A LOW-ENERGY DECOMPOSITION THEOREM

ANTAL BALOG* AND TREVOR D. WOOLEY

Abstract. We prove that any finite set of real numbers can be split into two parts, one part being highly non-additive and the other highly non-multiplicative.

1. Introduction

The Erdős-Szemerédi sum-product conjecture asserts that the additive structure of a finite set of real numbers should be essentially independent of its multiplicative structure. Given finite sets of real numbers A and B, define the sum set and product set by

$$A+B=\{a+b:(a,b)\in A\times B\} \quad \text{and} \quad A\cdot B=\{ab:(a,b)\in A\times B\}.$$

Then, on writing $|\mathcal{S}|$ for the cardinality of a set $\mathcal{S}$, the conjecture of Erdős and Szemerédi (see the introduction of [3]) asserts that for any $\varepsilon>0$ and for any sufficiently large finite set $A\subset\mathbb{R}$, one should have

$$\max\{|A+A|,|A\cdot A|\}\geqslant |A|^{2-\varepsilon}.$$

The sharpest conclusion in this direction available in the published literature is due to Solymosi [11, Corollary 2.2], and shows that

$$\max\{|A+A|,|A\cdot A|\}\geqslant \frac{|A|^{4/3}}{2\lceil\log|A|\rceil^{1/3}}.$$

This result has recently been improved by Konyagin and Shkredov, to the extent that the exponent $\frac{4}{3}$ may now be replaced by $\frac{4}{3}+c$, for any $c<1/20598$ (see [5, Theorem 3] and the discussion concluding the latter paper).

As is well known, should the elements of A be controlled by additive structure, then $|A+A|$ is small. Likewise, should A be controlled by multiplicative structure, then $|A\cdot A|$ is small. The Erdős-Szemerédi conjecture expresses the belief that these two behaviours cannot be exhibited simultaneously.

A concrete measure of the additivity of a set is its additive energy

$$E_+(A)=\operatorname{card}\{\mathbf{a}\in A^4:a_1+a_2=a_3+a_4\}.$$

Similarly, the multiplicativity of a set is measured by its multiplicative energy

$$E_\times(A)=\operatorname{card}\{\mathbf{a}\in A^4:a_1a_2=a_3a_4\}.$$

2010 *Mathematics Subject Classification.* 11B13, 11B30, 11B75.

Key words and phrases. Sum-product estimates, additive energy, multiplicative energy.

*Research supported by the Hungarian National Science Foundation Grants K104183 and K109789.

One also has corresponding measures of the energy between two sets, namely

$$E_+(A,B) = \mathrm{card}\{(\mathbf{a},\mathbf{b}) \in A^2 \times B^2 : a_1 + b_1 = a_2 + b_2\}$$

and

$$E_\times(A,B) = \mathrm{card}\{(\mathbf{a},\mathbf{b}) \in A^2 \times B^2 : a_1 b_1 = a_2 b_2\}.$$

Writing

$$r_{A+B}(x) = \mathrm{card}\{(a,b) \in A \times B : a + b = x\}$$

and

$$r_{A\cdot B}(x) = \mathrm{card}\{(a,b) \in A \times B : ab = x\},$$

we see that

$$E_+(A) = \sum_{x \in A+A} r_{A+A}(x)^2 \quad \text{and} \quad E_\times(A) = \sum_{x \in A\cdot A} r_{A\cdot A}(x)^2.$$

It follows from Cauchy's inequality that

$$|A|^4 = \bigg(\sum_{x \in A+A} r_{A+A}(x) \bigg)^2 \leqslant E_+(A)|A+A|, \tag{1.1}$$

so that, whenever $|A+A|$ is small, then $E_+(A)$ is big. In similar fashion, if $|A \cdot A|$ is small, then $E_\times(A)$ is necessarily big. Thus, one might naïvely believe that the sum-product conjecture is manifested by the phenomenon that one or other of $E_+(A)$ and $E_\times(A)$ is always small. However, a moments' reflection reveals that such is certainly not the case, since the respective converses of the above observations are in general false. Thus, if $N \in \mathbb{N}$ and

$$A = \{0, 1, \dots, N-1\} \cup \{N, N^2, \dots, N^N\}, \tag{1.2}$$

then

$$\min\{E_+(A), E_\times(A)\} \gg N^3 \gg |A|^3.$$

In §3, we show that any set A can be split into two parts B and C, having the property that both $E_+(B)$ and $E_\times(C)$ are small. Consequently, the naïve belief expressed above is obstructed only by examples closely related to that defined by (1.2).

Theorem 1.1. *Let A be a finite subset of the real numbers. Then, with $\delta = \frac{2}{33}$, there exist disjoint subsets B and C of A, with $A = B \cup C$,*

$$\max\{E_+(B), E_\times(C)\} \ll |A|^{3-\delta}(\log |A|)^{1-3\delta}$$

and

$$\max\{E_+(B,C), E_\times(B,C)\} \ll |A|^{3-\delta/2}(\log |A|)^{(1-3\delta)/2}.$$

This theorem shows that any finite set of real numbers can be split into a highly non-additive part and a highly non-multiplicative part, and indeed, at least half of the set is either highly non-additive or highly non-multiplicative. Moreover, this decomposition has a doubly orthogonal flavour, the respective parts B and C being approximately orthogonal in terms both of their mutual additive energy, and also their mutual multiplicative energy.

It is tempting to conjecture that such decompositions should exist having the property that $\max\{E_+(B), E_\times(C)\} \ll |A|^{2+\varepsilon}$, for any $\varepsilon > 0$. By applying

(1.1) and its multiplicative analogue, such would imply the Erdős-Szemerédi conjecture in full. However, as we demonstrate in §2, this tempting conjecture is over-ambitious. Let us describe the exponent β as being a *permissible low-energy decomposition exponent* when, for each $\varepsilon > 0$ and for all sufficiently large finite subsets A of $\mathbb{R}$, there exist disjoint sets B and C, with $A = B \cup C$ and

$$\max\{E_+(B), E_\times(C)\} \leqslant |A|^{2+\beta+\varepsilon}.$$

Theorem 1.2. *The infimum κ of all permissible low-energy decomposition exponents satisfies $\frac{1}{3} \leqslant \kappa \leqslant \frac{31}{33}$.*

In particular, there exist arbitrarily large finite subsets A of $\mathbb{R}$ for which every decomposition into two parts B and C satisfies the lower bound

$$\max\{E_+(B), E_\times(C)\} \gg |A|^{7/3}.$$

The problem of determining the infimal exponent κ seems interesting, as well as very delicate, and we do not have a reasonable conjecture as to its value.

Our methods extend naturally to other settings, with obvious adjustments to our previous definitions concerning additive and multiplicative energies, and associated concepts. For example, an analogous argument yields a related conclusion in the setting of the finite field $\mathbb{F}_p$ having p elements. This we establish in §4.

