On the Automorphism Groups of Strongly Regular Graphs II

László Babai

University of Chicago

Abstract

We derive strong constraints on the automorphism groups of strongly regular (SR) graphs, resolving old problems motivated by Peter Cameron's 1981 description of large primitive groups.

Trivial SR graphs are the disjoint unions of cliques of equal size and their complements. *Graphic* SR graphs are the line-graphs of cliques and of regular bipartite cliques (complete bipartite graphs with equal parts) and their complements.

We conjecture that the order of the automorphism group of a non-trivial, non-graphic SR graph is quasi-polynomially bounded, i. e., it is at most $\exp((\log n)^C)$ for some constant C, where n is the number of vertices.

While the conjecture remains open, we find surprisingly strong bounds on important parameters of the automorphism group. In particular, we show that the order of every automorphism is $O(n^8)$, and in fact $O(n)$ if we exclude the line-graphs of certain geometries. We prove the conjecture for the case when the automorphism group is primitive; in this case we obtain a nearly tight $n^{1+\log_2 n}$ bound.

We obtain these bounds by bounding the *fixicity* of the automorphism group, i. e., the maximum number of fixed points of non-identity automorphisms, in terms of the second largest (in magnitude) eigenvalue and the maximum number of pairwise common neighbors of a regular graph. We connect the order of the automorphisms to the fixicity through an old lemma by Ákos Seress and the author.

We propose to extend these investigations to primitive coherent configurations and offer problems and conjectures in this direction. Part of the

Email address: laci@cs.uchicago.edu (László Babai)

motivation comes from the complexity of the Graph Isomorphism problem.

Keywords: strongly regular graph, automorphism group, primitive group, coherent configuration
2010 MSC: 20B15, 05C65

Dedicated to the memory of Ákos Seress

1. Introduction

In 1981, Peter Cameron [19] described the structure of large primitive permutation groups, making heavy use of the classification of finite simple groups (CFSG)[1]. In particular, Cameron's result implies that the order of a primitive permutation group of sufficiently large degree n, other than A_n and S_n, is at most $n^{\sqrt{n}}$.

At the same time, partly motivated by the complexity of the graph isomorphism problem, this author studied a *combinatorial relaxation* of this question (where symmetry conditions such as a primitive group action are replaced by regularity constraints expressed in terms of numerical parameters of an underlying structure), resulting in an entirely elementary proof of a bound of $\exp(\widetilde{O}(n^{1/2}))$ on the order of primitive groups[2], nearly matching Cameron's tight bound.[3, 4][3]

Indeed, it is shown in [3] that nontrivial *primitive coherent configurations*[4] have at most $\exp(\widetilde{O}(n^{1/2}))$ automorphisms.

---

[1]Cameron's result was later sharpened by Liebeck and Shalev [34, 35], and finally by Maróti [38] (see Theorem 5.1 below).

[2]The $\widetilde{O}$ notation hides polylogarithmic ($O((\log n)^C)$) factors; the more exact bound proved in [3] is $\exp(4n^{1/2}(\log n)^2)$.

[3]While not relevant to the subject of this paper, we should mention that [4] gives, by elementary arguments, a subexponential bound of $\exp(\exp(c\sqrt{\log n}))$ on the order of doubly transitive permutation groups other than S_n and A_n; building on the framework of that paper, Pyber [45] improved the bound to quasipolynomial, $\exp(c(\log n)^4)$, still by entirely elementary arguments. As common in the theory of computing, we call a function f "subexponential" if for all $\epsilon > 0$ we have $f(n) < \exp(n^\epsilon)$ for all sufficiently large n; and "quasi-polynomially bounded" if $f(n) < \exp((\log n)^C)$ for some constant C.

[4]Coherent configurations are directed, edge-colored graphs satisfying certain strong regularity constraints; they are primitive if their constituent graphs (color classes) are connected. (See Section 7 for the definition.) While all primitive groups act on primitive coherent configurations, the converse is false, so a bound on the number of automorphisms of primitive coherent configurations is a stronger result than a corresponding bound on

It was expected that [3] would be the first step in a series of combinatorial relaxations of Cameron's question, with the goal of recovering combinatorial versions of deeper layers of Cameron's classification. Such results would be significt for the theory of highly regular combinatorial structures such as strongly regular (SR) graphs, association schemes, and coherent configurations, as well as to the complexity of the graph isomorphism problem. While for three decades this program has seen little progress, significant new results have emerged recently. The most important among these, by Xiaorui Sun and John Wilmes [50], further limits the number of automorphisms of primitive coherent configurations in the spirit of [3], moving one step deeper in Cameron's hierarchy: they give an upper bound of $\exp(\widetilde{O}(n^{1/3}))$, with the exceptions described by Cameron. We state the result, and a related conjecture, in section 7. A corollary to this result is an elementary proof that all primitive groups have order at most $\exp(\widetilde{O}(n^{1/3}))$ with the known exceptions.

The bulk of this paper concerns SR graphs which can be viewed as a subclass of primitive coherent configurations. Intuition gained from the study of SR graphs has proven useful in the study of primitive coherent configurations; indeed, the result of [3] was first proved for SR graphs [2] and the general case followed the basic outline as well as some of the conceptual and technical details of the SR case. To some extent the same can now be said of [50].

Primitive groups act on primitive coherent configurations. The largest among these groups, after S_n and A_n, act on certain strongly regular (SR) graphs, namely, on the line graphs of the complete graphs K_v ($n = \binom{v}{2}$) and of the complete bipartite graphs $K_{v,v}$ with equal parts ($n = v^2$). We shall call the SR graphs in these classes as well as their complements "*graphic* SR graphs." These have automorphism groups of order about $n^{c\sqrt{n}}$. The "*trivial* SR graphs" are those which are the unions of disjoint cliques of equal size, and their complements. They are not primitive except for the complete graph and its complement.

