REPORTS@SCM

AN ELECTRONIC JOURNAL OF THE
SOCIETAT CATALANA DE MATEMÀTIQUES

Explicit bounds for growth of sets in non-abelian groups

*Alberto Espuny Díaz
Universitat Politècnica de Catalunya
alberto.espuny@estudiant.upc.edu
*Corresponding author

Resum *(CAT)*

Les desigualtats de Plünnecke–Ruzsa proporcionen fites superiors del creixement de les sumes iterades d'un conjunt en un grup abelià. Aquesta mena de resultats han estat estesos recentment per Petridis i per Tao al cas no abelià. El resultat principal d'aquest treball és una demostració de la desigualtat de Plünnecke–Ruzsa pel cas no abelià que no fa servir el mètode de Petridis. També s'obtenen resultats anàlegs pel cas del producte iterat de dos conjunts diferents.

Abstract *(ENG)*

The Plünnecke–Ruzsa inequalities give upper bounds for the growth of iterated sumsets in an abelian group. These inequalities have been recently extended to the non-abelian case by Petridis and by Tao. The main result in this work is a proof of the non-abelian Plünecke–Ruzsa inequalities which makes no use of the method introduced by Petridis. Analogous inequalities for iterated products of two distinct sets are also obtained.

Keywords: *Additive combinatorics, combinatorial number theory, growth in groups.*
MSC (2010): *Primary 11B13, 11B30, 11P70. Secondary 20D60.*
Received: *December 2, 2015.*
Accepted: *December 31, 2016.*

Acknowledgement

The author was partially supported by grant 2015/COLAB/00069 of the Spanish Ministerio de Educación, Cultura y Deporte. He would also like to thank Profs. Juanjo Rué and Oriol Serra for their many insightful suggestions, as well as the anonymous referee, whose comments and remarks greatly improved the final version of this paper.

Societat Catalana de Matemàtiques

Institut d'Estudis Catalans

1. Introduction

The theory of set addition was initiated by Freiman [2] in the 1960's in the context of abelian groups. More recently, a lot of effort has been directed at extending this theory to the non-abelian case, as well as searching for connections between this and many other areas of mathematics, such as Lie group theory, number theory, or probability theory; see [1, 3]. In this context, the group operation is usually referred to as set multiplication, instead of set addition. The product of two sets is defined as

$$AB = \{ab \mid a \in A,\ b \in B\}.$$

One can also define iterated product sets recursively, and define the inverse of a set as the set of the inverses. Note that the inverse of a set has the same size as the set itself.

One of the most basic and important problems in this setting is bounding the growth of iterated product sets. Some trivial tight bounds can be found, but a more interesting problem arises when bounding iterated product sets, given a bound for the base product set $|AA| \leq \alpha|A|$. In this sense, the first important result is Plünnecke's inequality, which was first proved in Plünnecke [5] in the late 1960's, and has become one of the most commonly used tools in additive combinatorics. His proof is based on a graph-theoretic method, using what he called *commutative graphs* in order to obtain the following result.

Theorem 1.1 (Plünnecke's inequality)**.** *Let j, h be two non-negative integers such that $j < h$, and let A and B be finite sets in a commutative group. Assume that $|A| = m$ and $|AB^j| = \alpha m$. Then, there exists a non-empty set $X \subseteq A$ such that $|XB^h| \leq \alpha^{\frac{h}{j}}|X|$.*

The proof is simple in its technical parts, but long and arduous. Variations of this proof have been used to prove some more general results.

Ruzsa [6] rediscovered Plünnecke's work by providing a proof based on Menger's theorem on graph theory, and used some of his own techniques to obtain some more general results. One of the most important states as follows.

