ADDITIVE COMBINATORICS EXAMPLES SHEET 4: SOLUTIONS

ALED WALKER

These are the 'official' solutions for the fourth example sheet. This is not to say that they cannot be improved, nor that there are no alternative approaches, nor that there won't be the occasional small oversights or omissions! Nevertheless, this document should hopefully serve as a record of how to do all the questions, and be useful when it comes to your future revision and study.

If you have any questions about any of these solutions, please drop me an email at `aw530@cam.ac.uk`.

(1) Let

$$P = \{a + n_1v_1 + \cdots + n_dv_d : 0 \leqslant n_i < N_i\}$$

be a generalised aithmetic progression of rank d in $\mathbb{Z}$. Let

$$\Gamma = \{(m_1, \ldots, m_d) \in \mathbb{Z}^d : m_1v_1 + \cdots + m_dv_d = 0 \text{ and } |m_i| < N_i\}.$$

Recall that the volume of P is defined to be $\mathrm{vol}(P) := \prod_i N_i$. Show that

$$\frac{\mathrm{vol}(P)}{|P|} \leqslant |\Gamma| \leqslant 3^d \frac{\mathrm{vol}(P)}{|P|}.$$

Solution: For each $p \in P$, choose $b^{(p)} \in ([0, N_1) \times \cdots \times [0, N_d)) \cap \mathbb{Z}^d$ with

$$a + b_1^{(p)}v_1 + \cdots + b_d^{(p)}v_d = p.$$

Let $B = \{b^{(p)} : p \in P\}$. Trivially we have $|B| = |P|$. But also $|B + \Gamma| = |B||\Gamma|$, since if $b^{(p)} + \gamma = b^{(q)} + \gamma'$, with $\gamma, \gamma' \in \Gamma$, then $b^{(p)} - b^{(q)} \in \Gamma - \Gamma$ and hence

$$(b_1^{(p)} - b_1^{(q)})v_1 + \cdots + (b_1^{(p)} - b_1^{(q)})v_d = 0.$$

So

$$p = a + \sum_{i \leqslant d} b_i^{(p)}v_i = a + \sum_{i \leqslant d} b_i^{(q)}v_i = q,$$

and hence $b^{(p)} = b^{(q)}$.

By construction we have $B + \Gamma \subset (-N_1, 2N_1) \times \cdots \times (-N_d, 2N_d)$, and hence $|B + \Gamma| \leqslant 3^d \,\mathrm{vol}(P)$. Furthermore $B + \Gamma \supset [0, N_1) \times \cdots \times [0, N_d)$, since if $n \in [0, N_1) \times \cdots \times [0, N_d)$ we get $a + n_1v_1 + \cdots + n_dv_d \in P$. Let $p := a + n_1v_1 + \cdots + n_dv_d$. Then $n - b^{(p)} \in \Gamma$, and thus $n \in b^{(p)} + \Gamma \subset B + \Gamma$. So

$$\mathrm{vol}(P) \leqslant |B + \Gamma| = |B||\Gamma| = |P||\Gamma| \leqslant 3^d \,\mathrm{vol}(P),$$

which gives the desired inequalities.

(2) Let P be a proper generalised arithmetic progressions of rank d, and suppose $X \subset P$ has size $|X| < \varepsilon|P|$. Show that $P \setminus X$ contains a proper generalised arithmetic progressions Q of rank d with $|Q| \geqslant \varepsilon^{-1}C^{-d}$ for some constant C.

Solution: The conclusion is trivial if $\varepsilon \geqslant 8^{-d}$, so from now on we assume that $\varepsilon \leqslant 8^{-d}$. Let $N_1, \ldots, N_d \geqslant 2$ be natural numbers and $a, v_1, \ldots, v_d \in G$ such that

$$P = \{a + n_1v_1 + \cdots + n_dv_d : 0 \leqslant n_i < N_i \text{ for all } i\}.$$

Split each interval $[0, N_i)$ into disjoint subintervals $I_{k_i}^{(i)}$, $k_i \leqslant K_i$, with the properties that:

- $K_i \geqslant \varepsilon^{1/d} N_i$;
- $|I_{k_i}^{(i)} \cap \mathbb{Z}| \geqslant \varepsilon^{-1/d}/4$ for each k_i.

