Journal of Algebra 389 (2013) 61–77

Contents lists available at SciVerse ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

Explicit Helfgott type growth in free products and in limit groups

J.O. Button

Selwyn College, University of Cambridge, Cambridge CB3 9DQ, UK

A R T I C L E I N F O

Article history:
Received 27 September 2011
Available online 4 June 2013
Communicated by Aner Shalev

Keywords:
Group
Growth
Free product

A B S T R A C T

We adapt Safin's result on powers of sets in free groups to obtain Helfgott type growth in free products: if A is any finite subset of a free product of two arbitrary groups then either A is conjugate into one of the factors, or the triple product A^3 of A satisfies $|A^3| \geqslant (1/7776)|A|^2$, or A generates an infinite cyclic or infinite dihedral group. We also point out that if A is any finite subset of a limit group then $|A^3|$ satisfies the above inequality unless A generates a free abelian group. This gives rise to many infinite groups G where there exist $c > 0$ and $\delta = 1$ such that any finite subset A of G either satisfies $|A^3| \geqslant c|A|^{1+\delta}$ or generates a virtually nilpotent group.

1. Introduction

When A is a finite subset (always assumed non-empty in this paper) of an abelian group then there has long been interest in classifying when A has small doubling. Namely on being given a class of abelian groups (say all torsion free abelian groups or all finite abelian groups) and a real number $K \geqslant 1$, one wants to describe the structure of those A such that the size of $A + A$ is at most $K|A|$. However for finite subsets of non-abelian groups there were until recently very few equivalent results (say only Freiman's 3/2 Theorem from 1973 which gives a complete characterisation in any group G of all finite subsets A whose double product A^2 satisfies $|A^2| < (3/2)|A|$). An issue here is that in an infinite non-abelian group G one can have (in fact often has, see Section 4) a sequence of finite subsets A of G with $|A^2| < 4|A|$ but $|A^3|/|A| \to \infty$ as $|A| \to \infty$, so that control over the size of the double product A^2 does not give control of the triple product $|A^3|$ unlike in the abelian case.

A breakthrough came with the paper [7] of Helfgott, which showed that once A^3 has bounded size then so do all the higher product sets A^4, A^5, and so on. Indeed if A is a finite subset of any group

E-mail address: jb128@dpmms.cam.ac.uk.

0021-8693/$ – see front matter
http://dx.doi.org/10.1016/j.jalgebra.2013.05.013

and $|A^3| \leqslant K^2|A|$ then for $n \geqslant 3$ we have $|A^n| \leqslant K^{2(n-2)}|A|$. He then considered the collection of finite groups $SL(2, p)$ over all primes p and showed a strong growth property of triple products in this case. Of course in general we cannot expect triple product growth for all finite subsets of a group: examples of A such that $|A^3| < 3|A|$ would be when A is itself a finite subgroup (or consists of more than a third of a finite subgroup), or when A is an arithmetic progression, namely it consists of consecutive powers $\{x^n, x^{n+1}, \dots, x^{n+i}\}$ of any element x. Helfgott's result states (using the Gowers trick as in [1]) that there are absolute constants $c, \delta > 0$ such that if A is any generating set of $G = SL(2, p)$ for any prime p then either $|A| \geqslant 2|G|^{8/9}$ in which case $A^3 = G$, or $|A^3| \geqslant c|A|^{1+\delta}$ when $|A| < 2|G|^{8/9}$.

There has also been interest recently in approximate groups, following [13]. Given $K \geqslant 1$, we say that a finite subset A of a group G is a K-approximate group if it is symmetric, contains the identity, and there is a subset X of G with $|X|$ at most K such that $A^2 \subseteq AX$. An immediate consequence of this definition is that $|A^2| \leqslant K|A|$, $|A^3| \leqslant K^2|A|$ and $|A^{n+1}| \leqslant K^n|A|$, so certainly the size of all product sets is well behaved here. Indeed there is a close connection between K-approximate groups and sets of small tripling, because if $|A^3| \leqslant K^2|A|$ then $S = (A \cup A^{-1} \cup \{e\})^2$ is an $8K^6$-approximate group by Ruzsa'a covering lemma (see [13], Lemma 3.6).

There are results on the structure of K-approximate groups, culminating in [4] which completely characterises such subsets. As a consequence of this characterisation it is shown that there is a universal function $c(K)$ such that a K-approximate group A in any group G can be covered by $c(K)$ cosets of a finitely generated, virtually nilpotent subgroup of G. However this function given by the proof is completely inexplicit; indeed it is not known whether it could be polynomial in K.

However our interest here is in the existence of approximate groups inside infinite groups. Certainly any finite symmetric subset A containing the identity is a K-approximate group for some K, namely $K = |A|$. Thus in practice we fix K and ask how big subsets A of an infinite group G can be if they are K-approximate groups, or more generally if they satisfy $|A^3| \leqslant K^2|A|$. Moreover as there are certainly examples using finite subgroups or arithmetic progressions, we should insist that the subgroup $\langle A \rangle$ generated by A is not a virtually cyclic group. As our interest here is in that part of the spectrum of groups close to free groups, we will further insist that $\langle A \rangle$ is not virtually abelian or virtually nilpotent; indeed balls in virtually nilpotent groups also provide examples of approximate groups.

At this point it seems that a severe dearth of examples presents itself. For instance the author was unable to find in the literature a single case of an infinite group G and a real number $K > 1$ where there exist finite subsets A of G all generating non-virtually nilpotent subgroups and with $|A^3| \leqslant K^2|A|$ but $|A|$ unbounded. If there were no such examples then there would exist a function $f(K)$, possibly depending on the ambient group G, such that any K-approximate group A in G with $\langle A \rangle$ not virtually nilpotent has $|A| \leqslant f(K)$. In particular A can be covered by $f(K)$ cosets of the trivial subgroup. In fact examples do exist, such as the case when G is equal to the direct product of the rank 2 free group $F_2 = \langle x, y \rangle$ and the integers $\mathbb{Z} = \langle z \rangle$, whereupon we can take $A = \{(x, z^i), (y, z^i)\colon\ 0 \leqslant i \leqslant N-1\}$ with $|A^3| < 12|A|$ and $\langle A \rangle = F_2 \times \mathbb{Z}$ but $|A| = 2N$. We elaborate on this example in Proposition 4.2.

Moreover when we do have an infinite group G and a function $f = f_G$ such that $|A^3| \leqslant K^2|A|$ implies that $|A| \leqslant f(K)$ for all finite subsets A of G with $\langle A \rangle$ not virtually nilpotent, we can still ask how quickly f grows. We can make a connection here with Helfgott's results by using the following definition:

Definition 1.1. Given a group G, we say that G has *Helfgott type growth* if there exist $c, \delta > 0$ such that any finite subset A with $\langle A \rangle$ not virtually nilpotent satisfies $|A^3| \geqslant c|A|^{1+\delta}$.

It is clear that if this definition is satisfied then any K-approximate group A in G with $\langle A \rangle$ not virtually nilpotent has size at most $c^{-1/\delta}K^{2/\delta}$, thus our function f above will be polynomial in K. Moreover the application of Helfgott type growth to infinite groups G works well because we never have to worry about the finite subset A being "most" of G and we do not have to stick to the case when A generates G.

As for the degree of our polynomial function f, it is shown in Proposition 4.1 using an elementary construction that if a finitely generated group G which is not virtually nilpotent has Helfgott type growth then $\delta \leqslant 1$ (with the possible exception of groups having bounded exponent) so f cannot be subquadratic here. Thus if $\delta = 1$ holds in the above expression for some group G then it seems reasonable to say that G has no approximate groups, because any K-approximate group contained in G is either contained in a small (i.e. virtually nilpotent) subgroup of G or is the same order of magnitude as those K-approximate groups formed using basic constructions.

In this paper we show that a free product of two groups has no approximate groups if the two factors do not. We also show that limit groups have no approximate groups. More precisely, if G is a limit group and A a finite subset then we show Helfgott type growth in that either $|A^3| \geqslant c|A|^{1+\delta}$ for $\delta = 1$ (thus obtaining the best possible value for δ) or $\langle A \rangle$ is free abelian. As for free products $\Gamma = G * H$ where G and H are arbitrary groups, we show that either $|A^3| \geqslant c|A|^{1+\delta}$ for $\delta = 1$ (again best possible) or A can be conjugated into one of the factors of the free product, or $\langle A \rangle$ is infinite cyclic or infinite dihedral. We also make the value of c explicit and it is independent of the group, indeed we take $c = 1/7776$ throughout.

In [12] by Safin it was shown that in the free group F_2 of rank 2 (and hence in all free groups F_k of rank k) we have $|A^3| \geqslant c|A|^2$ for all finite subsets A, unless $\langle A \rangle$ is infinite cyclic. This was the first example of an infinite group G with Helfgott type growth where we can take $\delta = 1$. Of course this will also be true for subgroups of G but a subgroup of a free group is free. In [12] the constant c was not given but is explicit when followed through the paper and that is what we do here. Our result mirrors this proof of Safin closely by using the normal form for free products in place of words in the standard generators for the free group F_2, but we have to work harder at the beginning (in finding a suitable proportion of A where growth should take place) and at the end (when identifying the subgroup generated by those sets A with small triple product, which might not be cyclic).

The proof for free products is given in Section 2, then in Section 3 we consider limit groups and other examples of infinite groups with Helfgott type growth. Finally in Section 4 we give examples of groups which are not virtually nilpotent and which do not have Helfgott type growth for any positive values of c and δ. In particular there exist such examples which are free products with amalgamation and also HNN extensions, formed using only the integers $\mathbb{Z}$. Moreover these examples include all virtually polycyclic groups and $SL(3,\mathbb{Z})$. The method here is always to find finite subsets A_N of a group with $\langle A_N \rangle$ not virtually nilpotent and $|A_N| \to \infty$ but where $|A_N^3|/|A_N|$ stays bounded.

2. Helfgott type growth in free products

We begin with some standard facts on free products of groups, for which see [10], and periodic words following [12] (which in turn followed [11]).