Theorem 1.2 (Plünnecke–Ruzsa inequality)**.** *Let A and B be finite sets in a commutative group, and j be a positive integer. Assume that $|BA^j| \leq \alpha|B|$. Then, for any nonnegative integers k and l such that $j \leq \min\{k, l\}$, we have that $|A^l A^{-k}| \leq \alpha^{\frac{k+l}{j}}|B|$.*

The main limitation of these results is that they only hold in abelian groups (in fact, it is usual to write them using additive notation). Furthermore, one can find counterexamples for an extension to the non-commutative case. The only exception to this rule is when considering triple product sets; in this case, Plünnecke's graph-theoretic method can be used to obtain some results (see, for instance, Section 2). For this reason, finding statements that resemble those of Plünnecke and Ruzsa and hold in the non-commutative setting recently became an interesting problem.

Under these circumstances, Tao was the first to realise, in the late 2000's, that one has to impose a further restriction on the sets under consideration. In some sense, it is enough to see that the growth of triple products of a set is bounded, $|AAA| \leq \alpha|A|$, in order to bound all its iterated product sets. He also proved that one can weaken this condition to $|AaA| \leq \alpha|A|$ for every $a \in A$, and a bound for any product sets of A can be given. His more general theorem in this setting can be stated as follows.

Theorem 1.3 (Tao, [10]). *Let A be a finite set in a group. Assume that $|AaA| \leq \alpha|A|$ for every $a \in A$, and that $|AA| \leq \alpha|A|$. Then, there exists some absolute constant c such that, for any signs $\epsilon_1, \dots, \epsilon_h \in \{-1, 1\}$, $|A^{\epsilon_1}A^{\epsilon_2} \cdots A^{\epsilon_h}| \leq \alpha^{ch}|A|$.*

Setting all the signs to be equal in Theorem 1.3, one obtains the following corollary.

Corollary 1.4. *Let A be a finite set in a group such that $|AaA| \leq \alpha|A|$ for every $a \in A$, and $|AA| \leq \alpha|A|$. Then, there is an absolute constant c such that $|A^h| \leq \alpha^{ch}|A|$.*

In 2011, Petridis presented a new method to prove estimates of the growth of product sets; see [4]. With his new technique, he was able to give an elementary proof of Plünnecke's inequality and several other results. He also used his method to give a specific value to the absolute constant in Corollary 1.4.

Theorem 1.5 (Petridis). *Let A be a finite set in a group. Suppose that $|AA| \leq \alpha|A|$ and $|AaA| \leq \beta|A|$ for every $a \in A$. Then, for all $h > 2$, $|A^h| \leq \alpha^{8h-17}\beta^{h-2}|A|$.*

In the statement of Tao's theorem we had $\alpha = \beta$ so, Petridis's result gives a constant $c = 9$ as an upper bound for c. The same approach using Petridis's new method serves to obtain bounds in similar settings, when considering more than one set.

In this paper, we work with the growth of sets under multiplication in the non-commutative setting, and with results similar to Theorem 1.3 and Theorem 1.5. In particular, one of the results is a weaker version of Theorem 1.5 that can be obtained without reference to Petridis's new method, and hence could have been developed before.

Theorem 1.6. *Let A be a finite set in a group such that $|AA| \leq \alpha|A|$ and $|AaA| \leq \beta|A|$, for every $a \in A$. Then, for any $h > 2$, $|A^h| \leq \alpha^{9h-19}\beta^{h-2}|A|$.*

Additionally, we use Theorem 1.5 in order to obtain estimates for the size of iterated products of two different sets. We also exploit it in order to give a specific value for the constant c in Theorem 1.3.

Theorem 1.7. *Let A be a non-empty finite set in a group such that $|AA| \leq \alpha|A|$ and $|AaA| \leq \beta|A|$, for every $a \in A$. Then, for any signs $\epsilon_1, \dots, \epsilon_h \in \{-1, 1\}$, $|A^{\epsilon_1}A^{\epsilon_2} \cdots A^{\epsilon_h}| \leq \alpha^{8h-15}\,\beta^{h-2}|A|$.*

The remainder of this paper is divided in the following way. In Section 2 we present the three results that are needed in order to obtain our new results. In Section 3 we use these results to present the proof of Theorem 1.6, and use it to give a specific value to the constant in Corollary 1.4. Finally, in Section 4 we use Theorem 1.5 and the tools from Section 2 to prove Theorem 1.7. Furthermore, we prove several results when considering the product of two different sets.

