ACTA ARITHMETICA
158.4 (2013)

Upper bounds on the cardinality of higher sumsets

by

GIORGIS PETRIDIS (Rochester, NY)

1. Introduction. One of the core problems in additive number theory is to obtain estimates on the cardinality of sumsets. Given sets A and B in a commutative group the *sumset* of A and B is defined by

$$A + B = \{a + b : a \in A,\ b \in B\}.$$

In this paper we are concerned with obtaining upper bounds on the cardinality of sumsets of the from $A + hB$ recursively defined by $A + hB = (A + (h - 1)B) + B$. It is easy to check that under no further restriction the extremal examples are when A and B are disjoint sets consisting of generators of a free commutative group.

Usually in additive number theory the sets A and B are not generic. Very often a bound on $|A + B|$ is known: $|A + B| \leq \alpha|A|$ for some $\alpha \in \mathbb{R}^+$ that could depend on A, B. Given the trivial lower bound $|A+B| \geq |A|$ this extra condition measures how much adding B to A changes the cardinality. The question we address is how much adding B repeatedly to A changes the cardinality: we suppose that A and B are finite sets in a commutative group and that both $|A|$ and $|A + B|$ are given and ask for an upper bound on $|A + hB|$ in terms of $|A|$ and $|A + B|$.

The special case when $A = B$ has attracted most attention in the literature and the answer to our question is well understood. Helmut Plünnecke established in [Pl] that $|A + A| \leq \alpha|A|$ implies

$$|hA| \leq \alpha^h|A|. \tag{1.1}$$

The upper bound is sharp when A is a group and $\alpha = 1$. More importantly, it has the correct dependence on α and $|A|$: for infinitely many $\alpha \in \mathbb{Q}^+$ there are examples (natural generalisations of Theorem 9.5 in Chapter 1 of [Ru09]) where $|hA| = c(h)\alpha^h|A|$. In these examples $c(h)$ is of the order h^{-h}

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

DOI: 10.4064/aa158-4-1

and so there is reason to believe that the dependence on h in Plünnecke's upper bound can be improved when α is large.

A particular feature of (1.1) is the multiplicativity of the upper bound. By this we mean that replacing A by its r-fold tensor product gives the same inequality. This is because $|A|$ is then replaced by $|A|^r$, α by α^r, and $|hA|$ by $|hA|^r$.

On the other hand we can get the correct dependence on h, and in particular a submultiplicative upper bound, by not insisting on having the best possible power dependence on α. Imre Ruzsa has shown in [Ru99] that $|A+A| \leq \alpha|A|$ implies

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

The outlook changes when a different set B is added repeatedly to A. Ruzsa has studied the problem of bounding $|A+2B|$ in terms of $|A|$ and $|A+B|$ thoroughly. He has shown (Section 6 of [Ru07] and Theorem 9.1 in Chapter 1 of [Ru09]) that

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

The most significant difference with the $A = B$ case is that the exponent of $|A|$ is no longer one. One may initially suspect that the upper bound must therefore not be sharp, but Ruzsa has shown otherwise. In [Ru96] he gave examples (for every positive rational α and infinitely many $|A|$) where

$$|A+2B| \geq \left(\frac{\alpha-1}{4}\right)^2 |A|.$$

Ruzsa's method works equally well for $h \geq 2$ and yields the multiplicative upper bound

$$|A+hB| \leq \alpha^h |A|^{2-1/h}.$$

The upper bound can also be derived from a (more general and more recent) result of Balister and Bollobás (Theorem 5.1 in [BB]; for a different proof see Corollary 3.7 in [MMT]).

Ruzsa's upper bound is in the correct order of magnitude in α and $|A|$. We demonstrate this by extending an example of his [Ru07] to larger h.

Example 1.1. Let h be a positive integer. There exist infinitely many $\alpha \in \mathbb{Q}^+$ with the following property. For each such α there exist infinitely many m such that one can find finite sets A and B in a commutative group with $|A| = m$, $|A+B| \leq \alpha m$ and

$$|A+hB| \geq (1+o(1)) \frac{\alpha^h}{h(h+1)^h} m^{2-1/h}.$$

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

Ruzsa also noted that the behaviour of $|A+2B|$ (and in fact of $|A+hB|$) changes when α is close to one. He proved (Theorem 10.1 in Chapter 1 of [Ru09])

$$|A+2B| \leq \alpha m + \tfrac{3}{2}\alpha(\alpha-1)|A|^{3/2}$$

for $\alpha \leq 2$. His method works equally well for $h \geq 2$ and gives

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

It is not clear whether the stated upper bound has the correct dependence on α. Extending an example of Ruzsa [Ru09] to larger h nonetheless shows that the dependence on $\alpha - 1$ and $|A|$ is correct.

EXAMPLE 1.2. Let h be a positive integer and α a real in the interval $[1,2]$. For infinitely many m there exist finite sets A and B in a commutative group such that $|A| = m$, $|A+B| \leq (1+o(1))\alpha m$ and

$$|A+hB| \geq (1+o(1))\left(m + \frac{(\alpha-1)}{h}m^{2-1/h}\right).$$

The $o(1)$ term is $o_{m\to\infty}(1)$. The same notation will be used throughout.

The main goal of this paper is to improve Ruzsa's upper bounds by introducing a further term that decreases with h. This is a first step towards determining the correct dependence of $|A+hB|$ on h. We prove the following result.

THEOREM 1.3. *Let h be a positive integer, α a positive real number and m an arbitrarily large integer. Suppose that A, B are finite non-empty sets in a commutative group that satisfy $|A| = m$ and $|A+B| \leq \alpha m$. Then*

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

We also have

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

which is stronger for $\alpha \leq 1 + 1/(2h-1)$.

The $o(1)$ term tends to zero as m gets arbitrarily large and is of the order $O(m^{-1/h})$.

The biggest qualitative improvement comes from having a term that decreases with h while keeping the optimal dependence on α and m. The bound is furthermore submultiplicative, a sharp contrast to many results in the area when different sets are added to one another [B, GMR08, GMR10]. It should be noted that while it is easy to deduce a multiplicative upper bound from a supermultipicative upper bound, it is not easy to turn a multiplicative bound to submultiplicative. The former task can be done by applying the tensor product trick, which has been applied by Ruzsa and others on many occasions. We will not discuss it any further. A good summary of how powerful it is can be found in [T2].

As we will see, roughly speaking one factor of h is saved by strengthening Plünnecke's graph-theoretic method and another factor of h by replacing it with a more efficient elementary counting argument.

The distinction between the values of α is essential as in the latter case the difference between α and $\alpha - 1$ can be substantial. For example m is the dominant term in the second upper bound for $\alpha \leq 1 + he^{-h}m^{-1+1/h}$.

Another observation is that setting $B = A$ in Theorem 1.3 works better than applying (1.1) when $\alpha \geq m^{1-1/h}$ (for example when A consists of generators of a commutative group).

