# Primitive coherent configurations and the order of uniprimitive permutation groups

László Babai[*]

October 21, 2018

**Abstract**

These notes describe the author's elementary graph theoretic proof of the nearly tight $\exp(4\sqrt{n}\ln^2 n)$ bound on the order of primitive, not doubly transitive permutation groups (*Ann. Math., 1981*). The exposition incorporates a lemma by V. N. Zemlyachenko that simplifies the proof.

The central concept in the proof is *primitive coherent configurations*, a combinatorial relaxation of the action of primitive permutation groups. The exposition follows the authors' 2003 REU lecture; simple observations are listed as exercises.

## 1 Large primitive groups

We say that a permutation group is *uniprimitive* if it is primitive but not doubly transitive. The following result appeared in [Ba81] in 1981, solving a then century-old problem.

**Theorem 1.1.** *If $G$ is a uniprimitive permutation group of degree $n$ then $|G| < \exp(4\sqrt{n}\ln^2 n)$.*

In this note we give an exposition of the proof that incorporates a simplification by Viktor N. Zemlyachenko. The proof is an entirely elementary combinatorial argument. It does not even use the concept of groups except for the translation of the problem to a purely combinatorial question.

The bound is tight apart from a logarithmic factor in the exponent, as shown by the bullet point list below.

**Exercise 1.2.** All groups in the bullet point list below are primitive and all but $S_n$ and $A_n$ are uniprimitive.

[*] Based on a 2003 REU lecture; scribe: Tom Hayes. Revised: LB, May 2011 and October 2018.

Let $[n]$ denote the set $\{1,\dots,n\}$. Let $S_n$ and $A_n$ denote the symmetric and the alternating groups of degree $n$, respectively. For a permutation group $G \le S_n$ we write $G^{(t)}$ to denote the induced action of $G$ on the set of $\binom{n}{t}$ $t$-subsets of $[n]$, so $G_n^{(t)} \le S_{\binom{n}{t}}$.

We say that two sequences of numbers $a_n, b_n > 1$ are log-asymptotically equal if their logarithms are asymptotically equal: $\ln a_n \sim \ln b_n$, i. e.,

$$\lim_{n\to\infty} \frac{\ln a_n}{\ln b_n} = 1.$$

We write $a_n \approx b_n$ to denote this circumstance.

The following is a list of large primitive groups.

- $S_n$ and $A_n$ (of orders $n!$ and $n!/2$, respectively)
- $S_k^{(2)}$ and $A_k^{(2)}$ (for $n = \binom{k}{2}$), of orders $k!$ and $k!/2$, resp.; both numbers are log-asymptotically equal to $\exp(\sqrt{n/2}\ln n)$
- $S_k \wr S_2$ and $A_k \wr S_2$ (acting on $n = k^2$ elements), of orders $2(k!)^2$ and $(1/2)(k!)^2$, resp.; both numbers are log-asymptotically equal to $\exp(\sqrt{n}\ln n)$
- the unique group $H$ such that $A_k \wr S_2 < H < S_k \wr S_2$ (also for $n = k^2$); $H$ has order $k! \approx \exp(\sqrt{n}\ln n)$.

These are in fact the largest primitive groups.

**Theorem 1.3.** *The exists a constant $c$ such that for sufficiently large $n$, all primitive permutation groups not in the list above have order at most* $\exp(n^{1/3}(\ln n)^c)$.

This result follows from a 1981 result by Peter Cameron [Ca81] that heavily relies on the Classification of Finite Simple Groups (CFSG). As of 2015, an elementary proof also exists. Much stronger bounds on the order of doubly transitive groups were proved by Babai [Ba82] and Pyber [Py93] decades ago. The uniprimitive case was recently settled by Xiaorui Sun and John Wilmes in their remarkable work on uniprimitive coherent configurations [SW15].

In this note we focus on the uniprimitive case.

The problem of bounding the orders of primitive permutation groups goes back to the 19th century. The following papers were the milestones in the development of bounds that do not rely on the CFSG.