2. Tools

In this section we present the tools needed for the proofs of the results of Sections 3 and 4. Two of them are elementary, and their proofs are presented here for the sake of completeness. The third one is a non-commutative theorem by Ruzsa, which cannot be proved without a thorough presentation of the graph-theoretic method designed by Plünnecke. An account of its proof can be found, for example, in [9].

The first versions of the tools we present here were developed specifically for the abelian case. However, they could easily be extended to the non-commutative setting. The first of these tools is known as Ruzsa's triangle inequality.

Theorem 2.1 (Ruzsa's triangle inequality, [7]). *Let X, Y and Z be finite non-empty sets in a (not necessarily commutative) group. Then, $|X||YZ^{-1}| \leq |YX^{-1}||XZ^{-1}|$.*

Proof. The idea of the proof is to find an injection of $X \times (YZ^{-1})$ into $(YX^{-1}) \times (XZ^{-1})$. Since the sizes of these sets are $|X||YZ^{-1}|$ and $|YX^{-1}||XZ^{-1}|$, respectively, this yields the result.

Consider the following map:

$$\begin{aligned} \varphi\colon X \times (YZ^{-1}) &\longrightarrow (YX^{-1}) \times (XZ^{-1}) \\ (x, yz^{-1}) &\longmapsto (yx^{-1}, xz^{-1}). \end{aligned}$$

We would like to see that this is an injection. First, observe that an element $yz^{-1} \in YZ^{-1}$ may come from different elements $y, y' \in Y$ and $z, z' \in Z$ such that $yz^{-1} = y'z'^{-1}$. Hence, we must first fix a representation in Y, Z for each element of YZ^{-1}. We do so by defining an injection $f\colon YZ^{-1} \longrightarrow Y \times Z$ such that $f(a)_Y f(a)_Z^{-1} = a$ for every $a \in YZ^{-1}$, where $f(a)_Y$ denotes the first coordinate of $f(a)$, and $f(a)_Z$ denotes the second. Such an injection exists because of the definition of the set YZ^{-1}. For example, if we give the elements of Y some order $y_1 < y_2 < \cdots < y_k$, we could map a to the pair (y_i, z_j) such that $y_i z_j^{-1} = a$ and the index i is minimum.

Now, assume that $\varphi(x, a) = \varphi(x', a')$. Then, $f(a)_Y x^{-1} = f(a')_Y x'^{-1}$ and $xf(a)_Z^{-1} = x'f(a')_Z^{-1}$ and, multiplying these two equalities, we get that $f(a)_Y f(a)_Z^{-1} = f(a')_Y f(a')_Z^{-1}$. By definition of f, this means that $a = a'$. Substituting this in the former equations yields $x = x'$ so, φ is an injection. □

The second tool is the simplest of a group of results known as covering lemmas.

Lemma 2.2 (Ruzsa's covering lemma, [8]). *Let A and B be finite sets in a group G. Assume that $|AB| \leq \alpha|A|$. Then, there exists a non-empty set $S \subseteq B$ such that $|S| \leq \lfloor \alpha \rfloor$ and $B \subseteq A^{-1}AS$.*

Proof. The proof follows from choosing $S \subseteq B$ in the right way. Select S to be maximal subject to As_1 being disjoint with As_2 for every pair $s_1, s_2 \in S$. This is equivalent to choosing S to be maximal subject to $|AS| = |A||S|$ being true.

