SET ADDITION AND SET MULTIPLICATION

M.-C. Chang

Section 0. Introduction

Let A be a subset of a ring with cardinality $|A| = N$. The *sum set* and the *product set* are $2A = A + A = \{a_1 + a_2 \mid a_i \in A\}$ and $A^2 = AA = \{a_1 a_2 \mid a_i \in A\}$. The study of sum-product sets is to estimate the sizes of $2A$ and A^2 asymptotically when N is very large. Since Erdős and Szemerédi conjectured that if $A \subset \mathbb{Z}$, at least one of $|2A|$ and $|A^2|$ should be bigger than cN for any constant c, a lot of work has been done in this subject. In this paper, we give a survey of some of the main results in [C1]-[C5], and [BC1], [BC2]. In Section 1, we also put together the ideas in [C2]-[C4] and give a uniform treatment to some of the results there. Of particular importance is the role of Freiman's Theorem and the Subspace Theorem. In Section 2, we consider the noncommutative analogue in matrix spaces. In Section 3, we report on results of sum-product theorems for residue classes, especially prime fields. The results have striking applications to the theory of exponential sums, in particular Gauss sums of large degrees. In Section 4, we present a new and simpler proof of the Generalized Gauss sums Theorem for prime modulus [BGK], which is also included in the introduction of [BC2].

Section 1. Subsets of numbers

A well-known conjecture by Erdös and Szemerédi [ES] for $A \subset \mathbb{Z}$ is that $2A$ and A^2 cannot both be small. Precisely,

Conjecture 1. $\min_{|A|=N} |2A| + |A^2| > c_\varepsilon N^{2-\varepsilon}$, *for all* $\varepsilon > 0$.

More generally, for a fixed integer $h \geq 2$, let hA (respectively, A^h) be the set of sums (resp. products) of h elements in A. Erdös and Szemerédi made the following conjecture.

Conjecture 1′. $\forall h \geq 2$, $\min_{|A|=N} |hA| + |A^h| > c_{\varepsilon,h} N^{h-\varepsilon}$, *for all* $\varepsilon > 0$.

What they proved is the following

Theorem. (Erdös-Szemerédi) *If* $A \subset \mathbb{R}$ *is a finite set of real numbers, then*

$$|2A| + |A^2| > c|A|^{1+\delta}, \tag{1.1}$$

where $\delta > 0$ *is an absolute constant.*

Terminology. We say the sum-product theorem is true for a set A, if (1.1) holds.

Results with explicit δ are: $\delta = \frac{1}{31}$ by Nathanson [N], $\delta = \frac{1}{6}$ by Chen [Ch], $\delta = \frac{1}{15}$ by Ford [F], $\delta = \frac{1}{4}$ by Elekes [E], and $\delta = \frac{3}{11+\varepsilon}$ by Solymosi [S].

One approach to the conjecture is to use incidence geometry.

Szemerédi-Trotter Theorem. *Let* S *be a set of* k *points, and let* $L_1, \cdots, L_\ell$ *be* ℓ *lines, each containing* N *points in* S. *Then* k, ℓ, N *satisfy*

$$k^2 > c\, \ell N^3.$$

Elekes obtained his bound by taking $S = A^2 \times 2A$ and the N^2 lines

$$L_{xy} = \{(xz, y + z) \mid z \in \mathbb{R}\}, \forall x, y \in A.$$

Clearly, each line contains N points in S. Hence $(|A^2|\ |2A|)^2 > cN^2N^3$.

So far Solymosi obtained the best bound by applying Szemerédi-Trotter Theorem repeatedly.

Problem 1. Improve Solymosi's bound.

Recently, Elekes and Ruzsa [ER] established the following general inequality

$$|2A|^4\ |A^2|\ \log N > N^6 \tag{1.2}$$

again using the Szemerédi-Trotter Theorem. As a consequence of (1.2), it follows that Conjecture 1 holds if we assume moreover $|2A| < \alpha|A|$.

In the spirit of 'few products, many sums' and 'few sums, many products' we have the following results.

Theorem 1.a. ([C2], Theorem 1) *For all $h \geq 2$, if $|A^2| < \alpha N$, and $A \subset \mathbb{Z}$, then $|hA| > cN^h$, where $c = (2h^2 - h)^{-h\alpha}$.*

Theorem 1.b. ([C3], Theorem 2) *For all $h \geq 2$, $\varepsilon > 0$, if $|2A| < \alpha N$, and $A \subset \mathbb{C}$, then $|A^h| > cN^{h-\varepsilon}$, where $c = c(h, \alpha, \varepsilon)$.*

Little is known about Conjecture 1'. Elekes, Nathanson and Ruzsa have the following inequality involving $|hA|$ and $|A^h|$.

Elekes-Nathanson-Ruzsa [ENR]

$$|hA|\,|A^h| > cN^{3-2^{1-h}}$$

Hence they made the following conjecture which was also conjectured by Konyagin while working on Gauss sums.

E-N-R-Konyagin Conjecture. $\forall b \in \mathbb{N}, \exists\, h = h(b)$ *such that* $|hA|\,|A^h| > c|A|^b$.

Theorem BC. (Bourgain-Chang [BC1]) *E-N-R-Konyagin Conjecture holds for $A \subset \mathbb{Z}$, with $h \sim C^{b^4}$.*

Remark. In [BC1] the authors did not attempt for the best dependence of h on b.

