PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 136, Number 7, July 2008, Pages 2499–2504
S 0002-9939(08)09385-4
Article electronically published on March 10, 2008

A SLIGHT IMPROVEMENT TO GARAEV'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 Erdös and Szemerèdi made their well-known conjecture that

$$\max(|A + A|, |AA|) \geq C_\epsilon |A|^{2-\epsilon} \forall \epsilon > 0.$$

The conjecture is still open, and the best result to date is due to Solymosi [S], who showed that

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

In the finite field setting this situation is much more complicated because the main tool, the Szemerèdi-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 $|A| < p^{\frac{1}{2}}$, one has the estimate

$$\max(|A + A|, |AA|) \gtrapprox |A|^{\frac{15}{14}}.$$

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

Received by the editors March 21, 2007.
1991 *Mathematics Subject Classification.* Primary 42B25; Secondary 60K35.
The first author was supported by NSF grant DMS 0432237.

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

$$X \lessapprox Y$$

to mean

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

and $X \approx Y$ to mean $X \lessapprox Y$ and $Y \lessapprox X$, where C and α 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 $\frac{a_3 - a_4}{b_3 - b_4}$ 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]. $\square$

The following two lemmas, quoted by Garaev, are due to Ruzsa and may be found in [TV]. The first is usually referred to as Rusza'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 $X, B_1, \dots, B_k$ 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

$$|X_1 + B_1 + \cdots + B_k| \leq \alpha_1 \dots \alpha_k |X_1|. \tag{1.1}$$

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 $X, B_1, \dots, B_k$ be any subsets of F_p. Then*

$$|B_1 + \cdots + B_k| \leq \frac{|X + B_1| \dots |X + B_k|}{|X|^{k-1}}.$$

Proof. Simply bound $|B_1 + \cdots + B_k|$ by $|X_1 + B_1 + \cdots + B_k|$ and $|X_1|$ by $|X|$. □

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 $X, B_1, \dots, B_k$ be any subsets of F_p. Then there is $X' \subset X$ with $|X'| > \frac{1}{2}|X|$ so that*

$$|X' + B_1 + \cdots + B_k| \lesssim \frac{|X + B_1| \dots |X + B_k|}{|X|^{k-1}}.$$

Proof. Observe that for any $Y \subset X$ with $|Y| \geq \frac{|X|}{2}$, we have that

$$\frac{|Y + B_i|}{|Y|} \lesssim \frac{|X + B_i|}{|X|}.$$

Now recursively apply Lemma 1.3. That is, first apply it to $X, B_1, \dots, B_k$ obtaining a set X_1 satisfying

$$|X_1 + B_1 + \cdots + B_k| \lesssim \frac{|X + B_1| \dots |X + B_k|}{|X|^k} |X_1|.$$

If $|X_1| > \frac{1}{2}|X|$, then stop and let $X' = X_1$. Otherwise apply Lemma 1.3 to $X \backslash X_1, B_1, \dots, B_k$. 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

$$|X_j + B_1 + \cdots + B_k| \lesssim \frac{|X + B_1| \dots |X + B_k|}{|X|^k} |X_j|.$$

Summing all the inequalities we obtained before stopping gives us the desired result. □

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*

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

Proof. Following Garaev, we observe that

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

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

$$|b_0 A \cap aA| \approx N,$$

for every $a \in A_1$. Further

$$N \gtrapprox \frac{|A|^2}{|AA|} \tag{2.1}$$

and

$$|A_1| N \gtrapprox \frac{|A|^3}{|AA|}. \tag{2.2}$$

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

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

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

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

Apply Corollary 1.4 with $k = 4$, and with $B_1 = a_1 A$, $B_2 = -a_2 A$, $B_3 = b_1 A$, $B_4 = -b_2 A$, and $X = b_0 A$. 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

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

Applying (2.2), we get

$$N^2 |A|^9 \lessapprox |A+A|^8 |AA|^2, \tag{2.3}$$

and applying (2.1), we get

$$|A|^{13} \lessapprox |A+A|^8 |AA|^4. \tag{2.4}$$

The estimate (2.4) implies that

$$\max(|A+A|, |AA|) \gtrapprox |A|^{\frac{13}{12}} \gtrapprox |A|^{\frac{14}{13}},$$

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

$$|(a_1 - a_2)A_1 + (b_1 - b_2)A_1| \leq |a_1 A - a_2 A + b_1 A - b_2 A|$$

and applying Corollary 1.4 with $X = b_0 A$ and Corollary 1.6, we obtain

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

Applying (2.2), we get

$$N|A|^{12} \lessapprox |A+A|^9 |AA|^3. \tag{2.5}$$

Now applying (2.1), we get

$$|A|^{14} \lessapprox |A+A|^9 |AA|^4. \tag{2.6}$$

Inequality (2.6) proves the theorem. □

Acknowledgements

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

References

[BGK] Bourgain, J., Glibichuk, A.A., and Konyagin, S.V., *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. (2) **73** (2006), 380–398. MR2225493 (2007e:11092)

[BKT] Bourgain, J., Katz, N., and Tao, T., *A sum-product estimate in finite fields and applications*, Geom. Funct. Anal. **14** (2004), 27–57. MR2053599 (2005d:11028)

[G1] Garaev, M.Z., *An explicit sum-product estimate in* $\mathbb{F}_p$, preprint, http://arxiv.org/abs/math/0702780.

[G2] Garaev, M.Z., *The sum product estimate for large subsets of prime orders*, preprint, http://arxiv.org/abs/0706.0702.

[GK] Glibichuk, A.A., and Konyagin, S.V., *Additive properties of product sets in fields of prime order*, preprint.

[S] Solymosi, J., *On the number of sums and products*, Bull. London Math. Soc. **37** (2005), 491–494. MR2143727 (2006c:11021)

[TV] Tao, T. and Vu, V., *Additive Combinatorics*, Cambridge Univ. Press, 2006. MR2289012

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