**Theorem 1.4.** *Assume $G \le S_n$, $A_n \not\le G$, and $G$ is primitive.*

*1.* (Bochert, 1889 [Bo1889]) $\quad |G| \le \dfrac{n!}{\lceil n/2 \rceil !} \approx \exp\left(\dfrac{n}{2}\ln n\right)$

*2.* (Wielandt, 1934 [Wi34], Praeger–Saxl, 1980 [PrS80]) $|G| < 4^n$
(using nontrivial elementary group theory)

*3.* (Babai, 1981 [Ba81]) *If $G$ is uniprimitive then* $|G| < \exp(4\sqrt{n}\ln^2 n)$
(using no group theory at all, only graphs and a simple probabilistic argument)

*4.* (Babai, 1982 [Ba82]) *If $G$ is doubly transitive then* $|G| < \exp\exp(1.18\sqrt{\ln n})$
(using elementary group theory and a simple probabilistic argument)

*5.* (Pyber, 1993 [Py93]) *If $G$ is doubly transitive then* $|G| < \exp(O(\ln^4 n))$
(using elementary group theory and the probabilistic argument of [Ba82]) and $|G| < \exp(O(\ln^3 n))$ (using additionally an elementary group theoretic result of Wielandt [Wi34])

*6.* (Sun–Wilmes, 2015 [SW15]) *If $G$ is uniprimitive and not on the list above then* $|G| < \exp(O(n^{1/3}\ln^{7/3} n))$ (using no group theory at all, only graphs in the framework of [Ba81])

## 2 Coherent configurations

Remarks about symmetry and regularity: symmerty conditions are given in terms of automorphisms; regularity conditions in terms of numerical parameters. Symmetry condition imply regularity conditions (e. g., vertex-transitivity is a symmetry condition, which implies that the graph is regular, a regularity condition). The converse is seldom true. We shall define regularity conditions on a family of edge-colored digraphs which capture some combinatorial consequences of primitive group action. Using this translation, we shall prove a combinatorial result which implies a nearly optimal upper bound on the order of uniprimitive permutation groups.

Let $\Omega$ be a finite set, and $\Delta = \{(x, x) \mid x \in \Omega\}$ the *diagonal* of $\Omega \times \Omega$.

**Definition 2.1** (Coherent configuration)**.** Let us consider a structure of the form $\mathfrak{X} = (\Omega; R_0, \dots, R_{r-1})$, where $R_i \subseteq \Omega \times \Omega$ and the non-empty sets $R_i$ partition $\Omega \times \Omega = R_0 \dot\cup \dots \dot\cup R_{r-1}$. The number $r$ is the *rank* of $\mathfrak{X}$.

We call the digraph $X_i = (\Omega, R_i)$ the *color-$i$ constituent* of $\mathfrak{X}$. The color of a pair $x, y$ is defined as $c(x, y) = i$ if $(x, y) \in R_i$.

To be coherent, $\mathfrak{X}$ needs to satisfy the following three axioms.

A1: $c(x, x) = c(y, z) \Rightarrow y = z$. In other words, some of the $R_i$ form a partition of the diagonal $\Delta = R_0 \dot\cup \dots \dot\cup R_{i_0-1}$. Terminology: we call $c(x) := c(x, x)$ the color of vertex $x$.

A2: $(\forall i)(\exists j)(R_j = R_i^{-1})$. Terminology: $R_i$ is *self-paired* if $R_i = R_i^{-1}$, i. e., $X_i$ is undirected.

A3: $(\exists p_{i,j,k})(\forall (x, y) \in R_i)(\#\{z \mid c(x, z) = j, c(z, y) = k\} = p_{i,j,k})$

The $r^3$ parameters $p_{i,j,k}$ are called the *intersection numbers* of $\mathfrak{X}$.

**Exercise 2.2.** The number of $x \to \cdots \to y$ walks of a given length and given color-composition (given sequence of colors) only depends on $c(x, y)$.