Now, take $b \in B$. We distinguish two possible cases: if $b \in S$ then, for any $a \in A$, we have that $b = a^{-1}ab \in A^{-1}AS$. Otherwise, $b \notin S$, and b cannot be added to S without breaking the maximality condition so, there must be an element $s \in S$ such that $Ab \cap As \neq \varnothing$; equivalently, there exist some elements $s \in S$, $a, a' \in A$ such that $ab = a's$ hence, $b = a^{-1}a's \in A^{-1}AS$. □

Finally, Ruzsa's non-commutative bound for the product set of three sets in a non-commutative setting can be stated as follows.

Theorem 2.3 (Ruzsa,[9]). *Let A, B and C be finite sets in a group G. Assume that $|AB| \leq \alpha_1|A|$ and $|CA| \leq \alpha_2|A|$. Then, there exists a set $\varnothing \neq X \subseteq A$ such that $|CXB| \leq \alpha_1\alpha_2|X|$.*

3. An explicit value for Tao's theorem

A combination of the three tools presented in the previous section can be used to give a value to the constant c in Tao's Corollary 1.4. We start by using Ruzsa's triangle inequality to prove a lemma that

appeared in Petridis [4]. Let us mention that this lemma is not related to Theorem 1.5 of said paper, which is its main contribution.

Lemma 3.1 (Petridis)**.** *Let A and B be finite non-empty sets in a group. Suppose that $|AA| \leq \alpha|A|$ and $|ABA| \leq \alpha^2|A|$. Then, $|AB^{-1}BA^{-1}| \leq \alpha^6|A|$.*

Proof. In Theorem 2.1, take $X = A$ and $Y = Z = AB^{-1}$. Then, we have that

$$|A||AB^{-1}BA^{-1}| \leq |AB^{-1}A^{-1}||ABA^{-1}| = |ABA^{-1}|^2$$

since $\left(AB^{-1}A^{-1}\right)^{-1} = ABA^{-1}$ and a set and its inverse have the same cardinality. In order to bound this, take Theorem 2.1 again and consider $X = A^{-1}$, $Y = AB$ and $Z = A$. This yields

$$|A||ABA^{-1}| \leq |ABA||A^{-1}A^{-1}| = |ABA||AA| \leq \alpha^3|A|^2$$

so, $|ABA^{-1}| \leq \alpha^3|A|$. Substituting this above and dividing by $|A|$ results in the statement. □

We can use this to prove the following result.

Theorem 3.2. *Let A be a finite set in a group. Assume that $|AA| \leq \alpha|A|$ and $|AaA| \leq \beta|A|$, for every $a \in A$. Then, $|AAA| \leq \alpha^8\beta|A|$.*

Proof. We can use Theorem 2.3 setting $A = C = B$. The theorem states that there exists some set $T \subseteq A$ such that $|ATA| \leq \alpha^2|T|$.

We can now use the trivial bound $|TA| \leq |ATA| \leq \alpha^2|T|$ for the hypothesis of Lemma 2.2. Applying this covering lemma, we have that there exists a set $S \subseteq A$ of size $|S| \leq \alpha^2$ such that $A \subseteq T^{-1}TS$. Hence, we have that $AAA \subseteq AT^{-1}TSA$.

Consider Ruzsa's triangle inequality in the form of Theorem 2.1, and substitute $X = A$, $Y = AT^{-1}T$, and $Z = A^{-1}S^{-1}$ to obtain $|A||AAA| \leq |A||AT^{-1}TSA| \leq |AT^{-1}TA^{-1}||ASA|$.

Now, we can use Lemma 3.1 to bound the first of these product sets. We can do this because we have $|AA| \leq \alpha|A|$, and $|ATA| \leq \alpha^2|T| \leq \alpha^2|A|$ since $T \subseteq A$, so we have all the hypothesis needed. To bound the second one, consider

$$|ASA| = \left|\bigcup_{s\in S} AsA\right| \leq \sum_{s\in S} |AsA| \leq \sum_{s\in S} \beta|A| = |S|\beta|A| \leq \alpha^2\beta|A|.$$

Putting everything together, we have that $|A||AAA| \leq \alpha^6|A|\alpha^2\beta|A| = \alpha^8\beta|A|^2$; and dividing by $|A|$ gives the desired result. □

Now, we can use this theorem as a base case to inductively obtain bounds on the size of higher product sets.

