A SLIGHT IMPROVEMENT TO GARAЕV’S SUM PRODUCT ESTIMATE

NETS HAWK KATZ AND CHUN-YEN SHEN

(Communicated by Michael T. Lacey)

0. Introduction

Let $A$ and $B$ be two finite sets of integers. We let

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

and

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

There have been many studies of the size of the sum and product sets for the case $A = B$, since Erdős and Szemerédi made their well-known conjecture that

$$\max(|A + A|, |AA|) \geq C|A|^{2-\epsilon}$$

forall $\epsilon > 0$. This result is still open, and the best result to date is due to Solymosi [S], who showed that

$$\max(|A + A|, |AA|) \geq C\epsilon|A|^{14/11-\epsilon}.$$ 

In the finite field setting this situation is much more complicated because the main tool, the Szemerédi-Trotter incidence theorem, does not hold in the same generality. It is known, via the work in [BKT], that if $A$ is a subset of $F_p$, the field of $p$ elements with $p$ prime, and if $p^{\delta} < |A| < p^{1-\delta}$, where $\delta > 0$, then one has the sum product estimate

$$\max(|A + A|, |AA|) \geq |A|^{1+\epsilon}$$

for some $\epsilon > 0$. This result has found many applications in combinatorial problems and exponential sum estimates (see e.g. [BKT], [BGK], [G2]). Recently, Garaev [G1] showed that when $|A| < p^{1/2}$, one has the estimate

$$\max(|A + A|, |AA|) \geq |A|^{14/11}.$$ 

By using Plünnecke’s inequality in a slightly more sophisticated way, we improve this exponent to $14/13$. We believe that further improvements might be possible through aggressive use of the Ruzsa covering.
1. Preliminaries

Throughout this paper $A$ will denote a fixed set in the field $F_p$ of $p$ elements with $p$ prime. For $B$, any set, we will denote its cardinality by $|B|$.

Whenever $X$ and $Y$ are quantities we will use

$$X \lesssim Y$$

to mean

$$X \leq CY,$$

where the constant $C$ is universal (i.e. independent of $p$ and $A$). The constant $C$ may vary from line to line. We will use

$$X \lesssim Y$$

to mean

$$X \leq C(\log |A|)^\alpha Y,$$

and $X \approx Y$ to mean $X \lesssim Y$ and $Y \lesssim X$, where $C$ and $\alpha$ may vary from line to line but are universal.

We state some preliminary lemmas, mostly those stated by Garaev, but occasionally with different emphasis.

The first lemma is a consequence of the work of Glibichuk and Konyagin [GK].

**Lemma 1.1.** Let $A_1 \subset F_p$ with $1 < |A_1| < p^\frac{1}{2}$. Then for any elements $a_1, a_2, b_1, b_2$ so that

$$\frac{b_1 - b_2}{a_1 - a_2} + 1 \notin \frac{A_1 - A_1}{A_1 - A_1},$$

we have that for any $A' \subset A_1$ with $|A'| \gtrsim |A_1|$

$$|(a_1 - a_2)A' + (a_1 - a_2)A' + (b_1 - b_2)A'| \gtrsim |A_1|^2.$$

In particular such $a_1, a_2, b_1, b_2$ exist unless $\frac{A_1 - A_1}{A_1 - A_1} = F_p$. In the case $\frac{A_1 - A_1}{A_1 - A_1} = F_p$, we may find $a_1, a_2, b_1, b_2 \in A_1$ so that

$$|(a_1 - a_2)A_1 + (b_1 - b_2)A_1| \gtrsim |A_1|^2.$$

**Sketch of the proof.** If $\frac{A_1 - A_1}{A_1 - A_1} \neq F_p$, it is immediate that there exist $a_1, a_2, b_1, b_2 \in A_1$ with $1 + \frac{b_1 - b_2}{a_1 - a_2} \notin \frac{A_1 - A_1}{A_1 - A_1}$. This automatically implies

$$|(a_1 - a_2)A' + (a_1 - a_2)A' + (b_1 - b_2)A'| \gtrsim |A_1|^2.$$

(See [GK].) If $x \notin \frac{A_1 - A_1}{A_1 - A_1}$, then each element of $A_1 + xA_1$ has but one representative $a + xa'$. On the other hand, if

$$\frac{A_1 - A_1}{A_1 - A_1} = F_p,$$

then one can find $a_1, a_2, b_1, b_2 \in A_1$ so that $\frac{a_1 - a_2}{b_1 - b_2}$ has at most $|A_1|^2$ representatives as $\frac{a_1 - a_2}{b_1 - b_2}$ with $a_3, a_4, b_3, b_4 \in A_1$, which implies that $|A_1 + \frac{a_1 - a_2}{b_1 - b_2}A_1|$ is large. Again, for more details see [GK].

