ACTA ARITHMETICA
167.4 (2015)

The cardinality of sumsets: different summands

by

BRENDAN MURPHY (Rochester, NY),
EYVINDUR ARI PALSSON (Williamstown, MA) and
GIORGIS PETRIDIS (Rochester, NY)

1. Introduction. Given (non-empty) finite sets $A, B_1, \ldots, B_h$ in a commutative group, their *sumset* (also referred to as their *Minkowski sum*) is

$$A + B_1 + \cdots + B_h = \{a + b_1 + \cdots + b_h : a \in A,\ b_i \in B_i \text{ for } 1 \le i \le h\}.$$

We obtain an upper bound on the cardinality of $A + B_1 + \cdots + B_h$ in terms of h and the cardinalities of A and $A + B_1, \ldots, A + B_h$. Note that the question becomes trivial unless some constraints are put on the sets as $|A + B_1 + \cdots + B_h| \le |A|\,|B_1| \ldots |B_h|$; and the bound is attained when $A, B_1, \ldots, B_h$ are sets of distinct generators of a free commutative group.

The best known upper bound is as follows.

THEOREM 1.1. *Let h and m be positive integers and $\alpha_1, \ldots, \alpha_h$ be positive real numbers. Suppose that $A, B_1, \ldots, B_h$ are finite sets in a commutative group that satisfy $|A| = m$ and $|A + B_i| \le \alpha_i m$ for all $1 \le i \le h$. Then*

$$|A + B_1 + \cdots + B_h| \le \alpha_1 \ldots \alpha_h m^{2-1/h}.$$

Theorem 1.1 can be proved by different methods. It can be deduced from the work of Ruzsa in [10, 11]. It also follows by combining an inequality of Balister and Bollobás in [1] with an inequality of Ruzsa [9]. Madiman, Marcus and Tetali have given a different proof of the inequality of Balister and Bollobás in [5]. We discuss the various proofs in more detail in Section 2. It is worth pointing out here that the methods used by the three groups of authors are different: Ruzsa relied on graph theory; Bollobás and Balister on projections; and Madiman, Marcus and Tetali on entropy.

2010 *Mathematics Subject Classification*: Primary 11P99; Secondary 11B30.
Key words and phrases: sumsets, Plünnecke–Ruzsa inequality, commutative graphs.

DOI: 10.4064/aa167-4-4

The upper bound in Theorem 1.1 has the correct dependence on α and m. The following example (a modification of similar examples given by Ruzsa in [10, 11]) demonstrates this.

Example 1.2. Let h be a positive integer. There exist infinitely many $(\alpha_1, \dots, \alpha_h) \in (\mathbb{Q}^+)^h$ with the following property. For each such h-tuple $(\alpha_1, \dots, \alpha_h)$ there exist infinitely many m and sets $A, B_1, \dots, B_h$ in a commutative group with $|A| = m$, $|A + B_i| \le (1 + o(1))\alpha_i m$ and

$$|A + B_1 + \dots + B_h| \ge (1 + o(1))\frac{(1 - 1/h)^{h-1}}{h}\alpha_1 \dots \alpha_h m^{2-1/h}.$$

The $o(1)$ term is $o_{m\to\infty}(1)$.

We show that the sets in Example 1.2 are extremal to this problem by proving a matching upper bound and so settle the question of bounding from above the cardinality of higher sumsets in commutative groups.

Theorem 1.3. *Let h be a positive integer, $\alpha_1, \dots, \alpha_h$ be positive real numbers and m an arbitrarily large integer. Suppose that $A, B_1, \dots, B_h$ are finite sets in a commutative group that satisfy $|A| = m$ and $|A + B_i| \le \alpha_i m$ for all $1 \le i \le h$. Then*

$$\begin{aligned}|A + B_1 + \dots + B_h| &\le \frac{(1 - 1/h)^{h-1}}{h}\alpha_1 \dots \alpha_h (m^{2-1/h} + O(m^{2-2/h})) \\ &= (1 + o(1))\frac{(1 - 1/h)^{h-1}}{h}\alpha_1 \dots \alpha_h m^{2-1/h}.\end{aligned}$$

The $o(1)$ term is $o_{m\to\infty}(1)$.

Note. For large h the main term is roughly $\frac{e^{-1}}{h}\alpha_1 \dots \alpha_h m^{2-1/h}$.

The proof is a refinement of Ruzsa's graph-theoretic approach. The upper bound in Theorem 1.3 is submultiplicative with respect to direct products. In other words if one replaces A by, say, its Cartesian product $A \times A = \{(a, a') : a, a' \in A\}$ and the B_i by their Cartesian products $B_i \times B_i$, then (after standard calculations of the form $|(A\times A)+(B\times B)| = |(A+B)\times(A+B)| = |A + B|^2$) one obtains

$$\frac{\alpha_1 \dots \alpha_h}{\sqrt{h}}|A|^{2-1/h},$$

which is weaker than what the theorem gives. This particular feature of the upper bound makes using one of the key ingredients in Ruzsa's method, the product trick, more delicate. From a technical point of view this is the greatest difficulty that must be overcome.

The special case when $B_1 = \dots = B_h$ and $\alpha_1 = \dots = \alpha_h = \alpha$ was considered in [7]. The sumset $A + B_1 + \dots + B_h$ in this case is abbreviated to $A + hB$. The upper bound obtained there is slightly stronger:

$$|A + hB| \leq (1 + o(1))\frac{C}{h^2}\alpha^h m^{2-1/h} \tag{1.1}$$

for an absolute constant $C > 0$. The extra factor of h in the denominator can be accounted for by the fact that while $|S_1 + \cdots + S_h| \leq |S_1| \ldots |S_h|$ holds for general sets S_i, when the same set S is added to itself one has the stronger inequality $|S + \cdots + S| \leq \binom{|S|+h-1}{h}$. Inequality (1.1) probably does not have the correct dependence on h as the largest value of $|A + hB|$ in examples is of the order $h^{-h-1}\alpha^h m^{2-1/h}$. It would be of interest to bridge that gap.

The proof of Theorem 1.3 is similar to that of inequality (1.1). There are nonetheless technical differences. Roughly speaking, we combine ideas from the proof of (1.1) with a strategy used repeatedly in the literature (for example in [3, 12]) to prove a generalisation of the aforementioned result of Ruzsa. We could not find a result general enough for our purposes in the literature and so give a detailed proof in Section 5.

The paper is organised as follows. In Section 2 we discuss the different proofs of Theorem 1.1. The proof of Theorem 1.3 is done in Section 3. Example 1.2 is described in Section 4. In Section 5 the graph-theoretic framework of the proof is developed.

2. Proof of Theorem 1.1. The assertion follows by combining an inequality of Balister and Bollobás with an inequality of Ruzsa.

Theorem 2.1 (Balister–Bollobás, [1]). *Let h and m be positive integers and $\alpha_1, \ldots, \alpha_h$ be positive real numbers. Suppose that $A, B_1, \ldots, B_h$ are finite sets in a commutative group that satisfy $|A| = m$ and $|A + B_i| \leq \alpha_i m$ for all $1 \leq i \leq h$. Then for any subset $C \subseteq B_1 + \cdots + B_h$,*

$$|A + C| \leq (\alpha_1 \ldots \alpha_h)^{1/h} m|C|^{1-1/h}.$$

The proof given by Balister and Bollobás is short and elegant. It combines an idea of Gyarmati, Matolcsi and Ruzsa in [4] with the Box Theorem in [2]. Madiman, Marcus and Tetali gave a somewhat different proof based on entropy [5]. The theorem can also be proved by methods developed by Ruzsa (for example in [10, 11]).

To deduce Theorem 1.1 one naturally sets $C = B_1 + \cdots + B_h$. This gives

$$|A + B_1 + \cdots + B_h| \leq (\alpha_1 \ldots \alpha_h)^{1/h} m|B_1 + \cdots + B_h|^{1-1/h}. \tag{2.1}$$

We are left with bounding $|B_1 + \cdots + B_h|$ in terms of m and the α_i. Ruzsa achieved this by modifying a graph-theoretic method of Plünnecke in [8], a variant of which we describe in Section 5.

Theorem 2.2 (Ruzsa, [9]). *Let h and m be positive integers and $\alpha_1, \ldots, \alpha_h$ be positive real numbers. Suppose that $A, B_1, \ldots, B_h$ are finite* *sets in a commutative group that satisfy* $|A| = m$ *and* $|A + B_i| \leq \alpha_i m$ *for all* $1 \leq i \leq h$. *Then there exists a non-empty subset* $X \subseteq A$ *such that*

$$|X + B_1 + \cdots + B_h| \leq \alpha_1 \ldots \alpha_h |X|.$$

In particular

$$|B_1 + \cdots + B_h| \leq |X + B_1 + \cdots + B_h| \leq \alpha_1 \ldots \alpha_h |X| \leq \alpha_1 \ldots \alpha_h m.$$

Substituting the last inequality into (2.1) gives the bound in Theorem 1.1.