This is possible. Indeed, choose $I_{k_i}^{(i)}$ to have length exactly $N_i/\lceil \varepsilon^{1/d} N_i \rceil$, giving $K_i = \lceil \varepsilon^{1/d} N_i \rceil$. Then

$$|I_{k_i}^{(i)} \cap \mathbb{Z}| \geqslant \frac{N_i}{\lceil \varepsilon^{1/d} N_i \rceil} - 2 \geqslant \frac{1}{2\varepsilon^{1/d}} - 2 \geqslant \frac{1}{4\varepsilon^{1/d}}$$

since $\varepsilon \leqslant 8^{-d}$.

Then, for each $(k_1, \dots, k_d)$ with $k_i \leqslant K_i$ for all i we have that

$$P_{k_1,\dots,k_d} := \{a + n_1 v_1 + \cdots + n_d v_d : n_i \in I_{k_i}^{(i)} \text{ for all } i\}$$

is a proper generalised arithmetic progression of rank d and size at least

$$\prod_{i \leqslant d} |I_{k_i}^{(i)} \cap \mathbb{Z}| \geqslant (\varepsilon^{-1/d}/4)^d = \varepsilon^{-1} 4^{-d}.$$

Since there are at least $\varepsilon \prod_{i \leqslant d} N_i = \varepsilon |P| > |X|$ such GAPs $P_{k_1,\dots,k_d}$, by the pigeonhole principle there must be at least one such progression which is contained in $P \setminus X$.

(3) (a) Show that for any $s \geqslant 1$ and $d \geqslant 1$ every finite subset of $\mathbb{Z}^d$ is Freiman s-isomorphic to a subset of $\mathbb{Z}$.
(b) Hence deduce a Freiman–Ruzsa–Sanders inverse result of subsets of $\mathbb{Z}^d$ with small doubling.

Solution: Part(a). Let $A \subset \mathbb{Z}^d$ be a finite set. Translation is a Freiman isomorphism to all orders, so without loss of generality we may assume that $A \subset \mathbb{N}^d$.

Writing $a = (a_1, \dots, a_d)$ for each $a \in A$, define

$$K = \max_{\substack{a \in A \\ i \leqslant d}} a_i.$$

Let $M = sK + 1$. Then define the map $f : A \longrightarrow \mathbb{Z}$ by

$$f(n_1, \dots, n_d) = \sum_{i \leqslant d} a_i M^i,$$

i.e. use base M expansion.

This is a Freiman s-isomorphism. Indeed, if $a^{(1)} + \cdots + a^{(s)} = b^{(1)} + \cdots + b^{(s)}$ (with $a^{(j)}, b^{(j)} \in A$) then clearly $f(a^{(1)}) + \cdots + f(a^{(s)}) = f(b^{(1)}) + \cdots + f(b^{(s)})$, so the content is the reverse implication. So, assuming $f(a^{(1)}) + \cdots + f(a^{(s)}) = f(b^{(1)}) + \cdots + f(b^{(s)})$ we have

$$\sum_{i \leqslant d} \Big(\sum_{j \leqslant s} a_i^{(j)} - \sum_{j \leqslant s} b_i^{(j)} \Big) M^i = 0.$$

Suppose for contradiction that there is some i for which

$$\sum_{j \leqslant s} a_i^{(j)} - \sum_{j \leqslant s} b_i^{(j)} \neq 0.$$

Let i be maximal such. Then

$$\begin{aligned} M^i \leqslant \Big|\sum_{j\leqslant s} a_i^{(j)} - \sum_{j\leqslant s} b_i^{(j)}\Big| M^i = \Big|\sum_{k\leqslant i-1}\Big(\sum_{j\leqslant s} a_k^{(j)} - \sum_{j\leqslant s} b_k^{(j)}\Big)M^k\Big| &\leqslant \sum_{k\leqslant i-1}(2Ks)M^k \\ &= (2Ks)\frac{M^i-1}{M-1} \\ &= M^i - 1 \\ &< M^i, \end{aligned}$$

giving a contradiction. So no such i exists, and thus $\sum_{j\leqslant s} a^{(j)} = \sum_{j\leqslant s} b^{(j)}$ as required.