Theorem 1.3. *Let p be a large prime, and suppose that $A \subseteq \mathbb{F}_p$ satisfies $|A| \leqslant p^\alpha(\log p)^\beta$, where we write*

$$\alpha = \frac{101}{161} \quad \text{and} \quad \beta = \frac{71}{161}.$$

Then, with $\delta = 4/101$, there exist disjoint subsets B and C of A, satisfying $A = B \cup C$ and

$$\max\{E_+(B), E_\times(C)\} \ll |A|^{3-\delta}(\log|A|)^{1-\delta/2}.$$

When $|A| \geqslant p^\alpha(\log p)^\beta$, meanwhile, one has instead

$$\max\{E_+(B), E_\times(C)\} \ll |A|^3(|A|/p)^{1/15}(\log|A|)^{14/15}.$$

In the second of these conclusions, the upper bound for $\max\{E_+(B), E_\times(C)\}$ becomes non-trivial only when $|A|$ is smaller than about $p(\log p)^{-14}$. It may be worth emphasising that a bound here uniform in p is certainly not available, for a simple argument presented at the end of §4 confirms that in the setting of the finite field $\mathbb{F}_p$, one always has

$$E_+(B) \geqslant |B|^4/p \quad \text{and} \quad E_\times(C) \geqslant |C|^4/p, \tag{1.3}$$

whence

$$\max\{E_+(B), E_\times(C)\} \gg |A|^3(|A|/p).$$

We mention a prototype application for the low-energy decomposition theorem recorded in Theorem 1.3. In his Ph.D. thesis at the University of Toronto

(see [4, §4]), Brandon Hanson gives a non-trivial bound for the character sum

$$H_\chi(A,B,C,D) = \sum_{a\in A}\sum_{b\in B}\sum_{c\in C}\sum_{d\in D}\chi(a+b+cd), \tag{1.4}$$

where χ is a non-principal character modulo p, and A, B, C, D are subsets of the finite field $\mathbb{F}_p$. All four sets can be somewhat smaller than $\sqrt{p}$ in his work, and hence he breaks the "square-root barrier". Hanson makes use of different arguments according to whether $E_+(C)$ or $E_\times(C)$ is small. Such an argument would naturally utilise a conclusion of the shape recorded in Theorem 1.3: the sum (1.4) can be split into two sums by writing $C = C_1 \cup C_2$, with $E_+(C_1)$ and $E_\times(C_2)$ both small, and then each sum may be estimated in turn by appeal to one or other of Hanson's arguments. Thus, in [4, Corollary 1 to Theorem 2], Hanson shows that when $|A|$, $|B|$, $|C|$ and $|D|$ each exceed $p^{1/2-\tau}$, with $\tau = 1/176$, then $H_\chi(A,B,C,D) \ll p^{-\varepsilon}|A||B||C||D|$, for a positive number ε depending at most on δ. We describe the impact of estimates of the shape of that supplied by Theorem 1.3 for such conclusions in §6.

It is not hard to extend our results from the above notions of energy to the analogous concept of k-fold energy. Given finite subsets A_i of real numbers, define

$$E_+(A_1,\dots,A_k) = \mathrm{card}\{\mathbf{a},\mathbf{a}' \in A_1\times\dots\times A_k : a_1+\dots+a_k = a_1'+\dots+a_k'\},$$
$$E_\times(A_1,\dots,A_k) = \mathrm{card}\{\mathbf{a},\mathbf{a}' \in A_1\times\dots\times A_k : a_1\cdots a_k = a_1'\cdots a_k'\}.$$

For the sake of convenience, we then put

$$E_+^{(k)}(A) = E_+(\underbrace{A,\dots,A}_{k}) \quad \text{and} \quad E_\times^{(k)}(A) = E_\times(\underbrace{A,\dots,A}_{k}).$$

As an immediate consequence of Theorem 1.1, in §5 we obtain the following low-energy decomposition theorem for k-fold energies.

Theorem 1.4. *Let A be a finite subset of the real numbers, and suppose that m and n are integers with $m \geqslant 2$ and $n \geqslant 2$. Then, with $\delta = \frac{2}{33}$, there exist disjoint subsets B and C of A, with $A = B \cup C$,*

$$E_+^{(m)}(B) \ll |A|^{2m-1-\delta}(\log|A|)^{1-\delta}$$

and

$$E_\times^{(n)}(C) \ll |A|^{2n-1-\delta}(\log|A|)^{1-\delta}.$$

Our approach to proving this theorem involves a reduction to the 2-fold energy central to Theorem 1.1, and fails to make any use of the richer structure available for the k-fold energy. It seems unlikely that this approach is particularly effective. Rather, we simply want to point out that low-energy decomposition theorems are available for k-fold energies. One would like to see a much sharper result, involving a saving in the exponent which grows with m (or n) in place of the constant saving $\frac{2}{33}$ in the conclusion of Theorem 1.4. We note in this context that a construction analogous to that in §2 delivering Theorem 1.2 shows only that there exist arbitrarily large finite subsets A of $\mathbb{R}$

for which, for all natural numbers m and n with $m \geqslant 2$ and $n \geqslant 2$, and for every decomposition of A into two parts B and C, one has either

$$E_+^{(m)}(B) \gg |A|^{(4m-1)/3} \quad \text{or} \quad E_\times^{(n)}(C) \gg |A|^{(4n-1)/3}.$$

Throughout this paper, we write $\lceil \theta \rceil$ for the smallest integer no smaller than θ, and $\lfloor \theta \rfloor$ for the largest integer not exceeding θ. Also, when describing ranges for integers in the definitions of sets, for example, we write $n \leqslant N$ to denote the constraint $1 \leqslant n \leqslant N$.

The authors wish to express their gratitude to Misha Rudnev for an insightful suggestion relevant to low-energy decompositions in finite fields. His suggestion of the use of a relation of the shape $E_+(A) \ll |A \cdot A|^{3/2}|A|$ led us to formulate Lemma 4.6, and fostered the significant improvement of our previous bounds in Theorem 4.2 now recorded in Theorem 1.3. We thank him for his generous contribution to this paper, and also for his comments on an earlier draft of this paper. We are also grateful to the referee for detailed comments that have improved the exposition of this paper.

2. Permissible low-energy decomposition exponents

We begin our exploration of low-energy decompositions with the proof of Theorem 1.2. Here, we temporarily assume the truth of Theorem 1.1, deferring its proof to §3. Thus, we may suppose that, for each positive number ε, there exists a permissible low-energy decomposition exponent β with $\beta \leqslant \frac{31}{33} + \varepsilon$. It follows that the infimum κ of all such exponents satisfies $\kappa \leqslant \frac{31}{33}$. Consequently, it remains only to show that $\kappa \geqslant \frac{1}{3}$.

Fix a large positive integer N, and put

$$A = \{(2m-1)2^n : m \leqslant N^{2/3} \text{ and } n \leqslant N^{1/3}\}.$$

Thus, one has $|A| = N + O(N^{2/3})$. We claim that whenever $B \subseteq A$ and $|B| \geqslant |A|/2$, then one necessarily has both

$$E_+(B) \gg N^{7/3} \quad \text{and} \quad E_\times(B) \gg N^{7/3}. \tag{2.1}$$

Suppose that $B \subseteq A$ and $|B| \geqslant |A|/2$. We first examine the multiplicative energy $E_\times(B)$. Note that

$$B \cdot B \subseteq \{(2m-1)2^n : m \leqslant 2N^{4/3} \text{ and } n \leqslant 2N^{1/3}\},$$

so that $|B \cdot B| \leqslant 4N^{5/3}$. We therefore deduce from Cauchy's inequality that

$$(N/2)^4 \leqslant |B|^4 = \Big(\sum_{x \in B \cdot B} r_{B \cdot B}(x) \Big)^2 \leqslant |B \cdot B| \sum_{x \in B \cdot B} r_{B \cdot B}(x)^2 \leqslant 4N^{5/3} E_\times(B),$$

whence $E_\times(B) \geq N^{7/3}/2^6$.

