The Plünnecke–Ruzsa Inequality: An Overview

G. Petridis

Abstract In this expository article we present an overview of the Plünnecke–Ruzsa inequality: the known proofs, some of its well-known applications and possible extensions. We begin with the graph-theoretic setting in which Plünnecke and later Ruzsa worked in. The more purely combinatorial proofs of the inequality are subsequently presented. In the concluding sections we discuss the sharpness of the various results presented thus far and possible extensions of the inequality to the non-commutative setting.

Keywords Sumsets • Plünnecke–Ruzsa inequality

MSC 2010: 11B30

1 Introduction

Cardinality questions about the growth of sum sets lie in the core of additive number theory. For sets A and B in a commutative group $(\Gamma, +)$ their *sum set* is defined by

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

A central concept is that of sets of *small doubling*. That is sets that satisfy $|A + A| \leq \alpha|A|$ for some absolute constant α. In other words the sum set, whose size is trivially bounded from below by $|A|$, is rather small. The key property of sets of small doubling is that the h-iterated sum set, defined inductively by $hA = (h-1)\,A + A$, is also rather small. A slightly more general statement was proved by Plünnecke over forty years ago [15] and later simplified by Ruzsa [18]. For the time being

G. Petridis (✉)
University of Rochester, Rochester, NY, USA
e-mail: giorgis@cantab.net

M.B. Nathanson (ed.), *Combinatorial and Additive Number Theory*, Springer
Proceedings in Mathematics & Statistics 101, DOI 10.1007/978-1-4939-1601-6_16

we only state a corollary, which asserts that under the small doubling condition the *sum-and-difference sets*, defined by

$$kA - \ell A = \{a_1 + \cdots + a_k - a_{k+1} - \cdots - a_{k+\ell} : a_1, \ldots, a_{k+\ell} \in A\} ,$$

have cardinality bounded in terms of α and $|A|$.

Theorem 1 (The Plünnecke–Ruzsa inequality). *Let k and ℓ be positive integers and A be a finite set in a commutative group. Suppose that $|A + A| \leq \alpha|A|$ for a positive real number α. Then*

$$|kA - \ell A| \leq \alpha^{k+\ell}|A| .$$

This inequality has found applications in some of the highlights of additive combinatorics like Ruzsa's proof of Freiman's theorem [20], Gowers' proof of Szemerédi's theorem [3], the Bourgain–Katz–Tao sum-product theorem in finite fields [2], Helfgott's results about growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$ [9] and the Green–Tao inverse theorem for the Gowers 3-uniformity norm [6].

In this expository article we present an overview of the inequality. We do not present new results. Instead emphasis is given in explaining its proofs, applications and extensions. A more detailed and rigorous presentation of specific topics can be found in the rich literature on the subject [11, 22, 28].

The first task is to clarify the name given to the inequality. Plünnecke proved the special case of Theorem 1 concerning sum sets (i.e. when $\ell = 0$) in the late 1960s. In fact he proved an inequality concerning the growth of certain directed layered graphs. Ruzsa simplified Plüennecke's proof in the late 1980s and extended Plünnecke's result to sum-and-difference sets and applied it to a variety of problems. It has thus become costumary to name inequalities similar to Theorem 1 after both Plünnecke and Ruzsa. To remove a potential ambiguity we call *Plünnecke's inequality* the inequality about directed layered graphs and *Plünnecke–Ruzsa inequality* the one about sum-and-difference sets. A third name we ought to mention in this introduction is that of Tao, who has made numerous contributions to the subject.

The remaining sections are organised as follows. In Sect. 2 we present the graph-theoretic approach to studying the growth of sum sets: Plünnecke's inequality and some of its more well-known applications. In Sect. 3 two purely combinatorial approaches are discussed. In Sect. 4 we investigate the sharpness of the various results presented thus far. Finally in Sect. 5 we present some generalisations of the inequality to non-commutative groups.

2 Graph Theory

Plünnecke was interested in improving a result of Erdős on essential components. The reader can consult [11] for a detailed account of Plünnecke's contribution. To achieve this he worked with a class of directed layered graphs that obey a graph-theoretic notion of commutativity. He succeeded in bounding the *magnification ratios* of a directed, layered graph G, which are defined as

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

$\operatorname{Im}^{(i)}(Z)$ is the ith out-neighbourhood of Z and V_0 is the bottom layer of the graph.