One observes that the smaller the primitive group in Cameron's hierarchy, the greater the number of color classes in the corresponding coherent configuration.

---

the order of primitive groups; and such strengthenings are not amenable to a reduction to CFSG via the O'Nan–Scott structure theorem for primitive groups.

Motivated by this phenomenon, we have made the following conjecture.

Conjecture 1.1. *If X is a non-trivial, non-graphic SR graph with n vertices then the order of* $\mathrm{Aut}(X)$ *is quasi-polynomially bounded, i. e.,* $|\mathrm{Aut}(X)| \leq \exp((\log n)^C)$ *for some constant C.*

Work in this direction was started by this author in 1978 [2] with a $|G| < \exp(\widetilde{O}(n^{1/2}))$ bound where $G = \mathrm{Aut}(X)$. This bound was improved by Spielman (1996) [49] to $|G| < \exp(\widetilde{O}(n^{1/3}))$ and recently (2013) by Chen, Sun, and Teng to $|G| < \exp(\widetilde{O}(n^{9/37}))$ [23] (cf. [16, 22, 7]). Note that G is not assumed to be primitive in these results.

We observe that Conjecture 1.1 is equivalent to the following.

Conjecture 1.2. *If an elementary abelian group G acts on a non-trivial, non-graphic SR graph with n vertices then the order of G is quasi-polynomially bounded.*

1.1. Thickness, fixicity, order of automorphisms

While we are unable to prove the conjecture, we obtain surprisingly strong bounds on important parameters of $\mathrm{Aut}(X)$.

We define[5] the *thickness* $\theta(G)$ of a finite group G as the largest t such that the alternating group A_t is involved in G (as a section, i. e., a quotient of a subgroup).

Theorem 1.3. *Let X be a non-trivial, non-graphic SR graph with n vertices. Then* $\theta(\mathrm{Aut}(G)) = O(\log^2 n/\log\log n)$.

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 [6] and refinements of the result ([47, 33, 34, 38], cf. [35, Sec. 3] for a survey) we have the following.

Theorem 1.4. *If G is a primitive permutation group of degree n and thickness t then* $|G| = n^{O(t)}$.

This result plays an important role in the applications of Luks's group theoretic divide-and-conquer algorithms to the Graph Isomorphism problem

[5] In agreement with Peter Cameron.

(cf. [36, 8, 9, 11, 7]), one of the key motivations for this work. In particular, Theorem 1.4 combined with Theorem 1.3 removes the group theoretic obstacle from a potentially quasi-polynomially efficient application of Luks's method to testing isomorphism of SR graphs.

Theorem 1.3 is an immediate corollary to the following result.

Theorem 1.5. *Let X be a non-trivial, non-graphic SR graph with n vertices. Then every automorphism of X has order $\leq n^8$.*

Following Martin Liebeck, we say that the *fixicity* $\mathrm{fix}(G)$ of a permutation group G is the maximum number of elements fixed by non-identity permutations. We shall infer Theorem 1.5 from the following result.

Theorem 1.6. *If X is a non-trivial, non-graphic SR graph with n vertices then $\mathrm{fix}(\mathrm{Aut}(G)) \leq 7n/8$.*

Theorem 1.5 will follow from Theorem 1.6 via an old lemma by Ákos Seress and the author (see Lemma 3.8).

Given these consequences, further refinement of the fixicity bound is desirable. We offer such a refinement below (Theorem 1.7) using Neumaier's classification of SR graphs.

We shall define *geometric* SR graphs as the line-graphs of certain incidence geometries (Steiner 2-designs and transversal designs with lines of length ≥ 3 and $\leq v^{1/3}$ where v is the number of points of the geometry; see the full definitions in Section 2.1).

Theorem 1.7. *Assume X is a non-trivial, non-graphic, and non-geometric SR graph with n vertices and degree k.*

(a) If $k \geq n^{2/3}$ then the fixicity of $\mathrm{Aut}(X)$ is $\mathrm{fix}(\mathrm{Aut}(X)) = O(\sqrt{kn})$.

(b) Suppose $k \leq n^{3/4}$. Then $\mathrm{fix}(\mathrm{Aut}(X)) = O(n^{7/8})$.

We note that geometric SR graphs have few automorphisms. A *base* of a permutation group G acting on a set Ω a subset $\Delta \subseteq \Omega$ such that the pointwise stabilizer of Δ in G is trivial. It follows that $|G| \leq |\Omega|^{|\Delta|}$.

Theorem 1.8 ([42, 16, 22])**.** *If X is a geometric SR graph then $\mathrm{Aut}(X)$ has a base of size $O(\log n)$ and therefore $\mathrm{Aut}(X) \leq n^{O(\log n)}$.*

This was proved by Gary Miller [42] in 1980 for transversal designs. The far more difficult case of Steiner 2-designs was settled simultaneously in [16] and [22] in 2013.

Theorem 1.9. *Assume X is a non-trivial, non-graphic, and non-geometric SR graph with n vertices and degree $k \le n/(\log n)^2$. Then the order of every automorphism of X is $O(n)$.*

We note that if $n/(\log n)^2 \le k \le (n-1)/2$ then $|\operatorname{Aut}(X)|$ is quasi-polynomially bounded (at most $\exp(O((\log n)^4))$) by an old result of this author [2, 3] (see Theorem 2.1 below).

Summarizing, we obtain strong constraints on any potential family of counterexamples to Conjecture 1.1. This corollary can be viewed as the main result of this paper.

Corollary 1.10. *There exists a constant C such that the following holds. Let X be a non-trivial, non-graphic SR graph with n vertices and at least $\exp(C(\log n)^4)$ automorphisms. Then*

(i) $\operatorname{fix}(\operatorname{Aut}(X)) \le n/\log n$*;*

(ii) The order of every automorphism of X is $O(n)$.

