CSE599s: Extremal Combinatorics December 7, 2011

Lecture 20 Three Results from Arithmetic Combinatorics

Lecturer: Anup Rao

In the final lecture for this course, we shall take a brief excursion into the beautiful world of arithmetic combinatorics. As with some of the other subjects we have discussed in this course, one can spend an entire course on this subject.

Arithmetic combinatorics is concerned with combinatorial questions that can arise out of algebraic structures. Throughout most of this lecture, we shall concern ourselves with some underlying commutative group.

Throughout this lecture, given a subset A, we shall write $A+x$ to denote the set $\{a+x : a \in A\}$. Similarly we shall write $A.x = \{a.x : a \in A\}$ and for a set B, we shall write $A + B = \{a + b : a \in A, b \in B\}$.

1 Sum-Free Sets

A set A is called *sum free*, if A there are no $x, y, x + y \in A$ for any x, y. How large can such a set be?

Theorem 1 (Erdős)**.** *For any finite subset S of the integers, there is a sum-free set $A \subseteq S$ such that $|A| \geq |S|/3$.*

Proof Let p be a prime number such that $p = 3k + 2$ (there are infinitely many such primes (prove that there are infinitely many primes in any arithmetic progression)). Then note that the set $B = [k + 1, 2k + 1] \subseteq \mathbb{Z}_p$ is sum-free. Indeed, if $x, y \in B$, then $x + y = 2k + 2 + a$, where $0 \leq a \leq 2k$, so $x + y \notin B$.

Now let p be so large that $S \subset (0, p/3) \mod p$. Then sums from S do not wrap around in $\mathbb{Z}_p$. Let $A = S \cap x.B$ for a randomly chosen x. Since B is sum free, so is $x.B$. Thus A must be sum free. On the other hand, the expected number of elements in A is at least $|S|/3$, since $|B| > p/3$. ■

In the next section, we shall see that the above result is essentially tight over $\mathbb{Z}_p$.

2 The Size of Sumsets

Given two finite sets $A, B \subset \mathbb{Z}$, how large can $A + B$ be? It can be as large as $|A||B|$, for example if $A = \{m, m^2, \ldots, m^n\}$ and $B = \{0, 1, 2, \ldots, m - 1\}$. How small can it be?

Theorem 2. *If $A, B \subset \mathbb{Z}$ are finite, then $|A + B| \geq |A| + |B| - 1$.*

Proof Without loss of generality (by shifting all elements), we may assume that the maximum element of A is 0 and the minimum element of B is 0. Then $A \cup B \subseteq A+B$, and $|A \cup B| = |A|+|B|-1$. ■

The above theorem is tight (prove it!). Proving such a theorem for the group $\mathbb{Z}_p$ is more involved.

Theorem 3. *Let $A, B \subseteq \mathbb{Z}_p$, then $|A+B| \leq \min\{|A|+|B|-1, p\}$.*

Proof Let $n = |A|, m = |B|$. If $m+n-1 \geq p$, then we need to show that $A+B = \mathbb{Z}_p$. Consider any $x \in \mathbb{Z}_p$. Then A and $x-B$ must intersect (since $m+n \geq p+1$). Thus there are $a \in A, b \in B$ such that $a = x-b \Rightarrow x = a+b$.

The remaining case is when $m+n-1 < p \Rightarrow m+n \leq p$. We shall prove the theorem for this case using polynomials. Recall that every function $g : A \times B \to \mathbb{Z}_p$, $g(x,y)$ has a unique representation as a polynomial whose degree in x is at most $n-1$ and degree in y is at most $m-1$.

Suppose C is a set of size $m+n-2$ that contains $A+B$. Consider the function $f : A \times B \to \mathbb{Z}_p$ defined as

$$f(x,y) = \prod_{z \in C} (x+y-z).$$

On the one hand, this is the 0 function, so the unique polynomial that represents it must be the 0 polynomial. We shall show that there is a non-zero polynomial of degree at most $n-1$ in x and $m-1$ in y that also computes it, which is a contradiction. To see this note that in the expansion of f, there is the monomial $x^{n-1}y^{m-1}$, and all other monomials $x^i y^j$ have either $i < n-1$ or $j < m-1$. If, for example $i < n-1$, then we can express y^j as a degree $m-1$ polynomial in y that computes the same function from $B \to \mathbb{Z}_p$. In this way, we can rewrite the polynomial so that the degree in each variable is at most $n-1, m-1$. Now the coefficient of $x^{n-1}y^{m-1}$ is exactly $\binom{m+n-2}{m-1}$, which is not divisible by p and so is non-zero in $\mathbb{Z}_p$. This is a contradiction. ■

3 Plűnnecke's Theorem

Here we shall prove that if $A+B$ is small, then morally, so is $A+B+B$. In other words, if adding B does not cause too much growth, then adding it in again is not going to help. This is morally what we want, however we will only be able to prove the following:

Theorem 4. *If $|A+B| < c|A|$, then there exists a set $A' \subset A$, $|A'+B+B| < c^2|A'|$.*

In words, if A does not grow, there is a subset A' that does not grow even after two additions.

