International Journal of Pure and Applied Mathematics
Volume 67 No. 4 2011, 423-430

REMARKS ON THE EXPONENTIAL SUM-PRODUCT PROBLEMS

Junhuai Zhang[1 §], Yuan Yi[2]
[1,2]Research Center for Basic Science
Xi'an Jiaotong University
Xi'an, 710049, P.R. CHINA
[1]e-mail: zhang_junhuai@163.com
[2]e-mail: yuanyi@mail.xjtu.edu.cn

Abstract: Looking back upon the sum-product problems and the exponential sum-product problems, the main results on exponential sum-product problems on the finite field $\mathbb{F}_p$ of prime order are given firstly by I.E. Shparlinski. In this paper, we give other relative results about it.

AMS Subject Classification: 11B30
Key Words: sum-product problems, exponential sum, finite field

1. Introduction

There are three stages of the problems involved: The sum set problems, the sum-product problems, and the exponential sum-product problems.

Stage I. The sum set problems.

Let $\mathcal{S}_1, \mathcal{S}_2$ be subsets of a group $\mathbb{G}$, denoting its operation as addition, we define the sum of two sets as

$$\mathcal{S}_1 + \mathcal{S}_2 = \{x_1 + x_2 \mid x_1 \in \mathcal{S}_1,\ x_2 \in \mathcal{S}_2\}.$$

If $\mathbb{G}$ is the ring $\mathbb{Z}$ of integers, it is easy to prove that

$$|\mathcal{S}_1 + \mathcal{S}_2| \geq |\mathcal{S}_1| + |\mathcal{S}_2| - 1.$$

The "=" holds iff the two subsets are arithmetic progressions with the same

Received: December 18, 2010

§Correspondence author

common difference.

In 1813 Cauchy [5] proved the first theorem in the sum problems, that is, let $\mathbb{G}$ be the finite field $\mathbb{F}_p = \mathbb{Z}/(p)$, then

$$|\mathcal{S}_1 + \mathcal{S}_2| \geq \min(|\mathcal{S}_1| + |\mathcal{S}_2| - 1, p).$$

In 1934, this theorem was rediscovered by Davenport [8] and is known as the Cauchy-Davenport Theorem, which can be easily generated to the ring $\mathbb{Z}/(m)$ for any interger m, see Mann [19] for a refined proof.

The theorem was generalized in various ways to general Abelian groups, and even noncommutative groups, for more details one can see Mann [18] and the references therein.

We can call these the problems of sum set cardinality, or the sum set problems.

Since the groups considered in the sum set problems in the early time are also rings, it is natural to consider the two operations in the ring at the same time, the sum set problems were developed to the sum-product problems in 1970's.

Stage II. The sum-product problems.

Let $\mathcal{A}, \mathcal{B}$ be subsets of a ring $\mathbf{R}$, and $h \geq 2$ be an integer, taking notations as follows:

$$\mathcal{A} + \mathcal{B} = \{x + y |\ x \in \mathcal{A}\ \ y \in \mathcal{B}\},$$

$$h\mathcal{A} = \{x_1 + x_2 + ... + x_h |\ x_1, x_2, ..., x_h \in \mathcal{A}\},$$

and

$$\mathcal{A}^h = \{x_1 x_2 ... x_m |\ x_1, x_2, ..., x_h \in \mathcal{A}\},$$

and

$$E_h(\mathcal{A}) = \max(|h\mathcal{A}|, |\mathcal{A}^h|).$$

We can begin with the observation that: In the ring $\mathbb{Z}$ of integers, if $\mathcal{A}$ is a arithmetic progression, we have $|2\mathcal{A}| = 2|\mathcal{A}| - 1$, but $|\mathcal{A}^2| \geq |\mathcal{A}|^{2-\varepsilon}$, where ε is any fixed positive number; if $\mathcal{A}$ is a geometric progression, we have $|\mathcal{A}^2| = 2|\mathcal{A}| - 1$, but $|2\mathcal{A}| \geq |\mathcal{A}|^{2-\varepsilon}$. That is, $|2\mathcal{A}|$ and $|\mathcal{A}^2|$ cannot be small at the same time.

