ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 41, Number 3, 2011

SUM-PRODUCT PHENOMENON IN FINITE FIELDS NOT OF PRIME ORDER

CHUN-YEN SHEN

ABSTRACT. Let $F = F_{p^n}$ be a finite field and A a subset of F so that for any $A' \subset A$ with $|A'| \geq |A|^{15/16}$ 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

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

Then it must be that

$$\max(|A + A|, |F(A, A)|) \gtrapprox |A|^{17/16}$$

where $F : F_p \times F_p \to F_p$ is a function defined by $F(x, y) = x(g(x) + cy)$, where $c \in F_p^*$ and $g : F_p \to F_p$ is any function. The case $g = 0$ and $c = 1$ improves the exponent in [**6**] from 20/19 to 17/16.

0. 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

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

After breakthrough work by Bourgain, Katz and Tao [**2**], with subsequent refinement by Bourgain, Glibichuk and Konyagin [**1**], much work has been done to give a quantitative lower bound on $\max(|A+A|, |AA|)$ for the case $n = 1$ (see e.g., [**4–9**]). It is known that the problem is more complicated in fields not of prime order due to the presence of non-trivial subfields or their dilates. Recently, Tao [**8**] obtained a rigorous formulation of the sum-product phenomenon in arbitrary rings, and

2010 AMS *Mathematics subject classification.* Primary 11B75, Secondary 12E20.
Keywords and phrases. Sum-product estimates, expanding maps.
Received by the editors on September 24, 2008.

DOI:10.1216/RMJ-2011-41-3-941

Katz and the author [**6**] also obtained an analogous result in the sets of fields which are not necessarily of prime order under the hypotheses that 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 (see the Theorem). It is very interesting to try to find bounds which are numerically as strong as possible, and the present paper is an example of this endeavor. In this paper we extend the sum-product theorem in [**6**] to a more general setting and improve the exponent from 19/20 to 17/16. Precisely, we prove

Theorem. *Let $F = F_{p^n}$ be a finite field and A a subset of F so that for any $A' \subset A$ with $|A'| \geq |A|^{15/16}$ 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

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

Then it must be that

$$\max(|A + A|, |F(A, A)|) \gtrapprox |A|^{17/16}$$

where $F : F_p \times F_p \to F_p$ is a function defined by $F(x, y) = x(g(x) + by)$, where $b \in F_p^*$ and $g : F_p \to F_p$ is any function.

1. 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; most of them were proved in [**5, 6**].

Lemma 1.1. *Suppose $A \subset F$ and*

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

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

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

Lemma 1.2. *Suppose $A \subset F$ and $x \in F$ with $x \notin (A-A)/(A-A)$. Then*

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

Lemma 1.3. *Suppose $A \subset F$ with cardinality at least 3 and G is a subfield of F with*

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

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

$$A \subset cG + d.$$

Lemma 1.4. *Let $X, B_1, \ldots, B_k$ be any subsets of F_p. Then there is an $X' \subset X$ with $|X'| > 1/2|X|$ so that*

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

Lemma 1.5. *Let C and D be sets with $|D| \gtrsim |C|/K$ and with $|C+D| \leq K|C|$. Then there is a $C' \subset C$ with $|C'| \geq 9/10|C|$ so that C' can be covered by $\sim K^2$ translates of D. Similarly, there is $C'' \subset C$ with $|C''| \geq 9/10|C|$ so that C'' can be covered by $\sim K^2$ translates of $-D$.*

Proof. To prove the first half of the statement, it suffices to show that we can find one translate of D whose intersection with C is at least $|C|/K^2$. Once we find such a translate, we remove the intersection and then iterate. We stop when the size of the remaining part of C is less than $|C|/10$. To prove the second half of the statement we have to show there is a translate of $-D$ whose intersection with C is at least $|C|/K^2$. First, by Cauchy-Schwartz inequality, we have that

$$|(c,d,c',d') \in C \times D \times C \times D : c+d = c'+d'| \geq \frac{|C|^2|D|^2}{|C+D|},$$

which implies that

$$|(c,d,c',d') \in C \times D \times C \times D : c+d = c'+d'| \geq \frac{|C||D|^2}{K}.$$