An *automorphism* of a coherent configuration is a color-preserving permutation of its set of vertices. $\mathrm{Aut}(\mathfrak{X})$ denotes the group of automorphisms. So the permutation $\pi \in \mathrm{Sym}(\Omega)$ belongs to $\mathrm{Aut}(\mathfrak{X})$ if and only if $(\forall x, y)(c(x, y) = c(x^\pi, y^\pi))$.

## 3 The group case

**Definition 3.1.** An *orbital* $\Gamma$ of a permutation group $G \leq \mathrm{Sym}(\Omega)$ is an orbit of $G$ on the set of ordered pairs ($\Gamma \subset \Omega \times \Omega$). $\Gamma$ is *self-paired* when $\Gamma = \Gamma^{-1}$ (i. e., for $(x, y) \in \Gamma$ there exists $\sigma \in G$ such that $x^\sigma = y$ and $y^\sigma = x$). The *rank* $r$ of a permutation group is the number of its orbitals.

**Exercise 3.2.** If $n \geq 2$ then $G$ is doubly transitive if and only if $\mathrm{rk}(G) = 2$.

**Definition 3.3.** For $G \leq \mathrm{Sym}(\Omega)$, we set $\mathfrak{X}(G) := (\Omega; \text{orbitals})$.

**Exercise 3.4.** Prove: $\quad \mathfrak{X}(G)$ is a coherent configuration.

We refer to $\mathfrak{X}(G)$ as a "Schurian" coherent configuration;" collectively, they form "the group case."

**Exercise 3.5.** $G \leq \mathrm{Aut}(\mathfrak{X}(G))$.

**Remark 3.6.** There exist coherent configurations that are not Schurian. In fact, there are exponentially many rank-3 coherent configurations with no automorphisms.

## 4 Coherent configurations: homogeneous, primitive

In this section, $\mathfrak{X}$ is a coherent configuration.

**Definition 4.1.** $\mathfrak{X}$ is *homogeneous* if all vertices have the same color, i. e., the diagonal is one of the constituents. In this case we set $R_0 = \Delta$.

**Exercise 4.2.** $\mathfrak{X}(G)$ is homogeneous $\iff$ $G$ is transitive.

**Definition 4.3.** A digraph is *Eulerian* if every vertex has the same indegree and outdegree.

**Exercise 4.4.** Prove: in an Eulerian digraph, every weakly connected component is strongly connected.

**Exercise 4.5.** If $\mathfrak{X}$ is homogeneous, then every constituent is *biregular*, i. e.,
$(\forall i \leq r - 1)(\exists \rho_i)(\forall x \in \Omega)(\text{in-degree}_i(x) = \text{out-degree}_i(x) = \rho_i)$.

In particular, if $\mathfrak{X}$ is homogeneous then each constituent $X_i$ is Eulerian, and therefore its weak components are strongly connected.

**Exercise 4.6.** $\sum_{i=0}^{r-1} \rho_i = n$

**Definition 4.7.** $\mathfrak{X}$ is a *primitive* coherent configuration if $\mathfrak{X}$ is homogeneous and all constituent digraphs $X_i$ except the diagonal ($i \geq 1$) are connected.

**Exercise 4.8.** $\mathfrak{X}(G)$ is primitive $\iff$ $G$ is primitive.

**Definition 4.9.** The coherent configuration $\mathfrak{X}$ is *uniprimitive* if $\mathfrak{X}$ is primitive of rank $r \geq 3$.

**Exercise 4.10.** $\mathfrak{X}(G)$ is uniprimitive $\iff$ $G$ is uniprimitive (primitive but not doubly transitive).

## 5 Bases of permutation groups

Let $G \leq \mathrm{Sym}(\Omega)$. The *stabilizer* of $x \in \Omega$ in $G$ is the group $G_x = \{\sigma \in G \mid x^\sigma = x\}$. Let $\Psi \subseteq \Omega$. We denote the pointwise stabilizer of $\Psi$ in $G$ by $G_\Psi$, so $G_\Psi = \bigcap_{x \in \Psi} G_x$.