If G and H are any groups (implicitly assumed not to be the trivial group $I = \{id\}$) then the *free product* $G * H$ of the *factor groups* G, H consists of k-tuples $(x_1, \dots, x_k)$ of arbitrary length and where either the odd x_is are taken from $G - I$ and the even x_is from $H - I$ or the other way around. This tuple is referred to as the *normal form* of an element γ in $G * H$ but is really the definition of γ. If $k = 1$ then we have the element (x) for $x \in G - I$ or $x \in H - I$ and we may omit the brackets. The identity is represented by the empty tuple $\emptyset$ where $k = 0$.

This value of k is an important invariant of the element $\gamma \in G * H$ called the *syllable length* $\sigma(\gamma)$. In this paper we divide $(G * H) - I$ into four disjoint sets called *types*. The idea is that for any $\gamma \in (G * H) - I$ we need to take into account the parity of $\sigma(\gamma)$ and whether the normal form of γ starts with an element in G or an element in H (whereupon we would know in which factor the final entry lies). This gives rise to our four types of *G-even*, *H-even*, *G-odd*, *H-odd* and the notion of an *odd* or *even* element if we only require the parity of k.

Multiplication xy of elements $x = (x_1, \dots, x_k)$ and $y = (y_1, \dots, y_l)$ is given by first concatenating to get $(x_1, \dots, x_k)(y_1, \dots, y_l)$. If x_k and y_1 are in different factors (for instance if x is G-odd then this occurs precisely when y is H-even or H-odd) then we just remove the interior brackets to obtain this $(k+l)$-tuple for xy. However if say both x and y are G-odd then $x_k y_1$ is an element of G and one of two possibilities occurs. Either $x_k y_1 \neq id$ in which case we say that *absorption* has occurred in forming the product xy with normal form

$$(x_1, \dots, x_{k-1}, x_k y_1, y_2, \dots, y_l)$$

and syllable length $k+l-1$. Otherwise $x_k y_1 = id$ and we say there is *cancellation* in xy. So

$$(x_1, \ldots, x_{k-1}y_2, \ldots, y_l)$$

will be the normal form of xy if we now have absorption, that is if $x_{k-1}y_2 \neq id$. However we could have further cancellation and so the normal form is found by continuing to cancel until we have absorption (or we run out of letters in x or y).

We now follow [12] in defining periodic words, but here adapted to the free product case. A *periodic* element y of $G*H$ is one which is of the form $y = \bar{y}^s t$ where $s \geqslant 2$, $\bar{y} \in (G*H) - I$ and $t \in G*H$, no cancellation or absorption occurs anywhere in forming this product, and the normal form of t is a prefix of the normal form for $\bar{y}$. In particular $\bar{y}$ must be an even element, and if $\bar{y}$ is G-even say then t is G-even or G-odd (or empty). We assume throughout that $\bar{y}$ is not a proper power of some other word, in which case we call $\bar{y}$ the *period* and t the *tail* of the periodic word y: these are both uniquely defined. When t is empty we say that y is *totally periodic*.

We can also work from the right of the normal form, giving rise to the definition of a *right periodic* word (or totally right periodic if h is empty) $z = h\bar{z}^s$ where as before we have that $\bar{z}$ is the (unique) *right period* of z and h is a (unique) suffix of $\bar{z}$ called the *head* of z.

A word is periodic if and only if it is right periodic (explaining why we can use the term periodic above rather than left periodic). Moreover on taking two periodic words $y_1 = \bar{y}^{s_1} t_1$ and $y_2 = \bar{y}^{s_2} t_2$ with the same period, suppose that they also have the same right period. Then it follows that the tails are the same, so $t_1 = t_2$. (One can picture this by placing the entries of $\bar{y}$ clockwise in turn around a circle, starting from the top, so a word with period $\bar{y}$ corresponds to a clockwise walk from the top that runs at least twice around this circle. As $\bar{y}$ has no rotational symmetry by minimality of the period, we see that if the right periods of y_1 and y_2 coincide then the backwards walk of each word must have started in the same place.)

Finally we need to adapt the idea of a periodic element in the case of free products, in order to take account of odd elements. The problem is that if $\bar{y}^s t$ is a periodic word which is an odd element of $G*H$ then absorption (or even cancellation) takes place when forming its square which we need to control. Note that here the syllable length must be at least 5 because $\bar{y}$ is even, $s \geqslant 2$ and $t \neq \emptyset$, so the idea is that we do not worry about the first element or last element of the normal form. We therefore need the notion of what we call here an interior periodic element. This has exactly the same definition as before for even elements. However we say that the G-odd element y is *interior periodic* if there exist $g_1 \in G$ and $g_2 \in G - I$ such that $y = g_1 x g_2$ where x is G-even and periodic, so x can be written as $\bar{y}^s t$ for t a prefix of $\bar{y}$ and where $\bar{y}$ and t are both G-even elements (or t is empty). Thus $y = g_1 \bar{y}^s t g_2$ where absorption takes place between g_1 and $\bar{y}$ but no absorption or cancellation can occur otherwise in this expression. We cannot have cancellation between g_1 and $\bar{y}$ because then y would start with an element from H. Similarly $g_2 \neq id$ but we do allow g_1 to be the identity, thus interior periodic does include the definition of periodic by taking $g_1 = id$ and g_2 to be the appropriate element of $G - I$.

We have the corresponding definition of interior periodic words for H-odd elements too. We still call $\bar{y}$ the period and t the tail of the interior periodic element $y = g_1 \bar{y}^s t g_2$ as above (or tail tg_2 if tg_2 is a prefix of $\bar{y}$) and they are again uniquely defined. Similarly we also have the concept of an *interior right periodic* word, which again has a well-defined right period and head. As before, a word is interior periodic if and only if it is interior right periodic and if two interior periodic words have the same period and right period then they have the same tail as well. These facts can be seen by removing the first and last letters from the normal form of y, resulting in a genuine periodic word unless $s = 2$ and $t = \emptyset$, but the arguments continue to hold in this case too.

We begin our proof by first adapting Lemma 1 of [12] to the free product case. Here we note the obvious but useful fact that if we are given a finite subset A of any group Γ then the growth of A is the same as the conjugate subset $\gamma A \gamma^{-1}$ for all $\gamma \in \Gamma$, as $|A^n| = |\gamma A^n \gamma^{-1}| = |(\gamma A \gamma^{-1})^n|$.

Lemma 2.1. *Let A be any subset of $\Gamma = G*H$. Then there exists a conjugate subset $\gamma A \gamma^{-1}$ in Γ of A with the following property: there is no element x in $G - I$ or in $H - I$ such that more than half of the elements in $\gamma A \gamma^{-1}$ have normal form $(x, \ldots, x^{-1})$.*

Proof. Suppose there is such an $x = g$ in (without loss of generality) $G - I$, so that more than half of the elements in A are G-odd with normal form $(g, \dots, g^{-1})$. Then on forming the conjugate subset $g^{-1}Ag$, these elements will have their syllable length reduced by 2 (but see the note below). Now the syllable length of any other element can go up by at most 2 so the total syllable length of the elements in A must decrease. If the conclusion of the lemma is still not satisfied then we can continue the process of conjugating to reduce syllable length and it is clear that this process must eventually terminate. $\square$

Note: There is one case where the conclusion of Lemma 2.1 fails. This is if we have an element in normal form $(x, \dots, x^{-1})$ of syllable length 1. Now this can only happen if the element itself is equal to x in $G - I$ (say) with x of order 2, but on conjugating by x^{-1} we have $x^{-1}xx$ is still of length 1. Thus it would be possible not to decrease the total syllable length, but only if $|A| = 2k + 1$ for some k and where $k + 1$ elements, including x, have normal form $(x, \dots, x)$ and the other k elements are all H-odd. For instance consider the infinite dihedral group $\langle x\rangle * \langle y\rangle$ with x and y both of order 2, and

$$A = \left\{x, xyx, \dots, (xy)^k x, y, yxy, \dots, (yx)^{k-1} y\right\}.$$

However we only need the lemma for Theorem 2.2 and in this case the conclusions are immediately satisfied by taking X and Y to be the G-odd and the H-odd elements.

Theorem 2.2. *For any finite set $A \subseteq G * H$ there exist (not necessarily disjoint) subsets X, Y of a conjugate in $G * H$ of A such that $|X|, |Y| \geqslant (1/18)|A|$ and such that for any $x \in X$ and $y \in Y$ there is no cancellation in xy or in yx (although there may be absorption).*

Proof. We assume by conjugating that A satisfies the conclusions of Lemma 2.1 and we first divide A into the four G-odd, G-even, H-odd and H-even subsets. If the identity is in A then its type is not well defined, but we will place it in either of the odd subsets because cancellation does not occur when an element is multiplied by the identity.

If either of the two even subsets has size at least $|A|/18$ then we are happy to take $X = Y$ to be that subset. We are also happy taking X to be the G-odd elements and Y the H-odd elements if both have size $|A|/18$. Without loss of generality this only leaves the case where the set G_{odd} of G-odd elements satisfies $|G_{\text{odd}}| > (5/6)|A|$. In this case we require a more delicate argument which involves partitioning the elements in G_{odd} into two subsets of reasonable size in order to avoid cancellation, which will work unless a large proportion of elements in G_{odd} have normal form $(g, \dots, g^{-1})$.

Consider the map M from G_{odd} to $G \times G$ given by sending an element $(g, \dots, \gamma)$ in normal form to the ordered pair (g, γ^{-1}). This also makes sense for elements in G, including the identity which maps to (id, id). Of course $G \times G$ could be infinite but the image $\mathrm{Im}(M)$ is finite. Let $E = \{g_1, \dots, g_n\}$ be the set of elements of G that appear either as a first or second entry of $\mathrm{Im}(M)$. We have that $n \geqslant 2$ as not all elements in G_{odd} are of the form $(g, \dots, g^{-1})$ by Lemma 2.1. An obvious way to form two subsets of G_{odd} without cancellation between them is to divide E into two disjoint subsets $E_1 \cup E_2$ of roughly equal size, say $E_1 = \{g_1, \dots, g_{\lceil n/2\rceil}\}$ and $E_2 = \{g_{\lceil n/2\rceil+1}, \dots, g_n\}$. This gives a few possibilities for X and Y; namely we could set $X = Y$ to be the inverse image under M of $E_1 \times E_2$, or of $E_2 \times E_1$, or we could set X to be the inverse image of $E_1 \times E_1$ and Y that of $E_2 \times E_2$. We are done if in any of these three cases we have that both $|X|$ and $|Y|$ are at least $|G_{\text{odd}}|/15 > |A|/18$. Thus we could only fail here if the inverse images of $E_1 \times E_2$, of $E_2 \times E_1$ and (without loss of generality) $E_2 \times E_2$ is less than $|G_{\text{odd}}|/15$. This forces $M^{-1}(E_1 \times E_1) > (1 - 3/15)|G_{\text{odd}}|$.

