Primitive coherent configurations: On the order of uniprimitive permutation groups

László Babai*

May 1, 2011

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

For large n, the largest four primitive permutation groups are S_n and A_n, of order about $n!$, and $S_k^{(2)}$ (for $n = \binom{k}{2}$) and $S_k \wr S_2$ (for $n = k^2$), of order about $\exp(c\sqrt{n}\ln n)$. The classification of finite simple groups allows one to show that these are the largest and even to list the largest down to size about $\exp(\ln^2 n)$ (Cameron [4], cf. Maróti [5]). We can do reasonably well with elementary means.

Theorem 1.1. *Assume $G \le S_n$, $A_n \not\le G$, and G is primitive.*

1. *(Bochert, 1889 [3])* $|G| \le \frac{n!}{(n+1)/2)!} \approx e^{\frac{n}{2}\log n}$.
2. *(Wielandt, 1934 [8], Praeger-Saxl, 1980 [7])* $|G| < 4^n$ *(using nontrivial elementary group theory)*
3. *(Babai, 1981 [1]) If G is not doubly transitive then* $|G| < \exp(4\sqrt{n}\log^2 n)$ *(using graph theory and a simple probabilistic argument).*

*Based on a 2003 REU lecture; scribe: Tom Hayes. Revised: LB, May 2011.

4. *(Babai, 1982 [2] If G is doubly transitive then $|G| < \exp\exp c\sqrt{\log n}$ (using elementary group theory and a simple probabilistic argument)*

5. *(Pyber, 1993 [6])If G is doubly transitive then $|G| < \exp c\log^3 n$ (using elementary group theory and the probabilistic argument of [2]) and $|G| < \exp c\log^2 n$ (using additionally an elementary group theoretic result of Wielandt [8])*

Exercise 1.2. Doubly transitive implies primitive.

The following theorem is proved using the classification of finite simple groups; one can get close by elementary means.

Theorem 1.3. *If $G \le S_n$, $G \not\geq A_n$ is doubly transitive then $|G| < n^{1+\log_2 n}$.*

Exercise 1.4. Verify that this bound is essentially tight for $\mathrm{PSL}(d,q)$ and $\mathrm{AGL}(d,q)$, acting on the corresponding projective and affine spaces, resp., where q is fixed and $d \to \infty$.

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 (primitive but not doubly transitive) permutation groups.

Picture of D_6. $R_0 = \Delta = \{(x,x) \mid x \in \Omega\}$, diagonal. $\Omega \times \Omega = R_0 \cup R_1 \cup \cdots \cup R_{r-1}$. $r = \#$ colors $= \#$ orbits of G on $\Omega \times \Omega$. D_6 has rank 4, $r = 4$. In this case, all orbitals are self-paired.

Definition 1.5. An *orbital* Γ of a permutation group $G \le \mathrm{Sym}(\Omega)$ is an orbit of G on the set of ordered pairs ($\Gamma \subset \Omega \times \Omega$). Γ 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 1.6. If G is doubly transitive, then $\mathrm{rk}(G) = 2$. What do the two classes correspond to?

Definition 1.7. COHERENT CONFIGURATION of rank r:
$\mathfrak{X} = (\Omega; R_0, \ldots, R_{r-1})$, $R_i \subseteq \Omega \times \Omega$.
$\Omega \times \Omega = R_0 \dot\cup \ldots \dot\cup R_{r-1}$.
$X_i = (\Omega, R_i)$, i'th color digraph, called a *constituent digraph.* The color of a pair x, y is defined as $c(x,y) = i$ if $(x,y) \in R_i$.
To be coherent, the following 3 axioms must be satisfied:

A1: The diagonal is $\Delta = R_0 \dot\cup \ldots \dot\cup R_{i_0 - 1}$. Equivalently, $c(x,x) = c(y,z) \Rightarrow y = z$.

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

Definition 1.8. For $G \leq \mathrm{Sym}(\Omega)$, $\mathfrak{X}(G) := (\Omega; \text{orbitals})$. We refer to these as "the group case."

Exercise 1.9. $\mathfrak{X}(G)$ is a coherent configuration.

Exercise 1.10. $G \leq \mathrm{Aut}(\mathfrak{X}(G))$, the group of color-preserving permutations. $\pi \in \mathrm{Aut}(\mathfrak{X})$ if $(\forall x, y)(c(x,y) = c(x^\pi, y^\pi))$

Remark 1.11. There exist coherent configurations without a group. In fact, there are exponentially many rank-3 coherent configurations with no automorphisms.

