SUM AND PRODUCT OF DIFFERENT SETS

[1] Mei-Chu Chang
Department of Mathematics
University of California
Riverside, CA 92521
mcc@math.ucr.edu

Abstract. *Let A and B be two finite sets of numbers. The sum set and the product set of A, B are $A+B := \{a+b : a \in A, b \in B\}$, and $AB := \{ab : a \in A, b \in B\}$. We prove that $A+B$ is as large as possible when AA is not too big. Similarly, AB is large when $A+A$ is not too big. The methods rely on the λ_p constant of A, bound on the number of factorizations in a generalized progression containing A, and the subspace theorem.*

Let A and B be two finite sets of numbers. The *sum set* and the *product set* of A, B are $A+B := \{a+b : a \in A, b \in B\}$, and $AB := \{ab : a \in A, b \in B\}$. (We denote by jA the j-fold sumset $A + \cdots + A$.) There has been a lot of studies of the sizes of the sum and product sets for the case $A = B$ (cf particularly, [BC], [BKT], [C1]-[C5], [E], [ER], [ES], [F], [N1], [N2], [NT], [S]), since Erdös and Szemerédi [ES] made their well-known conjecture that for $|A|$ sufficiently large,

$$|A+A| + |AA| > c_\varepsilon |A|^{2-\varepsilon} \text{ for all } \varepsilon > 0.$$

The conjecture is still open. The best result to date is due to J. Solymosi [S] and states roughly that

$$|A+A| + |AA| > |A|^{\frac{14}{11}-\varepsilon}.$$

The method uses the Szemerédi-Trotter Theorem in incidence geometry. A similar approach is used in [ER] to show that, if $|A+A| < K|A|$, then $|AA| > |A|^{2-\epsilon}$. We point out that the geometric approach does not distinguish between sets of integers and sets of real numbers. On the other hand, it does not provide nontrivial lower bounds on $|A+B|+|AB|$, if the set B is much smaller that A. It is also not enough for showing that $|AB| > (|A||B|)^{1-\epsilon}$ for all A, B such that $|A+A| < K|A|$ and $\log|A| \sim \log|B|$, as we will prove here (Theorem 3).

In the paper [BKT], a sum-product theorem in prime fields $\mathbb{F}_p$ is established. The original motivation was to make progress on the so-called Kakeya problem in dimension 3. It turns out however that those results have quite significant application to the theory of exponential sums over finite fields and lead to no nontrivial

[1]partially supported by NSA grant No. MDA 904-03-1-0045.
2000 Mathematics Subject Classification. 05A99.

improvements in case where classical methods (such as Stepanov's approach) do not apply. (See [BGK]). But we will not discuss further the finite field setting here, which relies on different techniques.

Returning to the Erdös-Szemerédi conjecture, we also mention the following more general question brought up by Solymosi

Question. *Is there an absolute constant $c > 0$ such that for every $n \in \mathbb{N}$, there are finite sets A, B and C, with $|A| = |B| = |C| = n$, $|A+B| < n^{2-c}$, and $|AC| < n^{2-c}$?*

This question motivated the results established in this note.

It became increasingly clear that techniques such as the Szemerédi-Trotter Theorem are unable to settle the conjecture or the above question and other ideas are required. In earlier works, the author has brought several different approaches into play. They will be further exploited in this paper.

First, in [C2] a connection is made with the factorization theory in algebraic number fields. It was shown in [C2] that if A is a finite set of complex numbers and $|A + A| < K|A|$, then not only $|AA| > |A|^{2-\varepsilon}$ but more generally $|A^{(j)}| > |A|^{j-\varepsilon}$, where $A^{(j)} = A \cdots A$ is the j-fold product set. This is a contribution to the generalized Erdös-Szemerédi conjecture

$$|jA| + |A^{(j)}| > c_\varepsilon |A|^{j-\varepsilon} \text{ for all } j \geq 2 \text{ and } \varepsilon > 0.$$

The main result of [C2] actually consists in a bound on the number of factorizations in generalized arithmetic progressions, using the corresponding theory in algebraic number fields and a transference argument.