Indeed, if X is geometric, it has too few automorphisms by Theorem 1.8; if the degree is $n/(\log n)^2 \le k \le (n-1)/2$ then $|\operatorname{Aut}(X)| < \exp(O(\log n)^4)$ by Theorem 2.1; and in the reminaing cases, (i) follows from Theorem 1.7 and (ii) from Theorem 1.9.

Finally we ask the question whether large primitive groups can act on SR graphs.

Theorem 1.11. *Let G be a primitive permutation group of sufficiently large degree n acting on a non-trivial, non-graphic SR graph. Then $|G| \le n^{1+\log_2 n}$.*

We note that this bound is close to best possible.

Proposition 1.12. *For infinitely many values of n there exist non-trivial, non-graphic SR graphs with n vertices and with a primitive automorphism group of order greater than $n^{(\log_2 n - 1)/8}$.*

1.2. Relation of this paper to [5]

Some of the main results of this paper were announced, with proof, in the conference paper [5]. Since such conference papers cannot be refereed to the standards of a journal publication (the proceedings is handed out at the meeting), it is customary and even expected in the theory of computing to prepare a full journal version. The present paper bears the "II" designation

in the title to indicate that it does not fully supersede [5]. Here we list the differences of the two papers.

The two papers interpret the results from different perspectives. In particular, [5] discusses in considerable detail the relevance of these results to the algorithmic problem of Graph Isomorphism testing; we almost entirely omitted that discussion from this paper. In particular, we omitted nearly the entire material of Section 2 of that paper, as well as Section 7 which proves, based on our main results, that there is no functorial reduction from the Graph Isomorphism problem to the isomorphism problem of SR graphs [5, Thm. 22].

On the other hand, the present paper includes a number of results that do not appear in [5]. Theorems 1.3, 1.5, 1.6 of this paper also appear in [5]. Theorems 1.7, 1.9, Corollary 1.10 (the main result), Theorem 1.11, and Proposition 1.12 do not appear in [5].

2. Preliminaries

2.1. Strongly regular graphs

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.

The complement of a SR graph is SR, so we may always assume $k \leq (n-1)/2$. Also, connected SR graphs have diameter ≤ 2, and therefore degree $k \geq \sqrt{n-1}$.

We shall say that the strongly regular graph X is *trivial* if $n = 1$ or X or its complement is disconnected. So X is trivial if and only if either X or its complement is the disjoint union of cliques of equal size.

The *line graph* $L(Y)$ of the graph Y is defined as follows. The vertices of $L(Y)$ are the edges of Y; two edges of Y are adjacent in $L(Y)$ if they share a vertex in Y.

We shall say that X is a *graphic* SR graph if X or its complement is the line graph of 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 the line graph $L(Y)$ of the graph Y is SR exactly if Y is either a complete graph K_v or the complete bipartite graph $K_{v,v}$ or the cycle of length 5.

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

We describe two more important families of strongly regular graphs.

An *incidence geometry* is a triple $\mathfrak{X} = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ where $\mathcal{P}$ is a set of "points," $\mathcal{L}$ a set of "lines," and $\mathcal{I} \subseteq \mathcal{P} \times \mathcal{L}$ is an incidence relation. The *length* of a line is the number of points with which it is incident. The *line-graph* $L(\mathfrak{X})$ has vertex set $\mathcal{L}$; two lines are adjacent if they intersect (they are both incident with the same point in $\mathcal{P}$).

A *Steiner 2-design* is an incidence geometry where every line has the same length $s \geq 3$ and there is exactly one line passing through every pair of points. If the design has v points then it has $v(v-1)/s(s-1)$ lines.

A *transversal design* with $s \geq 3$ classes is an incidence geometry of which the points are divided into s equal "classes," every line intersects each class in exactly one point, and there is exactly one line through every pair of points from different classes. If the design has v points then it has $(v/s)^2$ lines.

The line-graphs of each of these designs are strongly regular.

Up to a certain threshold value s (as a function of v), each type of design is uniquely reconstructable from its line-graph (cf., e. g., [49, 16]). (This means in particular that every automorphism of the line-graph is induced by an automorphism of the underlying design.) In each case, the threshold value is asymptotically $s \lesssim v^{1/3}$. This corresponds to degree $k \lesssim n^{2/3}$. (The $a_n \lesssim b_n$ relation ["less than or asymptotically equal"] relation between sequences a_n, b_n is defined by the asymptotic equality $a_n \sim \min\{a_n, b_n\}$ (or equivalently, $b_n \sim \max\{a_n, b_n\}$).)

We say that the SR graph X is *geometric* if X or its complement is the line-graph of one of these two types of design, with the parameter s in the unique reconstructability regime.

We shall need the following result.

Theorem 2.1 ([2])**.** *If X is a non-trivial SR graph of degree $k \leq (n-1)/2$ then $\mathrm{Aut}(X)$ has a base of size $\leq 2(n/k)\ln n$ and therefore $\mathrm{Aut}(X) \leq n^{2(n/k)\ln n}$.*

2.2. Eigenvalues

By the *eigenvalues* of a graph we mean the eigenvalues of its adjacency matrix.

The following well-known facts easily follow from the definition, cf. [18, Lemma 1.1.1 and Theorem 1.3.1].

Proposition 2.2. *Let X be a non-trivial SR graph with parameters (n, k, λ, μ).*

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

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

(iii) If X *is a conference graph then its eigenvalues are* $r = (-1 + \sqrt{n})/2$ *and* $-s = (-1 - \sqrt{n})/2$*.*

(iv) If X *is not a conference graph then all eigenvalues are integers.*

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

We infer the following elementary estimates.

