SIAM J. DISCRETE MATH.
Vol. 33, No. 2, pp. 1044–1060

AN IMPROVED SUM-PRODUCT BOUND FOR QUATERNIONS*

ABDUL BASIT† AND BEN LUND‡

Abstract. We show that there exists an absolute constant $c > 0$, such that, for any finite set A of quaternions, $\max\{|A+A|, |AA|\} \gtrsim |A|^{4/3+c}$. This generalizes a sum-product bound for real numbers proved by Konyagin and Shkredov.

Key words. additive combinatorics, sum-product conjecture, quaternions

AMS subject classifications. 11B30, 68R05

DOI. 10.1137/18M1231468

1. Introduction. By $X \gg Y$ or $Y \ll X$, we mean that $X \geq cY$ for some absolute constant $c > 0$. The expression $X \approx Y$ means that both $X \gg Y$ and $X \ll Y$ hold. The expression $X \gtrsim Y$ or $Y \lesssim X$ means that $X \gg Y/(\log X)^c$ for some absolute constant $c > 0$. When dependence on a certain parameter needs to be emphasized, we write the parameter in the subscript, e.g., $Y \ll_\varepsilon X$ means that the hidden constant depends on ε. All logarithms have base 2.

Given finite subsets A, B of a ring, the *sum set* and *product set* are defined, respectively, as

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

and

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

Erdős and Szemerédi [4] conjectured that, for finite sets of integers, one of these must be nearly as large as possible.

CONJECTURE 1.1 (Erdős and Szemerédi). *Let A be a finite set of integers. Then, for any $\delta < 1$,*

$$|A + A| + |AA| \gg_\delta |A|^{1+\delta}. \tag{1.1}$$

In their initial work on the problem, Erdős and Szemerédi showed that Conjecture 1.1 holds for some fixed $\delta > 0$. Subsequent works by Nathanson [11], Ford [5], Elekes [2], and Solymosi [14] gave increasing values for δ. Solymosi used a beautiful and simple geometric argument to show that Conjecture 1.1 holds with $\delta \leq 1/3 - \varepsilon$ for any $\varepsilon > 0$ whenever A is a set of real numbers. This bound stood until 2015, when Konyagin and Shkredov [8] combined Solymosi's geometric insight with Shkredov's work in additive combinatorics to get a slight improvement. Further incremental progress was made by Konyagin and Shkredov [9], by Rudnev, Shkredov and Stevens [12], and by Shakan [13]. Shakan's result gives the current best bound for δ,

*Received by the editors December 10, 2018; accepted for publication (in revised form) April 30, 2019; published electronically June 25, 2019.
http://www.siam.org/journals/sidma/33-2/M123146.html
Funding: Work on this project by the second author was supported by NSF grant DMS-1344994 (RTG in Algebra, Algebraic Geometry, and Number Theory, at the University of Georgia).
†Department of Mathematics, 255 Hurley Hall, University of Notre Dame, Notre Dame, IN 46556 (abasit@nd.edu).
‡Department of Mathematics, Fine Hall, Princeton University, Princeton NJ 08544 (lund.ben@gmail.com).

showing that Conjecture 1.1 holds with $\delta \leq 1/3 + 5/5277$, whenever A is a finite set of real numbers.

The conjecture has also been studied for other fields and rings. Konyagin and Rudnev [7] generalized Solymosi's geometric argument to finite sets of complex numbers, showing that Conjecture 1.1 holds with $\delta \leq 1/3 - \varepsilon$ for any $\varepsilon > 0$ whenever $A \subset \mathbb{C}$. For quaternions, Chang [1] proved the bound $\delta \leq 1/54$. This was improved upon by Solymosi and Wong [16], who showed that, for finite sets of the quaternions, Conjecture 1.1 holds with $\delta \leq 1/3 - \varepsilon$ for any $\varepsilon > 0$. For more detail on the sum-product conjecture and its variants, see the recent survey of Granville and Solymosi [6].

Our contribution is to generalize Konyagin and Shkredov's proof to quaternions, hence passing the $\delta = 1/3$ barrier.

THEOREM 1.2. *There exists an absolute constant $c > 0$ such that, for any finite set A of quaternions,*

$$|A + A| + |AA| \gg |A|^{4/3+c}. \tag{1.2}$$

We make no attempt to prove Theorem 1.2 for the largest possible value of c, instead preferring to keep the exposition relatively simple and self contained.

Overview. Our proof follows the general outline of Konyagin-Shkredov in [8] and [9]. Since our aim is to keep this paper self contained rather than obtain the best value for c, at various points we make weaker estimates than the ones used in these papers.

We split the problem into two cases, depending on the additive energy of A (see section 2 for the definitions). In the case that this additive energy is small, we prove an appropriate generalization of Solymosi's argument, in the spirit of Konyagin-Rudnev [7] and Solymosi-Wong [16] (see section 4.3). In the case that this additive energy is large, we adapt the arguments of Konyagin and Shkredov [9] to work for quaternions (see section 4.2). This requires us to replace an application of the Szemerédi–Trotter theorem by a generalization proved by Solymosi and Tao [15] and to adapt the definitions and arguments of Konyagin and Shrkedov to work when multiplication is not commutative. This is done in section 3.

2. Preliminaries. Given finite subsets A, B of the quaternions, $\mathbb{H}$, the *sum set* and *product set* are defined, respectively, as

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

and

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

We define the *negation* of A to be

$$-A := \{-a : a \in A\}$$

and the *inverse* of A to be

$$A^{-1} := \{a^{-1} : a \in A,\ a \neq 0\}.$$

The *difference set* is defined to be $A - B$, and the *ratio set* is defined as $A/B := AB^{-1} \cap B^{-1}A$.

Denote by $\delta_{A+B}(x)$ and by $\delta_{AB}(x)$ the number of representations of x of the form $a+b$ and ab with $a \in A$, $b \in B$, respectively. Let

$$E_k^+(A,B) := \sum_x \delta_{A-B}(x)^k, \quad \text{and} \quad E_k^*(A,B) := \sum_x \delta_{AB}(x)^k.$$

The *additive energy of A and B*, denoted by $E^+(A,B)$, is defined to be

$$\begin{aligned} E^+(A,B) := E_2^+(A,B) &= \sum_x \delta_{A-B}(x)^2 = |\{(a,b,c,d) \in (A\times B)^2 : a-b=c-d\}| \\ &= |\{(a,b,c,d) \in (A\times B)^2 : a-c=b-d\}| = \sum_x \delta_{A-A}(x)\delta_{B-B}(x) \\ &= |\{(a,b,c,d) \in (A\times B)^2 : a+d=c+b\}| = \sum_x \delta_{A+B}(x)^2. \end{aligned}$$

Similarly, the *multiplicative energy of A and B*, denoted by $E^*(A,B)$, is defined to be

$$\begin{aligned} E^*(A,B) := E_2^*(A,B) &= \sum_x \delta_{AB}(x)^2 = |\{(a,b,c,d) \in (A\times B)^2 : ab=cd\}| \\ &= |\{(a,b,c,d) \in (A\times B)^2 : c^{-1}a=db^{-1}\}| \\ &= \sum_x \delta_{A^{-1}A}(x)\delta_{BB^{-1}}(x). \end{aligned}$$

When $A=B$, we write $E_k^+(A)$, $E^+(A)$, $E_k^*(A)$, and $E^*(A)$ to simplify notation. We note that, since multiplication of quaternions is not commutative, some care is necessary when dealing with product sets, ratio sets, and the multiplicative energy.

The Cauchy–Schwarz inequality implies the following lower bounds on the additive and multiplicative energies:

$$E^+(A,B) \geq \frac{|A|^2|B|^2}{|A+B|}, \quad \text{and} \quad E^+(A,B) \geq \frac{|A|^2|B|^2}{|A-B|}. \tag{2.1}$$

$$E^*(A,B) \geq \frac{|A|^2|B|^2}{|AB|}. \tag{2.2}$$

2.1. Results from incidence geometry. In this section, we set up some notation and results about *quaternionic lines*. In section 3, these results will be used to connect various energies with the sizes of the sum and product sets.