Problem 2. Find the optimal dependence between h and b.

The next proposition is the key ingredient of Theorem BC. The proof of the proposition relies on careful study of elementary but nontrivial graph theory. First, we will give a simplified definition of the Λ_q constant of a given finite set. (cf [R])

Notation. $e(\theta) = e^{2\pi i\theta}$

Definition. *Let $A \subset \mathbb{Z}$ be finite. The Λ_q constant of A is*

$$\lambda_{q,A} = \frac{\|\sum_{a\in A} e(ax)\|_q}{\sqrt{|A|}}$$

Proposition 1.1. [BC] *Given $\varepsilon > 0$ and $q > 2$, $\exists\ \delta = \delta(q, \varepsilon)$ such that if $A \subset \mathbb{Z}$, $|A^2| < |A|^{1+\varepsilon}$, then*

$$\lambda_q(A) < |A|^{\delta},$$

where $\delta \to 0$, if $\varepsilon \to 0$. Therefore, $\|\sum_{a\in A} e(ax)\|_q < |A|^{\delta+\frac{1}{2}}$.

To generalize Erdös-Szemerédi Conjecture to sums and products of different sets, Solymosi asked the following question.

Question. (Solymosi) $\exists\, c > 0$ *such that* $\forall N \in \mathbb{Z}^+$, $\exists\, A, B, C$ *with* $|A| = |B| = |C| = N$, $|A+B| < N^{2-c}$, *and* $|AC| < N^{2-c}$?

Inspired by Solymosi's question, we proved the following theorems.

Theorem 1.c. ([C4], Theorem 1) *Let* $A \subset \mathbb{Z}$ *with* $|A^2| < |A|^{1+\varepsilon}$. *Then* $\forall B \subset \mathbb{Z}$ *and* $\forall h \in \mathbb{N}$ *we have*

$$|hA + B| > |A|^h\ |B|\ (|A| + |B|)^{-\delta_h(\varepsilon)},$$

where $\delta_h(\varepsilon) \to 0$ *as* $\varepsilon \to 0$.

Theorem 1.d. ([C4], Theorem 2) *Let* $A \subset \mathbb{R}$ *with* $|A^2| < K|A|$. *Then* $\forall B \subset \mathbb{R}$, $\forall h \in \mathbb{N}$ *we have*

$$|hA + B| > |A|^h\ |B|\ (|A| + |B|)^{-\varepsilon},\ \forall \varepsilon$$

Theorem 1.e. ([C4], Theorem 3) *Let* $A \subset \mathbb{R}_+$ *with* $|2A| < K|A|$. *Then* $\forall B \subset \mathbb{R}_+$, $\forall h \in \mathbb{N}$, *we have*

$$|A^h B| > c_h(K, \varepsilon)\ |A|^h |B|\ \big(|A| + |B|\big)^{-\varepsilon}$$

We will outline the general idea of the proofs of Theorems 1.a - 1.e. To reduce the number of constants, we describe the case when $h = 2$ for Theorem 1.a and $h = 1$ for Theorems 1.c - 1.e. The argument for the general case is identical.

Let $r(n) = |\{(a, b) \in A \times B \mid a + b = n\}|$. Then $|A|\ |B| = \sum_{n \in A+B} r(n)$.

The following are easy to check by Parseval equality, Hőlder's inequality, and our definition of the Λ_q constant.

(1). $|A + B| \geq \frac{|A|^2 |B|^2}{\sum r(n)^2}$

(2). $\sum r(n)^2 \leq \|(\sum_{a \in A} e(ax))^2\|_q \quad \|(\sum_{b \in B} e(bx))^2\|_p$, where $\frac{1}{p} + \frac{1}{q} = 1$, p, q to be chosen.

(3). $\|(\sum_{a \in A} e(ax))^2\|_q = (\|\sum_{a \in A} e(ax)\|_{2q})^2 \leq (\lambda_{2q,A}\ |A|^{\frac{1}{2}})^2$

(4). $(\|(\sum_{b \in B} e(bx))^2\|_p)^p \leq \|\sum_{b \in B} e(bx)\|_\infty^{2p-2} \quad \int |\sum_{b \in B} e(bx)|^2 \leq |B|^{2p-1}$

Hence putting (1)-(4) together, we have

$$|A + B| \geq \frac{|A|\ |B|^{1-\frac{1}{q}}}{\lambda_{2q,A}^2} \tag{1.3}$$

and we need to have an upper bound on $\lambda_{2q,A}$.

For Theorem 1.c, we take $K = N^{\varepsilon}$ in Proposition 1.1, and choose q such that $\frac{1}{q}$ is as small as possible. Hence $2\delta + \frac{1}{q} \to 0$ as $\varepsilon \to 0$.

To prove Theorem 1.a, we take $A = B$ in (1), $p = q = 2$ in (2), and skip (4). Hence

$$|A + A| \geq \frac{|A|^2|A|^2}{(\lambda_{4,A}|A|^{\frac{1}{2}})^4} \geq \frac{|A|^2}{36^{\alpha}}.$$

The second inequality follows from the proposition below which was shown by simple combinatorics. (See [C2], the proof of Proposition 6.)

