AN IMPROVED SUM-PRODUCT INEQUALITY IN FIELDS OF PRIME ORDER

MISHA RUDNEV

Abstract. This note proves the sum-product inequality

$$\max(|A \cdot A|, |A + A|) \gg |A|^{1 + \frac{1}{\log |A|}}$$

for sets of cardinality $|A| < \sqrt{p}$ in prime fields $\mathbb{F}_p$.

1. Introduction

Let $A$ be a subset of the multiplicative group $\mathbb{F}_p^*$ of the prime residue field $\mathbb{F}_p$ ($p$ is thought to be large, the constants throughout being independent of $p$). The sum set $A + A$ is defined as $\{a_1 + a_2 : a_1, a_2 \in A\}$; in the same fashion one defines the difference, product, and ratio sets $A - A, A \cdot A, A : A$, respectively.

The sum-product estimate of Bourgain, Katz, and Tao [2] and Konyagin [5] establishes that as long as $|A| < p^{1 - \Delta}$, one has

$$\max(|A + A|, |A \cdot A|) \geq c(\Delta) |A|^{1 + \delta(\Delta)},$$

for some $c(\Delta)$ and $\delta(\Delta) > 0$. In what follows, finite set cardinalities are denoted via $|\cdot|$, $c$ and $C$ denote some universal constants, changing from one place to another.

The next question, along the lines of the Erdős-Szemerédi conjecture for the integers, is to establish quantitative estimates as to the relation $\delta(\Delta)$. Clearly, there is no trivial sum-product estimate in the case $\Delta = 0$, i.e. when the size of $A$ is commensurate with the size of the whole field. Therefore, in order to get a uniform quantitative estimate, one should impose a restriction on the size of $A$, which is usually $|A| < \sqrt{p}$, i.e. $\Delta \geq \frac{1}{2}$, which is assumed further. (When $\Delta$ becomes smaller than $\frac{1}{2}$, calculations involving exponential sums start yielding non-trivial results, rather quickly, as $\Delta$ decreases, overpowering the combinatorial estimates that this and the majority of the quoted papers deal with. See e.g. [4]. The case $|A| > \sqrt{p}$ is no longer discussed in the sequel.)

Garaev [3] succeeded in obtaining the first quantitative sum-product estimate in $\mathbb{F}_p$: either the sum or the product set shall have cardinality $|A|^{1 + \frac{1}{14}}$, up to a multiple of a power of $c \log |A|$. Katz and Shen [6] elaborated on a particular application of the Plünnecke-Ruzsa inequality (cited here as Lemma [1]) in Garaev’s proof and improved $\frac{1}{14}$ to $\frac{1}{13}$. Bourgain and Garaev [11] incorporated a covering argument (whose variant, taken from [9], is cited here as Lemma [2]) and improved $\frac{1}{13}$ to $\frac{1}{12}$.

2000 Mathematics Subject Classification. 68R05, 11B75.
And Li ([7]) showed that a multiple of a power of $\log |A|$ can be done away with, so today’s state-of-the art, for $|A| < \sqrt{p}$ is that

$$\max(|A \cdot A|, |A + A|) \geq c|A|^{1 + \frac{1}{12}},$$

for some absolute $c$. Moreover, one can replace either one or both the product set $A \cdot A$ with the ratio set $A : A$ and the sum set $A + A$ with the difference set $A - A$.

On the heuristic level, the proof of the above series of results effectively begins with assuming that the multiplicative energy of $A$ is large, which follows from the assumption that the product set (or the ratio set) is small. Then one chooses a “popular” dyadic interval, with approximately constant number of points of $A \times A$ on the lines through the origin in $\mathbb{F}_p \times \mathbb{F}_p$, corresponding to different ratios. The decision on the meaning of “popular” can be postponed to the end of the proof and depend on what the final estimates are. This fact that the notion of “popularity” could be adjusted to the final estimates, rather specified this in the “natural” way in the beginning of the proof was the observation due to Li ([7]), which enabled him to get rid of the factor $\log |A|$ which permeated the results preceding his. Throughout the main body of the proof one uses the “standard” arithmetic combinatorics technique: Plünnecke-Ruzsa inequalities, covering lemmas and additive pivoting, which is roughly speaking estimating the size of $A + rA$ for some dilation $r$, in order to bring the sum or the difference set into play (as one wishes, since the choice of $A \pm A$ is allowed in both Plünnecke-Ruzsa inequalities and the Covering lemma).