For part (b), the statement is the following. Let $K \geqslant 4$. Given a set $A \subset \mathbb{Z}^d$ with $|A+A| \leqslant K|A|$ there exists a proper generalised arithmetic progression $P \subset \mathbb{Z}^d$ with $A \subset P$, such that rank P is at most $K(\log K)^{O(1)}$ and $|P| \ll 2^{-K(\log K)^{O(1)}}|A|$. For the proof, the cleanest way is probably to let $A' \subset \mathbb{Z}$ be Freiman 16-isomorphic to A. Then $|A'+A'| \leqslant K|A'|$, and so from the Bogolyubov–Ruzsa style lemma from lectures we know that $4A'-4A'$ contains a proper GAP P of rank $(\log K)^{O(1)}$ and size $\exp(-(\log K)^{O(1)})|A'|$. Since f_{16}^{-1} extends to a 2-isomorphism on $4A'-4A'$, and 2-isomorphisms preserve proper GAPs, we have that $4A-4A$ contains a GAP $f_{16}^{-1}(P)$ with the same rank and size. Then finish as in the lectured proof of Freiman–Ruzsa for subsets of $\mathbb{Z}$.

(4) (a) Suppose that $A \subset \{1,\dots,N\}$ is such that $|A| = n \leqslant \frac{1}{2}\log\log N$. Show that, if n is sufficiently large, then there exists a prime p with

$$p \ll n^4 \log N \log\log N$$

and an integer $t \neq 0$ such that $0 \notin t\cdot((2A-2A)\setminus\{0\}) \bmod p$ and all the elements of $t\cdot A$ are congruent to an integer in $(-p/4, p/4)$ modulo p.

(b) Hence deduce that every finite set $A \subset \mathbb{Z}$ is 2-isomorphic to some $A' \subset \{1,\dots,N'\}$ where $N' \leqslant C^{C^{|A|}}$ for some constant $C > 1$.

NB: this is not exactly the version that is stated on the examples sheet, at least in the version that was available at the time of writing these solutions.

Solution: We call a prime p *bad* if there is some $x \in (2A-2A)\setminus\{0\}$ with $p|x$ (otherwise we say that p is *good*). Since such an x satisfies $|x| \leqslant 2N$, there are at most $\log(2N)/\log 2$ bad primes dividing such an x. Indeed, if $|x| = \prod_p p^{v_p(x)}$ then

$$|\{p : v_p(x) \geqslant 1\}| \leqslant \sum_p v_p(x) = \frac{\log(2^{\sum_p v_p(x)})}{\log 2} \leqslant \frac{1}{\log 2}\log\Big(\prod_p p^{v_p(x)}\Big) = \frac{\log|x|}{\log 2} \leqslant \frac{\log(2N)}{\log 2}.$$

Taking the union bound over all $x \in (2A-2A)\setminus\{0\}$, the number of bad primes is at most $(\log 2)^{-1}n^4\log(2N)$

Now let L be a large constant. If n is large enough then the number of primes between $Ln^4\log N\log\log N$ and $2Ln^4\log N\log\log N$ is at least

$$\frac{Ln^4\log N\log\log N}{2\log(2Ln^4\log N\log\log N)},$$

which is $\gg Ln^4\log N$ as $n \leqslant \frac{1}{2}\log\log N$. So, if L is large enough, there must be some good prime p in the range

$$Ln^4\log N\log\log N < p \leqslant 2Ln^4\log N\log\log N.$$

Fix such a p. Now break up the range $(-p/2, p/2)$ into four intervals each of length at most $p/4$, namely

$$I_1 = (-p/2, -p/4),\ I_2 = [-p/4, 0),\ I_3 = [0, p/4),\ \text{and}\ I_4 = [p/4, p/2).$$