Proposition 2.3. *Let* X *be a non-trivial SR graph of degree* $k \leq (n-1)/2$*. Then*

(a) $\mu \leq 2k^2/n$

(b) $\max\{r, s\} \leq \max\{\sqrt{2k}, 2\mu, 2\lambda\}$*.*

Proof. From part (i) of Prop. 2.2 we infer that $\mu((n-1)/2) \leq \mu(n-k-1) \leq k(k-1)$ and therefore $\mu \leq 2k(k-1)/(n-1) < 2k^2/n$, proving (a).

It follows from (v) that if $s/2 \leq r \leq 2s$ then $k \geq rs \geq (1/2)\xi^2$ (where $\xi = \max(r, s)$) and therefore $\xi \leq \sqrt{2k}$. If $r > 2s$ then $r/2 < r - s \leq \lambda$ and therefore $\xi = r < 2\lambda$. If $s > 2r$ then $\mu > \mu - \lambda = s - r \geq s/2$ and therefore $\xi = s < 2\mu$. □

The case $s = 2$ was characterized in the 1980s by Hoffman and Ray-Chaudhuri [26] and Seidel [48]. For a particularly elegant treatment, see [20].

Theorem 2.4 (Seidel [48], cf. [20, Theorem 4.13])**.** *If* X *is a non-trivial SR graph with* $n \geq 29$ *vertices and least eigenvalue* $-s = -2$ *then* X *is graphic (the line graph of* K_v *or* $K_{v,v}$*).*

This result was used as a key tool in [5] to separate the graphic cases from the other SR graphs.

2.3. The Neumaier classification of SR graphs

A far reaching generalization of Seidel's result was given by Neumaier [43, 44], highlighting the significance of the geometric case. We rephrase Neumaier's classification of SR graphs here.

Let X be a regular graph of degree k. Let $k = \xi_1 \geq \xi_2 \geq \cdots \geq \xi_n$ denote its eigenvalues. 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 $\sum x_i = 0$.)

Theorem 2.5 (Neumaier [43, 44])**.** *A strongly regular graph is either trivial, or graphic, or geometric, or a conference graph, or satisfies "Neumaier's claw bound."*

The *claw bound* is an inequality involving the parameters and the eigenvalues of the SR graph. What matters for us are the following asymptotic consequences of the claw bound.

First, if $k/n \to 0$ then μ is asymptotically determined (Spielman [49]):

$$\mu/n \sim (k/n)^2 \tag{1}$$

Strong bounds on λ also follow from the claw bound. Let

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

We assume $k \leq (n-1)/2$ (otherwise we can take the complement of G).

Theorem 2.6. *Let X be a SR graph with parameters (n,k,λ,μ) satisfying the claw bound. Then*

$$\frac{\lambda}{n} = O(h(n,k)).$$

The function $h(n,k)$ evaluates to

(i) $(k/n)^{4/3}$ for $k \leq n^{5/8}$

(ii) $n^{-1/2}$ for $n^{5/8} \leq k \leq n^{2/3}$

(iii) $(k/n)^{3/2}$ for $k \geq n^{2/3}$.

Part (i) is by Spielman [49]. Parts (ii) and (iii) are improvements over Spielman's bounds, obtained in [17], building on a clique structure found by Metsch [39, 40].

We note that the function $h(n,k)$ is continuous so up to constant factors the transition is continuous around the boundaries of the intervals above.

We note the following corollary.

Corollary 2.7. *For SR graphs satifying the claw bound and satisfying $k = o(n)$, we have $\lambda = o(k)$ and $\xi = o(k)$.*

2.4. A SR graph with large primitive automorphism group

In this section we prove Prop. 1.12.

Let X be the line-graph of the Steiner triple system consisting of the points and lines of $\mathrm{PG}(d,2)$, the d-dimensional projective space over $\mathbb{F}_2$. This is a SR graph with $n = (2^{d+1}-1)(2^d-1)/3 \sim 2^{2d+1}/3$ vertices. Its automorphism group is $\mathrm{PGL}(d+1,2)$, of order $\sim c2^{d(d+1)/2}$ where $c = \prod_{i=1}^{\infty}(1-2^{-i}) \approx 0.289$. Thus, $|\mathrm{Aut}(X)| > n^{(\log_2 n - 1)/8}$.

3. Fixed points of automorphisms

3.1. Fixed points: a spectral bound

The following general result does not assume that X is SR.

Proposition 3.1. *Let X be a regular graph of degree k. Suppose every pair of vertices in X has at most q common neighbors. Let ξ be the zero-weight spectral radius of X. Then*

(a) every non-identity automorphism of X has at most $n(q+\xi)/k$ fixed points;

(b) if $q + \xi < k$ then every non-identity automorphism of X has order at most $n^{k/(k-q-\xi)}$.

For the proof we need the following form of the "Expander Mixing Lemma" by Alon and Chung [1].

Lemma 3.2. *Let $X = (V, E)$ be a regular graph of degree k. Let $d(S)$ denote the average degree of the subgraph induced by $S \subseteq V$. Then*

$$|d(S) - (|S|/n)k| \leq \xi. \tag{2}$$

Therefore, there is a vertex in S that has at least $(1-|S|/n)k - \xi$ neighbors outside S.

For completeness we include the simple proof in the Appendix.

Proof of part (a) of Proposition 3.1. 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 Lemma 3.2, there exists $x \in S$ such that $|N(x)| \geq (1-|S|/n)k - \xi$. On the other hand, $N(x) = N(x^\sigma)$, therefore $|N(x)| \leq q$. We infer that $q \geq (1-|S|/n)k - \xi$, and therefore the number of points fixed by x is $n - |S| \leq n(q+\xi)/k$. □

3.2. Fixed points of automorphisms of SR graphs

The goal of this section is to prove Theorem 1.6, combining Proposition 3.1 and results from [2].

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

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

Lemma 3.3 ([2])**.** *Let X be a non-trivial SR 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. 2.2 and Lemma 3.3.