The technical issues involved in the estimates used to improve Garaev’s original $\frac{1}{11}$ to $\frac{1}{12}$ have piled up, and this note offers yet another one, which enables to reduce “the worst possible scenario” estimating the size of $A + rA$ in the state-of-the-art literature, (that is this case “to blame” for the final answer $\frac{1}{12}$) to the “normal case” which would yield $\frac{1}{11}$, only if it were shown to be the only scenario.

This is done essentially via an application of the pigeonhole principle in Lemma 3 below which is used in the case study in the forthcoming proof.

The main result is as follows.

**Theorem 1.** Let $A \subset \mathbb{F}_p^*$ with $|A| < \sqrt{p}$ and $p$ bigger than some absolute constant. Then, for some absolute $c$,

$$\max(|A \cdot A|, |A + A|) \geq c|A|^{1 + \frac{1}{12}} \log^{\frac{1}{11}} |A|.$$
1.1. Acknowledgments. The author would like to thank L. Li and A. Glibichuk for their comments on the initial draft of this paper, as well as T. Jones and O. Roche-Newton for helping him to identify errors in his earlier attempts to prove Theorem 1.

2. Lemmata

This section contains the two arithmetic combinatorics lemmas used. The first one is a slight, but very useful generalisation of the Plünnecke-Ruzsa inequality (see [8]), which is due to Katz and Shen ([6]).

Lemma 1. Let $Y; X_1, \ldots X_k$ be additive sets. Then for any $0 < \varepsilon \leq 1$, there exists a subset $|Y'| \subseteq Y$, with $|Y'| \geq (1 - \varepsilon)|Y|$, and some constant $C(\varepsilon)$, such that

\begin{equation}
|Y' + X_1 + \ldots + X_k| \leq C(\varepsilon) \frac{\prod_{i=1}^{k}|Y + X_i|}{|Y|^{k-1}}.
\end{equation}

The second one is a covering lemma, see e.g. [1], [9], [7].

Lemma 2. Let $X_1$ and $X_2$ be additive sets. Then for any $\varepsilon \in (0, 1)$ and some constant $C(\varepsilon)$, there exist $\frac{C(\varepsilon)}{|X_2|} \min(|X_1 + X_2|, |X_1 - X_2|)$ translates of $X_2$, whose union contains not less than $(1 - \varepsilon)|X_1|$ elements of $X_1$.

3. Proof of Theorem 1

The proof goes essentially along the lines of the lately well-established approach, which in particular does not distinguish between the $A \pm A$, and applies as well to $A : A$, in which case it gets a little easier. If at the outset one deals with the product set, then the analysis begins by looking at the multiplicative energy whereupon it starts essentially dealing with ratios, rather than products. Throughout, one uses Lemmas 1 and 2 which admit any $\pm$ sign variation, and uses additive pivots $A + rA$, although it can be $A - rA$ instead. Hence, what follows is confined to the sum and the product sets only. Suppose both $|A + A| \leq K|A|$ and $|A \cdot A| \leq K|A|$, for some $K$.

First off, let us refine $A$, if necessary, so that the additive Plünnecke-Ruzsa inequality applies to $A$ in full power as follows:

\begin{equation}
|A + A + A + A| \ll K^3|A|.
\end{equation}

This will be used in the end of each of the Cases (i–iii) constituting the main body of the proof.

Indeed, if (3.1) did not apply to $A$, one would, by Lemma 1 choose a large subset $A'$ of $A$ (containing, say 90% of its elements) such that with $A'$ replacing $A$, the estimate (3.1) would be in place, and proceed with $A'$. As several more refinements will be made in the sequel, this first one is adopted without the change of notation: $A$ from now on stands for the possibly refined original set, which satisfies (3.1) as well as the assumptions $|A + A| \leq K|A|$ and $|A \cdot A| \leq K|A|$.
The multiplicative energy of $E^*_a(A)$, i.e. the number of ordered quadruples $(a_1, a_2, a_3, a_4) \in A \times A \times A \times A$, satisfying the equation
\[
\frac{a_1}{a_3} = \frac{a_4}{a_2}
\]
is, by Cauchy-Schwartz, bounded from below as follows:

\[
E^*_a(A) \geq \frac{|A|^4}{|A \cdot A|} \gg \frac{|A|^3}{K}.
\]

The multiplicative energy, by its definition, is

\[
E^*_a(A) = \sum_{\xi} n^2(\xi),
\]

where $\xi$ is the slope of a line through the origin in $\mathbb{F}_p^2$, and $n(\xi)$ is the number of points of $A \times A$ on this line.