Secondly, there is the paper [BC] involved in the proof of Theorem 1 below. In [BC], which builds further on [C1], concepts and methods from harmonic analysis are brought into play. Roughly speaking, assuming A a finite set of integers and $|AA| < |A|^{1+\varepsilon}$, it is shown that for any fixed exponent $p > 2$, the so-called Lambda-p constant $\lambda_p(A)$ of A is bounded by $|A|^{\delta_p(\varepsilon)}$, where $\delta_p(\varepsilon) \to 0$ as $\varepsilon \to 0$. From this, it is shown that

$$|jA| + |A^{(j)}| > |A|^{b(j)} \tag{0}$$

where $b(j) \to \infty$ for $j \to \infty$. This is another contribution to the generalized conjecture. Coming back to the problem of finding the lower bound on $|A+B|+|AB|$ brought up earlier, notice that the following is true.

Let $A, B \subset \mathbb{Z}$ be finite and $|A|^r < |B| \leq |A|$. Then $|A + B| + |AB| > |A|^{1+\delta(r)}$.

Indeed, assume the contrary. Then the Plünnecke-Ruzsa inequality and (0) imply there exist $A', A'' \subset A$ such that

$$|A|^{rb(j)} < |B|^{b(j)} < |jB| + |B^{(j)}| < |A' + jB| + |A''B^{(j)}| < |A|^{1+j\delta}$$

for all $j \in \mathbb{N}$. Hence $\delta > \frac{rb(j)-1}{j}$ and taking $j > j(r)$ gives the conclusion. This illustrates the power of the method. So far no full analogue of the [BC] result is known for sets of real numbers, as we rely essentially on prime factorization. Theorem 2 below provides the first contribution in this setting, under the stronger assumption $A \subset \mathbb{R}, |AA| < K|A|$. The main ingredient in its proof is the subspace theorem, in its general and powerful form obtained in [ESS]. Roughly speaking,

if $|AA| < K|A|$, then A is contained in a multiplicative group Γ generated by K elements (by Freiman's Lemma). The [ESS] result implies then that there are only few additive relations among its elements, which is exactly what we need. Although the relation between the sum-product problems and the subspace theorem is indeed quite obvious, it was not pointed out earlier and this may be the main merit of this note.

Next we state our main results.

Theorem 1. *Let $A \subset \mathbb{Z}$ be a finite set such that*

$$|AA| < |A|^{1+\epsilon}. \tag{1}$$

Then for any $B \subset \mathbb{Z}$, and any $j \in \mathbb{N}$, we have

$$|jA + B| \geq |A|^j \, |B| \, \big(|A| + |B|\big)^{-\delta_j(\epsilon)},$$

where for fixed j, $\delta_j(\epsilon) \to 0$ as $\epsilon \to 0$.

The next result gives a corresponding bound in the real setting, but requires a stronger assumption on the product set.

Theorem 2. *Let $A \subset \mathbb{R}$ be a finite set such that*

$$|AA| < K|A|. \tag{2}$$

Then for any $B \subset \mathbb{R}$, any $j \in \mathbb{N}$, and $\varepsilon > 0$, we have

$$|jA + B| > |A|^j \, |B|^{1-\epsilon},$$

provided $K = o_{j,\varepsilon}(\log |A|)$.

Switching addition and multiplication, one may prove the following counterpart of Theorem 2 (by a very different method).