**Definition 5.1.** $\Psi \subseteq \Omega$ is a *base* of $G$ if $G_\Psi = \{1\}$.

**Exercise 5.2.** If $\Psi$ is a base of $G \leq S_n$ then $|G| \leq n^{|\Psi|}$.

In fact $|G| \leq n(n-1)\dots(n - |\Psi| + 1)$.

Therefore, Theorem 1.1 will follow from the following result.

**Theorem 5.3.** *If $G \leq S_n$ is a uniprimitive group then $G$ has a base of size $\leq 4\sqrt{n}\ln n$*

**Exercise 5.4.** How large is the smallest base for each permutation group listed in the bullet-point list in the Introduction?

## 6 Distinguishers

In this section, $\mathfrak{X} = (\Omega; R_0, \dots, R_{r-1})$ is a coherent configuration.

**Definition 6.1.** Vertex $z$ *distinguishes* vertices $x$ and $y$ if $c(x,z) \neq c(y,z)$. In this case we call $z$ a *distinguisher* of $x$ and $y$. $D(x,y) = \{z \mid c(x,z) \neq c(y,z)\}$ is the *set of distinguishers* of the pair $\{x,y\}$.

We shall see that the essence of our problem is to prove a strong lower bound on the size of the sets of pairwise distinguishers.

**Exercise 6.2.** If $\mathfrak{X} = \mathfrak{X}(G)$ and $z \in D(x,y)$, then $x, y$ are *not* in the same orbit of $G_z$. (Obvious, because the group preserves the colors.)

**Definition 6.3.** A *distinguishing set* of $\mathfrak{X}$ is any set $\Psi \subseteq \Omega$ such that $(\forall x \neq y)(\Psi \cap D(x,y) \neq \emptyset)$. In other words, for every pair $x, y$, $\Psi$ contains an element which distinguishes them.

**Exercise 6.4.** If $\Psi$ is a distinguishing set of $\mathfrak{X}$ then $\Psi$ is a base of $\mathrm{Aut}(\mathfrak{X})$. In particular, if $\Psi$ is a distinguishing set of $\mathfrak{X}(G)$ for a permutation group $G$ then $\Psi$ is a base of $G$.

Therefore, Theorem 5.3, and with it, Theorem 1.1, will follow from the following purely combinatorial result.

**Theorem 6.5.** *If $\mathfrak{X}$ is a uniprimitive coherent configuration with $n$ vertices then $\mathfrak{X}$ has a distinguishing set of size less than $4\sqrt{n}\ln n$.*

This will be an immediate consequence of the following.

**Theorem 6.6** (Main technical result)**.** *Let $\mathfrak{X}$ be a uniprimitive coherent configuration with $n$ vertices. Then every pair of distinct vertices has at least $\sqrt{n}/2$ distinguishers, i. e., for every $x \neq y$ we have $|D(x,y)| \geq \sqrt{n}/2$.*

## 7 A probabilistic argument

To derive Theorem 6.5 from our main technical result, Thm. 6.6, we use a standard probabilistic argument.

Let $\mathscr{H} = (\Omega, \mathscr{E})$ be a hypergraph with $m$ edges, i. e., $\mathscr{E} = \{E_1, \dots, E_m\}$. A *cover* of $\mathscr{H}$ is a set $C \subseteq \Omega$ that intersects each $E_i$. The *covering number* $\tau(\mathscr{H})$ is the minimum size of covers.

**Lemma 7.1** (folklore)**.** *If every edge of the hypergraph $\mathscr{H}$ has size $\geq k$ then*

$$\tau(\mathscr{H}) \leq \lceil (n/k) \ln m \rceil.$$

*Proof.* Pick $u_1, \dots, u_t \in \Omega$ independently at random. The probability that none of the $u_j$ hits the edge $E_i$ is $(1 - |E_i|/n)^t \leq (1 - k/n)^t < \exp(-kt/n)$. By the union bound, the probability that some edge is not hit is less than $m \cdot \exp(-kt/n)$. We conclude that if $m \cdot \exp(-kt/n) \leq 1$ then $\tau(\mathscr{H}) \leq t$. In other words, if $t \geq (n/k) \ln m$ then $\tau \leq t$. □

The following exercise connects this lemma with our subject.