Theorems 1.1 and 2.2 differ crucially in the exponent of m. Ruzsa has shown in [12] that if one is interested in bounding $|X + B_1 + \cdots + B_h|$ for a suitably chosen large subset of A, then the correct exponent of m is 1.

Specifically, he proved that for any $\varepsilon > 0$ there exists a non-empty subset $X \subseteq A$ such that $|X| > (1 - \varepsilon)|A|$ and

$$|X + B_1 + \cdots + B_h| \leq \frac{h\varepsilon^{1-h} - 1}{h - 1} \alpha_1 \ldots \alpha_h |X| \leq 2\varepsilon^{1-h} \alpha_1 \ldots \alpha_h |X|.$$

The exponent of $|X|$ in the upper bound remains 1 even when X is required to have very large density in A. The nature of the upper bound changes when the cardinality of the whole of $A + B_1 + \cdots + B_h$ is bounded.

3. Proof of Theorem 1.3. The upper bound in Theorem 1.3 is an increasing function of the α_i, and the ratios $|A+B_i|/|A|$ are rational numbers, so we may assume that $\alpha_i \in \mathbb{Q}^+$.

The next step is to reduce to the special case where all the α_i are equal. We prove the following.

Proposition 3.1. *Let* h *be a positive integer,* α *be a positive rational number and* m *an arbitrarily large integer. Suppose that* $A, B_1, \ldots, B_h$ *are finite sets in a commutative group that satisfy* $|A| = m$ *and* $|A + B_i| \leq \alpha m$ *for all* $1 \leq i \leq h$. *Then*

$$\begin{aligned}|A + B_1 + \cdots + B_h| &\leq \alpha^h m + \frac{(1 - 1/h)^{h-1}}{h} \alpha^h (m^{2-1/h} + O(m^{2-2/h})) \\ &= \frac{(1 - 1/h)^{h-1}}{h} \alpha^h (m^{2-1/h} + O(m^{2-2/h})).\end{aligned}$$

Theorem 1.3 is deduced from the above proposition in a standard way by working in direct products of groups (see for example [11, 12]).

Deduction of Theorem 1.3 from Proposition 3.1. Let $\alpha_i = p_i/q_i$ and set $n = q_1 \ldots q_h$. Furthermore, let $T_1, \ldots, T_h$ be pairwise disjoint sets of generators of a free abelian group F with cardinality $n_i := |T_i| = n \prod_{j \neq i} \alpha_j$; and let 0 denote the identity of F. Each n_i is chosen so that $\alpha_i n_i$ is equal to $n \prod_j \alpha_j$.

We apply Proposition 3.1 to the sets $A' = A \times \{0\}$, $B'_1 = B_1 \times T_1, \dots, B'_h = B_h \times T_h$. As

$$|A' + B'_i| = |T_i|\,|A + B_i| \le mn \prod_{j=1}^{h} \alpha_j = \Big(n \prod_{j=1}^{h} \alpha_j\Big)|A'|$$

for all $i = 1, \dots, h$, the proposition yields

$$\begin{aligned}|A' + B'_1 + \dots + B'_h| &\le \frac{(1-1/h)^{h-1}}{h}\Big(n \prod_{j=1}^{h} \alpha_j\Big)^h (m^{2-1/h} + O(m^{2-2/h}))\\ &= \frac{(1-1/h)^{h-1}}{h}\Big(\prod_{i=1}^{h} \alpha_i n_i\Big)(m^{2-1/h} + O(m^{2-2/h})).\end{aligned}$$

Theorem 1.3 follows by observing that

$$\begin{aligned}|A' + B'_1 + \dots + B'_h| &= |A + B_1 + \dots + B_h|\,|\{0\} + T_1 + \dots + T_h|\\ &= |A + B_1 + \dots + B_h| \prod_{i=1}^{h} n_i,\end{aligned}$$

and dividing by $n_1 \dots n_h$. ∎

We next prove Proposition 3.1. The rough strategy is as follows. We initially apply Theorem 2.2 to find a non-empty subset $X_1 \subseteq A$ whose growth under addition of the B_i can be bounded. We are left with bounding

$$(A + B_1 + \dots + B_h) \setminus (X_1 + B_1 + \dots + B_h).$$

We would like to iterate this process, which requires a stronger statement than Theorem 2.2. From a technical point of view, this is the heart of the argument. It requires a detour in graph-theoretic techniques developed by Plünnecke and Ruzsa and so is left for Section 5. The key result we employ in the proof of Proposition 3.1 is as follows. It will be proved in a slightly stronger form as Corollary 5.18.

Lemma 3.2 (Bound for sumsets with a component removed). *Let h be a positive integer. Suppose that $A, B_1, \dots, B_h$ are finite sets in a commutative group, and E a subset of A. If $\emptyset \ne X \subseteq A \setminus E$ minimises the quantity*

$$\mu(Z) := \frac{1}{h} \sum_{i=1}^{h} \frac{|(Z + B_i) \setminus (E + B_i)|}{|Z|}$$

over all non-empty $Z \subseteq A \setminus E$, then

$$(3.1) \qquad |(X + B_1 + \dots + B_h) \setminus (E + B_1 + \dots + B_h)| \le \mu^h |X|,$$

where

$$\mu = \mu(X) = \frac{1}{h}\sum_{i=1}^{h} \frac{|(X+B_i)\setminus(E+B_i)|}{|X|}.$$

Note that setting $E=\emptyset$ gives Theorem 2.2 for the special case when $\alpha_1=\cdots=\alpha_h=\alpha$, as

$$\mu = \min_{\emptyset\neq Z\subseteq A} \frac{1}{h}\sum_{i=1}^{h}\frac{|Z+B_i|}{|Z|} \le \frac{1}{h}\sum_{i=1}^{h}\frac{|A+B_i|}{|A|} \le \alpha.$$

The ultimate task for this section is to deduce Proposition 3.1 from the above estimate.

Proof of Proposition 3.1. Applying the bound stated above successively we partition A into $X_1\cup\cdots\cup X_k$ for some finite k (A is finite), whose exact value is irrelevant to the argument. More precisely, in the jth step we set $E=\bigcup_{\ell=1}^{j-1}X_\ell$ ($E=\emptyset$ for $j=1$) and choose X_j to be the *minimal* non-empty subset of $A\setminus E$ that minimises the quantity

$$\mu_j := \frac{1}{h}\sum_{i=1}^{h}\frac{|(Z+B_i)\setminus(E+B_i)|}{|Z|}.$$

The inequality we get is

$$\Big|(X_j+B_1+\cdots+B_h)\setminus\Big(\bigcup_{\ell=1}^{j-1}X_\ell+B_1+\cdots+B_h\Big)\Big| \le \mu_j^h|X_j|. \tag{3.2}$$

It is crucial to observe that the defining properties (and especially the minimality) of the X_j imply that the μ_j form an increasing sequence. Indeed, $\mu_j\le\mu_{j+1}$ as

$$\begin{aligned}
\mu_j|X_j|+\mu_j|X_{j+1}| &= \mu_j|X_j\cup X_{j+1}| \\
&\le \frac{1}{h}\sum_{i=1}^{h}\Big|((X_j\cup X_{j+1})+B_i)\setminus\Big(\bigcup_{\ell=1}^{j-1}X_\ell+B_i\Big)\Big| \\
&= \frac{1}{h}\sum_{i=1}^{h}\Big|(X_j+B_i)\setminus\Big(\bigcup_{\ell=1}^{j-1}X_\ell+B_i\Big)\Big| \\
&\quad + \frac{1}{h}\sum_{i=1}^{h}\Big|(X_{j+1}+B_i)\setminus\Big(\bigcup_{\ell=1}^{j}X_\ell+B_i\Big)\Big| \\
&= \mu_j|X_j|+\mu_{j+1}|X_{j+1}|.
\end{aligned}$$

When the μ_j are large it turns out that replacing the estimate in (3.2) by a more elementary one is more economical. We have

$$\Big|(X_j + B_1 + \cdots + B_h) \setminus \Big(\bigcup_{\ell=1}^{j-1} X_\ell + B_1 + \cdots + B_h\Big)\Big| \le |X_j + B_1 + \cdots + B_h| \\ \le |X_j|\,|B_1 + \cdots + B_h|.$$