Theorem 3. *Let $A \subset \mathbb{R}_+$ be a finite set such that*

$$|A + A| < K|A|. \tag{3}$$

Let $j \in \mathbb{N}$, and $\epsilon > 0$. Assume $K < K_{\epsilon,j,|A|}$, where $K_{\epsilon,j,|A|} \to \infty$ as $|A| \to \infty$ for ϵ, j fixed. Then for any $B \subset \mathbb{R}_+$,

$$|A^{(j)}B| > |A|^j \, |B| \, \big(|A| + |B|\big)^{-\epsilon}.$$

Remark. A more precise statement in Theorem 3 would require making in [C2] the dependence of certain constants on K explicit. Following the argument in [C2], the best one may hope for is a condition $K < o(\log \log |A|)$.

The following result from [BC] will be used in the proof of Theorem 1.

Proposition A. *[BC] Given $\gamma > 0$ and $p > 2$, there is a constant $\Lambda = \Lambda(\gamma, p)$ such that if $A \subset \mathbb{Z}$ is a finite set, $|A| = N, |AA| < KN$, then*

$$\lambda_p(A) < K^{\Lambda} N^{\gamma}.$$

Recall that by $\lambda_p(A)$, we mean the λ_p-constant of the finite set $A \subset \mathbb{Z}$, defined by

$$\lambda_p(A) = \max \big\| \sum_{n \in A} c_n \ e^{2\pi i n x} \big\|_{L^p(\mathbb{T})},$$

where $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ and the max is taken over all sequences $\{c_n\}_{n \in A}$ with $(\sum c_n^2)^{\frac{1}{2}} \leq 1$.

Remarks.
(i) By taking $\gamma = \epsilon_1$ and $K = |A|^{\epsilon}$ in Proposition A, we see that if $|AA| < |A|^{1+\epsilon}$, then for any $\epsilon_1 > 0$, we have

$$\lambda_p(A) < |A|^{\epsilon\Lambda + \epsilon_1}, \tag{4}$$

where $\Lambda = \Lambda(\epsilon_1, p)$.
(ii) To apply Proposition A, we only need the case when $c_n = \frac{1}{\sqrt{|A|}}$ for all n, but we do not have a proof simpler than the (rather technical) argument in [BC].

Proof of Theorem 1. For $k \in \mathbb{R}$, we let $r(k)$ be the number of representatives of k in $jA + B$.

$$r(k) = |\{(a_1, \ldots, a_j, b) \in A^j \times B : k = a_1 + \cdots + a_j + b\}| \tag{5}$$

Let

$$F(x) = \sum_{a \in A} e^{2\pi i a x}, \text{ and } G(x) = \sum_{b \in B} e^{2\pi i b x}. \tag{6}$$

Then the following properties hold. (Here $q' = \frac{q}{q-1}$.)

$$|jA + B| \geq \frac{|A|^{2j} |B|^2}{\sum r(k)^2} \tag{7}$$

$$\sum r(k)^2 = \int_0^1 |F(x)^j G(x)|^2 \tag{8}$$

$$\int |F|^{2j} \, |G|^2 \leq \Big(\int |F|^{2jq} \Big)^{\frac{1}{q}} \Big(\int |G|^{2q'} \Big)^{\frac{1}{q'}} \tag{9}$$

$$\Big(\int |F|^{2jq} \Big)^{\frac{1}{q}} < |A|^{j + 2j(\epsilon\Lambda + \epsilon_1)} \tag{10}$$

$$\Big(\int |G|^{2q'}\Big)^{\frac{1}{q'}} \le |B|^{1+\frac{1}{q}} \tag{11}$$

In fact, inequality (7) follows from the Cauchy inequality:

$$|A|^j|B| = |A^j \times B| = \sum_{k\in jA+B} r(k) \le |jA+B|^{\frac{1}{2}}\big(\sum r(k)^2\big)^{\frac{1}{2}}.$$

Equality (8) holds because

$$F^jG = \sum e^{2\pi i(a_1+\cdots+a_j+b)x} = \sum r(k)e^{2\pi ikx},$$

and Parseval's equality. Inequality (9) is Hölder's inequality. Inequality (10) follows from the definition of $\lambda_{2jq}(A)$ (with $c_n = \frac{1}{\sqrt{|A|}}$, for all $n \in A$), and inequality (4). Inequality (11) follows from the following easy estimate.