The paper is organised as follows. In Section 2 we strengthen Plünnecke's graph-theoretic method, a task which has interest in its own right. Sections 3 to 5 are devoted to motivating and presenting a proof of Theorem 1.3. In Section 6 Examples 1.1 and 1.2 are constructed. In Section 7 we state some graph-theoretic results that follow by a similar approach, but we do not provide proofs. Finally in Section 8 we discuss how the material in this paper relates to more recent advances in the subject.

2. Plünnecke's inequality. We begin by recalling Plünnecke's graph-theoretic method and explaining the refinement necessary to obtain Theorem 1.3. Much of the material in this section can be found in any of the standard references [N, Ru09, TV]. The notation used is however slightly different.

G will always be a directed layered graph with edge set $E(G)$ and vertex set $V(G) = V_0 \cup \cdots \cup V_h$, where the V_i are the *layers* of the graph. For any $S \subseteq V_i$ we write $S^c = V_i \setminus S$ for the complement of S in V_i and not in $V(G)$. We furthermore assume that directed edges exist only between V_i and V_{i+1}.

We are interested in a special class of such graphs which satisfy a graph-theoretic version of commutativity, the so-called Plünnecke's conditions. *Plünnecke's upward condition* states that if uv, $vw_i \in E(G)$ for $1 \leq i \leq k$, then there exists a vertex v_i for all $1 \leq i \leq k$ such that both uv_i and v_iw_i are in $E(G)$. *Plünnecke's downward condition* states that if vw, $u_iv \in E(G)$ for $1 \leq i \leq k$, then there exists a vertex v_i for all $1 \leq i \leq k$ such that both u_iv_i and v_iw are in $E(G)$. We call a graph G *commutative* when it satisfies both conditions.

The most typical example is $G_+(A, B)$, the *addition graph* of two sets A and B in an ambient commutative group. This is defined as the directed graph whose layers are $V_0 = A$ and, for all $i > 1$, $V_i = A + iB$. A directed edge exists between $x \in V_{i-1}$ and $y \in V_i$ if and only if $y - x \in B$.

A *path* of length l in G is a sequence of vertices $v_1, \ldots, v_l$ so that $v_i v_{i+1} \in E(G)$ for all $1 \le i \le l-1$. For any subgraph H of G we define $\mathrm{Im}_H^{(i)}(Z)$ to be the collection of vertices that can be reached from Z via paths of length i in H. When the subscript is omitted we are taking H to be G and when the superscript is omitted we are taking the neighbourhood of Z in H.

For $i > j$ and $U \subseteq V_i$, $V \subseteq V_j$, the graph consisting of all paths in G starting at U and ending in V is called a *channel*. A crucial observation we will use repeatedly is that any channel of a commutative graph is a commutative graph in its own right. For $Z \subseteq V_0$ the *channel of* Z is the graph consisting of all paths in G starting at Z and ending in V_h. It should be noted that in this case $\mathrm{Im}_H(v) = \mathrm{Im}_G(v)$ for all $v \in V(H)$.

Ruzsa introduced *restricted addition graphs*, which are addition graphs with a component removed. Given any three sets A, B and C we take $G_R(A,B,C)$ to be the graph with $V_0 = A$ and $V_i = (A+iB)\setminus(C+(i-1)B)$ for all $i > 0$. The edges between layers are determined similarly to addition graphs: $xy \in E(V_i, V_{i+1})$ if and only if $y - x \in B$. Therefore $G_R(A,B,C)$ consists of all the paths in $G_+(A,B)$ that end in $(A+hB)\setminus(C+(h-1)B)$ and so it is (a channel and in particular) a commutative graph.

For $i = 1, \ldots, h$ the ith *magnification ratio* of G is defined as

$$D_i(G) = \min_{\emptyset \ne Z \subseteq V_0} \frac{|\mathrm{Im}^{(i)}(Z)|}{|Z|}.$$

Plünnecke established in [Pl] the following.

Theorem 2.1 (Plünnecke). *Let G be a commutative graph. Then the sequence $D_i^{1/i}(G)$ is decreasing.*

Other proofs can be found in [Ru89, Pe11]. The standard application of the inequality highlights how powerful it is:

Corollary 2.2. *Let A and B be finite sets in a commutative group and h be a positive integer. Suppose that that $|A| = m$ and $|A+B| \le \alpha m$. Then*

$$|hB| \le D_1(G_+(A,B))^h m \le \alpha^h m.$$

Proof. We work in the addition graph $G = G_+(A,B)$. We know from Theorem 2.1 that

$$D_h(G) \le D_1(G)^h \le \alpha^h$$

and so there is a non-empty $X \subseteq V_0 = A$ such that

$$|X + hB| = |\mathrm{Im}^{(h)}(X)| \le D_1(G)^h |X| \le \alpha^h\, m.$$

The claim follows as $|hB| \le |X + hB|$. ∎

It should be noted that no information is given on the subset of V_0 which gives rise to $D_i(G)$. The first step towards the proof of Theorem 1.3 is to strengthen the inequality and prove that any $Z \subseteq V_0$ which satisfies the condition $|\mathrm{Im}^{(j)}(Z)| = D_j(G)|Z|$ exhibits restricted growth.

THEOREM 2.3. *Let G be a commutative graph with vertex set $V_0 \cup \cdots \cup V_h$. Suppose that $D_j(G) = |V_j|/|V_0|$. Then*

$$|V_j|^h \geq |V_0|^{h-j}|V_h|^j.$$

In particular $D_1(G) = |V_1|/|V_0|$ implies

$$|V_h| \leq \left\lfloor \frac{|V_1|^h}{|V_0|^{h-1}} \right\rfloor = \lfloor D_1(G)^h |V_0| \rfloor.$$

Proof. Suppose not. Let G be a counterexample where $|V_0|$ is minimum. Plünnecke's inequality implies that the collection

$$\{Z \subseteq V_0 : |\mathrm{Im}^{(h)}(Z)| \leq D_j^{h/j}(G)|Z|\}$$

is non-empty.

Let $S \subsetneq V_0$ be a set of maximal cardinality in the collection and H be the channel consisting of paths that start in S^c and end in $\mathrm{Im}^{(h)}(S)^c$. Suppose that $U_0 \cup U_1 \cup \cdots \cup U_h$ are the layers of H.