In 1976, Erdös [11] gave a conjecture that: $E_2(\mathcal{A}) \geq c(\varepsilon)|\mathcal{A}|^{2-\varepsilon}$ for any $\varepsilon > 0$.

In 1983, Erdös et al [12] got the following result: There exist two positive real numbers c_1, c_2, such that the following estimate holds:

$$|\mathcal{A}|^{1+c_1} \leq E_2(\mathcal{A}) \leq |\mathcal{A}|^2 \exp\{-c_2 \log(|\mathcal{A}|/\log\log(|\mathcal{A}|))\}.$$

Such kind of problems had nearly been forgotten for more than ten years, before in the year of 1997 Nathanson [20] published his result: Let $\mathcal{A}$ be a nonempty, finite set of positive integers, then the estimates

$$|E_2(\mathcal{A})| \geq c|\mathcal{A}|^{\frac{32}{31}},$$

hold, where the constant $c = 0.00028....$ This is the first time to get the estimates $|E_2(\mathcal{A})| \gg |\mathcal{A}|^{1+\delta}$ for an explicit constant; soon the constant $\delta = 1/31$ was improved to $1/15$ by Ford [13], and to $1/4$ by Elekes [10] who also extend the result to the real number, and to $\frac{3}{11+\epsilon}$ by Solymosi [22] which is the best estimates for real and complex numbers until now.

The analogy of this conjecture in finite field are also far from being solved. There are many results and applications on them.

It must be mentioned that, in the year of 2004, by using the result of Edgar et al [9], Bourgain et al [4] issued a celebrated paper in which they bring up a problem about the sum-product estimate, they gave the following result:

Proposition 1. *Suppose $\delta > 0$ and $\mathcal{A}$ is a subset of F_p of cardinality between p^{δ} and $p^{1-\delta}$, then there is some $\varepsilon > 0$ such that $E_2(\mathcal{A}) \geq |\mathcal{A}|^{1+\varepsilon}$.*

And some important applications of it were also given. This is a very important breakthrough in this direction and has motivated many researches on it and some new results appeared, such as Bourgain [2], Garaev [15] and references therein.

In 2007, Hart et al [17] obtained an explicit value of in certain ranges of $|\mathcal{A}|$, that is

$$E_2(\mathcal{A}) \gg \begin{cases} |\mathcal{A}|^{\frac{3}{2}} p^{-\frac{1}{4}}, & \text{if } p^{\frac{1}{2}} \lesssim |\mathcal{A}| \lesssim p^{\frac{7}{10}}, \\ |\mathcal{A}|^{\frac{2}{3}} p^{\frac{1}{3}}, & \text{if } p^{\frac{7}{10}} \lesssim |\mathcal{A}| \lesssim p. \end{cases}$$

In particular, if $|\mathcal{A}| \sim p^{\frac{7}{10}}$, then

$$E_2(\mathcal{A}) \gg |\mathcal{A}|^{\frac{8}{7}}.$$

Later in the same year, Garaev [15] obtained an explicit sum-product estimate for any range of $|\mathcal{A}| > 1$

$$E_2(A) \gg \min\left\{ \frac{|\mathcal{A}|^{\frac{15}{14}} |\mathcal{A}|^{\frac{1}{7}} p^{-\frac{1}{14}}}{(\log|\mathcal{A}|)^{\frac{2}{7}}}, \frac{|\mathcal{A}|^{\frac{11}{12}} p^{\frac{1}{12}}}{(\log|\mathcal{A}|)^{\frac{1}{3}}} \right\}.$$