Thus break up $(\mathbb{Z}/p\mathbb{Z})^n$ into 4^n boxes $I_{i_1,\dots,i_n} := I_{i_1} \times \cdots \times I_{i_n}$. Writing $A = \{a_1, \dots, a_n\}$, for each $t \in \mathbb{Z}$ we consider

$$\widetilde{t \cdot A} := (ta_1, \dots, ta_n) \bmod p \in (\mathbb{Z}/p\mathbb{Z})^n.$$

Now let t range over the sequence $1, 2, \dots, 4^n + 1$. By the pigeonhole principle, there is some box $I_{i_1,\dots,i_n}$ and two distinct $t_1, t_2 \leqslant 4^n + 1$ for which

$$\widetilde{t_1 \cdot A}, \widetilde{t_2 \cdot A} \in I_{i_1,\dots,i_n}.$$

Then, for each $a \in A$, we have that $(t_1 - t_2)a$ is congruent to an integer b modulo p which satisfies $|b| < p/4$ (the inequality is strict since there is no interval I_i both of whose endpoints are integers).

Let $t = t_1 - t_2$. Then

$$|t| \leqslant 4^n \leqslant 4^{\frac{1}{2}\log\log N} = (\log N)^{\log 2} < p,$$

since $\log 2 < 1$. So p does not divide t either, and hence $0 \notin t \cdot t((2A - 2A) \setminus \{0\})$ mod p as required.

For part (b), we argue as follows. Without loss of generality we may assume that $n = |A|$ is large. Now pick a large constant C and suppose that N' is minimal such that there exists some $A' \subset \{1, \dots, N'\}$ with A being 2-isomorphic to A'. If $N' \leqslant C^{C^n}$ we are done, so suppose otherwise. Then $|A| \leqslant \frac{1}{2}\log\log N'$ (if C is large enough), so we can apply part (a). Let $B \subset (-p/4, p/4)$ be the set $t \cdot A$ mod p, viewed as a subset of $\mathbb{Z}$. We claim that B is 2-isomorphic to A. Indeed, if $a_1 + a_2 = a_3 + a_4$ then $b_1 + b_2 = b_3 + b_4$ mod p, just by projection. But since

$$-p < b_1 + b_2 - b_3 - b_4 < p,$$

we have $b_1 + b_2 = b_3 + b_4$ in $\mathbb{Z}$. For the reverse implication, if $b_1 + b_2 = b_3 + b_4$ then $ta_1 + ta_2 = ta_3 + ta_4$ mod p, i.e. p divides $t(a_1 + a_2 - a_3 - a_4)$. But since p is good this means that $a_1 + a_2 - a_3 - a_4 = 0$.

Translating B, we find a 2-isomorphic image of A within $[1, p/2 + 1]$. This is a contradiction to the minimality of N' unless $p/2 + 1 \geqslant N'$, so we have

$$(\log\log N')^5 \log N' \geqslant n^4 \log N' \log\log N' \gg N'.$$

So $N' = O(1)$, and we are done.

There is a way of using Minkowski's first theorem to improve the bound in part (b) from C^{C^n} to just a single exponential C^n. See

`https://mathoverflow.net/questions/225773/freiman-isomorphic-sets`

for more.

(5) Let G be a finite abelian group of odd order and let $A \subset G$ be a set of density $\alpha = |A|/|G|$. For any $0 < \eta \leqslant 1$ let

$$\Delta_\eta(A) = \{\gamma \in \widehat{G} : |\widehat{1_A}(\gamma)| \geqslant \eta|A|\}.$$

(a) Show that there are $c_\gamma \in \mathbb{C}$ with $|c_\gamma| = 1$ such that for any $\Delta \subset \Delta_\eta(A)$ if

$$f(x) = \sum_{\gamma \in \Delta} c_\gamma \overline{\gamma(x)}$$

then for any $m \geqslant 1$

$$\|f\|_{2m} \geqslant \eta |A|^{1/2m}|\Delta|.$$

(b) Use Rudin's inequality (Question 8(c) on Examples Sheet 3) to deduce the strong Chang's dimension inequality: that $\Delta_\eta(A)$ is contained in $\mathrm{span}(\Gamma)$ for some multiset Γ of size $O(\eta^{-2}\log(2/\alpha))$.