Lemma 3.4. *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 3.3 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 2.2 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. 2.2 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. 2.2, we have $r < k/s \leq k/3$. Therefore $\mu + r < 2k/3$. □

Lemma 3.5. *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 $q + \xi < 7k/8$.*

Proof. Modulo the change of notation ($q = \vartheta_1$ and $\xi = r$), the conclusion of Lemma 3.5 is the same as the conclusion of part (B) of Lemma 3.4. We only need to justify the assumption $s \geq 3$ made in Lemma 3.4, part (B). We have $s \geq 2$ by item (ii) of Prop. 2.2 since X is nontrivial. If X is a conference

graph then $s \geq (1+\sqrt{29})/2 > 3$ by item (iii) of Prop. 2.2 since $n \geq 29$. If X is not a conference graph then s is an integer by item (iv) of Prop. 2.2. So we only need to rule out the case $s = 2$; this is done by Seidel's theorem (Theorem 2.4). □

These preparations will suffice for the proof of Theorem 1.6 in the case $k < n/4$. For the cases when k is large, we use a different tool.

Lemma 3.6. *Let X be a nontrivial SR 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 [2], we say that vertex x *distinguishes* vertices y and z if x is adjacent to exactly one of y and z.

Lemma 3.7 ([2])**.** *Let X be a nontrivial SR 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 3.6. According to part (A) of Lemma 3.4, we have $\vartheta_2 < k/2$ and therefore by Lemma 3.7, 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 $|F| < n - k/2$. □

Proof of Theorem 1.6. I. If $k < n/4$ then by Lemma 3.5 we have $q + \xi < 7k/8$ and therefore, by Prop. 3.1, σ fixes fewer than $7n/8$ points.

II. Let us now assume $n/4 \leq k \leq (n-1)/2$. Then, by Lemma 3.6, σ fixes fewer than $n - k/2 \leq 7n/8$ points. □

3.3. Fixed points vs. order

The following lemma was found by Ákos Seress and the author within hours of the beginning of their life-long collaboration. (See [5, 15] for detailed story and a list of applications of the lemma.)

Lemma 3.8 ([12, 15])**.** *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; this is remedied in [15] (see also [5]).

Now part (b) of Proposition 3.1 follows by combining part (a) with Lemma 3.8, and Theorem 1.5 follows by combining Theorem 1.6 with Lemma 3.8.

4. Finer estimation of the number of fixed points

In this section we use Neumaier's classification to prove Theorem 1.7.

Proof. By Prop. 3.1 it suffices to show that $q + \xi$ is bounded from above by $O(k^{3/2}/n^{1/2})$ in case (a) and by $O(k/n^{1/8})$ in case (b).

By part (b) of Prop. 2.3 it suffices to prove that $q = \max\{\lambda, \mu\}$ satisfies the required bound.
(a) Assume $k \geq n^{2/3}$. We need to show $q = O(k^{3/2}/n^{1/2})$. Now by part (a) of Prop. 2.3 we have $\mu < 2k^2/n < 2k^{3/2}/n^{1/2}$, and $\lambda = O(k^{3/2}/n^{1/2})$ by part (iii) of Theorem 2.6.
(b) In the range where parts (a) and (b) of Theorem 1.7 overlap, i. e., $n^{2/3} \leq k \leq n^{3/4}$, we have $\sqrt{kn} \leq n^{7/8}$, so part (b) follows from part (a).

For $k < n^{7/8}$ we have $\mu < 2k^2/n < 2k/n^{1/8}$ by part (a) of Prop. 2.3.

In the range $n^{5/8} \leq k \leq n^{2/3}$, we obtain $\lambda = O(n^{1/2}) = O(k/n^{1/8})$ by part (ii) of Theorem 2.6.

Finally, for $\sqrt{n-1} \leq k \leq n^{5/8}$ we have $\lambda = O(k^{3/2}/n^{1/2}) = O(k/n^{1/8})$ by part (i) of Theorem 2.6. □

Proof of Theorem 1.9. Putting both parts of Theorem 1.7 together, we see that for all $k \leq n/(\log_2 n)^2$ we have $\mathrm{fix}(X) = O(n/\log n)$. It follows by Lemma 3.8 that the order of every element of $\mathrm{Aut}(X)$ is $\leq n^{1+O(1/\log n)} = O(n)$. □

5. SR graphs with large primitive groups

Sharpening results of Cameron [19] and Liebeck [33], Attila Maróti [38] proved the following remarkably tight structural threshold for primitive permutation groups.

Theorem 5.1 (Maróti [38])**.** *Let G be a primitive permutation group of degree n. Then one of the following holds:*

(i) G is a subgroup of $S_m \wr S_r$ containing $(A_m)^r$, where $m \geq 5$, the action of S_m is on k-element subsets of $\{1, \ldots, m\}$, and the wreath product has the product action of degree $n = \binom{m}{k}^r$;

(ii) G is a Mathieu group M_{11}, M_{12}, M_{23} or M_{24} in its 4-transitive action;

(iii) $|G| < n^{1+\lfloor \log_2 n \rfloor}$.

We use this result in combination with Theorem 1.6 to prove Theorem 1.11.

Proposition 5.2. *If G is a primitive permutation group of degree $n \geq 25$ and $|G| \geq n^{1+\log_2 n}$ then G is in Maróti's case (i) with $m \geq \log_2 n$.*

Proof. It is clear that we are in case (i) of Maróti's theorem. We need to ensure $m \geq \log_2 n$.