Let us partition these lines, identified by their slopes, into dyadic groups as to how populated by points of $A \times A$ they are: a line in the $j$th group, $j = 1, 2, \ldots \leq 1 + \log_2 |A|$ will support $2^{j-1} \leq n(\xi) < 2^j$ points of $A \times A$. We shall consider a single “popular” dyadic group, to be specified in the end of the proof (although the choice will be straightforward). This dyadic group contains some number $L$ of lines, each supporting approximately $N$ points of $A \times A$, rendering the contribution $M$ into the multiplicative energy $E^*_a(A)$. One has

\[
LN^2 \approx M.
\]

This implies, since $LN \ll |A|^2$, and $N \ll |A|$, that

\[
L, N \gg \frac{M}{|A|^2}.
\]

Let $\Xi$ denote the set of slopes of the lines through the origin in the chosen dyadic group and $P$ denote the set of points of $A \times A$ supported on these lines. Since each line supports approximately the same number $N$ of points, one has

\[
|P| \approx LN.
\]

Let

\[
A_x = \{ y : (x, y) \in P \},
\]

\[
A_y = \{ x : (x, y) \in P \}.
\]

Namely $A_x$ is the set of *ordinates* of points of $P$ all having the same abscissa $x$ and $A_y$ the set of *abscissae* of points of $P$ all having the same ordinate $y$. For $y \in A_x$ let $A_{y/x} = A_\xi$ (with $\xi = \frac{y}{x}$) be the set of abscissae of the points of $P$ supported on the line through the origin with the slope $\xi = \frac{y}{x}$ passing through $(x, y)$. So, for all $y \in A_x$, $|A_{y/x}| \approx N$.

The next lemma is an important building block for the proof.
Lemma 3. There exist a popular abscissa $x = \tilde{x}$ and a popular ordinate $y = \tilde{y}$, i.e. such that $|A_{\tilde{x}}|, |A_{\tilde{y}}| \gg \frac{LN}{|A|^2}$, as well as a subset $\tilde{A}_{\tilde{x}} \subseteq A_{\tilde{x}}$, with

$$|\tilde{A}_{\tilde{x}}| \gg \frac{LM}{|A|^3},$$

such that for every $y \in \tilde{A}_{\tilde{x}}$, one has

$$|\tilde{A}_y \equiv A_y/\tilde{x} \cap A_{\tilde{y}}| \gg \frac{LMN}{|A|^4}.$$

Proof of Lemma 3. To be precise, one must run some popularity arguments about the sets $P$ and $\Xi$. In essence however, since $|P| \approx LN$ and the maximum population of a line with slope in $\Xi$ is “at most” $N$, this means that lower bounds pertaining to sums over the sets $\Xi, P$ also apply to the whole hierarchy of their “popular subsets”, for merely the price of the constants hidden in the $\gg$ symbols getting worse.

By the pigeonhole principle, a positive proportion of the points of $P$ have “popular ordinates”, namely such that a horizontal line passing through such an ordinate contains “at least” $\frac{LN}{|A|}$ points of $P$. Let $A'$ denote the set of these popular ordinates.

Let us call $P'$ the set of the points of $P$ having popular ordinates. One still has $|P'| \gg LN$ and $P'$ is still supported on no more than $L$ lines passing through the origin. Therefore, $P'$ still carries a positive proportion of the multiplicative energy $M \approx LN^2$ of $P$, and an average line (identified by its slope in $\xi \in \Xi$) still has $\sim N$ points of $P'$.

Now the abscissae of the points in the set $P'$ can be pruned in the same way, down to the “popular” ones, namely such that there are “at least” $\frac{LN}{|A|}$ points of $P'$ supported on a vertical line with a popular abscissa, whereupon $P'$ gets refined to $P''$. One can now disregard the lines that may have become “poor”, namely those supporting fewer than $cN$ points of $P''$. The remaining lines have a set of slopes $\Xi'$, whose cardinality is still “at least” $L$, and each of these lines still supports $\approx N$ points of $P''$.