$$\Big(\int |G|^{2q'}\Big) \le \big\|G\big\|_\infty^{2(q'-1)} \int |G|^2 \le |B|^{2(q'-1)+1} \tag{12}$$

Putting (8)-(11) together, we have

$$\sum r(k)^2 \le |A|^{j+2j(\epsilon\Lambda+\epsilon_1)}|B|^{1+\frac{1}{q}}. \tag{13}$$

Therefore, (7) and (13) give

$$\begin{aligned} |jA+B| &\ge \frac{|A|^{2j}|B|^2}{|A|^{j+2j(\epsilon\Lambda+\epsilon_1)}|B|^{1+\frac{1}{q}}} \\ &> |A|^j|B|\big(|A|+|B|\big)^{-2j(\epsilon\Lambda+\epsilon_1)-\frac{1}{q}}. \end{aligned}$$

Let

$$\delta_j(\epsilon) = 2j(\epsilon\Lambda+\epsilon_1)+\frac{1}{q}.$$

Here j is fixed. Recall that $\Lambda = \Lambda(\epsilon_1, 2jq)$, and thus, for all $\epsilon_1 > 0$, $q > 0$, there is an ϵ_0 such that $\delta_j(\epsilon) < 3j\epsilon_1 + \frac{1}{q}$ for all $\epsilon < \epsilon_0$. Hence, by taking ϵ_1 small and q large, we may clearly make $\delta_j(\epsilon) \to 0$. $\square$

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

Next, we pass to Theorem 2.

We recall that $f : \mathbb{R} \to \mathbb{R}$ is an almost periodic function, if for any $\varepsilon > 0$, there exists $\ell = \ell(\varepsilon) > 0$ such that every interval $[t_0, t_0+\ell]$ contains τ for which $|f(t) - f(t+\tau)| < \varepsilon$. Equivalently, f can be uniformly approximated by a finite combination of exponential functions. To prove Theorem 2, instead of periodic functions, we need to consider almost periodic functions, which will appear simply as a finite combination of exponential functions. The integral $\int_0^1$ needs to be replaced by the mean

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

where f is an almost periodic function on $\mathbb{R}$.

The L^p norm and Lambda-p constant are defined accordingly. If $A \subset \mathbb{R}$ is a finite set, we have in particular

$$\int' |\sum_{a\in A} c_a e^{iax}|^2 = \|\sum_{a\in A} c_a e^{iax}\|_2^2 = \sum_{a\in A} |c_a|^2. \tag{14}$$

Also Hölder's inequality applies. (We apply with fixed T and then letting $T \to \infty$.)

We need the following proposition to prove Theorem 2.

Proposition B. *Let $A \subset \mathbb{R}$, and $|AA| < K|A|$. Then*

$$\lambda_{2h}(A) \ll_h 1 + \frac{e^{cK}}{|A|^{\frac{1}{2h}}}. \tag{15}$$

Here $c = c(h)$.

Proof of Theorem 2.

Let

$$F(x) = \sum_{a\in A} e^{iax}, \text{ and } G(x) = \sum_{b\in B} e^{ibx}.$$

Obviously, (7) still holds. By (14), we may write (8) replacing $\int_0^1$ by $\int'$ and apply Hölder's inequality to get (9). Instead of (10), we have, by (15) applied with $h = jq$

$$\begin{aligned}\Big(\int' |F|^{2jq}\Big)^{\frac{1}{q}} &\ll_{jq} |A|^j \left(1 + \frac{e^{c_0 K}}{|A|^{\frac{1}{2jq}}}\right)^{2j} \\ &\ll_{jq} |A|^j \left(1 + \frac{e^{c_1 K}}{|A|^{1/q}}\right),\end{aligned}$$

where c_0, c_1 depend on jq. Clearly, (11) and (12) remain valid.