The quantity on the left hand side is equal to

$$\sum_{c \in C} \sum_{d' \in D} |(c+D) \cap (C+d')|.$$

Thus we can find $c \in C$ and $d' \in D$ so that

$$|(c+D) \cap (C+d')| \geq \frac{|D|}{K} \gtrsim |C|K^2.$$

Hence, $|(c-d'+D) \cap C| \gtrsim |C|/K^2$ which is just what we wanted to prove. To prove the second half of the statement we start with the inequality

$$\sum_{d \in D} \sum_{c \in C} |(c-D) \cap (C-d)| \geq \frac{|C||D|^2}{K^2}.$$

Proceeding as above, we find $c \in C$ and $d \in D$ such that

$$|(c+d-D) \cap C| \gtrsim |C|/K^2,$$

and the result follows. □

2. Proof of Theorem. We start with $|A+A| \leq K|A|$ and $|F(A,A)| \leq K|A|$. By using Plünnecke's inequality, we can find $A' \subset A$ with $|A'| \gtrsim |A|$ so that

$$|A'+A'+A'| \lesssim K^2|A|$$

and

$$|A'+A'+A'+A'| \lesssim K^3|A|.$$

First, by the Cauchy-Schwartz inequality, we have that

$$\sum_{a\in A'}\sum_{a'\in A'} |a(g(a)+cA') \cap a'(g(a')+cA')| \gtrsim |A'|^3 K.$$

Therefore, following Garaev's arguments [**3**], we can find $A'' \subset A'$ and $a_0 \in A'$ so that

$$|A''| \gtrapprox K^{-\beta}|A'|,$$

for some $\beta \geq 0$ and for every $a \in A''$ we have

$$|a(g(a)+cA') \cap a_0(g(a_0)+cA')| \gtrsim K^{\beta-1}|A|.$$

As in the argument of Garaev, the worst case is $\beta = 0$, so let us assume that for simplicity. Now there are three cases. In the first case, we have that $(A''-A'')/(A''-A'')$ is a field $G \subset F$. If we have $|A''| \lessapprox |A|^{15/16}$, then we already have the desired result since we have $|A''| \gtrapprox |a(g(a)+cA') \cap a_0(g(a_0)+cA')| \gtrsim |A|/K$ which implies $K \gtrapprox |A|^{1/16}$ which is what we wanted. Otherwise, by Lemma 1.3, we have that A'' is contained in an affine image of G so that by hypothesis

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

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

$$\begin{aligned}
|A''|^2 &\lesssim |(a_1-a_2)A'' + (b_1-b_2)A''| \\
&\leq |a_1A'' - a_2A'' + b_1A'' - b_2A''| \\
&= |a_1g(a_1) + a_1cA'' - a_2g(a_2) - a_2cA'' + b_1g(b_1) \\
&\quad + b_1cA'' - b_2g(b_2) - b_2cA''| \\
&= |a_1(g(a_1)+cA'') - a_2(g(a_2)+cA'') + b_1(g(b_1)+cA'') \\
&\quad - b_2(g(b_2)+cA'')|.
\end{aligned}$$

Now we apply Lemma 1.5 to find A''' whose size is at least $6/10$ of A'' so that $a_1(g(a_1)+cA''')$, $a_2(g(a_2)+cA''')$, $b_1(g(b_1)+cA''')$ and $b_2(g(b_2)+cA''')$ can be covered by $\sim K^2$ translates of $a_0(g(a_0)+cA')$, $-a_0(g(a_0)+cA''')$, $a_0(g(a_0)+cA''')$ and $-a_0(g(a_0)+cA''')$ respectively. But then $a_1(g(a_1)+cA''')-a_2(g(a_2)+cA''')+b_1(g(b_1)+cA''')-b_2(g(b_2)+cA''')$ can be covered by $\sim K^8$ translates of $a_0(g(a_0)+cA')+a_0(g(a_0)+cA')+a_0(g(a_0)+cA')+a_0(g(a_0)+cA')$. Since $|a_0(g(a_0)+cA')+a_0(g(a_0)+cA')+a_0(g(a_0)+cA')+a_0(g(a_0)+cA')| = |A'+A'+A'+A'| \lesssim K^3|A|$, by the definition of A'. Thus we get

