Garaev's inequality in Finite Fields not of prime order

Nets Hawk Katz[1] and Chun-Yen Shen
Indiana University

Submitted: March 22, 2007; Revised: August 7, 2007; Accepted: December 12, 2007; Published: Janaury 29, 2008

Subject Class: Primary: 42B25; Secondary: 60K35

1 Introduction

Let A be a subset of $F = F_{p^n}$, the field of p^n elements with p prime.

We let

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

and

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

Many authors have been proving lower bounds on $\max(|A + A|, |AA|)$ (see e.g. [BKT], [BGK], [G], [HI]). Recently, Garaev [G] showed that when $n = 1$ and $|A| < p^{\frac{1}{2}}$ one has the estimate

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

The authors in [KS] slightly improved this to

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

In the present paper, we extend Garaev's techniques to the set of fields which are not necessarily of prime order. Our goal here is just to find an explicit estimate in the supercritical setting where the set A has less cardinality than the square root of the cardinality of the field, and interacts in a less than half-dimensional way with any subfields. (We make this precise below.) Precisely, we prove

Main Theorem 1. *Let $F = F_{p^n}$ be a finite field. Suppose that A is a subset of F so that for any $A' \subset A$ with $|A'| \geq |A|^{\frac{18}{19}}$ and for any $G \subset F$ a subfield (not necessarily proper) and for any elements $c, d \in F$ if*

$$A' \subset cG + d,$$

then

$$|A'| \leq |G|^{\frac{1}{2}}.$$

Then it must be that

$$\max(|A + A|, |AA|) \gtrapprox |A|^{\frac{20}{19}}.$$

[1]The first author was supported by NSF grant DMS 0432237.

We thank the referee for a significant improvement in the exponents over our preliminary version. This was done by adapting techniques reminiscent of those of Glibichuk and Konyagin [GK] to reduce the complexity of the expression we have found which is not in $\frac{A-A}{A-A}$.

The hypotheses regarding interaction with subfields could be tightened slightly in various ways, but they certainly need to require that A be different from an affine translate of G. In many cases, they are vacuous, as when n is odd and $p^{\frac{7n+\epsilon}{20}} < |A| < p^{\frac{n}{2}}$. We think hypotheses as saying that in a certain sense, the dimension of A is at most $\frac{1}{2}$. An analogy may be drawn with the sum product theorem in [B] and it is possible that the techniques here would be useful in that setting.

2 Preliminaries

Throughout this paper A will denote a fixed set in the field $F = F_{p^n}$ of p^n elements with p a 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

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

where C and α may vary from line to line but are universal.

We state some preliminary lemmas.

Lemma 2.1. *Let $A \subset F$. Suppose that*

$$|\frac{A-A}{A-A}| \geq |A|^2.$$

Then there are $a_1, a_2, b_1, b_2 \in A$ with

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

Proof. Under the hypothesis, there is $x \in \frac{A-A}{A-A}$ with at most $|A|^2$ representations

$$x = \frac{a_1 - a_2}{b_1 - b_2}.$$

Thus there $\lesssim |A|^2$ solutions of

$$a_1 + b_2 x = a_2 + b_1 x.$$

Therefore

$$|A + xA| \gtrsim |A|^2.$$

But if

$$x = \frac{a_1 - a_2}{b_1 - b_2},$$

then

$$|A + xA| = |(a_1 - a_2)A + (b_1 - b_2)A|.$$

□

Lemma 2.2. *Let $A \subset F$. Suppose that $x \in F$ with $x \notin \frac{A-A}{A-A}$, then*

$$|A + xA| = |A|^2.$$

Proof. There are no nontrivial solutions of

$$a_1 + xb_2 = a_2 + xb_1,$$

with $a_1, a_2, b_1, b_2 \in A$. □

Lemma 2.3. *Let $A \subset F$ with cardinality at least 3. Suppose that G is a subfield of F with*

$$\frac{A-A}{A-A} \subset G,$$

then there exist $c, d \in F$ with

$$A \subset cG + d.$$

Proof. Suppose that the conclusion is false for all $c, d \in F$. Then we can find $a_1, a_2, b_1, b_2, c, d_1, d_2 \in A$ and $g_1, g_2, g_3, g_4 \in G$ with $b_1 \neq b_2$ and $\frac{d_1-d_2}{c} \notin G$, so that

$$a_1 = cg_1 + d_1; \quad a_2 = cg_2 + d_2; \quad b_1 = cg_3 + d_2; \quad b_2 = cg_4 + d_2. \tag{1}$$