Proof of Theorem 1.6. The proof is done by induction on h. The base case $h = 3$ has been proved in Theorem 3.2. Let us prove the general case. Assume that $h > 3$. Using Ruzsa's triangle inequality with $X = A^{-1}$, $Y = AA$ and $Z^{-1} = A^{h-2}$, we have

$$|A^h| \leq \frac{|AAA||A^{-1}A^{h-2}|}{|A|}.$$

Taking now $X = A$, $Y = A^{-1}$ and $Z^{-1} = A^{h-2}$ yields

$$|A^{-1}A^{h-2}| \leq \frac{|AA||A^{h-1}|}{|A|}.$$

Putting both equations together and using Theorem 3.2, we obtain $|A^h| \leq \alpha^9\beta|A^{h-1}|$, and the last term is bounded by the induction hypothesis. □

In the particular case when $\beta = \alpha$, this result gives us $c = 10$ in the statement of Tao's Corollary 1.4. This constant is worse that the one obtained in Petridis [4] by one unit. However, it can be obtained without using Petridis's new method, so it is interesting by itself. Observe that Plünnecke's graph-theoretic method is necessary in order to obtain this bound, as it is needed to prove Theorem 2.3.

4. Further results

We can use Theorem 1.6 in order to get new product estimates. One may consider more sets and impose further restrictions on them. For example, we may consider the iterated product of two sets A and B with restrictions over the product sets of A, the product sets of A and B, and the size of each other. With this, we can obtain a bound for iterated product sets of two sets. As we have already observed that Theorem 1.5 gives a better bound on product sets than Theorem 1.6, we will use Petridis's result in this section in order to obtain tighter bounds.

We start with a result giving a bound for the size of the product set of A and an iterated product of B's. From this point onwards, Ruzsa's triangle inequality (i.e., Theorem 2.1) will be used repeatedly without warning, with X always being a simple set A or B, or one of their inverses.

Theorem 4.1. *Let A and B be two finite non-empty sets in a group. Assume that $|AA| \leq \alpha|A|$, $|AaA| \leq \beta|A|$ for every $a \in A$, $|AB| \leq \delta|A|$, $|AbB| \leq \varepsilon|A|$ for every $b \in B$, and $|A| \leq \gamma|B|$. Then, for any $k \geq 2$,*

$$|AB^k| \leq \begin{cases} \alpha^{16(k-1)}\,\beta^{2(k-1)}\,\gamma^{k-2}\,\delta^{2k-3}\,\varepsilon^{k-1}|A| & \text{if } k \text{ is even,} \\ \alpha^{16(k-1)}\,\beta^{2(k-1)}\,\gamma^{k-1}\,\delta^{2k-1}\,\varepsilon^{k-1}|A| & \text{if } k \text{ is odd.} \end{cases}$$

Proof. The proof is done by induction on k. We need two base cases in order to complete the induction.

When $k = 2$ we can apply Ruzsa's covering lemma due to the third condition on the sets. This gives us a set $S \subseteq B$ such that $|S| \leq \lfloor\delta\rfloor$ and $B \subseteq A^{-1}AS$. Hence,

$$|ABB| \leq |AA^{-1}ASB| \leq \frac{|AA^{-1}AA^{-1}||ASB|}{|A|}.$$

The second term in this expression can be bounded as

$$|ASB| = \left|\bigcup_{s\in S} AsB\right| \leq \sum_{s\in S}|AsB| \leq \sum_{s\in S}\varepsilon|A| = |S|\varepsilon|A| \leq \delta\varepsilon|A|. \tag{1}$$

