Discrete Math, Second Series, 6th Problem Set (July 30)

REU 2003

Instructor: László Babai
Scribe: Ben Wieland

1 Revisit the first problem set

Definition 1.1. A **product-free set** in a group G is a subset $L \subset G$ such that the equation $xy = z$ has no solution in L.
For a **finite** group G, let $\alpha(G)$ be the proportion of G in the largest product free set; $\alpha(G) = |L|/|G|$, for $L \subset G$ the largest product-free set.

Exercise 1.2. If $G \to H$ is a surjective homomorphism, show that $\alpha(G) \geq \alpha(H)$.

Exercise 1.3. $\alpha(G) \leq \frac{1}{2}$.

Exercise 1.4. If G has a subgroup of index 2, then $\alpha(G) = \frac{1}{2}$. In particular, if $G = S_n$ $(n \geq 2)$ or G is an abelian groups of even order then $\alpha(G) = \frac{1}{2}$.

Exercise 1.5. If $G = K \times L$ then $\alpha(G) = \max\{\alpha(K), \alpha(L)\}$.

Definition 1.6. A group is *finitely generated* if it has a finite set of generators.

Exercise 1.7. Find an infinite group G such that G is not finitely generated but every proper subgroup of G is finite and cyclic of prime power order. *Hint.* Prove that such a group must be abelian. Look for such gtoups among the subgroups of the multiplicative group of complex numbers of unit absolute value.

Exercise 1.8. Let G be an infinite abelian group and let H be the subset consisting of the elements of finite order. Prove that H is a subgroup. (H is called the **torsion subgroup** of G.

Theorem 1.9 (Fundamental theorem of finitely generated abelian groups). *Every finitely generated abelian group is the direct product of a finite number of cyclic groups. The number of infinite cycic groups in this factorization is unique. The product of the finite abelian subgroups in this factorization is unique; it is the torsion subgroup of G.*

Exercise 1.10. Let G be a finitely generated abelian group. Then $G = L \times T$ where T is the torsion subgroup and L is a direct product of infinite cyclic groups in accordance with the Fundamental Theorem. Prove that the subgroup L is not unique, unless G is "torsion-free" ($T = \{1\}$

Exercise 1.11. Prove that $K \times L$ is, the direct product of two finite groups, is cyclic if and only if both K and L are cyclic and their orders are relatively prime. In particular, every finite cyclic group is the direct product of cyclic groups of prime power order.

Theorem 1.12 (Fundamental theorem of finite abelian groups). *Every finite abelian group is the direct product of cyclic groups of prime power order. The orders in this factorization are unique.*

Exercise 1.13. Show that the subgroups in this factorization need not be unique.

Thus to compute $\alpha(G)$ for finite abelian groups, it suffices to know $\alpha(\mathbb{Z}_{p^k})$.

Corollary 1.14 (Fundamental theorem of finite abelian groups, Smith normal form). *Every finite abelian group is the direct product of cyclic groups $\mathbb{Z}_{n_1} \times \ldots \mathbb{Z}_{n_k}$ where $2 \leq n_1$ and $n_{i-1} \mid n_i$ for all i. The values $n_1, \ldots, n_k$ are unique.*

Exercise 1.15. $\alpha(\mathbb{Z}_7) = 2/7$, contrary to the lower bound $\frac{1}{3}$ claimed in the first problem set.

Exercise$^+$ 1.16. (Cauchy-Davenport) For a prime p, if $A, B \subset \mathbb{Z}_p$ let $A + B = \{a + b \,|\, a \in A, b \in B\}$. Then $|A + B| = \max\{p, |A| + |B| - 1\}$.

Exercise 1.17. $\alpha(\mathbb{Z}_p) = \lfloor \frac{p+1}{3} \rfloor / p$
Hint. The lower bound is easy: take the middle third of the group. Use the Cauchy-Davenport Theorem for the upper bound.

Exercise 1.18. If G is abelian then $\frac{2}{7} \leq \alpha(G) \leq \frac{1}{2}$.

Exercise 1.19. What is the exact value of $\alpha(\mathbb{Z}/p^k)$? It's probably known, but the instructor did not check the literature. Search under the title "sum-free sets" (abelian groups are comonly written additively).

But the real question is for nonabelian groups. The most interesting cases would be classes of simple groups, starting with the alternating groups and the projective special linear groups.

Exercise 1.20. If $H \lneq G$ then $\alpha(G) \geq \frac{1}{[G:H]}$. *Hint.* take a coset.

Exercise 1.21. $\alpha(A_n) \geq \frac{1}{n}$.

Conjecture 1.22. $\alpha(A_n) = o(1)$ *(i. e.,* $\lim_{n\to\infty} \alpha(A_n) = 0$.*)*

Nothing better than the inequalities $1/n \leq \alpha(A_n) \leq 1/2$ appears to be known for $n \geq 5$. Perhaps $\alpha(A_n) = 1/n$ but the instructor would not bet on this one.