The claims of the Lemma are basically the average case for the sum

$$\Sigma = \sum_{x \in A'', y \in A'} \sum_{z \in A_x} |A_{z/x} \cap A_y|,$$

Let us write $z \sim x$ if $(x, z)$ is a point of $P$. Then

$$\Sigma \gg \sum_{x \in A'', y \in A', z: z \sim x} |A_{z/x} \cap A_y|.$$

Rearranging the summations by fixing the ratio $\xi = \tilde{x}$ and confining the sum only to the “popular” ratios in $\Xi'$ (these ratios each have “at least” $N$ realisations in terms of “popular” ordinates and abscissae) one gets:

$$\Sigma \gg N \sum_{\xi \in \Xi'} \sum_{y \in A'} |A''_\xi \cap A_y|,$$

The sum in the right-hand-side of (3.9) takes place over “at least” $L$ lines whose slopes are popular, with respect to the refined point set $P''$, i.e. each line supporting
“at least” $N$ points of the latter point set. Fixing a particular line $l$, let $A_l$ be the set of the (popular) abscissae of the points of $P''$ on this line. One has $|A_l| \gg N$, as well as $A_l \subseteq A''$, the set of popular abscissae. This means, by construction of the sets $A', A''$, that each element of $A_l$ belongs to “at least” $\frac{LN}{|A|}$ different sets $A_y$, with $y \in A'$.

Hence,

\begin{equation}
\sum \gg N \cdot L \cdot N \cdot \frac{LN}{|A|} \gg \frac{LMN}{|A|}.
\end{equation}

Now the claims (3.8) and (3.7) follow from (3.9–3.11) by the pigeonhole principle. Indeed, there is a pair of $(\tilde{x}, \tilde{y}) \in A'' \times A'$, such that

\begin{equation}
\sum_{z \in A_{\tilde{x}} \cap A_{\tilde{y}}} \gg \frac{LMN}{|A|^4}.
\end{equation}

One can restrict the summation in (3.12) to those values of $z$ only, for which

\[ |A_{z/\tilde{x}} \cap A_{\tilde{y}}| \gg \frac{LMN}{|A|^4}. \]

These $z$ are to form the set $\tilde{A}_{\tilde{x}}$, whose existence is stated in the Lemma. Since the maximum size of a single $A_{z/\tilde{x}}$ is “at most” $N$, then the number of such $z$ is “at least” $\frac{LM}{|A|^3}$. □

$A$ can be now scaled, so without loss of generality assume $\tilde{x} = 1$, and to save on the notations let $A_{\tilde{x}} \equiv B$ (and scale no more). Let us also use further the notations $C$ for the set $A_{\tilde{y}}$ and $\tilde{B}$ for the refinement of $B$, so that (3.8) holds for every $z \in \tilde{B}$. Heuristically, $C$ catches a large proportion of the abscissae of points of $P$ supported on every line through the origin, whose slope is in $\tilde{B}$.

With the parameter $r \in \mathbb{F}_p^*$, consider now (as a case study) “additive pivots” $C + rC$, $\tilde{B} + r\tilde{B}$, as well as finally $C + r\tilde{C}_p$, where $\tilde{C}_p$ will be subset of $C$ containing “many” abscissae of points of $P$ lying on the particular line to be specified, with the slope $p \in \tilde{B}$.

Introduce the following notation: for a pair of sets $S_1, S_2 \subseteq \mathbb{F}_p$, let

\begin{equation}
R(S_1, S_2) = \left\{ \frac{p-q}{s-t} : p, q, \in S_1, s, t \in S_2, p \neq q, s \neq t \right\}.
\end{equation}

One now faces with three cases that deal with the sets $R(C, C)$, $R(\tilde{B}, \tilde{B})$, and $R(C, \tilde{C}_p)$, where $\tilde{C}_p$ is the above-mentioned subset of $C$, to be chosen. Case (i) and (ii) will constitute the normal case, where the estimates somewhat repeat what has been done in the state-of-the-art literature. These estimates, from (3) on, it would give a better estimate securing the exponent $\frac{1}{11}$, rather than $\frac{1}{12}$ with the current state of the art. But there would always be the “worst possible scenario” which forced the denominator in the final answer to become by one bigger than rendered by the normal case. This “worst case scenario”, however, gets replaced below by Case (iii) which gives a similar estimate, as in the normal case.
Recall, by Lemma 3,

\[(3.14) \quad |\tilde{B}| \gg \frac{LM}{|A|^3}, \quad |C| \gg \frac{LN}{|A|}\]

**Case (i):** Suppose \(R(\tilde{B}, \tilde{B}) \neq R(C, C)\). Then there are two possibilities:

**Case (i.1):** There is \(r = \frac{p - q}{s - t} \in R(\tilde{B}, \tilde{B})\), such that \(r\) is not in \(R(C, C)\). Fix this \(r\) along with a quartet \(p, q, s, t\) representing it throughout the rest of Case (i.1).