**Exercise 7.2.** Let $\mathscr{H}(\mathfrak{X}) = (\Omega; D(x,y) \mid x \neq y)$ be the hypergraph of sets of pairwise distinguishers. Then the distinguishing number of $\mathfrak{X}$ is $\tau(\mathscr{H}(\mathfrak{X}))$.

Let now $\mathfrak{X}$ be a coherent configuration. The hypergaph $\mathscr{H}(\mathfrak{X})$ has $m = \binom{n}{2} < n^2/2$ edges, each of size $\geq D_{\min} = \min_{x \neq y} |D(x,y)|$.

**Corollary 7.3.** *Let $D^*_{\min} = \min\{D_{\min}\,, n \ln 2\}$. Then $\mathfrak{X}$ has a distinguishing set of size less than $2n \ln n / D^*_{\min}$.*

*Proof.* By Lemma 7.1 and Ex. 7.2, there is a distinguishing set of size less than
$(n/D_{\min})(2 \ln n - \ln 2) + 1 \leq 2n \ln n / D^*_{\min}$. □

Now by Theorem 6.6 we have $D_{\min} \geq \sqrt{n}/2$ and therefore $D^*_{\min} \geq \sqrt{n}/2$. Theorem 6.5 follows.

## 8 Minimum size of sets of pairwise distinguishers

This section contains the meat of the paper: the proof of our main technical result, Theorem 6.6. In this section, $\mathfrak{X}$ is a uniprimitive coherent configuration.

**Exercise 8.1.** $|D(x,y)|$ depends only on $c(x,y)$.

**Notation 8.2.** Let $D(i) := |D(x,y)|$, where $i = c(x,y)$.
Recall that $X_i = (\Omega; R_i)$ is the color-$i$ constituent. Let $X_i' = (\Omega; R_i \cup R_i^{-1})$ be the symmetrization of $X_i$, so $X_i'$ is an undircted graph.

**Notation 8.3.** For a graph $X$ and vertices $x, y$ we write $\text{dist}_X(x,y)$ to denote the *distance* of $x$ and $y$ in $X$ (length of shortest $x - \cdots - y$ paths). The *diameter* of $X$ is $\text{diam}(X) = \max_{x \neq y} \text{dist}(x,y)$.

**Exercise 8.4.** For all $i$, $\text{diam}(X_i') \leq r - 1$.

For a graph $X$, we denote the complement of $X$ by $\overline{X}$.

**Lemma 8.5.** *For $i \geq 1$, if $X_i'$ is not the complete graph, then* $\text{diam}(\overline{X_i'}) = 2$.

*Proof.* There exist $x, y$ at distance 2 in $\overline{X_i'}$, because there exist $x, z$ not adjacent in $\overline{X_i'}$, but $\overline{X_i'}$ is connected by primitivity, and so the third vertex of any minimal $x, z$-path is at distance 2 from $x$.

Now take any $u, v \in \Omega$, not adjacent in $\overline{X_i'}$. Need to show: $\text{dist}_{\overline{X_i'}}(u,v) \geq 2$. Need to show: $u, v$ have a common neighbor in $\overline{X_i'}$. $c(u,v) \in \{i, i^{-1}\}$. Implies # common neighbors of $u, v$ in $\overline{X_i'}$ is the same as for $x, y$. □

**Exercise 8.6.** If $X$ is a regular graph of degree $\rho$ and diameter 2, then $\rho \geq \sqrt{n-1}$.

**Lemma 8.7.** *Assume $n \geq 5$. Then $(\forall i \geq 1)(\rho_i \leq n - 1 - \sqrt{n-1})$.*

*Proof.* If $X'_i$ is the complete graph, then $\rho_i = (n-1)/2$ and we are done. Otherwise, use Lemma 8.5 and Exercise 8.6. □

**Notation 8.8.** We shall consider the *average* distinguishing number

$$\overline{D} = \frac{\sum_{x \neq y} |D(x,y)|}{n(n-1)}.$$

Also, let $\rho_{\max} := \max_i \rho_i$.