U_j does not intersect $\mathrm{Im}^{(j)}(S)$ as there would then exist a path in H leading to $\mathrm{Im}^{(h)}(S)$. We therefore have $|U_0| = |V_0| - |S|$ and $|U_j| \leq |V_j| - |\mathrm{Im}^{(j)}(S)| \leq |V_j| - D_j(G)|S| = |V_j|(1 - |S|/|V_0|) = |V_j|(|V_0| - |S|)/|V_0|$. Consequently,

$$D_j(H) \leq |U_j|/|U_0| \leq |V_j|/|V_0| = D_j(G). \tag{2.1}$$

Let $T \subseteq U_0$ be minimal subject to $|\mathrm{Im}_H^{(j)}(T)| = D_j(H)|T|$. Let us get a lower bound on $|\mathrm{Im}_H^{(h)}(T)|$. We know from the maximality of $|S|$ that

$$\begin{aligned} D_j^{h/j}(G)\,|S \cup T| < |\mathrm{Im}^{(h)}(S \cup T)| &= |\mathrm{Im}^{(h)}(S)| + |\mathrm{Im}^{(h)}(T) \setminus \mathrm{Im}^{(h)}(S)| \\ &= |\mathrm{Im}^{(h)}(S)| + |\mathrm{Im}_H^{(h)}(T)| \leq D_j^{h/j}(G)\,|S| + |\mathrm{Im}_H^{(h)}(T)|. \end{aligned}$$

This implies

$$|\mathrm{Im}_H^{(h)}(T)| > D_j^{h/j}(G)\,|T|. \tag{2.2}$$

Finally, we consider H', the channel of T in H. This is a commutative graph with layers $T_0 \cup \cdots \cup T_h$, and by the defining properties of T and (2.1),

$$|T_j|/|T_0| = D_j(H) \leq D_j(G). \tag{2.3}$$

By combining (2.2) and (2.3) we get

$$|T_0|^{h-j}|T_h|^j > (D_j(G)|T_0|)^h \geq |T_j|^h.$$

Thus H' is another counterexample. However, $|T_0| = |T| \leq |S^c| < |V_0|$, which contradicts the minimality of $|V_0|$. ∎

REMARK. It is shown in [Pe11] that the upper bound is best possible.

A disadvantage of the traditional form of Plünnecke's inequality is that it does not specify the subset of V_0 that exhibits restricted growth at level i. In addition it leaves the possibility open that different subsets need to be considered for different i. One can get round both difficulties by selecting any $Z \subseteq V_0$ that satisfies $|\mathrm{Im}(Z)| = D_1(G)|Z|$ and applying Theorem 2.3 to the channel of Z. It follows that $|\mathrm{Im}^{(i)}(Z)| \le D_1^i(G)|Z|$ for all $i = 1, \dots, h$.

This is in fact the way we will apply the theorem: partition the vertices of G into commutative subgraphs where the condition of the theorem is satisfied.

LEMMA 2.4. *Let G be a commutative graph with vertex set $V_0 \cup \dots \cup V_h$. Then V_0 can be partitioned into $Z_1, \dots, Z_k$ and the vertices of G into vertex disjoint commutative subgraphs $G_1, \dots, G_k$ such that*

(i) *Z_i is the bottom layer of G_i,*
(ii) *$\alpha_i := D_1(G_i)$ is a strictly increasing sequence,*
(iii) $|\mathrm{Im}_{G_i}(Z_i)| = D_1(G_i)|Z_i|$.

Proof. We select the commutative subgraphs G_i as follows. We let $G_1^\star = G$ and pick $Z_1 \subseteq V_0$ of maximal cardinality subject to $|\mathrm{Im}_{G_1^\star}(Z_1)| = D_1(G_1^\star)|Z_1|$. We then define G_1 to be the channel of Z_1 in $G_1^\star$ and $\alpha_1 = D_1(G_1) = D_1(G_1^\star)$.

We repeat this process in $G_2^\star$, the channel consisting of all paths in $G_1^\star$ that start in Z_1^c and end in $\mathrm{Im}_{G_1}^{(h)}(Z_1)^c$. The layers of G_1 and $G_2^\star$ do not intersect. We select $Z_2 \subseteq Z_1^c$ of maximal cardinality subject to $|\mathrm{Im}_{G_2^\star}(Z_2)| = D_1(G_2^\star)\,|Z_2|$. We then take G_2 to be the channel of Z_2 in $G_2^\star$ (and not in G) and $\alpha_2 = D_1(G_2) = D_1(G_2^\star)$. We carry on until V_0 is partitioned into $Z_1 \cup \dots \cup Z_k$. Consequently, we get a partition of the vertices of G into vertex disjoint commutative subgraphs $G_1, \dots, G_k$.

The sequence $\{\alpha_i\}$ is strictly increasing as the maximality of the Z_i implies

$$\begin{aligned}\alpha_i(|Z_i| + |Z_{i+1}|) < |\mathrm{Im}_{G_i^\star}(Z_i \cup Z_{i+1})| &= |\mathrm{Im}_{G_i}(Z_i)| + |\mathrm{Im}_{G_{i+1}}(Z_{i+1})| \\ &= \alpha_i|Z_i| + \alpha_{i+1}|Z_{i+1}|. \ \blacksquare\end{aligned}$$

Ruzsa combined Plünnecke's inequality with some other elementary estimates in a clever way to bound $|A + hB|$. The next section is devoted to explaining Ruzsa's method and motivating the proof of Theorem 1.3. The proof itself, found in Sections 4 and 5, is entirely self-contained.

3. Ruzsa's upper bound. Let us begin by stating again the results one gets by Ruzsa's method.

THEOREM 3.1 (Ruzsa). *Let A and B be finite sets in a commutative group and h a positive integer. Suppose that $|A| = m$ and $|A + B| \le \alpha m$.*

Then

$$(3.1) \qquad |A + hB| \le \alpha^h m^{2-1/h}.$$

For $\alpha \le 2$,

$$\begin{aligned} |A + hB| &\le \alpha m + (\alpha - 1)m^2 \sum_{j=2}^{h} (1 + 1/j)\alpha^{j-1} m^{-1/j} \\ &\le m + (1 + o(1))(1 + 1/h)\alpha^{h-1}(\alpha - 1)m^{2-1/h}. \end{aligned}$$

What follows is a heuristic presentation of Ruzsa's argument and the means by which we improve it. Our aim is to help the reader keep the bigger picture in mind in the coming sections and not to provide a detailed presentation.

The best introduction may be to reflect on the limitations of Plünnecke's inequality. They appear clearly in the proof of Corollary 2.2. In general there is no reason to assume that the magnification ratio is α, or that $|hB|$ is comparable to $|X + hB|$, or that $|X|$ is comparable to $|A|$. There are cases when all assertions hold, for example when A is a subgroup and B consists of points in distinct cosets of A, but there is much to be gained by a more careful analysis. With these remarks in mind, let us turn to Ruzsa's argument.

We work in $G := G_+(A, B)$, the addition graph of A and B. The first step is to partition A into $A_1 \cup A_2$, which can be thought of as the slow and fast expanding parts of A under addition with B. To bound $|A_2 + hB|$ we start with the trivial estimate $|A_2 + hB| \le |A_2|\,|hB|$ and use Corollary 2.2 to bound $|hB|$. The only known fact about $D_1(G)$ is that it is at most α, so it is tempting to replace $D_1(G)$ with α. Note however that when $D_1(G) = \alpha$, Theorem 2.3 can be applied and so $|A + hB| \le \alpha^h m$, which is small. We can therefore assume that $D_1(G) = \alpha_1 < \alpha$. This is the first novel point of our approach.