We have $n = (\binom{m}{k})^r \geq m^r$ and therefore $r \leq (\log_2 n)/(\log_2 m)$. Moreover we have $n^{1+\log_2 n} \leq |G| \leq (m!)^r r! < m^{rm} r! \leq n^m r!$. It follows that if $m \leq \log_2 n$ then $r! \geq n$ and therefore $r \log_2 r > \log_2 n$. On the other hand, $r \leq (\log_2 n)/(\log_2 m)$ and therefore $r \log_2 r < (\log_2 n)(\log_2 r)/\log_2 m$. It follows that $\log_2 r/\log_2 m \geq 1$ and therefore $r \geq m$. But then $n \geq m^r \geq m^m > m!$ and therefore $|G| \leq (m!)^r r! < n^r r! < (nr)^r$. But $r \leq (\log_2 n)/(\log_2 m) \leq (\log_2 n)/(\log_2 5) < n$, so $|G| < (nr)^r < (n^2)^{(\log_2 n)/(\log_2 5)} < n^{\log_2 n}$, contradicting the assumption that $|G| \geq n^{1+\log_2 n}$. □

Proof of Theorem 1.11. Let $G = \mathrm{Aut}(X)$. Assume $|G| \geq n^{1+\log_2 n}$. By the preceding proposition we are in case (i) of Maróti's theorem with $m \geq \log_2 n$ (assuming $n \geq 25$).

Let σ be a 3-cycle of the group A_m in the socle of G. The proportion of k-tuples that do not intersect the support of σ is $\alpha = \binom{m-3}{k}/\binom{m}{k}$. Clearly the permutation in G induced by σ fixes at least αn points. It follows from Theorem 1.6 that $\alpha \leq 7/8$. On the other hand, $\alpha > (1 - (k/(m-2)))^3$ and therefore $k \geq \beta(m-2)$ where $\beta = 1 - (7/8)^{1/3} \approx 0.04353 > 1/23$. It follows that for sufficiently large n (and therefore sufficiently large m) we have $k \geq m/23$. Therefore $\binom{m}{k} > (m/k)^k \geq 23^{m/23} > 2^{0.12m} > 2^{0.1187(m+1)} > 2^{(m+1)/9}$ so $n > 2^{((m+1)r)/9}$. On the other hand, $|G| < (m!)^r r! < (rm^m)^r < m^{(m+1)r} < n^{9\log_2 m}$. If now $|G| > n^{\log_2 n}$ then it follows that $m > n^{1/9}$. But $n \geq \binom{m}{k} > 2^k$, hence $k < \log_2 n$. Therefore $\alpha > (1 - (k/(m-2)))^3 > 1 - (3\log_2 n)/(n^{1/9} - 2) > 7/8$ for n greater than an absolute constant, a contradiction. (We estimate that $n \geq 4 \cdot 10^{30}$ suffices.) □

Remark 5.1. An alternative approach to proving and strengthening Theorem 1.11 would be the study of the subrings of the "cellular rings" associated with the coherent configurations corresponding to the large primitive permutation groups, in the spirit of the work initiated by Kaluzhnin and Klin in 1972 ([30], cf. [27, 25] and the bibliographies of those papers).

6. Appendix: the Expander Mixing Lemma

Included here for the reader's convenience, the "Expander Mixing Lemma," due to Alon and Chung [1], describes a powerful quasi-randomness property of graphs with small second eigenvalue.

Let A_X denote the adjacency matrix of the graph $X = (V, E)$ where $V = \{1, \ldots, n\}$. Assume X is k-regular. Let the eigenvalues of A_X be $k = \xi_1 \geq \xi_2 \geq \cdots \geq \xi_n$. Set $\xi = \max\{|\xi_i| \mid 2 \leq i \leq n\}$.

For 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.

Lemma 6.1. *Let $X = (V, E)$ be a k-regular graph with n vertices. Let $S, T \subseteq V$. Then*

$$\left| |E(S,T)| - \frac{|S||T|k}{n} \right| \leq \xi \sqrt{|S||T|}. \tag{3}$$

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

$$|E(S,T)| = \mathbf{1}_S^* A_X \mathbf{1}_T \tag{4}$$

and

$$|S||T| = \mathbf{1}_S^* J \mathbf{1}_T. \tag{5}$$

(The asterisk indicates transpose.) It follows that the left-hand side in equation (3) is equal to

$$|\mathbf{1}_S^* (A_X - (k/n)J) \mathbf{1}_T| \tag{6}$$

which by the Cauchy-Schwarz inequality is not greater than $\sqrt{|S||T|}$ times the spectral norm of $A_X - (k/n)J$. The eigenvalues of $A_X - (k/n)J$ are $0, \xi_2, \ldots, \xi_n$, so the spectral norm of $A_X - (k/n)J$ is ξ. □

Proof of Lemma 3.2. Note that $|E(S, S)| = |S|d(S)$ and apply Eq. (3) with $T = S$. □

7. Primitive coherent configurations

In this concluding section we describe the broader program underlying this work and offer several classes of open problems.

For a set V, let $\Delta(V) = \{(x, x) \mid x \in V\}$ denote the diagonal of V.

A *configuration* of rank r on a set V of vertices is an $(r+1)$-tuple $\mathfrak{X} = (V; R_0, \ldots, R_{r-1})$ where $(R_0, \ldots, R_{r-1})$ is a partition of $V \times V$ with the properties that

(o) none of the R_i is empty;

(i) for some $r_0 \le r$, the r_0-tuple $(R_0, \ldots, R_{r_0-1})$ is a partition of V;

(ii) for each i there exists j such that $R_i^{-1} = R_j$.

(Here $R_i^{-1} = \{(x,y) \mid (y,x) \in R_i\}$.)

The directed graph (digraph) $X_i = (V, R_i)$ is the i-th *constituent digraph* of $\mathfrak{X}$. The *proper constitutent digraphs* are the X_i with $i \ge r_0$ (i.e., $R_i \cap \Delta(V) = \emptyset$). We say that the pair $(x,y) \in V \times V$ has *color* i if $(x,y) \in R_i$.

A *coherent configuration* is a configuration with a list of r^3 "structure constants" p_{ij}^k such that

(iii) for all i, j, k, if $(x,y) \in R_k$ then

$$|\{z \in (x,z) \in R_i \text{ and } (z,y) \in R_j\}| = p_{ij}^k.$$

A configuration is *homogeneous* if

(iv) $r_0 = 0$, i. e., $R_0 = \Delta(V)$.