**Lemma 8.9.** $\overline{D} \geq n - \rho_{\max} \geq \sqrt{n-1} + 1 > \sqrt{n}$.

*Proof.* Count the triples $(x,y,z)$ such that $z \notin D(x,y)$. This means $c(x,z) = c(y,z) = \rho_i$ for some $i$. This is

$$n - \overline{D} = \frac{\sum_{i=1}^{r-1} \rho_i(\rho_i - 1)}{n-1} \leq \rho_{\max} \frac{\sum_{i=1}^{r-1} (\rho_i - 1)}{n-1} < \rho_{\max}.$$

□

**Lemma 8.10.** $D(i) \leq \operatorname{dist}_{X'_j}(i) \cdot D(j)$.

*Proof.* Let $x_0, x_1, \ldots, x_d$ be a in $X'_j$ path where $c(x_0, x_d) = i$. $D(x_0, x_d) \subseteq \bigcup_{i=1}^{d} D(x_{i-1}, x_i)$. The size on the left side is $D(i)$; all stes on the right side have size $D(j)$. □

**Notation 8.11.** $\operatorname{diam}(i) := \operatorname{diam}(X'_i)$.

**Corollary 8.12.** $D(j) \geq \overline{D}/\operatorname{diam}(j)$.

*Proof.* Need: $\overline{D} \leq \operatorname{diam}(j) D(j)$. Pick $i$ such that $D(i) \geq \overline{D}$. Then $\operatorname{dist}_{X'_j}(i) \leq \operatorname{diam}(X'_j) = \operatorname{diam}(j)$. □

**Corollary 8.13.** *If* $\operatorname{diam}(i) = 2$ *then* $D(i) > \sqrt{n}/2$.

*Proof.* Combine Lemma 8.9 and Cor. 8.12. □

**Lemma 8.14** (Zemlyachenko)**.** *If* $\operatorname{diam}(i) \geq 3$ *then* $D(i) \geq 2\rho_i/3$.

*Proof.* Let $\operatorname{dist}_i(x,w) = 3$ and let $x, y, z, w$ be a shortest path from $x$ to $w$ in $X'_i$. Let $X'_i(x) = \{$ neighbors of $x$ in color $i$ $\}$. The Lemma is immediate from the following claim.

**Claim 8.15.** $X'_i(x) \cup X'_i(w) \subseteq D(x,w)$ *;*
*the sets* $X'_i(x)$ *and* $X'_i(w)$ *are disjoint;*
*and* $D(i) \geq |D(x,w)|/3$.

The claim is easy: if some $X'_i$-neighbor $u$ of $x$ did not distinguish $x$ from $w$ then $c(u,w) = c(u,x) = i^{\pm}$, so $x - u - w$ would be an $X'_i$-path of length 2, contradicting the assumption that $\mathrm{dist}_i(x,w) = 3$. Same for $X'_i(w)$. Now if $u \in X'_i(x) \cap X'_i(w)$ then $x - u - w$ would again be a path of length 2 in $X'_i$ between $x$ and $w$. Finally, $|D(x,w)| \leq 3D(i)$ by Lemma 8.10. □

**Exercise 8.16.** Suppose there exists an edge of color $h$ between $X_i(x)$ and $X_j(x)$. Then there exist at least $\max(\rho_i, \rho_j)$ such edges.

**Lemma 8.17.** $(\forall h \neq 0)(\forall x)$(*$x$ distinguishes at least $n-1$ pairs of color $h$*).

*Proof.* Let us construct a graph $H$ using the set $V = \{0, 1, \ldots, r-1\}$ of colors as vertex set. Let $w(i,j)$ be the number of edges of color $h$ or $h^{-1}$ from $X_i(x)$ to $X_j(x)$. Put an edge between $i$ and $j$ if $w(i,j) \neq 0$; assign weight $w(i,j)$ to this edge. It follows from Exerciseconn-ex that if there is an $\{i,j\}$ edge then $w(i,j) \geq \max(\rho_i, \rho_j)$.