Well, we always lose in translation. The question is how much.

Exercise 1.12. The number of $x \to \cdots \to y$ walks of a given color-composition only depends on $c(x,y)$. E. g., how many walks from x to y of length 4 are colored red, blue, purple, blue (in order)?

Definition 1.13. $\mathfrak{X}$ is *homogeneous* if $R_0 = \Delta$ (i. e., $(\forall x, y)(c(x,x) = c(y,y))$).

Exercise 1.14. $\mathfrak{X}(G)$ is homogeneous $\iff$ G is transitive.

Exercise 1.15. If $\mathfrak{X}$ is homogeneous, then every weak component of each X_i is strongly connected.

Exercise 1.16. If $\mathfrak{X}$ is homogeneous, then $(\forall x)(\forall i)(\text{in-degree}_i(x) = \text{out-degree}_i(x) = \rho_i$ (ρ_i does not depend on x). So X_i is Eulerian, and indeed is regular.

By the way, $\sum_{i=0}^{r-1} \rho_i = n$, since every vertex is connected to every other (including itself) in the graph $\cup X_i$, whose edge set contains all n^2 ordered pairs.

Definition 1.17. $\mathfrak{X}$ is a *primitive* coherent configuration if $\mathfrak{X}$ is homogeneous and ALL constituent digraphs X_i, $i \geq 1$ are connected.

Exercise 1.18. $\mathfrak{X}(G)$ is primitive $\iff$ G is primitive. (DO!!!)

Definition 1.19. $\mathfrak{X}$ is uniprimitive coherent configuration if $\mathfrak{X}$ is primitive and rank ≥ 3.

Exercise 1.20. $\mathfrak{X}$ is uniprimitive $\iff$ G is uniprimitive (primitive but not doubly transitive).

$G \leq \mathrm{Sym}(\Omega)$, $\Psi \subseteq \Omega$. Look at the pointwise stabilizer, $G_\Psi, = \bigcap_{x \in \Psi} G_x$. If $G_\Psi = \{1\}$, then $|G| \leq n^{|\Psi|}$, in fact $|G| \leq n(n-1)\dots(n - |\Psi| + 1)$. Call such a Ψ a "base" of G.

We shall prove, using only elementary graph theoretic arguments, that

Theorem 1.21. *If G is uniprimitive, then* $|G| < \exp(4\sqrt{n}(\ln n)^2)$.

Lemma 1.22. *If G is uniprimitive, then* $(\exists \Psi \subseteq \Omega)(|\Psi| \leq 4\sqrt{n} \ln n$ *and* $G_\Psi = \{1\})$.

Examples: How large is the smallest base for various classes of permutation groups?

Definition 1.23. z *distinguishes* x and y if $c(x, z) \neq c(y, z)$. $D(x, y) = \{z \mid c(x, z) \neq c(y, z)\}$ is the *distinguishing set* for x, y.

Exercise 1.24. 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 1.25. 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, Ψ contains an element which distinguishes them.

Exercise 1.26. For $\mathfrak{X} = \mathfrak{X}(G)$, if Ψ is a distinguishing set, then Ψ is a base for G.

Theorem 1.21 will follow from the following result.

Theorem 1.27. *If $\mathfrak{X}$ is a uniprimitive coherent configuration, then there exists a distinguishing set Ψ such that* $|\Psi| < 4\sqrt{n} \ln n$.

This will be an immediate consequence of the following. From now on, let us always assume $\mathfrak{X}$ is a uniprimitive coherent configuration.

Theorem 1.28 (Main technical theorem)**.** *For every x, y,* $|D(x, y)| \geq \sqrt{n}/2$.

Proof: [Main technical theorem $\Rightarrow$ Theorem 1.27]. Pick $u_1, \ldots, u_m$ at random, and hope that we picked enough to hit each $D(x, y)$.

$$\begin{aligned} \Pr(D(x,y) \text{ not hit}) &= \left(1 - \frac{|D(x,y)|}{n}\right)^m \\ &\leq \exp\left(-\frac{|D(x,y)|m}{n}\right). \end{aligned}$$

Hence, by the Union Bound,

$$\begin{aligned} \Pr((\exists x, y)(D(x,y) \text{ not hit})) &< \binom{n}{2} \exp\left(-\frac{D_{\min} m}{n}\right) \\ &< \exp\left(-\frac{D_{\min} m}{n} + 2 \ln n\right), \end{aligned}$$

where $D_{\min} = \min_{x \neq y} |D(x, y)|$.

