ADDITIVE COMBINATORICS

ALEX THOLEN

1. Basic

Let's begin with an abelian additive group Z. For example, the integers. We define

Definition 1.1. Let A, B be two finite subsets of Z. We let $A + B := \{a + b | a \in A, b \in B\}$ and $A - B := \{a - b | a \in A, b \in B\}$

We can have quite a few questions with this. First, we can ask what are the relative sizes of $A, B, A + B, A - B, A + A, A - A, A + B + B$, etc. Another question we can ask is if $|A+A| \sim |A|$, do we get $|A-A| \sim |A|$, and do we get $|A+A+A| \sim |A|$? Here, we don't work with subgroups directly, where $|A + A| = |A|$, but we work with approximate subgroups. Now, this approximate is quite approximate. For example, with an arithmetic sequence of size N, then $|A + A| = 2N - 1$, however this does count as $|A + A| \sim |A|$. That is also true with multidimensional arithmetic sequences: $A := \{a + j_1 r_1 + j_2 r_2 + ... + j_d r_d | 1 \leq j_s \leq N_s, 1 \leq s \leq d\}$. Here we get $|A + A| \sim 2^d |A|$.

2. Bounds

Now, let's look at some bounds on the size of $A+B$. Obviously, we get $|A||B|$ as an upper bound, given that that's how many things we look at. However, a lower bound might also be equal. Let's first show that translations don't matter.

Lemma 2.1. $|A + B| = |C + B|$ *where* $C = \{a + d | a \in A\}$ *for some constant* d.

Proof. Let's look at $A + B$. That is $\{a + b | a \in A, b \in B\}$. We know that translations don't change the size of a set, so we get $|A + B| = \{a + b + d | a \in A, b \in B\}$ for all constants d. Now, if we look at $|C + B|$, we get $\{c + b | c \in C, b \in B\}$, which is the same as $\{(a + d) + b | a \in A, b \in B\}$, which means that $|A + B| = |C + D|$. ■

Alright. So, now let's get a lower bound.

Theorem 2.2. $|A + B| \geq |A| + |B| - 1$.

Proof. Since we have shown that translations don't change the size of their sum, we translate A such that $\sup(A) = 0$, and we translate B such that $\inf(B) = 0$. Now, since A, B are finite, we know that that means that $0 \in A, B$. So, that means that $A, B \subset A + B$. And since A is non-positive integers, and B is nonnegative integers, they can only share one element, so $|A + B| \geq |A| + |B| - 1$. ■

We know these bounds are tight, for example both bounds are hit with $|A| = |B| = 1$, so let's look at having a different group than $\mathbb{Z}$.

Date: December 25, 2017.

3. Integers Modulo

Now, let's look at integers modulo p. First, let's look at $p = 2$. This should be easy. The four subsets: $(), (0), (1), (0, 1)$. $()+ANYTHING = ()$, $(0)+ANYTHING = SAMETHING$, $(1) + (1) = (0), (1) + (0, 1) = (0, 1)$. Now, $p = 3$. With $p = 3$, we have 8 subsets, and this gets more complicated.