The following two lemmas, quoted by Garaev, are due to Ruzsa and may be found in [TV]. The first is usually referred to as Ruzsa’s triangle inequality. The second is a form of Plünnecke’s inequality.
Lemma 1.2. For any subsets \(X, Y, Z\) of \(F_p\) where \(X\) is nonempty, we have
\[
|Y - Z| \leq \frac{|Y - X||X - Z|}{|X|}.
\]

Lemma 1.3. Let \(X, B_1, \ldots, B_k\) be any subsets of \(F_p\) with
\[
|X + B_i| \leq \alpha_i |X|,
\]
for \(i\) ranging from 1 to \(k\). Then there exists \(X_1 \subset X\) with
\[
|X_1 + B_1 + \cdots + B_k| \leq \alpha_1 \cdots \alpha_k |X_1|.
\]

We record a number of corollaries. The first two can be found in [TV]. We first became aware of the last one in the paper of Garaev [G1].

Corollary 1.4. Let \(X, B_1, \ldots, B_k\) be any subsets of \(F_p\). Then
\[
|B_1 + \cdots + B_k| \leq \frac{|X + B_1| \cdots |X + B_k|}{|X|^{k-1}}.
\]

Proof. Simply bound \(|B_1 + \cdots + B_k|\) by \(|X_1 + B_1 + \cdots + B_k|\) and \(|X_1|\) by \(|X|\). \(\square\)

Corollary 1.4 is somewhat wasteful in that \(X_1\) is unlikely to be both a singleton element and a set with the same cardinality as \(X\). By applying Lemma 1.3 iteratively, we obtain the following corollary.

Corollary 1.5. Let \(X, B_1, \ldots, B_k\) be any subsets of \(F_p\). Then there is \(X' \subset X\) with
\[
|X' + B_1 + \cdots + B_k| \lesssim \frac{|X + B_1| \cdots |X + B_k|}{|X|^{k-1}}.
\]

Proof. Observe that for any \(Y \subset X\) with \(|Y| \geq \frac{|X|}{2}\), we have that
\[
\frac{|Y + B_1|}{|Y|} \lesssim \frac{|X + B_1|}{|X|}.
\]

Now recursively apply Lemma 1.3. That is, first apply it to \(X, B_1, \ldots, B_k\) obtaining a set \(X_1\) satisfying
\[
|X_1 + B_1 + \cdots + B_k| \lesssim \frac{|X + B_1| \cdots |X + B_k|}{|X|^{k-1}}|X_1|.
\]

If \(|X_1| > \frac{1}{2}|X|\), then stop and let \(X' = X_1\). Otherwise apply Lemma 1.3 to \(X \setminus X_1, B_1, \ldots, B_k\). Proceeding recursively if \(|X_1 \cup \cdots \cup X_{j-1}| > \frac{1}{2}|X|\), set
\[
X' = X_1 \cup \cdots \cup X_{j-1};
\]
otherwise obtain the inequality
\[
|X_j + B_1 + \cdots + B_k| \lesssim \frac{|X + B_1| \cdots |X + B_k|}{|X|^k}|X_j|.
\]

Summing all the inequalities we obtained before stopping gives us the desired result. \(\square\)
Corollary 1.6. Let $A \subset F_p$ and let $a, b \in A$. Then we have the inequalities

$$|aA + bA| \leq \frac{|A + A|^2}{|aA \cap bA|}$$

and

$$|aA - bA| \leq \frac{|A + A|^2}{|aA \cap bA|}.$$ 

Proof. To get the first inequality, apply Corollary 1.4 with $k = 2$, $B_1 = aA$, $B_2 = bA$, and $X = aA \cap bA$.