Solution: Let $c_\gamma \in \mathbb{C}$ with $|c_\gamma| = 1$ be defined to satisfy the relation

$$c_\gamma \widehat{1_A}(\gamma) = |\widehat{1_A}(\gamma)|.$$

Then on the one hand

$$\Big|\sum_x 1_A(x)f(x)\Big| = \Big|\sum_x 1_A(x)\sum_{\gamma\in\Delta} c_\gamma\overline{\gamma(x)}\Big| = \Big|\sum_{\gamma\in\Delta}\widehat{1_A}(\gamma)c_\gamma\Big| = \sum_{\gamma\in\Delta}|\widehat{1_A}(\gamma)| \geqslant \eta|\Delta||A|.$$

On the other hand, by Hölder

$$\Big|\sum_x 1_A(x)f(x)\Big| \leqslant |A|^{1-\frac{1}{2m}}\|f\|_{2m}.$$

Hence $\|f\|_{2m} \geqslant \eta|A|^{1/2m}|\Delta|$ as claimed.

For the second part, let $\Delta \subset \Delta_\eta(A)$ be a maximal dissociated subset. We apply Rudin's inequality to the function $g : \widehat{G} \longrightarrow \mathbb{C}$ defined by

$$g(\gamma) = \begin{cases} c_\gamma & \text{if } \gamma \in \Delta \\ 0 & \text{otherwise.} \end{cases}$$

We have to swap the roles of G and $\widehat{G}$, which will affect our normalisations. Now $f = \widehat{g}$, and from Rudin's inequality we get

$$N^{-1/2m}\|f\|_{2m} \ll m^{1/2}\|g\|_2 = m^{1/2}|\Delta|^{1/2}.$$

Concatenating with the lower bound on $\|f\|_{2m}$ and rearranging, we get

$$|\Delta| \ll m\eta^{-2}|A|^{-1/m}N^{1/m} = m\eta^{-2}\alpha^{-1/m}.$$

Now choose $m \asymp \log(2/\alpha)$. This yields $|\Delta| \ll \eta^{-2}\log(2/\alpha)$.

Now consider the multiset $\Delta' := \Delta \cup -\Delta \cup (2\cdot\Delta) \cup (-2\cdot\Delta)$ (where if an element appears in k of these four sets we count it k times in Δ'). We have $|\Delta'| \ll \eta - 2\log(2/\alpha)$. Furthermore, $\Delta_\eta(A) \subset \mathrm{span}(\Delta')$, since if $\gamma \in \Delta_\eta(A) \setminus \mathrm{span}(\Delta')$ then $\Delta \cup \{\gamma\}$ is dissociated, contradicting maximality of Δ.

(6) This question demonstrates how Bogolyubov–Ruzsa results were obtained in the days before almost-periodicity.

(a) Show that if $E(A) \geqslant \delta|A|^3$ then, if

$$\Delta = \{\gamma \in \widehat{G} : |\widehat{1_A}(\gamma)| \geqslant \frac{1}{2}\delta^{1/2}|A|\},$$

and B is the Bohr set with frequency set Δ and width $1/2$, then $B \subset 2A - 2A$.

(b) Use part (a), together with the strong Chang bound of Question 5, to deduce that if $A \subset \mathbb{Z}/N\mathbb{Z}$ wit $|A| \geqslant N/K$ then $2A - 2A$ contains a Bohr set with rank $O(K\log K)$ and width $1/K\log K$. Compare this to the Bogolyubov–Ruzsa lemma obtained in lectures.