Define a *left line* to be any set in $\mathbb{H}^2$ of the form $\{(a,b)+t(c,d) : t \in \mathbb{H}\}$ for some $a,b,c,d \in \mathbb{H}$ with $(c,d) \neq (0,0)$. Similarly, define *right*, *lr-mixed* and *rl-mixed lines* to be sets of the form $\{(a,b)+(c,d)t : t \in \mathbb{H}\}$, $\{(a,b)+(tc,dt) : t \in \mathbb{H}\}$, and $\{(a,b)+(ct,td) : t \in \mathbb{H}\}$, respectively. We say two lines are of the *same type* if both are sets of the same form. It is straightforward to check that any two distinct quaternionic lines *of the same type* intersect in at most one point. Throughout this write-up, a set of quaternionic lines is restricted to have all lines of the same type.

Given a point set $\mathcal{P}$ and a set of quaternionic lines $\mathcal{L}$, both in $\mathbb{H}^2$, we say that an incidence is a pair $(p,l) \in \mathcal{P}\times\mathcal{L}$ with the point p lying on the line l. We denote by $\mathcal{I}(\mathcal{P},\mathcal{L})$ the set of incidences in $\mathcal{P}\times\mathcal{L}$. The following theorem is a special case of a result of Solymosi and Tao [15].

THEOREM 2.1. *Let $\varepsilon > 0$. Then there exists a constant $A = A_\varepsilon > 0$ such that*

$$|\mathcal{I}(\mathcal{P},\mathcal{L})| \leq A|\mathcal{P}|^{2/3+\varepsilon}|\mathcal{L}|^{2/3} + \frac{3}{2}|\mathcal{P}| + \frac{3}{2}|\mathcal{L}|$$

whenever $\mathcal{P}$ is a finite set of points in $\mathbb{H}^2$, and $\mathcal{L}$ is a finite set of quaternionic lines in $\mathbb{H}^2$.

As a consequence, we have the following upper bound on the number of *k-rich lines* determined by a finite set in $\mathbb{H}^2$:

COROLLARY 2.2. *Let $\varepsilon > 0$. Then for any set $\mathcal{P}$ of points in $\mathbb{H}^2$ and for any integer $k \geq 2$ the number of quaternionic lines containing at least k points of $\mathcal{P}$, denoted by n_k, satisfies*

$$n_k \ll_\varepsilon \frac{|\mathcal{P}|^{2+\varepsilon}}{k^3} + \frac{|\mathcal{P}|}{k}.$$

Next, we use Corollary 2.2 to obtain the following upper bound on the number of collinear triples.

LEMMA 2.3. *Let $\varepsilon > 0$. For a finite set A of quaternions, let T be the number of collinear triples in $A \times A \subset \mathbb{H}^2$ (where the points in a triple are not necessarily distinct). Then*

$$T \ll_\varepsilon |A|^{4+\varepsilon}.$$

Proof. Consider a partitioning of the set of lines into dyadic blocks, where the *ith* block consists of lines containing between 2^i and 2^{i+1} points, with $1 \leq i \leq \lceil \log |A| \rceil$. Let n_i be the number of lines in the *ith* set. Then the number of collinear triples is

$$T \leq \sum_{i=1}^{\lceil \log |A| \rceil} \left(2^{i+1}\right)^3 n_i. \tag{2.3}$$

This allows us to use Corollary 2.2, with $|\mathcal{P}| = |A|^2$ and $\varepsilon' = \varepsilon/2$, to bound n_i, giving

$$\begin{aligned} T &\leq \sum_{i=1}^{\lceil \log |A| \rceil} \left(2^{i+1}\right)^3 n_i \ll_{\varepsilon'} \sum_{i=1}^{\lceil \log |A| \rceil} \left(2^{i+1}\right)^3 \left(\frac{|A|^{4+\varepsilon'}}{(2^i)^3} + \frac{|A|^2}{2^i} \right) \\ &\ll \sum_{i=1}^{\lceil \log |A| \rceil} \left(|A|^{4+\varepsilon'} + |A|^2 2^{2i} \right) \ll |A|^{4+2\varepsilon'}. \end{aligned}$$

∎

3. Bounding energies. In this section we collect various bounds on the sizes of sum and product in terms of energies. All the results and proofs presented in this section have appeared in various papers. We simply present the proofs and adapt them to our setting.

First, we give some basic estimates on additive energies using the Cauchy–Schwarz inequality. The following appears as Lemma 2.4 and 2.5 in [10].

LEMMA 3.1. *Let A, B be finite sets of quaternions. Then*

$$|B|^2 E^+_{1.5}(A)^2 \leq E^+_3(A)^{2/3} E^+_3(B)^{1/3} E^+(A, A+B).$$

Proof. Let $A_x = A \cap (A + x)$, and note that $|A_x| = \delta_{A-A}(x)$. Equation (2.1) implies that

$$|A_x|^{1.5} |B| \leq E^+(A_x, B)^{1/2} |A_x + B|^{1/2} |A_x|^{1/2}.$$

This gives

$$\begin{aligned} E^+_{1.5}(A)^2|B|^2 &= \left(\sum_{x\in A-A}\left(|A_x|^{1.5}|B|\right)\right)^2 \\ &\le \left(\sum_{x\in A-A}\left(E^+(A_x,B)^{1/2}|A_x+B|^{1/2}|A_x|^{1/2}\right)\right)^2 \\ &\le \sum_{x\in A-A}E^+(A_x,B)\sum_{x\in A-A}|A_x+B||A_x| \\ &\le \sum_{x\in A-A}E^+(A_x,B)\sum_{x\in A-A}|(A+B)_x||A_x| \\ &= \left(\sum_{x\in A-A}E^+(A_x,B)\right)E^+(A,A+B), \end{aligned} \tag{3.1}$$

where the second inequality follows from the Cauchy–Schwarz inequality, and the third inequality is implied by the set inclusion $A_x + B \subseteq (A+B)_x$.

Next, note that

$$\begin{aligned} \sum_x E^+(A_x,B) &= \sum_x\sum_y \delta_{A_x-A_x}(y)\delta_{B-B}(y) = \sum_x\sum_y \delta_{A_y-A_y}(x)\delta_{B-B}(y) \\ &= \sum_y\sum_x \delta_{A_y-A_y}(x)\delta_{B-B}(y) = \sum_y \delta_{A-A}(y)^2\delta_{B-B}(y) \\ &\le \left(\sum_y \delta_{A-A}(y)^3\right)^{2/3}\left(\sum_y \delta_{B-B}(y)^3\right)^{1/3} \\ &= E^+_3(A)^{2/3}E^+_3(B)^{1/3}, \end{aligned} \tag{3.2}$$

where the second to last step is a standard application of Hölder's inequality. ∎

The statement of the lemma now follows by combining (3.1) and (3.2).

The following lemma establishes a connection between the additive energy and the size of the product set and appears as Theorem 9 in [8]. The technique used here was introduced by Elekes and Ruza in [3].

LEMMA 3.2. *Let $\varepsilon > 0$, and A be a finite set of quaternions, with $0 \notin A$. Then*

$$E^+(A)^4 \ll_\varepsilon |AA||A|^{10+\varepsilon}.$$

Proof. In order to bound $E^+(A)$, we may restrict our attention to elements that have many realizations in $A + A$. Let F be the set of such elements, i.e.,

$$F = \left\{x \in A + A : \delta_{A+A}(x) > \frac{E^+(A)}{2|A|^2}\right\}.$$

Now

$$\sum_{x\notin F}\delta_{A+A}(x)^2 \le \frac{E^+(A)}{2|A|^2}\sum_{x\notin F}\delta_{A+A}(x) \le \frac{E^+(A)}{2}.$$

In particular, we have

$$E^+(A) \le 2\sum_{x\in F}\delta_{A+A}(x)^2.$$

Let $\mathcal{P} = (A \cup F) \times (A \cup F)$. We will double count the number of collinear triples in $\mathcal{P}$ (where points in a triple are not necessarily distinct), denoted by T.