To bound $|B_1 + \cdots + B_h|$ we adapt accordingly the argument in Theorem 2.2:

$$|B_1 + \cdots + B_h| \le |X_1 + B_1 + \cdots + B_h| \le \mu_1^h |X| \le \mu_1^h m.$$

Combining (3.2) with the last two inequalities gives

$$\Big|(X_j + B_1 + \cdots + B_h) \setminus \Big(\bigcup_{\ell=1}^{j-1} X_\ell + B_1 + \cdots + B_h\Big)\Big| \le \min\{\mu_j^h, \mu_1^h m\}|X_j|.$$

Summing over $j = 1, \dots, k$ leads to

$$|A + B_1 + \cdots + B_h| = \sum_{j=1}^{k} \Big|(X_j + B_1 + \cdots + B_h) \setminus \Big(\bigcup_{\ell=1}^{j-1} X_\ell + B_1 + \cdots + B_h\Big)\Big| \\ \le \sum_{j=1}^{k} \min\{\mu_j^h, \mu_1^h m\}|X_j|.$$

We are left with bounding the sum $\sum_{j=1}^{k} \min\{\mu_j^h, \mu_1^h m\}|X_j|$ subject to two constraints:

$$\sum_{j=1}^{k} |X_j| = m$$

and

$$\sum_{j=1}^{k} \mu_j |X_j| = \sum_{j=1}^{k} \Big(\frac{1}{h} \sum_{i=1}^{h} \Big|(X_j + B_i) \setminus \Big(\bigcup_{\ell=1}^{j-1} X_\ell + B_i\Big)\Big|\Big) \\ = \frac{1}{h} \sum_{i=1}^{h} \Big(\sum_{j=1}^{k} \Big|(X_j + B_i) \setminus \Big(\bigcup_{\ell=1}^{j-1} X_\ell + B_i\Big)\Big|\Big) \\ = \frac{1}{h} \sum_{i=1}^{h} |A + B_i| \le \alpha m.$$

The two quantities inside the min are equal if

$$\mu_j = \mu_* := \mu_1 m^{1/h}.$$

As $\mu_j \ge \mu_1$ for all $1 \le j \le h$, we can replace the min by the straight line

$$\mu_1^h + (\mu_j - \mu_1)\frac{\mu_*^h - \mu_1^h}{\mu_* - \mu_1},$$

which, thought of as a function of μ_j, intersects the curve μ_j^h at $\mu_j = \mu_1$ and $\mu_j = \mu_*$. The slope is bounded by

$$\mu_1^{h-1}\frac{m-1}{m^{1/h}-1} \le \mu_1^{h-1}(m^{1-1/h} + 2m^{1-2/h}).$$

Therefore

$$\begin{aligned}
|A + B_1 + \cdots + B_h| &\le \sum_{j=1}^{k}(\mu_1^h + \mu_1^{h-1}(\mu_j - \mu_1)(m^{1-1/h} + 2m^{1-2/h}))|X_j| \\
&= \mu_1^h \sum_{j=1}^{k} |X_j| + \mu_1^{h-1}(m^{1-1/h} + 2m^{1-2/h}) \sum_{j=1}^{k} \mu_j |X_j| \\
&\quad - \mu_1^h(m^{1-1/h} + 2m^{1-2/h}) \sum_{j=1}^{k} |X_j| \\
&\le \mu_1^h m + (\alpha - \mu_1)\mu_1^{h-1}(m^{2-1/h} + 2m^{2-2/h}) \\
&\le \alpha^h m + (\alpha - \mu_1)\mu_1^{h-1}(m^{2-1/h} + 2m^{2-2/h}).
\end{aligned}$$

The final task is to select the value of $1 \le \mu_1 \le \alpha$ that maximises this expression. Differentiating $(\alpha - \mu_1)\mu_1^{h-1}$ with respect to μ_1 shows that it is maximised when

$$(h-1)(\alpha - \mu_1) = \mu_1, \quad \text{so} \quad \mu_1 = (1 - 1/h)\alpha \text{ or } \alpha - \mu_1 = \alpha/h.$$

Substituting above gives

$$\begin{aligned}
|A + B_1 + \cdots + B_h| &\le \alpha^h m + \frac{(1-1/h)^{h-1}}{h}\alpha^h(m^{2-1/h} + 2m^{2-2/h}) \\
&= \alpha^h m + \frac{(1-1/h)^{h-1}}{h}\alpha^h(m^{2-1/h} + O(m^{2-2/h})). \ \blacksquare
\end{aligned}$$

This completes the proof of Proposition 3.1 modulo the proof of the estimate (3.1), which as we have seen implies Theorem 1.3. The proof of the estimate is given in Section 5. We next provide examples which show that the upper bound given by Theorem 1.3 is asymptotically sharp.

4. Examples. We construct the sets in Example 1.2. To keep the notation simple we assume that the α_i are all equal: $\alpha_1 = \cdots = \alpha_h = \alpha$.

Once these examples have been obtained, it is straightforward to construct ones for different $(\alpha_1, \ldots, \alpha_h)$ by considering direct products. Very much like in the first step of the proof of Theorem 1.3 in Section 3 we then consider sets $A' = A \times \{0\}$, $B_1' = B_1 \times T_1, \ldots, B_h' = B_h \times T_h$ to get a different h-tuple $(\alpha_1, \ldots, \alpha_h)$, where $\alpha_i = \alpha|T_i|$. The T_i are sets of distinct generators of a free commutative group. The details are as follows:

$$\frac{|A'+B_i'|}{|A'|}=\frac{|(A+B_i)\times T_i|}{|A|}=\frac{|A+B_i|}{|A|}|T_i|\le(1+o(1))\alpha|T_i|$$

and

$$\begin{aligned}|A'+B_1'+\cdots+B_h'|&=|(A+B_1+\cdots+B_h)\times(T_1+\cdots+T_h)|\\&=|A+B_1+\cdots+B_h|\,|T_1+\cdots+T_h|\\&\ge(1+o(1))\alpha^h|A|^{2-1/h}|T_1|\dots|T_h|\\&=(1+o(1))\alpha_1\dots\alpha_h|A'|^{2-1/h}.\end{aligned}$$

To construct the sets for the special case when $\alpha_i=\alpha$ for all i, we fix h and let a and l be integers, which we consider as variables with a assumed to be large and divisible by $h-1$. We set $b=la$ and work in $\mathbb{Z}_b^k$, where $k=h+a^{h-1}/(h-1)$. We write x_i for the ith coordinate of the vector x.

We consider $A=A_1\cup A_2$ where

$$A_1=\big\{x:x_i\in\{0,l,2l,\dots,(a-1)l\}\text{ for }1\le i\le h\text{ and }x_i=0\text{ otherwise}\big\}$$

and A_2 is a collection of $a^{h-1}/(h-1)$ independent points:

$$A_2=\bigcup_{j=h+1}^{k}\{x:x_j=1,\ x_j=0\text{ otherwise}\}.$$

We take B_i to be a copy of $\mathbb{Z}_b$:

$$B_i=\big\{x:x_i\in\{0,\dots,b-1\},\ x_j=0\text{ for all }j\ne i\big\}.$$

We now estimate the cardinality of the sets that interest us. We have

$$|A|=|A_1|+|A_2|=a^h+\frac{a^{h-1}}{h-1}=(1+o(1))a^h.$$

As h is fixed, different values of a result in different values of m.

To bound $|A+B_i|$ we note that $|A_1+B_i|$ equals

$$|\{x:x_i\in\{0,\dots,b-1\},\,x_j\in\{0,\ell,2\ell,\dots,(a-1)\ell\},j\ne i\}|=ba^{h-1}$$

and that

$$|A_2+B_i|=|A_2|\,|B_i|=\frac{ba^{h-1}}{h-1}.$$

Thus

$$\begin{aligned}|A+B_i|&\le|A_1+B_i|+|A_2+B_i|\le ba^{h-1}+\frac{ba^{h-1}}{h-1}\\&=\Big(1+\frac{1}{h-1}\Big)la^h=(1+o(1))\Big(1+\frac{1}{h-1}\Big)lm.\end{aligned}$$

Therefore

$$\alpha = \left(1 + \frac{1}{h-1}\right) l.$$

Since h is fixed, different values of l lead to different values of α.

