A SUM-PRODUCT ESTIMATE IN ALGEBRAIC DIVISION ALGEBRAS OVER $\mathbb{R}$

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

Let A be a finite subset of an integral domain, and let $|A|$ denote the cardinality of the set A. The *sum set* of A is

$$2A \equiv A + A \equiv \{a_1 + a_2 \mid a_i \in A\}, \tag{0.1}$$

and the *product set* of A is

$$A^2 \equiv A.A \equiv \{a_1 a_2 \mid a_i \in A\}. \tag{0.2}$$

In [7], Erdös and Szemerédi conjectured that $|2A|$ and $|A^2|$ cannot both be small. More precisely, they made the following

Conjecture. $|2A| + |A^2| > |A|^{2-\epsilon}$.

What they proved is the following

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

$$|2A| + |A^2| \gtrsim |A|^{1+\delta}, \tag{0.3}$$

where δ is a constant.

Notation 1. $X \gtrsim Y$ means $X > cY$, for some nonzero constant c.

Nathanson [9] showed that $\delta = \frac{1}{31}$.

---

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

Ford [12] obtained that $\delta = \frac{1}{15}$, and Elekes [5] showed that $\delta = \frac{1}{4}$ by using Szemerédi-Trotter Theorem [11].

So far, the best bound is obtained by Solymosi [13] who showed that $\delta = \frac{3}{11+\epsilon}$ also by using Szemerédi-Trotter Theorem cleverly.

In a different direction, Bourgain, Katz, and Tao [1] proved the theorem for the case that A is a subset of a finite field.

For other related results, see [2], [3], [4], [6], [8], [10].

In this paper, we generalize the Erdős-Szemerédi argument to sets of elements contained in $\mathbb{C}$, the field of complex numbers, or $\mathbb{K}$, the quaternions, or certain normed subspaces V of an $\mathbb{R}$ algebra (See Theorem 3) .

Theorem 1. *Let A be a finite subset of $\mathbb{C}$, or $\mathbb{K}$. Then*

$$|2A| + |A^2| \gtrsim |A|^{1+\frac{1}{54}}. \tag{0.4}$$

The proof of Erdős-Szemerédi Theorem uses the order of real numbers and therefore it does not generalize trivially for the complex case. The problem for the complex case was brought up by I. Ruzsa (private communication).

The theorem follows from the following special case.

Theorem 2. *Let R be the annulus,*

$$R \equiv \{z \mid r \leq |z| \leq 2r\}, \tag{0.5}$$

contained in $\mathbb{C}$, or $\mathbb{K}$ and let $B \subset R$ be a finite subset of R. Then

$$|2B| + |B^2| \gtrsim |B|^{1+\delta}, \tag{0.6}$$

where

$$\delta = (\frac{1}{3} - \epsilon)\delta_1, \quad \delta_1 = \frac{1}{9}, \quad \epsilon = \frac{1}{100}. \tag{0.7}$$

Our method to prove Theorem 2 is to cover R with disjoint boxes Q of equal size such that the maximal number of elements of B contained in each of the boxes is $|B|^{\delta_1}$. We fix one such a maximal box called Q_0, assuming $|2B| \lesssim |B|^{1+\delta}$ and $|B^2| \lesssim |B|^{1+\delta}$, and show that "most" of the boxes have nearly as many elements as $B \cap Q_0$. For each of these boxes, we find a "large" subset C_Q such that we can define a map from $(B \cap Q_0)^8$ to $C_Q \times C_Q$. The cardinalities of the domain and the range give us a bound on δ_1.

The following theorem can be used to prove a sum-product theorem for symmetric matrices.

Theorem 3. *Let* $\{\mathbb{R}^m, +, *\}$ *be an* $\mathbb{R}$*-algebra with* $+$ *the componentwise addition. For* $a = (a_1, \cdots, a_m)$*, let* $|a| = \sqrt{(\sum a_i^2)}$ *be the Hilbert-Schmidt norm, and let* $V \subset \mathbb{R}^m$ *such that*
1. $\exists\ c = c(m),\ \forall a, b \in V,\ |\,a * b| = c|\,a|\,|\,b|$
2. for any $a \in V \setminus \{0\}, a^{-1}$ *exists (in a possibly larger field).*
Then for any $A \subset V$*,* $|A + A| + |AA| > |A|^{1+\delta}$*.*

The paper is organized as follows:
In Section 1, we prove Theorem 2.
In Section 2, we reduce Theorem 1 to Theorem 2.