In this case we transfer elements one by one from E_1 to E_2, thus decreasing $M^{-1}(E_1 \times E_1)$ and increasing $M^{-1}(E_2 \times E_2)$, although $M^{-1}(E_1 \times E_2)$ and $M^{-1}(E_2 \times E_1)$ can go either way. We stop as soon as one of these last three quantities is at least $|G_{\text{odd}}|/15$ and we are done in the final two cases. We are also done when $M^{-1}(E_2 \times E_2) \geqslant |G_{\text{odd}}|/15$, which will occur at some point, unless $|M^{-1}(E_1 \times E_1)|$ is now less than $|G_{\text{odd}}|/15$. If so, suppose we have just moved $g \in E$, where our partition previously was $E = F_1 \cup F_2$ and now is $E = E_1 \cup E_2$ so that $F_1 = E_1 \cup \{g\}$ and $E_2 = F_2 \cup \{g\}$.

On doing this we have $|M^{-1}(F_1 \times F_1)| > (4/5)|G_{\mathrm{odd}}|$ but $|M^{-1}(E_1 \times E_1)|$ has dropped down to below $|G_{\mathrm{odd}}|/15$, which implies $M^{-1}(F_1 \times F_1 - E_1 \times E_1) > (11/15)|G_{\mathrm{odd}}|$. Now $F_1 \times F_1 - E_1 \times E_1 = (\{g\} \times E_1) \cup (E_1 \times \{g\}) \cup \{(g, g)\}$ and $M^{-1}(\{g\} \times E_1)$ is a subset of $M^{-1}(E_2 \times E_1)$. Thus if the former of these two sets has size at least $(1/15)|G_{\mathrm{odd}}|$ then we are done on taking $X = Y = M^{-1}(E_2 \times E_1)$. Similarly for $E_1 \times \{g\}$ so we are fine unless $|M^{-1}(\{(g, g)\})| > (9/15)|G_{\mathrm{odd}}| > |A|/2$. But this implies that more than half the elements of A have normal form $(g, \ldots, g^{-1})$, which was eliminated at the start of the proof by taking a suitable conjugate. $\square$

Lemma 2.3. *For any finite set $A \subseteq \Gamma = G * H$, there exist subsets X and Y of a conjugate of A such that $|X|, |Y| \geqslant (1/36)|A|$, with no cancellation in xy or yx for all $x \in X$, $y \in Y$ and such that the syllable length $\sigma(x) \leqslant \sigma(y)$ for all $x \in X$ and $y \in Y$.*

Proof. Take X and Y as in Theorem 2.2 but notice they can be swapped with the same conclusion holding. Let the elements x_i and y_i of each of these sets be placed in ascending order of syllable length and set σ_X to be the syllable length of the median element $x_{\lfloor (|X|+1)/2 \rfloor}$, and the same for σ_Y. If $\sigma_X \leqslant \sigma_Y$ then take the first $\lfloor \frac{|X|+1}{2} \rfloor$ elements for the new set X and the last $\lfloor \frac{|Y|+1}{2} \rfloor$ for the new set Y. If $\sigma_X > \sigma_Y$ then swap X and Y before doing the same. $\square$

The idea now, as based on Lemma 3 in [12], is to take an element $a \in A$ (usually a will be in Y) and consider the map F_a from $X \times X \to A^3$ given by $(x_1, x_2) \mapsto x_1 a x_2$. If this map is injective or even at most 2–1 then we have $|A^3| \geqslant (1/2)|X|^2$, so we examine when this fails with the aim of finding severe restrictions on X and Y. The fact that cancellation is not taking place between elements of X and elements of Y means that periodicity plays a big part in such restrictions, but we first need to eliminate very short words.

Lemma 2.4. *If X and Y are in Lemma 2.3 then either $|A^3| \geqslant (1/4)|X|^2$ or we can assume that all elements in Y have syllable length at least* 4.

Proof. Recall that however X and Y were obtained in Theorem 2.2 and Lemma 2.3, all elements in $X \cup Y$ have the same parity, so we first deal with odd elements. Suppose there is an element in Y with syllable length 1. Then $\sigma(x) = 1$ (or 0) for all $x \in X$; that is (without loss of generality) $X \subseteq G$. If there is any $a \in A$ which is not in G then the map F_a is injective on $X \times X$, giving $|A^3| \geqslant |X|^2$. This is because even though there might be absorption, we can read off (x_1, x_2) from the front and back of $x_1 a x_2$. If however $a \in G$ then we have absorption both before and after a, but now we are in the case where (after an initial conjugation) $A \subseteq G$.

Now suppose we have $y \in Y$ with $\sigma(y) = 3$. Then $\sigma(x) =$ (0 or) 1, or 3 for all $x \in X$ and so one of these will occur for at least $|X|/2$ elements. Again the map F_y will be injective on this subset of X because we may have absorption but do not have cancellation and we know the syllable length of the elements, so can recreate a pair of elements from their image. This gives $|A^3| \geqslant (|X|/2)^2$.

The argument is the same when all elements are even by replacing syllable lengths 1 and 3 with 2 and 4 respectively. Here we do not have to worry about A being conjugate into a factor. $\square$

As we now assume that all elements in Y have syllable length at least 4, we can start to look for periodic words.

Lemma 2.5. *Let X and Y be as in Lemma 2.3 and such that all elements of Y have syllable length at least* 4. *Take any $y \in Y$ and consider the map*

$$F_y : X \times X \to AyA \quad \text{given by} \quad F_y(u_1, u_2) = u_1 y u_2.$$

If a point in AyA has at least three preimages then y is interior periodic. Moreover when $X \cup Y$ does not consist solely of odd elements of the same type, we have that y is periodic with period $\bar{y}$ and one of the first components in these three preimages has normal form ending with $\bar{y}$.

In the case when all elements in $X \cup Y$ are odd elements of the same type, say G-odd without loss of generality, then there is $s \geqslant 2$ and $g \in G$, $\gamma \in G - I$ such that $y = g\overline{y}^s t\gamma$ for period $\overline{y}$ (a G-even element) and t a prefix of $\overline{y}$ which is either empty or also G-even. We also have that one of the first components in these three preimages ends with either $\overline{y}g^{-1}$ or $\omega g\overline{y}g^{-1}$, where ω is the final entry in one of the other two first components.

Proof. Suppose $u_1yu_2 = v_1yv_2 = w_1yw_2$. We will assume that all elements are G-odd with absorption but not cancellation taking place. This is because otherwise the proof is considerably easier in that we ignore all reference to absorption, making it close to the original proof of Lemma 3 in [12] for free groups.

We set

$$u_1 = (a_1, b_1, \dots, b_{j-1}, a_j), \qquad v_1 = (c_1, d_1, \dots, d_{k-1}, c_k), \qquad w_1 = (\gamma_1, \delta_1, \dots, \delta_{l-1}, \gamma_l)$$

and

$$y = (g_1, h_1, \dots, h_{N-1}, g_N) \quad \text{for } a_i, c_i, \gamma_i, g_i \in G \text{ and } b_i, d_i, \delta_i, h_i \in H.$$

Let us first assume that $j = k$, so that u_1 and v_1 have the same syllable length $2k - 1$. As $N > 1$ (because of the condition on syllable lengths of Y) and there is only absorption at each end, we can equate the two normal forms for $u_1yu_2 = v_1yv_2$ to obtain $a_i = c_i$ and $b_i = d_i$. Thus $u_1 = u_2$ and $v_1 = v_2$ anyway.

The same also holds if any two of j, k, l are equal so we now suppose that $2j - 1 = \sigma(u_1) < 2k - 1 = \sigma(v_1) < 2l - 1 = \sigma(w_1) \leqslant 2N - 1 = \sigma(y)$. On comparing respective entries for the element $u_1yu_2 = v_1yv_2$, we have $c_kg_1 = g_{k-j+1}$ and then the letters start to reoccur, so that $h_1 = h_{k-j+1}, h_2 = h_{k-j+2}, \dots$ which makes the sequence h_i repeat after the first $k - j$ elements. We also have the same property for the sequence g_i except that $c_kg_1 = g_{k-j+1}$ and $g_{N-k+j} = g_N\epsilon$, where $\epsilon \in G$ is the first element in the normal form of u_2. This means that the sequence

$$x = (c_kg_1, h_1, g_2, \dots, h_{N-1}, g_N\epsilon)$$

of length $2N - 1$ repeats after the first $2(k - j)$ elements. The same is true on replacing j with k, k with l, c_k with γ_l, and ϵ with the first element α in the normal form for v_2.

Now if $2(k - j)$ and $2(l - k)$ are both at least N then $2(l - j) \geqslant 2N$, but we know $1 \leqslant j, l \leqslant N$ which is a contradiction. Thus suppose that $2(k - j) < N$. Then x is periodic so we can write $x = \overline{y}^s\tau$ for $s \geqslant 2$ and with no cancellation, where τ is a prefix of $\overline{y}$. We also have that $\sigma(\overline{y})$ divides $2(k - j)$. Now $\overline{y}$ is a G-even element and τ is G-odd. Consequently we can say that $y = c_k^{-1}x\epsilon^{-1}$, where we have absorption, and we take $g = c_k^{-1}$ in the statement of the lemma. The same holds if $2(l - k) < N$ except that now $y = \gamma_l^{-1}x\alpha^{-1}$ and $g = \gamma_l^{-1}$, thus either way we conclude that the element y is interior periodic.