Our discussion of the corresponding additive energy $E_+(B)$ entails more effort. Here we view A as a union of arithmetic progressions. By showing that B must be dense on many of these progressions, we deduce that it has large additive energy. For a fixed natural number n, let

$$M_n = \{m \in \mathbb{N} : m \leqslant N^{2/3} \text{ and } (2m-1)2^n \in B\}.$$

Also, define

$$\mathcal{N} = \{n \in \mathbb{N} : |M_n| \geqslant \tfrac{1}{4}N^{2/3}\}.$$

Then it follows by means of an obvious averaging argument that

$$|\mathcal{N}| > \tfrac{1}{3}N^{1/3} + O(1).$$

Indeed, one has

$$\tfrac{1}{2}N + O(N^{2/3}) < |B| = \sum_{n\in\mathbb{N}} |M_n| \leqslant N^{2/3}|\mathcal{N}| + \tfrac{1}{4}N^{2/3}(N^{1/3} - |\mathcal{N}|),$$

from which the desired conclusion follows. Note also that for all natural numbers n, the sumset $M_n + M_n$ is a subset of the natural numbers not exceeding $2N^{2/3}$, and hence $|M_n + M_n| \leq 2N^{2/3}$. It therefore follows from Cauchy's inequality, much as before, that for any fixed $n \in \mathbb{N}$ we have

$$|M_n|^4 \leqslant |M_n + M_n|E_+(M_n),$$

and for $|M_n| \geqslant \frac{1}{4}N^{2/3}$ we arrive at the lower bound

$$E_+(M_n) \geqslant \left(\tfrac{1}{4}N^{2/3}\right)^4/(2N^{2/3}) = 2^{-9}N^2 \quad (n \in \mathcal{N}).$$

We thus conclude that

$$\begin{aligned} E_+(B) &\geqslant \sum_{n\in\mathcal{N}} \operatorname{card}\bigg\{\mathbf{m} \in M_n^4 : \sum_{i=1}^{4}(-1)^{i-1}(2m_i - 1)2^n = 0\bigg\} \\ &= \sum_{n\in\mathcal{N}} E_+(M_n) \geqslant \tfrac{1}{3}2^{-9}N^{7/3} + O(N^2). \end{aligned}$$

By combining these conclusions, we see that when $B \subseteq A$ and $|B| \geqslant |A|/2$, then one necessarily has both of the lower bounds (2.1), confirming our opening claim. In particular, whenever $\beta < \frac{1}{3}$, there exist arbitrarily large finite subsets A of $\mathbb{R}$ for which, for some positive number ε, every decomposition into two parts B and C satisfies the lower bound $\max\{E_+(B), E_\times(C)\} \gg |A|^{2+\beta+\varepsilon}$. Consequently, the infimum κ of all permissible low-energy decomposition exponents satisfies $\kappa \geqslant \frac{1}{3}$. This completes our proof of Theorem 1.2.

3. Low-energy decompositions

Our goal in this section is the proof of the low-energy decomposition theorem recorded in Theorem 1.1. The key ingredient in our proof of the latter is a version of the Balog-Szemerédi-Gowers lemma, which gives a quantitative version of the assertion that when $E_+(B)$ is large, then there exists a large subset A' of B for which $|A' + A'|$ is small (see [1, Theorem 2]). In order to extract the sharpest accessible conclusion, we apply the Balog-Szemerédi-Gowers lemma in the form given by Schoen (see [10, Theorem 1.2]).

Lemma 3.1. *Let B be a non-empty finite subset of an abelian group with $E_+(B) = \alpha|B|^3$. Then there exist subsets A' and B' of B such that*

$$\min\{|A'|, |B'|\} \gg \alpha^{3/4}\left(\log(2/\alpha)\right)^{-5/4}|B|$$

and

$$|A' - B'| \ll \alpha^{-7/2} \left(\log(2/\alpha)\right)^{5/2} \left(|A'||B'|\right)^{1/2}.$$

Here, the implicit constants are independent of the abelian group in question.

In order to proceed further, we must modify the conclusion of this lemma so that it supplies a bound for $|A' + A'|$. This we achieve through a consequence of Plünnecke's inequality.

Lemma 3.2. *Let A and B be non-empty finite subsets of an abelian group. Then we have $|A + A| \leq |A + B|^2/|B|$.*

Proof. This is a direct consequence of Plünnecke's inequality. See, for example, the case $k = 2$ of [12, Corollary 6.28]. We note that a new, simpler proof of Plünnecke's inequality has recently been given by Petridis [6, Theorem 1.1]. □

By combining Lemmata 3.1 and 3.2, we obtain a version of the Balog-Szemerédi-Gowers lemma suitable for our application.

Lemma 3.3. *Let G be an abelian group. Then there are positive constants c_1 and c_2, independent of G, with the following property. Suppose that N is a sufficiently large natural number. Let B be a non-empty finite subset of G with $|B| \leqslant N$, and suppose that δ and θ are real numbers with $0 < \delta < 1$. Then, either $E_+(B) \leqslant N^{3-\delta}(\log N)^\theta$, or else there exists a subset A' of B such that*

$$|A'| \geqslant c_1 N^{1-3\delta/4} (\log N)^{(3\theta-5)/4} \quad \textit{and} \quad |A' + A'| \leqslant c_2 N^{7\delta} (\log N)^{5-7\theta} |A'|.$$

Proof. Suppose that B, δ and θ satisfy the hypotheses of the statement of the lemma. If $E_+(B) \leqslant N^{3-\delta}(\log N)^\theta$, then there is nothing to prove, so we may suppose that $E_+(B) > N^{3-\delta}(\log N)^\theta$. Put $\alpha = E_+(B)/|B|^3$. Then we have

$$\alpha > N^{3-\delta}(\log N)^\theta/|B|^3 \geqslant N^{-\delta}(\log N)^\theta,$$

and we deduce from Lemma 3.1 that there exist subsets A' and B' of B with

$$\begin{aligned} \min\{|A'|, |B'|\} &\gg \left(N^{3-\delta}(\log N)^\theta/|B|^3\right)^{3/4} (\log N)^{-5/4} |B| \\ &\gg N^{1-3\delta/4} (\log N)^{(3\theta-5)/4} \end{aligned}$$

and

$$|A' - B'| \ll \alpha^{-7/2} \left(\log(1/\alpha)\right)^{5/2} \left(|A'||B'|\right)^{1/2}.$$

However, Lemma 3.2 leads from the latter bound to the relation

$$|A' + A'| \leqslant |A' - B'|^2/|B'| \ll \alpha^{-7} \left(\log(1/\alpha)\right)^5 |A'| \ll N^{7\delta} (\log N)^{5-7\theta} |A'|.$$

The conclusion of the lemma now follows. □

We also need the fact that the multiplicative energy between two sets exhibits some subadditive behaviour. This is folklore, and follows as a simple consequence of Cauchy's inequality.

