ADDITIVE COMBINATORICS EXAMPLES SHEET 1: SOLUTIONS

ALED WALKER

These are the 'official' solutions for the first 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 oversight or omission. 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) (a) Use Ruzsa's triangle inequality to show that if $|A+A| \leqslant K|A|$ then
$$|A-A| \leqslant K^2|A|.$$
(b) Use Plünnecke's inequality to show that if $|A-A| \leqslant K|A|$ then
$$|A+A| \leqslant K^2|A|.$$
(c) Show that for any set A
$$|A-A|^{3/4} \leqslant |A+A| \leqslant |A-A|^{4/3}.$$
(d) Show that the exponent of 2 in part (a) is best possible by considering
$$A = \{(x_1,\dots,x_d) \in \mathbb{N}^d : \sum_{i\leqslant d} x_i \leqslant n\}$$
for large n and d.

Solution: (a) The Ruzsa triangle inequality states that for any three finite sets $A, B, C \subset \mathbb{Z}$,
$$|A-C| \leqslant \frac{|A-B||B-C|}{|B|}.$$
Imputting $C = A$ and $B = -A$ one derives
$$|A-A| \leqslant \frac{|A+A||-A-A|}{|-A|} = \frac{|A+A|^2}{|A|} \leqslant K^2|A|$$
as required.

(b) Since $|A-A| \leqslant K|A|$ the Plünnecke inequality (for the set $B := -A$) shows that there is some non-empty $X \subset A$ for which
$$|X-A-A| \leqslant K^2|X|.$$
Therefore
$$|A+A| \leqslant |X-A-A| \leqslant K^2|X| \leqslant K^2|A|$$
as required.

(c) Since $|A-A| \leqslant |A|^2$ we have
$$|A-A|^3 \leqslant |A-A|^2|A|^2 \leqslant \Big(\Big(\frac{|A+A|}{|A|}\Big)^2|A|\Big)^2|A|^2 = |A+A|^4,$$

where the inequalities follow from part (a). So $|A-A|^{3/4} \leqslant |A+A|$ as required. The other inequality follows analogously, using part (b) instead of part (a).

(d) First let us describe the rough idea of this example. One observes that A consists of essentially all the lattice points in the convex region

$$R_A := \{(y_1,\dots,y_d) \in \mathbb{R}^d_{\geqslant 0} : \sum_{i \leqslant d} y_i \leqslant n\}.$$

A simple integration shows that $\mu_d(R_A) = n^d/d!$ (μ_d being d-dimensional Lebesgue measure), and so $|A| \approx n^d/d!$. One has

$$R_A + R_A = \{(y_1,\dots y_d) \in \mathbb{R}^d_{\geqslant 0} : \sum_{i \leqslant d} y_i \leqslant 2n\},$$

and therefore $\mu_d(R_A + R_A) = 2^d n^d/d!$, and so $|A+A|/|A| \approx 2^d =: K$.

We desire to show that $\mu_d(R_A - R_A)/\mu_d(R_A) \gg (2^d)^{2-\delta}$ for any fixed $\delta > 0$. We first claim that $R_A - R_A$ is the set S of all tuples $(y_1,\dots,y_d) \in \mathbb{R}^d$ for which there exist a partition $\{1,\dots,d\} = C_+ \cup C_0 \cup C_-$ into three disjoint (possibly empty) sets such that $y_i < 0$ for $i \in C_-$, $y_i = 0$ for $i \in C_0$, and $y_i > 0$ for $i \in C_+$, and for which $\sum_{i \in C_-} y_i \geqslant -n$ and $\sum_{i \in C_+} y_i \leqslant n$. The inclusion $R_A - R_A \supset S$ is immediate, since one can pick tuples $y := (y_1,\dots,y_d), y' := (y_1',\dots,y_d') \in R_A$ with disjoint support, and then $y - y' \in S$. But the inclusion $R_A - R_A \subset S$ also follows, since for any $y - y' \in R_A - R_A$ the sum over the negative coordinates of $y - y'$ is at least the sum over the coordinates of $-y'$, and therefore is at least $-n$. (The upper bound is analogous). So $R_A - R_A = S$.

To work out $\mu(S)$, we split S according to the sets of coordinates (C_-, C_+). We can assume that $C_0 = \emptyset$ (as these cases contribute zero volume). Then, by the product property of Lebesgue measure,

$$\mu_d(S) = \sum_{(C_-,C_+)} \frac{n^{|C_-|}}{|C_-|!}\frac{n^{|C_+|}}{|C_+|!} = \sum_{k=0}^{d} \binom{d}{k} \frac{n^k}{k!}\frac{n^{d-k}}{(d-k)!} = \frac{n^d}{d!}\sum_{k=0}^{d}\binom{d}{k}^2 = \frac{n^d}{d!}\binom{2d}{d},$$

and by Stirling's approximation one gets

$$\mu_d(S) = (1 + o_{d \to \infty}(1)) \frac{2^{2d} n^d}{d! (\pi d)^{1/2}}.$$

If d is large enough in terms of δ, then

$$(1 + o_{d\to\infty}(1)) \frac{2^{2d}}{(\pi d)^{1/2}} \geqslant (2^d)^{2-\delta}$$

as required.