Denote by δ_F the quantity $\sum_{x \in F} \delta_{A+A}(x)$. Since, for all x, $\delta_{A+A}(x) \leq |A|$, we have

$$\delta_F = \sum_{x \in F} \delta_{A+A}(x) \geq \sum_{x \in F} \frac{\delta_{A+A}(x)^2}{|A|} \geq \frac{E^+(A)}{2|A|}.$$

This gives

$$|F| + |A| \leq \sum_{x \in F} \left(\delta_{A+A}(x) \cdot \frac{2|A|^2}{E^+(A)} \right) + |A| \left(\delta_F \cdot \frac{2|A|}{E^+(A)} \right) = \frac{4|A|^2 \delta_F}{E^+(A)}.$$

Combining the above with Lemma 2.3 (with $\varepsilon' = \varepsilon/2$) implies

$$T \ll_{\varepsilon'} |A \cup F|^{4+\varepsilon'} \ll \left(\frac{|A|^2 \delta_F}{E^+(A)} \right)^{4+\varepsilon'}. \tag{3.3}$$

We now obtain a lower bound on T. For each $a \in A$, let $F_a = \{b \in A : a+b \in F\}$. Fix $(a,b) \in A^2$, and consider a quadruple of the form $(c,d,e,f) \in (F_a \times F_b)^2$ with $cd = ef$, or equivalently $df^{-1} = c^{-1}e$. Note that the line $\{(a,b) + (ct, tf) : t \in \mathbb{H}\}$ contains the points

$$(a,b), (a+c, b+f), (a+e, b+d) \in \mathcal{P},$$

with $t = 0$, $t = 1$, and $t = df^{-1} = c^{-1}e$, respectively. Since the quadruples (c,d,e,f) and (e,f,c,d) give the same collinear triple, by (2.2), each pair $(a,b) \in A^2$ gives at least

$$\frac{1}{2} \left(\frac{|F_a|^2 |F_b|^2}{|F_a F_b|} \right) \gg \frac{|F_a|^2 |F_b|^2}{|AA|}$$

distinct collinar triples. It follows that the number of collinear triples in $\mathcal{P}$ is at least

$$\begin{aligned} T &\gg \sum_{a,b \in A} \frac{|F_a|^2 |F_b|^2}{|AA|} = \frac{1}{|AA|} \left(\sum_{a \in A} |F_a|^2 \right)^2 \\ &\geq \frac{1}{|AA|} \left(\frac{1}{|A|} \left(\sum_{a \in A} |F_a| \right)^2 \right)^2 = \frac{\delta_F^4}{|AA||A|^2}. \end{aligned} \tag{3.4}$$

Combining (3.3) and (3.4) gives

$$E^+(A)^{4+\varepsilon'} \ll_{\varepsilon'} |A|^{10+2\varepsilon'} \delta_F^{\varepsilon'} |AA|.$$

Finally, since $E^+(A) \geq |A|^2$ and $\delta_F = \sum_{x \in F} \delta_{A+A}(x) \leq |A|^2$, we get

$$E^+(A)^4 \ll_{\varepsilon} |AA||A|^{10+\varepsilon}.$$

∎

An important tool in connecting incidence results and sum-product estimates is the quantity $d_*(A)$ defined below, which captures the multiplicative structure of A. We define

$$d_*(A) := \min_{t>0} \min_{\varnothing \neq Q,R \subset \mathbb{H} \setminus \{0\}} \frac{|Q|^2 |R|^2}{|A| t^3},$$

where the second minimum is taken over all sets Q and R such that $|Q| \geq \max\{|A|, |R|\}$, and, for every $a \in A$, the bound $|Q \cap Ra| \geq t$ holds.

Comment. Note that the definition of $d_*(A)$ is different from that in [9], where it was only required that $\max\{|Q|,|R|\} \geq |A|$. Noncommutativity of multiplication for the quaternions means that we require the stronger condition that $|Q| \geq \max\{|A|,|R|\}$. When A is a subset of the real numbers (or the complex numbers), we can assume, without loss of generality, that $|Q| \geq |R|$. This change in definition does not affect any of the proofs later.

The sets $Q = A$ and $R = \{1\}$ show that $d_*(A) \leq |A|$. Roughly speaking, the closer $d_*(A)$ is to $|A|$, the less multiplicative structure A has. The following is a key lemma concerning $d_*(A)$ and will be used to connect additive energies with the product set. The version for real numbers appeared as Lemma 13 in [9].

LEMMA 3.3. *Let $\varepsilon > 0$, and A, B be finite sets of quaternions, and $\tau \geq 1$ an integer. Then*

$$|\{x : \delta_{A-B}(x) \geq \tau\}| \ll_\varepsilon \frac{|A||B|^{2+\varepsilon}}{\tau^3} d_*(A)^{1+\varepsilon}.$$

Proof. Note that we may assume A and B are large (with respect to the hidden constant), since otherwise the statement is trivially true. Let $Q, R \subset \mathbb{H} \setminus \{0\}$ with $|Q| \geq \max\{|A|,|R|\}$, and $t > 0$ an integer such that, for all $a \in A$, $|Q \cap Ra| \geq t$. For any integer $\tau \geq 1$, let

$$D_\tau = \{x \in A - B : \delta_{A-B}(x) \geq \tau\}.$$

To prove the lemma, it suffices to show that

$$|D_\tau| \ll_\varepsilon \frac{|Q|^{2+\varepsilon}|R|^{2+\varepsilon}|B|^{2+\varepsilon}}{t^3\tau^3}. \tag{3.5}$$

Let $\sigma = |\{(a,b,x) : a - b = x,\, a \in A, b \in B, x \in D_\tau\}|$, and note that, by definition,

$$\sigma = \sum_{x \in D_\tau} \delta_{A-B}(x) \geq \tau |D_\tau|. \tag{3.6}$$

On the other hand, for each $a \in A$, $|Q \cap Ra| \geq t$ implies that $\delta_{R^{-1}Q}(a) \geq t$. This gives

$$\sigma \leq |\{(r,q,b,x) : r^{-1}q - b = x,\, r \in R, q \in Q, b \in B, x \in D_\tau\}| \cdot t^{-1}. \tag{3.7}$$

By ignoring the condition $x \in D_\tau$, (3.7) immediately implies the bound

$$\sigma \leq \frac{|Q||R||B|}{t}. \tag{3.8}$$

When $t^2\tau^2 \ll |Q||R||B|$, (3.6) and (3.8) imply

$$|D_\tau| \leq \frac{|Q||R||B|}{t\tau} \ll \frac{|Q|^2|R|^2|B|^2}{t^3\tau^3},$$

allowing us to restrict our attention to the case when $t^2\tau^2 \gg |Q||R||B|$.