Then the equation

\[(3.15) \quad a_1 + ra_2 = a_3 + ra_4,\]

where \(a_1, \ldots, a_4 \in C\), has only trivial solutions, i.e those with \(a_2 = a_4\). Thus for any \(C' \subseteq C\), which contains a positive proportion of the elements of \(C\), one has

\[(3.16) \quad |C' + rC'| \gg |C|^2.\]

Therefore,

\[(3.17) \quad |C|^2 \ll |C' + \frac{p - q}{s - t}C'| \ll |pC' - qC' + sC' - tC'|.\]

But \(p, q, s, t\) are elements of \(\tilde{B}\), and hence of the set of slopes \(\Xi\). Therefore one can bound the sizes of the corresponding dilates of \(C'\) from above, using Lemma 2

Lemma 2 specifies the refinement \(C'\) of \(C\) which is chosen in such a way that the sets involved get covered by translates of \(C\) from above, using Lemma 2.

Recall the notation \(A_\xi \subseteq A\) for the set of the abscissae of the line with the slope \(\xi\). For any \(\xi \in \Xi\), 99% of the set \(\xi C\) can be covered by “at most”

\[(3.18) \quad \frac{|\xi C + \xi A_\xi|}{|\xi A_\xi|} \ll \frac{|A + A|}{N} \ll \frac{K|A|}{N}\]

translates of \(\xi A_\xi \subseteq A\) (which have cardinality approximately \(N\)), and therefore translates of \(A\) itself. Now one can choose \(C' \subseteq C\), appearing in (3.16) as a subset containing at least every second element of \(C\), and such that the sets \(pC'\), \(-qC'\), \(sC'\), \(-tC'\), each get fully covered (independently) by “at most” \(\frac{K|A|}{N}\) translates of \(A\) each. Which means, the whole set \((s - t)C' + (p - q)C'\) has been fully covered by “at most” \(\left(\frac{K|A|}{N}\right)^4\) translates of \(A + A + A + A\).

Together with (3.16) this implies

\[(3.19) \quad N^4|C|^2 \ll K^4|A|^4|A + A + A| \ll K^7|A|^5,\]

after using (3.1).

**Case (i.2):** There is \(r = \frac{p - q}{s - t} \in R(C, C)\), such that \(r\) is not in \(R(\tilde{B}, \tilde{B})\). Fix this \(r\) along with a quartet \(p, q, s, t\) representing it. Recall that \(C = A_\tilde{y}\), the set of abscissae with a popular, with regard to \(P\), ordinate \(\tilde{y}\). Thus \(\frac{\tilde{y}}{p}, \frac{\tilde{y}}{q}, \frac{\tilde{y}}{s}, \frac{\tilde{y}}{t}\) are the slopes in \(\Xi\). And so are, since the point set \(P\) is symmetric with respect to the bisector \(y = x\), the ratios \(\xi_p = \frac{p}{y}, \xi_q = \frac{q}{y}, \xi_s = \frac{s}{y}, \text{ and } \xi_t = \frac{t}{y} \).
Thus
\begin{equation}
(3.20)\quad r = \frac{\xi_p - \xi_q}{\xi_s - \xi_t}.
\end{equation}
Repeat now the argument of Case (i.1) from (3.16) through (3.19) replacing there \(C\) with \(\tilde{B}\) and \((p, q, s, t)\) with \((\xi_p, \xi_q, \xi_s, \xi_t)\). This yields the analogue of the estimate (3.19):
\begin{equation}
(3.21)\quad N^4 |\tilde{B}|^2 \ll K^4 |A|^4 |A + A + A + A| \ll K^7 |A|^5.
\end{equation}
The estimate (3.21) is slightly worse than (3.19), since the estimate on the size of \(\tilde{B}\) in Lemma 3 is more restrictive than on the size of \(C\), see (3.14). So the estimate (3.19) will not be returned to.

