Application 3.2 (Ruzsa)**.** *Let $\alpha \in \mathbb{R}$ and A be a finite non-empty set in a commutative group. Suppose that $|A+A| \leq \alpha|A|$. Then for all positive integers $h \geq 2$*

$$|hA - A| \leq \binom{\alpha^4 + h - 2}{h-1} \alpha^2 |A|.$$

Proof.

□

Later on in the course a more efficient covering lemma of Chang.

Lemma 3.3 (Chang's covering lemma)**.** *Let $\alpha, \beta \in \mathbb{R}$ and A, B be finite non-empty sets in a commutative group. Suppose that $|A+B| \leq \beta|B|$ and $|A+A| \leq \alpha|A|$. Then there exists*

$$t \leq \lfloor (1 + \log_2(\alpha\beta)) \rfloor$$

and finite subsets $S_1, \ldots, S_t \subseteq A$ of cardinality at most $\lfloor 2\alpha \rfloor$ such that A can be covered as follows

$$A \subseteq B - B + S_t + (S_{t-1} - S_{t-1}) + \cdots + (S_1 - S_1).$$

Remark. One can add 0 to S_t to get the more symmetric form

$$A \subseteq B - B + (S_t - S_t) + (S_{t-1} - S_{t-1}) + \cdots + (S_1 - S_1).$$

As we will see the proof gives $|S_t| < 2\alpha$ and so $|S_t \cup \{0\}| \leq 2\alpha$. Note, however, that it is no longer necessarliy the case that $A_t \cup \{0\} \subseteq A$. Under very mild assumption on α and β we also get $t \leq 2\alpha \log(\alpha\beta)$.

Proof of Lemma 3.3.

□

What if we want to cover B by just translates of A? We succeed, but at a cost.

Lemma 3.4 (Covering by translates of the set)**.** *Let $\alpha \in \mathbb{R}$ and A, B be finite non-empty sets in a commutative group. Suppose that $|A - B| \leq \alpha|A|$. Then a set $S \subseteq B - A$ of cardinality at most $\lfloor \alpha \log(|B|) \rfloor$ such that $B \subseteq S + A$.*

Remarks. The example with the random subset found at the top of p.11 (the last page) of the first handout suggests that the bound on the number of necessary translates is sharp. The $\log(|A|)$ factor can in general make a huge difference. However, if we take cardinalities, then the power trick allows us to drop this additional factor. So in some circumstances this last covering lemma turns out to be the most efficient.

There are other similar covering lemmas. For example if $|A + B| \leq \alpha|A|$ then one can find $S \subseteq B - A$ of cardinality $O(\log(|A|)\alpha)$ such that $B \subseteq S + A$. The proofs of such results use additive energy and are not covered here.

The proof of the lemma is postponed until Section 5.

4 Freiman isomorphisms

Combinatorics is not enough to get a strong version of Freiman's theorem. One needs to be able to perform Fourier analysis on $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$, the integers modulo n.

For technical reasons it is often much better to do Fourier analysis on $\mathbb{Z}_n$ rather than $\mathbb{Z}$. It is even more advantageous to do Fourier analysis on the characteristic function of a set whose relative density in $\mathbb{Z}_n$ is not too small.

With this in mind we set a goal: start with a finite set $A \subset \mathbb{Z}$ and produce a "model" B for A. B will be a "somewhat dense" subset of $\mathbb{Z}_n$ for some n and crucially "encode all the additive structure of A".

Have to wait a week or two to see why this is a sound strategy. At this stage we only introduce one important notion and prove one important result.

Let us begin with a definition due to Freiman, which captures in a concise way the phrase "B encodes all the additive structure of A".

Definition. Let $k \geq 2$ be a positive integer and A a subset of a commutative group. A map $\phi : A \mapsto H$ from A to a commutative group H is a *k-Freiman homomorphism* if for all $x_1, \ldots, x_{2k} \in A$, the condition

$$x_1 + \cdots + x_k = x_{k+1} + \cdots + x_{2k}$$

implies that

$$\phi(x_1) + \cdots + \phi(x_k) = \phi(x_{k+1}) + \cdots + \phi(x_{2k}).$$

ϕ is a *k-Freiman isomorphism* if it is an injection and the condition

$$x_1 + \cdots + x_k = x_{k+1} + \cdots + x_{2k}$$

is equivalent to

$$\phi(x_1) + \cdots + \phi(x_k) = \phi(x_{k+1}) + \cdots + \phi(x_{2k}).$$

When no subscript appears, we assume $k = 2$.

We say A is *k-Freiman isomorphic* to $\phi(A)$.

Remark. A Freiman homomorphism is a map with domain A.

A strange definition, so let us familiarise ourselves with it.

Real time exercise. For each of the following you are given k, A, H and ϕ. Decide whether ϕ is a freiman k-homomorphism. If it is, decide whether it is a k-Freiman isomorphism.

(i) Any k, any A, any H and ϕ the trivial map that maps everything to zero (in H).

(ii) Any k, $A = \{1, \dots, n\} \subset \mathbb{Z}$, $H = \mathbb{Z}$ and $\phi(i) = 2i$.

(iii) $k = 2$, $A = \{0, 1\} \subset \mathbb{Z}$, $H = \mathbb{Z}_2$ and ϕ is "reduction mod 2" $\phi(i) = i \bmod 2$.