What remains is to make rigorous the approximation $|A| \approx \mu_d(R_A)$, and similar approximations throughout the argument. Though one could do this using precise combinatorial evaluation of $|A|$ and $|A-A|$ etc., it is perhaps cleaner to use the idea of Gauss to note that, by a lattice point counting argument

$$|A| = \mu_d(R_A) + O((\mu_{d-1}\partial(R_A))) = \mu_d(R_A) + O_d(n^{d-1}),$$

where $\partial(R_A)$ is the boundary of R_A. If $n \to \infty$ much faster than d, this error term doesn't contribute to the main argument.

(2) Recall that if $A \subset \mathbb{Z}$ satisfies $|A+A| = 2|A| - 1$ then A must be an arithmetic progression. In this exercise we will prove Vospoer's theorem, which is the analogous result in $\mathbb{F}_p$.

Let $A, B \subset \mathbb{F}_p$ be sets such that $|A|, |B| \geqslant 2$ and $|A+B| = |A| + |B| - 1 \leqslant p - 2$.

(a) Show that if either A or B is an arithmetic progression then the other must be an arithmetic progression with the same step.

(b) Show that if $A + B$ is an arithmetic progression then A and B must both also be arithmetic progressions of the same step.

(c) Using the previous two parts and induction on $|B|$, prove that in fact A and B are always arithmetic progressions of the same step.

Solution:

Before describing the solution, it will be useful to assign a name to a certain manoeuvre that came up in the proof of the Cauchy–Davenport lemma. Given two sets A and B in an additive group, and some $e \in A - B$, we define the *Dyson e-transform* of the pair by

$$\begin{aligned} A_{(e)} &:= A \cup (B + e) \\ B_{(e)} &:= (A - e) \cap B. \end{aligned}$$

It is easy to check that $A_{(e)} + B_{(e)} \subset A + B$, that $|A_{(e)}| + |B_{(e)}| = |A| + |B|$. Furthermore we have $|B_{(e)}| < |B|$ unless $B + e \subset A$.

(a) Assume that $A = \{a_0 + kd : 0 \leqslant k \leqslant n\}$ for some $n \geqslant 1$. Then by Cauchy–Davenport

$$\begin{aligned} |B| + n &= |A| + |B| - 1 \\ &= |A + B| \\ &= |\{a_0 + kd : 0 \leqslant k \leqslant n - 1\} + \{0, d\} + B| \\ &\geqslant |B + \{0, d\}| + n - 1, \end{aligned}$$

and so $|B + \{0, d\}| \leqslant |B| + 1$. But Cauchy–Davenport gives the reverse inequality, so $|B + \{0, d\}| = |B| + 1$. This means that B and $B + d$ differ by at most one element, which implies that B is also a progression with common difference d.

(b) Suppose that $A + B$ is an arithmetic progression with step d. Let

$$C := -(\mathbb{F}_p \setminus (A + B)).$$

Then C is also an arithmetic progression with step d (as p is prime) and

$$|C| = p - |A + B| = p + 1 - |A| - |B| \geqslant 2.$$

Furthermore $C + B \subset -(\mathbb{F}_p \setminus A)$, since if any element $-a$ of $-A$ were contained in $C + B$ then C would intersect $-a - B \subset -(A + B)$, a contradiction. Therefore $|C + B| \leqslant p - |A| = |C| + |B| - 1$, and hence by Cauchy–Davenport $|C + B| = |C| + |B| - 1$. Since C was an arithmetic progression of length at least 2, one sees from part (a) that B is as well, with the same step d. Similarly for A.

(c) We induct on the size of B. If $|B| = 2$ then B is an arithmetic progression already and the theorem has already been proved, so suppose that $|B| > 2$ and that the claim has already been proven for smaller B. Suppose first that we can find an element $e \in A - B$ such that the e-transform $B_{(e)}$ of B has size $1 < |B_{(e)}| < |B|$.

Then by Cauchy–Davenport

$$|A_{(e)}| + |B_{(e)}| - 1 \leqslant |A_{(e)} + B_{(e)}| \leqslant |A + B| = |A| + |B| - 1 = |A_{(e)}| + |B_{(e)}| - 1,$$

so

$$|A_{(e)} + B_{(e)}| = |A_{(e)}| + |B_{(e)}| - 1.$$

By the induction hypothesis we see that $A_{(e)}$ and $B_{(e)}$ are arithmetic progressions with the same step d, and so $A + B = A_{(e)} + B_{(e)}$ is also an arithmetic progression, and so the theorem follows from part (b).