In order to bound the first one, use Theorem 1.5 to obtain

$$|AA^{-1}AA^{-1}| \leq \frac{|AAA^{-1}|^2}{|A|} \leq \frac{(|AA||AAA|)^2}{|A|^3} \leq \alpha^{16}\beta^2|A|. \tag{2}$$

Putting the two expressions together we have

$$|ABB| \leq \alpha^{16}\beta^2\delta\varepsilon|A|. \tag{3}$$

For $k = 3$, we use again the covering lemma with the same conditions as above and get

$$|ABBB| \leq |AA^{-1}ASBB| \leq \frac{|AA^{-1}AA^{-1}||ASBB|}{|A|},$$

as $B \subseteq A^{-1}AS$ for some $S \subseteq B$ with $|S| \leq \delta$. The first term is bounded by (2). In order to bound the second term, consider that

$$|A||ASBB| \leq |ASBA^{-1}||AB| \leq \delta|ASBA^{-1}||A|,$$
$$|B||ASBA^{-1}| \leq |ASB||B^{-1}BA^{-1}| \leq \delta\varepsilon|B^{-1}BA^{-1}||A|,$$
$$|A||B^{-1}BA^{-1}| \leq |B^{-1}A^{-1}||ABA^{-1}| \leq \delta|ABA^{-1}||A|$$

and

$$|B||ABA^{-1}| \leq |ABB||B^{-1}A^{-1}| \leq \delta|A|\alpha^{16}\beta^2\delta\varepsilon|A|,$$

where the last inequalities in each line come from (1) in the second line, (3) in the fourth, and the statement hypothesis in all the others. With this,

$$|ASBA^{-1}| \leq \delta\varepsilon\frac{|A|}{|B|}\delta\delta\frac{|A|}{|B|}\alpha^{16}\beta^2\delta\varepsilon|A| \leq \alpha^{16}\beta^2\gamma^2\delta^4\varepsilon^2|A| \tag{4}$$

and $|ABBB| \leq \alpha^{16}\beta^2\delta\alpha^{16}\beta^2\gamma^2\delta^4\varepsilon^2|A| = \alpha^{32}\beta^4\gamma^2\delta^5\varepsilon^2|A|$.

For the general case, we can use the covering lemma in the same way. We have that

$$|AB^k| \leq |AA^{-1}ASB^{k-1}| \leq \frac{|AA^{-1}AA^{-1}||ASB^{k-1}|}{|A|}.$$

The first term is, again, bounded by (2), and the second is bounded as $|A||ASB^{k-1}| \leq |ASBA^{-1}||AB^{k-2}|$. The first term is now bounded by (4), and the second one is bounded by the induction hypothesis. Putting everything together the result follows. □

Using the previous result, we can give a general bound for iterated products of A's and B's, as long as all the A's come before the B's.

Theorem 4.2. *Let A and B be two finite non-empty sets in a group, with the conditions from Theorem 4.1. Then, for any $l \geq 2$ and $k \geq 2$,*

$$|A^lB^k| \leq \begin{cases} \alpha^{8l+16k-24}\,\beta^{2l+2k-3}\,\gamma^{k-2}\,\delta^{2k-3}\,\varepsilon^{k-1}|A| & \text{if } k \text{ is even,} \\ \alpha^{8l+16k-24}\,\beta^{2l+2k-3}\,\gamma^{k-1}\,\delta^{2k-1}\,\varepsilon^{k-1}|A| & \text{if } k \text{ is odd.} \end{cases}$$

Proof. As before, we can use Ruzsa's triangle inequality (twice) to bound

$$|A^lB^k| \leq \frac{|A^{l+1}||AB^k||AA|}{|A|^2}.$$

The three terms can now be bounded using Theorem 1.5, Theorem 4.1 and the statement hypotheses, respectively, and this immediately yields the result. □

In order to complete all the bounds of product sets of three or more sets as those we have presented so far, the only remaining case is that when $l \geq 2$ and $k = 1$.