Solution: We know that $(1_A * 1_A) \circ (1_A * 1_A)(x) > 0$ if and only if $x \in 2A - 2A$, and also that

$$(1_A * 1_A) \circ (1_A * 1_A)(x) = \mathop{\mathbb{E}}_{\gamma} |\widehat{1_A}(\gamma)|^4 \gamma(x).$$

Finally, $E(A) = \mathbb{E}_\gamma |\widehat{1_A}(\gamma)|^4$.

Now let $x \in \mathrm{Bohr}(\Delta, 1/2)$. We have

$$\begin{aligned}\Big| \mathop{\mathbb{E}}_{\gamma} |\widehat{1_A}(\gamma)|^4 \gamma(x) - E(A)\Big| &\leqslant \mathop{\mathbb{E}}_{\gamma} |\widehat{1_A}(\gamma)|^4 |\gamma(x) - 1| \\ &\leqslant \frac{1}{2N} \sum_{\gamma \in \Delta} |\widehat{1_A}(\gamma)|^4 + \frac{2}{N} \sum_{\gamma \notin \Delta} |\widehat{1_A}(\gamma)|^4 \\ &< \frac{1}{2} E(A) + \frac{1}{2N} \delta |A|^2 \sum_{\gamma} |\widehat{1_A}(\gamma)|^2 \\ &\leqslant \frac{1}{2} E(A) + \frac{1}{2} \delta |A|^3 \\ &\leqslant E(A)\end{aligned}$$

by the assumption $E(A) \geqslant \delta |A|^3$ and by Parseval. Therefore $(1_A * 1_A) \circ (1_A * 1_A) = \mathbb{E}_\gamma |\widehat{1_A}(\gamma)|^4 \gamma(x) > 0$, so $x \in 2A - 2A$ as required.

For part (b), since $|A| \geqslant N/K$ we know that $|A + A| \leqslant K|A|$, and hence that $E(A) \geqslant K^{-1}|A|^3$. Now apply part (a) with $\delta = K^{-1}$. This shows that, with Δ as in that part, $\mathrm{Bohr}(\Delta, 1/2) \subset 2A - 2A$. Now, let Δ' be a maximal dissociated subset of Δ and let $x \in \mathrm{Bohr}(\Delta', cK^{-1}(\log K)^{-1})$, for a suitably small constant $c > 0$. If $\gamma \in \Delta$, we have $\gamma \in \mathrm{span}(\Delta')$ and hence $\gamma = \prod_{\gamma' \in \Delta'} (\gamma')^{\varepsilon_{\gamma'}}$, for some $\varepsilon_{\gamma'} \in \{-1, 0, +1\}$. Hence

$$|\gamma(x) - 1| = \Big| \prod_{\gamma' \in \Delta'} (\gamma')^{\varepsilon_{\gamma'}}(x) - 1 \Big| \leqslant |\Delta'| \max_{\gamma' \in \Delta'} |\gamma'(x) - 1| \leqslant c|\Delta'| K^{-1} (\log K)^{-1},$$

where we used the telescoping identity

$$z_1 z_2 \dots z_d - w_1 w_2 \dots w_d = (z_1 - w_1) w_2 \dots w_d + z_1 (z_2 - w_2) w_3 \dots w_d + \dots + z_1 z_2 \dots z_{d-1} (z_d - w_d).$$

We know further that $|\Delta'| \ll (\delta^{1/2})^{-2} \log(2/\alpha) \ll K \log K$. So, if c is small enough we get $|\gamma(x) - 1| \leqslant 1/2$, and so $x \in \mathrm{Bohr}(\Delta, 1/2)$.

Putting everything together we conclude that

$$\mathrm{Bohr}(\Delta', cK^{-1}(\log K)^{-1}) \subset \mathrm{Bohr}(\Delta, 1/2) \subset 2A - 2A,$$

giving the Bohr set as required.

In lectures we used almost-periodicity to find a Bohr set in $4A - 4A$ with much smaller rank, namely $(\log K)^{O(1)}$, even if the width K^{-2} was somewhat smaller than the width we found in this exercise. In fact, in Sanders original work, he finds such a Bohr set in $2A - 2A$.