In conclusion, it follows that

$$\begin{aligned}|jA + B| &\geq \frac{|A|^{2j}|B|^2}{|A|^j\,|B|^{1+\frac{1}{q}}} \left(1 + \frac{e^{c_1 K}}{|A|^{\frac{1}{q}}}\right)^{-1} \\ &\geq |A|^j |B|^{1-\frac{1}{q}} \left(1 + \frac{e^{c_1 K}}{|A|^{\frac{1}{q}}}\right)^{-1}.\end{aligned} \tag{16}$$

Returning to the statement in Theorem 2, take $q = [\frac{1}{\epsilon}]$ so that $c_1 = c_1(j, \epsilon)$. The last factor in (16) may then be dropped provided $K < \frac{\epsilon}{2c_1} \log |A|$. □

The proof of Proposition B is based on the subspace theorem, which gives a bound on the number of solutions of a linear equation in a multiplicative group. Let

$$\sum_{i=1}^m c_i x_i = 1, c_i \in \mathbb{C}^* \tag{17}$$

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.

Theorem (Subspace Theorem, [*ESS*]). *Let $\Gamma < \langle(\mathbb{C}^*)^m, \cdot\rangle$ be a subgroup of $(\mathbb{C}^*)^m$ of rank s. Then*

$$|\{\textit{nondegenerate solutions of } (17) \textit{ in } \Gamma\}| < e^{(s+1)(6m)^{3m}}.$$

Remark. Let $\Gamma < \langle\mathbb{C}^*, \cdot\rangle$ be a subgroup of rank r, with $\gamma_1, \dots, \gamma_r$ as a set of generators. Then $\Gamma' = \Gamma \times \Gamma \times \cdots \times \Gamma < (\mathbb{C}^*)^m$ is generated by the rm elements $(1, \cdots, \gamma_i, \cdots, 1)$ with γ_i at the j-th coordinate and 1 elsewhere ($i = 1, \cdots, r$, and $j = 1, \cdots, m$). The right hand side of the inequality in the Subspace Theorem becomes $e^{(rm+1)(6m)^{3m}}$.

Lemma. *Let $\Gamma < \langle\mathbb{C}^*, \cdot\rangle$ be a subgroup of rank r, with $-1 \in \Gamma$. Let $A \subset \Gamma$ with $|A| = N$. Let $\sigma_1(m)$ and $\sigma_0(m)$ be the numbers of solutions in A of*

$$x_1 + \cdots + x_m = 1$$

and

$$x_1 + \cdots + x_m = 0$$

respectively. Then for $h \geq 1$,
1. $\sigma_1(2h+1), \sigma_0(2h) \ll_h N^{h-1}e^{rc} + N^h$,
2. $\sigma_1(2h), \sigma_0(2h-1) \ll_h N^{h-1}e^{rc}$.

Remark. In the lemma above, $c = c(h)$ (which will be of the form h^{Ch}) may refer to different constants depending on h.

Proof of Lemma. By induction.

The number of nondegenerate solutions of $x_1 + x_2 + x_3 = 1$ is bounded by $e^{18^9(3r+1)}$, according to the Subspace Theorem. The number of degenerate solutions is clearly bounded by $3\big(\sigma_1(2) + \sigma_0(2)\big) \ll e^{12^6(2r+1)} + N$, contributed from the solutions of equations of types $x_1 + x_2 = 1$ and $x_1 + x_2 = 0$. Therefore, $\sigma_1(3) \ll e^{18^9(3r+1)} + e^{12^6(2r+1)} + N \ll e^{18^9(3r+1)} + N$. By assuming that one of the unknowns of $x_1 + x_2 + x_3 = 0$ is nonzero and reducing the equation to $x_1 + x_2 = 1$, we see that $\sigma_0(3) \ll N\sigma_1(2) \ll Ne^{12^6(2r+1)}$.