The second has to do with bounding $|A_1 + hB|$. The standard way to do this is to first apply Plünnecke's inequality to G and get $Z_1 \subseteq A$ such that $|Z_1 + hB| \le \alpha^h |Z_1|$. Next apply Plünnecke's inequality to the channel of $A \setminus Z_1$ and get $Z_2 \subseteq A \setminus Z_1$ such that $|Z_2 + hB| \le \big(\frac{\alpha m}{m - |Z_1|}\big)^h |Z_2|$. Another application of Plünnecke's inequality to the channel of $A \setminus (Z_1 \cup Z_2)$ gives $Z_3 \subseteq A \setminus (Z_1 \cup Z_2)$ such that $|Z_3 + hB| \le \big(\frac{\alpha m}{m - |Z_1| - |Z_2|}\big)^h |Z_3|$. Iterating gives a subset $A_1 = Z_1 \cup \dots \cup Z_k \subset A$ which can be made arbitrarily large (subject to being contained in A of course). The cardinality $|A_1 + hB|$ can be bounded by $|Z_1 + hB| + \dots + |Z_k + hB|$. Ruzsa calls the resulting statement *Plünnecke's inequality for a large subset.*

The method is imbalanced. While V_0 is partitioned, the same is not done for V_1. This is largely due to the nature of Plünnecke's inequality, which gives no lower bounds on the image in V_1 of the set that exhibits restricted growth at level h. Using Theorem 2.3 instead works better. It introduces the magnification ratio α_1 into the calculations, which is welcome as $|hB|$ is bounded in terms of α_1, and also helps us partition V_1. As a consequence, the numerator of the fractions found near the end of the preceding paragraph gradually reduces. In fact we will show that a factor of $\alpha - \alpha_1$ appears in the main term. As a consequence, $|A_1 + hB|$ becomes rather small when α_1 is very close to α. On the other hand, the contribution coming from $|A_2 + hB|$ becomes larger as α_1 increases. The balancing that takes place is responsible for reducing Ruzsa's bound by a factor of h^{-1}.

To save the additional factor of h^{-1} we have to find a more efficient way to study the growth of A_2 than Plünnecke's inequality. To motivate it we examine an example that is typical of sets A and B where $A + hB$ grows fast. Suppose that A is a group and B a collection of points in different cosets of A. Then $|A + B| = |A|\,|B|$ and so $\alpha = |B|$. Plünnecke's inequality gives $|A + hB| \le |A|\,|B|^h$, but an elementary counting argument shows that in fact $|A + hB| \le |A| \binom{|B|+h-1}{h}$. With a little care one can extend the counting argument to a method of bounding V_h that works better for the fast growing part of addition graphs than Plünnecke's inequality.

Before presenting the details of our approach we note that Ruzsa's trick of bounding $|A_2 + hB|$ by $|A_2|\,|hB|$ for the "fast growing" A_2 will be vital, as will be the restricted addition graphs he introduced.

4. Restricted addition graphs.

As we saw in Section 3, Plünnecke's inequality appears to not always be optimal to study the growth of addition graphs. As noted, a much more elementary counting argument sometimes works better. To make the most of this simple observation one needs to at the very least achieve a similar improvement not only for addition graphs, but for the commutative graphs that result once a component has been removed. These are the restricted addition graphs we defined in Section 2. Our first step is to prove that the refinement we are suggesting is not hopeless.

LEMMA 4.1. *Let A, B and C be finite non-empty sets in a commutative group; G the restricted addition graph $G_R(A, B, C)$; and h a positive integer. For all $a \in V_0$,*

$$|\mathrm{Im}^{(h)}(a)| \le \binom{|\mathrm{Im}(a)| + h - 1}{h}.$$

Proof. The left hand side is the cardinality of the set

$$(a + hB) \setminus (C + (h-1)B).$$

Suppose that $a + b_1 + \cdots + b_h$ is an element of this set. If $a + b_i$ belonged to C for any i, then this element would also belong to $C + (h-1)B$. This does not happen and therefore

$$\begin{aligned}(a+hB)\setminus(C+(h-1)B) &\subseteq \{a+b_1+\cdots+b_h : b_i\in B,\ a+b_i\notin C\}\\ &= \{a+b_1+\cdots+b_h : b_i\in B\setminus(C-a)\}.\end{aligned}$$

The left hand side is therefore at most

$$\binom{|B\setminus(C-a)|+h-1}{h}=\binom{|(a+B)\setminus C|+h-1}{h},$$

which is the right hand side. ■

We use the lemma to partition the vertices of a restricted addition graph much like we did with Lemma 2.4 and get an estimate on the cardinality of its layers.

Proposition 4.2. *Let A, B and C be finite non-empty sets in a commutative group, $G=G_R(A,B,C)$ and h a positive integer. Define β, the* pseudo-cardinality *of B, to be the positive real number that satisfies*

$$\binom{\beta+h-1}{h}=|hB|.$$

Suppose that the layers of G are $V_0\cup\cdots\cup V_h$. Then

$$|V_h|\le\frac{|V_1|\,|hB|}{\beta}\le\left(1+\frac{h}{\beta}\right)\frac{e|V_1|\,|hB|^{1-1/h}}{h}.$$

Remark. The sets A and C, which have seemingly disappeared from the conclusion, are implicit in the quantity $|V_1|=|(A+B)\setminus(B+C)|$.

Proof of Proposition 4.2. Let $x=|V_0|$ and put an arbitrary order on the elements of A so that $A=\{a_1,\dots,a_x\}$.

Define a sequence of graphs by $G_1=G_R(a_1,B,C)$ and, for $i>1$, $G_i=G_R(a_i,B,C\cup(\{a_1,\dots,a_{i-1}\}+B))$. Hence, say, for $i>0$, $j>1$ the jth layer of G_i is $(a_i+jB)\setminus((\{a_1,\dots a_{i-1}\}+jB)\cup(C+(j-1)B))$. The vertex sets of the G_i therefore partition the vertex set of G and so

$$|V_j|=\sum_{i=1}^{x}|\mathrm{Im}^{(j)}_{G_i}(a_i)|\quad\text{ for } j=0,\dots,h.$$

To keep the notation simple we define the quantities $r_i=|\mathrm{Im}_{G_i}(a_i)|$ for all $i=1,\dots,x$. In particular $|V_1|=\sum_{i=1}^{x}r_i$.