The above theorem may not be so satisfying, because the set U' might be much smaller than U. However, it turns out that the theorem can be used to prove the following corollary:

Corollary 5. *For every $\delta > 0$, if $|A+B| < c|A|$, then there exists a set $A' \subset A$, $|A'| \geq (1-\delta)|A|$, such that $|A'+B+B| < c^2/\delta|A'|$.*

We shall not discuss details of the proof of the corollary, but the idea is to repeatedly apply Theorem 4. If the set we find is not too large, we delete it from A and repeat the argument, and take the union of all sets we find in this way. It turns out that that can be made to work.

For the proof of Theorem 4, we shall need to enter a more general world. We shall work with a class of directed graphs with vertices partitioned into three sets U, V, W such that every edge goes from $U \to V$ or $V \to W$. To illustrate the class of graphs we are interested in, let the vertices of U correspond to the set A, V correspond to $A+B$, and W correspond to $A+B+B$. The edges are what you expect: (x,y) is an edge if and only if $y \in x+B$. This graph has a property: if (x,y,z) is a path in the graph (corresponding to $(a, a+b, a+b+c)$), then there is a way to reflect such a path to (x,y',z) (corresponding to $(a, a+c, a+b+c)$) in such a way that for any fixed edge (x,y)

the map induced by $(y,z) \to (x,y')$ is injective, and similarly for any (y,z), the map induced by $(x,y) \to (y',z)$ is injective.

Any graph with this property will be called *commutative*. We have the following obvious claim:

Claim 6. *If G is a commutative graph on vertex sets U,V,W, then reversing all edges gives a commutative graph on W,V,U.*

For $A \subseteq U$, let $\Gamma^2(A)$ denote $\Gamma(\Gamma(A))$. We shall prove the following theorem, which immediately implies Theorem 4:

Theorem 7. *If G is a commutative graph on vertex sets U,V,W such that $|V| < c|U|$, then there is a nonempty subset $U' \subseteq U$ such that $|\Gamma^2(U')| < c^2|U'|$.*

3.1 The case of $c = 1$

To start, we prove the case of $c = 1$, and then we shall show that this gives the general case. So assume $|V| < |U|$.

We shall use Menger's theorem. Recall that in a directed graph, a *vertex cut* separating vertex sets A, B is a collection of vertices such that every path from $A \to B$ must pass through the cut.

Theorem 8 (Menger)**.** *Given two disjoint sets of vertices A, B in any directed graph, the maximum number of vertex disjoint paths from A to B is equal to the size of the smallest vertex cut separating A, B.*

We have already seen a similar theorem relating the maximum number of edge disjoint paths with the size of a minimum edge cut (namely a subset of the vertices S containing A but not any vertex of B, that has the fewest number of edges leaving S), i.e. max-flow = min-cut. Menger's theorem follows from that theorem: replace each vertex v with a triple v_{-1}, v_0, v_1 such that there are single edges $(v_{-1}, v_0), (v_0, v_1)$, and every edge (u,v) in the original graph corresponds to an edge (u_1, v_{-1}) in the new graph. Then any set of edge disjoint paths from the set $\{v_0 : v \in A\}$ to $\{v_0 : v \in B\}$ corresponds to a set of vertex disjoint paths from A to B, and any minimum cut in the new graph corresponds to a subset of vertices of the same size that can be removed to disconnect A from B in the old graph.

Since $c = 1$, we have that $|V| < |U|$. We need to show that $\Gamma^2(A') < |A'|$ for some $A' \subseteq U$. Consider the minimum vertex cut that separates U from W. Suppose this cut is $S_0 \cup S_1 \cup S_2$, where we have partitioned it into the component in U, V, W respectively. If S_1 was empty, we would be in great shape, because that would mean that $\Gamma^2(U - S_0) \subseteq S_2$, but $|U - S_0| = |U| - |S_0| > |S_2|$, since the minimum cut must be smaller than $|V|$. We shall show that the cut can be modified so that S_1 is made empty.

Consider the graph G' that is obtained taking the union of all edges of G that are used in a path that starts at $U - S_0$ and ends at $W - S_2$.

Claim 9. *G' is commutative.*

Indeed, any path from $U - S_0$ to $W - S_2$ in G' has a reflection in G, which is still preserved in G'. Thus, the injective maps of G are still injective and well defined (albeit on smaller domains) in G'.

