



On a conjecture of Gowers and Long

Ben Green

ABSTRACT

We show that rounding to a δ -net in $\mathrm{SO}(3)$ is not close to a group operation, thus confirming a conjecture of Gowers and Long.

1. Introduction

In a very interesting recent preprint [7], Gowers and Long considered somewhat associative binary operations, that is to say maps $\circ : X \times X \rightarrow X$ on a finite set X which satisfy the associativity relation $x \circ (y \circ z) = (x \circ y) \circ z$ for a positive fraction of $(x, y, z) \in X^3$. Their main result is that such operations are all near (in a sense they make precise) to the group operation on a metric group G .

It is natural to ask whether more might be true, namely whether such a binary operation \circ must actually agree with a group operation a positive fraction of the time. In their paper, Gowers and Long present an example of an operation for which they conjecture (see [7, Conjecture 1.6]) that this is not the case. In view of their main result, the example is rather natural: one takes a natural and tractable example of a non-abelian metric group G , namely $\mathrm{SO}(3)$, and a large but finite subset $X \subset G$. One then defines $\circ : X \times X \rightarrow X$ to be close to the group operation on G .

Here are the details. Take $\mathrm{SO}(3)$ with the group operation denoted by juxtaposition and with, for definiteness, the (bi-invariant) metric $d : \mathrm{SO}(3) \times \mathrm{SO}(3) \rightarrow [0, 2^{3/2}]$ given by $d(g, h) := \|g - h\|$, where $\|g\|$ is the Frobenius (or Hilbert–Schmidt) norm $\|M\| := \sqrt{\mathrm{tr}(M^T M)}$.

Throughout the paper we will take $\delta > 0$ to be a small parameter, and let X be a maximal δ -separated subset of $\mathrm{SO}(3)$. We have $|X| \sim \delta^{-3}$. Define a binary operation $\circ : X \times X \rightarrow X$ by defining $x \circ y$ to be the nearest point of X to xy (breaking ties arbitrarily). Since X is assumed to be maximal δ -separated, we always have

$$d(x \circ y, xy) \leq \delta. \quad (1.1)$$

CLAIM (Gowers–Long). For a positive proportion of triples $(x_1, x_2, x_3) \in X^3$ we have the associativity relation $(x_1 \circ x_2) \circ x_3 = x_1 \circ (x_2 \circ x_3)$.

As remarked above, Gowers and Long note that it seems very unlikely that any substantial portion of the multiplication table of \circ can be embedded in a group operation, and make a precise conjecture, [7, Conjecture 1.6], to this effect. The following result establishes their conjecture.

Received 26 November 2019; revised 3 April 2020.

2010 *Mathematics Subject Classification* 08A72, 11B30 (primary).

The author is supported by a Simons Investigator Grant.

© 2020 The Authors. *Bulletin of the London Mathematical Society* published by John Wiley & Sons Ltd on behalf of London Mathematical Society. This is an open access article under the terms of the [Creative Commons Attribution](#) License, which permits use, distribution and reproduction in any medium, provided the original work is properly cited.

THEOREM 1.1. *Let X be a maximal δ -separated subset of $\mathrm{SO}(3)$ with the associated binary operation \circ as defined above. Suppose that $\iota : X \rightarrow G$ is an injective map into a group G , with group operation \cdot . Then the number of pairs $(x_1, x_2) \in X \times X$ with $\iota(x_1) \cdot \iota(x_2) = \iota(x_1 \circ x_2)$ is at most $\varepsilon|X|^2$, where $\varepsilon \rightarrow 0$ as $\delta \rightarrow 0$.*

We remark that we do not obtain any effective information on the speed at which $\varepsilon \rightarrow 0$. This is because we rely on the structure theory of approximate groups [2], which uses ultrafilter arguments.

Notation. Our notation is fairly standard. Occasionally we will write, for instance, $o_{K;\delta \rightarrow 0}(1)$, which means some quantity tending to zero as $\delta \rightarrow 0$, but the rate at which this happens may depend on the parameter K . We write $X \gg Y$ to mean $X \geq cY$ for some absolute $c > 0$, and $X \sim Y$ means $Y \ll X \ll Y$.

Recall that $\|\cdot\|$ denotes the Hilbert–Schmidt norm and that we use this to define a distance on $\mathrm{SO}(3)$ by $d(g, h) := \|g - h\|$, where $\mathrm{SO}(3)$ is embedded in the space of 3-by-3 matrices by fixing an orthonormal basis for \mathbf{R}^3 . We write $|g| = d(g, 1)$ for the distance to the identity (which we will always denote by 1, the underlying group hopefully being clear from context). It may be computed that $|g| = 2^{3/2}|\sin(\theta/2)|$, where θ is the angle of the rotation g . Recall that the Hilbert–Schmidt norm is submultiplicative (that is, $\|ab\| \leq \|a\|\|b\|$ for all real 3-by-3 matrices). Additionally, using the conjugation invariance of trace and the fact that $g^T = g^{-1}$ for $g \in \mathrm{SO}(3)$, we have the $\mathrm{SO}(3)$ -invariance $\|a\| = \|ag\| = \|ga\|$ for all 3-by-3 matrices a and all $g \in \mathrm{SO}(3)$. In particular, $gN_\delta(1) = N_\delta(1)g$ for all $g \in \mathrm{SO}(3)$, where $N_\delta(1)$ denotes the δ -neighbourhood of 1.