Next we observe that

$$|\mathrm{Im}^{(h)}_{G_i}(a_i)|\le\min\left\{\binom{r_i+h-1}{h},|hB|\right\}.\tag{4.1}$$

The inequality follows from Lemma 4.1 and the bound

$$|\mathrm{Im}^{(h)}_{G_i}(a_i)|\le|a_i+hB|=|hB|.$$

To bound the minimum in (4.1) we observe that

$$\frac{\binom{r+h-1}{h}}{r} = \sum_{i=0}^{h-1} c_i r^i \quad \text{for positive constants } c_i \text{ that depend on } h.$$

So the function $r \mapsto \binom{r+h-1}{h}/r$ is increasing. In particular

$$\frac{1}{r}\min\left\{\binom{r+h-1}{h}, |hB|\right\} \le \frac{|hB|}{\beta}.$$

Consequently, for all $1 \le i \le x$ we have

$$|\mathrm{Im}_{G_i}^{(h)}(a_i)| \le \min\left\{\binom{r_i+h-1}{h}, |hB|\right\} \le \frac{|hB|}{\beta} r_i.$$

Summing over $i = 1, \ldots, x$ gives

$$|V_h| \le \sum_{i=1}^{x} \frac{|hB|}{\beta} r_i = \frac{|V_1|\,|hB|}{\beta}.$$

For the second inequality we observe

$$|hB| = \binom{\beta+h-1}{h} \le \left(\frac{e(\beta+h)}{h}\right)^h.$$

It follows that $(\beta+h)^{-1} \le eh^{-1}|hB|^{-1/h}$ and so

$$|V_h| \le \left(1+\frac{h}{\beta}\right)\frac{|V_1|\,|hB|}{\beta+h} \le \left(1+\frac{h}{\beta}\right)\frac{e|V_1|\,|hB|^{1-1/h}}{h}. \qquad \blacksquare$$

Balister and Bollobás obtained a similar upper bound on $|A+hB|$. It follows from Theorem 5.1 in [BB] that $|V_h| \le |V_1|\,|hB|^{1-1/h}$. The upper bound in Proposition 4.2 is better by about a factor of $1/h$ when $h = O(\beta)$.

The upper bound is furthermore sharp. Take A and B to be disjoint sets that consist solely of generators of a free commutative group and C to be the empty set. Then $|V_1| = |A+B| = |A|\,|B|$, $|V_h| = |A+hB| = |A|\,|hB|$ and $\beta = |B|$. In other words, in the proposition we are essentially establishing that $|V_h|$ is maximum when B consists of points that are independent with respect to addition with A.

It is also worth noting that the upper bound is sharp up to a constant even if β is much smaller than $|B|$. For all $\alpha \in \mathbb{Q}^+$ Ruzsa has constructed examples (Theorem 5.5 in [Ru07]) of integer sets A that satisfy $|2A| = \alpha|A|$ and $|3A| \ge c|2A|^3 = c\alpha^3|A|^{3/2}$ for some absolute constant $c > 0$. In this case β is $\sqrt{|2A|} = \sqrt{\alpha|A|}$ up to a constant and so the upper bound is, up to a constant, attained.

Setting $C = \emptyset$ and applying Corollary 2.2 gives

$$|A+hB| \le \left(1+\frac{h}{\beta}\right)\frac{e}{h}\alpha^h m^{2-1/h}.$$

For the purpose of proving Theorem 1.3 we can assume that β tends to infinity with $|A|$. This is because $\binom{\beta+h-1}{h} = |hB|$ can be taken to be at least $|A|^{1/3}$ (otherwise $|A+hB| \leq |A|\,|hB| \leq |A|^{2-2/3}$) and h is assumed to be a constant.

So Lemma 4.1 can be used to improve Theorem 3.1. Lemma 2.4 also leads to a similar upper bound on $|A+hB|$. We will not show how this is done, but only present a sketch for the benefit of the reader familiar with Ruzsa's paper. In Section 7 it is discussed how Lemma 2.4 leads to a stronger form of Plünnecke's inequality for a large subset (the term is defined in Section 3). Using the resulting Theorem 7.1 in Ruzsa's proof allows one to treat the magnification ratio α_1 of $G_+(A,B)$ as a variable that is not automatically assumed to equal α. This subtle change results in the additional factor of $1/h$. The best bound however comes by combining the two lemmata.

5. Upper bounds. To prove Theorem 1.3 we will apply Theorem 2.3 to the slowly growing part of the graph (where the magnification ratio plays a role and thus enters the calculations) and Proposition 4.2 to the fast growing part.

PROPOSITION 5.1. *Let h be a positive integer, α be a positive real number and m an arbitrarily large integer. Suppose that A, B are finite non-empty sets in a commutative group that satisfy $|A| = m$, $|A+B| \leq \alpha m$ and $D_1(G_+(A,B)) = \alpha_1$. Then*

$$|A+hB| \leq \frac{e}{h}\alpha_1^{h-1}(\alpha-\alpha_1)m^{2-1/h} + O(\alpha^h m^{2-2/h}).$$

In particular

$$|A+hB| \leq \frac{e}{h^2}\left(1-\frac{1}{h}\right)^{h-1}\alpha^h m^{2-1/h} + O(\alpha^h m^{2-2/(h+1)}).$$

Proof. We begin with some preliminary considerations. We set

$$s = |hB|/\beta$$

where the pseudocardinality β of B is defined in the statement of Proposition 4.2. If $s \leq \alpha^{h-1}$, then we are done, as by Proposition 4.2,

$$|A+hB| \leq s|A+B| \leq \alpha^h m.$$

So from now on we assume that $\alpha \leq s^{1/(h-1)}$.

Next we apply Lemma 2.4 and get a partition of A into $Z_1 \cup \cdots \cup Z_k$ and a resulting partition of the vertices of G into the vertices of a sequence of graphs $G_1, \ldots, G_k$. It follows that

$$|A+hB| = \sum_{i=1}^{k} |\mathrm{Im}^{(h)}_{G_i}(Z_i)|. \tag{5.1}$$

To estimate this sum we choose an index $j \in \{1, \ldots, k\}$. The value of j will be determined later. Applying Theorem 2.3 for $1 \le i \le j$ gives

$$|(Z_1 \cup \cdots \cup Z_j) + hB| = \sum_{i=1}^{j} |\mathrm{Im}_{G_i}^{(h)}(Z_i)| \le \sum_{i=1}^{j} \alpha_i^h |Z_i|.$$

To bound the size of $(A+hB) \setminus ((Z_1 \cup \cdots \cup Z_j)+hB)$ we apply Proposition 4.2 with $C = (Z_1 \cup \cdots \cup Z_j) + B$:

$$\begin{aligned}|(A + hB) \setminus ((Z_1 \cup \cdots \cup Z_j) + hB)| &\le s|(A + B) \setminus ((Z_1 \cup \cdots \cup Z_j) + B)| \\ &= s \sum_{i=j+1}^{k} \alpha_i |Z_i|.\end{aligned}$$

It is therefore clear that the optimal cutting point j is the largest index for which $\alpha_j \le s^{1/(h-1)}$. Note also that from the opening remarks we can assume that $\alpha_1 \le \alpha \le s^{1/(h-1)}$.

Equation (5.1) now becomes

$$|A + hB| \le \sum_{i=1}^{k} \min\{\alpha_i^h, s\alpha_i\} |Z_i|. \tag{5.2}$$

The minimum can be estimated by a linear function as follows.