(7) Show that if $f : \{1, \dots, N\} \longrightarrow \mathbb{Z}$ has at least $K^{-1}N^3$ many $x, y, z, w \in \{1, \dots, N\}$ such that

$$x + y = z + w \qquad \text{and} \qquad f(x) + f(y) = f(z) + f(w)$$

then there exists $a, b \in \mathbb{Q}$ such that

$$|\{1 \leqslant x \leqslant N : f(x) = ax + b\} \gg_K N^c,$$

where $c \gg_K 1$ is some constant depending only on K.

Solution: We may assume that N is large enough depending on K, else the conclusion is trivial. Now let

$$A = \{(x, f(x)) : x \in \{1, \dots, N\}\} \subset \mathbb{Z}^2.$$

Then $|A| = N$, and the hypotheses of the exercise give $E(A) \geqslant K^{-1}N^3$. So, by Balog–Szemeredi–Gowers there is a set $A' \subset A$ with $|A' + A'| \leqslant K^{O(1)}|A'|$ and $|A'| \geqslant K^{-O(1)}N$. By Freiman's theorem, there is a proper GAP P of size $|P| \ll_K |A|$ and rank $d = O_K(1)$, with $A' \subset P$.

If $M_1, \dots, M_d$ are the sizes of the different coordinate directions in the definition of P, with $|P| = M_1M_2 \cdots M_d$, there is some $M_i \geqslant |P|^{1/d} \gg_K N^{1/d}$. Using this direction, we may decompose P as the disjoint union of one-dimensional arithmetic progressions, each with length $\gg_K N^{1/d}$. Explicitly, we get progressions Q of the form

$$Q = \{a + \sum_{\substack{j \leqslant d \\ j \neq i}} n_j v_j + n_i v_i : 0 \leqslant n_i < M_i\}$$

for each fixed tuple $n_j \in [0, M_j)$ for those $j \neq i$.

By an averaging argument, there must be at least one such progression Q for which $|A' \cap Q| \gg_K |Q|$. Suppose that

$$Q = \{(h_1, h_2) + \ell(g_1, g_2) : 0 \leqslant \ell < L\},$$

where $L = |Q| \gg_K N^{1/d}$. So for each $(x, f(x)) \in A' \cap Q$ we have

$$x = h_1 + \ell g_1, \qquad \text{and} \qquad f(x) = h_2 + \ell g_2.$$

Hence

$$f(x) = \frac{g_2}{g_1}x + \frac{g_1h_2 - g_2h_1}{g_1},$$

provided $g_1 \neq 0$. However if $g_1 = 0$ then the first coordinate of all elements in $A' \cap Q$ must be equal to h_1, and hence $|A' \cap Q| \leqslant 1$ as A' is the graph of a function. Since $|Q| > 1$ (since N is large enough), this case doesn't occur.

Hence there are rational numbers $a = g_2/g_1$ and $b = (g_1h_2 - g_2h_1)/g_1$ with $f(x) = ax + b$ for a set of x of size at least $\gg_K N^{1/d}$, as required.

(8) (a) Let $K \geqslant 4$. Show that if $A \subset \mathbb{Z}$ has $|A + A| \leqslant K|A|$ and $|A|$ is sufficiently large depending on K then A contains a non-trivial three-term arithmetic progression.
(b) Explore what quantitative control you can get on how large is 'sufficiently large' using the bounds proved in lectures for Bourgain's theorem on three-term arithmetic progressions and the Freiman–Ruzsa–Sanders inverse theorem.

Solution: There is a moral to the story here, which is, "Learn methods, not just theorems." This is because a direction application of Ruzsa modelling does much better than a simple argument using Freiman's theorem (or even a less simple argument using Freiman's theorem).

