EXPLICIT SUM-PRODUCT THEOREMS FOR LARGE SUBSETS OF $\mathbb{F}_p$

Mei-Chu Chang

Abstract. *In this note, we use 'classical' methods to obtain sum-product theorems for subsets $A \subset \mathbb{F}_p$.*

Let A be a subset of a ring. The *sum set* and the *product set* of A are

$$A + A = 2A = \{a + b \,:\, a \in A, \text{ and } b \in A\}$$

and

$$AA = A^2 = \{ab \,:\, a \in A, \text{ and } b \in A\},$$

respectively.

Theorem 1. *Let $A \subset \mathbb{F}_p^*$. Then*

$$|AA|\ |A + A|^2 \geq \frac{1}{2} \min\Big(\frac{|A|^5}{p}, p|A|^2\Big). \tag{1}$$

The following corollary is obvious. It improves on earlier results [HIS], [V], and also slightly on [G].

2000 *Mathematics Subject Classification.* 11B75, 11T23.
Key words. sum set, product set, sum-product estimates.
Research partially financed by the National Science Foundation.

Corollary 2. *Let $A \subset \mathbb{F}_p^*$. Then*

$$\max\left(|A+A|, |AA|\right) \geq \frac{1}{\sqrt[3]{2}} \min\left(\left(\frac{|A|^2}{p}\right)^{1/3}, \left(\frac{p}{|A|}\right)^{1/3}\right)|A|. \tag{2}$$

Theorem 3. *Let $A \subset \mathbb{F}_p^*$. Then*

$$|AA|^2\ |A+A| \geq \frac{1}{2} \min\left(\frac{|A|^5}{p}, (p-1)|A|^2\right). \tag{3}$$

Note that Theorem 3 gives another proof of Corollary 2.

Combining Theorem 1 and Theorem 3, we have

Corollary 4. *Let $A \subset \mathbb{F}_p^*$. Then*

$$|A+A|\ |AA| \geq \frac{1}{\sqrt[3]{4}} \min\left(\frac{|A|^{4/3}}{p^{2/3}}, \left(\frac{p-1}{|A|}\right)^{2/3}\right)|A|^2. \tag{4}$$

Proof of Theorem 1.

Denote $e_p(\xi) = e^{2\pi i \xi/p}$.

Let $f, g : \mathbb{F}_p \to \mathbb{R}$ be functions. We define the following terms

(a.) $\hat{f}(\xi) = \sum_{x \in \mathbb{F}_p} f(x) e_p(-x\xi)$,

(b.) $f * g(x) = \sum_{y \in \mathbb{F}_p} f(x-y)g(y)$.

Then the following are easy to verify:

(c.) $f(x) = \frac{1}{p} \sum_{\xi \in \mathbb{F}_p} \hat{f}(\xi) e_p(x\xi)$,

(d.) $\widehat{f * g}(\xi) = \hat{f}(\xi)\hat{g}(\xi)$,

(e.) $\sum_{\xi \in \mathbb{F}_p} |\hat{f}(\xi)|^2 = \frac{1}{p} \sum_{x \in \mathbb{F}_p} |f(x)|^2$.

For a set $S \subset \mathbb{F}_p$, let $\mathbb{I}_S$ be the indicator function of S. Let $-S = \{-s : s \in S\}$. Then

(f.) $\widehat{\mathbb{I}_{-S}}(\xi) = \overline{\mathbb{I}_S(\xi)}$.

(g.) $\widehat{\mathbb{I}_S}(0) = |S|$.

It follows from the Cauchy-Schwarz inequality and change of variables that we have

$$
\begin{aligned}
|A|^2 &= \sum_{u\in\mathbb{F}_p}\sum_{y\in A}\mathbb{I}_A(u)\,\mathbb{I}_{2A}(u+y)\\
&= \sum_{v\in\mathbb{F}_p}\sum_{y\in A}\mathbb{I}_A(v-y)\,\mathbb{I}_{2A}(v)\\
&\le |A+A|^{\frac{1}{2}}\Big(\sum_{v}\big|\sum_{y\in A}\mathbb{I}_A(v-y)\big|^2\Big)^{\frac{1}{2}}\\
&= |A+A|^{\frac{1}{2}}\Big(\sum_{y_1,y_2\in A}\mathbb{I}_A*\mathbb{I}_{-A}(y_1-y_2)\Big)^{\frac{1}{2}}
\end{aligned}
\tag{5}
$$