We do this as follows: We select b_1, b_2 distinct in A. Since $b_1 - b_2$ is invertible, we can find c so that $(b_1 - b_2) \in cG$. Then there is d_2 with $b_1, b_2 \in cG + d_2$. We choose $a_2 \in cG + d_2 \cap A$. It need not be distinct from b_1 and b_2. Then we apply the assumption to pick $a_1 \in A$ but $a_1 \notin cG + d_2$. Applying (1.1), we see immediately

$$\frac{a_1 - a_2}{b_1 - b_2} \notin G.$$

□

The following two lemmas, quoted by Garaev, are due to Ruzsa, may be found in [TV]. The first is usually referred to as Ruzsa's triangle inequality. The second is a form of Plunnecke's inequality.

Lemma 2.4. *For any subsets X, Y, Z of F we have*

$$|X - Z| \leq \frac{|Y - X||X + Z|}{|X|}.$$

Lemma 2.5. *Let $X, B_1, \ldots, B_k$ be any subsets of F with*

$$|X + B_i| \leq \alpha_i |X|,$$

for i ranging from 1 to k. Then there exists $X_1 \subset X$ with

$$|X_1 + B_1 + \cdots + B_k| \leq \alpha_1 \ldots \alpha_k |X_1|. \tag{2}$$

We record a number of Corollaries. The first can be found in [TV]. The second one, we first became aware of in the paper of Garaev.

Corollary 2.6. *Let $X, B_1, \ldots, B_k$ be any subsets of F. Then*

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

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

Corollary 2.7. *Let $A \subset F$ 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 1.6 with $k = 2$, $B_1 = aA$, $B_2 = bA$, and $X = aA \cap bA$.

To get the second inequality, apply Lemma 1.4 with $Y = aA$, $Z = -bA$ and $X = -(aA \cap bA)$. □

3 Modified Garaev's inequality

In this section, we slightly modify Garaev's argument to obtain the desired result.

Proof of Main Theorem. 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

$$N \gtrapprox \frac{|A|^2}{|AA|}, \tag{3}$$

and

$$|A_1| N \gtrapprox \frac{|A|^3}{|AA|}. \tag{4}$$

Now there are three cases. In the first case, we have that $\frac{A_1 - A_1}{A_1 - A_1}$ is a field $G \subset F$. If we have $|A_1| \lessapprox |A|^{\frac{18}{19}}$, then we already have the desired result from (2.2) and $N \leq |A|$. Otherwise, by Lemma 1.3, we have that A_1 is contained in an affine image of G so that by hypothesis

$$\left|\frac{A_1 - A_1}{A_1 - A_1}\right| \gtrsim |A_1|^2.$$

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

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

Applying Corollary 1.6 with $k = 4$, $B_1 = a_1 A$, $B_2 = -a_2 A$, $B_3 = b_1 A$, $B_4 = -b_2 A$, and with $X = b_0 A$, and applying Corollary 1.7 to bound above $|X + B_j|$. Thus we get

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

or

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

Applying (2.2), we get

$$N^2|A|^9 \lessapprox |A+A|^8|AA|^2 \tag{5}$$

and applying (2.1), we get

$$|A|^{13} \lessapprox |A+A|^8|AA|^4. \tag{6}$$

The estimate (2.4) implies that

$$\max(|A+A|,|AA|) \gtrapprox |A|^{\frac{13}{12}} \gtrapprox |A|^{\frac{20}{19}},$$

so that we have more than we need in this case. We restrict to the setting where $\frac{A_1-A_1}{A_1-A_1}$ is not a field.