Lemma 3.4. *Let A_j $(1 \leqslant j \leqslant J)$ and B_k $(1 \leqslant k \leqslant K)$ be finite subsets of a ring. Then one has*

$$E_\times\Big(\bigcup_{j=1}^{J} A_j, \bigcup_{k=1}^{K} B_k\Big) \leqslant JK \sum_{j=1}^{J}\sum_{k=1}^{K} E_\times(A_j, B_k).$$

Finally, we recall a generalisation of the key ingredient of Solymosi [11] in proving his sum-product estimate.

Lemma 3.5. *Let A and B be non-empty finite subsets of the real numbers. Then*

$$E_\times(A,B) \ll |A+A| \cdot |B+B| \lceil \log(\min\{|A|,|B|\})\rceil.$$

Proof. The desired conclusion follows from [5, Theorem 6]. □

We are now equipped for the main act of this section.

The proof of Theorem 1.1. Let δ and θ be parameters with $0 < \delta < 1$ to be fixed in due course, and let c_1 and c_2 be the positive constants whose existence is guaranteed via Lemma 3.3. We consider a subset A of the real numbers with $|A| = N$, where N is a sufficiently large natural number. We prove first that there exist disjoint subsets B and C of A, with $A = B \cup C$ and

$$\max\{E_+(B), E_\times(C)\} \ll |A|^{3-\delta}(\log|A|)^\theta. \tag{3.1}$$

Should one have $E_+(A) \leqslant N^{3-\delta}(\log N)^\theta$, then $A = A \cup \emptyset$ is trivially a decomposition of the type we seek, and so we may suppose henceforth that $E_+(A) > N^{3-\delta}(\log N)^\theta$. We now proceed inductively to define certain subsets A_j of A for $1 \leqslant j \leqslant K$, for a suitable integer K. Suppose that $k \geqslant 0$ and that the first k of these sets have been defined. We put

$$C_k = \bigcup_{j=1}^{k} A_j \quad \text{and} \quad B_k = A \setminus C_k. \tag{3.2}$$

Should $E_+(B_k) \leqslant N^{3-\delta}(\log N)^\theta$, then we set $K = k$ and stop. Otherwise, we define the set A_{k+1} as follows. We may suppose that $E_+(B_k) > N^{3-\delta}(\log N)^\theta$, and so it follows from Lemma 3.3 that there exists $A_{k+1} \subseteq B_k \subseteq A$ such that

$$|A_{k+1}| \geqslant c_1 N^{1-3\delta/4}(\log N)^{(3\theta-5)/4}$$

and

$$|A_{k+1} + A_{k+1}| \leqslant c_2 N^{7\delta}(\log N)^{5-7\theta}|A_{k+1}|. \tag{3.3}$$

Having defined the set A_{k+1}, we may define B_{k+1} and C_{k+1} according to (3.2), and repeat this decomposition argument.

The iteration described in the last paragraph must terminate for a value of K satisfying $K \leqslant K_0$, where $K_0 = \lfloor c_1^{-1} N^{3\delta/4}(\log N)^{(5-3\theta)/4}\rfloor$. For

$$|B_k| = |A| - \sum_{j=1}^{k} |A_j| \leqslant N - kc_1 N^{1-3\delta/4}(\log N)^{(3\theta-5)/4},$$

whence B_{K_0} (if it exists) must satisfy $|B_{K_0}| \leqslant c_1 N^{1-3\delta/4}(\log N)^{(3\theta-5)/4}$. In such circumstances, a trivial estimate yields the bound

$$E_+(B_{K_0}) \leqslant \big(c_1 N^{1-3\delta/4}(\log N)^{(3\theta-5)/4}\big)^3 \leqslant N^{3-\delta},$$

and our iteration stops.

Now equipped with the sets $A_1, \dots, A_K$ defined by this iterative process, we ease our exposition by abbreviating B_K to B and C_K to C. Note that A is the disjoint union of B and C. The first observation is that a defining feature of our iteration is the bound $E_+(B) \leqslant N^{3-\delta}(\log N)^\theta$. In the first instance, the application of Lemmata 3.4 and 3.5 yields the bound

$$\begin{aligned} E_\times(C) = E_\times(C,C) &\leqslant K_0^2 \sum_{i,j} E_\times(A_i, A_j) \\ &\ll K_0^2 \log N \bigg(\sum_i |A_i + A_i| \bigg)^2. \end{aligned}$$

Consequently, on applying the property (3.3) of these subsets A_i, we infer that

$$E_\times(C) \ll K_0^2 N^{14\delta} (\log N)^{11-14\theta} \bigg(\sum_i |A_i| \bigg)^2.$$

Moreover, it is apparent that $\sum_i |A_i| = |C| \leqslant N$. Thus we deduce that

$$\begin{aligned} E_\times(C) &\ll N^{2+14\delta}(\log N)^{11-14\theta} \Big(N^{3\delta/4}(\log N)^{(5-3\theta)/4} \Big)^2 \\ &\ll N^{2+31\delta/2}(\log N)^{(27-31\theta)/2}. \end{aligned}$$

We now set $3-\delta = 2+31\delta/2$ and $\theta = (27-31\theta)/2$, which is to say $\delta = \frac{2}{33}$ and $\theta = \frac{9}{11}$, and conclude that

$$E_+(B) \leqslant N^{3-\delta}(\log N)^\theta \quad \text{and} \quad E_\times(C) \ll N^{3-\delta}(\log N)^\theta. \tag{3.4}$$

Since $N = |A|$, this confirms the relations (3.1). In order to complete the proof of Theorem 1.1, it now remains only to establish that

$$\max\{E_+(B,C), E_\times(B,C)\} \ll N^{3-\delta/2}(\log N)^{\theta/2}.$$

But rewriting the energy between the sets B and C in the form

$$E_+(B,C) = \sum_{x \in B+C} r_{B+C}(x)^2 = \sum_{y \in (B-B)\cap(C-C)} r_{B-B}(y) r_{C-C}(y),$$

we infer from Cauchy's inequality that

$$\begin{aligned} E_+(B,C) &\leqslant \bigg(\sum_{y \in B-B} r_{B-B}(y)^2 \bigg)^{1/2} \bigg(\sum_{y \in C-C} r_{C-C}(y)^2 \bigg)^{1/2} \\ &= E_+(B)^{1/2} E_+(C)^{1/2}. \end{aligned}$$

Thus we conclude from (3.4) and the trivial estimate $E_+(C) \ll N^3$ that

$$E_+(B,C) \ll \big(N^{3-\delta}(\log N)^\theta\big)^{1/2} (N^3)^{1/2} \ll N^{3-\delta/2}(\log N)^{\theta/2}.$$

By an entirely analogous argument, one finds also that

$$E_\times(B,C) \ll N^{3-\delta/2}(\log N)^{\theta/2}.$$

This completes the proof of the final claim of Theorem 1.1. □

4. Low-energy decompositions in finite fields

The strategy prosecuted in §3 may be adapted without serious difficulty to the setting of finite fields $\mathbb{F}_p$, with p prime. The only ingredient which requires serious modification is Lemma 3.5, which bounds the multiplicative energy of a set in terms of its sumset. One approach to handling this difficulty is by appeal to work of Bourgain [2] and Rudnev [8].