Therefore, there exists $y\in A$ such that

$$
\sum_{v\in A}\mathbb{I}_A*\mathbb{I}_{-A}(v-y)\ge\frac{|A|^3}{|A+A|}. \tag{6}
$$

Next, we look at

$$
\sum_{\substack{v\in A\\ z\in A}}\mathbb{I}_A*\mathbb{I}_{-A}(v-y)\,\mathbb{I}_{A^2}(vz)\ge\frac{|A|^4}{|A+A|}. \tag{7}
$$

After change of variables and the Cauchy-Schwarz inequality, the left-hand side of (7) is bounded by

$$
\sum_{\substack{x\in\mathbb{F}_p\\ z\in A}}\mathbb{I}_A*\mathbb{I}_{-A}\Big(\frac{x}{z}-y\Big)\,\mathbb{I}_{A^2}(x)\le|AA|^{\frac{1}{2}}\bigg(\sum_{x\in\mathbb{F}_p}\Big(\sum_{z\in A}(\mathbb{I}_A*\mathbb{I}_{-A})\big(\frac{x}{z}-y\big)\Big)^2\bigg)^{\frac{1}{2}}.
$$

Hence

$$
\sum_{x\in\mathbb{F}_p}\sum_{z_1,z_2\in A}\Big(\mathbb{I}_A*\mathbb{I}_{-A}\Big)\big(\frac{x}{z_1}-y\big)\ \Big(\mathbb{I}_A*\mathbb{I}_{-A}\Big)\big(\frac{x}{z_2}-y\big)\ge\frac{|A|^8}{|A+A|^2\,|AA|}. \tag{8}
$$

We write the Fourier expansion of $\mathbb{I}_A*\mathbb{I}_{-A}$.

$$
\Big(\mathbb{I}_A*\mathbb{I}_{-A}\Big)(u)=\frac{1}{p}\sum_{\xi\in\mathbb{F}_p}\big|\,\widehat{\mathbb{I}_A}(\xi)\big|^2\,e_p(\xi u).
$$

Hence

$$\Big(\mathbb{I}_A * \mathbb{I}_{-A}\Big)\big(\frac{x}{z} - y\big) = \frac{1}{p}\sum_{\xi\in\mathbb{F}_p} \big|\,\widehat{\mathbb{I}_A}(z\xi)\big|^2\, e_p(-z\xi y) e_p(\xi x)$$

and

$$\sum_x \Big(\mathbb{I}_A * \mathbb{I}_{-A}\Big)\big(\frac{x}{z_1} - y\big)\Big(\mathbb{I}_A * \mathbb{I}_{-A}\Big)\big(\frac{x}{z_2} - y\big) \le \frac{1}{p}\sum_{\xi\in\mathbb{F}_p} \big|\,\widehat{\mathbb{I}_A}(z_1\xi)\big|^2 \,\big|\,\widehat{\mathbb{I}_A}(z_2\xi)\big|^2. \qquad (9)$$

It follows from (8) and (9) that

$$\frac{1}{p}\sum_{z_1,z_2\in A}\sum_{\xi\in\mathbb{F}_p} \big|\,\widehat{\mathbb{I}_A}(z_1\xi)\big|^2 \,\big|\,\widehat{\mathbb{I}_A}(z_2\xi)\big|^2 \ge \frac{|A|^8}{|A+A|^2\,|AA|}. \qquad (10)$$

Hence, there exists $z_1 \in A$ such that

$$\begin{aligned}\frac{|A|^7}{|A+A|^2\,|AA|} \le& \frac{1}{p}\sum_{z\in A}\sum_{\xi\in\mathbb{F}_p} \big|\,\widehat{\mathbb{I}_A}(z_1\xi)\big|^2 \,\big|\,\widehat{\mathbb{I}_A}(z\xi)\big|^2 \\ =& \frac{|A|^5}{p} + \frac{1}{p}\sum_{z\in A}\sum_{\xi\in\mathbb{F}_p^*} \big|\,\widehat{\mathbb{I}_A}(z_1\xi)\big|^2 \,\big|\,\widehat{\mathbb{I}_A}(z\xi)\big|^2. \qquad (11)\end{aligned}$$

The second term in (11) is at most

$$\frac{1}{p}\sum_{z\in\mathbb{F}_p}\sum_{\xi\in\mathbb{F}_p^*} \big|\,\widehat{\mathbb{I}_A}(z_1\xi)\big|^2 \,\big|\,\widehat{\mathbb{I}_A}(z\xi)\big|^2.$$