To bound $|A + B_1 + \cdots + B_h|$ from below observe that $|B_1 + \cdots + B_h| = |\mathbb{Z}_b^h| = b^h$ and that for $a, a' \in A_2$ the intersection

$$(a + B_1 + \cdots + B_h) \cap (a' + B_1 + \cdots + B_h)$$

is empty. Thus

$$\begin{aligned} |A + B_1 + \cdots + B_h| \geq |A_2 + B_1 + \cdots + B_h| = |A_2|\,|B_1 + \cdots + B_h| = \frac{a^{h-1}}{h-1} b^h \\ = \frac{l^h}{h-1} a^{2h-1} = (1 + o(1)) \frac{(1 - 1/h)^h}{h-1} \alpha^h m^{2-1/h} \\ = (1 + o(1)) \frac{(1 - 1/h)^{h-1}}{h} \alpha^h m^{2-1/h}. \end{aligned}$$

We are done. As is expected, the structure of the sets presented here is such that every inequality in Section 3 is more or less attained.

5. Graph theory. In this section we develop the graph-theoretic framework necessary for our proof of the estimate (3.1), the last step of the proof of Theorem 1.3. The results and methods of this section are influenced by the work of Ruzsa [11, 12].

We define a type of layered commutative graph, called a *commutative hypercube graph*, that generalises the addition graph associated to sumsets of the form $A + B_1 + \cdots + B_h$, defined in Example 5.2 below. The class of commutative hypercube graphs includes graphs that result from removing a component from an addition graph. The main result of this section is an analog of Theorem 2.2 for commutative hypercube graphs.

Throughout this section $\biguplus$ stands for disjoint union.

5.1. Hypercube graphs and their products. Let Q_h denote the set of all subsets of $\{1, \ldots, h\}$, and for I in Q_h let $|I|$ denote the cardinality of I. Given I and I' in Q_h, we will write $I \to I'$ if $I' = I \cup \{i\}$ for some $i \notin I$.

Definition 5.1 (Hypercube graph). Let $\mathcal{G}$ be a directed graph with vertex set V and edge set E. We say that $\mathcal{G}$ is a *hypercube graph indexed by* Q_h if it satisfies two conditions:

(i) For each I in Q_h there exists a set $U_I \subseteq V$ such that V is the disjoint union of the U_Is: $V = \biguplus_{I \in Q_h} U_I$.

(ii) There is an edge $u \to v$ in E only if $u \in U_I$ and $v \in U_{I'}$ where $I \to I'$.

For short, we may say $\mathcal{G}$ is a Q_h-*hypercube graph*. Note that a Q_h-hypercube graph is a layered graph with $h+1$ layers: $V = V_0 \cup \cdots \cup V_h$, where $V_i = \biguplus_{|I|=i} U_I$.

We give some examples of hypercube graphs. The most important one is an addition graph with different summands, featuring in [12].

Example 5.2 (Addition graphs). Let $A, B_1, \ldots, B_h$ be finite subsets of a commutative group G. Their *addition graph* $\mathcal{G}_+(A, B_1, \ldots, B_h)$ is defined as follows: for each I in Q_h, let $U_I = A + \sum_{i\in I} B_i$. We consider each U_I to be contained in a separate copy of G, and we let $V = \biguplus_{I\in Q_h} U_I$. For each vertex x in U_I there is an edge to y in $U_{I'}$ if $I' = I \cup \{i\}$ and $y = x + b$ for some b in B_i. Thus $\mathcal{G}_+(A, B_1, \ldots, B_h)$ is a hypercube graph indexed by Q_h.

Note that any subgraph of a Q_h-hypercube graph is automatically a Q_h-hypercube graph. For certain induced subgraphs of a hypercube graph, we can say something more. We recall from [11] a definition.

Definition 5.3 (Channels of directed graphs). Given a directed graph $\mathcal{G} = \mathcal{G}(V, E)$ and two sets of vertices $X, Y \subseteq V$, the *channel* $\overline{\mathcal{G}}(X, Y)$ between X and Y is the subgraph of $\mathcal{G}$ induced by the set of vertices that lie on a path from X to Y (including endpoints).

Example 5.4 (Channels are hypercube graphs). Let $\mathcal{G}$ be a hypercube graph indexed by Q_h and let I and I' be elements of Q_h such that $I \subseteq I'$. Given subsets $X \subseteq U_I$ and $Y \subseteq U_{I'}$, the channel $\overline{\mathcal{G}}(X, Y)$ is a hypercube graph indexed by Q_j, where $j = |I' \setminus I|$.

Proof. Since the edges of $\overline{\mathcal{G}}$ are edges of $\mathcal{G}$, condition (i) of Definition 5.1 is automatically satisfied. Thus it remains to check (ii).

Note that the set of J in Q_h such that $I \subseteq J \subseteq I'$ is in one-to-one correspondence with Q_j. Fixing one such correspondence, let $\bar{J}$ denote the element in Q_j corresponding to J and set $U_{\bar{J}}(\overline{\mathcal{G}}) = V(\overline{\mathcal{G}}) \cap U_J$. Since any vertex in $V(\overline{\mathcal{G}})$ must be an element of some U_J with $I \subseteq J \subseteq I'$, we have $V(\overline{\mathcal{G}}) = \biguplus_{\bar{J}\in Q_j} U_{\bar{J}}(\overline{\mathcal{G}})$, as desired. ■

To prove the analog of Theorem 2.2, we must define a type of graph product between hypercube graphs that is motivated by addition graphs of product sets.

Definition 5.5 (Hypercube product). Let $\mathcal{G}'$ and $\mathcal{G}''$ be hypercube graphs indexed by Q_h. We construct a hypercube graph $\mathcal{G} = \mathcal{G}' \otimes \mathcal{G}''$ also indexed by Q_h as follows: for each $I \in Q_h$, we define $U_I(\mathcal{G}) = U_I(\mathcal{G}') \times U_I(\mathcal{G}'')$, and for $(u, v) \in U_I(\mathcal{G})$, $(u', v') \in U_{I'}(\mathcal{G})$, we have $(u, v) \to (u', v')$ if and only if $u \to u'$ and $v \to v'$. We call $\mathcal{G}$ the *hypercube product* of $\mathcal{G}'$ and $\mathcal{G}''$.

It is easy to see that $\mathcal{G}_+(A' \times A'', B_1' \times B_1'', \ldots, B_h' \times B_h'')$ is the hypercube product of $\mathcal{G}_+(A', B_1', \ldots, B_h')$ and $\mathcal{G}_+(A'', B_1'', \ldots, B_h'')$. In this sense, direct products in the group setting correspond to hypercube products in the graph setting and so hypercube products are natural objects.

5.2. Square commutativity. The key feature of addition graphs that makes them useful in additive number theory is that they capture in a graph-theoretic way the commutativity of addition. This particular feature was first exploited by Plünnecke [8], who worked with a class of directed layered graphs he called *commutative*. The importance of commutative graphs to additive number theory is detailed in [6, 14, 11]. We will only mention them briefly as we need a stronger form of commutativity in order to prove Theorem 2.2, one that works better for hypercube graphs.

First we make an auxiliary definition: given index sets I, I', I'' in Q_h such that $I \to I' \to I''$, there is a unique index set I'_c in Q_h such that $I'_c \neq I'$ and $I \to I'_c \to I''$; explicitly $I'_c = I \cup (I'' \setminus I')$. We will call I'_c the *associate* of I'.

Definition 5.6 (Square commutativity). Let $\mathcal{G}$ be a hypercube graph indexed by Q_h. We say that $\mathcal{G}$ is *square commutative* if it satisfies two conditions:

(1) Upward square commutativity: Given indices I, I' and I'' in Q_h such that $I \to I' \to I''$, and vertices $v \in U_I$, $v' \in U_{I'}$, and $v''_1, \dots, v''_n \in U_{I''}$ such that $v \to v' \to v''_i$ for $i = 1, \dots, n$, there exist distinct vertices $v'_1, \dots, v'_n \in U_{I'_c}$ such that $v \to v'_i \to v''_i$ for $i = 1, \dots, n$.
(2) Downward square commutativity: Given indices I, I' and I'' in Q_h such that $I \to I' \to I''$, and vertices $v_1, \dots, v_n \in U_I$, $v' \in U_{I'}$, and $v'' \in U_{I''}$ such that $v_i \to v' \to v''$ for $i = 1, \dots, n$, there exist distinct vertices $v'_1, \dots, v'_n \in U_{I'_c}$ such that $v_i \to v'_i \to v''$ for $i = 1, \dots, n$.

Square commutative graphs are commutative in the sense defined by Plünnecke; square commutativity strengthens commutativity by requiring that the alternate paths from v to v''_i (or from v_i to v'') go through the associate vertex set. This is an important observation as later on we will need to apply Plünnecke's result.