2. An initial reduction

We can fairly quickly reduce the task of proving Theorem 1.1 to that of establishing the following proposition which, since it does not involve the awkward \circ , is of a more conventional type.

PROPOSITION 2.1. *Let $\varepsilon, \delta > 0$. Let (G, \cdot) be a group, and let A be a finite subset of G of size n . Let $f : A \rightarrow \mathrm{SO}(3)$ be a map with δ -separated image, and with the property that there are at least εn^3 quadruples $(a_1, a_2, a_3, a_4) \in A^4$ with $a_1 \cdot a_2 = a_3 \cdot a_4$ and $d(f(a_1)f(a_2), f(a_3)f(a_4)) \leq \delta$. Then $n = o_{\varepsilon;\delta \rightarrow 0}(\delta^{-3})$.*

Proof of Theorem 1.1, assuming Proposition 2.1. Let X , $|X| = n$, be a maximal δ -net in $\mathrm{SO}(3)$, suppose that $\iota : X \rightarrow G$ is an injection from X into a group (G, \cdot) and that there are εn^2 pairs $(x_1, x_2) \in X \times X$ with $\iota(x_1) \cdot \iota(x_2) = \iota(x_1 \circ x_2)$. Take $A := \iota(X) \subset G$, and let $f : A \rightarrow \mathrm{SO}(3)$ be the inverse of ι . Let $\Omega \subset A \times A$ be the set of all pairs (a_1, a_2) , $a_1 = \iota(x_1)$, $a_2 = \iota(x_2)$, such that $a_1 \cdot a_2 = \iota(x_1 \circ x_2)$. Thus $|\Omega| \geq \varepsilon n^2$, and if $(a_1, a_2) \in \Omega$ then $a_1 \cdot a_2 \in A$. For $a \in A$, let $r(a)$ denote the number of pairs $(a_1, a_2) \in \Omega$ such that $a_1 \cdot a_2 = a$. Thus $\sum_{a \in A} r(a) \geq \varepsilon n^2$ and so, by Cauchy–Schwarz,

$$\sum_{a \in A} r(a)^2 \geq \frac{1}{|A|} \left(\sum_{a \in A} r(a) \right)^2 \geq \varepsilon^2 n^3.$$

The sum on the left is counting the number of quadruples (a_1, a_2, a_3, a_4) with $a_1 \cdot a_2 = a_3 \cdot a_4$ and $(a_1, a_2), (a_3, a_4) \in \Omega$. From the definition of Ω we have, for any such quadruple,

$$f(a_1) \circ f(a_2) = f(a_1 \cdot a_2) = f(a_3 \cdot a_4) = f(a_3) \circ f(a_4).$$

By (1.1) we also have

$$d(f(a_1) \circ f(a_2), f(a_1)f(a_2)), d(f(a_3) \circ f(a_4), f(a_3)f(a_4)) \leq \delta.$$

It follows from the triangle inequality that

$$d(f(a_1)f(a_2), f(a_3)f(a_4)) \leq 2\delta.$$

Applying Proposition 2.1 (with δ replaced by 2δ and ε by ε^2), we see that $|X| = n = o_{\varepsilon, \delta \rightarrow 0}(\delta^{-3})$, a contradiction if δ is small enough as a function of ε . \square

3. Outline of the rest of the argument

In this section we outline the rest of the argument. Recall that a K -approximate group is a subset B of some ambient group which is symmetric (that is, it contains the identity 1, and $B^{-1} = B$) and such that B^2 is covered by K left- (or equivalently right-) translates of B . See [10] for further discussion and background. Note that approximate groups need not be finite.

In the next section, we show that the existence of a map f as in Proposition 2.1 would imply the existence of an approximate homomorphism from a finite approximate group to $\mathrm{SO}(3)$ with a ‘thick’ image. In discussing approximate homomorphisms ϕ it is natural to introduce the notion of cocycle, defining $\partial\phi(x, y) := \phi(y)^{-1}\phi(x)^{-1}\phi(xy)$.

PROPOSITION 3.1. *Let $\varepsilon, \delta > 0$. Let (G, \cdot) be a group, and let A be a finite subset of G of size $n \sim \delta^{-3}$. Let $f : A \rightarrow \mathrm{SO}(3)$ be a map with δ -separated image, and with the property that there are at least εn^3 quadruples $(a_1, a_2, a_3, a_4) \in A^4$ with $a_1 \cdot a_2 = a_3 \cdot a_4$ and $d(f(a_1)f(a_2), f(a_3)f(a_4)) \leq \delta$. Then there is a finite K -approximate group $B \subset G$, $K \ll_{\varepsilon} 1$, and a map $\phi : B^{12} \rightarrow \mathrm{SO}(3)$ with the following two properties. First, ϕ has thick image in the sense that $\mu(N_{\delta}(\phi(B^4))) \sim_{\varepsilon} 1$. Second, ϕ is an approximate homomorphism in the sense that there is a set $S \subset \mathrm{SO}(3)$, $|S| \ll_{\varepsilon} 1$, such that whenever $x, y, xy \in B^{12}$ we have $d(\partial\phi(x, y), S) \leq \delta$.*

REMARKS. Here N_{δ} means the δ -neighbourhood (in the metric d) and μ is the normalised Haar measure on $\mathrm{SO}(3)$. As we will see, no particular properties of $\mathrm{SO}(3)$ are used in the proof, beyond the existence of d and μ and their basic properties. Note that the ‘approximateness’ of ϕ , whilst of two different types (the error set S and the parameter δ) is all in the range, whereas f is approximate in the domain, in that the weak homomorphism property only holds some of the time. This idea of moving the ambiguity from the domain to the range follows a line of argument pioneered by Gowers in his seminal works [5, 6] (based also on work of Ruzsa). Proposition 3.1 is a consequence of the metric entropy version of the non-commutative Balog–Szemerédi–Gowers theorem of Tao [10].