For the final part, first suppose that $2(l - k) \leqslant 2(k - j)$. We then compare the entries of w_1yw_2 and v_1yv_2 from the $(2k - 1)$th place to the $(2l - 1)$th place. This tells us that the element w_1 is such that

$$(\dots, \gamma_k, \delta_k, \dots, \gamma_{l-1}, \delta_{l-1}, \gamma_l) = \left(\dots, c_kg_1, h_1, \dots, g_{l-k}, h_{l-k}, g_{l-k+1}g_1^{-1}\right).$$

As $\gamma_l = g^{-1}$, we have that the normal form of w_1 ends in $\overline{y}g^{-1}$ when $2(l - k)$ is a proper multiple of the period of x. However if the period is exactly $2(l - k)$ then $\overline{y}$ starts with the element γ_lg_1, so γ_k is equal to $c_kg(\gamma_lg_1)$.

Otherwise we have $2(k - j) \leqslant 2(l - k)$ and we replace w_1yw_2 and v_1yv_2 in the above argument with v_1yv_2 and u_1yu_2 respectively. $\square$

Our aim now is to show that we have Helfgott type growth of the triple product A^3, unless all elements in Y are (interior) periodic with the same period.

Corollary 2.6. *Let X and Y be as in Lemma 2.5. If there exists $y \in Y$ which is not interior periodic, or y is interior periodic and equal to $\bar{y}^s t$ (for $X \cup Y$ not all odd elements of the same type) or $g\bar{y}^s t\gamma$ (when $X \cup Y$ is G-odd) and there is no element in X which ends $\bar{y}$ (in the first case) or $\eta\bar{y}g^{-1}$ for some $\eta \in G$ (in the second case) then $|A^3| \geqslant (1/2592)|A|^2$.*

Proof. On taking such a y, we have by Lemma 2.5 that the map F_y is at most 2 to 1, so $|A^3| \geqslant (1/2)|X|^2$ and $|X| \geqslant (1/36)|A|$. $\square$

Proposition 2.7. *Let X and Y be as in Lemma 2.5. Then either the triple product set XYX has size at least $(1/7776)|A|^2$ or all elements of Y are interior periodic with the same period.*

Proof. Again we assume that all elements are G-odd, with the other case being covered by replacing interior periodic with periodic. We suppose that we have two elements y_1 and y_2 in Y such that $y_1 = g_1\overline{y_1}^{s_1}t_1\gamma_1$ and $y_2 = g_2\overline{y_2}^{s_2}t_2\gamma_2$ for $s_1, s_2 \geqslant 2$.

If there is a subset B_1 of X containing no elements ending in g_1^{-1} and such that $|B_1| \geqslant 1/2|X|$ then we can apply Lemma 2.5 to the map F_{y_1} but with domain restricted to $B_1 \times X$, whereupon we conclude that $|A^3| \geqslant (1/2)|B_1||X| \geqslant (1/4)|X|^2 \geqslant (1/4)(|A|/36)^2$. The same statement holds for the equivalent subset B_2 so we are left with over half of the elements in X ending in g_1^{-1}, and over half ending in g_2^{-1}. Consequently there is something in the intersection which means that in fact $g_1 = g_2 = g$ say. We now assume that the periods $\overline{y_1}$ and $\overline{y_2}$ are distinct and define similar sets S_1 and S_2 where

$$S_1 = \{x \in X\colon\ x \text{ does not end } \eta\overline{y_1}g^{-1} \text{ for some } \eta \in G\}$$

and the same for S_2. Now in a similar fashion to before, we have that if $|S_1| \geqslant (1/3)|X|$ then we can again apply Lemma 2.5 to the map F_{y_1} but this time with domain $S_1 \times X$, thus $|A^3| \geqslant (1/2)|S_1||X| \geqslant (1/6)|X|^2 \geqslant (1/6)(|A|/36)^2$. The equivalent statement holds for S_2 so we are left with the complement S_1' of S_1 in X having $|S_1'| > (2/3)|X|$ and where every element of $|S_1'|$ ends $\eta\overline{y_1}g^{-1}$ for some $\eta \in G$. Now it appears that η varies over S_1' but another appeal to Lemma 2.5 using F_{y_1} with domain $S_1' \times X$ tells us that either $|A^3| \geqslant (1/2)|S_1'||X| \geqslant (1/3)|X|^2$ or something in $|S_1'|$ ends in either $\overline{y_1}g^{-1}$ or $\omega g\overline{y_1}g^{-1}$, where ω is the last entry in some other element in S_1'. But this is always g^{-1} thus everything in S_1' does in fact end $\overline{y_1}g^{-1}$.

The same argument tells us that the complement S_2' of S_2 consists solely of elements ending $\overline{y_2}g^{-1}$, and both S_1' and S_2' consist of over two thirds of X. Thus the intersection is not empty, but now this means that one of these sets will be contained in the other. Thus we have a set S consisting of over two thirds of X where every element in S ends with both these expressions. Consequently we may as well conjugate by g so that every element in S now ends with both $\overline{y_1}$ and $\overline{y_2}$, and with the new Y containing $\overline{y_1}^{s_1}t_1\gamma_1$ and $\overline{y_2}^{s_2}t_2\gamma_2$, where we have changed γ_i by postmultiplying with g.

We have now reached a position where we can essentially follow [12], Lemmas 2, 5 and 6, for the remainder of this proof. As $\overline{y_1} \neq \overline{y_2}$, we cannot have $\sigma(\overline{y_1}) = \sigma(\overline{y_2})$ so say $\sigma(\overline{y_1}) < \sigma(\overline{y_2})$ without loss of generality. Let T be the subset of (this new) S consisting of words in S which end $\overline{y_2}^2$. However the elements in T also end in $\overline{y_1}$. Take some $x \in T$ and let $n \geqslant 1$ be such that x ends in $\overline{y_1}^n$ but not in $\overline{y_1}^{n+1}$. Now take some other $x' \in T$. If $\sigma(\overline{y_1}^n) < \sigma(\overline{y_2}^2)$ then x' also ends in $\overline{y_1}^n$. However we cannot have $\sigma(\overline{y_1}^n) \geqslant \sigma(\overline{y_2}^2)$ because then $\overline{y_2}^2$ also ends in $\overline{y_1}^2$ at least, and this element is right periodic with two different right periods $\overline{y_1}$ and $\overline{y_2}$. However we can now swap the roles of x and x' to conclude that all elements of T end in $\overline{y_1}^n$ and none end $\overline{y_1}^{n+1}$.

We use Lemma 2.5 again (but now in the case where absorption does not occur) with Y replaced by the equal sized set $\overline{y_1}^nY$ and we take the map F_{v_1} where $v_1 = \overline{y_1}^n y_1$, with domain $T\overline{y_1}^{-n} \times X$. As nothing in the first factor ends in $\overline{y_1}$, we have that $|(T\overline{y_1}^{-n})v_1X| \geqslant (1/2)|T||X|$. However we now do the same with Y replaced by $\overline{y_2}Y$ and where the map is now F_{v_2} for $v_2 = \overline{y_2}y_2$ with domain $T'\overline{y_2}^{-1} \times X$, where T' is the complement of T in S. Lemma 2.5 also tells us that $|T'\overline{y_2}^{-1}v_2X| \geqslant (1/2)|T'||X|$ because no word in $T'\overline{y_2}^{-1}$ ends in $\overline{y_2}$ and v_2 has period $\overline{y_2}$. Hence $|Ty_1X| \geqslant (1/2)|T||X|$ and $|T'y_2X| \geqslant (1/2)|T'||X|$. Now we must have either T or T' having size at least $|S|/2$, with both subsets contained in X and $y_1, y_2 \in Y$ thus $|XYX| \geqslant (1/4)|S||X| \geqslant (1/6)|X|^2 \geqslant (1/7776)|A|^2$. □

Corollary 2.8. *Let X and Y be as in Lemma 2.5. Then either the triple product set XYX has size at least $(1/7776)|A|^2$ or every y in Y is interior periodic of the form $\bar{y}^s t$ (when $X \cup Y$ is not all odd elements of the same type) or $g\bar{y}^s t\gamma$ (when $X \cup Y$ is G-odd), where $g, \bar{y}, t, \gamma$ are all independent of y.*

Proof. As usual we only treat the second case. By Proposition 2.7 we have that if the inequality fails then all elements of Y are of the form $g\bar{y}^s t\gamma$ for fixed $\bar{y}$ and the proof gives that g is fixed too, although $s \geqslant 2, t$ and γ can vary across Y. But we can now run the whole argument from Lemma 2.5 in the opposite direction, meaning that we examine the end of elements in Y and the beginning of elements coming from the second factor of X in the domain of F_y. This will tell us that either the appropriate inequality is satisfied or all elements in Y are interior right periodic, so that they are of the form $g_0 r\bar{z}^s\gamma_0$, where now γ_0 and the right period $\bar{z}$ are independent of y, although $s \geqslant 2$, the suffix r of $\bar{z}$ and g_0 can vary with y. Putting these facts together gives us our conclusion. □

We now have enough information to turn interior periodic elements into elements that are genuinely periodic.

Lemma 2.9. *Let X and Y be as in Corollary 2.8, with all elements of $X \cup Y$ being G-odd. Then either the triple product set XYX has size at least $(1/7776)|A|^2$, or $|Y^3| \geqslant (1/1296)|A|^2$, or we can conjugate A so that all elements y of Y are periodic of the form $\bar{y}^s t$, for period $\bar{y}$ and tail t independent of y.*

Proof. By applying Corollary 2.8 we can assume that all elements y_i in Y are equal to $g\bar{y}^{s_i}t\gamma$. Let $\bar{y} = (g_1, h_1, \ldots, g_N, h_N)$ and $t = (g_1, h_1, \ldots, g_k, h_k)$ for $0 \leqslant k \leqslant N-1$. We now consider $|Y^2|$ directly and we have $|A^3| \geqslant |Y^3| \geqslant |Y^2|$. On taking any $y_i, y_j \in Y$ and forming y_iy_j we look for the $\gamma g g_1$ term in the product. This spoils the periodicity, allowing us to recover s_i, s_j then y_i and y_j which implies that $|Y^2| \geqslant |Y|^2$, unless one of two cases occurs. The first is that $\gamma g g_1 = g_{k+1}$ so that the periodicity is not broken at that place. But it will be in the very next entry, unless $h_1 = h_{k+1}$, and then we require $g_2 = h_{k+2}$ and so on. On repeating this argument through the whole period, we end up with $g_1 = g_{k+1}$ as well thus implying that γg is the identity. Now γ and g are constant so all elements in Y are of the form $g\bar{y}^s t g^{-1}$ with only s varying.