Plünnecke discovered that under the commutativity conditions, which are nowadays known as Plünnecke's, the sequence $D_i(G)^{1/i}$ is decreasing. The directed layered graphs that obey these conditions are called *commutative* (or Plünnecke) graphs. In particular Plünnecke proved the following [15].

Theorem 2 (Plünnecke's inequality). *Let G be a commutative graph with $D_h(G) = \Delta^h$. Then $D_i(G) \geq \Delta^i$ for all $1 \leq i \leq h$.*

Notation. To explain Plünnecke's method one has to introduce some notation. 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. Directed edges exist only between V_i and V_{i+1} for $0 \leq i \leq h-1$.

In order to introduce Plünnecke's conditions we briefly recall that given a bipartite undirected graph $G(X, Y)$ we say that a *matching* exists from X to Y if there exist distinct elements $\{y_x : x \in X\}$ in Y such that $xy_x \in E(G)$ for all $x \in X$.

Plünnecke's *upward* condition states that if $uv \in E(G)$, then there exists a matching from $\operatorname{Im}(v)$ to $\operatorname{Im}(u)$ (in the bipartite graph $G(\operatorname{Im}(u), \operatorname{Im}(v))$ where xy is an undirected edge if and only if it is a directed edge in G). Plünnecke's *downward* condition states that if $vw \in E(G)$, then there exists a matching from $\operatorname{Im}^{-1}(v)$ to $\operatorname{Im}^{-1}(w)$ (in the bipartite graph $G(\operatorname{Im}^{-1}(v), \operatorname{Im}^{-1}(w))$ where xy is an undirected edge if and only if it is a directed edge in G). Here $\operatorname{Im}^{(-1)}$ is the in-neighbourhood. A *commutative graph* is a directed layered graph that satisfies both properties.

The most typical example is $G_+(A, B)$, the *addition graph* of two finite sets A and B in a commutative group. This is defined as the directed graph whose ith layer V_i is $A + iB$ and a directed edge exists between $x \in V_{i-1}$ and $y \in V_i$ if and only if $y - x \in B$. We encourage the reader to verify that addition graphs are indeed commutative.

Proof of Plünnecke's Inequality. A direct and transparent proof of Theorem 2 is given in [13]. It was inspired by the simplification of Plunnecke's argument due to Ruzsa that appeared in [18, 19] and in particular by an exposition due to Tao [25]. Here we only present the backbone of the argument.

The key observation, which is due to Plünnecke, is the close relation between magnification ratios and separating sets in G. A *separating set* in G is a set $S \subseteq V(G)$ that intersects all directed paths of maximum length in G. To make the most of this relation one must work with weighted commutative graphs, i.e. a commutative graph with a weight function

$$w : V(G) \mapsto \mathbb{R}^+ .$$

Every vertex in V_i is given the weight Δ^{-i}. The reasons behind this choice will become apparent shortly, but different weights may be more suitable in other applications.

The heart of the proof of Theorem 2 is the following result from [13], which demonstrates how powerful Plünnecke's conditions are.

Lemma 1. *Let C be a positive real and G be a weighted commutative graph with vertex set $V_0 \cup \cdots \cup V_h$ and $w(v) = C^{-i}$ for all $v \in V_i$. A separating set of minimum weight that lies entirely in $V_0 \cup V_h$ exists.*

The proof is based on counting the edges between consecutive layers in two different ways by applying Plünnecke's conditions. A crucial corollary is that no separating set can have smaller weight than V_0.

Corollary 1. *Let G a weighted commutative graph with vertex set $V_0 \cup \cdots \cup V_h$ and $w(v) = \Delta^{-i} = D_h(G)^{-i/h}$ for all $v \in V_i$. The weight of any separating set is at least $|V_0|$.*

Proof. By applying Lemma 1 we can assume that $S_0 \cup S_h$ is a separating set of minimum weight with $S_i \subseteq V_i$. $\mathrm{Im}^{(h)}(V_0 \setminus S_0) \subseteq S_h$, as S is a separating set, and so $|S_h| \geq |\mathrm{Im}^{(h)}(V_0 \setminus S_0)| \geq D_h(G)|V_0 \setminus S_0|$. This in turn implies

$$w(S) = w(S_0) + w(S_h) = |S_0| + |S_h|\, D_h^{-1}(G) \geq |S_0| + |V_0 \setminus S_0| = |V_0|\,. \quad \square$$

Plünnecke's inequality follows in a straightforward manner.

