

[34] Shafi Goldwasser, Michael Sipser: Private coins versus public coins in interactive proof systems. *In: 18th STOC*, pp. 59–68, 1986.

[35] Zdeněk Hedrlín, Aleš Pultr: On full embeddings of categories of algebras. *Ill. J. Math.* **10** (1966) 392–406

[36] Zdeněk Hedrlín, Joachim Lambek: How comprehensive is the category of semigroups? *J. Algebra* **11** (1969) 195–212

[37] Harald Helfgott, Ákos Seress: On the diameter of permutation groups. *Annals of Mathematics.* To appear

[38] Alan J. Hoffman, Dijen K. Ray-Chaudhury: On a spectral characterization of regular line graphs. Unpublished mansucript, cited by [26]

[39] John Hopcroft, Robert Endre Tarjan: Isomorphism of planar graphs. In: *Complexity of Computer Computations* R. M. Miller, J. W. Thatcher, eds., Plenum Press 1972, pp. 131–152.

[40] John Hopcroft, Robert Endre Tarjan: Dividing a graph into triconnected components. *SIAM J. Computing* **2** (1973) 135–158

[41] Camille Jordan: Sur les assemblages de lignes. *J. Reine Angew. Math.* **70** (1869), 185–190

[42] Edmund Landau: *Handbuch der Lehre von der Verteilung von Primzahlen., Bd I.* Teubner, Leipzig, 1909.

[43] Martin W. Liebeck: On minimal degrees and base sizes of primitive permutation groups. *Arch. Math.* **43** (1984) 11–15.

[44] Martin W. Liebeck, Aner Shalev: Simple groups, permutation groups, and probability. *J. AMS* **12** (1999) 497-520.

[45] Martin W. Liebeck, Aner Shalev: Bases of primitive permutation groups. *In: Groups, Combinatorics, and Geometry (Durham 2001)*, pp. 147-154. World Scientific 2003.

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

[47] Brendan D. McKay, Ian M. Wanless, Xiande Zhang: The order of automorphisms of quasigroups. Manuscript, submitted for publication. 2013.

[48] Attila Maróti: On the orders of primitive groups. *J. Algebra* **258(2)** (2002) 631–640.

[49] Rudi Mathon: A note on the graph isomorphism counting problem. *Inf. Proc. Letters* **8** (1979) 131–132.

[50] Gary L. Miller: Graph isomorphism, general remarks. *In: Proc. 9th STOC*, pp. 143-150, 1977

[51] Gary L. Miller: On the $n^{\log n}$ isomorphism technique: A preliminary report. *In: 10th ACM STOC*, pp. 51–58, 1978.

[52] Gary L. Miller: Isomorphism of graphs which are pairwise k-separable. *Information and Control* **56(1-2)** (1983) 21–33.

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

[54] Arnold Neumaier: Quasiresidual 2-designs, $1\frac{1}{2}$-designs, and strongly regular multigraphs. *Geom. Dedicata* **12(4)** (1982) 351–366.

[55] Péter P. Pálfy: A polynomial bound on the orders of primitive solvable groups. *J. Algebra* **77** (1982) 127–137

[56] László Pyber. Unpublished, cited by [45]

[57] Johan Jacob Seidel: Strongly regular graphs with $(-1, 1, 0)$-adjacency matrix having eigenvalue 3. *Linear Algebra Appl.* **1** (1968) 281-298

[58] Ákos Seress: *Permutation Group Algorithms.* Cambridge Univ. Press, 2003

[59] Daniel A. Spielman: Faster isomorphism testing of strongly regular graphs. *In: 28th STOC*, pages 576–584, 1996.

[60] Boris Weisfeiler (ed): *On Construction and Identification of Graphs.* Springer Lect. Notes in Math. Vol 558, 1976.

[61] Boris Weisfeiler, Andrei A. Leman: A reduction of a graph to a canonical form and an algebra arising during this reduction. *Nauchno-Technicheskaya Informatsiya* **9** (1968) 12–16.

[62] Thomas R. Wolf: Solvable and nilpotent subgroups of $GL(n, q^m)$. *Canad. J. Math.* **34** (1982) 1097–1111

[63] Viktor N. Zemlyachenko, N. M. Korneenko, Regina I. Tyshkevich: Graph isomorphism problem. *Zapiski Nauchnykh Seminarov LOMI* **118** (1982), 83–158, 215.

APPENDIX

A. PERMUTATION GROUP CONCEPTS

If G, H are groups, the notation $H \leq G$ means H is a sugroup of G.