The other case is if there were cancellation completely, so that $\gamma g g_1 = id$. But then the previous term is now $h_k h_1$, again spoiling the periodicity which should give the term h_k unless this cancels too. Again we repeat this argument, requiring cancellation at every stage until we have gone backwards through the whole period. Then the cancellation required at this point tells us that $g_{k+1}g_1 = id$. But putting this together with $\gamma g g_1 = id$ means that for $y = g\bar{y}^s t\gamma$ we have $g^{-1}yg = \bar{y}^s\tau$ where $\tau = (g_1, h_1, \ldots, g_k, h_k, \gamma g)$. Now $\gamma g = g_{k+1}$ so τ is a prefix of $\bar{y}$. □

We are now able to characterise those subsets with a small triple product, although this is harder than in the free group case because we must deal with infinite dihedral groups. We now start to consider the subset YAY of A^3 and we will first assume that the elements of Y have empty tail.

Theorem 2.10. *Suppose that Y is a subset of $\Gamma = G * H$ such that all elements y_i of Y are totally periodic with the same period, so of the form $\bar{y}^{s_i}$ for $s_i \geqslant 2$. Then for any $a \in \Gamma$ either $|YaY| = |Y|^2$ or a and Y together generate an infinite cyclic or infinite dihedral subgroup of Γ.*

Proof. Let us assume all elements of Y are G-even and we will set $\bar{y} = (g_1, h_1, \ldots, g_N, h_N)$. If a is G-even then there is no cancellation or absorption in forming y_iay_j, so we have that $|YaY| \geqslant |Y|^2$ by recognising the periodicity, unless a is itself periodic with period $\bar{y}$ (or a is either $\bar{y}$ or $\emptyset$). But we can assume a is not in the cyclic subgroup generated by $\bar{y}$, or else $\langle a, Y\rangle$ is an infinite cyclic subgroup.

Now suppose that a is G-odd. We will adopt a similar argument to that in the last lemma, where we look for periodicity to establish injectivity of $(y_i, y_j) \mapsto y_i a y_j$. We set $a = (a_1, b_1, \dots, b_{M-1}, a_M)$, so the a_i are in $G - I$ and the b_i in $H - I$. We begin by supposing that $a_1 \neq g_1$ so that the periodicity is broken in the very first place of a. Then on forming $\bar{y}^{s_i} a \bar{y}^{s_j}$ for various integers s_i and s_j, we see that we can again recover s_i and s_j by looking for a_1 unless either of two possibilities occur. The first is that there is cancellation on the right of a when calculating $\bar{y}^{s_i} a \bar{y}^{s_j}$ such that all entries of a are removed except a_1, whereupon absorption takes place with the relevant entry of $\bar{y}^{s_j}$, changing a_1 into g_1 and with the uncancelled part of $\bar{y}^{s_j}$ being $(h_1, g_2, \dots, h_N)$ followed by $\bar{y}$ to some smaller power. But this would require that a_1 times the first entry of $\bar{y}$ is g_1, implying that a_1 is the identity.

The other possibility is that a_1 cancels completely with the appropriate entry g_k of $\bar{y}^{s_j}$. In fact this can occur but now the start of $\bar{y}^{s_i} a \bar{y}^{s_j}$ reads $\bar{y}^{s_i - 1}(g_1, h_1, \dots, g_N, h_N h_k)$ for some k between 1 and N. This allows us again to detect periodicity unless there is further cancellation between h_N and h_k. But this argument can be repeated, thus we require further cancellation between g_N and g_{k+1}, h_{N-1} and h_{k+1} (where all subscripts are taken modulo N), and so on until we have run through a period whereupon g_1 and $g_{N+k} = g_k$ cancel too. But this means that a_1 is equal to g_1 after all.

We can now argue that if $M > 1$ then $b_1 = h_1$ as well, by considering $y_i a y_j = g_1 \bar{z}^{s_i}(b_2, \dots, b_{M-1}) a_M g_1 \bar{z}^{s_j} g_1^{-1}$, where $\bar{z} = (h_1, g_2, \dots, h_N, g_1)$. The b_2 entry destroys periodicity unless it disappears or is changed, so some cancellation is needed in the above expression for $y_i a y_j$. But this can only occur initially between a_M and g_1 (apart from at the very end which merely takes away the final g_1), and on removing $a_M g_1$ we are back in the above case on swapping G and H.

Consequently we can continue this argument to conclude that if a is a G-odd element of A such that $|YaY| < |Y|^2$ then $a = \bar{y}^k t$ for some $k \geqslant 0$ and t equal to a prefix $(g_1, h_1, \dots, h_{n-1}, g_n)$ of $\bar{y}$ for some $1 \leqslant n \leqslant N$. We may as well assume here that $a = t$ because removing powers of $\bar{y}$ from the front of a will not change the group $\langle \bar{y}, a\rangle$.

Next we move on to when a is H-even and we will show that $|YaY| < |Y|^2$ can only occur when a is a negative power of $\bar{y}$. If a begins with h_N^{-1} then we can conjugate to get $h_N \bar{y}^{s_i} h_N^{-1} = (h_N, g_1, \dots, h_{N-1}, g_N)^{s_i}$ for the elements of Y and replace a with $h_N a h_N^{-1}$, so now the elements in Y are all H-even and a is G-even thus we are back in the same position on swapping G and H. Of course there could be further cancellation but at some point this process must stop if a is not a power of $\bar{y}$. Now that there is no cancellation in forming $\bar{y}a$ for the new $\bar{y}$ and a, we can follow the same argument as for G-odd elements above where we look to see whether the first element of a spoils the periodicity. This time we find that either the first entry of a cancels with h_N in the absorption case or is the identity in the cancellation case. But both of these are contradictions.

The final type to consider is when a is H-odd, but this is the same argument as the G-odd case, only with the words running the other way when G and H are swapped. Consequently we conclude that we can have $|YaY| < |Y|^2$ here but only when $a = r\bar{y}^k$ for some $k \geqslant 0$ and r equal to a suffix $(h_n, g_{n+1}, \dots, g_N, h_N)$ of $\bar{y}$ for some $1 \leqslant n \leqslant N$. However in this case we have that $\langle \bar{y}, a\rangle = \langle \bar{y}, t\rangle$ for $t = (g_1, h_1, \dots, h_{n-1}, g_n)$.

Thus if a is such that $|YaY| < |Y|^2$ but $a \notin \langle \bar{y}\rangle$ then we have seen that we can take $a = (g_1, h_1, \dots, h_{n-1}, g_n)$ in all cases. But from before we must also have cancellation between $\bar{y}^{s_i} a$ and $\bar{y}^{s_j}$ of at least a complete period. This gives us that

$$(h_n, g_{n+1}, \dots, g_N, h_N, g_1, \dots, h_{n-1}, g_n) \quad \text{and} \quad (g_1, h_1, \dots, g_N, h_N)$$

cancel completely, so are inverses (where all subscripts are modulo N). Let us set $(x_1, x_2, \dots, x_{2N-1}, x_{2N}) = (g_1, h_1, \dots, g_N, h_N)$ so that we have

$$(x_{2n}, x_{2n+1}, \dots, x_{2N-1}, x_{2N}, x_1, \dots, x_{2n-2}, x_{2n-1}) = \left(x_{2N}^{-1}, x_{2N-1}^{-1}, \dots, x_2^{-1}, x_1^{-1}\right).$$

This implies that x_n and x_{N+n} (where we now work modulo $2N$) are self-inverse elements so both are of order 2, and we have $x_i = x_{2n-i}^{-1}$ otherwise. Now we are interested in the group generated by t and

$t^{-1}\bar{y}$ and these two elements are $(x_1, x_2, \ldots, x_{2n-1})$ and $(x_{2n}, x_{2n+1}, \ldots, x_{2N})$. Under our equations, we see that the first element is a conjugate of x_n and the second of x_{N+n}. Thus we have an infinite group generated by two elements of order 2, which must therefore be the infinite dihedral group. □

We are not quite done for the case when the elements of Y are all totally periodic, because although we have obtained our conclusion for the group generated by Y and any $a \in A$, we do not yet know what happens when we throw in all elements of A.

Proposition 2.11. *Suppose that Y is a subset of $\Gamma = G * H$ such that all elements of Y are totally periodic with the same period. Then for S any finite subset of $\Gamma = G * H$, we have that either there exists $a \in S$ with $|YaY| = |Y|^2$ or $\langle S, Y\rangle$ is an infinite cyclic or infinite dihedral group.*

Proof. We are done by the proof of Theorem 2.10 apart from one case. This is when Y is contained inside the cyclic group $C = \langle\bar{y}\rangle$ for the even element $\bar{y} = (x_1, x_2, \ldots, x_{2N})$ and there is always n between 1 and N such that each a in $S - C$ is of the form $(x_1, x_2, \ldots, x_{2n-1})$ without loss of generality. Now n could well vary with a, but whenever this occurs we have x_i and x_{2n-i} are inverse pairs for all i between 1 and $2N$. If we think of a regular $2N$-gon P having vertices labelled $x_1, x_2, \ldots, x_{2N}$ in order then any element a defines an axis through the opposite vertices x_n and x_{N+n} of P, and pairs of elements x_i, x_{2n-i} which are swapped by reflection in this axis are inverse to each other.

Now let us take all such axes obtained from the various a and consider the dihedral group D thus generated. The reflections in the first two axes, through (say) the vertices x_k, x_{N+k} and x_{k+r}, x_{N+k+r} where r divides N, generate the whole of D. In particular consider the elements $\alpha = (x_1, x_2, \ldots, x_{2k-1})$ and $\beta = (x_1, x_2, \ldots, x_{2k+2r-1})$. By the dihedral symmetry these are conjugates of x_k and x_{k+r} respectively and so are both of order two. Now any a of the form $(x_1, \ldots, x_{2n-1})$ must be represented by an axis in D and so $n = k + mr$ for some integer m depending on n. But as x_i remains the same element under adding multiples of $2r$ to the suffix, because this corresponds to a rotational symmetry which is the product of two reflections and so the inverse has been taken twice, we have that all the elements $(x_1, \ldots, x_{2k+2mr-1})$ represented by axes are given by $\alpha, \beta, \beta\alpha\beta, \beta\alpha\beta\alpha\beta, \ldots$ for $m = 0, 1, 2, 3, \ldots$. Now $(\beta\alpha)^{N/r} = \bar{y}$ so that all of S and Y is contained inside the infinite dihedral group $\langle\alpha, \beta\rangle$. Moreover any subgroup of the infinite dihedral group is itself infinite dihedral or infinite cyclic. □

We can now finish our main result.