Proof of Theorem 2. We consider any $Z \subseteq V_0$ in the weighted version of G, where each $v \in V_i$ has weight Δ^{-i}. $(V_0 \setminus Z) \cup \mathrm{Im}^{(i)}(Z)$ is a separating set and thus

$$|V_0| \leq w((V_0 \setminus Z) \cup \mathrm{Im}^{(i)}(Z)) = w(V_0 \setminus Z) + w(\mathrm{Im}^{(i)}(Z)) = |V_0| - |Z| + |\mathrm{Im}^{(i)}(Z)|\, \Delta^{-i}.$$

That is, $|\mathrm{Im}^{(i)}(Z)| \geq \Delta^i |Z|$. Taking the minimum over all non-empty $Z \subseteq V_0$ gives the lower bound on $D_i(G)$. $\square$

Applications. Theorem 2 has many applications to additive problems. Theorem 1 is the most widely known. The reader will have to wait for a proof until the next section. In this section we present three other applications that offer a platform to introduce techniques that may be applied to a wider range of problems.

The first is a direct consequence of Theorem 2 when applied to the addition graph $G_+(A, B)$. It asserts that when $|A + B|$ is small compared to $|A|$, then there exists a non-empty subset X of A that grows slowly under repeated addition of B.

Corollary 2. *Let h be a positive integer and A and B be finite non-empty sets in a commutative group. Suppose that $|A + B| \leq \alpha |A|$ for a positive real number α. Then there exists $\emptyset \neq X \subseteq A$ such that*

$$|X + hB| \leq \alpha^h |X|\,.$$

In particular

$$|hB| \leq \alpha^h |A| \;.$$

Proof. We apply Theorem 2 to the commutative graph $G_+(A, B)$ and observe that

$$D_1(G_+(A,B)) \leq \frac{|V_1|}{|V_0|} = \frac{|A+B|}{|A|} \leq \alpha \;.$$

The existence of a suitable non-empty subset X of A follows from the definition of the hth magnification ratio. The second conclusion is immediate at $hB \subseteq X + hB$ and $X \subseteq A$. □

On first sight adding the same set repeatedly appears to be necessary. Ruzsa lifted this restriction in [18] and extended Corollary 2 to different summands.

Corollary 3. *Let h be a positive integer and A and $B_1, \ldots, B_h$ be finite non-empty sets in a commutative group. Suppose that $|A + B_i| \leq \alpha_i |A|$ for a positive rational number α_i for all $1 \leq i \leq h$. Then there exists $\emptyset \neq X \subseteq A$ such that*

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

The proof is not as straightforward as the one above. One has to find a suitable replacement for $G_+(A, B)$. The details of the method of proof can be found in [7], where the interested reader can also find more general versions of Corollary 3. We only present the key concepts for the special case when $h = 2$.

We consider a graph G with vertex set $V_0 \cup V_1 \cup V_2$. V_0 is taken to be A, V_1 the disjoint union of $U_1 := A + B_1$ and $U_2 := A + B_2$ (so that if an element $\gamma \in \Gamma$ lies in the intersection $(A + B_1) \cap (A + B_2)$, then it appears twice in V_1) and $V_2 = A + B_1 + B_2$. The edges of G are drawn as follows: an edge xy exists from V_1 to U_1 if $y - x \in B_1$; from V_1 to U_2 if $y - x \in B_2$; from U_1 to V_2 if $y - x \in B_2$; and from U_2 to V_2 if $y - x \in B_1$.