Proposition 1.2. *Let $A \subset \mathbb{Z}$ with $|A| = N$ and $|A^2| < \alpha N$. Then*

$$\lambda_{2h,A} < (2h^2 - h)^{\frac{\alpha}{2}}.$$

Therefore, $\| \sum_{a \in A} e(ax)\|_{2h} < (2h^2 - h)^{\frac{\alpha}{2}} N^{\frac{1}{2}}$.

Remark. In this proposition α is viewed as a much smaller constant comparing to N.

In Theorem 1.d we deal with real numbers. To be able to use (1.3), in the definition of the L_p-norm $\|f\|_p$, we replace $\int f$ by the *mean* of almost periodic functions,

$$\int' f = \lim_{T \to \infty} \frac{1}{T} \int_0^T f,$$

and we consider $\sum e^{iax}$ instead of $\sum e(ax)$ etc. Hence the Λ_p-constant $\lambda_{p,A}$ makes sense, and Parseval equality and Hőlder inequality hold. Therefore, we still have (1.3). However, Propositions 1.1 and 1.2 are replaced by

Proposition 1.3. ([C4], Proposition B) *Let $A \subset \mathbb{R}$ with $|A| = N$, and $|A^2| < K|A|$. Then*

$$\lambda_{2h,A} \ll_h 1 + e^{cK} N^{-\frac{1}{2h}}, \text{ where } c = c(h).$$

Therefore, $\| \sum_{a \in A} e^{iax}\|_{2h} <_h (1 + e^{cK} N^{-\frac{1}{2h}}) N^{\frac{1}{2}}$.

The proof of Proposition 1.3 is based on the Subspace Theorem [ESS] which gives an upper bound on the number of solutions of a linear equation. Let

$$\sum_{i=1}^{m} c_i x_i = 1, c_i \in \mathbb{C} \tag{1.4}$$

be a linear equation over $\mathbb{C}$.

A solution $(x_1, \cdots, x_m)$ is called *nondegenerate*, if $\sum_{j=1}^{k} c_{i_j} x_{i_j} \neq 0$, for all k. The bound given below is by Evertse, Schlickewei and Schmidt [ESS].

Theorem (Subspace Theorem, [ESS]**).** *Let $\Gamma < \langle \mathbb{C}^*, \cdot \rangle$ be a subgroup of the multiplicative group of $\mathbb{C}$, and let the rank of Γ be r. Then*

$$|\{\textit{nondegenerate solutions of } (1.4) \textit{ in } \Gamma\}| < e^{(r+1)(6m)^{3m}}.$$

Notation. $d \ll_h f$ means $d \leq c(h)f$, where $c(h)$ is a function of h.

The formulation of the Subspace Theorem we need is the following (see [C5])

Corollary. [C4] *Let $\Gamma < \langle \mathbb{C}^*, \cdot \rangle$ be a subgroup of rank r and $A \subset \Gamma$ with $|A| = N$. Then the numbers of solutions in A of*

$$x_1 + \cdots + x_{2h} = 0 \tag{1.5}$$

is bounded by $N^{h-1}e^{rc} + N^h$, up to a constant depending on h. Here $c = c(h)$.

In order to apply the theorem, we need the following (See [Fr], [Rud], [Bi].)

Freiman's Lemma. *Let $\langle G, \cdot \rangle$ be a torsion-free abelian group and $A \subset G$ with $|A^2| < K|A|$. Then*

$$A \subset \{g_1^{j_1} \cdots g_d^{j_d} : j_i = 1, \cdots, \ell_i, \textit{ and } g_i \in G\}, \tag{1.6}$$

where $d \leq K$, and $\prod \ell_i < c(K)|A|$.

We let $\Gamma < \langle \mathbb{C}^*, \cdot \rangle$ be the subgroup generated by $g_1, \cdots, g_d$. Then the rank of Γ is bounded by $d \leq K$ and the number of nondegenerate solutions of (1.4) in Γ is bounded by $e^{c_m K}$.

Lemma. [C4] *Let $A \subset \mathbb{C}$ with $|A| = N$, and $|A^2| < K|A|$. Then*

$$|\{ \textit{ solutions of } (1.5) \textit{ in } A\}| <_h N^{h-1} e^{cK} + N^h.$$

Proof of Proposition 1.3.

Let $r_h(k)$ be the number of representatives of k as the sum of h elements from A.

$$r_h(k) = |\{(a_1, \cdots, a_h) : k = a_1 + \cdots + a_h, a_i \in A\}|$$

Then

$$|\sum e^{iax}|^{2h} = |\sum e^{i(a_1+\cdots+a_h)x}|^2 = |\sum_{k \in hA} r_h(k) e^{ikx}|^2.$$

Parseval and the definition of $r_h(k)$ give

$$\int' |\sum e^{iax}|^{2h} = \sum_{k\in hA} r_h(k)^2 = |\{(a_1,\cdots,a_{2h})|\ a_1+\cdots a_h = a_{h+1}+\cdots+a_{2h}\}|,$$

which is $<_h N^{h-1}e^{cK} + N^h$ by the lemma above. $\square$

In Theorem 1.b we are bounding the number of factorizations with factors in A. Let $\pi_h(n)$ be the number of factorizations of n.

$$\pi_h(n) = |\{(a_1,\cdots,a_h) \mid n = a_1\cdots a_h, a_i \in A\}|.$$

We use Freiman's Lemma on $\langle \mathbb{C}, + \rangle$, so A lies in a generalized arithmetic progression (of dimension $\leq \alpha$). Then we bound the number of factorizations in a generalized arithmetic progression.