Theorem 4.3. *Let A and B be two finite non-empty sets in a group, with the conditions from Theorem 4.1. Then, for any $l \geq 2$, $|A^l B| \leq \alpha^{8(l-1)}\beta^{l-1}\delta|A|$.*

Proof. We start by proving the base case $l = 2$. Using Ruzsa's triangle inequality we have

$$|AAB| \leq \frac{|AAA^{-1}||AB|}{|A|}$$

and

$$|AAA^{-1}| \leq \frac{|AAA||AA|}{|A|}$$

so, using Theorem 1.5 and putting everything together, we get $|AAB| \leq \alpha^7\beta\alpha\delta|A|$.

For the general case ($l > 2$), observe that

$$|A^l B| \leq \frac{|AAA^{-1}||A^{l-1}B|}{|A|}.$$

The first term can be bounded using Theorem 2.1 and Theorem 1.5 as $|AAA^{-1}| \leq \alpha^8\beta|A|$, as before, and the second is bounded by the induction hypothesis. □

An easy corollary is obtained when taking $B = A^{-1}$ in Theorem 4.2. This would correspond to an extension of the Plünnecke–Ruzsa inequality to the non-commutative case, when $A = B$.

Corollary 4.4. *Let A be a non-empty finite set in a group such that $|AA| \leq \alpha|A|$ and $|AaA| \leq \beta|A|$, for every $a \in A$. For any $k, l \geq 2$, let $m = \min\{k, l\}$ and $n = \max\{k, l\}$. Then,*

$$|A^l A^{-k}| \leq \alpha^{8n+21m-27}\,\beta^{2n+3m-4}|A|.$$

Proof. Take $B = A^{-1}$. For this particular choice of sets we have $\gamma = 1$ and, in virtue of Ruzsa's triangle inequality, $|AA^{-1}| \leq \alpha^2|A|$ and $|AaA^{-1}| \leq \alpha\beta|A|$. Substituting these into Theorem 4.2, we can write

$$|A^l A^{-k}| \leq \begin{cases} \alpha^{8l+21k-31}\,\beta^{2l+3k-4}|A| & \text{if } k \text{ is even,} \\ \alpha^{8l+21k-27}\,\beta^{2l+3k-4}|A| & \text{if } k \text{ is odd.} \end{cases}$$

First, observe that this can be written in such a way that it does not depend on the parity by taking the worst exponent for each of the coefficients. Since these coefficients are all lower-bounded by 1 for this choice of sets, this means we must take the highest exponents, which correspond to the odd case. Then, for any $k, l \geq 2$ we may write

$$|A^l A^{-k}| \leq \alpha^{8l+21k-27}\,\beta^{2l+3k-4}|A|.$$

Observe now that this is a symmetric result. That is, the fact that a set and its inverse have the same size means that $|A^l A^{-k}| = |A^k A^{-l}|$. Then, as the bound given by the above expression is much weaker when $k > l$, if this occurs one can use the bound for the size of the inverse set to obtain a better bound. This is what allows us to take the minimum and the maximum of k and l. □

We can use this to obtain a particular bound for Tao's Theorem 1.3 if we impose $\alpha = \beta$. In this case, we have $|A^l A^{-k}| \leq \alpha^{10l+24k-31}|A|$.

If we want to obtain a constant c with respect to $h = l+k$, as appears in the statement of Theorem 1.3, we have to consider the following. The exponent $10l + 24k - 31$, for a fixed h, is increasing with k and maximized when $l = k$ because of the possibility to take the maximum and minimum of k and l. Hence,

$$10l + 24k - 31 \leq 10\frac{h}{2} + 24\frac{h}{2} - 31 \leq 34\frac{h}{2} = 17h$$

so, we have $c = 17$ for all these different cases.

However, we can obtain a much better constant, in a more general setting, if we work with the sets A and A^{-1} from the beginning.