LEMMA 5.2. *Let $1 \le i \le k$. In the notation established above,*

$$\min\{\alpha_i^h, s\alpha_i\} \le \alpha_i^h + t(\alpha_i - \alpha_1),$$

where

$$t = \frac{s^{h/(h-1)} - \alpha_1^h}{s^{1/(h-1)} - \alpha_1}.$$

Proof. For $1 \le i \le j$ the minimum is α_i^h. The inequality holds because the function $\alpha \mapsto \alpha^h$ is convex and the quantity t has been chosen so that the linear function equals α^h when $\alpha = \alpha_1$ or $s^{1/(h-1)}$. For $j < i \le k$ the minimum is $s\alpha_i$ and so we are comparing linear functions that meet at $\alpha = s^{1/(h-1)}$. It is therefore enough to observe that $s \le t$ to conclude the proof. ∎

Substituting the estimate we get from the above lemma in (5.2) yields

$$\begin{aligned}|A + hB| &\le \sum_{i=1}^{k} (\alpha_1^h + t(\alpha_i - \alpha_1))|Z_i| = \alpha_1^h m + t(\alpha - \alpha_1)m \\ &\le \alpha_1^h m + (\alpha - \alpha_1)m(s + hs^{(h-2)/(h-1)}\alpha_1).\end{aligned} \tag{5.3}$$

In the last inequality we used the assumption that $\alpha_1 \le s^{1/(h-1)}$.

Our next task is to bound s. The second inequality in Proposition 4.2 states

$$s \leq \left(1+\frac{h}{\beta}\right)\frac{e|hB|^{1-1/h}}{h}.$$

Very much as in the penultimate paragraph of Section 4 we can assume that h is fixed and β tends to infinity with m. It follows that $h/\beta = O(|hB|^{-1/h})$ and consequently

$$s \leq \frac{e|hB|^{1-1/h}}{h} + O(h^{-1}|hB|^{1-2/h}).$$

Corollary 2.2 gives $|hB| \leq \alpha_1^h m$ and so

$$s \leq \frac{e\alpha_1^{h-1}m^{1-1/h}}{h} + O(\alpha_1^{h-2}h^{-1}m^{1-2/h}).$$

Straightforward calculations give the first inequality:

$$|A+hB| \leq \frac{e(\alpha-\alpha_1)\alpha_1^{h-1}}{h}m^{2-1/h} + O(\alpha^h m^{1-2/h}).$$

The expression is maximised when $\alpha - \alpha_1 = \alpha/h$ and thus

$$|A+hB| \leq \frac{e}{h^2}\left(1-\frac{1}{h}\right)^{h-1}\alpha^h m^{2-1/h} + O(\alpha^h m^{2-2/(h+1)}). \blacksquare$$

We can now deduce Theorem 1.3.

Proof of Theorem 1.3. For the first part we observe that the function $h \mapsto (1-1/h)^{h-1}$ is decreasing. For large h the upper bound gets arbitrarily close to

$$h^{-2}\alpha^h m^{2-1/h}.$$

For the second part of the theorem, when α is close to one, we prove by induction that

$$|A+hB| \leq \alpha m + (\alpha-1)m\sum_{i=2}^{h} s_i, \tag{5.4}$$

where $s_i = |iB|/\beta_i$ and β_i is defined by $\binom{\beta_i+i-1}{i} = |iB|$.

The $h=1$ case is clear. For $h>1$ we consider a different restricted addition graph that was studied by Ruzsa in [Ru07].

We take any $b \in B$ and observe that

$$|A+hB| = |b+A+(h-1)B| + |(A+hB)\setminus(b+A+(h-1)B)|.$$

To bound the first term observe that $|b+A+(h-1)B| = |A+(h-1)B|$. By the induction hypothesis

$$|A+(h-1)B| \leq \alpha m + (\alpha-1)m\sum_{i=2}^{h-1} s_i.$$

To bound the second term we apply Proposition 4.2 to $G_R(A, B, b + A)$. The cardinality of V_1, the second layer of this restricted addition graph, is $(\alpha - 1)m$ and so

$$|(A + hB) \setminus (b + A + (h - 1)B)| \leq (\alpha - 1)ms_h.$$

This completes the proof of (5.4). To finish the proof of Theorem 1.3 we note that

$$s_i \leq (1 + o(1))\frac{e}{h}\alpha^{h-1}m^{1-1/h}.$$

and that replacing the first summand in (5.4) by m makes no difference to the asymptotic value. ∎

6. Examples. We now present Examples 1.1 and 1.2 in detail. As noted above, they are extensions of those given by Ruzsa in [Ru07, Ru09]. To keep the notation as simple as possible we will assume that all values are integers, as the construction works for sufficiently composite values of the parameters which make the rational values integer if necessary.

We begin with Example 1.1. Let a and l be integers, which we consider as variables with a assumed to be arbitrarily large. We let $b = la$ and fix h. We will work in $\mathbb{Z}_b^k$, where $k = h + a^{h-1}/h$. We write x_i for the ith coordinate of the vector x.

We consider $A = A_1 \cup A_2$ where

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

and A_2 is a collection of a^{h-1}/h independent points,

$$A_2 = \bigcup_{j=h+1}^{k} \{x : x_i = \delta_{ij} \text{ for all } i\}.$$

B is taken to be a collection of h copies of $\mathbb{Z}_b$,

$$B = \bigcup_{j=1}^{h} \{x : 1 \leq x_i \leq b\delta_{ij} \text{ for all } i\}.$$

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

$$|A| = a^h + a^{h-1}/h = (1 + o(1))a^h.$$

As h is fixed, different values of a lead to different values of m. To get an upper bound on $|A + B|$ we note that

$$|A_1 + B| \leq \sum_{j=1}^{h} |A_1 + \{x : 1 \leq x_i \leq b\delta_{ij}\}| \leq hba^{h-1}$$

and

$$|A_2 + B| \leq |B|\,|A_2| \leq hba^{h-1}/h = ba^{h-1}.$$

Thus

$$|A+B| \le |A_1+B| + |A_2+B| \le hba^{h-1} + ba^{h-1}$$
$$= (h+1)la^h = (1+o(1))\,(h+1)lm.$$

Therefore α is about $(h+1)l$. Since h is fixed, different values of l result in different α.

To bound $|A+hB|$ from below observe that $|hB| = b^h$ and that for $a, a' \in A_2$ the intersection $(a+hB) \cap (a'+hB)$ is trivial. Thus

$$|A+hB| \ge |A_2+hB| = 1 + (b^h-1)a^{h-1}/h = (1+o(1))b^h a^{h-1}/h$$
$$= (1+o(1))l^h a^{2h-1}/h = (1+o(1))\frac{\alpha^h}{h(h+1)^h} m^{2-1/h}.$$

We are done: we have constructed sets A and B with the desired property. As a and l assume greater values so do respectively m and α. In other words, the bounds of Theorems 1.3 and 3.1 are of the correct order of magnitude in α and m.

