Discrete Math, 13th Problem Set (August 13)

REU 2003

Instructor: Laszlo Babai
Scribes: Tom Hayes and Ben Wieland

1 Decision tree complexity

Definition 1.1. A boolean function in n variables is a function $f : \{0,1\}^n \to \{0,1\}$. Boolean functions are also referred to as "properties."

Definition 1.2. A property (boolean function) of several boolean variables is *monotone increasing* if its truth on an input implies its truth on any input in which at least the same variables are true (but some of the falses may have become true), i. e., if $f(x_1, \dots, x_n) \geq f(y_1, \dots, y_n)$ whenever $(\forall i)(x_i \geq y_i)$. A property is *monotone* if either it or its negation is monotone increasing.

"Graph properties" are boolean functions of the $\binom{v}{2}$ boolean variables expressing adjacency (v is the number of vertices); such a function must take the same value on isomorphic graphs, so the function must be *invariant* under the group $S_v^{(2)}$, the induced action of S_v on the $\binom{n}{2}$ pairs. Connectedness is a monotone increasing property. Planarity is monotone decreasing.

Definition 1.3. A *decision tree* is an algorithm for computing a function of an unknown input. Each vertex of the tree is labeled by a variable and the branches from that node are labeled by the possible values of the variable. The leaves are labeled by the output of the function. The process starts at the root, knowing nothing, works down the tree, choosing to learn the values of some of the variables based on those already known and eventually reaches a decision. The *decision tree complexity* of a function is the minimum depth of a decision tree that computes that function. A property is *evasive* if its decision tree complexity is equal to the number of variables.

Exercise 1.4. The planarity of a graph is evasive.

Conjecture 1.5. *All nontrivial (i. e., nonconstant) monotone graph properties are evasive.*

Theorem 1.6 (Rivest-Vuillemin). *A nontrivial monotone graph property has decision tree complexity at least $v^2/16$ (a constant fraction of the maximum).*

Exercise 1.7. Find a nontrivial graph property with decision tree complexity $O(v)$. (Note that such a property cannot be monotone.)

Theorem 1.8 (Rivest-Vuillemin). *If q is a prime power, and $f\colon \{0,1\}^q \to \{0,1\}$ is a boolean function that is invariant under the action of a transitive permutation group acting on the q variables, and $f(\underline{0}) \neq f(\underline{1})$, then f is evasive. (No assumption of monotonicity is needed.)*

Conjecture 1.9. *A monotone function invariant under a transitive group acting on the variables is evasive.*

Conjecture 1.5 is a special case of this. The group in that case is primitive ($S_v^{(2)}$). The case of other primitive groups are also of interest.

Proof of the Rivest-Vuillemin Theorem was given in class for a prime number of variables.

Exercise 1.10. Extend the proof in class to the case of a prime power number of variables. *Hint.* Recall (and prove) the earlier exercise that if G is a transitive permutation group acting on a set of size p^k then its Sylow p-subgroup is also transitive.

2 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 $e^{c\sqrt{n}\log n}$. The classification of finite simple groups allows us to show that these are the largest and even to list the largest down to size about $e^{\log^2 n}$. We can do reasonably well with elementary means.

Theorem 2.1. *Assume $G < S_n$, $A_n \not< G$, and G is primitive.*

1. *(Bochert c.1890) $|G| \leq \frac{n!}{(n+1)/2)!} \approx e^{\frac{n}{2}\log n}$.*
2. *(Wielandt, Praeger-Saxl, 1980) $|G| < 4^n$.*
3. *(Babai, 1981) If G is not doubly transitive, $|G| < e^{4\sqrt{n}\log^2 n}$ (using almost only graph theory).*

Exercise 2.2. Doubly transitive implies primitive.

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

Theorem 2.3. *If $G \leq S_n$, $G \not\geq A_n$ is doubly transitive then $|G| < n^{1+\log_2 n}$.*

Exercise 2.4. Verify this bound for PSL and AGL, acting on projective and affine spaces, resp.

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 2.5. An *orbital* Γ of a permutation group $G \leq \mathrm{Sym}(\Omega)$ is an orbit of G on the set of ordered pairs ($\Gamma \subset \Omega \times \Omega$). 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 2.6. If G is doubly transitive, then $\mathrm{rk}(G) = 2$. What do the two classes correspond to?