We begin with the special case where $\alpha_1 = \alpha_2 = \alpha$. The graph G is commutative and so one can apply Theorem 2 like in the proof of Corollary 2.

$$D_1(G) \leq \frac{|V_1|}{|V_0|} = \frac{|A+B_1| + |A+B_2|}{|A|} \leq 2\alpha \;.$$

Thus there exists a non-empty subset X of A such that $|X + B_1 + B_2| = |\operatorname{Im}^{(2)}(X)| \leq 4\alpha^2 |X|$. To eliminate the factor of 4 one has to use the multiplicativity of magnification ratios ([18]) and the tensor product trick (e.g. [26]).

For the case when $\alpha_1 \neq \alpha_2$ an integer k is chosen with the property that both $k_1 := k\,\alpha_1$ and $k_2 := k\,\alpha_2$ are also integers. One then applies the special case to the commutative group $\Gamma \times C_{k_1} \times C_{k_2}$ (here C_n is the cyclic group of order n as usual) and the sets $A' = A \times \{0\} \times \{0\}$, $B_1' = B_1 \times \{0\} \times C_{k_2}$ and $B_2' = B_2 \times C_{k_1} \times \{0\}$.

The two applications we have seen so far concern the growth of a non-empty subset of A under repeated set addition. Theorem 2 does not allow one to immediately deal with the whole of, say, $A+hB$. The difference is not as superficial as it may first seem. There are examples, essentially due to Ruzsa [14], which show that for infinitely many and arbitrarily large values of α there exist examples of Γ, A and B where $|A+B| \leq \alpha|A|$ and

$$|A+hB| \geq c_h \alpha^h |A|^{2-1/h} \tag{1}$$

for some constant c_h. c_h depends on h, which is assumed to be fixed, and can be thought to be h^{-h-1}. These examples contrast Corollary 2 where the exponent of $|A|$ is 1. Theorem 2 can nonetheless be employed to bound $|A+hB|$ in terms of α, $|A|$ and h. This was implicitly done by Ruzsa in [21] resulting in an upper bound that agrees with (1) on its dependence on α and $|A|$.

Corollary 4. *Let h be a positive integer and A and B finite sets in a commutative group. Suppose that $|A+B| \leq \alpha|A|$ for some positive real number α. Then*

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

An outline of the proof goes as follows. A is partitioned into $A_1 \cup A_2$, where A_1 can be thought of as a large and slow-growing part of A under repeated set addition of B and A_2 a small and fast-growing part. We have

$$|A+hB| \leq |A_1+hB| + |A_2+hB| \ .$$

The first term $|A+hB|$ is bounded above by repeated applications of Theorem 2. We start with a non-empty subset $X_1 \subseteq A$ such that $|X_1+hB| \leq \alpha^h|X_1|$. Theorem 2 is then applied to the addition graph $G_+(A \setminus X_1, B)$. This yields a non-empty subset $X_2 \subseteq A \setminus X_1$ such that

$$|X_2+hB| \leq \left(\frac{|A+B|}{|A \setminus X_1|}\right)^h |X_2| \leq \left(\frac{\alpha|A|}{|A \setminus X_1|}\right)^h |X_2| \ .$$

The process is repeated enough times until $X_1 \cup X_2 \cup \ldots$ is sufficiently large and is sometimes called in the literature ‘Plünnecke’s inequality for a large subset’. The second term is bounded above by Corollary 2:

$$|A_2+hB| \leq |A_2|\,|hB| \leq \alpha^h \, |A|\,|A_2| \ .$$

The details of the calculation are very similar to the material in [21] and are not presented here. Gyarmati, Matolcsi and Ruzsa used this strategy in [7, 8] to prove results of a similar kind. By refining it one can improve the upper bound of

Corollary 4 slightly. This is done in [14] where an additional dependence on h is inserted. It is shown that

$$|A + hB| \le \frac{e}{h^2}\alpha^h\,|A|^{2-1/h} + O(\alpha^h|A|^{2-2/(h+1)})\ . \tag{2}$$

It should be noted that Corollary 4 can also be derived by an inequality established by Balister and Bollobás [1] and Madiman, Marcus and Tetali [10] by entirely different means.