The only remaining case is if we have $|B_{(e)}| = 1$ or $|B_{(e)}| = |B|$ for all $e \in A - B$. But if $E \subset A - B$ denotes all the $e \in A - B$ such that $|B_{(e)}| = |B|$, then $B + E \subset A$. Hence $|E| \leqslant |A| - |B| + 1$ by Cauchy–Davenport.

Since $|A - B| \geqslant |A| + |B| - 1$ by Cauchy-Davenport, we thus see that $|B_{(e)}| = 1$ for at least $2|B| - 2$ values of e. Since $B_{(e)}$ is a singleton subset of B in this case, we conclude from the pigeonhole principle that there exists $e, e' \in A - B$ and $b \in B$ such that $B_{(e)} = B_{(e')} = \{b\}$. Since $|A + B| = |A| + |B| - 1$ by hypothesis, we conclude that

$$A + B = A_{(e)} + b = A_{(e')} + b$$

and hence

$$A \cup (B + e) = A \cup (B + e').$$

Since A intersects $B + e$ only in $b + e$, and A intersects $B + e'$ only in $b + e'$, we thus see that $B + e$ and $B + e'$ differ by at most one element. But this forces B to be a progression (of step $e' - e$), and the theorem follows.

(3) Show that if $|A + B| \leqslant K|A|$ then for any $\varepsilon > 0$ there is $X \subset A$ such that $|X| \geqslant (1 - \varepsilon)|A|$ and

$$|X + mB| \leqslant \varepsilon^{-k} K^m |X|.$$

Solution: Suppose for contradiction that there is no such set X. Now let $X_1 \subset A$ be a maximal subset for which $|X + mB| \leqslant \varepsilon^{-m} K^m |X|$ for all $m \geqslant 1$. Such a set X_1 must exist, since by Plünnecke there exists some $X \subset A$ with $|X + mB| \leqslant K^m |X|$. By our assumption, $|X_1| \leqslant (1 - \varepsilon)|A|$ then we are done.

Now let $A_2 = A \setminus X_1$. Then

$$|A_2 + B| \leqslant |A + B| \leqslant K|A| \leqslant K\varepsilon^{-1}|A_2|,$$

so by Plünnecke again there exists $X_2 \subset A_2$ with

$$|X_2 + mB| \leqslant (K\varepsilon^{-1})^m |X_2|.$$

Then

$$|(X_1 \cup X_2) + mB| \leqslant |X_1 + mB| + |X_2 + mB| \leqslant (K\varepsilon^{-1})^m (|X_1| + |X_2|) = (K\varepsilon^{-1})^m (|X_1 \cup X_2|)$$

since X_1 and X_2 are disjoint. But X_1 is a strict subset of $(X_1 \cup X_2)$, contradicting the assumed maximality of X_1.

(4) (a) Show that if $|A + B| \leqslant K|A|$ then there exists $A' \subset A$ (with $A' \neq A$) such that

$$|A + B + B| \leqslant |A' + B + B| + K^2(|A| - |A'|).$$

(b) Let B be a fixed set and $M \geqslant 1$ also be fixed. SHow that for any $N \geqslant M/|B + B|^{1/2}$, for all A such that $|A| \leqslant N$ and $|A + B| \leqslant M$ we have

$$|A + B + B| \leqslant 3M|B + B|^{1/2} - \frac{M^2}{N}.$$

(c) Deduce that, for any sets A and B, if $|A + B| \leqslant K|A|$ then

$$|A + B + B| \ll K^2 |A|^{3/2}.$$

(d) Show that the previous bound is best possible, in that there exist arbitrarily large A and B such with $|A+B| \ll |A|$ and $|A+B+B| \gg |A|^{3/2}$.

Solution:

(a). Plünnecke's inequality gives us a non-empty $X \subset A$ for which

$$|X+B+B| \leqslant K^2|X|.$$

Then letting $A' := A \setminus X$, we get $A+B+B = (A'+B+B) \cup (X+B+B)$, and so

$$|A+B+B| \leqslant |A'+B+B|+|X+B+B| \leqslant |A'+B+B|+K^2|X| = |A'+B+B|+K^2(|A|-|A'|)$$

as required.