Lemma 4.1. *Suppose that $A \subset \mathbb{F}_p$. Then*

$$E_\times(A) \ll |A+A|^{9/4}|A|^{1/2} + p^{-1/4}|A+A|^2|A|^{5/4}.$$

Moreover, provided that $|A| < \sqrt{p}$, one has the sharper bound

$$E_\times(A) \ll |A+A|^{7/4}|A|\lceil \log |A| \rceil.$$

Proof. The first bound on the multiplicative energy contained in this lemma is simply [2, Proposition 1], whilst the second is essentially [8, equation (3.22)]. □

By following the path described in §3 leading to the proof of Theorem 1.1, the reader will have little difficulty in obtaining the conclusion recorded in the following theorem.

Theorem 4.2. *Let p be a large prime, and suppose that $A \subseteq \mathbb{F}_p$ satisfies $|A| < \sqrt{p}$. Then, with $\delta = 4/227$, there exist disjoint subsets B and C of A, with $A = B \cup C$ and*

$$\max\{E_+(B), E_\times(C)\} \ll |A|^{3-\delta}(\log |A|)^{1+\delta/2}.$$

When $|A| \geqslant \sqrt{p}$, then with $\delta = 4/283$ and $\theta = 223/249$, one has instead

$$\max\{E_+(B), E_\times(C)\} \ll |A|^3(|A|/p)^\delta(\log |A|)^\theta.$$

Instead, we follow an alternative strategy in which the roles of addition and multiplication in our previous argument are interchanged. We begin by recording an appropriate analogue of Lemma 3.3.

Lemma 4.3. *There are positive constants c_1 and c_2 with the following property. Let p be a prime number. Suppose that N is a sufficiently large natural number. Let B be a non-empty finite subset of $\mathbb{F}_p$ with $|B| \leqslant N$, and suppose that δ and θ are real numbers with $0 < \delta < 1$. Then, either $E_\times(B) \leqslant 2N^{3-\delta}(\log N)^\theta$, or else there exists a subset A' of B such that*

$$|A'| \geqslant c_1 N^{1-3\delta/4}(\log N)^{(3\theta-5)/4} \quad \text{and} \quad |A' \cdot A'| \leqslant c_2 N^{7\delta}(\log N)^{5-7\theta}|A'|.$$

Proof. Let $g \in \mathbb{F}_p^\times$ be a primitive root, and put

$$I = \{r \in [1, p-1] : g^r \in B\}.$$

Taking account of the possibility that $0 \in B$, we see that

$$E_\times(B) \leqslant E_+(I) + 4|B|^2.$$

Consequently, if $E_\times(B) > 2N^{3-\delta}(\log N)^\theta$, then $E_+(I) > N^{3-\delta}(\log N)^\theta$. We therefore deduce from Lemma 3.3 that there exists a subset I' of I such that

$$|I'| \geqslant c_1 N^{1-3\delta/4}(\log N)^{(3\theta-5)/4} \quad \text{and} \quad |I'+I'| \leqslant c_2 N^{7\delta}(\log N)^{5-7\theta}|I'|.$$

Putting $A' = \{g^r : r \in I'\}$, the conclusion of the lemma follows. □

An appropriate analogue of Lemma 3.4 follows by applying Cauchy's inequality, just as before.

Lemma 4.4. *Let A_j $(1 \leqslant j \leqslant J)$ be finite subsets of a ring. Then one has*

$$E_+\Big(\bigcup_{j=1}^J A_j\Big) \leqslant J^3 \sum_{j=1}^J E_+(A_j).$$

Finally, before extracting a relation between the additive energy of a set and its corresponding product set, we recall a consequence of a lemma from recent work of Roche-Newton, Rudnev and Shkredov [7] that has its origins in a paper of Rudnev [9] concerning incidences between planes and points in three dimensions.

Lemma 4.5. *Let $A, B, C \subseteq \mathbb{F}_p$. Suppose that $|A||B||B \cdot C| \leqslant p^2$. Then*

$$E_+(A,C) \ll (|A||B \cdot C|)^{3/2}\,|B|^{-1/2} + |A||B \cdot C||B|^{-1}\max\{|A|, |B \cdot C|\}. \quad (4.1)$$

Proof. This is an immediate consequence of [7, Theorem 6]. □

We extract from this lemma upper bounds for $E_+(A)$ suitable for our subsequent applications.

Lemma 4.6. *Suppose that $A \subset \mathbb{F}_p$. Then*

$$E_+(A) \ll |A \cdot A|^{3/2}|A| + p^{-1}|A \cdot A|^2|A|^2.$$

Proof. Provided that $|A|^2|A \cdot A| \leqslant p^2$, the desired conclusion follows by applying Lemma 4.5 with $B = C = A$. We have only to note that $|A \cdot A| \leqslant |A|^2$, so that the second term on the right hand side of (4.1) is majorised by the first.

Suppose next that $|A|^2|A \cdot A| > p^2$. Put

$$n = \left\lfloor \frac{p^2}{|A||A \cdot A|} \right\rfloor.$$

Since $|A| \leqslant p$ and $|A \cdot A| \leqslant p$, we may suppose that $1 \leqslant n < |A|$. We take B to be any subset of A having n elements. Then we have $|A||A \cdot A||B| \leqslant p^2$. By applying Lemma 4.5 with $C = A$, we find that

$$E_+(A) \ll (|A||A \cdot B|)^{3/2}\,|B|^{-1/2} + |A||A \cdot B||B|^{-1}\max\{|A|, |A \cdot B|\}.$$

But since $B \subseteq A$, one has $A \cdot B \subseteq A \cdot A$, and hence

$$|A| \leqslant |A \cdot B| \leqslant |A \cdot A| \leqslant p.$$

Moreover, since $|B|^{-1} = n^{-1} \ll |A||A \cdot A|p^{-2}$, we obtain

$$\begin{aligned} E_+(A) &\ll (|A||A \cdot A|)^{3/2} \left(|A||A \cdot A|p^{-2}\right)^{1/2} + |A||A \cdot A|^2 \left(|A||A \cdot A|p^{-2}\right) \\ &\ll |A|^2|A \cdot A|^2p^{-1}. \end{aligned}$$

This completes the proof of the lemma. □

We now outline the proof of our low-energy decomposition theorem over $\mathbb{F}_p$.