3 Combinatorics

The graph-theoretic proof of Corollary 2 requires the introduction of commutative graphs. It is natural to ponder whether a more direct proof can be found, one confined to the world of commutative groups and their sum sets. Tao was the first to give such a proof more than thirty years after Plünnecke's paper appeared. A detailed account can be found in [5, 28]. We only sketch it here and focus on the tools used by Tao as they are often useful in additive problems and can effectively be combined with or replace Theorem 2.

The first tool is Ruzsa's *covering lemma*. Roughly speaking it asserts that when $|A + B|$ is small compared to $|A|$, then B can be covered by a few translates of $A - A$.

Lemma 2 (Covering lemma). *Let U and V be finite sets in a commutative group. Suppose that $|U + V| \le \alpha|U|$ for some positive real number α. Then there exists a subset $S \subseteq V$ of size at most α such that*

$$V \subseteq S + U - U\ .$$

The proof is remarkably elegant as one can simply choose S to be a maximal subset of V subject to the constrain $(s + U) \cap (s' + U) = \emptyset$ for all $s \ne s' \in S$. Applying the lemma to $U = A$ and $V = A - 2A$ one gets a subset $S \subseteq A - 2A$ of size at most $|2A - 2A|/|A|$ such that $2A - A \subseteq S + A - A$ and recursively that

$$kA - \ell A \subseteq kS - \ell S + A - A\ . \tag{3}$$

It follows that

$$|kA - \ell A| \le |S|^{k+\ell}\,|A - A| \le \left(\frac{|2A - 2A|}{|A|}\right)^{k+\ell} |A - A|\ . \tag{4}$$

The results we have presented thus far tell us nothing about the difference set of a set of small doubling. In order to pass from upper bounds on sum sets to upper bounds to difference sets one needs the so-called Ruzsa triangle inequality [17].

Lemma 3 (Triangle inequality). *Let U, V and W be finite sets in a commutative group. Then*

$$|V - W| \leq \frac{|U + V|\,|U + W|}{|U|}\ .$$

This lemma also has an elegant proof based on constructing an injection from $U \times (V - W)$ into $(U + V) \times (U + W)$. Setting $U = V = W = A$ we see that sets of small doubling have a small difference set. In particular $|A + A| \leq \alpha|A|$ implies $|A - A| \leq \alpha^2|A|$. To deal with the remaining term in (4) Tao used a covering lemma similar to Lemma 2 and thus obtained an entirely combinatorial proof of the Plünnecke–Ruzsa inequality, albeit with a slightly worse dependence on α.

A second purely combinatorial proof was given in [12]. The key result is the following.

Lemma 4. *Let A and B be finite sets in a commutative group. Suppose that $|A + B| \leq \alpha|A|$ for some positive real number α. Then there exists $\emptyset \neq X \subseteq A$ such that*

$$|X + B + C| \leq \alpha|X + C|$$

for all finite sets C in the ambient group.

The key idea in the proof is to choose X carefully and then perform induction on $|C|$. An eloquent presentation by Gowers can be found in [4]. X is chosen as to minimise the quantity $|X + B|/|X|$ over all non-empty subsets of A. In other words

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

holds for all non-empty $Z \subseteq A$.

The fact that the same X works for all C is new to this particular method of proof and is useful in applications. As a demonstration we derive Theorem 1. Choosing X as in the statement of Lemma 4 gives

$$|X + hB| = |X + B + (h-1)B| \leq \alpha|X + (h-1)B|\ .$$

Corollary 2 follows by induction on h. It is crucial to note that the same X works for different values of h. With this in mind we turn to Lemma 3.

$$|kA - \ell A| \leq \frac{|X + kA|\,|X + \ell A|}{|X|} \leq \frac{\alpha^{k+\ell}|X|^2}{|X|} \leq \alpha^{k+\ell}|A|\ .$$

Using the lemma also simplifies slightly the proof of Theorem 1.2 in [24]. Sanders' paper is noteworthy as to the best of our knowledge is the only instance where Corollary 2 is applied for large h, h in fact tends to infinity as $|A|$ gets arbitrarily large.

Reiher has obtained combinatorial proofs for some stronger forms of corollaries of Theorem 2. His results appear as comments to Gowers' blogpost [16]. Reiher's results are to these corollaries of the graph-theoretic method what Lemma 4 is to Corollary 2. The method of proof is the same: a suitable subset X is chosen and this forms the base of an inductive argument.