(b). We will prove this statement by induction on $|A|$. For notational simplicity we write $P := |B+B|^{1/2}$. If $|A| \leqslant M/P$ then the claim follows easily, since

$$|A+B+B| \leqslant |A||B+B| \leqslant \frac{M}{P}P^2 = MP \leqslant 3MP - MP \leqslant 3M|B+B|^{1/2} - \frac{M^2}{N}$$

since $N \geqslant M/P$ by assumption. So w.l.o.g. we may assume that $|A| > M/P$. Then, by part (a), we have some $A' \subset A$ with $|A'| < |A|$ and

$$|A+B+B| \leqslant |A'+B+B| + \Big(\frac{M}{|A|}\Big)^2(|A|-|A'|).$$

If $|A'| \leqslant MP^{-1}$ then we have already shown that $|A'+B+B| \leqslant MP$. So

$$|A+B+B| \leqslant MP + \frac{M^2}{|A|^2}(|A|-|A'|) \leqslant MP + \frac{M^2}{|A|} \leqslant 2MP = 3MP - \frac{M^2}{M/P} \leqslant 3MP - \frac{M^2}{N}$$

as required. If alternatively we have $|A'| \geqslant MP^{-1}$ then by the induction hypothesis we obtain

$$|A+B+B| \leqslant 3MP - \frac{M^2}{|A'|} + \frac{M^2}{|A|^2}(|A|-|A'|) \leqslant 3MP - \frac{M^2}{|A|} \leqslant 3MP - \frac{M^2}{N}$$

as required. So we are done in all cases.

(c). We look to apply the previous lemma with $M = K|A|$. If $|B+B|^{1/2} \leqslant K$ then $\frac{M}{|B+B|^{1/2}} \geqslant |A|$ and so we may substitute $N = \frac{M}{|B+B|^{1/2}}$ in part (b) to get

$$|A+B+B| \leqslant 3M|B+B|^{1/2} - \frac{M^2}{M/|B+B|^{1/2}} = 2M|B+B|^{1/2} \ll K^2|A| \ll K^2|A|^{3/2}.$$

If on the other hand $|B+B|^{1/2} > K$ then we can take $N = |A|$ in part (b) to get

$$|A+B+B| \leqslant 3M|B+B|^{1/2} - \frac{M^2}{|A|} < 3M|B+B|^{1/2} \leqslant 3K|A|(K^2|A|)^{1/2} \ll K^2|A|^{3/2},$$

where the intermediate step followed by Plünnecke.

(d). Let $A = \{(x,y,z) \in \mathbb{Z}^3 : 1 \leqslant x,y \leqslant N\} \cup \{(0,0,z) \in \mathbb{Z}^3 : 1 \leqslant z \leqslant N\}$, and $B = \{(x,0,0) \in \mathbb{Z}^3 : 1 \leqslant x \leqslant N\} \cup \{(0,y,0) \in \mathbb{Z}^3 : 1 \leqslant y \leqslant N\}$. Then $A+B$ is the union of 5 generalised arithmetic progressions of dimension 2 and size $(1+o(1))N^2$, whereas $A+B+B$ contains the cube $\{(x,y,z) \in \mathbb{Z}^3 : 1 \leqslant x,y,z \leqslant N\}$. So $|A+B| \ll N^2 \ll |A|$, but $|A+B+B| \gg N^3 \gg |A|^{3/2}$.

(5) Show that the following are equivalent 'up to polynomial losses', in that if one property holds with parameter K then the others hold with parameters $K^{O(1)}$:

(a) $|A+A| \leqslant K|A|$,

(b) there exists B such that $|A+B| \leqslant K|A|^{1/2}|B|^{1/2}$,
(c) there exists a symmetric set H containing the origin such that $H+H \subset H+X$ for some $|X| \leqslant K$, and $A \subset x+H$ for some x, and $|A| \geqslant K^{-1}|H|$.

Solution: It is obvious that (a) $\Rightarrow$ (b), by taking $B = A$. Furthermore the implication (c) $\Rightarrow$ (a) is straightforward, since if $A \subset x+H$ for such an H then

$$|A+A| \leqslant |H+H| \leqslant |H+X| \leqslant |X||H| \leqslant K|H| \leqslant K^2|A|.$$

It remains to show that (b) $\Rightarrow$ (c). To this end note that

$$|A| \leqslant |A+B| \leqslant K|A|^{1/2}|B|^{1/2},$$

and so $|A| \leqslant K^2|B|$. Hence $|A+B| \leqslant K^2|B|$, and, arguing symmetrically, $|A+B| \leqslant K^2|A|$.

By Ruzsa's covering lemma, there is a set X with $|X| \leqslant K^{O(1)}$ for which $A \subset X+B-B$. By Plünnecke we also have $|(B-B)+(B-B)+B| \leqslant K^{O(1)}|B|$, and so by the Ruzsa covering lemma again there is also a set Y with $|Y| \leqslant K^{O(1)}$ and $(B-B)+(B-B) \subset Y+B-B$. Picking $H = X-X+B-B$, we therefore see that H satisfied the conditions for part (c).