The proof of Theorem 1.3. We proceed precisely as in the proof of Theorem 1.1, save that the roles of addition and multiplication are interchanged. For the sake of concision, we are expedient in implicity employing the appropriate analogue of all notation used therein. However, we provide essentially complete details of the argument. In the current situation, should one have $E_\times(A) \leqslant 2N^{3-\delta}(\log N)^\theta$, then $A = \emptyset \cup A$ is trivially a decomposition of the type we seek, and so we may suppose henceforth that $E_\times(A) > 2N^{3-\delta}(\log N)^\theta$. We proceed inductively to define subsets A_j of A for $1 \leqslant j \leqslant K$, for a suitable integer K. Suppose that $k \geqslant 0$ and that the first k of these sets have been defined. Put

$$B_k = \bigcup_{j=1}^{k} A_j \quad \text{and} \quad C_k = A \setminus B_k. \tag{4.2}$$

Should $E_\times(C_k) \leqslant 2N^{3-\delta}(\log N)^\theta$, then we set $K = k$ and stop. Otherwise, we define the set A_{k+1} as follows. We may suppose that $E_\times(C_k) > 2N^{3-\delta}(\log N)^\theta$, and so it follows from Lemma 4.3 that there exists $A_{k+1} \subseteq C_k \subseteq A$ such that

$$|A_{k+1}| \geqslant c_1 N^{1-3\delta/4}(\log N)^{(3\theta-5)/4} \tag{4.3}$$

and

$$|A_{k+1} \cdot A_{k+1}| \leqslant c_2 N^{7\delta}(\log N)^{5-7\theta}|A_{k+1}|. \tag{4.4}$$

Having defined the set A_{k+1}, we may define B_{k+1} and C_{k+1} according to (4.2), and repeat this decomposition argument.

As in the corresponding proof of Theorem 1.1 in §3, the iteration defined in the last paragraph must terminate for some $K \leqslant \lfloor c_1^{-1} N^{3\delta/4}(\log N)^{(5-3\theta)/4} \rfloor$. We again put $B = B_K$ and $C = C_K$, and note that A is the disjoint union of B and C. In particular, we now have $E_\times(C) \leqslant 2N^{3-\delta}(\log N)^\theta$. We group the subsets A_j by cardinality, taking $\mathfrak{A}_m$ to be the union of those subsets A_j for which $2^{-m}N < |A_j| \leqslant 2^{1-m}N$. Notice that cardinality constraints ensure that each set $\mathfrak{A}_m$ consists of no more than 2^m of the subsets A_j, and, moreover, one has $m = O(\log N)$. The application of Lemma 4.4 leads to the estimate

$$E_+(B) \ll (\log N)^3 \sum_k E_+(\mathfrak{A}_k) \ll (\log N)^3 \sum_k \sum_{A_i \subseteq \mathfrak{A}_k} 2^{3k} E_+(A_i).$$

By applying Lemma 4.6, we obtain the bound

$$E_+(B) \ll (\log N)^3 \sum_k \sum_{A_i \subseteq \mathfrak{A}_k} 2^{3k} \left(|A_i \cdot A_i|^{3/2}|A_i| + p^{-1}|A_i \cdot A_i|^2|A_i|^2\right).$$

Next, on applying the property (4.4) of these subsets A_i, we infer that

$$E_+(B) \ll \big(N^\delta (\log N)^{1-\theta}\big)^{21/2} \sum_k 2^{3k} \sum_{A_i \subseteq \mathfrak{A}_k} \Big(|A_i|^5 + p^{-2} N^{7\delta} (\log N)^{5-7\theta} |A_i|^8 \Big)^{1/2}.$$

But the property (4.3) of the subsets $A_i \subseteq \mathfrak{A}_k$ ensures that the inner sum here is empty whenever

$$2^{1-k} N < c_1 N^{1-3\delta/4} (\log N)^{(3\theta-5)/4}. \tag{4.5}$$

Moreover, it is apparent that for each k one has

$$\sum_{A_i \subseteq \mathfrak{A}_k} |A_i| \leqslant N.$$

Note also that the definition of $\mathfrak{A}_k$ ensures that when $A_i \subseteq \mathfrak{A}_k$, then one has $2^k |A_i| \leqslant 2N$. Thus we deduce that

$$\begin{aligned} E_+(B) &\ll N^{(3+21\delta)/2} (\log N)^{21(1-\theta)/2} \big(N^{3\delta/4} (\log N)^{(5-3\theta)/4} \big)^{3/2} N \\ &\qquad + p^{-1} N^{3+14\delta} (\log N)^{13-14\theta} N \log N \\ &\ll \big(N^{20+93\delta} (\log N)^{99-93\theta} \big)^{1/8} + p^{-1} N^{4+14\delta} (\log N)^{14(1-\theta)}. \end{aligned} \tag{4.6}$$

Recall the definitions of α and β from the statement of Theorem 1.3. We take ω and ν to be any real numbers with $p = \frac{1}{10} N^\omega (\log N)^\nu$. In the first instance, we constrain our choices of δ and θ to satisfy the inequalities

$$\delta \leqslant \frac{8\omega - 12}{19} \quad \text{and} \quad \theta \geqslant \frac{13 - 8\nu}{19}. \tag{4.7}$$

In such circumstances, one finds that it is the first term on the right hand side of (4.6) that dominates. We consequently define δ and θ by means of the equations $8(3-\delta) = 20 + 93\delta$ and $8\theta = 99 - 93\theta$, which is to say that $\delta = 4/101$, and $\theta = 99/101$. These choices for δ and θ satisfy the constraint (4.7) provided that

$$\omega \geqslant \frac{19\delta + 12}{8} = \frac{161}{101} \quad \text{and} \quad \nu \geqslant \frac{13 - 19\theta}{8} = -\frac{71}{101},$$

and this may be assured when $p \geqslant \frac{1}{10} N^{1/\alpha} (\log N)^{-\beta/\alpha}$. This latter constraint is satisfied when $N \leqslant p^\alpha (\log p)^\beta$. Under the latter condition, therefore, we obtain the bound

$$\max\{E_+(B), E_\times(C)\} \ll N^{3-\delta} (\log N)^{1-\delta/2}.$$

Since $N = |A|$, this confirms the first conclusion of Theorem 1.3.

We next take ω and ν to be any real numbers with $p = 10 N^\omega (\log N)^\nu$. In this second instance, we constrain our choices of δ and θ to satisfy the inequalities

$$\delta \geqslant \frac{8\omega - 12}{19} \quad \text{and} \quad \theta \leqslant \frac{13 - 8\nu}{19}. \tag{4.8}$$

In such circumstances, one finds that it is the second term on the right hand side of (4.6) that dominates. We consequently define δ and θ by means of the equations $3 - \delta = 4 + 14\delta - \omega$ and $\theta = 14(1-\theta) - \nu$, which is to say that

$\delta = (\omega - 1)/15$ and $\theta = (14 - \nu)/15$. These choices for δ and θ satisfy the constraint (4.8) provided that

$$\omega \leqslant \frac{19\delta + 12}{8} = \frac{19\omega + 161}{120} \quad \text{and} \quad \nu \leqslant \frac{13 - 19\theta}{8} = \frac{19\nu - 71}{120}.$$

These conditions are satisfied provided that

$$\omega \leqslant \frac{161}{101} \quad \text{and} \quad \nu \leqslant -\frac{71}{101},$$

and this may be assured when $p \leqslant 10N^{1/\alpha}(\log N)^{-\beta/\alpha}$. This latter constraint is satisfied when $N \geqslant p^\alpha(\log p)^\beta$. Under the latter condition, therefore, we obtain the bound

$$\max\{E_+(B), E_\times(C)\} \ll N^{3-\delta}(\log N)^\theta = N^3(N/p)^{1/15}(\log N)^{14/15}.$$