For the general case, we let $\mu_1(2h+1) = \mu_0(2h) = N^{h-1}e^{rc_h} + N^h$ and $\mu_1(2h) = \mu_0(2h-1) = N^{h-1}e^{rc'_h}$. Now

$$\begin{aligned}
\sigma_1(m) \leq\ & e^{(mr+1)(6m)^{3m}} + \sum_{i=1}^{m-1} \binom{m}{i} \sigma_1(i)\sigma_0(m-i) \\
\ll_m & e^{(mr+1)(6m)^{3m}} + \sum_{i=1}^{m-1} \binom{m}{i} \mu_1(i)\mu_0(m-i) \\
\ll_m & \mu_0(m-1) = \mu_1(m)
\end{aligned}$$

and

$$\sigma_0(m) \leq mN\sigma_1(m-1) \ll_m N\mu_1(m-1) \leq \mu_0(m). \qquad \square$$

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

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

$$A \subset \{g_1^{j_1} \cdots g_d^{j_d} : j_i = 1, \cdots, \ell_i, \text{ and } g_i \in G\}, \tag{18}$$

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

We may assume $A \subset \langle \mathbb{R}^*, \cdot\rangle$. Hence, assumption (2) implies that (18) holds with $g_i \in \mathbb{R}^*$. Let $\Gamma \subset \langle \mathbb{C}^*, \cdot\rangle$ be the subgroup generated by $\{-1, g_1, \ldots, g_d\}$. Then

$$r = rk(\Gamma) \leq d + 1 \leq K + 1.$$

Corollary. *Let $A \subset \mathbb{R}$, $|A| = N$, and $|AA| < K|A|$. Then for $h \geq 2$*

$$|\{ \text{ solutions of } \sum_{i=1}^{2h} x_i = 0 \text{ in } A\}| \ll_h N^{h-1}e^{cK} + N^h,$$

$$|\{ \text{ solutions of } \sum_{i=1}^{2h-1} x_i = 0 \text{ in } A\}| \ll_h N^{h-1}e^{cK}.$$

Here $c = c(h)$.

Proof of Proposition B. Let $r_h(k)$ be the number of representatives of k in hA.

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

To bound $\lambda_{2h}(A)$, we see that

$$\begin{aligned}
\int' |\sum e^{iax}|^{2h} &= \int' |\sum e^{i(a_1+\cdots+a_h)x}|^2 \\
&= \int' |\sum_{k\in hA} r_h(k)e^{ikx}|^2 \\
&= \sum_{k\in hA} r_h(k)^2 \\
&= |\{(a_1, \cdots, a_{2h}) \in A^{2h} : a_1 + \cdots a_h = a_{h+1} + \cdots + a_{2h}\}| \\
&\ll_h N^{h-1}e^{cK} + N^h.
\end{aligned}$$

The third equality is (14) and the last inequality follows from the corollary above.

Hence

$$\|\sum e^{iax}\|_{2h} \ll_h N^{\frac{1}{2}-\frac{1}{2h}} e^{c\frac{K}{2h}} + N^{\frac{1}{2}}. \qquad \square$$

We will use the following proposition to prove Theorem 3.

Proposition C. [C2] *Let $A \subset \mathbb{C}$ be a finite set such that*

$$|A+A| < K|A|$$

for some constant K. For $n \in \mathbb{C}$, let

$$\pi_\ell(n) = |\{(a_1, \cdots, a_\ell) \in A^\ell : n = a_1 \cdots a_\ell\}|.$$

Then

$$\pi_\ell(n) < |A|^{\frac{C_\ell(K)}{\log\log|A|}}.$$

Here $C_\ell(K)$ is a constant depending on K and ℓ only.