In this scenario, we reformulate (3.7) as an incidence problem. For $r \in R$ and $d \in D_\tau$, let $l_{r,d} = \{(x,y) : r^{-1}y - x = d\}$ be a quaternionic line. Consider the family $\mathcal{L} = \{l_{r,d} : r \in R, d \in D_\tau\}$ of $|R||D_\tau|$ lines. Let $\mathcal{P}$ be the point set $B \times Q$. Now, by Theorem 2.1, for $\varepsilon' = \varepsilon/3$, we have

$$\begin{aligned} \sigma &\leq |\mathcal{I}(\mathcal{P},\mathcal{L})| \cdot t^{-1} \\ &\ll \left(A_{\varepsilon'}|\mathcal{P}|^{2/3+\varepsilon'}|\mathcal{L}|^{2/3} + |\mathcal{P}| + |\mathcal{L}|\right) \cdot t^{-1}. \end{aligned} \tag{3.9}$$

If the first term in (3.9) dominates, we have

$$t\tau|D_\tau| \ll A_{\varepsilon'}|\mathcal{P}|^{2/3+\varepsilon'}|\mathcal{L}|^{2/3} = A_{\varepsilon'}(|Q||B|)^{2/3+\varepsilon'}(|R||D_\tau|)^{2/3}.$$

Rearranging gives

$$|D_\tau| \ll_\varepsilon \frac{|Q|^{2+\varepsilon}|B|^{2+\varepsilon}|R|^2}{t^3\tau^3}.$$

Now suppose that the bound (3.5) does not hold. If the second term dominates, then

$$\frac{|Q|^2|R|^2|B|^2}{t^2\tau^2} \ll t\tau|D_\tau| \ll |\mathcal{P}| = |Q||B|. \tag{3.10}$$

Note that we must have $t \le \min\{|Q|,|R|\} = |R|$, $\tau \le |B|$, and $\tau \le |A| \le |Q|$. Together with (3.10), this gives a contradiction.

Finally, if the third term dominates, then

$$t\tau|D_\tau| \ll |\mathcal{L}| = |R||D_\tau|.$$

Combined with the assumption that $t^2\tau^2 \ge |Q||R||B|$, this implies

$$|Q||B||R| \ll |R|^2.$$

But this is a contradiction, since $|Q| \ge |R|$ and B is large enough. ∎

We now give some consequences of Lemma 3.3. The proof of all three corollaries follows the same basic outline.

COROLLARY 3.4. *Let $\varepsilon > 0$, and A be a finite set of quaternions. Then*

$$E^+(A) \ll_\varepsilon |A|^{1+\varepsilon} d_*(A)^{1/3+\varepsilon} E^+_{1.5}(A)^{2/3}.$$

Proof. Let Δ be a parameter to be specified later, and recall that

$$E^+(A) = \sum_x \delta_{A-A}(x)^2 = \sum_{x\,:\,\delta_{A-A}(x)<\Delta} \delta_{A-A}(x)^2 + \sum_{x\,:\,\delta_{A-A}(x)\ge\Delta} \delta_{A-A}(x)^2.$$

We first consider sums with fewer than Δ realizations.

$$\begin{aligned}\sum_{x\,:\,\delta_{A-A}(x)<\Delta} \delta_{A-A}(x)^2 &\le \max_{x\,:\,\delta_{A-A}(x)<\Delta}\{\delta_{A-A}(x)^{1/2}\} \sum_{x\,:\,\delta_{A-A}(x)<\Delta} \delta_{A-A}(x)^{1.5} \\ &\le \Delta^{1/2} E^+_{1.5}(A). \end{aligned} \tag{3.11}$$

To bound the contribution of sums with more than Δ realizations, we use a dyadic decomposition along with Lemma 3.3 (with $B = A$ and $\varepsilon' = 3\varepsilon/2$):

$$\begin{aligned}\sum_{x\,:\,\delta_{A-A}(x)\ge\Delta} \delta_{A-A}(x)^2 &= \sum_{j=1}^{\lceil \log|A|\rceil+1} \sum_{x\,:\,\Delta 2^{j-1}\le\delta_{A-A}(x)<\Delta 2^j} \delta_{A-A}(x)^2 \\ &\ll_{\varepsilon'} \sum_{j=1}^{\lceil \log|A|\rceil+1} \frac{|A|^{3+\varepsilon'} d_*(A)^{1+\varepsilon'}}{(\Delta 2^{j-1})^3} (\Delta 2^j)^2 \\ &\ll \frac{|A|^{3+2\varepsilon'} d_*(A)^{1+2\varepsilon'}}{\Delta}. \end{aligned} \tag{3.12}$$

Combining (3.11), (3.12), and setting $\Delta = (\frac{|A|^{3+2\varepsilon'} d_*(A)^{1+2\varepsilon'}}{E^+_{1.5}(A)})^{2/3}$ finishes the proof. ∎

COROLLARY 3.5. *Let $\varepsilon > 0$, and A, B be finite sets of quaternions. Then*

$$E^+(A,B) \ll_\varepsilon |A||B|^{3/2+\varepsilon} d_*(A)^{1/2+\varepsilon}.$$

Proof. Let Δ be a parameter to be specified later. Then

$$\begin{aligned} E^+(A,B) &= \sum_x \delta_{A-B}(x)^2 \\ &= \sum_{x\,:\,\delta_{A-B}(x)<\Delta} \delta_{A-B}(x)^2 + \sum_{j=1}^{\lceil \log |B| \rceil + 1} \sum_{x\,:\,\Delta 2^{j-1} \le \delta_{A-B}(x) < \Delta 2^j} \delta_{A-B}(x)^2 \\ &\ll_\varepsilon \Delta |A||B| + \sum_{j=1}^{\lceil \log |B| \rceil + 1} \frac{|A||B|^{2+\varepsilon} d_*(A)^{1+\varepsilon}}{(\Delta 2^{j-1})^3} (\Delta 2^j)^2 \\ &\ll \Delta |A||B| + \frac{|A||B|^{2+2\varepsilon} d_*(A)^{1+2\varepsilon}}{\Delta}. \end{aligned}$$

Setting $\Delta = (|B|^{1+2\varepsilon} d_*(A)^{1+2\varepsilon})^{1/2}$ completes the proof. ∎

COROLLARY 3.6. *Let $\varepsilon > 0$, and A be a finite set of quaternions. Then*

$$E_3^+(A) \ll_\varepsilon |A|^{3+\varepsilon} d_*(A)^{1+\varepsilon}.$$

Proof.

$$\begin{aligned} E_3^+(A) = \sum_x \delta_{A-A}(x)^3 &= \sum_{j=1}^{\lceil \log |A| \rceil + 1} \sum_{x\,:\,2^{j-1} \le \delta_{A-A}(x) < 2^j} \delta_{A-A}(x)^3 \\ &\ll_{\varepsilon'} \sum_{j=1}^{\lceil \log |A| \rceil + 1} \frac{|A|^{3+\varepsilon'} d_*(A)^{1+\varepsilon'}}{(2^{j-1})^3} (2^j)^3 \ll |A|^{3+2\varepsilon'} d_*(A)^{1+2\varepsilon'}. \end{aligned}$$

∎

We now give the main result of this section. The following theorem will be used in section 4.2 when the multiplicative energy is small.

THEOREM 3.7. *Let $\varepsilon > 0$, and A be a finite set of quaternions. Then*

$$|A+A| \gg_\varepsilon \frac{|A|^{14/9-\varepsilon}}{d_*(A)^{5/9}}.$$

Proof. The proof combines (2.1), Corollary 3.4, Lemma 3.1, Corollary 3.5, and Corollary 3.6 (in the specified order). This gives, for $\varepsilon' = 9\varepsilon/22$,

$$\begin{aligned} \frac{|A|^{12}}{|A+A|^3} &\le E^+(A)^3 \\ &\ll_{\varepsilon'} |A|^{3+3\varepsilon'} d_*(A)^{1+3\varepsilon'} E_{1.5}^+(A)^2 \\ &\le |A|^{1+3\varepsilon'} d_*(A)^{1+3\varepsilon'} E_3^+(A) E^+(A, A+A) \\ &\ll_{\varepsilon'} |A|^{2+3\varepsilon'} d_*(A)^{3/2+4\varepsilon'} E_3^+(A) |A+A|^{3/2+\varepsilon'} \\ &\ll_{\varepsilon'} |A|^{5+4\varepsilon'} d_*(A)^{5/2+5\varepsilon'} |A+A|^{3/2+\varepsilon'}. \end{aligned}$$

This implies

$$|A+A|^{9/2+\varepsilon'} \gg_{\varepsilon'} \frac{|A|^{7-4\varepsilon'}}{d_*(A)^{5/2+5\varepsilon'}}.$$

The theorem now follows by noting that $|A+A| \le |A|^2$ and $d_*(A) \le |A|$. ∎

4. Main theorem. We are finally ready to prove Theorem 1.2. The section is organized as follows: in section 4.1, we use standard arguments to find a large subset of A with properties that will be convenient to work with. Section 4.2 will deal with the case when the additive energy of this subset is large, and section 4.3 will deal with the case when the additive energy is small.