4 Sharpness of the Various Inequalities

Given the widespread use of the results presented so far it is natural to investigate their sharpness. Let us begin with Theorem 2. It was shown in [13] that for all $\varDelta \in \mathbb{Q}^+$ and all $h \in \mathbb{Z}^+$ there exists a commutative graph G with magnification ratios $D_i(G) = \varDelta^i$ for all $1 \leq i \leq h$. Lemma 4 is likewise sharp. Let A, B and T be finite groups and $\varGamma = A \times B \times T$. Take $A' = A \times \{0\} \times \{0\}$ and $B' = \{0\} \times B \times \{0\}$. Then $\alpha = |B|$ and for any subset $X' = X \times \{0\} \times \{0\}$ of A' and set $C' = \{0\} \times \{0\} \times C$ in $\varGamma$ we have

$$|X' + B' + C'| = |X|\,|B|\,|C| = \alpha |X' + C'|\,.$$

Similar considerations show that Corollary 3 is sharp.

When the same set is added repeatedly the outlook changes slightly. We have already noted that Corollary 4 gives the correct order of magnitude in α and $|A|$. It is however expected that the examples giving rise to (1) are closer to the truth. In other words we have the correct dependence in α and $|A|$, but not in h. The upper bound in (2) is a step in the right direction, but the gap to be bridged remains large.

The upper bounds in Theorem 1 and Corollary 2 have a similar quality: they are sharp in their dependence in α and $|A|$, but probably not in respectively k, ℓ and h. A distinction has to be made as taking $\alpha = 1$ forces a subgroup structure and the upper bounds are attained. For larger values of α one can construct nearly extremal examples using products of groups. We focus on Corollary 2. Let $\varGamma_1$ be any finite commutative group and $\varGamma_2$ a free commutative group generated by $\{\gamma_1, \ldots, \gamma_n\}$ and $\varGamma = \varGamma_1 \times \varGamma_2$. Now set $A = \varGamma_1 \times \{0\}$ and $B = \{0\} \times \{\gamma_1, \ldots, \gamma_n\}$. Then $\alpha = n$ and for all subsets $X \subseteq A$ we have

$$|X + hB| \leq \binom{n+h-1}{h} |X| = \binom{\alpha+h-1}{h} |X|\,.$$

It is suspected that a bound of this form (crucially correct for $\alpha = 1$) must be closer to the truth than Plünnecke's. To prove such a bound one cannot solely rely on existing tools. One must use in an essential way the fact that the same set is added repeatedly. Ruzsa has partly achieved this for the important special case when $A = B$. Setting $k = h$ and $\ell = 0$ in (3) and combining Theorem 1 with the elementary estimate

$$|hS| \leq \binom{|S| + h - 1}{h} ,$$

which holds for any set S in a commutative group, gives

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

This type of bound is of the correct order of magnitude in $|A|$ and has a much better dependence on h, but no longer on α. Proving a bound that combines the best of both worlds would be of interest to the author.

5 The Non-commutative Setting

The results we have presented hold in any commutative group. Once commutativity is no longer assumed the outlook changes. To stress the difference we symbolise the group operation with $\cdot$ instead of $+$ and consider *product sets*

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

In this setting some of the results presented in Sect. 2 and Sect. 3, like Lemma 2 and Lemma 3, carry over [9,27]. On the other hand the Plünnecke–Ruzsa inequality need not hold. This is hardly unexpected given some results on the growth of product sets in specific non-commutative groups. Helfgott has for example shown that for all $A \subseteq SL_2(\mathbb{Z}/p\mathbb{Z})$, which are not subgroups and satisfy $|A| < p^{3-\delta}$ for some absolute $\delta > 0$, we have $|A \cdot A \cdot A| \geq |A|^{1+\varepsilon}$ for some $\varepsilon > 0$ depending only on δ [9]. A non-commutative Plünnecke inequality would imply that for a set of small doubling $|A \cdot A \cdot A|$ is comparable to $|A|$. One can nevertheless generalise Corollary 2 by introducing further conditions, which are trivial in the commutative setting, but nevertheless allow one to obtain Plünnecke-type upper bound for product sets.