Now there are two remaining cases, either

$$(\frac{A_1-A_1}{A_1-A_1})(\frac{A_1-A_1}{A_1-A_1}) \not\subset \frac{A_1-A_1}{A_1-A_1}$$

or

$$(\frac{A_1-A_1}{A_1-A_1})(\frac{A_1-A_1}{A_1-A_1}) = (\frac{A_1-A_1}{A_1-A_1}), \frac{A_1-A_1}{A_1-A_1} + \frac{A_1-A_1}{A_1-A_1} \not\subset \frac{A_1-A_1}{A_1-A_1}.$$

In the first case for some $a_i, b_i, c_i, d_i \in A_1$, we have

$$\frac{a_1-b_1}{c_1-d_1}\frac{a_2-b_2}{c_2-d_2} \notin \frac{A_1-A_1}{A_1-A_1}$$

which can be rewritten as

$$\frac{a_1-b_1}{a_1}\frac{a_1}{a_1-c_1}\frac{a_1-c_1}{c_1}\frac{c_1}{c_1-d_1}\frac{a_2-b_2}{c_2-d_2} \notin \frac{A_1-A_1}{A_1-A_1}.$$

From this we deduce that for some $a, b, x, y, z, t \in A_1$, we have

$$\frac{a-b}{a}\frac{x-y}{z-t} \notin \frac{A_1-A_1}{A_1-A_1}.$$

Thus

$$|A_1|^2 \leq |(a-b)(x-y)A_1 + a(z-t)A_1| \leq |a(x-y)A - b(x-y)A + a(z-t)A|.$$

We now apply Corollary 1.6 first with $X = a(x-y)A$ to get

$$|A_1|^2 \leq \frac{|A+A||aA-bA||(x-y)A+(z-t)A|}{|A|^2}.$$

and then with $X = b_0 A$ together with Corollary 1.7, this gives

$$|A|^{20} \lessapprox |A+A|^{13}|AA|^6.$$

This implies that

$$\max(|A+A|,|AA|) \gtrapprox |A|^{\frac{20}{19}}$$

In the second case, for some $a_i, b_i \in A_1$ we have

$$\frac{a_1 - a_2}{b_1 - b_2} + \frac{a_3 - a_4}{b_3 - b_4} \notin \frac{A_1 - A_1}{A_1 - A_1},$$

which, in view of $(\frac{A_1 - A_1}{A_1 - A_1})(\frac{A_1 - A_1}{A_1 - A_1}) = \frac{A_1 - A_1}{A_1 - A_1}$,implies that there exist elements $a, b, c, d \in A_1$ such that

$$\frac{a-b}{c-d} + 1 = \frac{b_3 - b_4}{a_3 - a_4}\frac{a_1 - a_2}{b_1 - b_2} + 1 = \frac{b_3 - b_4}{a_3 - a_4}(\frac{a_1 - a_2}{b_1 - b_2} + \frac{a_3 - a_4}{b_3 - b_4}) \notin \frac{A_1 - A_1}{A_1 - A_1}$$

Thus we have

$$|A_1|^2 \leq |(c-d)A + (a-b)A + (c-d)A|.$$

Now applying Corollary 1.6 first with $k = 3$,$X = (c-d)A$ and then $X = b_0 A$ together with Corollary 1.7, we obtain

$$|A|^{15} \lessapprox |A + A|^{10}|AA|^4.$$

Since $\frac{15}{14} \geq \frac{20}{19}$, we get more than we need in this case.

□

References

[1] Bourgain, J. *On the Erdős-Volkmann and Katz-Tao ring conjectures*, GAFA **13**, (2003) 334-365.

[2] 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.

[3] Bourgain, J., Katz, N, and Tao, T., *A sum product estimate in finite fields and Applications*, GAFA **14**, (2004) 27–57.

[4] Hart, D. and Iosevich, A., *Sums and Products in Finite Fields: An Integral Geometric Viewpoint*, preprint.

[5] Garaev, M.Z., *An explicit sum-product estimate in* $\mathbb{F}_p$, preprint.

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

[7] Katz,N.H. and Shen,C.Y., *A Slight Improvement to Garaev's Sum Product Estimate*, preprint.

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