4.1. Initial setup and pigeonholing. Let A be a finite set of quaternions. Since we are not concerned about constants, it suffices to prove (1.2) for a subset $A' \subseteq A$ containing a positive proportion of elements of A. We view a quaternion $a = w + xi + yj + zk$ as a vector $(w, x, y, z) \in \mathbb{R}^4$ and say that w and (x, y, z) are, respectively, the *real* and *imaginary* parts of a. By a simple pigeonholing argument, there exists a set A' of size at least $|A|/16$ such that all elements of A' lie in the same orthant of $\mathbb{R}^4$. We assume that $0 \notin A'$ and that each element of A' has nonnegative real part. The latter is without loss of generality since multiplication by reals is commutative and, hence, doesn't affect the sizes of the sum and product sets. To simplify notation, we identify A' with A, and assume that A satisfies the properties that we need.

To estimate the multiplicative energy, we will consider a subset of A/A, which we build incrementally. Let $R_0 = \{\lambda \in A/A : \delta_{A^{-1}A}(\lambda) \geq \delta_{AA^{-1}}(\lambda)\}$, and assume, without loss of generality, that

$$\sum_{\lambda \in R_0} \delta_{A^{-1}A}(\lambda)\delta_{AA^{-1}}(\lambda) \geq \sum_{\lambda \notin R_0} \delta_{A^{-1}A}(\lambda)\delta_{AA^{-1}}(\lambda).$$

This gives

$$E^*(A) = \sum_{\lambda \in A/A} \delta_{A^{-1}A}(\lambda)\delta_{AA^{-1}}(\lambda) \leq 2 \sum_{\lambda \in R_0} \delta_{A^{-1}A}(\lambda)\delta_{AA^{-1}}(\lambda) \leq 2 \sum_{\lambda \in R_0} \delta_{A^{-1}A}(\lambda)^2.$$

Next, we restrict our attention to $\lambda \in R_0$ with $\delta_{A^{-1}A}(\lambda) \geq E^*(A)/4|A|^2$. Let $R_1 = \{\lambda \in R_0 : \delta_{A^{-1}A}(\lambda) \geq E^*(A)/4|A|^2\}$. This is possible because ratios in $R_0 \setminus R_1$ can not account for too much the multiplicative energy, i.e.,

$$\sum_{\lambda \in R_0 \setminus R_1} \delta_{A^{-1}A}(\lambda)^2 < \frac{E^*(A)}{4|A|^2} \sum_{\lambda \in R_0 \setminus R_1} \delta_{A^{-1}A}(\lambda) \leq \frac{E^*(A)}{4} \leq \frac{1}{2} \sum_{\lambda \in R_0} \delta_{A^{-1}A}(\lambda)^2.$$

This implies that ratios in R_1 give the following bound on the multiplicative energy:

$$E^*(A) \ll \sum_{\lambda \in R_1} \delta_{A^{-1}A}(\lambda)^2. \tag{4.1}$$

For a positive integer τ, let S'_τ be the set $S'_\tau = \{\lambda \in R_1 : \tau \leq \delta_{A^{-1}A}(\lambda) < 2\tau\}$. Since $1 \leq \delta_{A^{-1}A}(\lambda) \leq |A|$, a dyadic decomposition of the summation in (4.1) gives

$$\sum_{\lambda \in R_1} \delta_{A^{-1}A}(\lambda)^2 = \sum_{i=0}^{\lceil \log |A| \rceil} \sum_{\lambda \in S'_{2^i}} \delta_{A^{-1}A}(\lambda)^2.$$

It follows, by the pigeonhole principle, that there exists a $\tau \geq E^*(A)/4|A|^2$ such that elements of S'_τ contribute at least $1/\lceil \log |A| \rceil$ to the sum. This implies

$$E^*(A) \lesssim \sum_{\lambda \in S'_\tau} \delta_{A^{-1}A}(\lambda)^2 \ll |S'_\tau|\tau^2.$$

Finally, for each $\lambda \in S'_\tau$, consider the set $A_\lambda := A \cap A\lambda$. Then $|A_\lambda| = \delta_{A^{-1}A}(\lambda)$, which implies that $\tau^2 \leq E^+(A_\lambda) \leq 8\tau^3$. A dyadic decomposition of this interval, along with the pigeonhole principle, implies that there exists $K \geq 1$ such that the set $S_\tau = \{\lambda \in S'_\tau : \tau^3/2K \leq E^+(A_\lambda) < \tau^3/K\}$ has cardinality $|S_\tau| \gtrsim |S'_\tau|$.

To sum up, for an integer

$$\tau \gg E^*(A)/|A|^2, \tag{4.2}$$

we have found a set $S_\tau \subseteq A/A$ such that

$$E^*(A) \lesssim |S_\tau|\tau^2, \tag{4.3}$$

and, for every $\lambda \in S_\tau$, we have

$$\delta_{A^{-1}A}(\lambda) \geq \delta_{AA^{-1}}(\lambda),\ |A_\lambda| = \delta_{A^{-1}A}(\lambda) \approx \tau, \text{ and } E^+(A_\lambda) \approx \tau^3/K \text{ for some } K \geq 1.$$

4.2. The case when K is small. We will show that there exists a *large* set $A' \subseteq A$ such that $d_*(A')$ is *small*. The result will then follow by using Theorem 3.7.

Recall that for $\lambda \in A/A$, $A_\lambda = A \cap A\lambda \subseteq A$. We will require the *Katz–Koester* inclusion, i.e., for any $\lambda \in A/A$, $A_\lambda A_\lambda \subseteq (AA) \cap (AA)\lambda$. Clearly $A_\lambda A_\lambda \subseteq (AA)$, so it suffices to show $A_\lambda A_\lambda \subseteq (AA)\lambda$. To see this, consider $a = b \cdot c \in A_\lambda A_\lambda$. Since $c \in A_\lambda$, there exists $c' \in A$ such that $c = c'\lambda$, that is, $c' = c\lambda^{-1} \in A$. Now we may write $a = b \cdot c = b \cdot c \cdot \lambda^{-1} \cdot \lambda = b \cdot c'\lambda \in (AA)\lambda$.

Note that

$$\sum_{a \in A} |A \cap aS_\tau| = \sum_{\lambda \in S_\tau} |A \cap A\lambda| \geq |S_\tau|\tau.$$

Then, by the pigeonhole principle, there exists $a \in A$ such that $A' := A \cap aS_\tau$ has size at least $|S_\tau|\tau/|A|$. Observe that Lemma 3.2 implies that, for all $\lambda \in S_\tau$,

$$|A_\lambda A_\lambda| \gg_{\varepsilon'} \frac{E^+(A_\lambda)^4}{|A_\lambda|^{10+\varepsilon'}} \approx \frac{\tau^{2-\varepsilon'}}{K^4}.$$

Now, for $b \in A'$ we can write $b = a\lambda$ for some $\lambda \in S_\tau$. This implies

$$|(AA) \cap (AAa^{-1})b| = |(AA) \cap (AA)\lambda| \geq |A_\lambda A_\lambda| \gg_{\varepsilon'} \frac{\tau^{2-\varepsilon'}}{K^4}.$$

Since this holds for any $b \in A'$, we get

$$d_*(A') \ll_{\varepsilon'} \frac{|AA|^4}{|A'|(\tau^{2-\varepsilon'}/K^4)^3} = \frac{|AA|^4 K^{12}}{|A'|\tau^{6-3\varepsilon'}},$$

by letting $Q = AA$, $R = AAa^{-1}$, and $t = \tau^{2-\varepsilon'}/K^4$ in the definition of $d_*(A')$.