For simplicity, we prove the theorems for complex numbers, and describe the differences for the cases of the quaternions and the normed subspace in Remark 2 (Section 1) and Remark 5 (Section 2) for those who care about the constant c as in Notation 1. (The exponents are the same for both $\mathbb{C}$ and $\mathbb{K}$.)

Section 1. The Theorem for an annulus.

Let $r > 0$ be as in (0.5). We define

$$A' = \{\frac{1}{r}a : a \in A\}.$$

Then

$$|A| = |A'|, |A + A| = |A' + A'|, |A.A| = |A'.A'|, \tag{1.1}$$

and we may rescale the annulus R and assume

$$R \equiv \{z \in \mathbb{C} : 1 \le |z| \le 2\}. \tag{1.2}$$

For any $\rho > 0$, the complex plane is covered by disjoint squares

$$O_{j,k} = \{p\rho + \sqrt{-1}\ q\rho : (j-1) \le p < j, (k-1) \le q < k\}, \tag{1.3}$$

where $j, k \in \mathbb{Z}$. (For convenience, sometimes we denote $Q_{j,k}$ by Q.)

We choose ρ such that

$$max_Q|B \cap Q| \sim |B|^{\delta_1}. \tag{1.4}$$

(See (0.7) for δ_1.)

Let

$$\mathcal{P} \equiv \{Q : Q \cap B \neq \emptyset\},$$

and Q_0 be an element of $\mathcal{P}$ with

$$|B \cap Q_0| \sim |B|^{\delta_1}. \tag{1.5}$$

First, we will show that the number of the sets $Q + Q_0$ and QQ_0 containing a fixed point is bounded by an absolute constant.

Claim 1. *Fix $Q \in \mathcal{P}$.*
1. For any $x \in Q + Q_0, |\{Q : x \in Q + Q_0\}| \leq 4$.
2. For any $x \in QQ_0, |\{Q : x \in QQ_0\}| \leq 25$.

Proof. (1) Let $Q_{j,k}$ be as in (1.3),

$$Q_{j,k} = \{p\rho + \sqrt{-1}\ q\rho : (j-1) \leq p < j, (k-1) \leq q < k\},$$

and Q_0 be as in (1.5),

$$Q_0 = \{p_0\rho + \sqrt{-1}\ q_0\rho : (j_0 - 1) \leq p_0 < j_0, (k_0 - 1) \leq q_0 < k_0\}.$$

Then $Q_{j,k} + Q_0$ is the set

$\{(p+p_0)\rho + \sqrt{-1}\ (q+q_0)\rho : (j+j_0-2) \leq p+p_0 < (j+j_0), (k+k_0-2) \leq q+q_0 < (k+k_0)\}$,

The only sums of squares intersecting $Q_{j,k}+Q_0$ are $Q_{j+1,k}+Q_0$,$Q_{j,k+1}+Q_0$, $Q_{j+1,k+1}+Q_0$.

(2) To count the number of products of squares containing x, we enclose each square by a disc with the same center and count the number of discs containing the product of the discs. We will use the "multiplicative" property of the Hilbert-Schmidt norm.

Let z_Q be the center of Q. Then any $z \in Q$ is contained in a disc centered at z_Q with radius $\frac{\rho}{\sqrt{2}}$. Therefore, we have

$$z = z_Q + d, \quad \text{where } |d| < \frac{\rho}{\sqrt{2}}. \tag{1.6}$$

Similarly, let z_{Q_0} be the center of Q_0. Then for any $z_0 \in Q_0$, we have

$$z_0 = z_{Q_0} + d_0, \quad \text{where } |d_0| < \frac{\rho}{\sqrt{2}}. \tag{1.7}$$

We see easily that zz_0 is contained in a disc centered at $z_Q z_{Q_0}$ with radius $\frac{7}{2}\rho$. In fact,

$$\begin{aligned} |zz_0 - z_Q z_{Q_0}| &\leq |dz_{Q_0}| + |d_0 z_Q| + |dd_0| \\ &\leq 2\frac{\rho}{\sqrt{2}}\,2 + \frac{\rho^2}{2} \\ &< \frac{7}{2}\rho. \end{aligned}$$

For the second inequality, we use the fact that $|z_Q|, |z_{Q_0}| \leq 2$.