(6) Show that if $|A+A-A-A| < 2|A|$ then $A-A$ is a group.

Solution: In fact we will prove the same conclusion under the weaker hypothesis $|A+A-A| < 2|A|$.

It suffices to show that $A+A-A-A \subset A-A$. To this end, let $a_1, a_2, a_1', a_2' \in A$ and consider a_1-a_2 and $a_1'-a_2'$. Since the sets a_1-a_2-A and $a_1'-a_2'-A$ are both subsets of $A-A-A$, by the size constraints they must have non-empty intersection. Therefore there are some $a_3, a_3' \in A$ and some z for which

$$\begin{aligned} a_1 - a_2 - a_3 &= z \\ a_1' - a_2' - a_3' &= z. \end{aligned}$$

Rearranging, we obtain

$$(a_1 - a_2) - (a_1' - a_2') = a_3 - a_3'$$

as required.

(7) Adapt the proof of the Balog–Szemerédi–Gowers lemma to show to your satisfaction that the following asymmetric version holds: Let $E(A,B)$ count the number of solutions to $a_1+b_1 = a_2+b_2$ with $a_1, a_2 \in A$ and $b_1, b_2 \in B$. Show that if $E(A,B) \geqslant K^{-1}|A|^{3/2}|B|^{3/2}$ then there exist $A' \subset A$ and $B' \subset B$ such that
(a) $|A'| \gg K^{-O(1)}|A|$,
(b) $|B'| \gg K^{-O(1)}|B|$, and
(c) $|A'-B'| \ll K^{O(1)}|A|^{1/2}|B|^{1/2}$.

NB: This is slightly different to the printed question, which asked for K^{-1} factors in the first two expressions, but this proof is a bit cleaner.

Solution: Let $c > 0$ be a small constant to be chosen later, and without loss of generality let us assume that $|B| \leqslant |A|$. Observe however that

$$|A||B|^2 \geqslant E(A,B) \geqslant K^{-1}|A|^{3/2}|B|^{3/2},$$

so we have $|B| \geqslant K^{-2}|A|$.

Let $X := A \cap (B+s)$ and $Y := (A-s) \cap B$, where s is chosen from $A - B$ at random with probability $1_A \circ 1_B(s)|A|^{-1}|B|^{-1}$. Note that $X = Y + s$, so in particular $|X| = |Y|$. Then by linearity of expectation we have

$$\begin{aligned}\mathbb{E}\,|X| &= \frac{1}{|A||B|}\sum_{a\in A}\sum_{s} 1_A \circ 1_B(s)1_B(a-s)\\ &= \frac{1}{|A||B|}\sum_{s}(1_A \circ 1_B)(s)^2\\ &= \frac{E(A,B)}{|A||B|}.\end{aligned}$$

Now for any set $G \subset A \times B$,

$$\begin{aligned}\mathbb{E}(|(X\times Y)\cap G|) &= \sum_{(a,b)\in G}\mathbb{P}((a,b)\in X\times Y)\\ &= \sum_{(a,b)\in G}\mathbb{P}(a\in B+s \text{ and } b\in A-s)\\ &= \sum_{(a,b)\in G}\mathbb{P}(a-s\in B \text{ and } b+s\in A)\\ &= \sum_{(a,b)\in G}\sum_{s}\frac{1_A\circ 1_B(s)}{|A||B|}1_B(a-s)1_A(b+s)\\ &\leqslant \frac{1}{|A|}\sum_{(a,b)\in G}1_A * 1_B(a+b).\end{aligned}$$

Therefore, if G is defined to be the set of those pairs $(a,b) \in A \times B$ for which

$$1_A * 1_B(a+b) \leqslant \frac{c^2E(A,B)^2}{100|A|^2|B|^3},$$

we have (by the trivial bound $|G| \leqslant |A||B|$)

$$\mathbb{E}(|(X\times Y)\cap G|) \leqslant \frac{c^2E(A,B)^2}{100|A|^2|B|^2}.$$

So, by linearity of expectation and Cauchy–Schwarz

$$\mathbb{E}(|X|^2 - c^{-1}|X\times Y\cap G|) \geqslant \mathbb{E}(|X|)^2 - c^{-1}\,\mathbb{E}(|(X\times Y)\cap G|) \geqslant \frac{1}{2}\frac{E(A,B)^2}{|A|^2|B|^2}.$$

From this we conclude that there must exist some $s \in A - B$ for which both

$$|X| = |Y| \gg \frac{E(A,B)}{|A||B|} \gg K^{-1}|A|^{1/2}|B|^{1/2} \gg K^{-O(1)}|A|,$$

and

$$|(X\times Y)\cap G| \leqslant c|X||Y|.$$

In other words, for all but a proportion c of the pairs $(x,y) \in X \times Y$, we have

$$1_A * 1_B(x+y) \geqslant \frac{c^2E(A,B)^2}{100|A|^2|B|^3} \geqslant \frac{c^2|A|}{100K^2}.$$