Proposition 1.4. ([C3], Theorem 1) *Let $A \subset \mathbb{C}$ with $|A| = N$ and $|2A| < \alpha N$. Then*

$$\pi_h(n) < N^{\frac{C_h(\alpha)}{\log\log N}},\ \textit{for all } n \in A^h.$$

To prove Theorem 1.e, we replace $r(n)$ by

$$\pi(k) = \{(ab) \in A\times B \mid k = ab\}|.$$

Properties (1)-(4) can be replaced by $(1') - (4')$ below. In $(2')$ to use the harmonic analysis language as in (2), we consider the set $\log A = \{\log a \mid a \in A\}$ instead of A.

$(1')$. $|AB| \geq \frac{|A|^2|B|^2}{\sum \pi(n)^2}$

$(2')$. $\sum \pi(n)^2 = \int' |(\sum_a e^{ix\log a})(\sum_b e^{ix\log b})|^2 \leq \|(\sum_a e^{ix\log a})^2\|_q \ \ \|(\sum_b e^{ix\log b})^2\|_p$, where $\frac{1}{p}+\frac{1}{q} = 1$, p, q to be chosen.

$(3')$. $\|(\sum_a e^{ix\log a})^2\|_q = (\int' |\sum_a e^{ix\log a}|^{2q})^{\frac{1}{q}} = \left(\sum \pi_q(n)^2\right)^{\frac{1}{q}} < \left(|A|^q\ |A|^{\ \frac{c}{\log\log|A|}}\right)^{\frac{1}{q}}$

$(4')$. $(\|(\sum_b e^{ix\log b})^2\|_p)^p \leq \|\sum_b e^{ix\log b}\|_\infty^{2p-2} \ \ \int |\sum_b e^{ix\log b}|^2 \leq |B|^{2p-1}$

Section 2. Subsets of matrices

Though the sum-product theorem is true for the quaternions (see Proposition 2.3), it is false in general for subsets of noncommutative rings. For example, let

$$A = \left\{ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} : k = 1,\cdots,N \right\}.$$

It is easy to see that $|A| = N$, $|A+A| = 2N-1$ and $|A\cdot A| = 2N-1$. However, the following theorems are true.

Theorem 2.a. ([C5], Theorem A) *Let $A \subset Mat(d)$ and $|A| = N$. If*

$$\det(a - a') \neq 0, \ \ \forall\, a \neq a' \in A, \tag{2.1}$$

then

$$|2A| + |A^2| > \phi(N)N,$$

where $\phi(N) \to \infty$ as $N \to \infty$.

Theorem 2.b. ([C5], Theorem B) *For all d, there is $\varepsilon = \varepsilon(d) > 0$ such that if $A \subset Sym(d)$ and $|A| = N$, then*

$$|2A| + |A^2| > N^{1+\varepsilon}.$$

The next lemma for Theorem 2.a is the multi-variable version of the fundamental theorem of algebra.

Lemma 2.1. ([C5], Lemma 1.2) *Let $S \subset [1, J_1] \times \cdots \times [1, J_k] \cap \mathbb{Z} \times \cdots \times \mathbb{Z}$, with*

$$|S| > \frac{1}{cN^{\varepsilon}} J_1 \cdots J_k,$$

and let $p(x_1, \cdots, x_k)$ be a polynomial of degree D, such that $p(S) = \{0\}$. Then there is an affine space $W \subset \mathbb{R}^k$ such that $p(W) = \{0\}$ and

$$|W \cap S| > \frac{J_1 \cdots J_k}{(cN^{\varepsilon})^k D^{k-1} 2^{k(k-1)}}.$$

To prove Theorem 2.a, we assume $|2A| < K|A|$ for K bounded. So by Freiman's Lemma, A lies in a generalized arithmetic progression. Therefore, $\det(A)$, the set of determinants of matrices in A lies in a generalized arithmetic progression. The assumption $|A^2| < K|A|$ guaranteers the existence of a matrix $b \in A^2$ with at least $\frac{N}{K}$ many factorizations. Applying the bound on the number of factorizations on the generalized progression containing $\det(A)$, we conclude that A has a large subset, in which every matrix has the same determinant. Lemma 2.1 provides a linear space $V \subset Mat(d)$, and $A_1 \subset A$ with $|A_1| > cN^{1-\varepsilon}$, such that $\det(V) = \{0\}$ and $a - a' \in V$ for $a, a' \in A_1$. This is a contradiction.

For Theorem 2.b, we use the technical proposition below. This proposition says if the sum set is small, then there is an affine space V which has a large intersection with A, and any algebraic property holds for most of the intersection holds for V. Note that conditions on the rank of matrices and identities of matrices are all algebraic properties.

Proposition 2.2. ([C5], Proposition 2.1) *Let $A \subset \mathbb{R}^m$ be a finite set, $|A| = N$ and*

$$|2A| < KN. \tag{2.1}$$

Then there is $E \subset A$ and an affine space $V \subset \mathbb{R}^m$ such that

(i) $\frac{|E|}{|A|} = \delta > K^{-c}$, *where* $c = c(m)$

(ii) $E \subset V$

(iii) *If $\Gamma \subset \mathbb{R}^m$ is algebraic of degree $< m^{10}$ and*

$$|\Gamma \cap E| > \delta^{10} K^{-10} |E|, \tag{2.2}$$

then

$$V \subset \Gamma.$$

Using Proposition 2.2, we prove that $\{a^2 : a \in V\}$ forms a commutative multiplicative system. Therefore, we use this system to decompose $\mathbb{R}^d$ as eigen-subspaces, use regularization and use induction to finish the proof. For the initial step of the induction, we use the following variant of Erdős-Szemerédi argument ([C6]).