Combining this with Theorem 3.7 gives

$$|A + A|^9 \gg_{\varepsilon'} \frac{|A'|^{14-\varepsilon'}}{d_*(A')^5} \gg_{\varepsilon'} \frac{|A'|^{19-\varepsilon'}\tau^{30-15\varepsilon'}}{K^{60}|AA|^{20}}.$$

We then apply (4.3), (4.2), and (2.2), in the specified order, to get

$$\begin{aligned}
K^{60}|AA|^{20}|A+A|^9 &\gg_{\varepsilon'} |A'|^{19-\varepsilon'}\tau^{30-15\varepsilon'} \geq \left(\frac{|S_\tau|\tau}{|A|}\right)^{19-\varepsilon'} \cdot \tau^{30-15\varepsilon'} \\
&= \left(|S_\tau|\tau^2\right)^{19-\varepsilon'} \cdot \frac{\tau^{11-14\varepsilon'}}{|A|^{19-\varepsilon'}} \gtrsim E^*(A)^{19-\varepsilon'} \cdot \frac{\tau^{11-14\varepsilon'}}{|A|^{19-\varepsilon'}} \\
&= \left(\frac{E^*(A)}{|A|}\right)^{19-\varepsilon'} \cdot \tau^{11-14\varepsilon'} \gg \left(\frac{E^*(A)}{|A|}\right)^{19-\varepsilon'} \cdot \left(\frac{E^*(A)}{|A|^2}\right)^{11-14\varepsilon'} \\
&= \frac{E^*(A)^{30-15\varepsilon'}}{|A|^{41-29\varepsilon'}} \geq \frac{1}{|A|^{41-29\varepsilon'}} \cdot \left(\frac{|A|^4}{|AA|}\right)^{30-15\varepsilon'} \\
&= \frac{|A|^{79-31\varepsilon'}}{|AA|^{30-15\varepsilon'}}.
\end{aligned}$$

That is, we have

$$|AA|^{50}|A+A|^9 \gtrsim_\varepsilon \frac{|A|^{79-\varepsilon}}{K^{60}}.$$

When $K \leq |A|^\delta$ for some fixed $\delta > 0$, this implies $|A+A| + |AA| > |A|^{4/3+c}$ where $c > 0$ is an absolute constant.

4.3. The case when K is large. Now we handle the case that $K > |A|^\delta$, where δ is the parameter chosen at the end of the previous section. For convenience of notation, we label the slopes in S_τ by distinct integers, and let $A_i = A_{\lambda_i} = A \cap A\lambda_i$ for each $\lambda_i \in S_\tau$.

A key observation, first exploited by Solymosi in the real case [14] and by Solymosi and Wong [16] for quaternions, is that, for distinct $\lambda_i, \lambda_j \in S_\tau$ and $a_1, a_2 \in A_i, b_1, b_2 \in A_j$ with $(a_1, b_1) \neq (a_2, b_2)$, we have $(a_1, a_1\lambda_i) + (b_1, b_1\lambda_j) \neq (a_2, a_2\lambda_i) + (b_2, b_2\lambda_j)$. Indeed, since $\lambda_i \neq \lambda_j$, we have that $(\lambda_i - \lambda_j)$ is invertible. Hence, given $x, y \in \mathbb{H}$, we can solve the equations

$$a + b = x, \qquad a\lambda_i + b\lambda_j = y$$

uniquely for a, b.

For pairs of distinct elements $\{\lambda_i, \lambda_j\}, \{\lambda_k, \lambda_\ell\} \in \binom{S_\tau}{2}$, we say that $\{\lambda_i, \lambda_j\}$ *conflicts* with $\{\lambda_k, \lambda_\ell\}$ if $\{\lambda_i, \lambda_j\} \neq \{\lambda_k, \lambda_\ell\}$ and

$$((A_i + A_j) \times (A_i\lambda_i + A_j\lambda_j)) \cap ((A_k + A_l) \times (A_k\lambda_k + A_l\lambda_l)) \neq \emptyset.$$

In order to find a large set of distinct elements of $(A+A) \times (A+A)$, we will consider sums $((a, a\lambda_i) + (b, b\lambda_j)) \in ((A_i, A_i\lambda_i) + (A_j, A_j\lambda_j))$ for edges $\{\lambda_i, \lambda_j\}$ in a carefully selected graph $G \subset \binom{S_\tau}{2}$. We construct G so that few pairs of edges conflict. For each pair of edges that does conflict, we apply an observation of Konyagin and Shkredov [8] (adapted from the real to quaternionic case) to bound the number of elements of $(A+A) \times (A+A)$ that we count more than once.

First we give the observation of Konyagin and Shkredov. Using the assumption on the additive energy of each A_i, we can bound the number of repeated sums coming from each pair of conflicting edges.

LEMMA 4.1. *Let $\{\lambda_i, \lambda_j\}$, $\{\lambda_k, \lambda_\ell\}$ be a pair of conflicting edges. Then,*

$$|((A_i + A_j) \times (A_i\lambda_i + A_j\lambda_j)) \cap ((A_k + A_\ell) \times (A_k\lambda_k + A_\ell\lambda_\ell))| \lesssim \tau^2 K^{-1/2}. \tag{4.4}$$

Proof. Suppose, without loss of generality, that λ_ℓ is distinct from λ_i and λ_j. Note that quadruples $(a_i, a_j, a_k, a_\ell) \in A_i \times A_j \times A_k \times A_\ell$ that contribute to (4.4) satisfy

$$a_i + a_j = a_k + a_\ell, \tag{4.5}$$

$$a_i\lambda_i + a_j\lambda_j = a_k\lambda_k + a_\ell\lambda_\ell. \tag{4.6}$$

Subtracting (4.5) multiplied by λ_ℓ on the right from (4.6), we obtain

$$a_i(\lambda_i - \lambda_\ell) + a_j(\lambda_j - \lambda_\ell) = a_k(\lambda_k - \lambda_\ell). \tag{4.7}$$

Hence, $|((A_i + A_j) \times (A_i\lambda_i + A_j\lambda_j)) \cap ((A_k + A_\ell) \times (A_k\lambda_k + A_\ell\lambda_\ell))|$ is bounded above by the number T of $(a_i, a_j, a_k) \in A_i \times A_j \times A_k$ that satisfy (4.7).

Applying Cauchy–Schwarz twice, we obtain

$$\begin{aligned} T &\le |A_k|^{1/2} E^+(A_i(\lambda_i - \lambda_l), A_j(\lambda_j - \lambda_l))^{1/2}, \\ &\le |A_k|^{1/2} E^+(A_i)^{1/4} E^+(A_j)^{1/4}. \end{aligned}$$

By construction, $|A_i| \approx \tau$ and $E^+(A_i) \approx \tau^3 K^{-1}$ for each i. Hence,

$$T \lesssim \tau^2 K^{-1/2},$$

as claimed. ∎

We also need to limit the number of pairs $(\lambda_i, \lambda_j), (\lambda_k, \lambda_\ell) \in G$ for which this intersection is nonempty. This involves controlling when such intersections can occur and choosing G accordingly.

First, we establish that any ratio $(a_i + a_j)^{-1}(a_i\lambda_i + a_j\lambda_j)$ with $a_i \in A_i, a_j \in A_j$ must be close to λ_i. This is Lemma 7 in Solymosi and Wong [16].