In particular, if $1 < |\mathcal{A}| < p^{\frac{7}{13}} \log p^{\frac{7}{13}}$, we have

$$E_2(\mathcal{A}) \gg \frac{|\mathcal{A}|^{\frac{15}{14}}}{(\log|\mathcal{A}|)^{\frac{2}{7}}}.$$

Last year Tao [24] extended these results to arbitrary rings $\mathcal{R}$ which is not necessary to be commutative or to contain a multiplicative identity 1, just making the assumption that $\mathcal{A}$ encounters few zero-divisors of $\mathcal{R}$. His result is like that form: If $\mathcal{A}$ is a finite nonempty subset of a ring $\mathcal{R}$ for which certain additive and multiplicative combinations of $\mathcal{A}$ are small, and $\mathcal{A}$ is non-degenerate in the sense described above, then $\mathcal{A}$ can be efficiently contained in a ring, or a slight modification of a ring.

In the same year, Croot et al [7] got some result in $\mathbb{C}[x]$ unconditionally. And for other directions, the readers can see references Szemerédi [23] and Chang [6], etc.

Stage III. The exponential sum-product problems.

In 2008, I. Shparlinski [21] studied the exponential sum-product problems and got some results by using the results on double exponential sums of Garaev et al [16] and Bourgain [2]. Let p a sufficient large prime and g a fixed element in the finite field $\mathbb{F}_p$ of multiplicative order T. Denote by $\mathbb{Z}_m$ the residue ring modulo m, and $\mathbb{Z}_m^*$ the set of multiple units of $\mathbb{Z}_m$.

Let $\mathcal{A}, \mathcal{B} \subseteq \mathbb{Z}_T^*$. Consider the sets

$$\mathcal{U} = \{g^{ab} : a \in \mathcal{A}, b \in \mathcal{B}\},\ \mathcal{V} = \{g^a + g^b : a \in \mathcal{A}, b \in \mathcal{B}\}.$$

Shparlinski got the following two propositions.

Proposition 2. *For $T \geq p^{\frac{1}{2}+\varepsilon}$, integer $v \geq 1$, the sets $\mathcal{U}$ and $\mathcal{V}$ defined as above, as $p \to \infty$, then*

$$\max\{|\mathcal{U}|, |\mathcal{V}|\} \geq \min\{\sqrt{p|\mathcal{B}|}, |\mathcal{A}|^{\alpha_v}|\mathcal{B}|^{\beta_v}T^{-\tau_v}p^{-\rho_v}\}p^{o(1)},$$

where ε is any fixed positive number,

$$\alpha_v = \frac{v^2+2v}{3v^2+2v-1}, \quad \beta_v = \frac{2v}{3v-1},$$
$$\tau_v = \frac{1}{3v-1}, \quad \rho_v = \frac{v}{2(3v^2+2v-1)}.$$

Proposition 3. *For any $\varepsilon > 0$ and $\delta > 0$, there are some $\eta > 0$ and $\kappa > 0$ such that for $T \geq p^{\varepsilon}$ and arbitrary sets $\mathcal{A}, \mathcal{B} \subseteq Z_T^*$ such that*

$$T^{1-\delta} \geq |\mathcal{A}|, \quad |\mathcal{B}| \geq T^{\delta+\eta} \quad (\text{as } p \to \infty),$$

then for the sets $\mathcal{U}, \mathcal{V}$ as above,

$$\max\{|\mathcal{U}|, |\mathcal{V}|\} \geq \max\{|\mathcal{A}|, |\mathcal{B}|\}p^{\kappa}.$$

2. Some New Results

By checking the proofs of Proposition 1 and Proposition 2 in detail, we find that the condition $\mathcal{A} \subseteq \mathbb{Z}_T^*$ cannot be changed since the invertibility of the elements in $\mathcal{A}$ is needed, but $\mathcal{B} \subseteq \mathbb{Z}_T^*$ can be replaced by $\mathcal{B} \subseteq \mathbb{Z}_T$.

