Problems for Week I

Note: Starred exercises are additional, in the sense that they are not as central to the course. They are usually longer, though not necessarily harder than the rest.

Problem 1. Give a rigorous proof of Ruzsa’s triangle inequality: $|A||B - C| \leq |B - A||A - C|$.

Problem 2. Another proof of Ruzsa’s triangle inequality.

Recall that the convolution of two functions $f$ and $g$ (with discrete support) is defined as

$$f * g(x) = \sum_z f(z)g(x - z).$$

Prove the triangle inequality by comparing a lower and an upper bound for the quantity

$$Q = \sum_{v \in B-C} 1_{B-A} * 1_{A-C}(v).$$

As usual, $1_S$ is the characteristic function of a set $S$ defined as $f(x) = \begin{cases} 1, & x \in S \\ 0, & x \notin S \end{cases}$.

Problem 3*. An explanation of the term ‘triangle inequality’. Let $X$, $Y$ and $Z$ be finite non-empty sets in a group. Let

$$d(X, Y) = \log \left( \frac{|X - Y|}{|X|^{1/2}|Y|^{1/2}} \right).$$

Prove that $d(X, Z) \leq d(X, Y) + d(Y, Z)$. Is $d$ a metric (on the set of finite non-empty subsets of the commutative group)?

Problem 4. Let $n \geq 4$ be a positive integer.

(i) Suppose that $|A + A - A| \leq \alpha |A|$. Find an upper bound for the cardinality of the $n$-fold sumset $A + A - A + \cdots + (-1)^n A$ in terms of $\alpha$ and $|A|$.

(ii) Suppose that $|A + A + A| \leq \beta |A|$. Find an upper bound for the cardinality of the $n$-fold sumset $A + A - A + \cdots + (-1)^n A$ in terms of $\beta$ and $|A|$.

Problem 5. Let $A$ and $B$ be finite non-empty sets of a commutative group. We have seen the
importance of the subset $X$ that minimises the quantity $\frac{|Z + B|}{|Z|}$ over all non-empty subsets $Z$ of $A$. In each of the following three examples identify $X$.

(i) $A$ is a subgroup and $B$ is any non-empty set of the ambient group.

(ii) $A = B$ is an arithmetic progression in $\mathbb{Z}$.

(iii) $A = B$ is the subset of $\mathbb{Z}^3$ that consists of the union of the “discrete cube” $\{(x, y, z) : 1 \leq x, y, z \leq n\}$ with three “elongated edges” $\{(x, 0, 0) : 1 \leq x \leq n^2\}$ and $\{(0, 0, z) : 1 \leq z \leq n^2\}$.

**Problem 6*. Let $A$, $B$ and $C$ be finite non-empty sets of a commutative group and $X$ the minimiser associated with $A$ and $B$ described in the problem above. Here is a proof of the inequality $|X||X + B + C| \leq |X + B||X + C|$ that was given by Reiher.

(i) Use Hall’s marriage theorem a.k.a. König’s theorem to prove the existence of a bijection $\phi$ from $X \times (X + B)$ to itself with the special property that if $\phi(r, s) = (x, y)$, then $y - r \in B$.

(ii) Use $\phi$ to construct an injection $\theta : X \times (X + B + C) \mapsto (X + B) \times (X + C)$ as follows:

- order the elements of $C$ in some way;
- write each $s \in X + B + C$ as the sum $t + c$, where $t \in X + B$ and $c \in C$ is minimal in the chosen order;
- map $(a, s) \in X \times (X + B + C)$ to $(y, x + c)$, where $s = t + c$ as above and $(x, y) = \phi^{-1}(a, t)$.

**Problem 7*. Can you prove the inequality $|A||B + C| \leq |A + B||A + C|$ in a similar way to the triangle inequality?

**Problem 8*. Plünnecke’s inequality for a large subset. Let $\varepsilon > 0$. We prove that there exists $\emptyset \neq Y \subseteq A$ of cardinality at least $(1 - \varepsilon)|A|$ such that $|Y + hA| \leq (\alpha/\varepsilon)^h|A|$. Fill in the details in the following steps.

Apply Plünnecke’s inequality to the pair $(A, A)$ to find $\emptyset \neq X_1 \subseteq A$ such that $|X_1 + hA| \leq \alpha^h|X_1|$. If $X_1$ is large enough we are done.

Otherwise apply Plünnecke’s inequality to the pair $(A \setminus X_1, A)$ to find $\emptyset \neq X_2 \subseteq A \setminus X_1$ such that $|X_1 + hA|$ is bounded in a reasonable way (your job is to find a reasonable bound).