The difference between Example 1.1 and Theorem 1.3 is huge in terms of h. To get a feel of where the two calculations differ we look back at the proof and examine the points where it could be generous. The only point where the proof and the example agree is $|A_1+hB| = |hB|$. On the other hand, the greatest disparity appears in the growth of $|A_1+hB|$. By applying Theorem 2.3 we assume the growth is exponential. This means that $|A_1+hB|$ (and crucially also $|hB|$) should be in the order of

$$\left(\frac{|A_1+hB|}{|A_1|}\right)^h |A_1| = (1+o(1))\left(\frac{hb}{a}\right)^h |A_1|.$$

In the example, however,

$$|hB| = b^h = (1+o(1))\left(\frac{b}{a}\right)^h |A_1|.$$

We now turn to Example 1.2. This time we fix $1 < \alpha \le 2$ and h. We let a be an arbitrarily large integer and set $b = (\alpha-1)a^{h-1}/h$.

We work in a commutative group that has subgroups $B_1, \dots, B_h$ of cardinality a with pairwise trivial intersection. We take

$$A_1 = B_1 + \dots + B_h$$

of cardinality a^h and

$$A_2 = \{a_1, \dots, a_b\}$$

to be a collection of points lying in distinct non-zero cosets of A_1. We set

$$A = A_1 \cup A_2 \quad \text{and} \quad B = \bigcup_{i=1}^{h} B_i.$$

We estimate the cardinality of various sets as before. First,

$$|A| = a^h + b = (1 + o(1))a^h.$$

Thus different values of a result in different values of m. As we are free to choose a, we are free to assign infinitely many values to m.

For $A + B$ we observe that $A_1 + B = A_1$ and $|A_2 + B| \leq |A_2|\,|B| \leq bha$. Thus

$$|A + B| \leq |A_1 + B| + |A_2 + B| \leq a^h + bha = \alpha a^h = (1 + o(1))\alpha m.$$

For $A + hB$ we observe that $hB = A_1$ and so $A_1 + hB = A_1$ and $A_2 + hB$ consists of $|A_2|$ translates of A_1. Therefore $A + hB$ consists of $|A_2| + 1$ translates of A_1 whose pairwise intersections are trivial. We are done, as

$$\begin{aligned}|A + hB| &= 1 + ((b + 1)a^h - 1) = (1 + o(1))(a^h + ba^h)\\ &= (1 + o(1))\left(m + \frac{(\alpha - 1)}{h}m^{2-1/h}\right).\end{aligned}$$

7. Results about commutative graphs. In this section we present three further results about general commutative graphs. All three are similar to the results we have obtained thus far and can be proved by a similar method to the proof of Theorem 1.3: a partitioning of the vertices of the graph (similar to that given by Lemma 2.4 or Lemma 4.1) followed by an optimisation process similar to the proof of Proposition 4.2.

The first result strengthens what was earlier referred to as Plünnecke's inequality for a large subset. Often in applications one is not solely interested in a subset of V_0 that exhibits restricted growth, but in a large subset with this property. A repeated application of Plünnecke's inequality as described in Section 3 takes care of this (cf. Corollary 7.1 in [T1] and Theorem 3.2 in [Ru07]). Our method is a little more efficient.

THEOREM 7.1. *Let G be a commutative graph with vertex set $V_0 \cup \cdots \cup V_h$. Suppose that $|V_0| = m$ and $|V_1| = n$. For any $m > t \in \mathbb{R}$ there exists non-empty $X \subseteq V_0$ with $|X| > t$ such that*

$$|\mathrm{Im}^{(h)}(X)| \leq (|X| - t)\left(\frac{n}{m - t}\right)^h.$$

If we furthermore suppose that $D_1(G) = \alpha_1$, then

$$|\mathrm{Im}^{(h)}(X)| \leq \alpha_1^h\, t + (|X| - t)\left(\frac{n - \alpha_1 t}{m - t}\right)^h.$$

The first inequality is a small improvement over the above mentioned results. As we have seen, the biggest potential gain comes by introducing the magnification ratio of the graph in the second inequality. It should be noted that the bound cannot be significantly improved even when we consider addition graphs. As mentioned in Section 4, combining Ruzsa's argument in [Ru07] with Theorem 7.1 leads to $|A + hB| \ll h^{-1}\alpha^h m^{2-1/h}$.

The second result is the generalisation of Proposition 4.2 to general commutative graphs.

THEOREM 7.2. *Let G be a commutative graph with vertex set $V_0 \cup \cdots \cup V_h$. Suppose that M is the maximal cardinality of the images in V_h of one-element sets*

$$M = \max_{v \in V_0} |\mathrm{Im}^{(h)}(v)|$$

and the quantity β is given by

$$M = \binom{\beta + h - 1}{h}.$$

Then

$$|V_h| \leq \frac{M|V_1|}{\beta}.$$

The theorem can be used as an alternative to the trivial estimate $|V_h| \leq M|V_0|$. The proof is identical to that of Proposition 4.2 with only one difference: Lemma 4.1 no longer applies. The conclusion $|\mathrm{Im}^{(h)}(v)| \leq \binom{|\mathrm{Im}(v)|+h-1}{h}$ nonetheless holds for all $v \in V_0$ in general commutative graphs. It can be proved by an inductive argument (e.g. Lemma 4.4 of [Pe11]). The rest of the proof is identical to that of Proposition 4.2.

By combining the preceding two theorems one can bound the cardinality of the layers of commutative graphs in terms of the cardinality of the bottom two layers. This is a generalisation of what we have seen so far, as $|A + hB|$ is simply the cardinality of the hth layer of $G(A, B)$.

We can contract V_0 to a single vertex and get another commutative graph where the cardinality of the rest of the layers remains unchanged. The generalisation of Lemma 4.1 to commutative graphs implies that $|V_h| \leq \binom{|V_1|+h-1}{h}$ for all commutative graphs. This upper bound is in fact best possible under no further assumption on G as all but one elements of V_0 may have empty image. To eliminate this sort of examples we assume that $D_h(G)$ is non-zero. Even in this case the bound obtained from the contraction is reasonably accurate. It can nonetheless be improved.

THEOREM 7.3. *Let G be a commutative graph with vertex set $V_0 \cup \cdots \cup V_h$. Suppose that $|V_0| = m$, $|V_1| = n$ and $D_h(G) > 0$. Then $n \geq m^{1-1/h}$ and*

$$|V_h| \leq (1 + o(1)) \frac{(n - m^{1-1/h} + 3h)^h}{h!}.$$

The $o(1)$ term is as usual $o_{m\to\infty}(1)$. The proof is very similar to the proof of Theorem 1.3. The bound we get is much larger, as Ruzsa's trick of bounding the faster growing parts of V_0 using Corollary 2.2 no longer applies. It should also be noted that the condition $n \geq m^{1-1/h}$ follows from the assumption $D_h(G) > 0$ and Theorem 2.3. The perhaps mysterious $m^{1-1/h}$ term that appears in the numerator is the minimum value that $\alpha_1 m$ can attain, where as usual α_1 is the first magnification ratio of the graph.

The bound is furthermore reasonably sharp. An *independent addition graph* is $G_+(\{0\}, \{\gamma_1, \ldots, \gamma_n\})$ where 0 is the identity and $\gamma_1, \ldots, \gamma_n$ the generators of a free commutative group. The *inverse* of a commutative graph is the commutative graph we obtain by reversing the direction of the paths. When we consider the union of a suitably chosen independent addition graph and the inverse of another suitably independent addition graph, we see that the bound in Theorem 7.3 cannot be improved much.