In our language, Ruzsa has already shown in [12, pp. 597–598] that addition graphs are square commutative:

Proposition 5.7 (Ruzsa, [12]). *Let $A, B_1, \dots, B_h$ be subsets of a commutative group. Then their addition graph $\mathcal{G}_+(A, B_1, \dots, B_h)$ is square commutative.*

Channels of square commutative hypercube graphs are also square commutative.

Lemma 5.8. *Let $\mathcal{G}$ be a square commutative hypercube graph indexed by Q_h, and let $\overline{\mathcal{G}} = \overline{\mathcal{G}}(X, Y)$ be a channel of $\mathcal{G}$. Then $\overline{\mathcal{G}}$ is square commuta-*

tive. Additionally, if $X \subseteq U_I$ and $Y \subseteq U_{I'}$ where $I \subsetneq I' \in Q_h$, then $\overline{\mathcal{G}}$ is a Q_j square commutative hypercube graph, where $j = |I' \setminus I|$.

Proof. We have already shown in Example 5.4 that $\overline{\mathcal{G}}$ is a hypercube graph indexed by $Q_{|I'\setminus I|}$. That it is square commutative follows from the fact that $\mathcal{G}$ is square commutative combined with the fact that if $x, z \in V(\overline{\mathcal{G}})$ and $x \to y \to z$ then $y \in V(\overline{\mathcal{G}})$. ∎

Now that we have shown that the main examples of hypercube graphs are square commutative, we will prove that square commutativity is inherited by products.

LEMMA 5.9. *Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be square commutative hypercube graphs indexed by Q_h, and let $\mathcal{G} = \mathcal{G}_1 \otimes \mathcal{G}_2$ be their hypercube product. Then $\mathcal{G}$ is square commutative.*

Proof. The proof is a straightforward verification of square commutativity. We will only prove the upward condition, since the proof of the downward condition is similar.

Let I, I', and I'' be indices in Q_h such that $I \to I' \to I''$, and suppose we have vertices $(u,v) \in U_I(\mathcal{G})$, $(u',v') \in U_{I'}(\mathcal{G})$, and $(u_1'',v_1''),\dots,(u_n'',v_n'') \in U_{I''}(\mathcal{G})$ such that $(u,v) \to (u',v') \to (u_i'',v_i'')$ for $i = 1,\dots,n$. We must find $(u_1',v_1'),\dots,(u_n',v_n') \in U_{I_c'}(\mathcal{G})$ such that $(u,v) \to (u_i',v_i') \to (u_i'',v_i'')$ for $i = 1,\dots,n$.

Consider the sequences of vertices $u \to u' \to u_i''$ in $\mathcal{G}_1$. Since $\mathcal{G}_1$ is square commutative, there exist distinct vertices $u_i' \in U_{I_c'}(\mathcal{G}_1)$ such that $u \to u_i' \to u_i''$ for $i = 1,\dots,n$. Similarly there exist distinct vertices $v_i' \in U_{I_c'}(\mathcal{G}_2)$ such that $v \to v_i' \to v_i''$ for $i = 1,\dots,n$. Thus we have distinct vertices $(u_i',v_i') \in U_{I_c'}(\mathcal{G}_1) \times U_{I_c'}(\mathcal{G}_2) = U_{I_c'}(\mathcal{G})$ such that $(u,v) \to (u_i',v_i') \to (u_i'',v_i'')$ for $i = 1,\dots,n$, as desired. ∎

5.3. A Plünnecke-type inequality for square commutative graphs. The main goal in this section is to extend Ruzsa's Theorem 2.2. Our result can furthermore be thought of as an extension to square commutative graphs of Plünnecke's inequality (Theorem 5.10 below). Before we do this, we need to establish some notation and lemmas regarding magnification ratios.

Given a directed graph $\mathcal{G}$ and subsets $X, Y \subseteq V(\mathcal{G})$, we will use $\mathrm{Im}_{\mathcal{G}}(X,Y)$ to denote the set of elements in Y that can be reached from X by paths in $\mathcal{G}$.

If $\mathcal{G}$ has layers $V_0,\dots,V_h$, we will use $\mu_i(\mathcal{G})$ to denote the *ith magnification ratio* of $\mathcal{G}$, which is defined as

$$\mu_i(\mathcal{G}) := \min_{\emptyset \neq Z \subseteq V_0} |\mathrm{Im}_{\mathcal{G}}(Z,V_i)|/|Z|.$$

We will say that $\emptyset \neq X \subseteq V_0$ *achieves* $\mu_i(\mathcal{G})$ when $\mu_i(\mathcal{G}) = |\mathrm{Im}_{\mathcal{G}}(X,V_i)|/|X|$.

Plünnecke bounded the growth of magnification ratios of commutative graphs. We state a special case of his result that will be applied later.

THEOREM 5.10 (Plünnecke, [8]). *Let $h \geq 1$ be a positive integer and $\mathcal{G}$ be a commutative graph. Then*

$$\mu_h(\mathcal{G}) \leq \mu_1(\mathcal{G})^h.$$

Square commutative graphs are commutative, so Theorem 5.10 applies; however, the bound on $\mu_h(\mathcal{G})$ is not adequate for our purpose. The goal of this subsection is to improve it for square commutative graphs.

If $\mathcal{G}$ is a hypercube graph indexed by Q_h, then the magnification of a subset $\emptyset \neq X \subseteq V_0$ in U_I, where $I \in Q_h$, is defined as

$$\beta_I(X) := |\mathrm{Im}_{\mathcal{G}}(X, U_I)|/|X|.$$

If $I = \{i\}$, then we will use $\beta_i(X)$ to denote $\beta_{\{i\}}(X)$. The following lemma relates the β_I to the usual magnification ratio μ_i.

LEMMA 5.11. *Let $\mathcal{G}$ be a hypercube graph indexed by Q_h. For any $\emptyset \neq X \subseteq V_0(\mathcal{G})$ we have*

$$\mu_i(\mathcal{G}) \leq \sum_{|I|=i} \beta_I(X),$$

with equality if and only if X achieves $\mu_i(\mathcal{G})$.

Proof. By the definition of $\mu_i(\mathcal{G})$ we have

$$\mu_i(\mathcal{G}) \leq |\mathrm{Im}_{\mathcal{G}}(X, V_i)|/|X|$$

with equality if and only if X achieves $\mu_i(\mathcal{G})$. Since V_i is a disjoint union of the U_I such that $|I| = i$, we have

$$\frac{|\mathrm{Im}_{\mathcal{G}}(X, V_i)|}{|X|} = \frac{|\biguplus_{|I|=i} \mathrm{Im}_{\mathcal{G}}(X, U_I)|}{|X|} = \sum_{|I|=i} \frac{|\mathrm{Im}_{\mathcal{G}}(X, U_I)|}{|X|} = \sum_{|I|=i} \beta_I(X).$$

Combining these two equations yields the desired inequality. ∎

Later we will also need the following elementary identity, which asserts that the β_i are multiplicative.

LEMMA 5.12. *Let $\mathcal{G}', \mathcal{G}''$ be hypercube graphs indexed by Q_h and $\mathcal{G} = \mathcal{G}' \otimes \mathcal{G}''$. Then for all $i = 1, \ldots, h$ and $Z' \subseteq V_0(\mathcal{G}')$, $Z'' \subseteq V_0(\mathcal{G}'')$ we have*

$$\beta_i(Z' \times Z'') = \beta_i(Z')\beta_i(Z'').$$

Proof. We have $V_1(\mathcal{G}') = \biguplus_{i=1}^h U'_{\{i\}}$ and $V_1(\mathcal{G}'') = \biguplus_{i=1}^h U''_{\{i\}}$. The way $\mathcal{G}$ is constructed gives $V_1(\mathcal{G}) = \biguplus_{i=1}^h (U'_{\{i\}} \times U''_{\{i\}})$. Note that

$$\mathrm{Im}_{\mathcal{G}}(Z' \times Z'', U'_{\{i\}} \times U''_{\{i\}}) = \mathrm{Im}_{\mathcal{G}'}(Z', U'_{\{i\}}) \times \mathrm{Im}_{\mathcal{G}''}(Z'', U''_{\{i\}}).$$

The claim follows by taking cardinalities:

$$\beta_i(Z' \times Z'') = \frac{|\mathrm{Im}_{\mathcal{G}}(Z' \times Z'', U'_{\{i\}} \times U''_{\{i\}})|}{|Z' \times Z''|}$$
$$= \frac{|\mathrm{Im}_{\mathcal{G}'}(Z', U'_{\{i\}})|}{|Z'|} \frac{|\mathrm{Im}_{\mathcal{G}''}(Z'', U''_{\{i\}})|}{|Z''|} = \beta_i(Z')\beta_i(Z''). \blacksquare$$

Magnification ratio is multiplicative with respect to tensor product of layered graphs. However, for hypercube graphs this is only true for the top level magnification ratio, which is multiplicative for square commutative hypercube graphs. Square commutativity is not necessary, but it is sufficient (logically and for our purposes).