Corollary 2.12. *Given any finite set A of the free product $\Gamma = G * H$, we have that either A is conjugate into one of the factors, or $|A^3| \geqslant (1/7776)|A|^2$, or $\langle A\rangle$ is infinite cyclic or infinite dihedral.*

Proof. We follow through the results of this section, first applying Theorem 2.2 and Lemma 2.3 to obtain subsets X, Y of (a conjugate of) A. Then Lemma 2.4 tells us that either $|A^3| \geqslant (1/5184)|A|^2$, or A is conjugate into one of the factors, or we can apply Lemma 2.5, Corollary 2.6, Proposition 2.7, Corollary 2.8 and Lemma 2.9 to X and Y. We conclude that either $|A^3| \geqslant (1/7776)|A|^2$ or we can further conjugate A so that all elements of Y are periodic with the same period $\bar{y}$ and tail t. If t is empty then Proposition 2.11 gives us that either $|A^3| \geqslant (1/1296)|A|^2$ or $\langle A\rangle$ is infinite cyclic or infinite dihedral.

For the case where $Y = \{\bar{y}^{s_i}t\}$ with tails, let us set $E = \{\bar{y}^{s_i}\}$ without the tail. Thus $Y = Et$ and $|E| = |Y|$. First note that the elements in Y^2 are of the form $\bar{y}^{s_i}t\bar{y}^{s_j}t$, which will have the same cardinality as if the final t was missing. Now let Z be the set of all a in (our final conjugate of) A along with the identity. We can regard tZ as S and E as Y in Proposition 2.11, which tells us that either there is $a \in A$ (or equal to the identity) with $|EtaE| = |Y|^2$ thus $|A^3| \geqslant |YaY| \geqslant (1/36)^2|A|^2$, or the subgroup generated by E and tZ is infinite cyclic or infinite dihedral. But as $t \in tZ$, this is the same as the subgroup generated by t, E and A, which in turn contains $\langle A\rangle$. □

Therefore we have a full understanding of growth in a free product if we understand growth of subsets in the factors: for instance:

Corollary 2.13. *Let $\Gamma = G_1 * \cdots * G_n$ be a free product of groups where the factor groups G_i are all virtually cyclic, or all virtually abelian, or all virtually nilpotent. Then for any finite subset A of Γ, we have that $|A^3| \geqslant (1/7776)|A|^2$ unless the subgroup $\langle A \rangle$ is virtually cyclic, respectively virtually abelian, respectively virtually nilpotent.*

A particular case of this is the free product of finite groups and $\mathbb{Z}$:

Corollary 2.14. *Let $\Gamma = G_1 * \cdots * G_n$ be any free product of groups where each G_i is either finite or equal to $\mathbb{Z}$. Then for any finite subset A of Γ, we have that $|A^3| \geqslant (1/7776)|A|^2$ unless the subgroup $\langle A \rangle$ is finite or infinite cyclic, or (when one of the groups G_i has even order) is equal to the infinite dihedral group $C(2) * C(2)$.*

In particular this gives that $|A^3| \geqslant (1/7776)|A|^2$ for any finite subset A of a Fuchsian group F (a non-elementary discrete subgroup of $PSL(2,\mathbb{R})$) which is not cocompact, because any finitely generated subgroup of F is a free product of (finite or infinite) cyclic groups. Thus this applies to the modular group $PSL(2,\mathbb{Z}) = C(2) * C(3)$, with A satisfying our growth condition unless $\langle A \rangle$ is cyclic or equal to $C(2) * C(2)$. This growth estimate improves a result in [11] which states that for this group we have an unspecified $d > 0$ such that $|A^3| \geqslant |A|^2/(\log|A|)^d$.

3. Other groups with Helfgott type growth

Historically the first group (or infinite sequence of groups) that was thought of as being most "free-like", after free groups themselves and free products, was probably the surface group S_g, which is the fundamental group of the closed orientable surface of genus $g \geqslant 2$. One would surely hope that this group also demonstrates Helfgott type growth, but it is not a free product (for instance see [9], Chapter II, Proposition 5.14). It is both an amalgamated free product and an HNN extension, but we will see in the next section that in general neither of these constructions give rise to groups with Helfgott type growth.

However the proof that S_g has Helfgott type growth, with the same growth expression as in Section 2, follows once we expand our interest to a wider class of groups. In fact the proof is surprisingly easy provided the right choice of groups is made.

Definition 3.1. Let $\mathcal{C}$ be a class of groups. A group G is *fully residually* $\mathcal{C}$ if for any list of k distinct elements $g_1, g_2, \dots, g_k \in G$, we have a surjective homomorphism θ from G to a group in $\mathcal{C}$ such that the images $\theta(g_1), \theta(g_2), \dots, \theta(g_k)$ are distinct.

If $\mathcal{C}$ is the class of free groups then we say that G is *fully residually free*. Such a group will be torsion free and subgroups of fully residually free groups are also fully residually free. This property implies that of being residually free but is stronger in general: for instance the direct product $G = F_k \times \mathbb{Z}$ is residually free, but any homomorphism from G to a non-abelian free group would send the generator z of $\mathbb{Z}$ to the identity. Thus if $k \geqslant 2$ and x, y are non-commuting elements of F_k then on taking the identity, z and the commutator $[x, y]$, we cannot satisfy the above definition. In fact B. Baumslag shows in [2] that if a group G is finitely generated then it is fully residually free if and only if it is residually free and does not contain $F_2 \times \mathbb{Z}$ as a subgroup.

Finitely generated fully residually free groups are also known as *limit groups* and are important in a number of areas, for instance logic and topology. Indeed recent results indicate that limit groups have a very strong claim to be the smallest naturally defined class of torsion free groups properly containing the free groups F_k.

The following result is now almost immediate.

Corollary 3.2. *Let G be a fully residually free group and let A be any finite subset of G. Then either $|A^3| \geqslant (1/7776)|A|^2$ or $\langle A \rangle$ is a free abelian subgroup of G.*

Proof. We assume that $\langle A \rangle$ is non-abelian, because a finitely generated abelian subgroup of a torsion free group is free abelian. List the elements of A as $\{a_1, a_2, \dots, a_n\}$ and assume that a_1 and a_2 do not commute. Now find a surjective homomorphism $\theta : G \mapsto F$ where F is free and the images of the set $A \cup \{[a_1, a_2], id\}$ are distinct. As $\theta([a_1, a_2])$ is not the identity, we set $S = \theta(A)$ with $|S| = n$ and note that $\langle S \rangle$ is non-abelian (and free as it is a subgroup of F). Next we apply Corollary 2.12 to S in F (or in $\langle S \rangle$ if F is infinitely generated) to obtain $|S^3| \geqslant (1/7776)n^2$. But the triple product S^3 is equal to $\theta(A^3)$ so the triple product A^3 must be at least as big. $\square$

Corollary 3.3. *If S_g is the fundamental group of a closed orientable surface of genus $g \geqslant 2$ and A is any finite subset of S_g then either $|A^3| \geqslant (1/7776)|A|^2$ or $\langle A \rangle$ is infinite cyclic.*

Proof. By [3] S_g is a limit group, and it does not contain $\mathbb{Z} \times \mathbb{Z}$. $\square$

In fact the same proof allows an immediate generalisation of Corollary 3.2: suppose $\mathcal{C}$ is a class of groups all having Helfgott type growth for the same c and δ where there is $n \in \mathbb{N}$ such that every virtually nilpotent subgroup of a member of $\mathcal{C}$ is nilpotent with class at most n. Then any group which is fully residually $\mathcal{C}$ has Helfgott type growth for this c, δ.

We finish this section by mentioning other groups shown in the literature to have Helfgott type growth. In [6], which follows closely Helfgott's original method, Helfgott type growth was established for $SL(2, \mathbb{C})$ with unspecified $c, \delta > 0$ unless $\langle A \rangle$ is finite or metabelian (note not virtually abelian as claimed there: see the example after Proposition 4.2). This was apparently generalised in [14], Theorem 4.2, which replaces $\mathbb{C}$ by any characteristic zero integral domain D and which gave the exceptions as $\langle A \rangle$ is finite or metabelian. However this is actually the same result because if we embed D into its field of fractions $\mathbb{F}$, we have that a finitely generated subgroup of $SL(2, \mathbb{F})$ is a subgroup of $SL(2, \mathbb{C})$, by embedding $\mathbb{Q}(x_1, \ldots, x_n)$ into $\mathbb{C}$, where $x_1, \ldots, x_n$ are the matrix entries of a generating set. Now this need not be true if our group G is infinitely generated but $c, \delta > 0$ are absolute constants, and so will apply to any A by working in $\langle A \rangle$.

Then in [11] it was shown that for the free group F_2 there is (an unspecified) $d > 0$ such that $|A^3| \geqslant |A|^2/(\log|A|)^d$ unless $\langle A \rangle$ is infinite cyclic (or $|A| = 1$). Thus although this does not give $\delta = 1$ for growth in F_2, it does so for every $\delta < 1$. After that we have Safin's result on free groups which was the only example up till now with $\delta = 1$. Actually this result in [11] is also shown to hold for virtually free groups G (with infinite cyclic replaced by virtually cyclic) but now d will depend on G: consider virtually free groups of the form $G = F_2 \times N$ when N is a finite group. On taking $A = \{(x, n), (y, n){:}\ n \in N\}$ for $F_2 = \langle x, y \rangle$, we have that $\langle A \rangle$ contains a copy of F_2 with $|A| = 2|N|$ but $|A^3| = 8|N|$. Thus although G has Helfgott type growth with $\delta = 1$ by Proposition 3.4 below, we see by increasing N that there is no absolute $c, \delta > 0$ (nor d in the above expression) that will work for all virtually free groups. We do not know if we can always take $\delta = 1$ (but necessarily varying c) for all virtually free groups. Similarly if G is virtually a surface group, such as the triangle groups, then G has Helfgott type growth by Corollary 3.3 and Proposition 3.6 below but again we do not know if we can take $\delta = 1$.