Ruzsa was the first to suggest how a non-commutative Plünnecke inequality might look like (e.g. in [21]).

Question 1. Does there exist an absolute constant c with the following property: let h be a positive integer and A and B finite non-empty sets in a group that satisfy $|A \cdot B| \leq \alpha|A|$ and $|A \cdot b \cdot B| \leq \alpha|A|$ for all $b \in B$ for some positive real number α; then there exists $\emptyset \neq X \subseteq A$ such that

$$|X \cdot B^h| \leq \alpha^{ch}|X| ?$$

It follows from the non-commutative analogue of Lemma 3 that it is enough to establish the upper bound for $h = 2$ [9, 23, 27]. Tao answered Ruzsa's question for the special case when $A = B$ [27].

Theorem 3 (Tao). *Let A be a finite non-empty set in a group. Suppose that $|A \cdot A| \leq \alpha|A|$ and $|A \cdot a \cdot A| \leq \alpha|A|$ for all $a \in A$ and some positive real number α. Then there exists an absolute constant c' such that*

$$|A \cdot A \cdot A| \leq \alpha^{c'}|X| .$$

It was shown in [12] that c' can be taken to be 9. The proof uses the noncommutative analogues of Lemma 2 and Lemma 3 and a non-commutative generalisation of Corollary 3 due to Ruzsa [23]. Ruzsa observed that the method of proof of the corollary still applies to general groups provided that A is placed in the middle of the triple product.

Theorem 4 (Ruzsa). *Let A, B_1 and B_2 be finite non-empty sets in a group. Suppose that $|B_1 \cdot A| \leq \alpha_1|A|$ and that $|A \cdot B_2| \leq \alpha_2|A|$ for positive real numbers α_1 and α_2. Then there exists $\emptyset \neq X \subseteq A$ such that*

$$|B_1 \cdot X \cdot B_2| \leq \alpha_1\alpha_2|X| .$$

To prove Theorem 3 we set $B_1 = B_2 = A$ and select such a subset X of A. By the analogue of Lemma 2 there exists a subset S of A of size at most $|X \cdot A|/|A| \leq |A \cdot X \cdot A|/|A| \leq \alpha^2$ such that $A \subseteq X^{-1} \cdot X \cdot S$. It follows that

$$|A \cdot A \cdot A| \leq |A \cdot X^{-1} \cdot X \cdot S \cdot A| .$$

By the non-commutative analogue of Lemma 3 the above becomes

$$|A \cdot A \cdot A| \leq |A \cdot X^{-1} \cdot X \cdot A|\frac{|A \cdot S \cdot A|}{|A|} .$$

The second term is at most

$$\sum_{s \in S} \frac{|A \cdot s \cdot A|}{|A|} \leq |S|\alpha \leq \alpha^3 .$$

To finish off the proof of Theorem 3 one must bound the first term by $\alpha^6|A|$. This can be achieved by a repeated application of the non-commutative analogue of Lemma 3 and an application of Theorem 4. Details can be found in [12].

Lemma 4 can also be generalised to the non-commutative setting provided that A is placed in the middle of the triple product.

Lemma 5. *Let A and B be finite non-empty sets in a group. Suppose that $|A \cdot B| \leq \alpha|A|$ for some positive real number α. Then there exists $\emptyset \neq X \subseteq A$ such that*

$$|C \cdot X \cdot B| \leq \alpha|C \cdot X|$$

for all finite sets C in the ambient group.

The method of proof as described in Sect. 3 still applies.

Acknowledgements The author would like to thank Seva Lev, Mel Nathanson and Tom Sanders for their encouragement.