LEMMA 5.13. *Let $\mathcal{G}_1$ and $\mathcal{G}_2$ be commutative hypercube graphs indexed by Q_h, and let $\mathcal{G}_3$ be the hypercube product $\mathcal{G}_1 \otimes \mathcal{G}_2$. Then*

$$\mu_h(\mathcal{G}_3) = \mu_h(\mathcal{G}_1)\mu_h(\mathcal{G}_2).$$

Proof. For $i = 1, 2, 3$, we will define an auxiliary layered graph $\hat{\mathcal{G}}_i$ as follows: $V_0(\hat{\mathcal{G}}_i) := V_0(\mathcal{G}_i)$, $V_1(\hat{\mathcal{G}}_i) := V_h(\mathcal{G}_i)$, and $(v, v') \in E(\hat{\mathcal{G}}_i)$ if and only if there is a path from v to v' in $\mathcal{G}_i$. The proof rests on the following fact:

CLAIM 5.14. $\hat{\mathcal{G}}_3 = \hat{\mathcal{G}}_1 \times \hat{\mathcal{G}}_2$.

In words, $\hat{\mathcal{G}}_3$ is the directed layered tensor product of $\hat{\mathcal{G}}_1$ and $\hat{\mathcal{G}}_2$. It should be noted here that this would not be the case if we were working with ith magnification ratios for $1 \le i < h$, and that square commutativity is essential for our proof.

Proof of Claim. It suffices to show that for any pair of vertices (u_0, v_0) in $V_0(\mathcal{G}_1) \times V_0(\mathcal{G}_2)$ and any pair of vertices (u_h, v_h) in $V_h(\mathcal{G}_1) \times V_h(\mathcal{G}_2)$, we can find a sequence of index sets $\emptyset \to I_1 \to \cdots \to I_h = \{1, \ldots, h\}$ and paths $u_0 \to u_1 \to \cdots \to u_h$ in $\mathcal{G}_1$ and $v_0 \to v_1 \to \cdots \to v_h$ in $\mathcal{G}_2$ such that $u_j \in U_{I_j}(\mathcal{G}_1)$ and $v_j \in U_{I_j}(\mathcal{G}_2)$. This guarantees that the product path $(u_0, v_0) \to (u_1, v_1) \to \cdots \to (u_h, v_h)$ is contained in the hypercube product $\mathcal{G}_1 \otimes \mathcal{G}_2$, hence the edge $(u_0, v_0) \to (u_h, v_h)$ is contained in $\hat{\mathcal{G}}_3$.

Let $u_0 \to u_1 \to \cdots \to u_h$ be any path in $\mathcal{G}_1$ from u_0 to u_h. We will use square commutativity to show that there is a path $u_0 \to u'_1 \to \cdots \to u'_{h-1} \to u_h$ such that $u'_j \in U_{\{1,\ldots,j\}}$. Applying the same argument for a path $v_0 \to v_1 \to \cdots \to v_h$ will prove the claim.

For each u_j, let I_j be the index set in Q_h such that $u_j \in U_{I_j}(\mathcal{G}_1)$. By definition, $u_j \to u_{j+1}$ only if there exists i_{j+1} such that $I_{j+1} = I_j \cup \{i_{j+1}\}$. Thus we may represent the sequence of index sets by a permutation:

$$\begin{pmatrix} 1 & 2 & \cdots & h \\ i_1 & i_2 & \cdots & i_h \end{pmatrix}.$$

Applying upward square commutativity to the sequence $I_{j-1} \to I_j \to I_{j+1}$ is equivalent to switching the pair i_j and i_{j+1}. An example that illustrates this fact is that by applying upward square commutativity to the layers V_0, V_1, V_2 we transform the sequence $V_0 = U_\emptyset \to U_{\{i_1\}} \to U_{\{i_1,i_2\}}$ to $V_0 = U_\emptyset \to U_{\{i_2\}} \to U_{\{i_1,i_2\}}$ and so, in the permutation notation, we get

$$\begin{pmatrix} 1 & 2 & 3 & \cdots & h \\ i_1 & i_2 & i_3 & \cdots & i_h \end{pmatrix} \to \begin{pmatrix} 1 & 2 & 3 & \cdots & h \\ i_2 & i_1 & i_3 & \cdots & i_h \end{pmatrix}.$$

Thus by repeated application of upward square commutativity, we can find a path $u_0 \to u_1' \to u_2' \to \cdots \to u_h$ such that $u_1' \in U_{\{1\}}(\mathcal{G}_1)$. Again by repeated application of square commutativity, we can find a path $u_0 \to u_1' \to u_2'' \to u_3'' \to \cdots \to u_h$ such that $u_2'' \in U_{\{1,2\}}(\mathcal{G}_1)$, and so on. ∎

Now we continue with the proof of the lemma. By definition of $\hat{\mathcal{G}}_i$, we have $\mu_1(\hat{\mathcal{G}}_i) = \mu_h(\mathcal{G}_i)$ for $i = 1, 2, 3$. Since $\hat{\mathcal{G}}_3$ is the layered product of $\hat{\mathcal{G}}_1$ and $\hat{\mathcal{G}}_2$, by the multiplicativity of magnification ratios of directed layered graphs (e.g. [6, Theorem 7.1]) we have $\mu_1(\hat{\mathcal{G}}_3) = \mu_1(\hat{\mathcal{G}}_1)\mu_1(\hat{\mathcal{G}}_2)$. Thus $\mu_h(\mathcal{G}_3) = \mu_h(\mathcal{G}_1)\mu_h(\mathcal{G}_2)$, as desired. ∎

We are now ready to state and prove the theorem.

Theorem 5.15 (A Plünnecke-type inequality for square commutative graphs). *Let $\mathcal{G}$ be a square commutative graph indexed by Q_h. Then for every $\emptyset \neq Z \subseteq V_0$ we have*

$$\mu_h(\mathcal{G}) \le \beta_1(Z) \dots \beta_h(Z).$$

Moreover,

$$\mu_h(\mathcal{G}) \le (\mu_1(\mathcal{G})/h)^h.$$

Proof. As usual $\biguplus_{i=0}^h V_i$ is the vertex set of $\mathcal{G}$ and $V_1 = \biguplus_{i=1}^h U_{\{i\}}$.

We observe that $\mathcal{G}$ is a square commutative graph and so in particular it is commutative. Applying Theorem 5.10 and Lemma 5.11 successively gives

$$\mu_h(\mathcal{G}) \le \mu_1(\mathcal{G})^h \le \Big(\sum_{i=1}^h \beta_i(Z)\Big)^h,$$

for all $\emptyset \neq Z \subseteq V_0$. A first improvement is as follows.

Claim 5.16. *For all $\emptyset \neq Z \subseteq V_0$, we have*

$$\mu_h(\mathcal{G}) \le \Big(\max_{1\le i\le h} \beta_i(Z)\Big)^h. \tag{5.1}$$

Proof. We use the tensor product trick ([12], see also [13]). Let n be any positive integer. We let $\mathcal{G}^n = \mathcal{G}\otimes\cdots\otimes\mathcal{G}$ denote the n-fold hypercube product of $\mathcal{G}$ with itself and $S^n \subseteq V_i(\mathcal{G}^n)$ the subset of $V_i(\mathcal{G}^n)$ that is precisely the n-fold product of S with itself.

By Lemma 5.13, Theorem 5.10 and Lemma 5.9 we find that, for all positive integers n,

$$\mu_h(\mathcal{G})^n = \mu_h(\mathcal{G}^n) \leq \mu_1(\mathcal{G}^n)^h.$$

By Lemmas 5.11 and 5.12 we have $\mu_1(\mathcal{G}^n) \leq \sum_{i=1}^h \beta_i(Z^n) = \sum_{i=1}^h \beta_i(Z)^n$ and so

$$\mu_h(\mathcal{G}) \leq \Big(\sum_{i=1}^h \beta_i(Z)^n\Big)^{h/n}.$$

Letting n go to infinity proves Claim 5.16. ■

To deduce the first inequality in the statement of Theorem 5.15 we use a trick of Ruzsa (e.g. [11]), which appears in his proof of Theorem 2.2 and is similar to that used in the deduction of Theorem 1.3 from Proposition 3.1.