(iv) Any k, any $A \subset \mathbb{R}^d$, $H = \mathbb{R}^d$ and $\phi(\mathbf{v}) = A\mathbf{v} + \mathbf{b}$ for some invertible $d \times d$ matrix A and some $\mathbf{b} \in \mathbb{R}^d$.

Solution.

Example 4.1. *(i) Let $k, n \geq 2$ be positive integers and $A \subset \mathbb{Z}$ a finite set of positive integers. Reduction* $\mathrm{mod} n$*, $\phi : A \mapsto \mathbb{Z}_n$ given by $\phi(i) = i \bmod n$, is a k-Freiman homomorphism. It is a k-Freiman isomorphism if there is no wrap-around: $k \max\{A\} < n$.*

(ii) Let $k \geq 2$ be a positive integer, p be a prime, $0 \neq q \in \mathbb{Z}_p$ and $A \subseteq \mathbb{Z}_p$ a set of residues. Multiplication by q is a k-Freiman isomorphism, $\phi : A \mapsto \mathbb{Z}_p$ given by $\phi(i) = qi \bmod p$.

(iii) Let $k \geq 2$ be positive integer, p be a prime and $A \subseteq \mathbb{Z}_n$ a finite set of residues. Mapping $x \in \mathbb{Z}_n$ to the unique residue in $\{0, \ldots, n-1\}$ is a k-Freiman isomorphism provided that $A \subseteq I_j = (\frac{(j-1)n}{k}, \frac{jn}{k}]$. $\phi : A \mapsto \mathbb{Z}$ defined by $\phi(x) = x$.

Proof. In principle, we must establish two properties: ϕ is an injection and

$$x_1 + \cdots + x_k = x_{k+1} + \cdots + x_{2k} \iff \phi(x_1) + \cdots + \phi(x_k) = \phi(x_{k+1}) + \cdots + \phi(x_{2k}).$$

In fact must only check the if and only if statement!

Injectivity of ϕ follows from $\Longleftarrow$ by taking $x_1 = \cdots = x_k = x$ and $x_{k+1} = \cdots = x_{2k} = y$: If $\phi(x) = \phi(y)$, then $k\phi(x) = k\phi(y)$ so $kx = ky$. When the ambient group is $\mathbb{Z}$ of $\mathbb{Z}_p$, "k is cancelled" and so we get $x = y$.

Only show $k = 2$ here.

□

Proposition 4.2 (Ruzsa)**.** *Let $A \subset \mathbb{Z}$ be a finite non-empty set of integers and $\alpha \in \mathbb{R}$. Suppose that $|A+A| \leq \alpha|A|$. Let $k \geq 2$ be a positive integer and $m > \alpha^{2k}|A|$ be another positive integer. There exists a subset $A' \subseteq A$ of cardinality at least $|A|/k$ that is k-Freiman isomorphic to a subset of $\mathbb{Z}_m$.*

Proof.

□

Theorem 4.3 (Green-Ruzsa)**.** *Let A be a finite non-empty set in a commutative group and $\alpha \in \mathbb{R}$. Suppose that $|A+A| \leq \alpha|A|$. Then for all $k \geq 2$ there exists a group G of cardinality at most $C|A|$ such that A is k-Freiman isomorphic to a subset of G.*

C depends on k and α and may be taken to be $C = (10k\alpha)^{10\alpha^2}$.

5 Representations and additive energy

The topic now becomes more tangible. Let A and B be finite non-empty sets in a commutative group. We study the number of representations of an element x in the ambient group as a sum $a+b$ with $a \in A$ and $b \in B$.

It turns out there are a few equivalent ways to define this quantity.

$$\begin{aligned} r_{A+B}(x) &= \#\text{ representations of } x \text{ as a sum in } A+B \\ &= |\{(a,b) \in A \times B : x = a+b\}| \\ &= |(x-A) \cap B| \\ &= |A \cap (x-B)|. \end{aligned}$$

Note that $r_{A+B}(x) \leq \min\{|A|, |B|\}$.

r_{A+B} is *supported* on $A+B$ – the set of x where $r_{A+B}(x) \neq 0$ is $A+B$.

Real time exercise. (i) Let $A = B = \mathbb{Z}_p$. Find $r_{A+B}(x)$, for all x in the support of r_{A+A}.

(ii) Let $A = \mathbb{Z}_p \times \{\mathbf{0}\}$ and $B = \{0\} \times \{\mathbf{e}_1 \ldots, \mathbf{e}_d\}$ in $\mathbb{Z}_p \times \mathbb{Z}^d$. Find $r_{A+B}(x)$, for all x in the support of r_{A+B}.

Solution.

Let us now compute the sum of $r_{A+B}(x)$ over all x in the ambient group.

$$\sum_x r_{A+B}(x) =$$

Definition. Let A and B be finite non-empty sets in a commutative group. Their *additive energy* is

$$E(A,B) = \sum_{x \in A+B} r_{A+B}(x)^2.$$

Let us now see some of the basic properties of the additive energy.

Lemma 5.1 (Cauchy–Schwarz lower bound)**.** *Let A and B be finite non-empty sets in a commutative group. Then*

$$E(A,B) \geq \frac{|A|^2|B|^2}{|A+B|}.$$

In particular, if $|A+B| \leq \alpha|A|$, then $E(A,B) \geq \dfrac{|A|B|^2}{\alpha}$.

Proof.

□