Keep going this way until $|X_1| + \cdots + |X_k| > (1 - \varepsilon)|A|$.

One cannot take $Y = A$ in general. Can you find an example?
Problem 9. Plünnecke’s inequality and one of the many inequalities of Ruzsa we have seen imply that if $|A + A| \leq \alpha |A|$, then

$$|A + A + A| \leq \min\{\alpha^3|A|, \alpha^{3/2}|A|^{3/2}\}.$$ 

Modify the example given in Problem 5 (iii) to show that the bound is up to constant sharp (for infinitely many values of $\alpha$ that form an unbounded sequence).

Problem 10. A covering lemma of Green and Ruzsa. Let $A$ and $B$ be finite non-empty sets in a commutative group. Suppose that $|A + B| \leq \alpha |A|$. Prove there exists a set $S$ of cardinality at most $2\alpha$ such that every element $b \in B$ can be expressed in at least $|A|/2$ ways as a sum $b = s + a - a'$ where $a, a' \in A$ and $s \in S$, i.e. prove that for all $b \in B$

$$|\{(s, a, a') \in S \times A \times A : b = s + a - a'\}| \geq \frac{|A|}{2}.$$ 

Problem 11*. For those that like the probabilistic method. We prove that with high probability $\log(n)$ translates of a random subset of $\{1, \ldots, n\}$ are not adequate to cover the entire set.

A random subset of $\{1, \ldots, n\}$ is formed by including each element uniformly with probability $1/2$ independently of all the others. Let $A$ be such a random set and $S \subseteq \{1, \ldots, n\}$ be a set of cardinality $\log(n)$.

(i) Find the probability that $i \in \{1, \ldots, n\}$ belongs to $S + A$.

(ii) Deduce an upper bound for the probability that $S + A$ covers $\{1, \ldots, n\}$ i.e., that $\{1, \ldots, n\} \subseteq A + S$.

(iii) Use a so-called union bound to prove that with probability $1 - o(1)$ there is no set $S$ of cardinality $\log(n)$ such that $S + A$ covers $\{1, \ldots, n\}$.

We have therefore established that with high probability, $\log(n)$ translates of a random set do not cover $\{1, \ldots, n\}$. This is an existence proof. We know that most subsets of $\{1, \ldots, n\}$ have this property, but our proof does not provide us with an explicit example.

Problem 12*. Use Problem 11 (as a black box, if necessary) to prove that for, say, all $\alpha > 2$ there exist sets $A$ and $B$ such that $|A + B| \leq \alpha |A|$ and $B$ cannot be covered with fewer than $c \log(|A|)\alpha$ translates of $A$, where $c$ is an absolute constant.
Problem 13. Let $A$ be a finite non-empty set in a commutative group. Suppose that $|A + A| \leq \alpha |A|$. Here is another proof of the bound $|A + A + A| \leq \alpha^3 |A|$ in four steps:

(i) Find an $\emptyset \neq X \subseteq A$ such that both $|X + A|$ and $|X + A + A|$ are “small”.

(ii) Cover $A$ by translates of $X$.

(iii) Deduce a covering for $A + A + A$ by translates of $X + A + A$.

(iv) Apply the power trick.

Problem 14. Let $A_1$ and $A_2$ be finite non-empty sets in a commutative group. Suppose that $|A_1| \leq \alpha_1 |A|$ for $\alpha_1 \in \mathbb{Q}$. In this exercise we establish the bound $|A_1 + A_2| \leq \alpha_1 \alpha_2 |A|$.

We saw that if $\alpha_1 = \alpha_2 = \alpha$, then $|A_1 + A_2| \leq \alpha^2 |A|$. Let us now deduce the general case from this.

Let $n_1$ and $n_2$ be positive integers such that $n_1 \alpha_1 = n_2 \alpha_2 \in \mathbb{Z}$. Why do such $n_i$ exist? Work in the direct product of the ambient group with $\mathbb{Z}^{n_1} \times \mathbb{Z}^{n_2}$. Apply the above result to $A' = A \times \{0\} \times \{0\}$, $B_1' = B_1 \times \mathbb{Z}^{n_1} \times \{0\}$ and $B_2' = B_2 \times \{0\} \times \mathbb{Z}^{n_2}$.

Problem 15. For each of the following provide a proof or counter example.

(i) Every Freiman homomorphism is a homomorphism between the ambient groups.

(ii) Every homomorphism between the ambient groups is a Freiman isomorphism between a set and its image.