We begin by recalling that Z is fixed. Let $T_1, \ldots, T_h$ be pairwise disjoint sets of generators of a free abelian group with identity 0. For now we leave $n_i = |T_i|$ undetermined, but note that they will depend on Z.

Let $\mathcal{T}$ denote the addition graph $\mathcal{G}_+(\{0\}, T_1, \ldots, T_h)$ and let $\mathcal{G}' = \mathcal{G} \otimes \mathcal{T}$. The subsets of $V_0(\mathcal{G}')$ are of the form $S \times \{0\}$ for $S \subseteq V_0$.

Combining Claim 5.16 with Lemma 5.12 gives

$$\mu_h(\mathcal{G}') \leq \Big(\max_{1\leq i\leq h} \beta_i(Z\times\{0\})\Big)^h = \Big(\max_{1\leq i\leq h} \beta_i(Z)\beta_i(\{0\})\Big)^h = \Big(\max_{1\leq i\leq h} \beta_i(Z)n_i\Big)^h.$$

We now choose the values of the n_i. The $\beta_i(Z)$ are rational numbers so we set $\beta_i(Z) = p_i/q_i$ and $n = q_1 \ldots q_h$. By choosing $n_i = n\prod_{j\neq i} \beta_j(Z)$ we have $\beta_i(Z)n_i = n\prod_{\ell=1}^h n_\ell = \beta_j(Z)n_j$ for all $i, j = 1, \ldots, n$. Thus

$$\Big(\max_{1\leq i\leq k} \beta_i(Z)n_i\Big)^h = \prod_{i=1}^h \beta_i(Z)n_i.$$

On the other hand, Lemma 5.13 gives

$$\mu_h(\mathcal{G}') = \mu_h(\mathcal{G})\mu_h(\mathcal{T}) = \mu_h(\mathcal{G})|T_1 + \cdots + T_h| = \mu_h(\mathcal{G})n_1 \ldots n_h.$$

Combining the above proves the first inequality in the statement of the theorem:

$$\mu_h(\mathcal{G}) = \frac{\mu_h(\mathcal{G}')}{n_1 \ldots n_h} \leq \frac{(\max_{1\leq i\leq h} \beta_i(Z)n_i)^h}{n_1 \ldots n_h} = \frac{\prod_{i=1}^h \beta_i(Z)n_i}{n_1 \ldots n_h} = \prod_{i=1}^h \beta_i(Z).$$

To get the second inequality, we first apply the arithmetic mean–geometric mean inequality to obtain

$$\mu_h(\mathcal{G}) \leq \beta_1(Z) \ldots \beta_h(Z) \leq \Big(\frac{1}{h}\sum_{i=1}^h \beta_i(Z)\Big)^h.$$

The last step is to let $\emptyset \neq X \subseteq V_0$ be the subset that achieves the first magnification ratio $\mu_1(\mathcal{G})$, i.e., $\mu_1(\mathcal{G}) = |\mathrm{Im}_{\mathcal{G}}(X, V_1)|/|X|$. Lemma 5.11 gives $\sum_{i=1}^{h} \beta_i(X) = \mu_1(\mathcal{G})$ and we are done. ∎

Now a couple of remarks of some interest.

Considering $\mathcal{G} = \mathcal{G}_+(\{0\}, T_1, \ldots, T_h)$ as constructed above with $|T_1| = \cdots = |T_h|$ shows that the upper bound cannot be trivially improved.

Theorem 5.10 follows from Theorem 5.15. Let $\mathcal{G}$ be a commutative graph with vertex set $V_0, V_1, \ldots, V_h$. We construct a hypercube graph $\mathcal{H}$ as follows: $U_I = V_{|I|}$ and for every $I \to I'$, $u \in U_I$ and $v \in I'$, $uv \in E(\mathcal{H})$ if and only if $uv \in E(\mathcal{G})$.

One may think of the ith layer of $\mathcal{H}$ as consisting of $\binom{h}{i}$ copies of V_i, and the set of edges between U_I and $U_{I'}$ is a copy of the set of edges between $V_{|I|}$ and $V_{|I'|}$ whenever $I \to I'$.

A routine calculation confirms that $\mathcal{H}$ is square commutative, that $\mu_h(\mathcal{H}) = \mu_h(\mathcal{G})$ and that $\mu_1(\mathcal{H}) = h\mu_1(\mathcal{G})$. Therefore,

$$\mu_h(\mathcal{G}) = \mu_h(\mathcal{H}) \leq (\mu_1(\mathcal{H})/h)^h = \mu_1(\mathcal{G})^h.$$

5.4. A stronger Plünnecke-type inequality for square commutative graphs. Theorem 5.15 has one unsatisfactory aspect from a technical point of view: it does not provide any information on the subset $\emptyset \neq Z \subseteq V_0$ that achieves $\mu_h(\mathcal{G})$, i.e., the one with $\mu_h(\mathcal{G}) = |\mathrm{Im}_{\mathcal{G}}(Z, V_h)|/|Z|$. We strengthen Theorem 5.15 by proving that the subset $\emptyset \neq X \subseteq V_0$ that achieves $\mu_1(\mathcal{G})$ has restricted growth and in fact satisfies the bound given in the theorem. A similar result was proved for commutative graphs in [7].

THEOREM 5.17. *Let $\mathcal{G}$ be a square commutative graph with vertex set $V_0 \cup \cdots \cup V_h$. Suppose that $\emptyset \neq X \subseteq V_0$ achieves $\mu_1(\mathcal{G})$, i.e., $\mu_1(\mathcal{G}) = |\mathrm{Im}_{\mathcal{G}}(X, V_1)|/|X|$. Then*

$$|\mathrm{Im}_{\mathcal{G}}(X, V_h)| \leq (\mu_1(\mathcal{G})/h)^h |X|.$$

Proof. We work in the channel $\mathcal{G}' = \overline{\mathcal{G}}(X, V_h)$ rather than the original square commutative graph. In this context we will prove that if $\mathcal{G}'$ is a commutative graph with vertex set $V_0' \cup \cdots \cup V_h'$, which satisfies $\mu_1(\mathcal{G}') = |V_1'|/|V_0'|$, then

$$|V_h'| \leq (\mu_1(\mathcal{G}')/h)^h |V_0'|.$$

Suppose not. Let $\mathcal{G}'$ be a counterexample where $|V_0'|$ is minimal. Theorem 5.15 implies that the collection

$$\{\emptyset \neq Z \subseteq V_0' : |\mathrm{Im}_{\mathcal{G}'}(Z, V_h')| \leq (\mu_1(\mathcal{G}')/h)^h |Z|\}$$

is non-empty.

Let $S \subsetneq V_0'$ be a set of maximal cardinality in the collection (S cannot equal V_0' because we have assumed that $\mathcal{G}'$ is a counterexample), and $\mathcal{H} = \overline{\mathcal{G}'}(V_0' \setminus S, V_h' \setminus \mathrm{Im}_{\mathcal{G}'}(S, V_h'))$. In words, $\mathcal{H}$ is the channel consisting of all paths in $\mathcal{G}'$ that do not start in S and do not end in its image in V_h'. Suppose that $W_0 \cup W_1 \cup \cdots \cup W_h$ are the layers of $\mathcal{H}$. Observe also that for all $Z \subseteq W_0$ and all $i = 1, \ldots, h$ we have $\mathrm{Im}_{\mathcal{H}}(Z, W_i) = \mathrm{Im}_{\mathcal{G}'}(Z, W_i)$.