$H$ is a connected graph. This follows from the primitivity of $\mathfrak{X}$ (why?). Let $T$ be a spanning tree of $H$. Let us orient $T$ away from vertex (color) 0. $x$ distinguishes $\geq \tau$ edges of color $h$, where $\tau :=$ total weight of edges of $T$.

$$\tau = \sum_{i \to j} w(i,j) \geq \sum_{i \to j} \rho_j = \sum_{i=1}^{r-1} \rho_j = n - 1.$$

□

**Corollary 8.18.** *$D(i) \geq (n-1)/\rho_i$.*

*Proof.* Count the triples $N = |\{(x,y,z) \mid c(x,y) = i, z \in D(x,y)\}|$ in two different ways.

Count by $(x,y)$. The number of pairs $(x,y)$ such that $c(x,y) = i$ is $n\rho_i$. For each such pair, there are $D(i)$ choices for $z$. Thus,

$$N = n\rho_i D(i).$$

Now count by $z$. There are $n$ choices for $z$. Given $z$, there are at least $n-1$ pairs $(x,y)$ distinguished by $z$. Thus

$$N = n\rho_i D(i) \geq n(n-1),$$

and so

$$\rho_i D(i) \geq n - 1.$$

□

**Corollary 8.19.** *If* $\mathrm{diam}(i) \geq 3$ *then* $D(i) \geq \sqrt{2(n-1)/3}$.

*Proof.* Multiplying the expressions for $D(i)$ from Lemma 8.14 and Corollary 8.18, we get

$$D(i)^2 \geq \frac{2\rho_i}{3} \cdot \frac{n-1}{\rho_i} = \frac{2(n-1)}{3}.$$

□

Observing that $\sqrt{2(n-1)/3} > \sqrt{n}/2$ (for $n \geq 2$), Cor. 8.19, combined with Corollary 8.13, completes the proof of Theorem 6.6.

## 9 Concluding remarks

The *degree* of a permutation $\sigma$ is the size of its support, i. e., the number of elements not fixed by $\sigma$. The *minimal degree* of a permutation group $G \leq \mathrm{Sym}(\Omega)$ the minimum of the degrees of the non-identity elements of $G$. Let us denote this quantity by $m(G)$.

For instance, $m(S_n) = 2$ and $m(A_n) = 3$.

**Exercise 9.1.** Prove: for all groups $G$ other than $S_n$ and $A_n$ in the bullet point list in the Introduction, $m(G) = \Theta(\sqrt{n})$, i. e., there exist constants $c_1 > c_2 > 0$ such that

$$c_2\sqrt{n} \leq m(G) \leq c_1\sqrt{n}.$$

The minimal degree of permutation groups has been studied since the 19th century. The objective is to prove general lower bounds. Two early highlights are a result by Jordan [Jo1871] (as simplified by de Séguièr [dS12, p. 58]) and one by Bochert [Bo1892].

**Theorem 9.2** (Jordan). *If $G$ is a uniprimitive permutation group of degree $n$ then $m(G) \geq (1 - o(1))\sqrt{8n/\ln n}$.*

**Theorem 9.3** (Bochert). *If $G$ is a doubly permutation group of degree $n$, other than $S_n$ or $A_n$, then $m(G) > n/4 - 1$.*

We obtain a slight strengthening of Jordan's result and extend it to uniprimitive coherent configurations.

**Exercise 9.4.** If $G \geq H$ then $m(G) \leq m(H)$. In particular, $m(G) \geq m(\mathrm{Aut}(\mathfrak{X}(G))$.

**Exercise 9.5.** Let $\mathfrak{X}$ be a coherent configuration. Then $m(\mathrm{Aut}(\mathfrak{X})) \geq D_{\min}$.

A combination of these two observations yields the following corollary to Theorem 6.6.