Problem 16. For each of the following you are given a finite set $A$ and a positive integer $k$. Find a set $B \subset \mathbb{Z}$ and an explicit formula for a Freiman $k$-isomorphism from $A$ to $B$.

(i) $A = \{(x, y) \in \mathbb{Z}^2 : 0 \leq x, y \leq n - 1\}$, is the discrete square of side length $n$ and $k = 2$.

(ii) $A = \{(x, y) \in \mathbb{Z}^2 : 0 \leq x, y \leq n - 1\}$, is the discrete square of side length $n$ and $k = n$.

(ii) $A = \{(x_1, \ldots, x_d) \in \mathbb{Z}^d : 0 \leq x_1, \ldots, x_n \leq n - 1\}$, is the discrete $d$-dimensional cube of side length $n$ and $k = n^2$.

Problem 17. Let $A$ and $B$ be two sets in a commutative group that contain 0. Suppose that $\theta : A + A \mapsto B + B$ is a $k$-Freiman isomorphism that satisfies $\theta(0) = 0$. Prove that $A$ is $(2k)$-Freiman isomorphic to $B$. 
Problem 18*. Is there a non-trivial Freiman isomorphism from the unit circle $\mathbb{T} := \mathbb{R}/\mathbb{Z}$ to a subset of $\mathbb{R}$ that is a continuous function (on $\mathbb{T}$)?

Problem 19. For each of the following you are given a set of integers and positive integers $k$. Go through the proof of Ruzsa’s Freiman-isomorphism theorem and construct a $k$-Freiman isomorphic subset of $\mathbb{Z}_p$ for a suitable $p$.

(i) $A = \{1, 3, 5, \ldots, 17\}$ and $k = 2$.
(ii) $A = \{2, 3, 5, 8\}$ and $k = 4$.

Problem 20. For each of the following sets get an exact formula for the required quantity.

(i) The additive energy of an arithmetic progression of length $n$.

(ii) The additive energy of a Sidon set (a set where the sums $x + y$ are distinct) of cardinality $n$.

(iii) The expected value of the additive energy of an random set in $\mathbb{Z}/p\mathbb{Z}$ where each element appears with probability $p$.

Problem 21. We have seen that small doubling implies large additive energy and that large additive energy implies small doubling for a large subset.

Estimate the doubling constant and the additive energy of the set

$$A = \{1, \ldots, n\} \cup \{n^2, n^3, \ldots, n^n\}.$$

What does this example tell us?

Problem 22. The Balog-Szemerédi-Gowers theorem continues to hold when “addition takes place along the edges of a graph $G \subseteq A \times B$”.

Let $A$ and $B$ be sets in a commutative group. Define $A +_G B = \{a + b : (a, b) \in G\}$.

(i) Find $A +_G B$ when $A = B = \{1, \ldots, 2n\} \subset \mathbb{Z}$ and $G = \{1, \ldots, n\} \times \{1, \ldots, n\} \subset \mathbb{Z}^2$.

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

(iii) Prove that if $E(A, B) \geq \frac{|A|^{3/2}|B|^{3/2}}{K}$, the there exists $G \subset A \times B$ of density at least $1/K$ that satisfies $|A + G B| \leq \frac{K|G|}{\sqrt{|A||B|}}$. 

5
**Problem 23.** Find the exact number of point-line incidences when $P = \{1, \ldots, n\} \times \{1, \ldots, 2n^2\}$ and $L$ is the set of lines $y = ax + b$ where $(a, b) \in \{1, \ldots, n\} \times \{1, \ldots, n^2\}$.

What does this example show?

**Problem 24.** We establish the so-called Cauchy-Schartz lower bound on the number of point-line incidences. Let $L$ be a finite collection of lines and $P$ be a finite set of points in the plane $\mathbb{R}^2$. For each $\ell \in L$ let $n_\ell$ denote the number of points from $P$ that are on $\ell$.

Complete each of the following steps.

(i) Evaluate $\sum_{\ell \in L} n_\ell$.

(ii) Deduce $\sum_{\ell \in L} (n_\ell - 1)$.

(iii) Explain why $\sum_{\ell \in L} \left(\frac{n_\ell}{2}\right) \leq \binom{|P|}{2}$ is true.

(iv) Deduce an upper bound for $\sum_{\ell \in L} (n_\ell - 1)^2$.

(v) Finally prove

$$I(P, L) \leq |L| + |L|^{1/2}|P|.$$ 

**Problem 25*.** Formulate and prove an analogue to the Szemerédi-Trotter theorem for the number of incidences between a finite set of points $P$ and a finite collection of circles of equal radii $C$ in the plane.