For this, it is sufficient to show

$$\exp\left(\frac{D_{\min} m}{n} + 2 \ln n\right) \leq 1$$

or equivalently

$$\frac{D_{\min}m}{n} + 2\ln n \le 0$$

which follows from

$$m \ge \frac{2n\ln n}{D_{\min}} \le 4\sqrt{n}\ln(n) =: m.$$

The last inequality used the Main technical theorem, which gives a lower bound on $D_{\min}$.

2 Min size of distinguishing sets

We spend the rest of this class with proving the Main technical theorem above.

Exercise 2.1. $|D(x, y)|$ depends only on $c(x, y)$.

Notation 2.2. Let $D(i) := |D(x, y)|$, where $i = c(x, y)$. $X_i = (\Omega; R_i)$. Let $X_i' = (\Omega; R_i \cup R_i^{-1})$ be the corresponding undirected graph.

Lemma 2.3. *For $i \ge 1$, if X_i' is not the complete graph, then* $\operatorname{diam}(\overline{X_i'}) = 2$.

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: $\operatorname{dist}_{\overline{X_i'}}(u, v) \ge 2$. 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 2.4. If X is a regular graph of degree ρ and diameter $= 2$, then $\rho \ge \sqrt{n-1}$.

Exercise$^+$ 2.5. $\rho = \sqrt{n-1}$ under the above conditions implies $\rho \in \{2, 3, 7, 57\}$. *Hint.* Figure out a connection to girth. This exercise is only for students who took the first half of this course.

Lemma 2.6. $(\forall i \ge 1)(\rho_i \le n - 1 - \sqrt{n-1})$.

Proof: If X_i' is the complete graph, then $\rho_i = (n-1)/2$ and we are done. Otherwise, use Lemma 2.3 and Exercise 2.4.

Notation 2.7. We shal consider the *average* distinguishing number

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

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

Lemma 2.8. $\overline{D} \geq n - \rho_{\max} \geq \sqrt{n-1} + 1 \sim \sqrt{n}$.

Proof: Count the number of 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 2.9. $D(i) \leq \operatorname{dist}_{X'_j}(i) D(j)$.

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

Notation 2.10. $\operatorname{diam}(i) := \operatorname{diam}(X'_i)$.

Corollary 2.11. $D(j) \geq \overline{D}/\operatorname{diam}(j)$.

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 2.12. *If* $\operatorname{diam}(i) = 2$ *then* $D(i) \gtrsim \sqrt{n}/2$.

Lemma 2.13 (Zemlyachenko)**.** *If* $\operatorname{diam}(i) \geq 3$ *then* $D(i) \geq \rho_i/3$.

Proof: Let x, y, z, w be a shortest path from z to w in X'_i. Let $X'_i(x) = \{$ neighbors of x in color i $\}$.

Claim 2.14. $X'_i(x) \subseteq D(x, w)$ *and* $D(i) \geq |D(x, w)|/3$. *The Lemma is immediate from the following claim:*

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 $\operatorname{dist}_i(x, w) = 3$. Now $|D(x, w)| \leq 3D(i)$ by Lemma 2.9.

Exercise 2.15. 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 2.16. $(\forall h \neq 0)(\forall x)$($x$ *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 2.17. $D(i) \geq (n-1)/\rho_i$.

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 2.18. *If* $\operatorname{diam}(i) \geq 3$ *then* $D(i) \gtrsim \sqrt{n/3}$.

Proof: Multiplying the expressions for $D(i)$ from Lemma 2.13 and Corollary 2.17, we get

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

Thus

$$D(i) \geq \sqrt{\frac{n-1}{3}} \sim \frac{\sqrt{n}}{\sqrt{3}}.$$

This result, combined with Corollary 2.12, completes the proof of the Main Theorem.

This proof is based on L. Babai: "On the order of uniprimitive permutation groups," Annals of Math. 113 (1981), 553–568, as simplified by N. Zemlyachenko a year later.

Conjecture 2.19. *For uniprimitive coherent configurations,* $D_{\min} = \Omega(n - \rho_{\max})$. *(Note that this is true for the average rather than the minimum size of distinguishing sets by Lemma 2.8.)*

Another open question:

Conjecture 2.20. *For primitive coherent configurations of rank* $r \geq 4$, $D_{\min} = \Omega(n^{1-1/(r-1)})$). *Or at least* $D_{\min} = \Omega(n^{1-f(r)})$, *where* $f(r) \to 0$.

Note that the first statement is true for $r = 2$.

References

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

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

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

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

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

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

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

[8] 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.