A homogeneous configuration is *primitive* if

(v) all proper constituent graphs are (strongly) connected.

Note that in a homogeneous configuration, a weakly connected proper constitutent graph is necessarily strongly connected.

The *automorphisms* of a configuration are those permutations of the vertex set that preserve edge color, i. e., $\mathrm{Aut}(\mathfrak{X}) = \bigcap_{i=0}^{r-1} \mathrm{Aut}(V, R_i)$.

A digraph $X = (V, E)$ gives rise to a homogeneous configuration $\mathfrak{X}(X) = (V; \Delta(V), E, E')$ where $E' = (V \times V) \setminus (\Delta(V) \cup E)$. (If $E = \emptyset$ then E needs to be omitted from the list; same about E'.) Observe that if X is an *undirected* graph (i. e., $E^{-1} = E$) then $\mathfrak{X}(X)$ is coherent if and only if X is strongly regular.

If $X = (V, E)$ is a tournament (i. e., $E \cap E^{-1} = \emptyset$ and $\Delta(V) \cup E \cup E^{-1} = V \times V$) and $\mathfrak{X}(X)$ is coherent then we call X a *SR tournament.*

If G is a permutation group on the set V then let $\mathfrak{X}(G)$ denote the configuration $(V; R_0, \ldots, R_{r-1})$ where the R_i are the orbits of the G-action on $V \times V$, arranged in order such that the union of the first r_0 is the diagonal. (Here r_0 is the number of orbits of G on V.) Note that this configuration is coherent; its rank is called the rank of G. We refer to the coherent configurations $\mathfrak{X}(G)$ as the *group case*. Note that $G \leq \mathrm{Aut}(\mathfrak{X}(G))$. However, coherent configurations in general do not need to have nontrivial automorphisms.

Observe that G is *transitive* if and only if $\mathfrak{X}(G)$ is *homogeneous*; and G is *primitive* if and only if $\mathfrak{X}(G)$ is primitive.

1. It would be interesting to extend some of the current work on automorphisms of SR graphs to primitive coherent configurations.

Conjecture $P(\epsilon)$**.** *There exists a threshold* $n(\epsilon)$ *such that if a primitive coherent configuration* $\mathfrak{X}$ *with* $n \geq n(\epsilon)$ *vertices has more than* $\exp(n^\epsilon)$ *automorphisms then* $\mathrm{Aut}(\mathfrak{X})$ *is a primitive group.*

Given Cameron's explicit description of the large primitive groups [19], this would amount to characterizing all primitive coherent configurations with large automorphism groups[6].

Let ϵ_0 denote the infimum of those values $\epsilon > 0$ for which $P(\epsilon)$ holds. Ideally we would have $\epsilon_0 = 0$. In case $\epsilon_0 > 0$, one would expect interesting families of primitive coherent configurations to arise.

It was proved in [3] (1981) that $\epsilon_0 \leq 1/2$, and by Sun and Wilmes [50] (2014) that $\epsilon_0 \leq 1/3$.

Let $P(\epsilon, \mathrm{SRG})$ denote the restriction of $P(\epsilon)$ to SR graphs and $\epsilon_0(\mathrm{SRG})$ the infimum of those values $\epsilon > 0$ for which $P(\epsilon, \mathrm{SRG})$ holds. Obviously, $\epsilon_0(\mathrm{SRG}) \leq \epsilon_0$. It was proved in [2] (1980) that $\epsilon_0(\mathrm{SRG}) \leq 1/2$; this was improved by Daniel Spielman [49] (1996) to $\epsilon_0(\mathrm{SRG}) \leq 1/3$; and by Xi Chen, Xiaorui Sun, and Shang-Hua Teng [23] (2013) to $\epsilon_0(\mathrm{SRG}) \leq 9/37$.

We note that a SR tournament has at most $n^{O(\log n)}$ automorphisms [3], so $P(\epsilon)$ restricted to SR tournaments is true for every $\epsilon > 0$.

Subclasses of interest, other than SR graphs, include primitive (metric) association schemes (generated by distance-transitive graphs), and primitive coherent configurations of bounded rank.

[6] A study of the combinatorial structure of the Cameron schemes – the rpimitive coherent configurations corresponding to the large primitive groups – was a key ingredient in this author's work with Gene Luks and Ákos Seress in designing a highly paralellel "NC algorithm" for permutation group membership [9].

2. Extend Theorem 1.3 to primitive coherent configurations as follows.

Thickness Conjecture. *For every $\epsilon > 0$ there exists a threshold $n(\epsilon)$ such that if the automorphism group of a primitive coherent configuration X with $n \geq n(\epsilon)$ vertices involves an alternating group of degree $\geq n^\epsilon$ (i. e., $\theta(\mathrm{Aut}(X)) \geq n^\epsilon$) then $\mathrm{Aut}(X)$ is a primitive group.*

It follows from Theorem 1.3 that the Thickness Conjecture is true if restricted to SR graphs. It is also clear that the Thickness Conjecture holds for every $\epsilon > \epsilon_0$.

3. We state a conjecture that is weaker than Conj. 1.1.

Subexponential order conjecture. *If X is a non-trivial, non-graphic SR graph with n vertices then $|\mathrm{Aut}(X)| = \exp(n^{o(1)})$.*

Below we describe a possible approach to this problem,

Recall that for a permutation group G, we write $\mathrm{fix}(G)$ to denote the maximum number of elements fixed by a non-identity element of G. (So $\mathrm{fix}(G) = n - \mu(G)$ where $\mu(G)$ is the minimum degree of G.)

A permutation group is *2-closed* if it is the automorphism group of an edge-colored directed graph. For instance, the only 2-closed doubly transitive group is S_n.