Proof of Theorem 3. We will consider the sets $\log A$, and $\log B$ in order to replace multiplication by addition. Also, as in Theorem 2, we will use $\int' f$ instead of $\int f$. Returning to the argument in Theorem 1, we replace (5)-(8) and (10) by the following.

$$\pi(k) = |\{(a_1, \cdots, a_j, b) \in A^j \times B : k = a_1 \cdots a_j b\}| \tag{5'}$$

$$F(x) = \sum_{a\in A} e^{i(\log a)x}, \text{ and } G(x) = \sum_{b\in B} e^{i(\log b)x} \tag{6'}$$

$$|A^{(j)}B| > \frac{|A|^{2j}|B|^2}{\sum \pi(k)^2} \tag{7'}$$

$$\sum_k \pi(k)^2 = \int' |F(x)^j\ G(x)|^2 dx. \tag{8'}$$

$$\begin{aligned} \Big(\int' |F(x)|^{2jq}\Big)^{\frac{1}{q}} &= \Big(\sum_{n\in\mathbb{R}} \pi_{jq}(n)^2\Big)^{\frac{1}{q}} \qquad (10') \\ &< \Big(|A|^{jq}\ |A|^{\frac{2C_{jq}(K)}{\log\log|A|}}\Big)^{\frac{1}{q}} \\ &\le\ |A|^j\ |A|^{\frac{c_{jq}(K)}{q\log\log|A|}}, \qquad (19) \end{aligned}$$

where in (19) we used Proposition C with $l = jq$ and $\sum_n \pi_{jq}(n) = |A|^{jq}$.

We obtain that

$$|A^{(j)}B| > |A|^j\ |B|^{1-\frac{1}{q}}\ |A|^{\frac{-c_{jq}(K)}{\log\log|A|}}. \tag{20}$$

Take $q = [\frac{3}{\epsilon}]$. The last factor in (20) will be at least $|A|^{-\frac{\epsilon}{2}}$, provided K satisfies $c_{j[\frac{3}{\epsilon}]}(K) < \frac{\epsilon}{2}\log\log|A|$. $\square$

Acknowledgement. The authors would like to thank the referee for many helpful comments.

References

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

[BC]. J. Bourgain, M.-C. Chang, *On the size of k-fold sum and product sets of integers*, JAMS Vol. 17, No. 2, (2004), 473-497.

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

[C1]. M.-C. Chang, *Erdös-Szemeredi problem on sum set and product set*, Annals of Math. 157 (2003), 939-957.

[C2]. ———, *Factorization in generalized arithmetic progressions and applications to the Erdös-Szemerédi sum-product problems*, Geom. Funct. Anal. 113, (2002), 399-419.

[C3]. ———, *On sums and products of distinct numbers*, J. of Combinatorial Theory, Series A 105, (2004), 349-354.

[C4]. ———, *A sum-product estimate in algebraic division algebras over* $\mathbb{R}$, Israel J. of Math. (to appear).

[C5]. ———, *A sum-product theorem in semi-simple commutative Banach algebras*, J. Funct Anal, 212, (2004), 399-430..

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

[ER]. G. Elekes, J. Ruzsa, *Few sums, many products*, Studia Sci. Math. Hungar. 40 (2003).

[ES]. P. Erdös and E. Szemerédi, *On sums and products of integers*, in Studies in Pure Mathematics, Birkhauser, Basel, (1983), 213-218.

[ESS]. J.-H. Evertse, H. Schlickewei, W. Schmidt, *Linear equations in variables which lie in a multiplicative group*, Annals Math 155, (2002), 807-836.

[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.

[N1]. M.B. Nathanson, *The simplest inverse problems in additive number theory*, in Number Theory with an Emphasis on the Markoff Spectrum (A. Pollington and W. Moran, eds.), Marcel Dekker, 1993, pp. 191–206.

[N2]. ———, *On sums and products of integers*, Proc. Amer. Math. Soc. 125, (1997), 9-16.

[N3]. ———, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, Springer (1996).

[NT]. M. Nathanson and G. Tenenbaum, in Structure Theory of Set Addition, Astérisque 258 (1999).

[R]. 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).