The Cauchy Davenport Theorem

Arithmetic Combinatorics (Fall 2016)
Rutgers University
Swastik Kopparty
Last modified: Thursday 22$^{\text{nd}}$ September, 2016

1 Introduction and class logistics

- See

  `http://www.math.rutgers.edu/~sk1233/courses/additive-F16/`

  for the course website (including syllabus).
- Class this Thursday is cancelled. We will schedule a makeup class sometime.
- Office hours: Thursdays at 11am.
- References: Tao and Vu, Additive combinatorics, and other online references (including class notes).
- Grading: there will be 2 or 3 problem sets.

2 How small can a sumset be?

Let A, B be subsets of an abelian group $(G, +)$. The sumset of A and B, denoted $A + B$ is given by:

$$A + B = \{a + b \mid a \in A, b \in B\}.$$

We will be very interested in how the size of $A + B$ relates to the sizes of A and B (for A,B finite).
Some general comments. If A and B are generic, then we expect $|A + B|$ to be big. Only when A and B are very additively structured, and furthermore if their structure is highly compatible, does $|A + B|$ end up small.
If G is the group of real numbers under addition, then the following simple inequality holds:

$$|A + B| \geq |A| + |B| - 1.$$

Proof: Let $A = \{a_1, \ldots, a_k\}$ where $a_1 < a_2 < \ldots < a_k$. Let $B = \{b_1, \ldots, b_\ell\}$, where $b_1 < \ldots < b_\ell$. Then $a_1 + b_1 < a_1 + b_2 < \ldots < a_1 + b_\ell < a_2 + b_\ell < a_3 + b_\ell < \ldots < a_k + b_\ell$, and thus all these elements of $A + B$ are distinct. Thus we found $|A| + |B| - 1$ distinct elements in $A + B$. Equality is attained if and only if A and B are arithmetic progressions with the same common difference (In case of equality we need to have either $a_i + b_j = a_1 + b_{j+i-1}$ or $a_i + b_j = a_{i+j-\ell} + b_\ell$).
Now let us move to a general group. Then at the very least we have $|A + B| \geq \max\{|A|, |B|\}$.
Equality can hold, for example if $A = B$ is a subgroup of G. In fact, every equality case is closely related to this.
Suppose $|A| \leq |B|$. Then $|A + B| = |B|$ if and only if there is a subgroup H of G, such that A is contained in a coset of H, and B is a union of cosets of H.
Proof: Suppose $|A + B| = |B|$. We may assume $0 \in A$ (by subtracting some fixed element $a_0 \in A$ from all elements of A). Then $B \subseteq A + B$, and so $B = A + B$. Thus $a + B = B$ for each $a \in A$.
Let $H = \{h \in G \mid h + B = B\}$. Note that H is a group! Then we just saw that $A \subseteq H$. We need to show that for all $b \in B$ and $h \in H$, $b + h \in B$. But this follows from the definition of H.

3 The Cauchy-Davenport Theorem

Now let p be prime and let $A, B \subseteq \mathbb{Z}_p$. There are no nontrivial subgroups in $\mathbb{Z}_p$, so $|A+B| = \max\{|A|, |B|\}$ cannot happen except in trivial cases.
The Cauchy-Davenport theorem shows that in fact $|A+B|$ is as large as in the case of the real numbers, except for the obvious constraint that it cannot be larger than p.

Theorem 1.
$$|A+B| \geq \min\{|A|+|B|-1, p\}.$$

Proof. By induction on $|B|$. If $|B| = 0$ or 1 then the claim is obvious. If $|A| = p$ the claim is obvious.
Now let $|B| > 1$. By the previous result, we know that $|A+B| > |A|$ (this is the only place where we use the fact that p is prime!). Since $A + B \not\subseteq A$, there is an element $a_0 \in A$ such that $a_0 + B \not\subseteq A$. Let $B_0 = \{b \in B \mid a_0 + b \notin A\}$. We have $|B_0| \geq 1$.
Define $A' = A \cup (a_0 + B_0)$, and $B' = B \setminus B_0$. By definition, $a_0 + B_0 \cap A = \emptyset$, so $|A'| = |A| + |B_0|$. Further, $|B'| = |B| - |B_0|$.
Finally, note that $A' + B' \subseteq A + B$. Clearly we only need to show that $(a_0 + B_0) + (B \setminus B_0) \subseteq A + B$. Take any element $b_0 \in B_0$ and $b \in B \setminus B_0$. We want to show that $a_0 + b_0 + b \in A + B$. Since $b \in B \setminus B_0$, there is some element $a \in A$ such that $a_0 + b = a$. Then $a_0 + b_0 + b = (a_0 + b) + b_0 = a + b_0 \in A + B$.
The induction hypothesis applied to A', B' completes the proof. □

4 Proof via Combinatorial Nullstellensatz

We now see another proof, this time using polynomials(!), due to Alon-Nathanson-Ruzsa.
The following basic fact will underlie the approach.