More generally, the $o(1)$ is likely to hold for all finite simple groups:

Conjecture 1.23. *Let G_n be an infinite sequence of finite simple groups ($|G_n| \to \infty$). Then $\alpha(G_n) = o(1)$.*

It would be of interest to prove this various inifinite classes of finite simple groups, such as the projective special linear groups.

2 Finite probability spaces.

Exercise 2.1. Let $G \leq S_n$ is a transitive permutation group and $A, B \subset \Omega = \{1, \ldots, n\}$. Pick $\sigma \in G$ at random (from the uniformly distribution, i. e., each $g \in G$ has the same probability $1/|G|$ to be selected as σ). Prove that the expected size of the intersection of A and B^σ is

$$E(|A \cap B^\sigma|) = \frac{|A||B|}{n}.$$

Hint. Use indicator random variables. (See the Finite Probability Spaces handout.)

Interpretation: we can consider A and B as events on the probability space Ω (randomly pick a point $x \in \Omega$; the events are whether $x \in A$ and whether $x \in B$). We call A and B "independent events" if $P(A \cap B) = P(A)P(B)$, i e., if $P(x \in A \cap B) = P(x \in A)P(x \in B)$, or yet in other words, if $|A \cap B|/n = (|A|/n)(|B|/n)$. The intuitive meaning of the formula stated in the exercise becomes more evident in this context if we divide each side by n:

$$E(\frac{|A \cap B^\sigma|}{n}) = \frac{|A|}{n} \cdot \frac{|B|}{n}.$$

This means A and B^σ behave like independent events in the expectation.

Enhanced hint. Show that if x is randomly chosen from Ω and σ is randomly chosen from a transitive group G then the events $x \in A$ and $x \in B^\sigma$ are independent. (This is immediate if $G = S_n$ (why?) but remains true for any transitive group G.) Then use indicator variables to show how this translates into the expected intersection size of A and B^σ.

3 Graphs

Definition 3.1. The **right regular representation** of a group G is the homomorphism $\rho\colon G \to \mathrm{Sym}(G)$ given by $g \mapsto \rho_g$, where ρ_g is the permutation that acts as $x^{\rho_g} = xg$. The image (which is isomorphic to G) is denoted $R(G)$.

Corollary 3.2 (Cayley). *Every group is isomorphic to a permutation group.*

Definition 3.3. If G is generated by a set S, then the **Cayley Color Diagram** $\Gamma_c(G, S)$ is the colored digraph on the vertex set G with edges pointing from g to sg labeled (colored) by s for all $g \in G$ and $s \in S$. Automorphisms of such a colored digraph preserve the colors by definition.

Exercise 3.4. $\mathrm{Aut}(\Gamma_c(G, S)) = R(G)$. It contains $R(G)$ because right multiplication commutes with left multiplication, which defines Γ_c.

Exercise 3.5. (Frucht's Theorem) For any group G there exists a graph X with $\mathrm{Aut}(X) \cong G$. (X is an undirected, uncolored graph.)

Exercise$^+$ 3.6. (Babai) X can be chosen with $\leq 2|G|$ vertices, unless G is the cyclic group of order 3, 4, or 5.

3.1 Automorphisms of finite projective planes

Please consult the handout about Finite Projective Planes.

Conjecture 3.7. *Not every finite group is isomorphic to the group of automorphisms (collineations) of a finite projective plane. In fact, not every finite group is isomorphic even to a subgroup of the automorphism group of a finite projective plane. A_6 appears to be a candidate; A_{100} looks like an easier one to rule out as a subgroup.*

Exercise 3.8. If P is a finite projective plane of order n and Q is a subplane, then the order of Q is at most $\sqrt{n}$.

Exercise 3.9. Let P be a finite projective plane of order n. Prove that $|\mathrm{Aut}(P)| \leq n^{5+\log\log n}$. (log to base 2.)
Hint. Use the above exercise: $\log n$ is the number of times you can iteratively divide n by 2; $\log\log n$ is the number of times you can iteratively take the square root of n.

Exercise 3.10. If P is a finite Galois plane of order q then $|\mathrm{Aut}(P)| = O(q^8 \log q)$.
Hint. If $P = PG(2, q)$ then $\mathrm{Aut}(P) = P\Gamma L(3, q)$ where $P\Gamma L$ is the same as PGL except we permit the field automorphisms to act on the matrix elements. If $q = p^r$ is the order of the field of definition of P then $|\mathrm{Aut}(\mathbb{F}_q)| = r \leq \log_2 q$.

Conjecture 3.11. *If P is a projective plane of order n, then $|\mathrm{Aut}(P)| \leq n^C$ for some constant C. Perhaps, $|\mathrm{Aut}(P)| \leq n^{8+o(1)}$.*

3.2 Symmetry and connectivity of graphs

Definition 3.12. An undirected graph $X = (V, E)$ is **connected** if every pair of vertices is connected by a path. It is **k-connected** if it remains connected after removing any $k - 1$ vertices (except the complete graph K_n which is $n-1$-connected by convention). Let $\kappa(X)$ be the maximum k such that X is k-connected. $\kappa(X)$ is called the *vertex-connectivity* of X.