Proposition 2.1, and hence Theorem 1.1, follows immediately from Proposition 3.1 and the next result, which says that the two properties of ϕ in the conclusion of Proposition 3.1 are incompatible: an approximate homomorphism from a finite approximate group to $\mathrm{SO}(3)$ has a thin image.

PROPOSITION 3.2. *Let B be a finite K -approximate group, let $S \subset \mathrm{SO}(3)$ be a set of size at most K , and suppose that $\phi : B^{12} \rightarrow \mathrm{SO}(3)$ satisfies $d(\partial\phi(x, y), S) \leq \delta$ whenever $x, y, xy \in B^{12}$. Then $\mu(N_{\delta}(\phi(B^4))) = o_{K, \delta \rightarrow 0}(1)$.*

The proof of this uses quite different techniques and we appeal to some fairly specific features of $\mathrm{SO}(3)$, though it would probably be possible to adapt the proof so as to work with $\mathrm{SO}(3)$ replaced by, for example, any simple Lie group. We divide into two cases, according to whether or not the cocycle $\partial\phi$ takes values far from the identity. Recall that, for $g \in \mathrm{SO}(3)$, $|g|$ means $d(g, 1)$.

Case 1. There exist $x, y \in B^4$ with $|\partial\phi(x, y)| > \sqrt{\delta}$. Then a fairly direct argument shows that $\phi(B^4)$ must lie in a union of $O(1)$ translates of an ‘almost centraliser’ of $\partial\phi(x, y)$, and a further argument shows this has small measure.

Case 2. We have $|\partial\phi(x, y)| < \sqrt{\delta}$ for all $x, y \in B^4$, that is to say ϕ satisfies $\phi(xy) \approx \phi(x)\phi(y)$ up to an error of $\sqrt{\delta}$ in the range. If $B = B^4$ were actually a finite group, a result of Kazhdan [9] then implies that we can correct ϕ by $O(\sqrt{\delta})$ to get a genuine homomorphism $\tilde{\phi} : B \rightarrow \mathrm{SO}(3)$. In particular, $\phi(B^4)$ lies within $O(\sqrt{\delta})$ of a finite subgroup of $\mathrm{SO}(3)$. However, these are all cyclic, dihedral or contained in S_5 and hence $\phi(B^4)$ is ‘thin’ in the sense discussed above. It is tempting to try and mimic the arguments of [9] when B is merely an approximate group, but this does not work in any obvious way. Rather we use the classification of approximate groups due to Breuillard, Tao and the author [2] and then invoke Kazhdan’s result as a black box, ending up showing that $\phi(B^4)$ can be partitioned into $O(1)$ pieces, each of which almost satisfies a non-trivial word equation, which then implies that $\phi(B^4)$ is thin. In particular we do not prove that ϕ can be corrected to a homomorphism $\tilde{\phi}$; it would be interesting to explore this direction. For further remarks see Section 7.

4. An application of Tao’s metric entropy BSG theorem

In this section we establish Proposition 3.1. Let $\mathbf{G} := G \times \mathrm{SO}(3)$, and let $\mathbf{d} : \mathbf{G} \times \mathbf{G} \rightarrow \mathbf{G}$ be the product of the discrete (extended) metric d_{triv} on G , where the distance between distinct points is ∞ , and the metric d on $\mathrm{SO}(3)$. Let $\boldsymbol{\mu} = \mu_{\mathrm{triv}} \times \mu$, where μ_{triv} is the counting measure on G (that is, the measure of any finite set $A \subset G$ is simply $|A|$) and μ is normalised Haar measure on $\mathrm{SO}(3)$. The group \mathbf{G} , endowed with the measure $\boldsymbol{\mu}$ and the (extended) metric \mathbf{d} , is *locally reasonable* in the sense of Tao [10, Definition 6.3][†].

To state the result from [10] that we will need, we recall the definition of covering numbers used in that paper: if X is a subset of a metric space, $\mathcal{C}_\eta(X)$ is the least number of balls of radius η necessary to cover X . We also define the η -approximate multiplicative energy $E_\eta(X, X)$ of a set to be $\mathcal{C}_\eta(Q_\eta(X, X))$, where

$$Q_\eta(X, X) := \{(x_1, x_2, x_3, x_4) \in X^4 : \mathbf{d}(x_1x_2, x_3x_4) \leq \eta\}.$$

The metric entropy here is with respect to the product metric on X^4 .

The following is the implication (i) \Rightarrow (iv) of [10, Theorem 6.10], specialised to our setting.