Theorem 2 (Combinatorial Nullstellensatz)**.** *Let $\mathbb{F}$ be a field. Let $S_1, \ldots, S_m \subseteq \mathbb{F}$ be sets of size $k_1, \ldots, k_m$. Suppose $P(X_1, \ldots, X_m) \in \mathbb{F}[X_1, \ldots, X_m]$ be nonzero polynomial such that for each i, the degree in X_i of P at most $k_i - 1$.*
Then there exists $(a_1, \ldots, a_m) \in \prod_i S_i$ such that $P(a_1, \ldots, a_m) \neq 0$.

The $m = 1$ case is simply the statement that polynomial of degree d has at most d roots. The general case can be proved by induction on m (exercise!). The key is to write

$$P(X_1, \ldots, X_m) = \sum_{j=0}^{k_m - 1} P_j(X_1, \ldots, X_{m-1}) X_m^j.$$

Since P is nonzero, some P_j is nonzero.
Now we prove the Cauchy-Davenport theorem. Take sets $A, B \subseteq \mathbb{F}_p$. Let $|A| = r$, $|B| = s$, $|A+B| = t$. Suppose the Cauchy-Davenport theorem didn't hold in this case, i.e., $t \leq r + s - 2$ and $t \leq p - 1$. Consider the polynomial
$$Q(X, Y) = \prod_{c \in A+B} (X + Y - c).$$

Observe that Q vanishes on every point $(a, b) \in A \times B$.
We cannot apply the Combinatorial Nullstellensatz directly, since Q has individual degree t in each variable. However, we can apply some transformations to Q. Let $P_A(X) = \prod_{a \in A}(X - a)$. Let $P_B(Y) = \prod_{b \in B}(Y - b)$. Then $P_A(a)$ and $P_B(b)$ also vanish on all points $(a, b) \in A \times B$. Thus if we *reduce* $Q(X, Y)$ mod $P_A(X)$ and $P_B(Y)$ (namely, whenever we see X^r in $Q(X, Y)$, we replace it with the polynomial $X^r - P_A(X)$, and whenever we see Y^s, we replace it with $Y^s - P_B(Y)$), the resulting polynomial $\hat{Q}(X, Y)$ will also vanish on all points in $A \times B$. Further, this polynomial will have degree at most $r - 1$ and $s - 1$ in X and Y. Thus we may apply the Combinatorial Nullstellensatz to $\hat{Q}$.

This means that $\hat{Q}(X,Y)$, which we know is of the form $Q(X,Y) - u(X,Y)P_A(X) - v(X,Y)P_B(Y)$, is the zero polynomial.
We will now get a contradiction. Consider the coefficient of the monomial $M = X^{r-1}Y^{t-(r-1)}$ in $Q(X,Y)$. It equals $\binom{t}{r-1}$, which is nonzero mod p since $t \leq p-1$ (this is the place where we use that p is prime!). Since $t \leq r+s-2$, we have that $t-(r-1) \leq s-1$. Thus M has individual degrees at most $r-1$ and $s-1$, and appears in Q with a nonzero coefficient. Furthermore, by looking at degrees, we see that M cannot appear in $u(X,Y)P_A(X) + v(X,Y)P_B(Y)$ with a nonzero coefficient. Thus M must appear in $\hat{Q}$ with a nonzero coefficient, which contradicts the fact that $\hat{Q}$ is the zero polynomial.

5 The Erdos-Heilbronn Conjecture

We now study a different situation, the case of distinct sums.
For a set A, we define $A \hat{+} A$ by:

$$A \hat{+} A = \{a + a' \mid a, a' \in A, a \neq a'\}.$$

How small can $A \hat{+} A$ be? In the real numbers, if A is an arithmetic progression, we have $|A \hat{+} A| = 2|A| - 3$. In fact, we have the bound $|A \hat{+} A| \geq 2|A| - 3$ for all sets $A \subseteq \mathbb{R}$.
Next class we will see a polynomial-based proof that this inequality holds even in $\mathbb{F}_p$.