By Lemma 3, one has
\begin{equation}
(3.22)\quad |\tilde{B}| \gg \frac{LM}{|A|^4}, \quad \text{and as } M \approx LN^2, \text{ (3.21) implies that}
\end{equation}
\begin{equation}
(3.23)\quad M^4 \ll K^7 |A|^{11}.
\end{equation}
From now on let us assume that \(R(C, C) = R(\tilde{B}, \tilde{B}) \equiv R\).

Case (ii): Suppose \(|R| \gg \min(|C|^2, p)\). The original assumption \(|A| < \sqrt{p}\) ensures that the minimum is achieved when \(|R| \gg |C|^2\). For \(r \in R\), let \(E_r(C)\) denote the number of ordered quadruples \((a_1, a_2, a_3, a_4) \in C \times C \times C \times C\) satisfying the equation (3.15).

The equation (3.15) has trivial solutions – when \(a_2 = a_4\) – and non-trivial ones – when \((a_1, a_2, a_3, a_4)\) determines \(r\). Summing over all \(r\), one has, under the Case (ii) assumption:
\begin{equation}
(3.24)\quad \sum_{r \in R} E_r(C) = |R||C|^2 + |C|^4 \ll |R||C|^2.
\end{equation}
Hence, there exists \(r \in R\), such that \(E_r(C) \ll |C|^2\). Fix this \(r\) throughout the rest of Case (ii), together with some quartet \(p, q, s, t \in C\) representing it. Observe that the same bound is certainly satisfied by \(E_r(C')\), namely when the equation (3.15) is restricted to a subset \(C' \subseteq C\). If \(C'\) contains a positive proportion of the elements of \(B\), then by Cauchy-Schwartz,
\begin{equation}
(3.25)\quad |C' + rC'| \gg |C|^2.
\end{equation}
Now use the representation (3.20) for \(r\) and repeat verbatim – with \((\xi_p, \xi_q, \xi_s, \xi_t)\) replacing \((p, q, s, t)\) there – the argument from (3.16) on within Case (i.1).

From now on assume that \(R(C, C) = R(\tilde{B}, \tilde{B}) \equiv R\) and \(|R| \ll |C|^2\). This takes one into the final Case (iii) – the analog of worst possible scenario in the former literature which turns out to be a regular one here. This, together with Lemma 3 is central for the proof.

Case (iii): There exists some \(r = \frac{p - q}{s - t} \in R\), such that \(r + 1 \not\in R\) (otherwise \(R = \mathbb{F}_p^*\), and the condition \(|A| < \sqrt{p}\), returns one into Case (ii)). Fix this \(r\), together with a quartet \(p, q, s, t \in \tilde{B}\) representing it.
Consider now the quantity $p \in \tilde{B}$ and the set $\tilde{C}_p$, a subset of $C$, furnished by Lemma 3 with “at least” $\frac{LMN}{|A|^4}$ elements (set in (3.8) $y = p$ and recall that $\tilde{x} = 1$ after scaling). The members of $\tilde{C}_p$ are the abscissae of points of $P$, supported on the line through the origin with the slope $p$. They also lie in the set $C$. By the assumption of Case (iii) one has $R(C, C) = R(\tilde{B}, \tilde{B}) = R$, and it follows that since $r + 1$ is not in $R$, it is not in $R(C, \tilde{C}_p) \subseteq R$.

Thus, using Lemma 3 which guarantees that $|C| \gg \frac{LN}{|A|^4}$, as well as (3.8), for any positive proportion subsets $C', \tilde{C}'_p$ of $C, \tilde{C}_p$, respectively, one has

$$|C' + (r + 1)\tilde{C}'_p| \geq \frac{LN LMN}{|A| |A|^4}. \tag{3.25}$$

Let us use Lemma 1 in the following form: for any positive proportion subset $C'$ of $C$ ($C'$ is to be specified later, in the ensuing covering argument), there is $C'' \subseteq C'$, containing, say 99% of the members of $C'$, and such that, by (3.25), one has:

$$\frac{LN LMN}{|A| |A|^4} \ll |C'' + (r + 1)\tilde{C}'_p| \ll \left| C'' + \tilde{C}'_p + \frac{p - q}{s - t} \tilde{C}_p \right|$$

$$\ll \left| C' + \tilde{C}'_p \right| \left| C' + \frac{p - q}{s - t} \tilde{C}_p \right|$$

$$\ll K\frac{|A|}{|C|} (s - t)C' + (p - q)\tilde{C}'_p$$

$$\ll K\frac{|A|}{|C|} sC' - tC' - q\tilde{C}_p + A. \tag{3.26}$$

Indeed, $p\tilde{C}_p \subseteq A$, since $p \in \Xi$ is a slope and $\tilde{C}_p$ is a subset of the abscissae of the points of $P$ supported on the corresponding line through the origin. In comparison to the above Cases (i,ii), the covering argument is now to be applied only three rather than four times.