Proof of Theorem 1.7. We start with the base case $h = 3$. We must consider all the possible signs that can appear in the exponents. By using Theorem 1.5, we have that

$$|AAA| \leq \alpha^7\beta|A|,$$

$$|AAA^{-1}| \leq \frac{|AAA||AA|}{|A|} \leq \alpha^8\beta|A|,$$

$$|A^{-1}AA| \leq \frac{|AA||AAA|}{|A|} \leq \alpha^8\beta|A|,$$

and

$$|AA^{-1}A| \leq \frac{|AA^{-1}A^{-1}||AA|}{|A|} \leq \alpha^9\beta|A|.$$

The other four possible configurations are the inverses of these ones. Hence, in general,

$$|A^{\epsilon_1}A^{\epsilon_2}A^{\epsilon_3}| \leq \alpha^9\beta|A|.$$

For the general case, there are two different possibilities. First, assume $\epsilon_1 = \epsilon_2$. Then, take $X = A^{-\epsilon_1}$ in the statement of Ruzsa's triangle inequality to obtain

$$|A||A^{\epsilon_1}A^{\epsilon_1}A^{\epsilon_3}\cdots A^{\epsilon_h}| \leq |A^{\epsilon_1}A^{\epsilon_1}A^{\epsilon_1}||A^{-\epsilon_1}A^{\epsilon_3}\cdots A^{\epsilon_h}| \leq \alpha^7\beta|A^{-\epsilon_1}A^{\epsilon_3}\cdots A^{\epsilon_h}||A|.$$

If, on the contrary, $\epsilon_1 = -\epsilon_2$, we have

$$\begin{aligned}|A||A^{\epsilon_1}A^{\epsilon_2}A^{\epsilon_3}\cdots A^{\epsilon_h}| &\leq |A^{\epsilon_1}A^{\epsilon_1}||A^{\epsilon_2}A^{\epsilon_2}A^{\epsilon_3}\cdots A^{\epsilon_h}| \\ &\leq \alpha|A^{\epsilon_2}A^{\epsilon_2}A^{\epsilon_2}||A^{-\epsilon_2}A^{\epsilon_3}\cdots A^{\epsilon_h}| \\ &\leq \alpha^8\beta|A^{-\epsilon_2}A^{\epsilon_3}\cdots A^{\epsilon_h}||A|.\end{aligned}$$

The worst exponent is given in the second case. The two last sets can be bounded by the induction hypothesis. □

Taking $\alpha = \beta$ in the statement of Theorem 1.7, we obtain $|A^{\epsilon_1}A^{\epsilon_2}\cdots A^{\epsilon_h}| \leq \alpha^{9h-17}|A|$, for any signs $\epsilon_1, \ldots, \epsilon_h \in \{-1, 1\}$. With this, we have an explicit constant value for the statement of Tao's Theorem 1.3, $c \leq 9$, so we have that the same constant working when all signs are set to be equal serves in the rest of cases as well.

References

[1] E. Breuillard, B. Green, and T. Tao, "The structure of approximate groups", *Publ. Math. Inst. Hautes Études Sci.* **116** (2012), 115–221.

[2] G.A. Freĭman, "Foundations of a structural theory of set addition", American Mathematical Society, Providence, R.I. (1973), vii+108.

[3] H.A. Helfgott, "Growth in groups: ideas and perspectives", *Bull. Amer. Math. Soc.* **52**(3) (2015), 357–413.

[4] G. Petridis, "New proofs of Plünnecke-type estimates for product sets in groups", *Combinatorica* **32**(6) (2012), 721–733.

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

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

[7] I.Z. Ruzsa, "Sums of finite sets", in "Number theory", (1996) Springer, New York, 281–293.

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

[9] I.Z. Ruzsa, "Sumsets and structure", *Adv. Courses Math. CRM Barcelona* (2009), Birkhäuser Verlag, Basel, 87–210.

[10] T. Tao, "Product set estimates for non-commutative groups", *Combinatorica* **28**(5) (2008), 547–594.