Problem 7.1. True or false: For every $\epsilon > 0$ there exists $n(\epsilon)$ such that if $n \geq n(\epsilon)$ and G is a 2-closed elementary abelian permutation group of degree n and order $|G| \geq \exp(n^\epsilon)$ then $\mathrm{fix}(G) \geq n^{1-\epsilon}$.

Note: Clearly true for $\epsilon > 1/2$ even without the assumption of 2-closedness. However, for small ϵ the statement is false without the assumption of 2-closedness.

Note: if the answer is "true" then the subexponential order conjecture follows.

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 [16, 22, 7]; and a conversation with Ian Wanless about the order

of automorphisms of quasigroups, the subject of a paper by McKay, Wanless, and Zhang [37]. 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.

And above all, I'd like to recognize my debt to Ákos Seress, my number one collaborator with 15 joint papers over a period of a quarter century. Ákos's mark can be found all over my work of the past several decades; most relevant to the present paper are [9**?** , 11, 12, 13, 14], partly because all of them employ Lemma 3.8 (cf. [15]).

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

References

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

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

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

[4] László Babai: On the order of doubly transitive permutation groups. *Invent. Math.* **65** (1982) 473–484.

[5] László Babai: On the automorphism groups of strongly regular graphs I. *In: Proc. 5th Innovations in Computer Science conf. (ITCS'14)*, ACM Press, 2014, pp. 359-368. DOI: 10.1145/255497.2554830. Available on author's home page, http://people.cs.uchicago.edu/∼laci/papers/

[6] 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.

[7] László Babai, Xi Chen, Xiaorui Sun, Shang-Hua Teng, John Wilmes: Faster Canonical Forms For Strongly Regular Graphs. *In: 54th IEEE FOCS*, 2013, pp. 157-166. Journal version to appear in the FOCS'13 special issue of SIAM J. on Computing

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

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

[10] László Babai, Eugene M. Luks, Ákos Seress: Fast management of permutation groups. In: Proc 29th IEEE FOCS, 1988, 272–282

[11] László Babai, Eugene M. Luks, Ákos Seress: Fast management of permutation groups I. *SIAM J. Comput.* **26** (1997), 1310–1342

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

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

[14] László Babai, Ákos Seress: On the diameter of permutation groups. *Europ. J. Comb.* **13** (1992), 231–243

[15] László Babai, Ákos Seress: Element order versus minimal degree in permutation groups: an old lemma with new applications. Eprint, 2014: arXiv:1401.0489

[16] László Babai, John Wilmes: Quasipolynomial-Time Canonical Form for Steiner Designs. *In: 45th ACM STOC*, 2013, pp 261–270

[17] László Babai, John Wilmes: Asymptotic Delsarte cliques in distance-regular graphs. Manuscript, 2014. Available on author's home page, http://people.cs.uchicago.edu/∼laci/papers/

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

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

[20] 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

[21] Alan R. Camina, Johannes Siemons: Block transitive automorphism groups of $2-(v,k,1)$ block designs. J. Combinatorial Theory Ser. A **51(2)** (1989) 268-276.

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

[23] Xi Chen, Xiaorui Sun, Shang-Hua Teng: On the order of the automorphism groups of strongly regular graphs. Manuscript, 2013.

[24] D. Huw Davies: *Automorphisms of Designs.* Ph.D. Thesis, University of East Anglia, 1987.

[25] Igor A. Faragiev, Alexander A. Ivanov, Mikhail H. Klin: Galois correspondence between permutation groups and cellular rings (association schemes). *Graphs and Combinatorics* **6** (1990) 303–332.

[26] Alan J. Hoffman, Dijen K. Ray-Chaudhury: On a spectral characterization of regular line graphs. Unpublished mansucript, cited by [20]

[27] Gareth A. Jones, K. D. Soomro: The maximality of certain wreath products in alternating and symmetric groups. *Quart. J. Math. Oxford (2)* **37(4)** (1986) 419–435.

[28] Camille Jordan: Sur la limite de transitivité des groupes non alternés. *Bull. Soc. Math. France* **1** (1873), 40–71

[29] Camille Jordan: Nouvelles recherches sur la limite de transitivité des groupes qui ne continennent pas le groupe alterné. *J. Math, (5)* **1** (1895), 35–60

[30] Lev A. Kaluzhnin, Mikhail H. Klin: On some maximal subgroups of symmetric and alternating groups. *Mat. Sb. Nov. Ser.* **87** (1972) 91–121 (in Russian)

[31] William M. Kantor: Permutation representations of the finite classical groups of small degree or rank. *J. Algebra* **60** (1979) 158–168.

[32] Peter B. Kleidman, Martin W. Liebeck: On a theorem of Feit and Tits. *Proc. AMS* **107(2)** (1989) 315–322.

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

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

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

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

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

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

[39] Klaus Metsch: Improvement of Bruck's completion theorem. *Designs, Codes, and Cryptography* **1(2)** (1991), 99–116.

[40] Klaus Metsch: On a characterization of bilinear forms graphs. *Europ. J. Comb.* **20(4)** (1999), 99–116

[41] Brendan D. McKay, Alison Meynert, Wendy Myrvold: Small Latin squares, quasigroups and loops. *J. Combinatorial Designs* **15** (2007) 98–119.

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

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

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

[45] László Pyber: On the orders of doubly transitive permutation groups, elementary estimates. *J. Combinat. Theory, Ser. A* **62(2)** (1993) 361–366.

[46] László Pyber: How abelian is a finite group? *In: The Mathematics of Paul Erdős*, Vol. I., R. L. Graham and J. Nešetřil, eds., "Algorithms and Combinatorics" Vol. 13, Springer 1997, pp.372–384.

[47] László Pyber. Unpublished, cited by [35]

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

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

[50] Xiaorui Sun and John Wilmes, Primitive coherent configurations with many automorphisms, manuscript, 2014.