The covering argument now proceeds in exactly the same way as it was in Cases (i,ii), since $s, t, q$ are members of $B \subseteq \Xi$. The subsets $C'$ of $C$, as well as $\tilde{C}_p$ of $\tilde{C}_p$ are chosen so that their dilates $sC', -tC', -q\tilde{C}_p$ are each fully covered (independently) by “at most” $\frac{K|A|}{N}$ translates of $A$. (E.g. $-q\tilde{C}_p$ gets covered by no more than $\frac{|-q\tilde{C}_p - qA_q|}{|A_q|} \ll \frac{K|A|}{N}$ translates of $qA_q \subseteq A$, and therefore $A$ itself.)

Then (3.26) yields

$$\frac{LMN}{|A|^4} \left( \frac{LN}{|A|} \right)^2 N^3 \ll K^4|A|^4 |A + A + A| \ll K^7|A|^5,$$

by (3.1). Since $M \approx LN^2$, this means:

$$M^4 \ll K^7|A|^{11},$$

restating the estimate (3.22), which therefore shall be taken as the final one in the above Case study.
To conclude the proof, all one has to do is choose $M$. In view of the latter estimate, which only contains the multiplicative energy $M$, one can only do the straightforward pigeonholing

$$M \gg \frac{E_*(A)}{\log |A|} \gg \frac{|A|^3}{K \log |A|},$$

since by the pigeonhole principle, there is a dyadic group of lines through the origin furnishing “at least” the above amount of multiplicative energy.

Therefore

$$K \gg \left( \frac{|A|}{\log^4 |A|} \right)^{\frac{1}{11}}.$$

This completes the proof of Theorem 1. □

The final remark is that having in the outset the ratio set $A : A$, rather than the product set $A \cdot A$ makes the multiplicative energy argument superfluous and matters more transparent. $\Xi$ would be denote the set of “popular lines” with the slopes in $\Xi$, each supporting “at least” $\frac{|A|}{K}$ points of $A \times A$. This rids one of the necessity of using dyadic pigeonholing with the set of slopes and as the result, there is no logarithm in the final estimate. Altogether the lines with the slopes in $\Xi$ support a positive proportion of the set $A \times A$. The sets $B, \tilde{B}$, and $C$ then become positive proportion subsets of $A$, and the relations affecting the left-hand side of the estimate (3.22) would assume the simpler form $LN \gg |A|^2, N \gg \frac{|A|}{K}$.

References

[1] J. Bourgain, M.Z. Garaev. On a variant of sum-product estimates and explicit exponential sum bounds in prime fields. Math. Proc. Cambridge Philos. Soc. 146 (2009), no. 1, 1–21.
[2] J. Bourgain, N. Katz and T. Tao. A sum-product estimate in finite fields and their applications. Geom. Func. Anal. 14 (2004), 27-57.
[3] M.Z. Garaev. An explicit sum-product estimate in $\mathbb{F}_p$. Intern. Math. Res. Notices (2007), no 11, 1–11.
[4] M.Z. Garaev. The sum-product estimates for large subsets of prime fields. Proc. Amer. Math. Soc. 137 (2008), 2735 – 2739.
[5] S.V. Konyagin. A sum-product estimate in fields of prime order. Preprint arXiv:math/0304217 (2003), 9pp.
[6] N.H. Katz, C.-Y. Shen. A slight improvement to Garaev’s sum product estimate. Proc. Amer. Math. Soc. 136 (2008), 2499–2504.
[7] L. Li. Slightly improved sum-product estimates in fields of prime order. Preprint arXiv:math/0907.2051 (2009), 9pp.
[8] I. Z. Ruzsa. An application of graph theory to additive number theory. Scientia, Ser. A 3 (1989), 97–109.
[9] Ch.-Y. Shen. An extension of Bourgain and Garaev’s sum-product estimates. Acta Arith. 135 (2008), 351-356.

Misha Rudnev, Department of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom
E-mail address: m.rudnev@bristol.ac.uk