Example 3.13. The cycle graph has $\kappa(C_n) = 2$ for all $n \geq 3$. One should think of this as a topological invariant and all cycles have the same shape. This requires the convention that $\kappa(C_3) = \kappa(K_3) = 2$.

Definition 3.14. If s, t are vertices in a graph X, then the **s-t-connectivity** $\kappa(X; s, t)$ is the minimum number of vertices to delete to prevent there from being a path from s to t. (If there's a direct edge from s to t, count deleting it as deleting a vertex.) Then $\kappa(X) = \min_{s,t}\{\kappa(X; s, t)\}$. There is a similar notion $\kappa^+(X; s, t)$ for directed graphs and directed paths from s to t. There is also the **edge s-t-connectivity** $\rho(X; s, t)$, the minimum number of edges to delete to prevent there from being a path from s to t. This has a global version $\rho(X) = \min_{s,t}\{\rho(X; s, t)\}$ and a directed version ρ^+.

Theorem 3.15 (Menger). *$\kappa(X; s, t)$ is also the number of vertex-disjoint paths from s to t. $\rho(X; s, t)$ is also the number of edge-disjoint paths from s to t. The analogous directed versions are also true.*

Exercise 3.16. Assume we know the directed-edge-version of Menger's Theorem. Deduce the other three versions.

Exercise 3.17. (Fundamentals of Combinatorial Duality Theory.) Deduce the directed-edge-version of Menger's Theorem from the Max-flow-min-cut Theorem in network flows. Deduce the Max-flow-min-cut Theorem from the Duality Theorem of Linear Programming. Ask about these theorems in tutorial.

Exercise 3.18. $\kappa \leq \rho \leq \min_{v \in V} \deg(v)$.

Definition 3.19. X is a **vertex-transitive** graph if its automorphism group acts transitively on its vertices. Similarly, it is **edge-transitive** if the automorphism group acts transitively on the edges. It is **vertex-** or **edge-primitive** if the automorphism group acts primitively on the set of vertices (edges, respectively).

Exercise 3.20. Every vertex transitive graph is regular (all vertices have the same degree).

Exercise 3.21. Construct a graph which is vertex-transitive but not edge-transitive.

Exercise 3.22. (easy) Construct a graph which is edge-transitive but not vertex-transitive.

Exercise$^+$ 3.23. Construct a graph which is edge-transitive, not vertex-transitive, but is **regular**.

Theorem 3.24 (Mader-Watkins). *If X is an undirected, connected, vertex-transitive graph, regular of degree d, then*

1. *$\kappa(X) \geq \lceil \frac{2d+1}{3} \rceil$;*
2. *$\rho(X) = d$;*
3. *if X is edge-transitive or vertex-primitive, then $\kappa(X) = d$.*

Exercise 3.25. Show that $\lceil \frac{2d+1}{3} \rceil$ is tight for infinitely many d. That is, construct graphs with exactly that value of κ.

Definition 3.26. A directed graph is **strongly connected** if for every pair of vertices s and t, there is a directed path from s to t. It is **weakly connected** if it is a connected as an undirected graph when we ignore the orientation of the edges.

Definition 3.27. A directed graph X satisfies the **Euler condition** if for each vertex the in-degree is equal to the out-degree.

Exercise 3.28. (a) Prove that every finite vertex-transitive digraph satisfies the Euler condition. (b) Prove that this statemnt is false for infinite vertex-transitive graphs.

Exercise 3.29. If a directed graph X satisfies the Euler condition then it is strongly connected if and only if it is weakly connected.

Theorem 3.30 (Hamidoune). *If X a finite, connected vertex-transitive digraph then*

1. $\kappa^+(X) \geq \lceil \frac{d+1}{2} \rceil$;
2. $\rho^+(X) = d$;
3. *if X is edge-transitive or vertex-primitive, then $\kappa^+(X) = d$.*

Exercise 3.31. Use Hamidoune's theorem to prove the Cauchy-Davenport Theorem.
Hint. Use the vertex-primitive version.

A typesetting command error (a signle omitted backslash) rendered a paragraph unintelligible in the previous handout. It was the paragraph connecting two theorems. Here we reproduce the two theorems with the corrected paragraph inbetween.

Theorem 3.32 (B–Seress). *Let S generate S_n.* $\operatorname{diam}(S_n, S) < m_n^{1+o(n)}$.

This result suffers from the "element-order bottleneck." The two tricks used are commutators and raising elements to powers. A recent result gives a polynomial upper bound under the condition that one of the generators fixes 70% of the permutation domain. So now all is left to prove is that we can reach such a permutation in a polynomially bounded number of steps. Somebody in this audience may be able to do this with a fresh idea.

Theorem 3.33 (B–Beals–Seress). *Let S generate S_n. If $\exists s \in S$ with the* $\deg s < 0.3n$ *then* $\operatorname{diam}(S_n, S) < n^C$ *($C = 12$?). (Recall that the* degree *of a permutation is size of its* support*, the set of elements that it actually moves.)*