LEMMA 4.2. *For any distinct $\lambda_i, \lambda_j \in S_\tau$ and $a_i \in A_i$, $a_j \in A_j$, we have*

$$\|(a_i + a_j)^{-1}(a_i\lambda_i + a_j\lambda_j) - \lambda_i\| \le \|\lambda_j - \lambda_i\|.$$

Proof. Recall that a_i and a_j are in the same orthant, so $\|a_i + a_j\| \ge \|a_j\|$. Using the identity $(a_i + a_j)^{-1} = (1 - (a_i + a_j)^{-1}a_j)a_i^{-1}$, we have

$$\begin{aligned} \|(a_i + a_j)^{-1}(a_i\lambda_i + a_j\lambda_j) - \lambda_i\| &= \|(1 - (a_i + a_j)^{-1}a_j)\lambda_i + (a_i + a_j)^{-1}a_j\lambda_j - \lambda_i\|, \\ &= \|(a_i + a_j)^{-1}a_j(\lambda_j - \lambda_i)\|, \\ &= \|\lambda_j - \lambda_i\| \, \|a_j\| \, \|a_i + a_j\|^{-1}, \\ &\le \|\lambda_j - \lambda_i\|. \end{aligned}$$

∎

Now we define G. Let M be a positive integer parameter that we will fix later. Let G be the graph on vertex set S_τ formed by joining each $\lambda \in S_\tau$ to its M closest neighbors, breaking ties arbitrarily. Since the degree of each vertex of G is at least M, the number of edges in G is at least $M|S_\tau|/2$. We also need to bound the number of conflicting pairs of edges in G.

Let B_i be the smallest closed ball centered at λ_i that contains at least $M + 1$ points of S_τ (including λ_i itself), and let R_i be the radius of B_i. While a given ball B_i may contain an arbitrary number of points of S_τ, the interior of each ball contains at most M points.

Note that if $\{\lambda_i, \lambda_j\} \in G$, then at least one of $\lambda_i \in B_j$ or $\lambda_j \in B_i$. In addition, from Lemma 4.2, we have that, for any distinct λ_i, λ_k, if there exist $\lambda_j \in B_i, \lambda_\ell \in B_k$ such that $\{\lambda_i, \lambda_j\}$ conflicts with $\{\lambda_k, \lambda_\ell\}$, then $B_i \cap B_k \neq \emptyset$.

For each λ_i, let L_i be the set of λ_j such that $R_j \geq R_i$ and $B_i \cap B_j \neq \emptyset$. Given any λ_i, and $\lambda_j \in L_i$, the number of pairs of edges $\{\lambda_i, \lambda_k\}, \{\lambda_j, \lambda_\ell\}$ that conflict is bounded above by the product of the degrees of λ_i and λ_j. Hence, to bound the number of conflicting pairs of edges, it will suffice to place upper bounds on the degree of each vertex of G, and the size of each set L_i. This is done in Lemmas 4.4 and 4.5, respectively.

The proofs of both Lemma 4.4 and 4.5 both rely on similar geometric averaging arguments. In each case, for a fixed λ_i, we bound the number of interesting λ_j in an arbitrary cone of constant size with vertex λ_i. By linearity of expectation, this gives an upper bound on the number of interesting λ_j in all directions from λ_i.

The following simple geometric lemma used in both proofs.

LEMMA 4.3. *Let $\mathbf{x}, \mathbf{y}$ be arbitrary vectors in $\mathbb{R}^4$, and let $\mathbf{u}$ be a unit vector. Let $\mathbf{x}^\perp$ and $\mathbf{y}^\perp$ be the projections of $\mathbf{x}$ and $\mathbf{y}$ onto the subspace orthogonal to $\mathbf{u}$. Then,*

$$\|\mathbf{x} - \mathbf{y}\|^2 \leq \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 - 2(\mathbf{x} \cdot \mathbf{u})(\mathbf{y} \cdot \mathbf{u}) + 2\|\mathbf{x}^\perp\|\|\mathbf{y}^\perp\|.$$

Proof.

$$\begin{aligned}
\|\mathbf{x} - \mathbf{y}\|^2 &= \|(\mathbf{x} \cdot \mathbf{u} - \mathbf{y} \cdot \mathbf{u})\mathbf{u} + \mathbf{x}^\perp - \mathbf{y}^\perp\|^2, \\
&= (\mathbf{x} \cdot \mathbf{u} - \mathbf{y} \cdot \mathbf{u})^2 + \|\mathbf{x}^\perp - \mathbf{y}^\perp\|^2, \\
&\leq (\mathbf{x} \cdot \mathbf{u} - \mathbf{y} \cdot \mathbf{u})^2 + (\|\mathbf{x}^\perp\| + \|\mathbf{y}^\perp\|)^2, \\
&= \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 - 2(\mathbf{x} \cdot \mathbf{u})(\mathbf{y} \cdot \mathbf{u}) + 2\|\mathbf{x}^\perp\|\|\mathbf{y}^\perp\|. \qquad \square
\end{aligned}$$

LEMMA 4.4. *For each i, the degree $\deg(\lambda_i)$ of λ_i in G is bounded by*

$$\deg(\lambda_i) \ll M.$$

Proof. Take λ_i to be at the origin. Let $\mathbf{u}$ be an arbitrary unit vector, and let C be the cone

$$C = \{\mathbf{x} : \mathbf{x} \cdot \mathbf{u} > (\sqrt{3}/2)\|\mathbf{x}\|\}.$$

We will use the decomposition $\mathbf{x} = (\mathbf{x} \cdot \mathbf{u})\mathbf{u} + \mathbf{x}^\perp$. Note that if $\mathbf{x} \in C$, then

$$\|\mathbf{x}^\perp\|^2 = \|\mathbf{x}\|^2 - (\mathbf{x} \cdot \mathbf{u})^2 < (1/4)\|\mathbf{x}\|^2.$$

Let $\mathbf{x}, \mathbf{y}$ be vectors in C with $\|\mathbf{x}\| \geq \|\mathbf{y}\|$. By Lemma 4.3,

$$\begin{aligned}
\|\mathbf{x} - \mathbf{y}\|^2 &\leq \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 - 2(\mathbf{x} \cdot \mathbf{u})(\mathbf{y} \cdot \mathbf{u}) + 2\|\mathbf{x}^\perp\|\|\mathbf{y}^\perp\|, \\
&< \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 - \|\mathbf{x}\|\|\mathbf{y}\|, \\
&\leq \|\mathbf{x}\|^2.
\end{aligned}$$

To put this another way, the distance between any pair of points in C is less than the distance from the more distant point to λ_i.

Consequently, λ_i has at most M neighbors in C. Indeed, suppose for contradiction that there are $M + 1$ neighbors in C, and let λ be a neighbor at the largest distance from λ_i. Then, all of the remaining M of the neighbors are closer to λ than λ_i is. This is a contradiction, since only the M closest points to λ are selected as neighbors.

The preceding argument applies for an arbitrary unit vector $\mathbf{u}$. Suppose, for contradiction, that λ_i has more than cM neighbors for a sufficiently large constant c. Then, the expected number of neighbors in the cone corresponding to a uniformly random $\mathbf{u}$ will be greater than M, but we have shown that there cannot be any $\mathbf{u}$ for which this number is greater than M. ∎

Next we bound $|L_i|$ for an arbitrary λ_i.

LEMMA 4.5. *For each i,*

$$|L_i| \ll M.$$

Proof. Take λ_i to be at the origin. Let $\mathbf{u}$ be an arbitrary unit vector, and let C be the cone

$$C = \{\mathbf{x} : \mathbf{x} \cdot \mathbf{u} > 0.99\|\mathbf{x}\|\}.$$

Note that, if $\mathbf{x} \in C$, then

$$\|\mathbf{x}^{\perp}\|^2 = \|\mathbf{x}\|^2 - (\mathbf{x} \cdot \mathbf{u})^2 < 0.02\|\mathbf{x}\|^2.$$

If $\mathbf{x}, \mathbf{y}$ are vectors in C, then by Lemma 4.3,

$$\begin{aligned} \|\mathbf{x} - \mathbf{y}\|^2 &\leq \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 - 2(\mathbf{x} \cdot \mathbf{u})(\mathbf{y} \cdot \mathbf{u}) + 2\|\mathbf{x}^{\perp}\|\|\mathbf{y}^{\perp}\|, \\ &< \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 - 1.92\|\mathbf{x}\|\|\mathbf{y}\|. \end{aligned} \tag{4.8}$$

Define the following subsets of C:

$$\begin{aligned} C_1 &= \{\mathbf{x} \in C : \|\mathbf{x}\| < R_i\}, \\ C_2 &= \{\mathbf{x} \in C : R_i \leq \|\mathbf{x}\| < 1.5R_i\}, \\ C_3 &= \{\mathbf{x} \in C : 1.5R_i \leq \|\mathbf{x}\|\}. \end{aligned}$$

We will show that each of C_1, C_2, and C_3 contains at most M points of L_i.