8. Further remarks about sumsets. We conclude the paper by discussing Theorem 2.3 in the context of set addition. Let A and B be finite sets in an abelian group. We wish to apply Theorem 2.3 to the addition graph $G_+(A, B)$. Note that in this context $\mathrm{Im}^{(i)}(Z) = Z + iB$ for any $Z \subseteq A$. There is no reason why $D_1(G_+(A, B)) = |A + B|/|A|$ and so we pick $\emptyset \neq X \subseteq A$ such that $|X + B| = D_1(G_+(A, B))|X|$. Applying Theorem 2.3 to the addition graph $G_+(X, B)$ (the details can be found below in the proof of Corollary 8.1) gives

$$|X + hB| \leq D_1(G_+(A, B))^h |X| = \left(\frac{|X + B|}{|X|}\right)^h |X|.$$

The bound holds for all h. The traditional form of Plünnecke's inequality does not guarantee that the same X works for all h. The key property of X which allows this is that for all $\emptyset \neq Z \subseteq X$ we have

$$\frac{|X + B|}{|X|} \leq \frac{|Z + B|}{|Z|}.$$

This property of the suitably chosen subset X was extended further in [Pe]. It was shown there that X has an even stronger property,

$$|S + X + B| \leq \frac{|X + B|}{|X|}|S + X| \tag{8.1}$$

for any finite set S. The inequality can also be extended to not necessarily commutative groups.

Theorem 2.3 has a longer proof than (8.1) (one has to first establish Plünnecke's inequality), but on the other hand is much more general, as it applies to commutative and not just to addition graphs. For example it allows one to work in restricted addition graphs and/or compare $|V_h|/|V_0|$ to $|V_j|/|V_0|$ for any $1 \leq j \leq h$. As an illustration we present the following application, which is a variation on Ruzsa's restricted addition graphs.

Corollary 8.1. *Let h be a positive integer and X, B and J be finite sets in a commutative group with $J \cap X = \emptyset$. Suppose that*

$$\frac{|(X + jB) \setminus (J + jB)|}{|X|} = \alpha^j$$

for some $1 \le j \le h$, and

$$\frac{|(X + jB) \setminus (J + jB)|}{|X|} \le \frac{|Z + jB) \setminus (J + jB)|}{|Z|}$$

for all $\emptyset \ne Z \subseteq X$. Then

$$|(X + hB) \setminus (J + hB)| \le \alpha^h |X|.$$

Proof. Let H be the commutative subgraph of $G_+(X, B)$ that consists of all paths that end in $(X + hB) \setminus (J + hB)$. The layers of H are $V_0 = X$ and $V_i = (X + iB) \setminus (J + iB)$ for $i > 1$. For $Z \subseteq V_0 = A$ we have $\operatorname{Im}(Z) = (Z + iB) \setminus (J + iB)$. Thus the condition on X is equivalent to

$$D_j(H) = \frac{|V_j|}{|V_0|} = \alpha^j.$$

Theorem 2.3 gives the desired bound on $|V_h| = |(X + hB) \setminus (J + hB)|$. ∎

Christian Reiher [Re] has obtained a generalisation of the corollary in the spirit of (8.1). He has shown that under the same assumptions on X, B, J and α the following inequality holds for all finite sets S:

$$|(X + jB + S) \setminus (J + jB + S)| \le \alpha |(X + (j-1)B + S) \setminus (J + (j-1)B + S)|.$$

The proof is relatively short and purely combinatorial. Corollary 8.1 can easily be deduced by induction on h by setting $S = B$.

Reiher's inequality could therefore have been used to derive Theorem 1.3 instead of the material in Section 2. We opted to present the graph-theoretic approach, as Theorem 2.3 may be helpful in other contexts.

Acknowledgements. The research leading to the results of the paper was done while the author was at the University of Cambridge. The author would like to thank Imre Ruzsa for detailed comments that improved the quality of the paper. In particular the proofs of Propositions 4.2 and 5.1 were simplified considerably. Suggestions of Tim Gowers, Ben Green and Peter Keevash have also helped make the paper better.

References

[BB] P. Balister and B. Bollobás, *Projections, entropy and sumsets*, Combinatorica 32 (2012), 125–141.

[B] B. Bukh, *Sums of dilates*, Combin. Probab. Comput. 17 (2008), 627–639.

[GMR08] 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.

[GMR10] K. Gyarmati, M. Matolcsi and I. Z. Ruzsa, *A supperadditivity and submultiplicativity property for cardinalities of sumsets*, Combinatorica 30 (2010), 163–174.

[MMT] M. Madiman, A. W. Marcus and P. Tetali, *Entropy and set cardinality inequalities for partition-determined functions*, Random Structures Algorithms 40 (2012), 399–424.

[N] M. B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer, New York, 1996.

[Pe11] G. Petridis, *Plünnecke's inequality*, Combin. Probab. Comput. 20 (2011), 921–938.

[Pe] G. Petridis, *New proofs of Plünnecke-type estimates for product sets in groups*, Combinatorica, to appear; arXiv:1101.3507.

[Pl] H. Plünnecke, *Eine zahlentheoretische Anwendung der Graphentheorie*, J. Reine Angew. Math. 243 (1970), 171–183.

[Re] C. Reiher, Comments on *A new way of proving sumset estimates*, http://gowers.wordpress.com/2011/02/10/a-new-way-of-proving-sumset-estimates/.

[Ru89] I. Z. Ruzsa, *An application of graph theory to additive number theory*, Sci. Ser. A Math. Sci. (N.S.) 3 (1989), 97–109.

[Ru96] I. Z. Ruzsa, *Sums of finite sets*, in: Number Theory. New York Seminar 1991–1995, D. V. Chudnovsky et al. (eds.), Springer, New York, 1996, 281–293.

[Ru99] I. Z. Ruzsa, *An analog of Freiman's theorem in groups*, Astérisque 258 (1999), 323–326.

[Ru07] 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.

[Ru09] I. Z. Ruzsa, *Sumsets and Structure*, in: Combinatorial Number Theory and Additive Group Theory, Birkhäuser, Basel, 2009, 87–210.

[T1] T. Tao, *Arithmetic Combinatorics* (lecture notes), http://www.math.ucla.edu/~tao/254a.1.03w/notes1.dvi.

[T2] T. Tao, *Tricks Wiki article: The tensor power trick*, http://terrytao.wordpress.com/2008/08/25/tricks-wiki-article-the-tensor-product-trick/.

[TV] T. Tao and V. H. Vu, *Additive Combinatorics*, Cambridge Univ. Press, Cambridge, 2006.

Giorgis Petridis
Department of Mathematics
915 Hylan Building
University of Rochester
RC Box 270138
Rochester NY 14627, U.S.A.
E-mail: giorgis@cantab.net

Received on 8.6.2011
and in revised form on 30.11.2012 (6723)