There are two further basic constructions, both involving finite normal subgroups, which allow us to obtain new groups with Helfgott type growth from old ones. If G has Helfgott type growth then of course arbitrary quotients of G need not possess this property, as every group is a quotient of a free group. However we do have:

Proposition 3.4. *If N is a finite normal subgroup of the infinite group G such that G/N has Helfgott type growth then G has Helfgott growth for the same δ but c replaced by $c/(|N|^{1+\delta})$. Conversely if G has Helfgott type growth then so does G/N, again with the same δ but now with c replaced by $c|N|^{\delta}$.*

Proof. This is a bit like Corollary 3.2. On being given a finite subset A of G with $H = \langle A \rangle$ not virtually nilpotent and taking the image $\pi(A) = AN/N$ of A under the natural homomorphism from G to G/N, we have that $\pi(H) = \langle \pi(A) \rangle$ is isomorphic to $H/(H \cap N)$ and so is also not virtually nilpotent. (As H is finitely generated here, a quick way of showing this is to note that the virtually polycyclic group H is residually finite so we can find a finite index subgroup L of H intersecting $S = H \cap N$ only in the identity, thus the virtually nilpotent subgroup $L = L/(L \cap S) \cong LS/S$ of H/S is also a finite index subgroup of H.) Thus $|A^3| \geqslant |\pi(A^3)| \geqslant c|\pi(A)|^{1+\delta}$ but $|\pi(A)| \geqslant |A|/|N|$.

As for the other way round, on taking $S \subseteq G/N$ with $\langle S\rangle$ not virtually nilpotent, let $A \subseteq G$ map injectively onto S under π and consider the subset AN of G with $|AN| = |A||N|$. Certainly $\pi(AN) = S$ so $\langle AN\rangle$ cannot be virtually nilpotent. Therefore $|(AN)^3| \geqslant c|AN|^{1+\delta}$ but $|A^3N| = |S^3||N|$ by counting preimages, and normality of N tells us that $(AN)^3 = A^3N$. □

This allows us to give the best possible δ and a specific $c > 0$ for $SL(2,\mathbb{Z})$, improving the results in [6] and [11] for this group.

Corollary 3.5. *The group $SL(2,\mathbb{Z})$ has Helfgott type growth with $\delta = 1$ and $c = 1/31\,104$.*

Proof. The quotient $PSL(2,\mathbb{Z})$ of $SL(2,\mathbb{Z}) = C_4 *_{C_2} C_6$ satisfies Corollary 2.12 and the kernel has size 2. □

In fact this argument works whenever we have an amalgamated free product $G = A *_N B$ of groups A and B where the amalgamated subgroup N is finite and normal in both A and B. This is because N is then normal in G (as $A \cup B$ generates G) and G/N is then isomorphic to the free product $A/N * B/N$, so Corollary 2.12 applies here.

Moreover if we want further examples with $\delta = 1$ or some other $\delta > 0$ then we can take a finite collection of groups known to have Helfgott type growth along with the minimum δ for these groups, then form their free product Γ which will not reduce δ by Corollary 2.12. We can then do other things, for instance any G with $G/N = \Gamma$ for N a finite normal subgroup will also have Helfgott type growth with the same δ, and then we can form more free products and so on.

It is immediate that a subgroup H of a group G with Helfgott type growth also has Helfgott type growth with the same c, δ. What does not seem so neat is the converse when H has finite index in G. Here we show that this is true, although we do not know whether we can always preserve the value of δ.

Proposition 3.6. *If H has Helfgott type growth and has index n in G then G also has Helfgott type growth.*

Proof. On taking $A \subseteq G$ with $\langle A\rangle$ not virtually nilpotent, which we first assume is symmetric with e, and $K \geqslant 1$ such that $|A^3| = K^2|A|$, we have $a \in A$ such that $|A \cap aH| \geqslant |A|/n$ by the pigeonhole principle. Now $\langle A\rangle \cap H$ has index at most n in $\langle A\rangle$ and so is also not virtually nilpotent. Consequently there is a generating set for $\langle A\rangle \cap H$ with word length at most $2n-1$ in terms of the elements of A (this result, which is sometimes called the Shalen–Wagreich lemma and is occasionally rediscovered, in fact follows immediately from Reidemeister–Schreier rewriting). Thus on setting $B = A^{2n-1} \cap H$ we have that $\langle B\rangle$ is not virtually nilpotent, with $a^{-1}A \cap H \subseteq B$ by the symmetry of A, thus $|B| \geqslant |A|/n$.

We now introduce $L \geqslant 1$ where $|B^3| = L^2|B|$, implying that $|B| \leqslant c^{-1/\delta}L^{2/\delta}$ where H has Helfgott type growth for this c and δ. Then

$$L^2|B| = \left|B^3\right| \leqslant \left|A^{6n-3}\right| \leqslant K^{12n-10}|A| \leqslant nK^{12n-10}|B|$$

so $L^2 \leqslant nK^{12n-10}$. Thus $|A| \leqslant (cn^{-1-\delta})^{-1/\delta}K^{(12n-10)/\delta}$, giving tripling of symmetric subsets. In general we set $S = A \cup A^{-1} \cup \{e\}$ so that $8|A^3| \geqslant |S^3|$ and $|S| \geqslant |A|$, giving Helfgott type growth in G with c replaced by $cn^{-(1+\delta)}/8$ and δ replaced by $\delta/(6n-5)$. □

4. Groups without Helfgott type growth

We first show that $\delta = 1$ is the best possible value for a group with Helfgott type growth, with the exception of one particular class of groups.

Proposition 4.1. *If G has Helfgott type growth for some $c > 0$ and $\delta > 1$ then either G is locally virtually nilpotent or G has bounded exponent.*

Proof. If all finitely generated subgroups of G are virtually nilpotent then G vacuously has Helfgott type growth for any $c, \delta > 0$. Otherwise let $H = \langle g_1, \dots, g_l \rangle$ be a subgroup of G that is not virtually nilpotent. We take x_N to be an element of G with infinite order, or order at least $2N$, and set $A = \{g_1, \dots, g_l, x_N, x_N^2, \dots, x_N^N\}$. Thus $N \leqslant |A| \leqslant N + l$ with $H \leqslant \langle A \rangle$ but a quick count reveals that $|A^2| \leqslant 2(l+1)N - 2 + l^2$. This means that $|A^3| \leqslant |A||A^2| < 2(l+1)N(N+l) + l^2(N+l)$ so Helfgott type growth would imply that the right hand side of this inequality is always greater than $cN^{1+\delta}$. We now let $N \to \infty$ to get a contradiction if $\delta > 1$. □

Note that the existence of finitely generated infinite groups with bounded exponent is highly non-trivial. We have a result on this in [8] using model theory: Corollary 4.18 states that there is a function $f(K, e)$ such that if G is any group with exponent dividing e and A is a K-approximate group in G then there exists a subgroup H of G such that A and H are contained in $f(K, e)$ left cosets of each other. In particular let us take the examples of Ol'shanskiĭ where for a sufficiently large prime p we have a 2 generator infinite group $G(p)$ of exponent p such that the only proper non-trivial subgroups are cyclic of order p. Then this result implies that any K-approximate group A in $G(p)$ has $|A| \leqslant pf(K, p)$ so it could happen that $G(p)$ has Helfgott type growth if f were polynomial in K. However this function is not given explicitly.

We now discuss examples of groups without Helfgott type growth. First we elaborate on our comment in the introduction that balls in virtually nilpotent groups always provide examples of approximate groups. Here a ball in a finitely generated group G is just S^n for some $n \in \mathbb{N}$ where S is a finite symmetric subset containing e and generating G. By a result of Bass, if G is virtually nilpotent then there is $C, c, d > 0$ such that $cn^d \leqslant |S^n| \leqslant Cn^d$ for all n, thus on taking $A = S^n$ we have $|A| \to \infty$ but $|A^3|/|A| \leqslant C3^d/c$. Conversely if in a finitely generated group G there is S and $\lambda \geqslant 1$ such that $|S^{3n}| \leqslant \lambda|S^n|$ for all n then $|S^{3^n}| \leqslant \lambda^n|S|$, giving $|S^m| \leqslant m^s|S|$ for $m = 3^n$ (and $s = \log_3 \lambda$). By an extension of Gromov's famous theorem on polynomial growth due to Van der Dries and Wilkie, if the sequence $|S^n|$ has a subsequence with polynomial growth then G is virtually nilpotent. (In fact even if $|S^{3n'}| \leqslant \lambda|S^{n'}|$ for infinitely many n', we obtain the same conclusion from the results of [4] by following the proof of Theorem 1.13: this is because $S^{2n'}$ is a μ-approximate group for μ depending only on λ and arbitrarily high n'.)

Consequently we see that virtually nilpotent groups will always have finite subsets, indeed naturally defined finite subsets at that, which possess small tripling thus showing why we require virtually nilpotent subgroups to be removed from the definition of Helfgott type growth.

But what about examples of other approximate groups? For instance in the introduction to [4] eight examples of how to construct approximate groups are given but all of these generate virtually nilpotent groups. We can adapt the basic idea in Proposition 4.1 so we start by examining it in more detail. We see that A^3 is made up of eight different types of product, according to whether we choose an element g_i or a power x_N^i in each of the three places. It is also clear that the sizes of seven of these eight types are each linear in N but the interesting point is the size of $\{x_N^i g_k x_N^j\}$ for $1 \leqslant i, j \leqslant N$ and $1 \leqslant k \leqslant l$, which will determine whether $|A^3|/|A|$ stays bounded as $N \to \infty$. For instance we mentioned in the introduction the case of $F_n \times \mathbb{Z}$ which is the only example of a non-virtually nilpotent group without Helfgott type growth given so far. It might seem that this is a particular manifestation of the direct product but in fact it is much more general.