Since $N = |A|$, this confirms the second conclusion of Theorem 1.3, and completes the proof of Theorem 1.3. □

We finish this section by confirming the lower bounds (1.3) presented following Theorem 1.3. This is a simple exercise in exponential sums over finite fields, in which we employ the standard notation $e_p(x) = e^{2\pi ix/p}$. When $B, C \subseteq \mathbb{F}_p$, write

$$f(u) = \sum_{b \in B} e_p(ub) \quad \text{and} \quad g(u) = \sum_{c_1, c_2 \in C} e_p(uc_1c_2).$$

Then, by orthogonality, one finds that

$$E_+(B) = p^{-1} \sum_{u=0}^{p-1} |f(u)|^4 \quad \text{and} \quad E_\times(C) = p^{-1} \sum_{u=0}^{p-1} |g(u)|^2.$$

Using positivity, and discarding all terms in each sum save for that with $u = 0$, we thus conclude that

$$E_+(B) \geqslant p^{-1} f(0)^4 = p^{-1}|B|^4 \quad \text{and} \quad E_\times(C) \geqslant p^{-1} g(0)^2 = p^{-1}|C|^4.$$

Of course, analogous arguments apply when $\mathbb{F}_p$ is replaced by any group of finite order. The argument we have employed has the merit of indicating that if the lower bound is achieved, then both $f(u)$ and $g(u)$ must be zero for $u \neq 0$. A proof free of Fourier analysis may be obtained by applying Cauchy's inequality. Thus, for example, one has

$$E_+(B) = \sum_{m=0}^{p-1} r_{B+B}(m)^2 \geqslant p^{-1} \Big(\sum_{m=0}^{p-1} r_{B+B}(m) \Big)^2 = p^{-1}|B|^4,$$

and a similar argument applies to show that $E_\times(C) \geqslant p^{-1}|C|^4$. This confirms the desired lower bounds.

5. Higher order energies

We finish our account of low-energy decomposition theorems with a brief discussion of higher order energies, and in particular the proof of Theorem 1.4. With $\mathbf{b}$ as shorthand for $(b_3, \dots, b_k)$, write

$$T(\mathbf{a}, \mathbf{a}') = \mathrm{card}\{(a_1, a_2), (a_1', a_2') \in A_1 \times A_2 : a_1 + \cdots + a_k = a_1' + \cdots + a_k'\}.$$

For $k \geq 2$, one obtains cheap bounds on the k-fold additive energy between sets $A_1, \dots, A_k$ by means of the relation

$$\begin{aligned} E_+(A_1, \dots, A_k) &= \sum_{\mathbf{a},\mathbf{a}' \in A_3 \times \dots \times A_k} T(\mathbf{a}, \mathbf{a}') \\ &\leqslant |A_3|^2 \cdots |A_k|^2 \max_b U(b), \end{aligned}$$

where we write

$$U(b) = \mathrm{card}\{(a_1, a_2), (a_1', a_2') \in A_1 \times A_2 : a_1 + a_2 + b = a_1' + a_2'\}.$$

By Cauchy's inequality, for any fixed value of b, one has

$$\begin{aligned} U(b) &= \sum_{x \in A_1 + A_2} r_{A_1+A_2}(x-b) r_{A_1+A_2}(x) \\ &\leqslant \Big(\sum_{x \in A_1 + A_2 - b} r_{A_1+A_2}(x)^2 \Big)^{1/2} \Big(\sum_{x \in A_1 + A_2} r_{A_1+A_2}(x)^2 \Big)^{1/2} \\ &\leqslant E_+(A_1, A_2). \end{aligned}$$

Thus we obtain the bound

$$E_+(A_1, \dots, A_k) \leqslant |A_3|^2 \cdots |A_k|^2 E_+(A_1, A_2).$$

An entirely analogous argument coughs up the corresponding bound

$$E_\times(A_1, \dots, A_k) \leqslant |A_3|^2 \cdots |A_k|^2 E_\times(A_1, A_2).$$

Given a finite subset A of the real numbers, consider positive integers m and n with $m \geqslant 2$ and $n \geqslant 2$. With $\delta = \frac{2}{33}$, it follows from Theorem 1.1 that there exist disjoint subsets B and C of A, with $A = B \cup C$, and

$$\max\{E_+(B), E_\times(C)\} \ll |A|^{3-\delta} (\log |A|)^{1-\delta}.$$

Using these same subsets B and C, it follows from our opening discussion in this section that

$$E_+^{(m)}(B) \leqslant |A|^{2m-4} E_+(B) \ll |A|^{2m-1-\delta} (\log |A|)^{1-\delta},$$

and likewise

$$E_\times^{(n)}(C) \leqslant |A|^{2n-4} E_\times(B) \ll |A|^{2n-1-\delta} (\log |A|)^{1-\delta}.$$

This completes the proof of Theorem 1.4.

Notice that in our proof of Theorem 1.4, the decomposition of A into the sets B and C does not depend on m and n. We have deliberately avoided stating Theorem 1.4 with such dependence suppressed, however, in order to stress that the central interest is in obtaining the sharpest permissible exponents.

6. Hanson's estimate

We illustrate the application of conclusions of the type described in Theorem 1.3 by considering inexpensive consequences of such estimates for results of Hanson's type for the quantity $H_\chi(A,B,C,D)$ defined in (1.4). We suppose that a conclusion of the same shape as that of Theorem 1.3 is available in which the exponent $4/101$ is replaced by a certain positive number δ_0 with $0<\delta_0<1$. Thus, we may suppose that for any positive number δ with $\delta<\delta_0$, there exist disjoint subsets C_+ and $C_\times$ of C, satisfying $C=C_+\cup C_\times$, and satisfying the conditions

$$E_+(C_+)\ll |C|^{3-\delta} \quad \text{and} \quad E_\times(C_\times)\ll |C|^{3-\delta}. \tag{6.1}$$

We develop estimates for $H_\chi(A,B,C,D)$ following the path of Hanson [4], with some simplifications. Suppose that δ is a permissible decomposition exponent in the context of (6.1). Our goal is to show that when $0<\tau<\delta/(8+2\delta)$, there is a positive number $\omega=\omega(\delta,\tau)$ for which, whenever A, B, C and D are subsets of $\mathbb{F}_p$ each containing at least $p^{1/2-\tau}$ elements, then

$$H_\chi(A,B,C,D)\ll p^{-\omega}|A||B||C||D|. \tag{6.2}$$

In particular, there is non-trivial cancellation in the character sum

$$\sum_{a\in A}\sum_{b\in B}\sum_{c\in C}\sum_{d\in D}\chi\left(a+b+cd\right).$$

We note that our methods avoid reference to Weil's bounds for character sums.

We begin with a lemma that makes use of little more than orthogonality. Here we temporarily make use of the intuitively transparent convention that when B and C are subsets of $\mathbb{F}_p$, and $b\in B$ and $c\in C$, then $b\times c=bc$ and $B\times C=B\cdot C$.