The rest of the argument is very similar to the lectured material, although one needs to tweak the graph theory ever so slightly. Indeed, constructing a bipartite graph on the vertex set $X \times Y$ where (x, y) is an edge if $1_A * 1_B(x+y) \geqslant \frac{c^2|A|}{100^2K}$, the number of edges is at least $0.99|X||Y|$ (say), if c is small enough. Letting

$$A' = \{x \in X : \deg(x) \geqslant 0.49|Y|\}$$

and

$$B' = \{y \in Y : \deg(y) \geqslant 0.49|X|\},$$

we observe that $|A'| \geqslant 0.49|X|$ and $|B'| \geqslant 0.49|Y|$, say. Indeed, if $|A'| < 0.49|X|$ then the number of edges in the graph would be at most $0.49|X||Y|$ (the contribution from those vertices in X with degree at most $0.49|Y|$) plus $0.49|X||Y|$ (the contribution from those vertices in A'), which would mean that the total number of edges is less than $0.98|X||Y|$, a contradiction. The same argument holds for B'.

We claim that for each $(a, b) \in A' \times B'$, there are $\gg K^{-O(1)}|A|^2$ paths of length three in the above graph, starting at a and finishing at b. Indeed, the number of edges between $\Gamma(a)$ and $\Gamma(b)$ (the neighbourhoods of a and b) is at least

$$|\Gamma(a)||\Gamma(b)| - 0.01|X||Y| \geqslant 0.48^2|X||Y| - 0.01|X||Y| \gg |X||Y| \gg K^{-O(1)}|A|^2$$

as claimed.

We now claim that all of the above observations imply that $|A' + B'| \ll K^{O(1)}|A|$. Indeed, for each $x \in A' + B'$ fix an expression $a_x + b_x = x$. We know that there are $\gg K^{-O(1)}|A|^2$ choices $(b_1, a_1) \in B \times A$ for which (a_x, b_1), (b_1, a_1) and (a_1, b_x) are all edges of the graph. Writing

$$x = a_x + b_x = a_x + b_1 - b_1 - a_1 + a_1 + b_x,$$

we generate a further $K^{-O(1)}|A|^3$ sextuples $(c_1, d_1, c_2, d_2, c_3, d_3)$ for which

$$a_x + b_1 = c_1 + d_1,\ b_1 + a_1 = c_2 + d_2,\ c_3 + d_3 = a_1 + b_x.$$

Summing over all (b_1, a_1) this leaves us with $K^{-O(1)}|A|^5$ sextuples, and they are all distinct, since we can recover x by

$$c_1 + d_1 - c_2 - d_2 + c_3 + d_3 = x,$$

and therefore recover the fixed pair (a_x, b_x) and thus (b_1, a_1) as well by the relations $a_x + b_1 = c_1 + d_1$ etc.

Summing over all x, the total number of sextuples generated must be at most $|A|^3|B|^3$, which is at most $|A|^6$. Therefore

$$|A' + B'|K^{-O(1)}|A|^5 \ll |A|^6,$$

which yields

$$|A' + B'| \ll K^{O(1)}|A| \ll K^{O(1)}|A|^{1/2}|B|^{1/2}.$$

This is nearly what we required, excepting for the fact that that we have $A' + B'$ instead of $A' - B'$. However, by running the argument with $-B$ in place of B we may also prove the version with a difference set.

(8) (a) Prove the following generalisation of Plünnecke's inequality: if we have h sets $B_1, \dots, B_h$ such that $|A + B_i| \leqslant K_i|A|$ for $1 \leqslant i \leqslant h$ then there is an $X \subset A$ such that

$$|X + B_1 + \cdots + B_h| \ll_h K_1 \cdots K_h|X|,$$

and in particular

$$|B_1 + \cdots + B_h| \ll_h K_1 \cdots K_h|A|.$$

(b) By considering what happens if we replace A by $A \times \cdots \times A$ and B_i by $B_i \times \cdots B_i$, show that the second conclusion can be upgraded to

$$|B_1 + \cdots + B_h| \leqslant K_1 \cdots K_h|A|.$$

Solution: (a): Without loss of generality we may assume that the K_i's are integers. Take auxiliary sets $T_1, \dots, T_h \subset G$ such that $|T_i| = n_i$ (which will be specified later) such that all the sums

$$y + t_1 + \cdots + t_h,\ y \in A + B_1 + \cdots + B_h,\ t_i \in T_i$$

are distinct. (This may be impossible in a finite group, but in that case embed the problem into a infinite group first.) Now apply Plünnecke's theorem with

