2 Small Doubling

In this section we will focus our attention on subsets A of an abelian group G which satisfy the equation $|A + A| \leq t|A|$ for some fixed constant t. We will say that such a set A has *small doubling*. First let us consider this phenomena when the group G is the integers. As we know, arithmetic progressions have the smallest possible doubling constant. An arithmetic progression given by $A = \{a + jb \mid 0 \leq j \leq m\}$ will satisfy $|A + A| < 2|A|$. More generally, let us define a *d-dimensional* arithmetic progression to be any set of the following form

$$A = \{a + j_1 b_1 + \ldots + j_d b_d \mid 0 \leq j_i \leq m_i\}.$$

In this case the set $A + A$ will have a similar form to A but the upper bounds for the j_i indices will double. This gives us

$$A + A = \{2a + j_1 b_1 + \ldots + j_d b_d \mid 0 \leq j_i \leq 2m_i\}$$

and again this structure results in small doubling. Here is another way to construct a set with small doubling. Suppose that we already have a set A for which $|A + A| \leq t|A|$, and we choose $A' \subseteq A$ so that $|A'| \geq \delta|A|$. Then we have $|A' + A'| \leq |A + A| \leq t|A| \leq t\delta|A'|$ so again A' has small doubling. The following famous theorem of Freiman asserts that these are the only reasons a set of integers has small doubling.

Theorem 2.1 (Freiman) *For every t there exist $\delta > 0$ and d with the following property. If $A \subseteq \mathbb{Z}$ satisfies $|A+A| \leq t|A|$, then A is contained in a d-dimensional arithmetic progression A^* for which $|A| \geq \delta|A^*|$.*

In more general abelian groups, subgroups give another structure which can result in small doubling. There is a generalization of Freiman's Theorem to this setting due to Green and Ruzsa where the term "arithmetic progression" is replaced by the pre-image of an arithmetic progression under the canonical homomorphism from G to G/H for some $H \leq G$. In fact, this result has even been generalized to the setting of arbitrary groups by Breulliard, Green, and Tao, but even the statement of their result is beyond our scope here.

Let's get going by introducing some basic tools for working with sets of small doubling.

Basic Tools

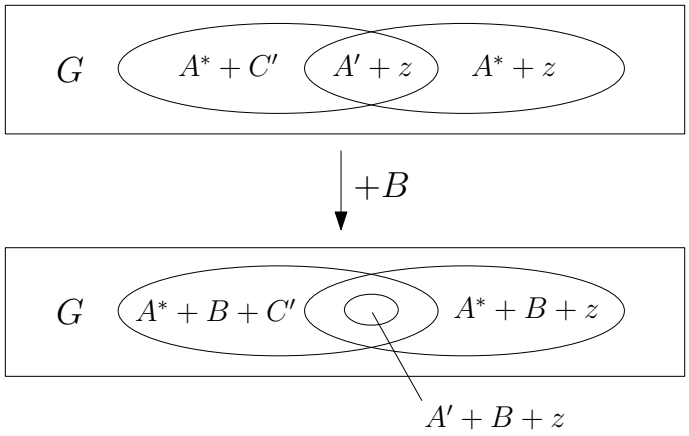
Lemma 2.2 (Petridis) *Let $A, B \subseteq G$ be finite and nonempty, and choose $A^* \subseteq A$ so that $t = \frac{|A^*+B|}{|A^*|}$ is minimum. Then for every finite nonempty set $C \subseteq G$ we have*

$$|A^* + B + C| \leq t|A^* + C|.$$

Proof: We proceed by induction on $|C|$. As a base case, observe that when $|C| = 1$ we have $|A + B + C| = |A + B| \leq t|A| = k|A + C|$. For the inductive step, $|C| \geq 2$ and we choose $z \in C$ and define $C' = C \setminus \{z\}$. Define the set $A' = \{a \in A^* \mid a + z \subseteq A^* + C'\}$ and note the following key property

$$A' + z = (A^* + z) \cap (A^* + C')$$

Next, we consider a bipartite graph on two copies of G where we join an element x in the first copy to an element y in the second if $y \in x + B$.



A nice feature of this bipartite graph is that we can easily consider the effect of adding B to the set $A^* + C = (A^* + C') \cup (A^* + z)$ in our graph by considering the set of points $A^* + C$ in the first copy of G and looking at their neighbours in the second copy of G. Applying the inductive hypothesis and the fact that $|A' + B| \geq t|A'|$ (since $A' \subseteq A$) we find

$$\begin{aligned}
|A^* + B + C| &= |A^* + B + C'| + |A^* + B + z| - |(A^* + B + C') \cap (A^* + B + z)| \\
&\leq |A^* + B + C'| + |A^* + B + z| - |A' + B + z| \\
&\leq t|A^* + C'| + t|A^*| - t|A'| \\
&= t|A^* + C| \qquad \square
\end{aligned}$$