PROPOSITION 4.1 (Tao). *Suppose that $E_\eta(X, X) \geq \frac{1}{K}\mathcal{C}_\eta(X)^3$. Then there exists a $K^{O(1)}$ -approximate subgroup $H \subset \mathbf{G}$ and an element $g \in \mathbf{G}$ such that (1) $\mathcal{C}_\eta(H) \sim K^{O(1)}\mathcal{C}_\eta(X)$ and (2) $\mathcal{C}_\eta(X \cap gH) \sim K^{O(1)}\mathcal{C}_\eta(X)$.*

Proof of Proposition 3.1. Let us first recall the hypotheses under which we are operating, which are those of Proposition 3.1, namely that $f : A \rightarrow \mathrm{SO}(3)$ is a map with the property that there are at least εn^3 quadruples (a_1, a_2, a_3, a_4) with $a_1 \cdot a_2 = a_3 \cdot a_4$ and $d(f(a_1)f(a_2), f(a_3)f(a_4)) \leq \delta$.

Take $X = \{(a, f(a)) : a \in A\} \subset \mathbf{G}$ to be the graph of f . Let $\pi : \mathbf{G} \rightarrow G$ be projection. Then, since π is injective on X and the metric on G is discrete,

$$\mathcal{C}_\delta(X) = |X| = |A| = n.$$

[†]Although Tao does not explicitly allow extended metrics, this creates no problems in his arguments, and is necessary to ensure the doubling property $\mu_{\mathrm{triv}}(B(2r)) \sim \mu_{\mathrm{triv}}(B(r))$ for balls $B()$ in the discrete (extended) metric. In fact if one applies his results to the discrete (extended) metric, one recovers the standard finitary theory of non-commutative sumset estimates.

By assumption, $|Q_\delta(X, X)| \geq \varepsilon n^3$. Since $\pi^{\otimes 4} : \mathbf{G}^4 \rightarrow G^4$ is injective on $Q_\delta(X, X)$, we have $E_\delta(X, X) = |Q_\delta(X, X)| \geq \varepsilon n^3$. Therefore the hypothesis of Proposition 4.1 is satisfied with $K = \varepsilon^{-1}$. For the rest of the proof of Proposition 3.1, all instances of the \gg , \ll and $O()$ notations may depend on ε but this will not be explicitly indicated. Applying Proposition 4.1, we obtain an $O(1)$ -approximate subgroup $H \subset \mathbf{G}$ and an element $g = (x, y) \in \mathbf{G}$ satisfying

$$\mathcal{C}_\delta(H) \sim \mathcal{C}_\delta(X \cap gH) \sim \mathcal{C}_\delta(X) = n. \quad (4.1)$$

Let $B_0 := \pi(g^{-1}X \cap H)$. Using the fact that π is injective on X and that G is discrete, we have

$$|B_0| = |\pi(g^{-1}X \cap H)| = |X \cap gH| \sim n. \quad (4.2)$$

Using the fact that the metric on G is discrete once more, we also have $|\pi(H)| \leq \mathcal{C}_\delta(H)$, and hence from (4.1), (4.2) it follows that

$$|\pi(H)| \sim n. \quad (4.3)$$

(Note that H itself may well be infinite.) Let $\phi : B_0 \rightarrow \mathrm{SO}(3)$ be such that $(b, \phi(b)) \in g^{-1}X \cap H$ for all $b \in B_0$. Then $\phi(b)$ takes values in $y^{-1}f(A)$ and hence (since the metric on $\mathrm{SO}(3)$ is bi-invariant) is δ -separated.

Now the property of being an approximate group is preserved under π . Thus $\pi(H)$ is an $O(1)$ -approximate group and in particular $|\pi(H)^3| \ll |\pi(H)|$. From (4.2), (4.3) it follows that $|B_0^3| \ll |B_0|$. Therefore by [10, Corollary 3.11] we see that $B := (B_0 \cup \{1\} \cup B_0^{-1})^3$ is an $O(1)$ -approximate group.

Extend ϕ to a map from B^{12} to $\mathrm{SO}(3)$ as follows: for each $x \in B^{12} \setminus B_0$, write $x = b_1^{\varepsilon_1} \cdots b_{36}^{\varepsilon_{36}}$ with $\varepsilon_1, \dots, \varepsilon_{36} \in \{-1, 0, 1\}$ and $b_1, \dots, b_{36} \in B_0$. If there is more than one such representation of a given x , choose one arbitrarily. Now define

$$\phi(x) := \phi(b_1)^{\varepsilon_1} \cdots \phi(b_{36})^{\varepsilon_{36}}.$$

Note that $\phi(B^4)$ contains $\phi(B_0)$ which, as observed above, is a collection of $\sim n$ δ -separated points. Since $n \sim \delta^{-3}$ (and the volume of a $(\delta/2)$ -neighbourhood in $\mathrm{SO}(3)$ is $\sim \delta^3$), it follows that $\mu(N_\delta(\phi(B^4))) \sim 1$.

To conclude the proof, we must show that the cocycle $\partial\phi(x, y)$ takes values δ -close to some small set S , whenever $x, y, xy \in B^{12}$. Since $\{(b, \phi(b)) : b \in B_0\} \subset H$, we see that if $x, y, xy \in B^{12}$ then $\partial\phi(x, y) = \phi(y)^{-1}\phi(x)^{-1}\phi(xy)$ lies in the fibre $F := \pi^{-1}(1) \cap H^{36}$. To conclude the proof of Proposition 3.1, it is therefore enough to prove that

$$\mathcal{C}_\delta(F) \sim 1. \quad (4.4)$$

To prove (4.4), observe first that, since H is a K -approximate group for some $K = O(1)$, H^{37} is covered by K^{36} translates of H , and so (by (4.1) and the bi-invariance of the metric) we have

$$\mathcal{C}_\delta(H^{37}) \sim n. \quad (4.5)$$

However, H^{37} contains a translate of F above every point of $\pi(H)$, and thus

$$|\pi(H)|\mathcal{C}_\delta(F) \leq \mathcal{C}_\delta(H^{37}).$$

The desired estimate (4.4) follows immediately from this, (4.3) and (4.5). \square