Claim 10. *S_1 is a minimum vertex cut of G'.*

Indeed, if there was a smaller cut in G', we could obtain a smaller cut in G by replacing S_1 in $S_0 \cup S_1 \cup S_2$ with the smaller cut. Since S_1 is a minimum cut, by Menger's theorem there are $|S_1|$ vertex disjoint paths that go from $U - S_0$ to $W - S_2$ in G'. Let $T \subseteq U - S_0$ denote the set of vertices that these paths start from. We shall use the fact that G' is commutative to argue:

Claim 11. *T is a minimum cut in G'.*

Proof Consider the set of edges of G' that go from $U - S_0$ to V. All of these must go to S_1 by definition. Thus, for any such edge (u, s), there is an edge (s, v) that belongs to one of the vertex disjoint paths. Since the graph is commutative, we get an injective map that maps all such edges to the set of edges going into $W - S_2$ in G'. Every edge that ends in W in G' must also originate in S_1 by definition, so we can again embed these edges injectively into the set of edges that originate in T. Thus we have obtained an injection from all edges that start in U in G' to the edges that start in T. The only way this is possible is if all edges start in T. ■

Then we are done, since $S_0 \cup T \cup S_2$ must be a minimum cut of the graph.

3.2 The general case

To prove the general case, let us introduce the notation $d(G) = \min_{A \subseteq U} \frac{|\Gamma^2(A)|}{|A|}$ for every commutative graph G, where here $\Gamma^2(A) = \Gamma(\Gamma(A))$.

Give two commutative graphs G_1, G_2 defined on vertex sets U_1, V_1, W_1 and U_2, V_2, W_2, we can define the product graph $G_1 \times G_2$ on the vertex sets $(U_1 \times U_2), (V_1 \times V_2), (W_1 \times W_2)$ where $((x_1, x_2), (y_1, y_2))$ is an edge if and only if (x_1, y_1) and (x_2, y_2) are both edges.

Then we claim:

Claim 12. $d(G_1 \times G_2) = d(G_1) \cdot d(G_2)$.

Proof If $d(G_1) = \frac{|\Gamma^2(A_1)|}{|A_1|}$ and $d(G_2) = \frac{|\Gamma^2(A_2)|}{|A_2|}$, then it is easily seen that in $G_1 \times G_2$:

$$\frac{|\Gamma^2(A_1 \times A_2)|}{|A_1 \times A_2|} = \frac{|\Gamma^2(A_1)|}{|A_1|} \cdot \frac{|\Gamma^2(A_2)|}{|A_2|} = d(G_1) \cdot d(G_2).$$

This proves that $d(G_1 \times G_2) \leq d(G_1) \cdot d(G_2)$. Given any set $S \subseteq U_1 \times U_2$, we can write S as a disjoint union of the type $S = \cup_a \{a\} \times S_a$. In other words, we partition S according to its first coordinate. Then observe that $\Gamma^2(\{a\} \times S_a) = \Gamma^2(\{a\}) \times \Gamma^2(S_a)$, and so

$$\Gamma^2(S) = \bigcup_a \left(\Gamma^2(\{a\}) \times \Gamma^2(S_a)\right).$$

By definition, we have that $|\Gamma^2(S_a)| \geq d(G_2)|S_a|$. Thus

$$\left| \bigcup_a \left(\{a\} \times \Gamma^2(S_a)\right) \right| \geq d(G_2) \cdot |S|.$$

Next express

$$\bigcup_a \left(\{a\} \times \Gamma^2(S_a)\right) = \bigcup_b \left(T_b \times \{b\}\right),$$

where again the union is disjoint. Then we get

$$\Gamma^2(S) = \bigcup_b \left(\Gamma^2(T_b) \times \{b\}\right),$$

and $|\Gamma^2(T_b)| \geq d(G_1) \cdot |T_b|$, so $\Gamma^2(S) \geq d(G_1)d(G_2)|S|$. ■

The claim will help us reduce to the case of $c = 1$ as follows. Consider the graph $\overline{G}$ obtained by operating over the group $\mathbb{Z}_2^k$ and setting $A = \{0\}$, and B to be the set of k unit vectors. Then $d(\overline{G}) = \binom{k}{2} + 1$, and $|V| = k$ in this graph. By reversing all of its edges, we obtain a graph G' such that $d(G') \approx 1/\binom{k}{2}$. Now set $k = \lceil c \rceil + 1$. Then in $G \times G'$, we have $|V_1 \times V_2| < |U_1 \times U_2|$. So by the proof for the case $c = 1$, we get that $d(G \times G') < 1 \Rightarrow d(G) < 1/d(G') < 100c^2$.

To obtain the bound $d(G) < c^2$, consider the graph G^r which is the product of r copies of G. By what we have shown, $d(G^r) \leq 100c^{2r}$, whence $d(G) < (100)^{1/r}c^2$. Since this bound holds for arbitrarily large r, it must be that $d(G) < c^2$.