$$B := \cup_i (B_i + T_i).$$

Observe that

$$|A + B| \leqslant \sum_i |A + B_i + T_i| \leqslant \sum_i |A + B_i||T_i| \leqslant |A| \sum_i K_i n_i,$$

so we thus obtain a set $X \subset A$ for which

$$|X + hB| \leqslant |X| \Big(\sum_i K_i n_i \Big)^h.$$

On the other hand $X + hB \supset X + B_1 + \cdots + B_h + T_1 + \cdots + T_h$, and consequently we have

$$|X + hB| \geqslant |X + B_1 + \cdots + B_h| n_1 \dots n_k$$

by the disjointness property of the T_i's. Putting these inequalities together gives

$$|X + B_1 + \cdots + B_h| \leqslant \Big(\sum_i n_i K_i \Big)^h (n_1 \dots n_h)^{-1} |X|.$$

Choosing $n_i = n/K_i$ for some n which is a multiple of all the K_i's, we obtain

$$|X + B_1 + \cdots + B_h| \leqslant h^h K_1 \dots K_h |X|$$

as required.

(b): Letting $B_i^{\otimes m}$ denote $B_i \times \cdots \times B_i$ m times, we have

$$|A^{\otimes m} + B_i^{\otimes m}| = |(A + B_i)^{\otimes m}| = |A + B_i|^m \leqslant K_i^m |A|.$$

So by part (a), there is an absolute constant C_h for which

$$|B_1 + \cdots + B_h|^m = |B_1^{\otimes m} + \cdots + B_h^{\otimes m}| \leqslant C_h K_1^m \dots K_h^m |A^{\otimes m}| = C_h K_1^m \dots K_h^m |A|^m.$$

Taking m^{th} roots we get

$$|B_1 + \cdots + B_h| \leqslant C_h^{1/m} K_1 \dots K_h |A|.$$

Sending $m \to \infty$ yields the result.

(9) This exercise shows how to improve the exponent in the Balog–Szemerédi–Gowers lemma. This proof is due to Scheon (2014) and the exponent of K^3 here remains the best known – if you can do any better on the exponent by any method, that would be big news!

Fix some set A such that $E(A) \geqslant K^{-1}|A|^3$.

(a) Let $G \subset A^2$ be the set of pairs (a, b) such that $1_A \circ 1_A(a - b) < cE(A)/|A|^2$. Show that there exists some $\frac{1}{4K} \leqslant \lambda < 1$ such that if

$$S = \{x : \lambda|A| < 1_A \circ 1_A(x) \leqslant 2\lambda|A|\}$$

then

$$\sum_{(a,b)\in G} |(A - a) \cap (A - b) \cap S| \leqslant 2c\lambda^2 |S||A|^2.$$

(b) By considering X of the form $A\cap(A+s)$, where s is chosen uniformly at random from S, show that there is $X\subset A$ of size $|X|\gg K^{-1}|A|$ such that for all but at most $c|X|^2$ many pairs $(a,b)\in X^2$ we have
$$1_A\circ 1_A(a-b)\gg cK^{-1}|A|.$$

(c) Deduce that there exists $A'\subset A$ with $|A'|\gg K^{-1}|A|$ and $|A'-A'|\ll K^3|A|$.

Solution:

(a): Let I be the natural number for which $2^I\geqslant(2K)^{-1}$, and for $1\leqslant i\leqslant I$ let
$$S_i:=\{x:2^{-i}|A|<1_A\circ 1_A(x)\leqslant 2^{-i+1}|A|\}.$$

Then on the one hand
$$\begin{aligned}\sum_{i\leqslant I}\sum_{(a,b)\in G}|(A-a)\cap(A-b)\cap S_i| &= \sum_{(a,b)\in G}\sum_{i\leqslant I}\sum_{s\in S_i}1_A(s+a)1_A(s+b)\\ &\leqslant \sum_{(a,b)\in G}1_A\circ 1_A(a-b)\\ &\leqslant cE(A),\end{aligned}$$

by the trivial bound $|G|\leqslant|A|^2$. On the other hand
$$\begin{aligned}2c\sum_{i\leqslant I}(2^{-i}|A|)^2|S_i| &\geqslant 2c\sum_{i\leqslant I}\sum_{x\in A-A}(1_A\circ 1_A(x))^2 1_{S_i}(x)\\ &\geqslant 2c\sum_{\substack{x\in A-A\\ 1_A\circ 1_A(x)\geqslant\frac{|A|}{2K}}}(1_A\circ 1_A(x))^2\\ &\geqslant cE(A),\end{aligned}$$