Proposition 2.3. ([C4], Theorem 3) *Let $\{\mathbb{R}^m, +, *\}$ be an $\mathbb{R}$-algebra with multiplicative identity and $+$ being the componentwise addition. For $a = (a_1, \cdots, a_m)$, let $|a| = \sqrt{(\sum a_i^2)}$ be the Hilbert-Schmidt norm, and let $V \subset \mathbb{R}^m$ be a subspace such that*

1. *There exists $c = c(m)$ such that for any $a, b \in V$, $|a * b| = c|a||b|$.*
2. *All nonzero elements of V are invertible.*

Then for any $A \subset V$, $|2A| + |A^2| > |A|^{1+\delta}$.

Remark. In view of the example in the beginning of Section 2, sum-product theorem is certainly not true for matrices over $\mathbb{F}_p$. However Helfgott proves that 'product theorem' is true for $A \subset SL_2(p)$. In particular, $|A^3|$ is much larger than $|A|$, unless A is contained in proper a subgroup. This result has nice application to the theory of expanders and Lubotski problem.

The corresponding results for $SL_3(p)$ has not been obtained yet.

Section 3. Subsets of $\mathbb{Z}_q$

The sum-product theorem is not true for $\mathbb{Z}_q$ without constraints. For instance, take $A = \mathbb{Z}_q$. Then $|2A| = |A^2| = |A|$.

The following theorem says that for a prime modulus p, sum-product theorem holds if A is not too close to be the entire ring. It was first proved by Bourgain, Katz and Tao for $p^\delta < |A| < p^{1-\delta}$, then improved by Bourgain, Glibichuk and Konyagin. Now there is a simpler proof in the book by Tao and Vu [TV].

Theorem ([BKT], [BGK]). *Let p be a prime. Given $\delta > 0$, there is $\varepsilon = \varepsilon(\delta) > 0$ such that if $A \subset \mathbb{Z}_p$ and*

$$1 < |A| < p^{1-\delta}.$$

Then

$$|2A| + |A^2| > c|A|^{1+\epsilon},$$

where $c = c(\delta)$.

However, for composite modulus q, further restrictions are needed. For example, take $A = (p) \subset \mathbb{Z}_{p^2}$. Then $2A = A$, and $A^2 = 0$. Theorem 3.a says that these are essentially all the exceptions.

The results described in this section are joint work with J. Bourgain. ([BC2])

We assume the composite modulus q has few large prime factors. This assumption is sufficient for our applications to exponential sums, though unnecessary for the sum-product theorem for $\mathbb{Z}_q$. Assume q has the prime factorization

$$q = p_1^{\alpha_1} \cdots p_r^{\alpha_r} \text{ with } p_i > q^{\beta}, \text{ for some constant } \beta > 0. \qquad (*)$$

In particular,

$$\alpha_1 + \cdots + \alpha_r < \frac{1}{\beta}, \text{ and } \quad r < \frac{1}{\beta}.$$

Theorem 3.a. ([BC2], Theorem 1.10) *Assume that q satisfies $(*)$. Let $A \subset \mathbb{Z}_q$ with $|2A| + |A^2| < q^{\epsilon}|A|$. Then one of the following holds.*

(a) $|A| > q^{1-\epsilon'}$.

(b) *there exists a prime $p|q$ such that $\big|A \cap \big(a + (p)\big)\big| > q^{-\epsilon'}|A|$, where $\epsilon' = \epsilon'(\beta, \epsilon) \to 0$ as $\epsilon \to 0$.*

Let $e_q(\theta) = e^{\frac{2\pi i \theta}{q}}$, $A \subset \mathbb{Z}_q$ and $k \in \mathbb{N}$. For $\xi \in \mathbb{Z}_q^*$, we define

$$S_k(\xi, A) = \sum_{x_1, \ldots, x_k \in A} e_q(x_1 \ldots x_k \xi).$$

The exponential sums problem is to show

$$|S_k(\xi, A)| < |A|^k q^{-\varepsilon}, \text{ for some } \varepsilon > 0.$$

Our approach is to use harmonic analysis. Let

$$\mu_k = |A|^{-k} \sum_{x_1, \ldots, x_k \in A} \delta_{x_1 \ldots x_k},$$

where δ_z is the Dirac measure at $z \in \mathbb{Z}_q$.

For a function $\mu: \mathbb{Z}_q \to \mathbb{R}$, let $\hat{\mu}(\xi) = \sum_{x \in \mathbb{Z}_q} \mu(x) e_q(x\xi)$ be the Fourier transform of μ. Then

$$\hat{\mu}_k(\xi) = |A|^{-k} \, S_k(\xi, A).$$

Next, we will state a rather technical proposition about probability measure. ($\mu(x)$ is a *probability measure* if $\mu \geq 0$ and $\sum \mu(x) = 1$.) In Section 4, we will give a proof of a special case of an exponential sum bounds by using the sum-product theorems. The proof carries the general idea behind the proposition without the technicalities.

