The Erdos-Heilbronn conjecture and Schnirelmann Density

Arithmetic Combinatorics (Fall 2016)
Rutgers University
Swastik Kopparty
Last modified: Thursday 22nd September, 2016

1 The Erdos-Heilbronn conjecture

Now we prove the Erdos-Heilbronn conjecture, via the proof of Alon-Nathanson-Ruzsa.
Recall that $A\hat{+}A = \{a + a' \mid a, a' \in A, a \neq a'\}$.

Theorem 1. *If p is prime, and $A \subseteq \mathbb{F}_p$, then*

$$|A\hat{+}A| \geq \min\{2|A| - 3, p\}.$$

Proof. As in the previous lecture, we will use polynomials and the combinatorial nullstellensatz.
Let $|A| = r$, $|A\hat{+}A| = t$. Suppose $t \leq p - 1$ and $t \leq 2|A| - 4$.
Let $Q(X, Y) = (X - Y) \cdot \prod_{c \in A\hat{+}A}(X + Y - c)$. The key observation is that Q vanishes on $A \times A$.
Now to apply the combinatorial nullstellensatz to this setting, we need our polynomial to have X degree and Y degree at most $r - 1$. As in the proof of the Cauchy-Davenport theorem, we get this by reducing $Q(X, Y)$ mod $P_A(X) = \prod_{a \in A}(X - a)$ and $P_A(Y)$.
Let $\hat{Q}(X, Y)$ be this reduction. Then we know that the X-degree and Y-degree of $\hat{Q}$ is at most $r - 1$. We also know that $\hat{Q}$ can be expressed as:

$$\hat{Q}(X, Y) = Q(X, Y) + u(X, Y)P_A(X) + v(X, Y)P_A(Y). \tag{1}$$

Since Q vanishes on $A \times A$ and P_A vanishes on A, we get that $\hat{Q}$ vanishes on $A \times A$. By the combinatorial nullstellensatz, we get that $\hat{Q}$ is the zero polynomial.
Now we get a contradiction by finding a monomial that appears in $\hat{Q}$ with a nonzero coefficient. For $i + j = t + 1$, let us compute the coefficient of $X^i Y^j$ in $Q(X, Y)$. It equals: $\binom{t}{i-1} - \binom{t}{i}$, which equals:

$$\binom{t}{i} \cdot (1 - \frac{t - i + 1}{i}) = \binom{t}{i} \cdot \frac{i - j}{i}.$$

This is nonzero mod p if $i \neq j \mod p$.
Now choose $i = r - 1$, and set $j = t + 1 - i = t - r + 2$. Since $t \leq 2r - 4$, we have $j \leq r - 2$. Thus $i \neq j$ and $i, j < p$. So the coefficient of $X^i Y^j$ in $Q(X, Y)$ is nonzero mod p.
Finally, by (1), we have that the ceofficient of $\hat{Q}(X, Y)$ is nonzero mod p. □

2 Schnirelmann Density

Convention: 0 is a natural number.
We now start investigating the behavior of sumsets of natural numbers. To measure the size of set of natural numbers, it is particularly convenient to use the (strange) notion of Schnirelmann density:

$$\delta(A) = \inf_{i \geq 1} \frac{|A \cap [i]|}{i}.$$

Note that this is inf and not lim inf. In particular, if $1 \notin A$, then $\delta(A) = 0$. *We will be applying this notion to sets $A \subseteq \mathbb{N}$ with $0 \in A$.* Note that whether or not $0 \in A$ does not affect the density of A.

The lim inf density is more natural, but the above notion has nicer properties from the point of view of sumsets and is still useful for some applications.
The first basic theorem about Schnirelmann density and sumsets is the following.

Theorem 2. *Let $A, B \subseteq \mathbb{N}$ with $0 \in A$, $0 \in B$. Then*

$$\delta(A+B) \geq \delta(A) + \delta(B) - \delta(A)\delta(B).$$

Proof sketch: $\delta(A)$ fraction of the natural numbers are already in A. $\delta(B)$-fraction of the gaps between the elements of A are further included in $A+B$. So the total density is $\delta(A) + (1-\delta(A)) \cdot \delta(B)$.
Another important theorem is:

Theorem 3. *Let $0 \in A$. If $\delta(A) > 1/2$, then $A + A = \mathbb{N}$.*

Proof sketch: for each $n \in \mathbb{N}$, by the pigeonhole principle, at least one k exists with $k, n-k$ both in A.
Using the previous two theorems, we get the following conclusion: If $0 \in A$ and $\delta(A) > 0$, then there exists an integer ℓ such that $A + A + \ldots + A$ (ℓ times) equals $\mathbb{N}$. Taking the sumset ℓ times amplifies the density to $1 - (1-\delta(A))^\ell$ by the first theorem. This can make the density approach 1. Then applying the second theorem, we get the conclusion.
Schnirelmann used his theorem to prove that there is an integer ℓ such that every sufficiently large integer can be written as a sum of ℓ primes. Of course, the primes do not have positive density, but it turns out that a positive density of integers can be written as a sum of two primes.
Later in the course we will use Schnirelmann density to give an answer to Waring's problem: we will show that for all integers $k > 0$, there is an ℓ such that every positive integer can be written as a sum of at most ℓ k^{th} powers.
Next class we will see Mann's theorem, which gives an improved estimate on the density of a sumset:

$$\delta(A+B) = \delta(A) + \delta(B).$$

The proof turns out to be surprisingly tricky.