5. Case 1: a large element in the error set

We turn now to the proof of Proposition 3.2. The reader may wish to recall the outline given in Section 3. In this section we look at the first case discussed there, in which there are $x, y \in B^4$ such that $|\partial\phi(x, y)| > \sqrt{\delta}$. Before giving the main argument, let us record a lemma

concerning almost commuting rotations. This must surely exist in the literature but I could not locate a reference. Here, and in what follows, we define the conjugate a^g to be $g^{-1}ag$ and the commutator $[a, g]$ to be $a^{-1}g^{-1}ag$.

LEMMA 5.1. *Let $a, g \in \text{SO}(3)$, $a \neq 1$. Then $d(g, C(a)) \ll \frac{|[a, g]|}{|a|}$, where $C(a)$ denotes the centraliser of a .*

Proof. It is easy to check that if the statement is true for a , then it is true for any conjugate of a , and thus we may assume that

$$a = r(\theta) := \begin{pmatrix} \cos \theta & \sin \theta & 0 \\ -\sin \theta & \cos \theta & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Suppose that $|[a, g]| = \eta$. By the existence of Euler angles, every g can be written as $g = r(\beta_1)r'(\alpha)r(\beta_2)$, where

$$r'(\alpha) := \begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos \alpha & \sin \alpha \\ 0 & -\sin \alpha & \cos \alpha \end{pmatrix}.$$

Since $r(\beta_1), r(\beta_2)$ commute with a we have $|[a, r'(\alpha)]| = |[a, g]| = \eta$. A computation gives

$$|[a, r'(\alpha)]| = d(r(\theta)r'(\alpha), r'(\alpha)r(\theta)) = 2^{5/2}xy(1 - x^2y^2)^{1/2},$$

where $x := |\sin(\theta/2)|$, $y = |\sin(\alpha/2)|$. Thus

$$xy(1 - x^2y^2)^{1/2} \ll \eta. \quad (5.1)$$

If $xy \leq \frac{1}{2}$ then $(1 - x^2y^2)^{1/2} > \frac{1}{2}$ and so (5.1) implies that $xy \ll \eta$. If $xy \geq \frac{1}{2}$ then (5.1) implies that $(1 - x^2y^2)^{1/2} \ll \eta$, and so $x^2y^2 \geq 1 - O(\eta^2)$. Since $x \leq 1$, this implies that $y^2 \geq 1 - O(\eta^2)$, and hence that $y \geq 1 - O(\eta^2)$. Summarising, we see that either (i) $xy \ll \eta$, or (ii) $y \geq 1 - O(\eta^2)$.

Note also that $x = 2^{-3/2}|a|$.

In case (i),

$$|r'(\alpha)| = 2^{3/2}|\sin(\alpha/2)| = 2^{3/2}y \ll \eta/x \ll \eta/|a|.$$

Therefore

$$\begin{aligned} d(g, C(a)) &\leq d(g, r(\beta_1 + \beta_2)) \quad (\text{since } r(\beta_1 + \beta_2) \text{ commutes with } a) \\ &= \|r(\beta_1)(r'(\alpha) - 1)r(\beta_2)\| \\ &\leq 8|r'(\alpha)| \quad (\text{since } \|\cdot\| \text{ is submultiplicative}) \\ &\ll \eta/|a|. \end{aligned}$$

This concludes the proof in this case.

In case (ii),

$$d(r'(\alpha), r'(\pi)) = 2^{3/2}|\cos(\alpha/2)| = 2^{3/2}(1 - y^2)^{1/2} \ll \eta.$$

Therefore

$$\begin{aligned} d(g, C(a)) &\leq d(g, r(\beta_1)r'(\pi)r(\beta_2)) \quad (\text{since } r(\beta_1), r(\beta_2), r'(\pi) \text{ all commute with } a) \\ &= \|r(\beta_1)(r'(\alpha) - r'(\pi))r(\beta_2)\| \\ &\ll \eta \quad (\text{since } \|\cdot\| \text{ is submultiplicative}). \end{aligned}$$

This completes the proof of the lemma. \square

Now we return to the proof of Proposition 3.2 (first case). Let $z \in B^4$ be arbitrary. Recall that the cocycle $\partial\phi(u, v)$ is defined by $\phi(uv) = \phi(u)\phi(v)\partial\phi(u, v)$. Thus we may compute

$$\phi(xyz) = \phi(x)\phi(yz)\partial\phi(x, yz) = \phi(x)\phi(y)\phi(z)\partial\phi(y, z)\partial\phi(x, yz)$$

and also

$$\begin{aligned}\phi(xyz) &= \phi(xy)\phi(z)\partial\phi(xy, z) = \phi(x)\phi(y)\partial\phi(x, y)\phi(z)\partial\phi(xy, z) \\ &= \phi(x)\phi(y)\phi(z)\partial\phi(x, y)^{\phi(z)}\partial\phi(xy, z),\end{aligned}$$

where $a^g = g^{-1}ag$ denotes conjugation. Comparing these two expressions gives the cocycle equation