Proposition 3.1. ([BC2], Proposition 2.1) *Let $R = \prod_j \mathbb{Z}_{q_j}$ be a commutative ring with $|R| = q$. Let μ be a probability measure on R. Let $\varepsilon > 0$. Then one of the following alternatives hold:*

(i.) $\displaystyle\sum_{\xi, y \in R} |\hat{\mu}(\xi)|^2 |\hat{\mu}(y\xi)|^2 \mu(y) < q^{-\varepsilon} \sum_{\xi \in R} |\hat{\mu}(\xi)|^2$

(ii.) $\displaystyle\max_{x \in R} \mu\big(x + (R \backslash R^*)\big) > c q^{-\tau}$

(iii.) *There is a subset $\bar{S}$ of R^* such that*

$$|\bar{S}| . \left(\sum |\hat{\mu}(\xi)|^2 \right) < 10 q^{1+\varepsilon},$$
$$|\bar{S} + \bar{S}| + |\bar{S} . \bar{S}| < q^{C\varepsilon} |\bar{S}|,$$
$$\max_{x \in R} \mu(x + \bar{S}) > q^{-C\varepsilon},$$

where c, C are some constants.

Applying Proposition 3.1 to the exponential sums setting with some work, one can show

Theorem 3.b. ([BC2], Theorem 3.2) *Let $R = \prod_j \mathbb{Z}_{q_j}$ be a commutative ring with $|R| = q$ and let $A \subset R^*$ with $|A| = q^\delta$ for $0 < \delta \leq 1$. Assume there exist $\kappa_0, \kappa_1 > 0$ such that the following properties hold*

(i.) $\max_x \big|A \cap \big(x + (R \backslash R^*)\big)\big| < q^{-\kappa_0} |A|$.

(ii.) $\max_x \big|A \cap (x + S)\big| < q^{-\kappa_0} |A|$, *whenever $S \subset R^*$ satisfies*

(a.) $|S| < q^{1-\kappa_1}$,

(b.) $|S + S| + |S.S| < q^{\kappa_0} |S|$.

Then there is $k = k(\kappa_0)$ and $\varepsilon = \varepsilon(\kappa_0)$ such that

$$\max_{\xi \in R^*} |S_k(\xi, A)| < |A|^k q^{-\varepsilon}.$$

Putting Theorem 3.a and Theorem 3.b together, we have

Theorem 3.c. ([BC2], Theorem 4.1) *Let $q \in \mathbb{N}$ satisfy $(*)$, and $A \subset \mathbb{Z}_q$ with $|A| = q^\delta$. Assume*

$$\max_{p|q, t\in\mathbb{Z}_p} |A \cap \pi_p^{-1}(t)| < q^{-\gamma}|A|$$

with $0 < \gamma < \frac{\delta}{25}$.

Then for $k > k(\gamma), \varepsilon = \varepsilon(\gamma)$

$$\max_{\xi\in\mathbb{Z}_q^*} |S_k(\xi, A)| < |A|^k q^{-\varepsilon}.$$

The following applications are straightforward from Theorem 3.c.

Theorem 3.d (Generalized Gauss sums). ([BC2], Corollary 4.2) *Let $q \in \mathbb{N}$ satisfy $(*)$, and let $H < \mathbb{Z}_q^*$ be a subgroup with $|H| = q^\delta$ and*

$$\min_{p|q} |\pi_p(H)| > q^{\delta'}.$$

Then

$$\max_{\xi\in\mathbb{Z}_q^*} \left| \sum_{x\in H} e_q(\xi x) \right| < |H| q^{-\varepsilon}$$

with $\varepsilon = \varepsilon(\delta')$.

Theorem 3.e (Gauss sums). ([BC2], Corollary 4.3) *Let $q = \prod_\alpha p_\alpha^{\nu_\alpha}$ satisfy $(*)$, and $k \in \mathbb{Z}_q$ satisfy*

$$(k, p_\alpha - 1) < (p_\alpha - 1)q^{-\delta} \text{ for all } \alpha, \text{ for some } \delta.$$

Then

$$\max_{\xi\in\mathbb{Z}_q^*} \left| \sum_{x=0}^{q-1} e_q(\xi x^k) \right| < q^{1-\delta'}$$

where $\delta' = \delta'(\delta, C_0)$.

Theorem 3.f (Heilbronn's exponential sums). ([BC2], Corollary 4.4)

$$\max_{(\xi,p)=1} \Big| \sum_{x=1}^{p} e_{p^m}(\xi x^{p^{m-1}}) \Big| < p^{1-\delta_m}$$

for some $\delta_m > 0$ and p large enough.

Section 4. A simpler proof of the Generalized Gauss sums Theorem for prime modulus

We will use the Laczkovich-Ruzsa version [LR] of Balog-Szemerédi-Gowers Theorem.

Theorem BSG-LR 1. *Let $G \subset A \times A$ with $|G| > K^{-1}|A|^2$. Denote*

$$A \overset{G}{+} A = \{a + a' \ : \ (a, a') \in G\}.$$

If $|A \overset{G}{+} A| < K|A|$, then there is a subset $A' \subset A$ such that

$$|A' + A'| < K^c|A|$$
$$|(A' \times A') \cap G| > K^{-c}|A|^2,$$

where c is an absolute constant.