Lemma 2.3 (Ruzsa's Triangle Inequality) *If $A, B, C \subseteq G$ are finite and nonempty,*

$$|A||B - C| \leq |A + B||A + C|.$$

Proof: For every $z \in B - C$ we choose $\beta(z) \in B$ and $\gamma(z) \in C$ so that $\beta(z) - \gamma(z) = z$. Now we shall construct a map $\phi : A \times B - C \to A + B \times A + C$ by the rule that $\phi(a, z) = (a + \beta(z), a + \gamma(z))$. If $\phi(a, z) = \phi(a', z')$ then we have

$$z = \beta(z) - \gamma(z) = (a + \beta(z)) - (a + \gamma(z)) = (a' + \beta(z')) - (a' + \gamma(z')) = \beta(z') - \gamma(z') = z'.$$

It follows that $a = a'$ so ϕ is an injection. This completes the proof. □

Generalizing our earlier notation, we define $mA = \underbrace{A + A + \ldots + A}_{m}$.

Theorem 2.4 (Plünnecke) *If $A \subseteq G$ is finite and nonempty and $|A + A| \leq t|A|$ then*

$$|\ell A - mA| \leq t^{\ell+m}|A|.$$

Proof: Choose $A^* \subseteq A$ so that $t^* = \frac{|A^*+A|}{|A^*|}$ is minimum and note that $t^* \leq t$. First we shall use Petridis' Lemma to get an upper bound on $|A^* + \ell A|$

$$|A^* + \ell A| = |A^* + A + (\ell - 1)A| \leq t^*|A^* + (\ell - 1)A| \ldots \leq (t^*)^\ell |A^*| \leq t^\ell |A^*|$$

Now for the general case, we apply Ruzsa's Triangle Inequality as follows

$$|A^*||\ell A - mA| \leq |A^* + \ell A||A^* + mA| \leq t^{\ell+m}|A^*|^2.$$

Cancelling one factor of $|A^*|$ then gives $|\ell A - mA| \leq t^{\ell+m}|A^*| \leq t^{\ell+m}|A|$ as desired. □

Bounded Torsion

Now we shall turn our attention to sets with small doubling in abelian groups with bounded torsion (i.e. those for which every element has bounded order). In this case there is no need to contend with arithmetic progressions, so subgroup structure will be the only cause for sets to have small doubling.

Theorem 2.5 (Ruzsa) *Assume that every element in G has order $\leq r$ and let $A \subseteq G$ be finite and nonempty. If $|A + A| \leq t|A|$ then there exists $A \subseteq H \leq G$ with $|H| \leq t^2 r^{t^4}|A|$.*

Proof of Theorem 2.5: Choose a maximal collection of elements $B \subseteq 2A - A$ so that the sets $b - A$ and $b' - A$ are disjoint whenever $b, b' \in B$ are distinct. Since each set of the form $b - A$ has size $|A|$ and they are all contained in $2A - 2A$ we have $|B||A| \leq |2A - 2A| \leq t^4|A|$. This gives us the following bound on $|B|$ which is independent of $|A|$.

$$|B| \leq t^4$$

Now consider an arbitrary element $x \in 2A - A$. By the maximality of B there must exist $b \in B$ for which $(x - A) \cap (b - A) \neq \emptyset$. So, there must exist $a, a' \in A$ for which $x - a = b - a'$ and this gives us $x = b - a' + a$ and then $x \in B - A + A$. Since x was arbitrary, we have

$$2A - A \subseteq B - A + A.$$

Next we show that the above property generalizes nicely to higher order sums.
Claim: $(j+1)A - A \subseteq jB + A - A$ for all positive integers j.

We shall prove the claim by induction on j. The base case when $j = 1$ we have just verified. Now for the inductive step we have

$$\begin{aligned}(j+1)A - A &= (2A - A) + (j-1)A \\ &\subseteq B + A - A + (j-1)A \\ &= B + jA - A \\ &\subseteq B + \big((j-1)B + A - A\big) \\ &= jB + A - A\end{aligned}$$

Let K be the subgroup generated by B. Then K is generated by at most t^4 elements each of which has order at most r which gives the following bound

$$|K| \leq r^{t^4} \tag{1}$$

Now let H denote the subgroup generated by A. Every element in H may be expressed as a sum of elements of A so (adopting the convention that $0B = \{0\}$) we have

$$H \subseteq \cup_{j=1}^{\infty}(jA - A) \subseteq \cup_{j=1}^{\infty}\big((j-1)B + A - A\big) \subseteq K + A - A \tag{2}$$

Now combining equations 1 and 2 and applying our lemma again we find

$$|H| \leq |K + A - A| \leq |K||A - A| \leq |K|t^2|A| \leq t^2 r^{t^4}|A|$$

as desired. $\square$