The point zz_0 is in a disc centered at $z_Q z_{Q_o}$ if and only if $z_Q z_{Q_0}$ is in a disc centered at zz_0 with the same radius. Therefore, counting the number of discs containing zz_0 is the same as counting the number of $z_Q z_{Q_0}$ in the disc centered at zz_0. Since

$$|z_Q z_{Q_0} - z_{Q'} z_{Q_0}| \geq \rho, \tag{1.8}$$

a disc of radius $\frac{7}{2}\rho$ with center zz_0 contains at most 49 of the points $z_Q z_{Q_0}$. Therefore, every point zz_0 in QQ_0 is contained in at most 49 discs centered at $z_Q z_{Q_0}$, hence zz_0 is contained in at most 49 of the sets QQ_0 centered at $z_Q z_{Q_0}$.

Remark 2. *If $R \subset \mathbb{K}$, then we cover R with boxes Q of volume ρ^4. Therefore, every point is contained in at most 16 of the sets $Q + Q_0$, and at most 9^4 of the sets QQ_0. More generally, if V is as in Theorem 3, then a point in V is contained in at most 2^m of the sets $Q + Q_0$ and at most $[1 + 2(2\sqrt{m} + \frac{m}{4})]^2$ of the sets QQ_0.*

Next, we show that most squares have almost the maximal number of elements of B, if $|2B| < |B|^{1+\delta}$.

Claim 3. *We assume*

$$|2B| \; < \; |B|^{1+\delta}, \tag{1.9}$$

and let

$$\mathcal{P}_0 \equiv \{Q \in \mathcal{P} : \, |B|^{\delta_1 - (1+\epsilon)\delta} \; \leq \; |B \cap Q| \; \leq \; |B|^{\delta_1}\}. \tag{1.10}$$

Then

$$|\mathcal{P}_0| \; \gtrsim \; |B|^{1-\delta_1}. \tag{1.11}$$

Proof. First, it follows from (1.9), Claim 1 and (1.5) that

$$\begin{aligned} |B|^{1+\delta} > |\, 2B| >& |\bigcup_{Q \in \mathcal{P}} (B \cap Q_0) + (B \cap Q)| \\ >& \frac{1}{4} \sum_{Q \in \mathcal{P}} |(B \cap Q_0) + (B \cap Q)| \\ \gtrsim& |\mathcal{P}| \, |B \cap Q_0| \sim |\mathcal{P}||B|^{\delta_1} \end{aligned} \tag{1.12}$$

Therefore,

$$|\mathcal{P}| \; \lesssim \; |B|^{1+\delta-\delta_1}. \tag{1.13}$$

Next, we see that (1.10) and (1.13) imply

$$\sum_{Q \in \mathcal{P} \setminus \mathcal{P}_0} |B \cap Q| \; < |\mathcal{P} \setminus \mathcal{P}_0||B|^{\delta_1 - (1+\epsilon)\delta} \; \leq \; |\mathcal{P}| \, |B|^{\delta_1 - (1+\epsilon)\delta} \; \lesssim \; |B|^{1-\epsilon\delta}, \tag{1.14}$$

which is $< \frac{1}{2}|B|$, when $|B|$ is sufficiently large. Hence

$$\sum_{Q \in \mathcal{P}_0} |B \cap Q| \; > \; \frac{1}{2}|B| \, , \tag{1.15}$$

which, together with (1.4) gives (1.11).

The next claim shows that for almost all $Q \in \mathcal{P}_0$, the sum sets of $B \cap Q$ and $B \cap Q_0$ are not too big, if $|2B| < |B|^{1+\delta}$.

Claim 4. *We assume*

$$|2B| \ < \ |B|^{1+\delta}, \tag{1.16}$$

and let

$$\mathcal{P}_1 \equiv \{Q \in \mathcal{P}_0 \ : \ |(B \cap Q) + (B \cap Q_0)| \ < \ |B|^{\delta_1 + (1+\epsilon)\delta}\}. \tag{1.17}$$

Then

$$|\mathcal{P}_1| \ \gtrsim \ |B|^{1-\delta_1}. \tag{1.18}$$

Proof. By (1.16), Claim 1, and (1.17), we have

$$\begin{aligned} |B|^{1+\delta} \ > \ |2B| \ &> \ |\bigcup_{Q \in \mathcal{P}_0 \setminus \mathcal{P}_1} (B \cap Q_0) + (B \cap Q)| \\ &> \ \frac{1}{4} \sum_{Q \in \mathcal{P}_0 \setminus \mathcal{P}_1} |(B \cap Q) + (B \cap Q_0)| \\ &\geq \ |\mathcal{P}_0 \setminus \mathcal{P}_1| \, |B|^{\delta_1 + (1+\epsilon)\delta}. \end{aligned} \tag{1.19}$$

Hence,

$$|\mathcal{P}_0 \setminus \mathcal{P}_1| \ \leq \ |B|^{1-\delta_1-\epsilon\delta}. \tag{1.20}$$

Now, (1.18) follows from (1.11) and (1.20).