Making a change of variables $z \to \frac{z}{\xi}$ and using Parseval identity, we get

$$\frac{1}{p}\Big(\sum_{\xi\in\mathbb{F}_p^*} \big|\,\widehat{\mathbb{I}_A}(z_1\xi)\big|^2\Big)\,\Big(\sum_{z\in\mathbb{F}_p} \big|\,\widehat{\mathbb{I}_A}(z)\big|^2\Big) = \frac{1}{p}\big(p|A| - |A|^2\big)\, p|A|. \qquad (12)$$

Combining (11) and (12), we have

$$\frac{|A|^7}{|A+A|^2\,|AA|} \le \frac{|A|^5}{p} + |A|^2(p - |A|), \qquad (13)$$

which implies (1). $\square$

Proof of Theorem 3.

We denote the multiplicative convolution of f and g by

$$(f \otimes g)(x) = \sum_y f(xy^{-1}) g(y).$$

One can easily write down the multiplicative versions of (a)-(g).

The starting argument is similar to that of Theorem 1, so we will be brief.

$$\begin{aligned}
|A|^2 &= \sum_{u \in \mathbb{F}_p} \sum_{y \in A} \mathbb{I}_A(u)\, \mathbb{I}_{A^2}(uy) \\
&= \sum_{v \in \mathbb{F}_p} \sum_{y \in A} \mathbb{I}_A(\frac{v}{y})\, \mathbb{I}_{A^2}(v) \\
&\leq |AA|^{\frac{1}{2}} \Big(\sum_{y_1, y_2 \in A} \mathbb{I}_A \otimes \mathbb{I}_{A^{-1}}(\frac{y_1}{y_2}) \Big)^{\frac{1}{2}}
\end{aligned} \tag{14}$$

Therefore, by (14), there exists $y \in A$ such that

$$\sum_{v \in A} \Big(\mathbb{I}_A \otimes \mathbb{I}_{A^{-1}} \Big)(\frac{v}{y}) \geq \frac{|A|^3}{|AA|}. \tag{15}$$

Next, we look at

$$\sum_{\substack{v \in A \\ z \in A}} \Big(\mathbb{I}_A \otimes \mathbb{I}_{A^{-1}} \Big)(\frac{v}{y})\ \ \mathbb{I}_{A+A}(v+z) \geq \frac{|A|^4}{|AA|}. \tag{16}$$

After change of variables and the Cauchy-Schwarz inequality, the left-hand side of (16) is bounded by

$$\sum_{\substack{x \in \mathbb{F}_p \\ z \in A}} \Big(\mathbb{I}_A \otimes \mathbb{I}_{A^{-1}} \Big) \Big(\frac{x-z}{y} \Big)\, \mathbb{I}_{A+A}(x) \leq |A+A|^{\frac{1}{2}} \bigg(\sum_{x \in \mathbb{F}_p} \Big(\sum_{z \in A} (\mathbb{I}_A \otimes \mathbb{I}_{A^{-1}})(\frac{x-z}{y}) \Big)^2 \bigg)^{\frac{1}{2}}.$$

Hence

$$\sum_{x \in \mathbb{F}_p} \sum_{z_1, z_2 \in A} \Big(\mathbb{I}_A \otimes \mathbb{I}_{A^{-1}} \Big)(\frac{x-z_1}{y})\ \Big(\mathbb{I}_A \otimes \mathbb{I}_{A^{-1}} \Big)(\frac{x-z_2}{y}) \geq \frac{|A|^8}{|AA|^2\, |A+A|}. \tag{17}$$

Expanding in multiplicative characters ψ, we have

$$\Big(\mathbb{I}_A \otimes \mathbb{I}_{A^{-1}}\Big)(u) = \frac{1}{p-1}\sum_{\psi} \big|\,\widehat{\mathbb{I}_A}(\psi)\big|^2\ \psi(u).$$

We extend ψ to all of $\mathbb{F}_p$ by setting $\psi(0)=0$. Note that the previous equality remains valid. Hence

$$\Big(\mathbb{I}_A \otimes \mathbb{I}_{A^{-1}}\Big)\big(\frac{x-z}{y}\big) = \frac{1}{p-1}\sum_{\psi} \big|\,\widehat{\mathbb{I}_A}(\psi)\big|^2\ \overline{\psi(y)}\ \psi(x-z)$$

and the left-hand side of (17) is bounded by

$$\frac{1}{(p-1)^2}\sum_{\psi_1,\psi_2} \big|\,\widehat{\mathbb{I}_A}(\psi_1)\big|^2\ \big|\,\widehat{\mathbb{I}_A}(\psi_2)\big|^2 \Big|\sum_{x\in\mathbb{F}_p}\ \sum_{z_1,z_2\in A} \psi_1(x-z_1)\psi_2(x-z_2)\Big|. \tag{18}$$