Now, W_1 does not intersect $\mathrm{Im}_{\mathcal{G}'}(S, V_1')$ as there would then exist a path in $\mathcal{H}$ leading to $\mathrm{Im}_{\mathcal{G}'}(S, V_h')$. We therefore have

$$\begin{aligned}|W_1| &\le |V_1'| - |\mathrm{Im}_{\mathcal{G}'}(S, V_1')| \le |V_1'| - \mu_1(\mathcal{G}')|S| \\ &= |V_1'| - \frac{|V_1'|}{|V_0'|}|S| = |V_1'|\frac{|V_0'| - |S|}{|V_0'|} = |W_0|\frac{|V_1'|}{|V_0'|},\end{aligned}$$

as $|W_0| = |V_0'| - |S|$. Consequently,

$$\mu_1(\mathcal{H}) \le \frac{|W_1|}{|W_0|} \le \frac{|V_1'|}{|V_0'|} = \mu_1(\mathcal{G}'). \tag{5.2}$$

Let $\emptyset \ne T \subseteq W_0$ be any subset that satisfies $|\mathrm{Im}_{\mathcal{H}}(T, W_1)| = \mu_1(\mathcal{H})|T|$. Let us get a lower bound on $|\mathrm{Im}_{\mathcal{H}}(T, W_h)|$. We know from the maximality of $|S|$ that

$$\begin{aligned}(\mu_1(\mathcal{G}')/h)^h|S \cup T| &< |\mathrm{Im}_{\mathcal{G}'}(S \cup T, V_h')| \\ &= |\mathrm{Im}_{\mathcal{G}'}(S, V_h')| + |\mathrm{Im}_{\mathcal{G}'}(T, V_h') \setminus \mathrm{Im}_{\mathcal{G}'}(S, V_h')| \\ &= |\mathrm{Im}_{\mathcal{G}'}(S, V_h')| + |\mathrm{Im}_{\mathcal{H}}(T, W_h)| \\ &\le (\mu_1(\mathcal{G}')/h)^h|S| + |\mathrm{Im}_{\mathcal{H}}(T, W_h)|.\end{aligned}$$

This implies

$$|\mathrm{Im}_{\mathcal{H}}(T, W_h)| > (\mu_1(\mathcal{G}')/h)^h|T|. \tag{5.3}$$

Finally, consider $\mathcal{H}' = \overline{\mathcal{H}}(T, W_h)$, the channel consisting of all paths in $\mathcal{H}$ starting at T. We see that $\mathcal{H}'$ is a square commutative graph with layers $T_0 \cup \cdots \cup T_h$ and magnification ratio $\mu_1(\mathcal{H}') = \mu_1(\mathcal{H})$. By (5.3) and (5.2) we get

$$\begin{aligned}|T_h| &= |\mathrm{Im}_{\mathcal{H}'}(T, W_h)| = |\mathrm{Im}_{\mathcal{H}}(T, W_h)| \\ &> (\mu_1(\mathcal{G}')/h)^h|T| \ge (\mu_1(\mathcal{H})/h)^h|T_0| = (\mu_1(\mathcal{H}')/h)^h|T_0|.\end{aligned}$$

Thus $\mathcal{H}'$ is another counterexample. However, $|T_0| = |T| \le |W_0| = |V_0' \setminus S| < |V_0'|$, which contradicts the minimality of $|V_0'|$. ∎

5.5. Application to sumsets with a component removed. Our final task is to deduce from Theorem 5.17 the upper bound on sumsets with a component removed, which was used in Section 3.

COROLLARY 5.18. *Let h be a positive integer. Suppose that $A, B_1, \ldots, B_h$ are finite sets in a commutative group and $E \subseteq A$ is a subset of A. If $\emptyset \ne X \subseteq A \setminus E$ is a subset of $A \setminus E$ that minimises the quantity*

$$\sum_{i=1}^{h} \frac{|(Z + B_i) \setminus (E + B_i)|}{|Z|}$$

over all non-empty subsets $Z \subseteq A \setminus E$*, then*

$$|(X + B_1 + \cdots + B_h) \setminus (E + B_1 + \cdots + B_h)| \le \mu^h |X|,$$

where

$$\mu := \mu(X) = \frac{1}{h}\sum_{i=1}^{h} \frac{|(X + B_i) \setminus (E + B_i)|}{|X|}.$$

Proof. We work in the hypercube graph $\mathcal{G}$ indexed by Q_h with vertex set given by $U_I = (A + \sum_{i\in I} B_i) \setminus (E + \sum_{i\in I} B_i)$, and edge set determined as follows: an edge exists between $u \in V_I$ and $v \in V_{I\cup\{j\}}$ if $v - u \in B_j$.

The graph $\mathcal{G}$ is square commutative by Lemma 5.8, because it is precisely the channel

$$\overline{\mathcal{G}}\Big(A \setminus E, \Big(A + \sum_{i=1}^{h} B_i\Big) \setminus \Big(E + \sum_{i=1}^{h} B_i\Big)\Big)$$

in the square commutative addition graph $\mathcal{G}_+(A, B_1, \ldots, B_h)$.

Identifying $Z \subseteq A \setminus E$ with the corresponding subset of $V_0(\mathcal{G})$ gives

$$\sum_{i=1}^{h} \frac{|(Z + B_i) \setminus (E + B_i)|}{|Z|} = \frac{|\mathrm{Im}_{\mathcal{G}}(Z, V_1)|}{|Z|}.$$

In particular the defining property of X implies that X achieves $\mu_1(\mathcal{G})$ and so

$$\begin{aligned}
\frac{\mu_1(\mathcal{G})}{h} &= \frac{1}{h}\,\frac{|\mathrm{Im}_{\mathcal{G}}(X, V_1)|}{|X|}\\
&= \frac{1}{h}\sum_{i=1}^{h} \frac{|\mathrm{Im}_{\mathcal{G}}(X, U_{\{i\}})|}{|X|}\\
&= \frac{1}{h}\sum_{i=1}^{h} \frac{|(X + B_i) \setminus (E + B_i)|}{|X|}\\
&= \mu.
\end{aligned}$$

The condition in Theorem 5.17 is satisfied and hence

$$\begin{aligned}
|(X + B_1 + \cdots + B_h) \setminus (E + B_1 + \cdots + B_h)| &= \mathrm{Im}_{\mathcal{G}}(X, V_h)\\
&\le (\mu_1(\mathcal{G})/h)^h = \mu^h |X|,
\end{aligned}$$

as claimed. ∎

Acknowledgements. The authors would like to thank the referee for the careful reading of the manuscript and helpful suggestions. The second author would like to thank the University of Rochester for their funding during his postdoc there where the bulk of this project was completed. The third author would like to thank Imre Ruzsa for his help in simplifying some of the proofs in the related paper [7], which made the proof of the main result of the present paper simpler than what it would have otherwise been.

References

[1] P. Balister and B. Bollobás, *Projections, entropy and sumsets*, Combinatorica 32 (2012), 125–141.
[2] B. Bollobás and A. Thomason, *Projections of bodies and hereditary properties of hypergraphs*, Bull. London Math. Soc. 27 (1995), 417–424.
[3] K. Gyarmati, M. Matolcsi and I. Z. Ruzsa, *Plünnecke's inequality for different summands*, in: Building Bridges: Between Mathematics and Computer Science, M. Grötschel and Gy. O. H. Katona (eds.), Bolyai Soc. Math. Stud. 19, Springer, Berlin, 2008, 309–320.
[4] K. Gyarmati, M. Matolcsi and I. Z. Ruzsa, *A superadditivity and submultiplicativity property for cardinalities of sumsets*, Combinatorica 30 (2010), 163–174.
[5] M. Madiman, A. W. Marcus and P. Tetali, *Entropy and set cardinality inequalities for partition-determined functions*, Random Structures Algorithms 40 (2012), 399–424.
[6] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Grad. Texts in Math. 165, Springer, New York, 1996.
[7] G. Petridis, *Upper bounds on the cardinality of higher sumsets*, Acta Arith. 158 (2013), 299–319.
[8] H. Plünnecke, *Eine zahlentheoretische Anwendung der Graphentheorie*, J. Reine Angew. Math. 243 (1970), 171–183.
[9] I. Z. Ruzsa, *An application of graph theory to additive number theory*, Scientia Ser. A Math. Sci. (N.S.) 3 (1989), 97–109.
[10] I. Z. Ruzsa, *Cardinality questions about sumsets*, in: Additive Combinatorics, A. Granville et al. (eds.), CRM Proc. Lecture Notes 43, Amer. Math. Soc., Providence, RI, 2007, 195–205.
[11] I. Z. Ruzsa, *Sumsets and structure*, in: Combinatorial Number Theory and Additive Group Theory, Adv. Courses Math. CRM Barcelona, Birkhäuser, Basel, 2009, 87–210.
[12] I. Z. Ruzsa, *Towards a noncommutative Plünnecke-type inequality*, in: An Irregular Mind: Szemerédi is 70, I. Bárány and J. Solymosi (eds.), Bolyai Soc. Math. Stud. 21, Springer, Berlin, 2010, 591–605.
[13] T. Tao, *Tricks Wiki article: The tensor power trick*, http://terrytao.wordpress.com/2008/08/25/tricks-wiki-article-the-tensor-product-trick/.
[14] T. Tao and V. H. Vu, *Additive Combinatorics*, Cambridge Univ. Press, Cambridge, 2006.

Brendan Murphy, Giorgis Petridis
Department of Mathematics
University of Rochester
Rochester, NY 14627, U.S.A.
E-mail: murphy@math.rochester.edu
giorgis@cantab.net

Eyvindur Ari Palsson
Department of Mathematics and Statistics
Williams College
Williamstown, MA 01267, U.S.A.
E-mail: eap2@williams.edu

Received on 2.6.2014
and in revised form on 9.12.2014 (7827)