Now we consider the pairs of sets

$$\mathcal{U}_1 = \{g^{ab} : a \in \mathcal{A}, b \in \mathcal{B}\},\ \mathcal{V}_1 = \{g^a - g^b : a \in \mathcal{A}, b \in \mathcal{B}\},$$

or

$$\mathcal{U}_2 = \{g^{b/a} : a \in \mathcal{A}, b \in \mathcal{B}\},\ \mathcal{V}_2 = \{g^{\frac{1}{a}} - g^b : a \in \mathcal{A}, b \in \mathcal{B}\},$$

or

$$\mathcal{U}_3 = \{g^{\frac{b}{a}} : a \in \mathcal{A}, b \in \mathcal{B}\},\ \mathcal{V}_3 = \{g^a + g^b : a \in \mathcal{A}, b \in \mathcal{B}\},$$

or

$$\mathcal{U}_4 = \{g^{\frac{b}{a}} : a \in \mathcal{A}, b \in \mathcal{B}\},\ \mathcal{V}_4 = \{g^a - g^b : a \in \mathcal{A}, b \in \mathcal{B}\}.$$

For each pair of such sets, we can get some similar results as in Proposition 2 and Proposition 3 by the similar methods. Here we list the results and give a brief proof of them.

Theorem 4. *For the case $T \geq p^{\frac{1}{2}+\varepsilon}$, for integer $v \geq 1$ and for the sets $\mathcal{U}_4$ and $\mathcal{V}_4$ defined as above, as $p \to \infty$, we have*

$$\max\{|\mathcal{U}_4|,\ |\mathcal{V}_4|\} \geq \min\{\sqrt{p|\mathcal{B}|}, |\mathcal{A}|^{\alpha_v}|\mathcal{B}|^{\beta_v}T^{-\tau_v}p^{-\rho_v}\}p^{o(1)},$$

where

$$\alpha_v = \frac{v^2+2v}{3v^2+2v-1}, \quad \beta_v = \frac{2v}{3v-1},$$
$$\tau_v = \frac{1}{3v-1}, \quad \rho_v = \frac{v}{2(3v^2+2v-1)}.$$

Theorem 5. *Under the same notations and conditions of Theorem 4, the same results also hold for each pairs $\mathcal{U}_1, \mathcal{V}_1$, $\mathcal{U}_2, \mathcal{V}_2$, and $\mathcal{U}_3, \mathcal{V}_3$.*

Proof of Theorem 4. Consider the equation over $\mathbb{F}_p$

$$-u^{a_1} + g^{a_2} = v, \quad a_1, a_2 \in \mathcal{A}, \quad u \in \mathcal{U}_4, \quad v \in \mathcal{V}_4$$

Call J the number of solutions. Since $(a_1, a_2, u, v) = (a_1, a_2, g^{\frac{b}{a_1}},\ g^{a_2} - g^b)$, $a_1, a_2 \in \mathcal{A}$, $b \in \mathcal{B}$ are pairwise distinct solutions to the equation above, we have

$$J \geq |\mathcal{A}|^2|\mathcal{B}|.$$

To get the upper bound on J, we write

$$\begin{aligned} J &= \sum_{a_1,a_2\in\mathcal{A}}\sum_{u\in\mathcal{U}_4}\sum_{v\in\mathcal{V}_4}\frac{1}{p}\sum_{\lambda=0}^{p-1}e_p(\lambda(-u_1^a+g_2^a-v)) \\ &= \frac{1}{p}\sum_{\lambda=0}^{p-1}\sum_{a_1\in\mathcal{A}}\sum_{u\in\mathcal{U}_4}e_p(-\lambda u^{a_1})\sum_{a_2\in\mathcal{A}}e_p(\lambda g^{a_2})\sum_{v\in\mathcal{V}_4}e_p(-\lambda v). \end{aligned}$$