S_n denotes the symmetric group of degree n, i. e., the group of all permutations of a set Ω of n elements; Ω is the *permutation domain.*

G is a *permutation group of degree* n if $G \leq S_n$.

The *order* of a group G is $|G|$, the number of elements of G. The order of an element $g \in G$ is the order of the subgroup generated by g. For $x \in \Omega$ and $g \in G$ we write x^g to denote the image of x under G. The *orbit* of x is the set $x^G = \{x^g \mid g \in G\}$. The orbits partition the permutation domain. G is *transitive* if $x^G = \Omega$ for some (and therefore, for any) $x \in \Omega$.

Definition 26. A transitive permutation group G is *primitive* if there is no nontrivial G-invariant equivalence relation on the permutation domain. Otherwise G is *imprimitive.*

The blocks of a G-invariant partition are called *blocks of imprimitivity.* Orbits and non-trivial blocks provide a natural setting for divide-and-conquer algorithms for permutation groups [46].

B. COMPARISON WITH PRIOR THICKNESS BOUNDS

In this section we explain the comment made immediately after Theorem 2 abut thickness bounds *inferable* from prior work.

Most prior results from which thickness bounds for $\mathrm{Aut}(X)$ are inferable were of the following form: "the pointwise stabilizer of ℓ points in $\mathrm{Aut}(X)$ is the identity." This was proved for all non-trivial s. r. graphs with $\ell = \widetilde{O}(n^{1/2})$ in [4]; for all non-trivial and non-graphic s. r. graphs with $\ell = \widetilde{O}(n^{1/3})$ in [59]; and with $\ell = \widetilde{O}(n^{1/5})$ for degree $k \gtrsim n^{3/5}$ in [9]. Now such a bound implies that $|\mathrm{Aut}(X)| \leq n^\ell$ and therefore, if $\theta(\mathrm{Aut}(X)) = t$ then $t!/2 \leq n^\ell$ which implies $t \lesssim \ell \ln n$, from which the bounds $\theta(\mathrm{Aut}(X)) = \widetilde{O}(n^s)$ follow with $s = 1/2, 1/3$, and $1/5$, respectively.

For $k \lesssim n^{3/5}$, [9] combined with [20] and [27] proved that by fixing $\ell = O(\log n)$ points, we obtain a group with thickness $\leq \mu$ where $\mu \sim k^2/n$, so if $k \lesssim n^{3/5}$ then $\mu \lesssim n^{1/5}$. To understand the implication of this on the thickness of $\mathrm{Aut}(X)$, we need the following lemma.

LEMMA 27. *Let $G \le S_n$ be a permutation group. Suppose there is a subset Δ of the permutation domain such that $\theta(G_\Delta) = \tau$, where G_Δ denotes the pointwise stabilizer of Δ. Let $|\Delta| = \ell$ and $\theta(G) = t$. Then $t = O(\ell \log n + \tau)$, and if $\tau = n^{\Omega(1)}$ then $t = O(\ell + \tau)$.*

PROOF. Observe that $t!/\tau! \le n^\ell$. □

Taking $G = \mathrm{Aut}(X)$ and $\tau = \widetilde{O}(n^{1/5})$ we infer that $\theta(\mathrm{Aut}(X)) = \widetilde{O}(n^{1/5})$.

C. THE INDIVIDUALIZATION/REFINEMENT HEURISTIC

The most natural heuristic for isomorphism rejection colors the vertices in a canonical way (e. g., the color could indicate the degree of a vertex or the number of triangles containing the vertex) and then applies a canonical refinement procedure to the coloring (e. g., the new color of vertex v would encode the old color of v as well as the number of neighbors of v of any given old color). Iteration of the procedure leads to a stable coloring. In the case described, each color class of the stable refinement induces a regular graph and each pair of color-classes induces a biregular bipartite graph between the two color classes. Applying such a procedure simultaneously to two graphs leads to isomorphism rejection if in one of the graphs a color appears that does not exist in the other. (In connected graphs this automatically means that the sets of colors in the two graphs are disjoint.)

Canonicity of coloring and refinement means all isomorphisms are preserved. If the stable coloring *completely splits the graph*, i. e., it assigns a unique color to each vertex, then only one candidate isomorphism with any other (not rejected) graph remains, so this leads to a rapid isomorphism test. (This works for almost all graphs [11, 13].)