Denote χ_0 the principal character mod p. In (18), the contribution of $\psi_1=\psi_2=\chi_0$ is

$$\frac{|A|^4}{(p-1)^2}\Big[\big(|A|^2-|A|\big)(p-2)+|A|(p-1)\Big] = \frac{|A|^5}{(p-1)^2}\big[(p-2)|A|+1\big], \tag{19}$$

while the contribution of $\psi_1=\chi_0, \psi_2\neq\chi_0$ or $\psi_1\neq\chi_0, \psi_2=\chi_0$ is at most

$$2\frac{|A|^4}{(p-1)^2}\big(p-1-|A|\big)\big(|A|-1\big). \tag{20}$$

Now assume $\psi_1\neq\chi_0, \psi_2\neq\chi_0$. Then

$$\begin{aligned}
&\sum_{x\in\mathbb{F}_p}\ \sum_{z_1,z_2\in A} \psi_1(x-z_1)\psi_2(x-z_2)\\
=&\sum_{x\in\mathbb{F}_p}\ \sum_{z_1,z_2\in A} \psi_1(x)\psi_2(x+z_1-z_2)\\
=&\sum_{x\in\mathbb{F}_p}\ \sum_{u\in\mathbb{F}_p} \psi_1(x)\psi_2(x+u)\Big(\mathbb{I}_A * \mathbb{I}_{-A}\Big)(u)\\
=&\sum_{x\in\mathbb{F}_p}\ \sum_{u\in\mathbb{F}_p} \psi_1(x)\psi_2(x+u)\Big(\frac{1}{p}\sum_{\xi\in\mathbb{F}_p} \big|\,\widehat{\mathbb{I}_A}(\xi)\big|^2\ e_p(\xi u)\Big|\\
\le&\frac{1}{p}\sum_{\xi\in\mathbb{F}_p} \big|\,\widehat{\mathbb{I}_A}(\xi)\big|^2 \Big|\sum_{x,u\in\mathbb{F}_p} \psi_1(x)\psi_2(x+u)\ e_p(\xi u)\Big|\\
\le&|A|\quad\max_{\xi}\Big|\sum_{x,u\in\mathbb{F}_p} \psi_1(x)\psi_2(u)\ e_p\big(\xi(u-x)\big)\Big|\\
=&|A|\quad\max_{\xi}\Big|\sum_{x} \psi_1(x)e_p(-\xi x)\Big|\ \Big|\sum_{u}\psi_2(u)\ e_p(\xi u)\Big|\\
\le&p\ |A|.
\end{aligned} \tag{21}$$

(The last inequality is by the Gauss sum estimate.) Hence the corresponding contribution to (18) is bounded by

$$\frac{p|A|^3}{(p-1)^2}\big(p-1-|A|\big)^2. \tag{22}$$

From (17)-(20), and (22), it follows that

$$\begin{aligned}
&\frac{|A|^8}{|AA|^2\,|A+A|}\\
\leq&\frac{|A|^5}{(p-1)^2}\left[(p-2)|A|+1\right]+2\frac{|A|^4}{(p-1)^2}(p-1-|A|)(|A|-1)+\frac{p|A|^3}{(p-1)^2}(p-1-|A|)^2\\
<&\frac{|A|^6}{p-1}+p\,|A|^3.
\end{aligned}$$

The last inequality holds because

$$-3\frac{|A|^5(|A|-1)}{(p-1)^2}+2\frac{|A|^4(|A|-1)}{(p-1)}-\frac{2p|A|^4}{p-1}+\frac{p|A|^5}{(p-1)^2}<0. \tag{23}$$

.

Now it is clear that (3) follows from (23). □

Acknowledgement. The author would like to thank the referees for many helpful comments.

References

[G]. M.Z. Garaev, *An explicit sum-product estimate in* $\mathbb{F}_p$, Int. Math. Res. Notices (to appear).

[HIS]. D. Hart, A. Iosevich, J. Solymosi, *Sum product estimates in finite fields via Kloosterman sums*, Int. Math. Res. Notices (to appear).

[V]. V. Vu, *Sum-product estimates via directed expanders*, Mathematical Research Letters 15 (2008), 375-388.