If $|A + A| \leqslant K|A|$ then we know there is a proper GAP P with rank $d = O(K(\log K)^{O(1)})$ and size $|P| \ll 2^{-K(\log K)^{O(1)}}|A|$ such that $A \subset P$. Decomposing P as a disjoint union of rank 1 progressions Q_i each with size $|Q_i| \geqslant |P|^{1/d}$, as in our solution to Q7, we have some such rank 1 progression Q with $|A \cap Q| \gg 2^{-K(\log K)^{O(1)}}|Q|$. By Bourgain's theorem on three-term arithmetic progressions, $A \cap Q$ contains a non-trivial three term AP provided $2^{K(\log K)^{O(1)}} \leqslant c(\log |Q|)^{1/2-\delta}$ for some fixed $\delta > 0$ and

small absolute constant $c > 0$. It is therefore sufficient to have

$$2^{K(\log K)^{O(1)}} \leqslant c(d^{-1}\log|A|)^{1/2-\delta}.$$

Rearranging and using $d = O(K(\log K)^{O(1)})$, it suffices to have

$$|A| \geqslant \exp(\exp(O(K(\log K)^{O(1)}))).$$

Here's an immediate improvement, using the following version of Freiman's theorem that follows quickly from the Bogolyubov–Ruzsa lemma but which I don't think was stated in the printed lecture notes:

Theorem 1. *Let $K \geqslant 4$. Suppose $A \subset \mathbb{Z}$ with $|A+A| \leqslant K|A|$. Then there exists a proper GAP P with rank $\ll (\log K)^{O(1)}$ such that $|P \cap A| \gg \exp(-(\log K)^{O(1)})|A|$ and $|P| \ll K^{O(1)}|A|$.*

Note that by passing to a large subset of A we can dramatically improve the rank bound from the version of Freiman's theorem you had in lectures.

Proof. We know from Bogolyubov–Ruzsa that there is a GAP $P \subset 4A-4A$ with rank $\ll (\log K)^{O(1)}$ and size $\gg \exp(-(\log K)^{O(1)})|A|$ such that $P-P$ is a proper GAP. Now let $S \subset A$ be maximal such that $(S-S)\cap(P-P) = \{0\}$. Then $|P||S| = |P+S| \leqslant |5A-4A| \leqslant K^9|A|$, and hence $|S| \leqslant \exp((\log K)^{O(1)})$. The translates $P-P+s$ cover A. Otherwise, there would be some $a \in A$ for which $a \notin P-P+S$, and this implies, defining $S' := S\cup\{a\}$, that $(P-P)\cap(S'-S') = \{0\}$, contradicting the maximality of S. Now choose $s \in S$ such that $|A\cap(P-P+s)|$ is maximised. We must have

$$|A\cap(P-P+s)| \geqslant \frac{|A|}{|S|} \gg \exp(-(\log K)^{O(1)})|A|.$$

This finishes the theorem, taking the GAP $P-P+s$. □

Now we use Theorem 1 to find non-trivial 3APs in A. Indeed, let $A' = A\cap P$. Applying the same argument as above, but to A' instead, A' has a non-trivial 3AP provided

$$\exp((\log K)^{O(1)}) \leqslant c(d^{-1}\log|A'|)^{1/2-\delta}.$$

Rearranging and using the improved bound $d = O((\log K)^{O(1)})$, it suffices to have

$$|A'| \geqslant \exp(\exp((\log K)^{O(1)})),$$

so it suffices to have

$$|A| \geqslant \exp(\exp((\log K)^{O(1)})).$$

But both of these bounds are blown out of the water by a direct application of Ruzsa modelling. Indeed, by Ruzsa modelling we know that there is a subset $A' \subset A$ with $|A'| \geqslant \frac{1}{2}|A|$ such that A' is 2-isomorphic to a set $B \subset \mathbb{Z}/N\mathbb{Z}$ with $|B| \geqslant N/(4K^4)$. Now B contains a non-trivial 3AP provided

$$4K^4 \leqslant c(\log N)^{1/2-\delta}$$

for some small constant c. So it suffices to have

$$4K^4 \leqslant c(\log|B|)^{1/2-\delta},$$

which rearranging gives $|B| \geqslant \exp(K^{O(1)})$. Since 2-isomorphisms preserve 3APs,

$$|A| \geqslant \exp(K^{O(1)})$$

suffices to find 3APs in A.