To get the second inequality, apply Lemma 1.2 with $Y = aA$, $Z = -bA$, and $X = -(aA \cap bA)$. □

2. Modified Garaev’s inequality

In this section, we slightly modify Garaev’s argument to obtain

Theorem 2.1. Let $A \subset F_p$ with $|A| < p^{\frac{1}{2}}$; then

$$\max(|AA|, |A + A|) \gtrsim |A|^{\frac{14}{13}}.$$ 

Proof. Following Garaev, we observe that

$$\sum_{a \in A} \sum_{b \in A} |aA \cap bA| \gtrsim \frac{|A|^4}{|AA|}.$$ 

Therefore, we can find an element $b_0 \in A$, a subset $A_1 \subset A$ and a number $N$ satisfying

$$|b_0A \cap aA| \approx N,$$

for every $a \in A_1$. Further

(2.1) $$N \gtrsim \frac{|A|^2}{|AA|}$$

and

(2.2) $$|A_1|N \gtrsim \frac{|A|^3}{|AA|}.$$ 

Now there are two cases. In the first case, we have

$$A_1 - A_1 = F_p.$$ 

If so, applying Lemma 1.1, we can find $a_1, a_2, b_1, b_2 \in A_1$ so that

$$|A_1|^2 \lesssim |(a_1 - a_2)A_1 + (b_1 - b_2)A_1| \leq |a_1A - a_2A + b_1A - b_2A|.$$ 

Apply Corollary 1.4 with $k = 4$, and with $B_1 = a_1A$, $B_2 = -a_2A$, $B_3 = b_1A$, $B_4 = -b_2A$, and $X = b_0A$. Then we apply Corollary 1.6 to bound above $|X + B_j|$. This yields

$$|A_1|^2 \lesssim \frac{|A + A|^8}{N^4|A|^3}$$

or

$$|A_1|^2 N^4|A|^3 \lesssim |A + A|^8.$$ 

Applying (2.2), we get

(2.3) $$N^2|A|^9 \lesssim |A + A|^8|AA|^2,$$ 

License or copyright restrictions may apply to redistribution; see https://www.ams.org/journal-terms-of-use
A SLIGHT IMPROVEMENT TO GARAEV’S SUM PRODUCT ESTIMATE

and applying (2.1), we get

(2.4) \[ |A|^{13} \lesssim |A + A|^8|AA|^4. \]

The estimate (2.4) implies that

\[
\max(|A + A|, |AA|) \gtrsim |A|^{12} \gtrsim |A|^{14},
\]

so that we have more than we need in this case.

Thus we are left with the case that

\[
\frac{A_1 - A_1}{A_1 - A_1} \neq F_p.
\]

Thus we can find \(a_1, a_2, b_1, b_2\) so that for any refinement \(A' \subset A_1\) with \(|A'| \gtrsim |A_1|\), we have

\[
|A_1|^2 \lesssim |(a_1 - a_2)A' + (a_1 - a_2)A' + (b_1 - b_2)A'|.
\]

Now we apply Corollary 1.5, choosing \(A'\) so that

\[
|(a_1 - a_2)A' + (a_1 - a_2)A_1 + (b_1 - b_2)A_1| \lesssim \frac{|A + A|(|a_1 - a_2)A_1 + (b_1 - b_2)A_1|}{|A_1|}.
\]

This is where we have improved on Garaev’s original argument.

Then, as in the first case, estimating

\[
|(a_1 - a_2)A_1 + (b_1 - b_2)A_1| \leq |a_1A - a_2A + b_1A - b_2A|
\]

and applying Corollary 1.4 with \(X = b_0A\) and Corollary 1.6, we obtain

\[
|A_1|^3 N^4 |A|^3 \lesssim |A + A|^9.
\]

Applying (2.2), we get

(2.5) \[ N|A|^{12} \lesssim |A + A|^9|AA|^3. \]

Now applying (2.1), we get

(2.6) \[ |A|^{14} \lesssim |A + A|^9|AA|^4. \]

Inequality (2.6) proves the theorem.

\[ \square \]

Acknowledgements

We would like to express our gratitude to the referee for valuable comments in developing the final version of this article.

References


Department of Mathematics, Indiana University, Rawles Hall, 831 East Third St., Bloomington, Indiana 47405

Department of Mathematics, Indiana University, Rawles Hall, 831 East Third St., Bloomington, Indiana 47405