since otherwise we would have
$$\begin{aligned}E(A) &= \sum_{\substack{x\in A-A\\ 1_A\circ 1_A(x)\geqslant\frac{|A|}{2K}}}(1_A\circ 1_A(x))^2+\sum_{\substack{x\in A-A\\ 1_A\circ 1_A(x)<\frac{|A|}{2K}}}(1_A\circ 1_A(x))^2\\ &< \frac{E(A)}{2}+\frac{|A|}{2K}\sum_{x\in A-A}1_A\circ 1_A(x)\\ &= \frac{E(A)}{2}+\frac{|A|^3}{2K},\end{aligned}$$

thus implying that $E(A)<K^{-1}|A|^3$, contrary to assumption. This implies that
$$\sum_{i\leqslant I}\sum_{(a,b)\in G}|(A-a)\cap(A-b)\cap S_i|\leqslant\sum_{i\leqslant I}2c(2^{-i}|A|)^2|S_i|,$$

and so there is some $i\leqslant I$ for which
$$\sum_{(a,b)\in G}|(A-a)\cap(A-b)\cap S_i|\leqslant 2c(2^{-i}|A|)^2|S_i|.$$

Picking $\lambda=2^{-i}$, and noting that $1>\lambda>(4K)^{-1}$, we obtain the claim.

(b). Let $X=A\cap(A+s)$, with s chosen uniformly at random from S. We have
$$\mathbb{E}\,|X|=\frac{1}{|S|}\sum_{s\in S}1_A\circ 1_A(s)\geqslant\lambda|A|\gg K^{-1}|A|.$$

Letting G be the subset of pairs from part (a), we have that

$$\begin{aligned}\mathbb{E}(|(X \times X) \cap G|) &= \sum_{(a,b)\in G} \frac{1}{|S|} \sum_{s\in S} 1_A(s+a)1_A(s+b)\\ &= \frac{1}{|S|} \sum_{(a,b)\in G} |(A-a)\cap(A-b)\cap S|\\ &\leqslant 2c\lambda^2|A|^2.\end{aligned}$$

Therefore by Cauchy–Schwarz and linearity of expectation,

$$\begin{aligned}\mathbb{E}(|X \times X| - \frac{1}{100c}|(X \times X)\cap G|) &\geqslant \mathbb{E}(|X|)^2 - \frac{1}{100c}\mathbb{E}\,|(X\times X)\cap G|\\ &\geqslant \lambda^2|A|^2 - \frac{1}{50}\lambda^2|A|^2\\ &\gg \lambda^2|A|^2\\ &\gg K^{-2}|A|^2\end{aligned}$$

Therefore there exists some choice of $s \in S$ for which $|X| \gg K^{-1}|A|$ and $\leqslant 100c|X|^2$ pairs $(a,b) \in X^2$ satisfy $(a,b) \in G$. By replacing c with $100c$, we conclude that for all but at most $c|X|^2$ many pairs $(a,b) \in X^2$ we have

$$1_A \circ 1_A(a-b) \gg cK^{-1}|A|,$$

as required.

(c). The conclusion is exactly as in the lectured proof of BSG, so we only sketch the details here. We construct a bipartite graph on vertex set $X \times X$ with (a,b) being an edge if $1_A \circ 1_A(a-b) \gg cK^{-1}|A|$ (with the same implied constant as in the conclusion of part (b)). This graph has at least $(1-c)|X|^2$ edges, and so, assuming that $c < 1/100$ say, letting

$$A' := \{x \in X : \deg(x) \geqslant \frac{3}{4}|X|\}$$

we get $|A'| \gg |X|$.

Now, for each $(a_1, a_2) \in A' \times A'$, there are $\gg K^{-1}|A|$ elements $a \in X$ for which (a_1, a) and (a, a_2) are edges of the graph (since $\Gamma(a_1) \cap \Gamma(a_2)$ is suitably large). [A path of length 2, whereas in Q7 we used paths of length 3.]

Now, for each $x \in A' - A'$ we fix some $(a_x, b_x) \in A' \times A'$ with $a_x - b_x$. For each a such that (a_x, a) and (a, b_x) are edges of the graph, we may associate at least $(cK^{-1}|A|)^2$ quadruples $(y_1, y_2, z_1, z_2) \in A^4$ such that $y_1 - y_2 = a_x - a$ and $z_1 - z_2 = a - b_x$. Since we can recover x and a from the quadruple via

$$y_1 - y_2 + z_1 - z_2 = x,$$

summing over choices of a shows that each $x \in A' - A'$ yields $\gg c^2K^{-3}|A|^3$ quadruples, and these quadruples are disjoint for each x.

Therefore, summing over x, we get

$$|A' - A'|c^2K^{-3}|A|^3 \ll |A|^4$$

. Picking $c = 1/100$ and rearranging we get $|A' - A'| \ll K^3|A|$ as required.