$$\partial\phi(y, z)\partial\phi(x, yz) = \partial\phi(x, y)^{\phi(z)}\partial\phi(xy, z),$$

which we prefer to write as

$$a^{\phi(z)} = \partial\phi(y, z)\partial\phi(x, yz)\partial\phi(xy, z)^{-1}, \quad (5.2)$$

where $a := \partial\phi(x, y)$. Since $x, y, z \in B^4$, all the pairwise products as well as the triple product xyz lie in B^{12} , and hence by the hypotheses of Proposition 3.2 the three cocycles $\partial\phi(y, z)$, $\partial\phi(x, yz)$, $\partial\phi(xy, z)$ lie in the δ -neighbourhood of S . It follows from (5.2) that, for all $z \in B^4$, $d(a^{\phi(z)}, SSS^{-1}) \leq 3\delta$. Consequently, we may find a set z_1, \dots, z_k , $k \leq |SSS^{-1}| \leq K^3$, of elements of B^4 such that for every $z \in B^4$ there is some i such that $d(a^{\phi(z)}, a^{\phi(z_i)}) \leq 6\delta$. Equivalently, $[[a, \phi(z)\phi(z_i)^{-1}]] \leq 6\delta$. By Lemma 5.1 we see that for every $z \in B^4$ there is some i such that $d(\phi(z)\phi(z_i)^{-1}, C(a)) \leq \sqrt{\delta}$. Thus $\phi(B^4)$ is contained in the $(\sqrt{\delta})$ -neighbourhood of at most k translates of $C(a)$, a set whose measure tends to 0 as $\delta \rightarrow 0$, uniformly in $a \neq 1$. This concludes the proof in the first case.

6. Case 2: almost homomorphisms

We now turn to the second case of Proposition 3.2. This is the case in which $|\partial\phi(x, y)| \leq \sqrt{\delta}$ whenever $x, y, xy \in B^{12}$, and we wish to conclude that $\mu(N_\delta(\phi(B^4))) = o_{K; \delta \rightarrow 0}(1)$. For notational convenience, redefine $\sqrt{\delta}$ to δ , thus we have $|\partial\phi(x, y)| \leq \delta$, or equivalently ϕ satisfies the almost-homomorphism property

$$d(\phi(xy), \phi(x)\phi(y)) \leq \delta \quad (6.1)$$

whenever $x, y, xy \in B^{12}$. We wish to conclude that $\mu(N_\delta(\phi(B^4))) = o_{K; \delta \rightarrow 0}(1)$.

We will repeatedly use the fact, easily established using (6.1) and induction, that if Q is a symmetric set with $Q^m \subset B^{12}$ then

$$d(\phi(w(x, y)), w(\phi(x), \phi(y))) \leq m\delta \quad (6.2)$$

for all $x, y \in Q$, where w is any word of length at most m in the variables x, y . Of particular interest to us will be the commutator words $w_1(a, b) := [a, b]$, $w_{i+1}(a, b) := [a, w_i(a, b)]$. The length of w_s is $\ell(w_s) = 3 \cdot 2^s - 2$.

We will also use the following result of Breuillard, Tao and the author [2].

THEOREM 6.1. *Suppose that B is a K -approximate group. Then there is some $s = O_K(1)$, a symmetric set Q of size $\gg_K |B|$ and a finite group $H \subset B^4$ such that*

- (1) $Q^m \subset B^4$, where $m = 10\ell(w_s)$;
- (2) If $x, y \in Q^4$ then $w_s(x, y) \in H$.

Proof ([2, Theorem 2.10]). states that B^4 contains an $O_K(1)$ -proper coset nilprogression $P = P_H(u_1, \dots, u_r; N_1, \dots, N_r)$ with rank $r = O_K(1)$, step $s = O_K(1)$, and with $|P| \gg_K |B|$.

We refer the reader to [2, Section 2] for the definitions required here, though the reader can fairly happily treat these concepts as black boxes for the purpose of this discussion. In particular, since P contains H , so does B^4 . Set $m = 10\ell(w_s)$, thus $4 \leq m \ll_K 1$, and let $Q := P_H(u_1, \dots, u_r; \frac{1}{m}N_1, \dots, \frac{1}{m}N_r)$. It follows from the definitions in [2, Section 2] that Q is symmetric and $Q^m \subset P$, and it follows from [2, Lemma C.1] that $|Q| \gg_{K,m} |P|$. Finally, if $x, y \in Q^4$ then certainly $x, y \in P$, and so from the fact that P/H is s -step nilpotent we see that indeed $w_s(x, y) \in H$. \square

From now on we drop explicit mention of K ; all bounds can (and will) depend on K . The (non-abelian) Ruzsa covering lemma [10, Lemma 3.6] states that if U, V are finite sets in some group and if $|UV| \leq C|U|$ then V is contained in the union of at most C translates of $U^{-1}U$. Take $U = Q$ and $V = B^4$. Since $Q \subset B^4$, we have $|UV| \leq |B^8|$. However, B is a K -approximate group and so $|B^8| \ll |B|$. Since $|Q| \gg |B|$, we may take $C = O(1)$. Applying the Ruzsa covering lemma (and noting that Q is symmetric, so $Q^{-1}Q = Q^2$) it follows that B^4 is a union of $O(1)$ translates Q^2g_i , where $g_i \in B^4$. Evidently it suffices to show that $\mu(N_\delta(\phi(Q^2g_i))) = o_{\delta \rightarrow 0}(1)$ for each i . Fix some i and set $g := g_i$.