Theorem BSG-LR 2. *Let $G \subset A \times B$ with $|G| > K^{-1}|B|^2$ and $|B| \geq |A| \geq c_1|B|$. Denote*

$$A \overset{G}{+} B = \{a + b \ : \ (a, b) \in G\}.$$

If $|A \overset{G}{+} B| < K|B|$, then there is a subset $B' \subset B$ such that

$$|B' + B'| < K^c|B|$$
$$|B'| > K^{-c}|B|,$$

where c is an absolute constant.

Let $H < \langle \mathbb{Z}_q^*, \cdot \rangle$ be a multiplicative subgroup. For simplicity, we assume $H = -H$.

Denote $\nu_-(x) = \nu(-x)$.

Lemma 4.1. *Let ν be a probability measure with $\nu = \nu_-, \hat{\nu} \in \mathbb{R}$. Assume $\exists\ \tau > 0$, and $\exists\ \Gamma \subset \mathbb{Z}_q$ with $\Gamma = -\Gamma$, such that $\forall\ \zeta \in \Gamma, \hat{\nu}(\zeta) > q^{-\tau}$. Then for given $\delta > 0$, one of the following holds*

(1) *$\exists\ \Gamma'$ with $|\Gamma'| > |\Gamma|^{1+\delta}$ such that $\forall\ \zeta \in \Gamma', \hat{\nu}(\zeta) > \frac{1}{2}q^{-2\tau}$.*

(2) *$\exists\ \Gamma_1 \subset \Gamma$ with $|\Gamma_1| > |\Gamma|^{1-\delta c}$ and $|\Gamma_1 + \Gamma_1| < |\Gamma_1|^{\frac{1}{1-\delta c}}$ for some $c > 0$.*

Lemma 4.2. *Let ν be an $H-$invariant probability measure. Assume $\exists\ \tau > 0$, and $\exists\ \Gamma_1 \subset \mathbb{Z}_q^*$, such that $\forall\ \zeta \in \Gamma_1, \hat{\nu}(\zeta) > q^{-\tau}$. Then for given $\delta_1 > 0$, one of the following holds*

(i) *$\exists\ \Gamma'$ with $|\Gamma'| > |\Gamma_1|^{1+\delta_1}$ such that $\forall\ \zeta \in \Gamma', \hat{\nu}(\zeta) > \frac{1}{2}q^{-\tau}$.*

(ii) *$\exists\ \Gamma_2 \subset \Gamma_1$ with $|\Gamma_2| > |\Gamma_1|^{1-\delta_1 c}$ and $|\Gamma_2\Gamma_2| < |\Gamma_2|^{\frac{1}{1-\delta_1 c}}$ for some $c > 0$*

Proof of Lemma 4.1. The assumption implies

$$\sum_{\xi_1,\xi_2\in\Gamma} \hat{\nu}(\xi_1-\xi_2) > q^{-2\tau}|\Gamma|^2$$

and hence, denoting

$$G = \left\{(\xi_1,-\xi_2)\in\Gamma\times\Gamma:\ \hat{\nu}(\xi_1-\xi_2) > \frac{1}{2}q^{-2\tau}\right\},$$

we have

$$|G| > \frac{1}{2}q^{-2\tau}\ |\Gamma|^2.$$

Let

$$\Gamma \overset{G}{+} \Gamma = \{\xi_1-\xi_2:\ (\xi_1,\xi_2)\in G\}$$

If $|\Gamma \overset{G}{+} \Gamma| > |\Gamma|^{1+\delta}$, then we have Case (1) by taking $\Gamma' = \Gamma \overset{G}{+} \Gamma$. Otherwise, we apply Theorem BSG-LR1 with $K = |\Gamma|^{\delta}$. $\square$

Proof of Lemma 4.2. Define the probability measure ν_1 on $\mathbb{Z}_q$

$$\nu_1(x) = \frac{1}{|\Gamma|}\sum_{\xi\in\Gamma}\nu(x\xi^{-1}).$$

Since ν is H-invariant, so is ν_1. Moreover $\hat{\nu}_1(1) > q^{-\tau}$, hence $\hat{\nu}_1(\zeta) > q^{-\tau}$ for all $\zeta\in H$. This means that

$$\sum_{\zeta\in H,\xi\in\Gamma}\hat{\nu}(\zeta\xi) > q^{-\tau}|H|\ |\Gamma|.$$

Denote now

$$G_1 = \{(\zeta,\xi)\in H\times\Gamma:\ \hat{\nu}(\zeta\xi) > \frac{1}{2}q^{-\tau}\}$$

for which $|G_1| > \frac{1}{2}q^{-\tau}|H||\Gamma|$. Assume

$$\left|H \overset{G_1}{\times} \Gamma\right| = \left|\{\zeta\xi:\ (\zeta,\xi)\in G_1\}\right| < |\Gamma|^{1+\delta}$$

Applying Theorem BSG-LR2 in multiplicative form, we obtain $\Gamma'\subset\Gamma$. $\square$

Proof of Theorem 3.d.

Let μ_H be the probability measure on H. i.e. $\mu_H(x) = \frac{1}{|H|}$, if $x \in H$, and 0 otherwise.