Separating the term corresponding to $\lambda=0$, we have

$$J=\frac{|\mathcal{A}|^2|\mathcal{U}_4||\mathcal{V}_4|}{p}+\frac{1}{p}\sum_{\lambda=1}^{p-1}\sum_{a_1\in\mathcal{A}}\sum_{u\in\mathcal{U}_4}e_p(-\lambda u^{a_1})\sum_{a_2\in\mathcal{A}}e_p(\lambda g^{a_2})\sum_{v\in\mathcal{V}_4}e_p(-\lambda v).$$

By using the result of Garaev et al [16]

$$W(\lambda,\mathcal{R},\mathcal{S})=\sum_{r\in\mathcal{R}}\sum_{s\in\mathcal{S}}e_p(\lambda g^{rs})\le|\mathcal{R}|^{1-\frac{1}{2v}}|\mathcal{S}|^{1-\frac{1}{2v+2}}T^{\frac{1}{2v}}p^{\frac{1}{4v}+o(1)},$$

and

$$\begin{aligned} &\sum_{\lambda=1}^{p-1}|\sum_{a_2\in\mathcal{A}}e_p(\lambda g^{a_2})\sum_{v\in\mathcal{V}_4}e_p(-\lambda v)|\le\sum_{\lambda=0}^{p-1}|\sum_{a_2\in\mathcal{A}}e_p(\lambda g^{a_2})\sum_{v\in\mathcal{V}_4}e_p(-\lambda v)| \\ \le\ &\sqrt{\sum_{\lambda=0}^{p-1}|\sum_{a_2\in\mathcal{A}}e_p(\lambda g^{a_2})|^2}\sqrt{\sum_{\lambda=0}^{p-1}|\sum_{v\in\mathcal{V}_4}e_p(-\lambda v)|^2}=p\sqrt{|\mathcal{A}||\mathcal{V}_4|}, \end{aligned}$$

we obtain

$$\begin{aligned} &\frac{1}{p}\sum_{\lambda=1}^{p-1}\sum_{a_1\in\mathcal{A}}\sum_{u\in\mathcal{U}_4}e_p(-\lambda u^{a_1})\sum_{a_2\in\mathcal{A}}e_p(\lambda g^{a_2})\sum_{v\in\mathcal{V}_4}e_p(-\lambda v) \\ \le\ &\frac{1}{p}\sum_{\lambda=1}^{p-1}|\sum_{a_1\in\mathcal{A}}\sum_{u\in\mathcal{U}_4}e_p(-\lambda u^{a_1})||\sum_{a_2\in\mathcal{A}}e_p(\lambda g^{a_2})\sum_{v\in\mathcal{V}_4}e_p(-\lambda v)| \\ \le\ &|\mathcal{U}_4|^{1-\frac{1}{2v}}|\mathcal{A}|^{1-\frac{1}{2v+2}}T^{\frac{1}{2v}}p^{-1+\frac{1}{4v}+o(1)}|\sum_{a_2\in\mathcal{A}}e_p(\lambda g^{a_2})\sum_{v\in\mathcal{V}_4}e_p(-\lambda v)| \\ \le\ &|\mathcal{U}_4|^{1-\frac{1}{2v}}|\mathcal{V}_4^{\frac{1}{2}}||\mathcal{A}|^{\frac{3}{2}-\frac{1}{2v+2}}T^{\frac{1}{2v}}p^{\frac{1}{4v}+o(1)}. \end{aligned}$$

Hence

$$|\mathcal{A}|^2|\mathcal{B}|\le J\le\frac{|\mathcal{A}|^2M^2}{p}+M^{\frac{3}{2}-\frac{1}{2v}}|\mathcal{A}|^{\frac{3}{2}-\frac{1}{2v+2}}T^{\frac{1}{2v}}p^{\frac{1}{4v}+o(1)},$$

where $M = \max\{\mathcal{U}_4, \mathcal{V}_4\}$. From the last two inequations we complete the proof. □

Note. Shparlinski [21] provided an problem, that means the exponential sum-product problems in finite field of prime order can be generated to the ring $\mathbb{Z}_m$ by using the results of Bourgain [3], and Friedlander [14], where m is any nonzero integer. But it is even hard to the case when $m = p^k$ is a prime power, since for the ring $\mathbb{Z}_{p^k}$ we cannot use Weil's estimate to the key triangle sums appearing in the proof of $W(\lambda, \mathcal{R}, \mathcal{S})$. These are still open problems.