Suppose that $x_1, x_2, x_3, x_4 \in Q^2g$. Then $x_1x_2^{-1}, x_3x_4^{-1} \in Q^4$, and so by Theorem 6.1 (2), $w_s(x_1x_2^{-1}, x_3x_4^{-1}) \in H$. It follows from (6.2) (and Theorem 6.1 (1)) that

$$d(w_s(\phi(x_1x_2^{-1}), \phi(x_3x_4^{-1})), \phi(H)) = O(\delta). \quad (6.3)$$

Since $Q^4 \subset B^4$ and $g \in B^4$, we have $x_1, x_2^{-1}, x_3, x_4^{-1}, x_1x_2^{-1}, x_3x_4^{-1} \in B^8$, and so by (6.1) we have

$$d(\phi(x_1x_2^{-1}), \phi(x_1)\phi(x_2)^{-1}), d(\phi(x_3x_4^{-1}), \phi(x_3)\phi(x_4)^{-1}) \leq \delta.$$

Using this many times in (6.3) (and the fact that the δ -neighbourhood of 1 is normalised by $\text{SO}(3)$, to move all the errors of δ to the right) we obtain

$$d(\tilde{w}_s(\phi(x_1), \phi(x_2), \phi(x_3), \phi(x_4)), \phi(H)) = O(\delta), \quad (6.4)$$

where $\tilde{w}_s(t_1, t_2, t_3, t_4) := w_s(t_1t_2^{-1}, t_3t_4^{-1})$. Now since $H \subset B^4$ we see that ϕ is defined on all of H , and of course it still satisfies the approximate homomorphism condition (6.1).

It is known that under these conditions there is a genuine homomorphism $\tilde{\phi} : H \rightarrow \text{SO}(3)$ such that $d(\phi(h), \tilde{\phi}(h)) = O(\delta)$ for all $h \in H$. This follows from [9, Theorem 1], which states[†] the following. Let H be a finite[‡] group, and let $\phi : H \rightarrow U$ be an ϵ -representation of H into the group U of unitary transformations of a Hilbert space (which means that (6.1) is satisfied with $\delta = \epsilon/2$). Then there exists a representation $\tilde{\phi} : H \rightarrow U$ such that $d(\phi(h), \tilde{\phi}(h)) \leq \epsilon$ for all $h \in H$. In our application, one takes the Hilbert space to be \mathbf{R}^3 , so U is the orthogonal group $\text{O}(3)$; it is easy to see that if ϕ takes values in $\text{SO}(3)$, then so does the corrected map $\tilde{\phi}$.

Thus, writing $\Sigma \subset \text{SO}(3)$ for the subgroup $\tilde{\phi}(H)$, it follows that

$$d(\tilde{w}_s(\phi(x_1), \phi(x_2), \phi(x_3), \phi(x_4)), \Sigma) = O(\delta) \quad (6.5)$$

for all $x_1, x_2, x_3, x_4 \in Q^2g$. However, it is well known[§] that all finite subgroups of $\text{SO}(3)$ are either cyclic, dihedral or isomorphic to a subgroup of S_5 . In particular there is some fixed universal word w_* (for instance, $w_*(a, b) = [[a, b]^b, [a, b]]^{60}$, where $[a, b]^b$ means $[a, b]$ conjugated

[†]Kazhdan acknowledges that in the compact case the result was obtained earlier by Grove, Karcher and Ruh [8], and in fact similar ideas go back to Turing [11].

[‡]In fact Kazhdan states the theorem for amenable groups, but all finite groups are amenable.

[§]One could get away with weaker results here, such as Jordan's theorem.

by b), which is trivial on $\Sigma \times \Sigma$. Since w_* is Lipschitz[†], it follows from (6.5) that for all $y_1, \dots, y_8 \in \phi(Q^2g)$ we have

$$|w(y_1, \dots, y_8)| = d(w(y_1, \dots, y_8), 1) = O(\delta),$$

where $w(t_1, \dots, t_8) := w_*(\tilde{w}_s(t_1, t_2, t_3, t_4), \tilde{w}_s(t_5, t_6, t_7, t_8))$. Using the Lipschitz property of w , the same is true if $y_1, \dots, y_8 \in N_\delta(\phi(Q^2g))$, of course at the expense of weakening the implicit constant in $O(\delta)$. That is, the Cartesian product of 8 copies of $N_\delta(\phi(Q^2g))$ is contained in $W_{O(\delta)}$, where

$$W_\eta := \{(y_1, \dots, y_8) \in \mathrm{SO}(3)^8 : |w(y_1, \dots, y_8)| \leq \eta\}.$$

It therefore suffices to check that $\lim_{\eta \rightarrow 0} \mu^{\otimes 8}(W_\eta) = 0$ which, by basic measure theory, is equivalent to the statement that

$$\mu^{\otimes 8}\{(y_1, \dots, y_8) \in \mathrm{SO}(3)^8 : w(y_1, \dots, y_8) = 1\} = 0. \quad (6.6)$$

However, this is so because (see [4]) almost all 8-tuples of elements of $\mathrm{SO}(3)$ generate a free group.