Proposition 4.2. *If G is a group possessing an element z of infinite order such that its centraliser $C(z)$ in G contains a finitely generated subgroup which is not virtually nilpotent then G does not have Helfgott type growth.*

Proof. If H is such a subgroup (which contains z without loss of generality) then extend $\{z\}$ to a finite generating set $\{z, h_1, \dots, h_l\}$ of H where no h_i is in $\langle z \rangle$. Thus the set $A_N = \{z, \dots, z^N, h_1, \dots, h_l\}$ of size $N + l$ has $\langle A_N \rangle = H$ and any element in A_N^3 of the form $z^i h_k z^j$ can be written as $h_k z^{i+j}$, thus $|A_N^3|/|A_N|$ is bounded. □

Continuing this theme, suppose that in a group G we can take x of infinite order and g such that $\langle x, g\rangle$ is not virtually nilpotent. On setting $A = \{g, x, x^2, \dots, x^N\}$ we can examine the subset $\{x^i g x^j\colon\ 1 \leqslant i, j \leqslant N\}$ of A^3. If this achieves its maximum size of N^2 then we obtain sets A with $\langle A\rangle$ not virtually nilpotent and $|A^2| < 4|A|$ but $|A^3|/|A| \to \infty$ as $N \to \infty$, which was mentioned in the introduction. Otherwise a collision occurs, namely there exist $(i, j) \neq (k,l)$ such that $x^i g x^j = x^k g x^l$. Now $i = k$ gives rise to a contradiction on the order of x and similarly we see that $j \neq l$. Thus we have the relation $g x^{j-l} g^{-1} = x^{k-i}$ holding in our group G, suggesting the famous family in combinatorial group theory of Baumslag–Solitar groups $BS(m,n)$ for integers $m, n \neq 0$ which are defined by the presentation $\langle x, g | g x^m g^{-1} = x^n\rangle$. Indeed it can be shown using normal forms (although we give a much more general result below in Theorem 4.3) that if a group G contains a Baumslag–Solitar group $BS(m,n)$ where $|m|, |n|$ are not both equal to 1 (or even the image of a Baumslag–Solitar group where x has infinite order and such that the image is not virtually nilpotent) then G does not have Helfgott type growth, because $|A_N^3| < (10 + |m| + |n|)|A_N|$ for the set A_N above.

The reason for excluding the group $BS(\pm 1, \pm 1)$ is because it is either $\mathbb{Z} \times \mathbb{Z}$ or has $\mathbb{Z} \times \mathbb{Z}$ as an index 2 subgroup, so is virtually nilpotent. Otherwise $BS(m,n)$ is not virtually nilpotent, indeed if neither $|m|$ nor $|n|$ is equal to 1 then $BS(m,n)$ contains a non-abelian free group. The interesting case is when $|m| = 1$, say $m = 1$ without loss of generality, but $|n| \neq 1$ as then $BS(1,n)$ is metabelian but not virtually nilpotent. Moreover $BS(1,n)$ is linear, in fact is a subgroup of $SL(2,\mathbb{C})$ on taking

$$x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad y = \begin{pmatrix} \sqrt{n} & 0 \\ 0 & \sqrt{1/n} \end{pmatrix}$$

so is also a subgroup of $SL(2,\mathbb{R})$ for $n \geqslant 2$ and is even in $SL(2,\mathbb{Q})$ when n is a square. We mention this because in [6] it is claimed that $SL(2,\mathbb{C})$ has Helfgott type growth with the exception of virtually abelian subgroups, but on putting $n = 4$ in these matrices we have that the set A_N in $BS(1,4)$ from above satisfies $|A_N|^3 < 15|A_N|$ even though $\langle A_N\rangle$ is not virtually abelian. The correct statement is that there is Helfgott type growth away from metabelian and finite subgroups, as shown in Theorem 4.2 of [14].

We now give our generalisation of these examples.

Theorem 4.3. *Suppose that V is a finitely generated, virtually nilpotent, infinite subgroup of G. If there is $g \in G$ and a finite index subgroup W of V such that $gWg^{-1} \leqslant V$ but $\langle g, V\rangle$ is not virtually nilpotent then G does not have Helfgott type growth.*

Proof. Let $v_1, \dots, v_r$ be a transversal for W in V and let S be a finite symmetric generating set for W containing e. We set $A_n = \{g, v_1, \dots, v_r, S^n\}$ and $X = \{g, v_1, \dots, v_r\}$ so that $\langle A_n\rangle = \langle g, V\rangle$ is not virtually nilpotent and $|A_n| \to \infty$ because W is infinite. Therefore we are done on showing $|A_n^3|/|A_n|$ is bounded. As in our examples earlier in this section, we need only check $|S^n X S^n|$ as the other seven subsets have size at most S^{3n}, with $cn^d \leqslant |S^n| \leqslant Cn^d$ because W is virtually nilpotent.

On extending S to a generating set U for V, we also have $b, B > 0$ such that $bn^d \leqslant |U^n| \leqslant Bn^d$. Now there exists a positive integer k which is independent of n such that for all $s \in S$ and $x \in X$ we have $xsx^{-1} \in U^k$ by taking the maximum of the word lengths of these conjugates with respect to U, as xsx^{-1} is always in V. Thus for all $n \in \mathbb{N}$ and $x \in X$ we have $xS^n x^{-1} \subseteq U^{nk}$ and $S^n \subseteq U^n$, so $S^n x S^n \subseteq U^{n(k+1)}x$. This gives $|S^n x S^n|/|S^n| \leqslant (Bn^d(k+1)^d)/(cn^d)$ thus $|S^n X S^n| < (B/c)(k+1)^d |A_n|$. $\square$

Corollary 4.4. *A virtually polycyclic group G does not have Helfgott type growth (unless it is virtually nilpotent).*

Proof. If G is virtually nilpotent then it has Helfgott type growth from the definition. Otherwise by dropping to a finite index subgroup we can assume there is

$$\{e\} = G_n \trianglelefteq G_{n-1} \trianglelefteq \cdots \trianglelefteq G_0 = G \quad \text{with} \quad G_i/G_{i+1} \cong \mathbb{Z}.$$

Let j be the largest integer such that G_j is not virtually nilpotent then G_{j+1} is finitely generated, virtually nilpotent and infinite. On taking $g \in G_j$ which projects onto a generator of G_j/G_{j+1} we have that $gG_{j+1}g^{-1} = G_{j+1}$ but $G_j = \langle g, G_{j+1}\rangle$ is not virtually nilpotent so Theorem 4.3 applies. $\square$

Corollary 4.5. *The group $SL(3,\mathbb{Z})$ does not have Helfgott type growth.*

Proof. The polycyclic group $\mathbb{Z}^2 \rtimes_\alpha \mathbb{Z}$ with $\mathbb{Z}^2 = \langle x, y\rangle$ and $\mathbb{Z} = \langle t\rangle$ given by $txt^{-1} = \alpha(x) = x^2y, tyt^{-1} = \alpha(y) = xy$ is not virtually nilpotent because no non-identity element has a centraliser of finite index but embeds in $SL(3,\mathbb{Z})$ (and in fact also in $SL(2,\mathbb{C})$ via Theorem 5.1 of [5]) via

$$x = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad y = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad t = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & -1 & 2 \end{pmatrix}. \qquad \square$$

Note that this gives genuinely different examples of approximate groups (for instance, if g is an element of infinite order in $SL(3,\mathbb{Z})$ then its centraliser is virtually nilpotent so Proposition 4.2 does not apply). We also obtain from Theorem 4.3 the Baumslag–Solitar examples mentioned earlier by taking $V = \langle x\rangle$ and $W = \langle x^m\rangle$. In fact if neither $|m|$ nor $|n|$ is equal to 1 then $BS(m,n)$ does satisfy the conditions of Proposition 4.2 but the centraliser of any element in $BS(1,n)$ is abelian (though it need not be finitely generated abelian) so this is not covered by Proposition 4.2.

Baumslag–Solitar groups are fundamental examples of HNN extensions in that the base and amalgamated subgroups are just copies of $\mathbb{Z}$. As for amalgamated free products, we can similarly form the group $\langle x, y | x^2 = y^3\rangle$ which is not virtually nilpotent; indeed it is the fundamental group of the trefoil knot. Now the infinite order element $z = x^2 = y^3$ is central (as it commutes with both x and y), so this group does not have Helfgott type growth by applying either Proposition 4.2 or Theorem 4.3. Moreover if we are to find further examples with Helfgott type growth, we must only look at groups where our two results do not apply. We finish with two questions on particular groups of this type.

1. Do all word hyperbolic groups have Helfgott type growth?
2. Is there a soluble (but not locally virtually nilpotent) group with Helfgott type growth?

References

[1] L. Babai, N. Nikolov, L. Pyber, Product growth and mixing in finite groups, in: Proceedings of the Nineteenth Annual ACM-SIAM Symposium on Discrete Algorithms, ACM, New York, 2008, pp. 248–257.
[2] B. Baumslag, Residually free groups, Proc. Lond. Math. Soc. 17 (1967) 402–418.
[3] G. Baumslag, On generalised free products, Math. Z. 78 (1962) 423–438.
[4] E. Breuillard, B. Green, T. Tao, The structure of approximate groups, http://arxiv.org/abs/1110.5008, 2012.
[5] J.O. Button, Groups possessing only indiscrete embeddings in $SL(2,\mathbb{C})$, http://arxiv.org/abs/1210.2691, 2012.
[6] M.-C. Chang, Product theorems in SL_2 and SL_3, J. Inst. Math. Jussieu 7 (2008) 1–25.
[7] H.A. Helfgott, Growth and generation in $SL_2(\mathbb{Z}, /p\mathbb{Z})$, Ann. of Math. 167 (2008) 601–623.
[8] E. Hrushovski, Stable group theory and approximate subgroups, J. Amer. Math. Soc. 25 (2012) 189–243.
[9] R.C. Lyndon, P.E. Schupp, Combinatorial Group Theory, Springer-Verlag, Berlin, Heidelberg, New York, 1977.
[10] W. Magnus, A. Karrass, D. Solitar, Combinatorial Group Theory, Dover Publications, Inc., Mineola, New York, 1976.
[11] A.A. Razborov, A product theorem in free groups, http://people.cs.uchicago.edu/~razborov/files/free_group.pdf, 2007.
[12] S. Safin, Powers of sets in free groups, translation in Sb. Math. 202 (2011) 1661–1666.
[13] T. Tao, Product set estimates for non-commutative groups, Combinatorica 28 (2008) 547–594.
[14] V.H. Vu, M. Matchett Wood, P. Matchett Wood, Mapping incidences, J. Lond. Math. Soc. 84 (2011) 433–445.