Definition 2.7. 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 2.8. For $G \leq \mathrm{Sym}(\Omega)$, $\mathfrak{X}(G) := (\Omega; \text{orbitals})$. We refer to these as "the group case."

Exercise 2.9. $\mathfrak{X}(G)$ is a coherent configuration.

Exercise 2.10. $G \leq \mathrm{Aut}(\mathfrak{X}(G))$, 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 2.11. 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 2.12. 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 2.13. $\mathfrak{X}$ is *homogeneous* if $R_0 = \Delta$ (i. e., $(\forall x, y)(c(x, x) = c(y, y))$).

Exercise 2.14. $\mathfrak{X}(G)$ is homogeneous $\iff$ G is transitive.

Exercise 2.15. If $\mathfrak{X}$ is homogeneous, then every weak component of each X_i is strongly connected.

Exercise 2.16. 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 2.17. $\mathfrak{X}$ is a *primitive* coherent configuration if $\mathfrak{X}$ is homogeneous and ALL constituent digraphs X_i, $i \geq 1$ are connected.

Exercise 2.18. $\mathfrak{X}(G)$ is primitive $\iff$ G is primitive. (DO!!!)

Definition 2.19. $\mathfrak{X}$ is uniprimitive coherent configuration if $\mathfrak{X}$ is primitive and rank ≥ 3.

Exercise 2.20. $\mathfrak{X}$ 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_Ψ, $= \cap_{x \in \Psi} G_x$. 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 "fixing set."

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

Theorem 2.21. *If G is uniprimitive, then $|G| < e^{4\sqrt{n}(\ln n)^2}$.*

Lemma 2.22. *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 fixing set for various classes of permutation groups?

Definition 2.23. *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 2.24. 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 2.25. 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 2.26. For $\mathfrak{X} = \mathfrak{X}(G)$, if Ψ is a distinguishing set, then Ψ is a fixing set for G.

Theorem 2.21 will follow from the following result.

Theorem 2.27. *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 2.28 (Main technical theorem). *For every x, y, $|D(x,y)| \geq \sqrt{n}/2$.*

Proof: [Main technical theorem $\Rightarrow$ Theorem 2.27]. 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

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

which follows from

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

The last inequality used the Main technical theorem, which lower bounds $D_{\min}$. □

3 Min size of distinguishing sets

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

Exercise 3.1. $|D(x,y)|$ depends only on $c(x,y)$.

Notation 3.2. 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 3.3. *For $i \geq 1$, 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: $\operatorname{dist}_{\overline{X_i'}}(u,v) \geq 2$. 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 3.4. If X is a regular graph of degree ρ and diameter $= 2$, then $\rho \geq \sqrt{n-1}$.

Exercise$^+$ 3.5. $\rho = \sqrt{n-1}$ 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 3.6. $(\forall i \geq 1)(\rho_i \leq n - 1 - \sqrt{n-1})$.

Proof: If X_i' is the complete graph, then $\rho_i = (n-1)/2$ and we are done. Otherwise, use Lemma 3.3 and Exercise 3.4. □

Notation 3.7. We shal 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 3.8. $\overline{D} \geq n - \rho_{\max} \geq \sqrt{n-1} + 1 \sim \sqrt{n}$.

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 3.9. *$D(i) \leq \mathrm{dist}_{X'_j}(i) D(j)$.*

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 3.10. $\mathrm{diam}(i) := \mathrm{diam}(X'_i)$.

Corollary 3.11. *$D(j) \geq \overline{D} / \mathrm{diam}(j)$.*

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

Corollary 3.12. *If $\mathrm{diam}(i) = 2$ then $D(i) \gtrsim \sqrt{n}/2$.*

Lemma 3.13 (Zemlyachenko). *If $\mathrm{diam}(i) \geq 3$ 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 3.14. *$X'_i(x) \subseteq D(x, w)$ 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 $\mathrm{dist}_i(x, w) = 3$. Now $|D(x, w)| \leq 3D(i)$ by Lemma 3.9. □

Exercise 3.15. 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 3.16. *$(\forall h \neq 0)(\forall x)(x$ 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 3.17. *$D(i) \geq (n-1)/\rho_i$.*

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

Proof: Multiplying the expressions for $D(i)$ from Lemma 3.13 and Corollary 3.17, 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 3.12, 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 3.19. *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 3.8.)*

Another open question:

Conjecture 3.20. *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 $r = 2$.