**Corollary 9.6.** *If $\mathfrak{X}$ is a uniprimitive coherent configuration then $m(\mathrm{Aut}(\mathfrak{X})) \geq \sqrt{n}/2$. In particular, the minimal degree of a uniprimitive permutation group is at least $\sqrt{n}/2$.*

We conclude this note with three conjectures. The first of these is stated in [Ba81]. In each conjecture, $\mathfrak{X}$ is a primitive coherent configuration of rank $r$ with $n$ vertices. $\rho_{\max} = \max_i \rho_i$ is the maximum outdegree among the constituents.

**Exercise 9.7.** $D_{\min} \geq (n - \rho_{\max})/(r-1)$ .

(Hint: Lemma 8.9, Cor. 8.12, and Ex. 8.4.)
It follows by Cor. 7.3 that $\mathfrak{X}$ has a distinguishing set of size $\le 2(r-1)(n \ln n)/(n - \rho_{\max}))$.

We believe the dependence on $r$ is not necessary; the situation can only get better with growing rank.

**Conjecture 9.8** ([Ba81]). *$\mathfrak{X}$ has a distinguishing set of size $O(n \ln n/(n - \rho_{\max}))$.*

Note that by the above, this is true for bounded $r$.

In proposing Conj. 9.8, the following stronger problem was on my mind.

**Conjecture 9.9.** *For uniprimitive coherent configurations, $D_{\min} = \Omega(n - \rho_{\max})$.*

By Cor. 7.3, this conjecture implies Conj. 9.8.

Conj. 9.9 is true for bounded rank by Ex. 9.7.

Compare Conj. 9.9 with Lemma 8.9. The Lemma asserts that the *average* size of pairwise distinguishers is $\overline{D} \ge n - \rho_{\max}$.

**Conjecture 9.10.** *For primitive coherent configurations of rank $r \ge 3$, $D_{\min} = \Omega(n^{1-1/(r-1)}))$. Or at least $D_{\min} = \Omega(n^{1-f(r)})$, where $f(r) \to 0$.*

The first statement holds for $r = 3$ by our main technical result, Theorem 6.6.

## References

[Ba81] László Babai: On the order of uniprimitive permutation groups. *Annals of Math.* **113** (1981), 553–568.

[Ba82] László Babai: On the order of doubly transitive permutation groups. *Inventiones Math.* **65** (1982), 473–484.

[Bo1889] Alfred Bochert: Ueber die Zahl der verschiedenen Werthe, die eine Function gegebener Buchstaben durch Vertauschung derselben erlangen kann. *Mathematische Annalen* **33** (1889), 584–590.

[Bo1892] Alfred Bochert: Über die Classe der transitiven Substitutionengruppen. *Math. Ann.* **40** (1892), 192–199.

[Ca81] Peter J. Cameron: Finite permutation groups and finite simple groups. *Bull. London Math. Soc.* **13** (1981), 1–22.

[Jo1871] Camille Jordan: Theéorèmes sur les groupes primitifs. *J. Math. Pures. Appl.* **16** (1871) 383–408.

[Ma02] Attila Maróti: On the orders of primitive groups. *J. Algebra* **258(2)** (2002), 631–640.

[PrS80] Cheryl E. Praeger and Jan Saxl: On the orders of primitive permutation groups. *Bull. London Math. Soc.* **12** (1980) 303–307.

[Py93] László Pyber: On the orders of doubly transitive permutation groups: elementary estimates. *J. Combinat. Theory. Ser. A* **62(2)** (1993), 361–366.

[dS12] J.-A. de Seguier: *Groupes de Substitutions.* Gauthier–Villars, 1912.

[SW15] Xiaorui Sun and John Wilmes: Faster canonical forms for primitive coherent configurations. *In: Proc. 47th ACM Symp. on Theory of Computing (STOC'15)*, 2015, pp. 693–702.

[Wi34] Helmut Wielandt: Abschätzungen für den Grad einer Permutationsgruppe von vorgeschriebenem Transitivitätsgrad. Dissertation, Berlin 1934. *Schriften des Math. Seminars und des Instituts für angewandte Mathematik der Universität Berlin* **2** (1934), 151–174.