To show

$$\Big| \sum_{x \in H} e_q(x\xi) \Big| < q^{-\varepsilon} \, |H|,$$

is equivalent to showing

$$|\hat{\mu}_H(\xi)| < q^{-\varepsilon}.$$

To prove by contradiction, we assume $|\hat{\mu}_H(a)| > q^{-\varepsilon}$ for some $a \in \mathbb{Z}_q^*$. Let $\mu = \mu_H * \mu_H$, the convolution of μ_H and μ_H. Since μ is $H-$invariant,

$$\hat{\mu}(\xi) > q^{-2\varepsilon}, \text{ for all } \xi \in aH$$

Starting from aH, one aim is to construct consecutively larger and larger sets $\Lambda \subset \mathbb{Z}_q$ such that $\hat{\mu}(\xi) > q^{-\tau}$ for $\xi \in \Lambda$. (τ may get larger and larger.) This will violate the fact that

$$|\{\xi\colon \, |\hat{\mu}(\xi)| > q^{-\tau}\}| < \frac{q^{1+\tau}}{|H|}.$$

Applying Lemma 4.1 to μ and $\Gamma = aH$. Case 1 is what we want. For Case 2, we apply Lemma 4.2 to the smaller set Γ_1 and choose $\delta_1 > \frac{1}{1-\delta c} - 1$. If we get Case (i), the set Γ' with $|\Gamma'| > |\Gamma_1|^{1+\delta_1} > |\Gamma|^{(1+\delta_1)(1-\delta c)}$ is a good enlargement. If we get Case (ii), then the set Γ_2 has the properties

$$|\Gamma_2| > N^{(1-\delta c)(1-\delta_1 c_1)}, \;\; |\Gamma_2\Gamma_2| < |\Gamma_2|^{\frac{1}{1-\delta_1 c_1}}, \;\; |\Gamma_2 + \Gamma_2| < |\Gamma_2|^{\frac{1}{1-\delta c}\frac{1}{1-\delta_1 c_1}},$$

which contradicts Theorem 3.a.

References

[Bi]. Y. Bilu, *Structure of sets with small sumset*, in 'Structure Theory of Set Addition', Astérisque 258 (1999), 77-108.

[BS]. L.I. Borevich, I.R. Shafarevich, *Number Theory*, Academic Press, 1966.

[BC1]. J. Bourgain, M-C. Chang, *On the size of k-fold Sum and Product Sets of Integers*, JAMS.

[BC2]. J. Bourgain, M-C. Chang, *Exponential sum estimates over subgroups and almost subgroups of $\mathbb{Z}_q^*$, where q is composite with few prime factors*, GAFA.

[BGK]. J. Bourgain, A. Glibichuk, S. Konyagin, *Estimate for the number of sums and products and for exponential sums in fields of prime order*, submitted to J. London MS.

[BKT]. J. Bourgain, N. Katz, T. Tao, *A sum-product estimate in finite fields and their applications*, GAFA 14 (2004), n1, 27–57.

[C1]. M-C. Chang, *A Polynomial bound in Freiman's theorem*, Duke Math. J. Vol. 113, No. 3, (2002), 399-419.

[C2]. M-C. Chang, *Erdös-Szemeredi problem on sum set and product set*, Annals of Math. 157 (2003), 939-957.

[C3]. M-C. Chang, *Factorization in generalized arithmetic progressions and applications to the Erdös-Szemerédi sum-product problems*, GAFA Vol. 113, (2002), 399-419.

[C4]. M-C. Chang, *Sum and product of different sets*, Contributions to Discrete Math. Vol. 1, 1 (2006).

[C5]. M-C. Chang, *Additive and multiplicative structure in matrix spaces*, Comb. Prob., Computing (to appear).

[C6]. M-C. Chang, *A sum-product estimate in algebraic division algebras*, Israel JM.

[Ch]. Y.G. Chen, *(1997) (private communication).*

[E]. G. Elekes, *On the number of sums and products*, Acta Arithm., 81, 4 (1997), 365-367.

[ENR]. G. Elekes, M. Nathanson, I. Ruzsa, *Convexity and sumsets*, J. Number Theory, (to appear).

[ER]. G. Elekes, J. Ruzsa, *Few sums, many products*, preprint.

[ES]. P. Erdös, E. Szemerédi, *On sums and products of integers*, In P. Erdös, L. Alpàr, G. Haláz (editors), Stud. Pure Math., to the memory of P. Turán, p. 215–218.

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

[Fr]. G. Freiman, *'Foundations of a structural theory of set addition'*, Translations of Math. Monographs, 37, AMS, 1973.

[LR]. Laczkovich, I. Ruzsa, *The number of homothetic subsets,*, in 'The mathemattics of P. Erdős, II. (R.L. Grham, J. Nesetril, eds.), Springer, Algorithms Combin. 14 (1997), 294-302.

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

[R]. W. Rudin, *Trigonometric series with gaps*, J. Math. Mech. 9 (1960), 203–227.

[Ruz]. I.Z. Ruzsa, *Generalized arithmetic progressions and sumsets*, Acta Math. Hungar. 65 (1994), no 4, 379-388.

[S]. J. Solymosi, *On the number of sums and products*, Bulletin LMS (to appear).

[ST]. E. Szemerédi, W. Trotter, *Extremal problems in Discrete Geometry*, Combinatorics, 3 (3-4), 387–392 (1983).

[T-V]. T. Tao, V. Vu, *Additive Combinatorics (preprint).*

Math Department, University of California, Riverside, CA 92521

E-mail address: mcc@math.ucr.edu