$$|a_1A'''-a_2A'''+a_3A'''-a_4A'''| \lesssim K^{11}|A|.$$

Therefore

$$|A'|^2 \lesssim K^{11}|A|,$$

which implies that $K \gtrapprox |A|^{1/11} \gtrapprox |A|^{1/16}$, so that we have more than we need in this case. We restrict to the setting where $(A''-A'')/(A''-A'')$ is not a field. Now there are two remaining cases, either

$$\left(\frac{A''-A''}{A''-A''}\right)\left(\frac{A''-A''}{A''-A''}\right) \not\subset \frac{A''-A''}{A''-A''}$$

or

$$\left(\frac{A''-A''}{A''-A''}\right)\left(\frac{A''-A''}{A''-A''}\right) = \left(\frac{A''-A''}{A''-A''}\right), \frac{A''-A''}{A''-A''}+\frac{A''-A''}{A''-A''} \not\subset \frac{A''-A''}{A''-A''}.$$

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

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

which can be rewritten as

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

From this we deduce that for some $a, b, x, y, z, t \in A''$, we have

$$\frac{a-b}{a}\frac{x-y}{z-t} \notin \frac{A''-A''}{A''-A''}.$$

Thus

$$\begin{aligned}|A''|^2 &\leq |(a-b)(x-y)A'' + a(z-t)A''| \\ &\leq |a(x-y)A'' - b(x-y)A'' + a(z-t)A''|.\end{aligned}$$

We now apply Lemma 1.4 with $X = a(x-y)A''$ to get

$$\begin{aligned}|A''|^2 &\lesssim \frac{|aA''-bA''||(x-y)A''+(z-t)A''|}{|A|} \\ &\lesssim |a(g(a)+cA'')-b(g(b)+cA'')||A| \\ &\times \frac{|x(g(x)+cA|A|)-y(g(y)+cA|A|)+z(g(z)+cA|A|)}{|A|} \\ &\quad \frac{-t(g(t)+cA|A|)|}{|A|}.\end{aligned}$$

Proceeding as above, this implies that

$$|A''|^2 \lesssim K^{16}|A|,$$

which implies that $K \gtrapprox |A|^{1/16}$. In the second case, for some $a_i, b_i \in A''$ we have

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

which, in view of $(A''-A'')/(A''-A'')(A''-A)/(A''-A'') = (A''-A'')/(A''-A'')$, implies that there exist elements $a', b', c', d' \in A''$ such that

$$\begin{aligned}\frac{a'-b'}{c'-d'} + 1 &= \frac{b_3-b_4}{a_3-a_4}\frac{a_1-a_2}{b_1-b_2} + 1 \\ &= \frac{b_3-b_4}{a_3-a_4}\left(\frac{a_1-a_2}{b_1-b_2} + a_3 - a_4b_3 - b_4\right) \notin \frac{A''-A''}{A''-A''}.\end{aligned}$$

Thus we have

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

Now by applying Lemma 1.4 , we get

$$|A''|^2 \lesssim \frac{|A+A|}{|A|}|(a'-b')A'' + (c'-d')A''|.$$

Applying the same argument as above, we get

$$|A''|^2 \lesssim K^{12}|A|,$$

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

Acknowledgments. The author wishes to thank Nets Katz for many helpful discussions and pointing out the useful covering lemma (Lemma 1.5).

REFERENCES

1. J. Bourgain, A. Glibichuk and S. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. **73** (2006), 380–398.

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

3. M. Garaev, *An explicit sum-product estimate in* $\mathbf{F}_p$, Internat. Math Res. Notices **2007** (2007).

4. D. Hart, A. Iosevich and J. Solymosi, *Sum product estimates in finite fields via Kloosterman sums*, Inter. Math. Res. Notices **2007** (2007).

5. N. Katz and C-Y Shen, *A slight improvement to Garaev's sum product estimate*, Proc. Amer. Math. Soc. **136** (2008), 2499–2504.

6. ———, *Garaev's inequality in finite fields not of prime order*, Online J. Anal. Comb. **3** (2008).

7. C-Y Shen, *An extension of Bourgain and Garaev's sum-product estimates*, Acta. Arith., to appear.

8. T. Tao, *The sum-product phenomenon in arbitrary rings*, preprint.

9. T. Tao and V. Vu, *Additive combinatorics*, Cambridge University Press, 2006.

Department of Mathematics, Indiana University, Rawles Hall, 831 East Third St, Bloomington, Indiana 47405
Email address: shenc@indiana.edu