7. Further comments and open questions

We have already remarked that it would be interesting to understand more about the structure of approximate homomorphisms $\phi : B \rightarrow \mathrm{SO}(3)$ where B is an approximate group. Does an analogue of Kazhdan's theorem hold for them, that is to say if (6.1) holds, is there $\tilde{\phi} : B \rightarrow \mathrm{SO}(3)$ satisfying $\tilde{\phi}(xy) = \tilde{\phi}(x)\tilde{\phi}(y)$ and with $d(\phi(x), \tilde{\phi}(x)) = O(\delta)$ for all x ? It might be possible to answer this question using the thesis of Carolino [3], applied to the graph of ϕ . This would allow for an alternative to the arguments of Section 6 by appealing to [1], which says that finite approximate subgroups of $\mathrm{SO}(3)$ are almost abelian.

The example of Gowers and Long considered in this paper is natural, but has the slightly unsatisfactory property that the operation \circ is not cancellative. It is only weakly cancellative in the sense that for a given x and z there are at most $O(1)$ values of y for which $x \circ y = z$. I have some notes on a potential example which is fully cancellative, so its multiplication table is a Latin square. Roughly speaking, it comes from replacing $\mathrm{SO}(3)$ by a compact portion of the Heisenberg group (Jason Long informs me that he and Gowers also considered such examples). I initially thought that the Heisenberg group, being almost abelian, would be much easier to analyse than $\mathrm{SO}(3)$, but this turned out not to be the case. The main reason is that the Heisenberg group does contain approximate subgroups with 'thick' image.

The following question, which I cannot currently resolve, came from this line of thinking. It is probably key to a rigorous analysis of the example just mentioned. Consider the Heisenberg group $\mathrm{H}(\mathbf{R}) = \{(x, y, z) : x, y, z \in \mathbf{R}\}$ with the group operation $*$ being $(x_1, y_1, z_1) * (x_2, y_2, z_2) = (x_1 + x_2, y_1 + y_2, z_1 + z_2 + x_1 y_2)$.

QUESTION 7.1. Let K be a fixed real parameter and let N be a large integer. Suppose that B is a K -approximate group, and that $\phi : B \rightarrow \mathrm{H}(\mathbf{R})$ is a map with the following properties:

- (1) ϕ takes values in $\{(x, y, z) \in \mathrm{H}(\mathbf{R}) : x, y \in \frac{1}{N}\mathbf{Z}, |x|, |y|, |z| \leq 10\}$;
- (2) for every $x, y \in \frac{1}{N}\mathbf{Z}$ with $|x|, |y| \leq 1$ there is some $|z| \leq 10$ such that $(x, y, z) \in \phi(B)$;
- (3) $\partial\phi$ takes values in $\{(0, 0, z) \in \mathrm{H}(\mathbf{R}) : |z| \leq 10/N\}$.

Must it be the case that $|B|/N^3 \rightarrow \infty$ as $N \rightarrow \infty$?

[†]Any word map is Lipschitz with Lipschitz constant the length of the word, since if $d(t_i, t'_i) \leq \delta$ then $d(t_1 \dots t_m, t'_1 \dots t'_m) \leq m\delta$, by an easy induction.

Taking B to consist of the elements $(\frac{a}{N}, \frac{b}{N}, \frac{c}{N^2}) \in H(\mathbf{R})$ together with their inverses, for $-N \leq a, b \leq N$, $-N^2 \leq c \leq N^2$, and ϕ to be the identity map, one obtains an example with $|B| \sim N^4$. Note that in this case $\partial\phi$ is trivial.

Acknowledgements. I would like to thank Emmanuel Breuillard for helpful conversations, and the referee for making some useful suggestions to improve the readability of the paper.

References

1. E. BREUILLARD and B. GREEN, ‘Approximate groups III: the unitary case’, *Turkish J. Math.* 36 (2012) 199–215.
2. E. BREUILLARD, B. GREEN and T. TAO, ‘The structure of approximate groups’, *Publ. Math. Inst. Hautes Études Sci.* 116 (2012) 115–221.
3. P. K. CAROLINO, ‘The structure of locally compact approximate groups’, PhD Thesis, University of California, Los Angeles, CA, 2015.
4. D. B. A. EPSTEIN, ‘Almost all subgroups of a Lie group are free’, *J. Algebra* 19 (1971) 261–262.
5. W. T. GOWERS, ‘A new proof of Szemerédi’s theorem for arithmetic progressions of length four’, *Geom. Funct. Anal.* 8 (1998) 529–551.
6. W. T. GOWERS, ‘A new proof of Szemerédi’s theorem’, *Geom. Funct. Anal.* 11 (2001) 465–588.
7. W. T. GOWERS and J. LONG, ‘Partial associativity and rough approximate groups’, Preprint, <https://arxiv.org/abs/1904.08732>.
8. K. GROVE, H. KARCHER and E. RUH, ‘Jacobi fields and Finsler metrics on compact Lie groups with an application to differentiable pinching problems’, *Math. Ann.* 211 (1974) 7–21.
9. D. KAZHDAN, ‘On ε -representations’, *Israel J. Math.* 43 (1982) 315–323.
10. T. TAO, ‘Product set estimates for non-commutative groups’, *Combinatorica* 28 (2008) 547–594.
11. A. M. TURING, ‘Finite approximations to Lie groups’, *Ann. of Math.* (2) 39 (1938) 105–111.

Ben Green
 Mathematical Institute
 Radcliffe Observatory Quarter
 University of Oxford
 Woodstock Road
 Oxford OX2 6GG
 United Kingdom

ben.green@maths.ox.ac.uk