Lemma 6.1. *When $A,B,C,D\subseteq\mathbb{F}_p$, and χ is a non-trivial character, we have*

$$\Big|\sum_{a\in A}\sum_{b\in B}\sum_{c\in C}\chi(a+b\circ c)\Big|^2\leqslant (p-|A|)|A|E_\circ(B,C)\quad(\circ\in\{+,\times\}).$$

Proof. Let $\circ$ be one of $+$ and $\times$. Then, we find via Cauchy's inequality that

$$\begin{aligned}\Big|\sum_{a\in A}\sum_{b\in B}\sum_{c\in C}\chi(a+b\circ c)\Big|^2&=\Big|\sum_{x\in\mathbb{F}_p}\sum_{a\in A}r_{B\circ C}(x)\chi(a+x)\Big|^2\\&\leqslant\Big(\sum_{x\in\mathbb{F}_p}r_{B\circ C}(x)^2\Big)\sum_{x\in\mathbb{F}_p}\Big|\sum_{a\in A}\chi(a+x)\Big|^2\\&=E_\circ(B,C)\sum_{a,a'\in A}\Upsilon(a,a'),\end{aligned}$$

where

$$\Upsilon(a,a')=\sum_{y\in\mathbb{F}_p}\overline{\chi}(y)\chi(y+a-a')=\begin{cases}p-1, & \text{when } a=a',\\ -1 & \text{when } a\neq a'.\end{cases}$$

The proof of the lemma is completed by noting that

$$\sum_{a,a' \in A} \Upsilon(a,a') = (p-1)|A| - |A|(|A|-1).$$

□

We begin our proof of (6.2) by noting that there is no loss of generality in supposing that $0 \notin D$. After all, were this not the case, then a trivial estimate for the contribution to $H_\chi(A,B,C,D)$ arising from the element 0 in D is $|A||B||C| = o(p^{-\omega}|A||B||C||D|)$. Next, applying the decomposition $C = C_+ \cup C_\times$ in combination with Lemma 6.1, one sees that $H_\chi(A,B,C,D)$ is bounded above by

$$\begin{aligned}&\sum_{a\in A}\Big|\sum_{u\in a+B}\sum_{c\in C_\times}\sum_{d\in D}\chi(u+cd)\Big| + \sum_{d\in D}\Big|\sum_{a\in A}\sum_{b\in B}\sum_{v\in dC_+}\chi(a+b+v)\Big|\\ &\leqslant \sum_{a\in A}\sqrt{p|a+B|E_\times(C_\times,D)} + \sum_{d\in D}\sqrt{p|A|E_+(B,dC_+)}.\end{aligned}$$

Thus we deduce via (6.1) that $H_\chi(A,B,C,D)$ is bounded above by

$$\begin{aligned}&p^{1/2}\big(|A||B|^{1/2}E_\times(C_\times)^{1/4}E_\times(D)^{1/4} + |D||A|^{1/2}E_+(B)^{1/4}E_+(C_+)^{1/4}\big)\\ &\ll p^{1/2}\big(|A||B|^{1/2}|C|^{(3-\delta)/4}|D|^{3/4} + |A|^{1/2}|B|^{3/4}|C|^{(3-\delta)/4}|D|\big).\end{aligned}$$

It therefore follows that

$$\frac{H_\chi(A,B,C,D)}{|A||B||C||D|} \ll \max\left\{\left(\frac{p^2}{|B|^2|C|^{1+\delta}|D|}\right)^{1/4}, \left(\frac{p^2}{|A|^2|B||C|^{1+\delta}}\right)^{1/4}\right\}. \quad (6.3)$$

Since, by hypothesis, we may suppose that $|A|$, $|B|$, $|C|$ and $|D|$ each exceed $p^{1/2-\tau}$, we find that (6.2) holds for a positive number ω, provided only that $(4+\delta)\big(\frac{1}{2}-\tau\big) > 2$, which is to say that $\tau < \delta/(8+2\delta)$. This completes our proof of the estimate (6.2) of Hanson type.

We note that versions of Theorem 1.3 may be obtained in which a low-energy decomposition is obtained in such a manner that additive and multiplicative energies are of differing orders of magnitude. Such asymmetrical decompositions offer the prospect of some improvement in the bound $\tau < \delta/(8+2\delta)$. There is also the option of decomposing both C and D, this offering the prospect of replacing the first term denominator $|C|^{1+\delta}|D|$ on the right hand side of (6.3) by $(|C||D|)^{1+\delta}$.

The symmetrical permissible exponent $\delta = 4/101$ that delivers Theorem 1.3 suffices to cheaply establish that any positive number τ not exceeding $1/204$ is permissible. We do not have a good guess as to the largest permissible value of δ in the decomposition (6.1), though if (in line with Theorem 1.2) one could take δ to be any positive number smaller than $2/3$, then it would follow already from the present cheap analysis that any exponent τ not exceeding $1/14$ would be permissible in the above discussion.

References

[1] A. Balog, *Many additive quadruplets*, Additive combinatorics, CRM Proc. Lecture Notes, 43, Amer. Math. Soc., Providence, RI, 2007, pp. 39–49.

[2] J. Bourgain, *Sum-product theorems and applications*, Additive number theory, Springer, New York, 2010, pp. 9–38.

[3] P. Erdős and E. Szemerédi, *On sums and products of integers*, Studies in pure mathematics, Birkhäuser, Basel, 1983, pp. 213–218.

[4] B. Hanson, *Estimates for character sums with various convolutions*, preprint, arXiv:1509.04354.

[5] S. V. Konyagin and I. D. Shkredov, *On sum sets of sets having small product set*, Proc. Steklov Inst. Math. **290** (2015), 288–299.

[6] G. Petridis, *New proofs of Plünnecke-type estimates for product sets in groups*, Combinatorica **32** (2012), no. 6, 721–733.

[7] O. Roche-Newton, M. Rudnev and I. D. Shkredov, *New sum-product type estimates over finite fields*, Adv. Math. **293** (2016), 589–605.

[8] M. Rudnev, *An improved sum-product inequality in finite fields of prime order*, Int. Math. Res. Not. (2012), no. 16, 3693–3705.

[9] M. Rudnev, *On the number of incidences between planes and points in three dimensions*, preprint, arXiv:1407.0426v3.

[10] T. Schoen, *New bounds in Balog-Szemerédi-Gowers theorem*, Combinatorica **35** (2015), no. 6, 695–701.

[11] J. Solymosi, *Bounding multiplicative energy by the sumset*, Advances in Math. **222** (2009), no. 2, 402–408.

[12] T. Tao and V. Vu, *Additive combinatorics*, Cambridge Studies in Advanced Mathematics, **105**, Cambridge University Press, Cambridge, 2006.

Alfréd Rényi Institute of Mathematics, Reáltanoda u. 13-15, H-1053 Budapest, Hungary.

E-mail address: balog@renyi.mta.hu

School of Mathematics, University of Bristol, University Walk, Clifton, Bristol BS8 1TW, United Kingdom

E-mail address: matdw@bristol.ac.uk