Since every point of S_τ that is at distance less than R_i from λ_i is a neighbor of λ_i, it is immediate that C_1 contains fewer than M points of S_τ.

Let $\mathbf{x}, \mathbf{y}$ be vectors in C_2 with $R_i \leq \|\mathbf{y}\| \leq \|\mathbf{x}\| < 1.5R_i$. By (4.8),

$$\begin{aligned} \|\mathbf{x} - \mathbf{y}\|^2 &< \|\mathbf{x}\|^2 + \|\mathbf{y}\|^2 - 1.92\|\mathbf{x}\|\|\mathbf{y}\|, \\ &\leq \|\mathbf{x}\|^2 + \|\mathbf{x}\|\|\mathbf{y}\| - 1.92\|\mathbf{x}\|\|\mathbf{y}\|, \\ &\leq \|\mathbf{x}\|^2 - 0.92\|\mathbf{x}\|R_i, \\ &< 0.87R_i^2. \end{aligned}$$

In other words, each pair of vectors in C_2 is at distance less than R_i. By assumption, if R is the radius of the ball associated to any $\lambda \in L_i$, we have $R \geq R_i$. If there are $M+1$ points of L_i in C_2, then the ball associated to each of these points contains all $M+1$ of the points in its interior, which contradicts the construction of the balls.

Let $\mathbf{x}, \mathbf{y}$ be vectors in C_3 with $1.5R_i \leq \|\mathbf{y}\| \leq \|\mathbf{x}\|$. We claim that

$$\|\mathbf{x} - \mathbf{y}\|^2 < (\|\mathbf{x}\| - R_i)^2. \tag{4.9}$$

From (4.8), in order to prove (4.9), it is enough to show that

$$\|\mathbf{y}\|^2 + 2\|\mathbf{x}\|R_i - 1.92\|\mathbf{x}\|\|\mathbf{y}\| - R_i^2 < 0, \tag{4.10}$$

$$\text{under the assumption that} \qquad \|\mathbf{x}\| \geq \|\mathbf{y}\| \geq 1.5R_i. \tag{4.11}$$

When the left-hand side of (4.10) is constrained to the line $\|\mathbf{x}\| = \|\mathbf{y}\|$, we have

$$-0.98\|\mathbf{x}\|^2 + 2\|\mathbf{x}\|R_i + R_i^2.$$

The derivative of this is negative for $\|\mathbf{x}\| \geq 1.5R_i$. Furthermore, when $\|\mathbf{y}\| \geq 1.5R_i$, the left-hand side of (4.10) is decreasing in $\|\mathbf{x}\|$. Hence, it suffices to consider the point $\|\mathbf{x}\| = \|\mathbf{y}\| = 1.5R_i$. At this point, the left-hand side of (4.10) is $-.07R_i < 0$, as claimed.

The meaning of (4.9) is that, given any two points in C_3, the distance from the point that is further from λ_i to the nearest point of B_i is greater than the distance between the two points. Consequently, if C_3 contains $M+1$ points of L_i, the ball around the furthest point (which intersects B_i) must contain all $M+1$ points strictly in its interior, which is a contradiction. ∎

Let $T \subset G^2$ be the set of pairs of edges in G that conflict. Applying Lemmas 4.4 and 4.5,

$$|T| \leq \sum_i \deg(\lambda_i) \sum_{\lambda_j \in L_i} \deg(\lambda_j) \ll |S_\tau| M^3. \tag{4.12}$$

We have

$$(A+A) \times (A+A) \supset \bigcup_{\{\lambda_i, \lambda_j\} \in G} (A_i + A_j) \times (A_i\lambda_i + A_j\lambda_j).$$

Using inclusion-exclusion and Lemma 4.1, this implies that

$$|(A+A) \times (A+A)| \geq |G|\tau^2 - c|T|\tau^2 K^{-1}$$

for some $c > 0$. Since the degree of each $\lambda_i \in G$ is at least M, we have $|G| \geq |S_\tau|M/2$. Together with (4.12), we get

$$|(A+A) \times (A+A)| \geq |S_\tau| M\tau^2/2 - c|S_\tau| M^3 \tau^2 K^{-1/2}.$$

Taking $M = c'K^{1/6}$ for a sufficiently small constant c', we obtain

$$|A+A|^2 \gg |S_\tau|\tau^2 K^{1/6} \gtrsim E^*(A) K^{1/6} \geq |A|^4 |AA|^{-1} K^{1/6}.$$

Assuming that $K > |A|^\delta$ for some fixed $\delta > 0$, this shows that $|A+A| + |AA| \gtrsim |A|^{4/3+\delta/18}$, as claimed.

Acknowledgments. We would like to thank Oliver Roche-Newton for sharing his unpublished notes on Konyagin and Shkredov's sum-product bound. We would like to thank Adam Sheffer for extensive discussions on an earlier version of this paper.

REFERENCES

[1] M.-C. Chang, *A sum-product estimate in algebraic division algebras*, Israel J. Math., 150 (2005), pp. 369–380.
[2] G. Elekes, *On the number of sums and products*, Acta Arithmetica, 81 (1997), pp. 365–367.
[3] G. Elekes and I. Ruzsa, *Few sums, many products*, Stud. Sci. Math. Hungar., 40 (2003), pp. 301–308.
[4] P. Erdős and E. Szemerédi, *On sums and products of integers*, in Studies in Pure Mathematics, Springer, New York, 1983, pp. 213–218.
[5] K. Ford, *Sums and products from a finite set of real numbers*, Ramanujan J., 2 (1998), pp. 59–66.

[6] A. Granville and J. Solymosi, *Sum-product formulae*, in Recent Trends in Combinatorics, Springer, New York, 2016, pp. 419–451.
[7] S. Konyagin and M. Rudnev, *On new sum-product–type estimates*, SIAM J. Discrete Math., 27 (2013), pp. 973–990.
[8] S. Konyagin and I. Shkredov, *On sum sets of sets having small product set*, Proc. Steklov Institute Math., 290 (2015), pp. 288–299.
[9] S. Konyagin and I. Shkredov, *New results on sums and products in* $\mathbb{R}$, Proc. Steklov Institute Math., 294 (2016), pp. 78–88.
[10] L. Li, *On a theorem of Schoen and Shkredov on sumsets of convex sets*, preprint arXiv:1108.4382, 2011.
[11] M. Nathanson, *On sums and products of integers*, Proc. Amer. Math. Soc., 125 (1997), pp. 9–16.
[12] M. Rudnev, I. Shkredov, and S. Stevens, *On the energy variant of the sum-product conjecture*, preprint, arXiv:1607.05053, 2016.
[13] G. Shakan, *On higher energy decompositions and the sum–product phenomenon*, in Mathematical Proceedings of the Cambridge Philosophical Society, Cambridge University Press, Cambridge, 2018, pp. 1–19.
[14] J. Solymosi, *Bounding multiplicative energy by the sumset*, Adv. Math., 222 (2009), pp. 402–408.
[15] J. Solymosi and T. Tao, *An incidence theorem in higher dimensions*, Discrete Comput. Geom., 48 (2012), pp. 255–280.
[16] J. Solymosi and C. Wong, *An application of kissing numbers in sum-product estimates*, preprint, arXiv:1709.08758, 2017.