If the process does not lead to a satisfactory refinement (e. g., the process described does not even start if the graph is regular), *individualization* can be applied. This means the assignment of a unique color to each member of a set of say ℓ vertices. For valid isomorphism rejection, this process then needs to be repeated for every ordered ℓ-tuple. If for some ℓ-tuple the coloring leads to a complete split, this gives an isomorphism test (against any other graph) in time $n^{\ell+O(1)}$. This idea is the basis of the complexity bounds on testing isomorphism of s. r. graphs in [4, 59, 20, 27, 28] as well as in [9] for $k \gtrsim n^{2/3}$. For smaller degrees, [9] combines this idea with the group theoretic method.

D. THE B–SERESS LEMMA ON PERMUTATIONS: ORDER VS. FIXED POINTS

In this section we review the proof of Lemma 11. We repeat the statement.

LEMMA 28 ([18]). *Let σ be a permutation of n elements. Assume σ has order n^α for some $\alpha > 0$. Then some non-identity power of σ has at least $(1 - 1/\alpha)n$ fixed points.*

PROOF. Let σ act on the set Ω where $|\Omega| = n$. Let the order of σ be $N = n^\alpha = \prod_{i=1}^r q_i$ where $q_i = p_i^{\beta_i} > 1$ are powers of distinct primes p_i. For each $x \in \Omega$, let us consider the set $P(x)$ of those i for which q_i divides the length of the σ-cycle through x. Clearly, for each $x \in \Omega$,

$$\prod_{i \in P(x)} q_i \le n. \tag{5}$$

Let $n(i)$ denote the number of points $x \in \Omega$ such that $i \in P(x)$. Let us estimate the weighted average W of the $n(i)$ with weights $\log q_i$:

$$W = \frac{\sum n(i) \log q_i}{\sum \log q_i}. \tag{6}$$

Recall that the sum of weights is $\sum \log q_i = \log N = \alpha \log n$, therefore (using Eq. (5))

$$W = \sum_{x \in \Omega} \sum_{i \in P(x)} \frac{\log q_i}{\alpha \log n} \le \frac{n \log n}{\alpha \log n} = \frac{n}{\alpha}. \tag{7}$$

It follows that $n(i) \le n/\alpha$ for some $i \le r$. Let $m = N/p_i$ be the corresponding maximal divisor of N. Clearly σ^m is not the identity and it fixes all but $n(i)$ points. □

The original paper [18] made the unnecessary additional assumption that σ contains cycles of distinct *prime* lengths of which the product is $\ge n^\alpha$. While we drop this assumption here, the above proof is almost verbatim identical with the one in [18].

I ask those who may use the lemma in its present form to co-credit Seress.

E. THE EXPANDER MIXING LEMMA

While the simple proof of this result of Alon and Chung [1] has been reproduced in many places, we reproduce it here for the readers's convenience and because of its central role in our main result.

For a graph $X = (V, E)$ and subsets $S, T \subseteq V$ let $E(S, T)$ denote the set of ordered pairs (s, t) such that $s \in S$, $t \in T$, and s, t are adjacent. (Note that $|E(S, T)|$ doubly counts each edge in $S \cap T$.)

LEMMA 29. *Let $X = (V, E)$ be a k-regular graph with n vertices. Let $S, T \subseteq V$. Then*

$$\left| |E(S,T)| - \frac{|S||T|k}{n} \right| \le \xi \sqrt{|S||T|}. \tag{8}$$

where ξ is the zero-weight spectral radius of X (as defined before Thm. 4).

For completeness, we include the simple proof.

PROOF. Let $\mathbf{1}_W$ denote the incidence vector of the subset $W \subseteq V$ written as a column vector. Note that $||\mathbf{1}_W|| = \sqrt{|W|}$. Let J denote the $n \times n$ all-ones matrix (all entries 1). Then

$$|E(S,T)| = \mathbf{1}_S^* A \mathbf{1}_T \tag{9}$$

and

$$|S||T| = \mathbf{1}_S^* J \mathbf{1}_T. \tag{10}$$

(The asterisk indicates transpose.) It follows that the left-hand side in equation (8) is equal to

$$|\mathbf{1}_S^* (A - (k/n)J) \mathbf{1}_T| \tag{11}$$

which by Cauchy-Schwarz is not greater than $\sqrt{|S||T|}$ times the spectral norm of $A - (k/n)J$. If the eigenvalues of A are $k = \xi_1 \ge \xi_2 \ge \cdots \ge \xi_n$ then the eigenvalues of $A - (k/n)J$ are $0, \xi_2, \ldots, \xi_n$, so the spectral norm of $A - (k/n)J$ is ξ. □

Lemma 10 now follows, noting that $|E(S, S)| = |S| d(S)$ and applying Lemma 29 with $T = S$.