References

1. P. Balister, B. Bollobás, Projections, entropy and sumsets. Combinatorica **32**, 125–141 (2012)
2. J. Bourgain, N. Katz, T. Tao, A sum-product estimate in finite fields, and applications. Geom. Funct. Anal. **14**, 27–57 (2004)
3. W.T. Gowers, A new proof of Szemerédi's theorem. Geom. Funct. Anal. **11**, 465–588 (2001)
4. W.T. Gowers, A new way of proving sumset estimates (2011), http://gowers.wordpress.com/2011/02/10/a-new-way-of-proving-sumset-estimates/
5. A. Granville, An introduction to additive combinatorics, in *Additive Combinatorics*, ed. by A. Granville, M.B. Nathanson, J. Solymosi. CRM Proceedings and Lecture Notes (American Mathematical Society, New York, 2007), pp. 1–27
6. B.J. Green, T. Tao, An inverse theorem for the Gowers $U^3(G)$ norm. Proc. Edin. Math. Soc. (2) **51**(1), 75–153 (2008)
7. K. Gyarmati, M. Maltolcsi, I.Z. Ruzsa, Plünnecke's inequality for different summands, in *Building Bridges: Between Mathematics and Computer Science*, ed. by M. Grötschel, G.O.H. Katona. Bolyai Society Mathematical Studies, vol. 19 (Springer, New York, 2008), pp. 309–320
8. K. Gyarmati, M. Maltolcsi, I.Z. Ruzsa, A superadditivity and submultiplicativity property for cardinalities of sumsets. Combinatorica **30**(2), 163–174 (2010)
9. H.A. Helfgott, Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$. Ann. Math. **167**, 601–623 (2008)
10. M. Madiman, A.W. Marcus, P. Tetali, Entropy and set cardinality inequalities for partition-determined functions, with applications to sumsets. Random Structures Algorithms **40**, 399–424 (2012)
11. M.B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets* (Springer, New York, 1996)
12. G. Petridis, New proofs of Plünnecke-type estimates for product sets in groups. Combinatorica **32**, 721–733 (2012)
13. G. Petridis, Plünnecke's inequality. Combin. Probab. Comput. **20**, 921–938 (2011)
14. G. Petridis, Upper bounds on the cardinality of higher sumsets. Acta Arith. **158**, 299–319 (2013)
15. H. Plünnecke, Eine zahlentheoretische anwendung der graphtheorie. J. Reine Angew. Math. **243**, 171–183 (1970)
16. C. Reiher, Comments on 'A new way of proving sumset estimates' by Gowers, W.T. (2011), http://gowers.wordpress.com/2011/02/10/a-new-way-of-proving-sumset-estimates/
17. I.Z. Ruzsa, On the cardinality of $A + A$ and $A - A$, in *Combinatorics (Keszthely 1976)*, ed. by A. Hajnal, V.T. Sós. Coll. Math. Soc. J. Bolyai, vol. 18 (North Holland, Amsterdam, 1978), pp. 933–938

18. I.Z. Ruzsa, An application of graph theory to additive number theory. Scientia Ser. A **3**, 97–109 (1989)
19. I.Z. Ruzsa, Addendum to: an application of graph theory to additive number theory. Scientia Ser. A **4**, 93–94 (1990/1991)
20. I.Z. Ruzsa, Generalized arithmetical progressions and sumsets. Acta Math. Hungar. **65**(4), 379–388 (1994)
21. I.Z. Ruzsa, Cardinality questions about sumsets, in *Additive Combinatorics*, ed. by A. Granville, M.B. Nathanson, J. Solymosi. CRM Proceedings and Lecture Notes (American Mathematical Society, New York, 2007), pp. 195–205
22. I.Z. Ruzsa, Sumsets and structure, in *Combinatorial Number Theory and Additive Group Theory* (Springer, New York, 2009)
23. I.Z. Ruzsa, Towards a noncommutative Plünnecke-type inequality, in *An Irregular Mind Szemeredi is 70*, ed. by I. Bárány, J. Solymosi. Bolyai Society Mathematical Studies, vol. 21 (Springer, New York, 2010), pp. 591–605
24. T.W. Sanders, Green's sumset problem at density one half. Acta Arith. **146**(1), 91–101 (2011)
25. T. Tao, Additive combinatorics. http://www.math.ucla.edu/~tao/254a.1.03w/notes1.dvi
26. T. Tao, The tensor power trick. http://terrytao.wordpress.com/2008/08/25/tricks-wiki-article-the-tensor-product-trick/
27. T. Tao, Product set estimates for non-commutative groups. Combinatorica **28**(5), 574–594 (2008)
28. T. Tao, V.H. Vu, *Additive Combinatorics* (Cambridge University Press, Cambridge, 2006)