References

[1] J. Bourgain, On the Erdös-Volkmann and Katz-Tao ring conjectures, *Geom. Funct. Anal.*, **13** (2003), 334-365.

[2] J. Bourgain, Estimates on exponential sums related to Diffie-Hellman distributions, *Geom. Funct. Anal.*, **15** (2005), 1-34.

[3] J. Bourgain, Exponential sum estimates in finite commutative rings and applications, *J. Anal. Math.*, **101** (2007), 325-355.

[4] J. Bourgain, N. Katz, T. Tao, A sum-product theorem in finite fields and applications, *Geom. Funct. Anal.*, **14** (2004), 27-57.

[5] Cauchy, Recherche sur les nombres, *J. Ecole Polytechn.*, **9** (1813), 99-106.

[6] M.C. Chang, Additive and multiplicative structure in matrix spaces, *Comb. Probab. Comput.*, **16** (2007), 219-238.

[7] E. Croot, D. Hart, On sums and products in C[x], *Preprint.*

[8] H. Davenport, On the addition of residue classes, *J. London Math. Soc.*, **10** (1935), 30-32.

[9] G.A. Edgar, C. Miller, Borel subrings of the reals, *Proc. Amer. Math. Soc.*, **131** (2003), 1121-1129.

[10] G. Elekes, On the number of sums and products, *Acta Arith.*, **81** (1997), 365-367.

[11] P. Erdös, *Problems and Results on Combinatorial Number Theory III, Number Theory Day*, Lecture Notes in Math., Volume 626, Springer-Verlag, Berlin (1977).

[12] P. Erdös, E. Szemerédi, *On Sums and Products of Integers*, Studies in Pure Mathematics, Birkhäuser, Basel (1983).

[13] K. Ford, Sums and products from a finite set of real numbers, *Ramanujan J.*, **2** (1998), 59-66.

[14] J.B. Friedlander, S. Konyagin, I.E. Shparlinski, Some doubly exponential sums over Zm, *Acta Arithm.*, **105** (2002), 349-370.

[15] M.Z. Garaev, An explicit sum-product estimate in $\mathbf{F}_p$, *Int. Math. Res. Notices*, **2007** (2007), 1-11.

[16] M.Z. Garaev, A.A. Karatsuba, New estimates of double trigonometric sums with exponential functions, *Arch. Math.*, **87** (2006), 33-40.

[17] D. Hart, A. Iosevich, J. Solymosi, Sum product estimates in finite fields via Kloosterman sums, *Int. Math. Res.* (2007), 1-14.

[18] H.B. Mann, *The Addition Theorems of Group Theory and Number Theory*, Interscience, New York (1965).

[19] H.B. Mann, Additive group theory – a progress report, *Bull. Amer. Math. Soc.*, **79** (1973), 1069-1075.

[20] M.B. Nathanson, On sums and products of integers, *Proc. Amer. Math. Soc.*, **125** (1997), 9-16.

[21] I.E. Shparlinski, On the exponential sum-product problem, *Indag. Mathem.*, **19** (2008), 325-331.

[22] J. Solymosi, On the number of sums and products, *Bull. London Math. Soc.*, **37** (2005), 491-494.

[23] E. Szemerédi, W.T. Trotter, Extremal problems in discrete geometry, *Combinatorica*, **3** (1983), 381-392.

[24] T. Tao, The sum-product phenomenon in arbitrary rings, *Preprint.*