Standard Construction

Let $Q \in \mathcal{P}_1$ be fixed, and let Y be a maximal subset of $B \cap Q$, such that the sets $y + (B \cap Q_0)$ for $y \in Y$ are all disjoint. The following gives an estimate of $|Y|$.

Claim 5. $|Y| \ < \ |B|^{(1+\epsilon)\delta}$.

Proof. The claim follows from (1.5) and the following inequality

$$|Y| \, |B \cap Q_0| = \sum_{y \in Y} |y + (B \cap Q_0)| \leq |(B \cap Q) + (B \cap Q_0)| < |B|^{\delta_1 + (1+\epsilon)\delta}.$$

The last inequality is by (1.17).

Claim 6. *For $z \in B \cap Q$, we define $B_z = (B \cap Q) \cap \big(z + (B \cap Q_0) - (B \cap Q_0)\big)$. Then there is a point $z_Q \in B \cap Q$, such that*

$$|B_{z_Q}| \; > \; |B|^{\delta_1 - 2(1+\epsilon)\delta}. \tag{1.21}$$

Proof. The maximality of Y implies that

$$B \cap Q \subset \bigcup_{y \in Y} \big(y + (B \cap Q_0) - (B \cap Q_0)\big). \tag{1.22}$$

Therefore,

$$B \cap Q \; = \; \bigcup_{y \in Y} \Big((B \cap Q) \cap \big(y + (B \cap Q_0) - (B \cap Q_0)\big)\Big), \tag{1.23}$$

and there is $z_Q \in Y$, such that

$$|B_{z_Q}| = |(B \cap Q) \cap \big(z_Q + (B \cap Q_0) - (B \cap Q_0)\big)| \; \geq \; \frac{|B \cap Q|}{|Y|}. \tag{1.24}$$

Hence,

$$|B_{z_Q}| \geq |B|^{\delta_1 - (1+\epsilon)\delta - (1+\epsilon)\delta},$$

because of (1.10) and Claim 5.

Remark 6.1. Denoting B_{z_Q} by B_Q, we have

$$B_Q = (B \cap Q) \cap \big(z + (B \cap Q_0) - (B \cap Q_0)\big). \tag{1.25}$$

Hence

$$B_Q - B_Q \subset 2(B \cap Q_0) - 2(B \cap Q_0). \tag{1.26}$$

Now, we will do the same construction with the product sets.

Claim 7. *We assume*

$$|B^2| \; < \; |B|^{1+\delta}, \tag{1.27}$$

and let

$$\mathcal{P}_2 \equiv \{Q \in \mathcal{P}_1 : \, |(B \cap Q)(B \cap Q_0)| \; < \; |B|^{\delta_1 + (1+\epsilon)\delta}\}. \tag{1.28}$$

Then

$$|\mathcal{P}_2| \; > \; |\mathcal{P}_1| - |B|^{1 - \delta_1 - \epsilon\delta}.$$

In particular, if $|2B| + |B^2| < |B|^{1+\delta}$, then

$$|\mathcal{P}_0| \sim |\mathcal{P}_1| \sim |\mathcal{P}_2| \sim |B|^{1-\delta_1}. \tag{1.29}$$

Proof. The same as Claim 4.

Fix $Q \in \mathcal{P}_2$, and let Y' be a maximal subset of $B \cap Q$, such that the sets $y'(B \cap Q_0)$ for $y' \in Y'$ are all disjoint.

Claim 8. $|Y'| < |B|^{(1+\epsilon)\delta}$.

Proof. The same as Claim 5.

Remark 8.1. *Here we use the fact that* $|B \cap Q_0| = |y'(B \cap Q_0)|$. *This property holds for* V *in Theorem 3, because* $(y')^{-1}$ *exists.*

Since our results hold for the case when multiplication is not commutative, we will use the notation of inverse set.

Notation 2. $A^{-1} = \{a^{-1} : a \in A\}$

Claim 9. *For* $z' \in B_Q$, *we define* $C_{z'} = B_Q \cap z'(B \cap Q_0)(B \cap Q_0)^{-1}$. *Then there is a point* $z'_Q \in B_Q$, *such that*

$$|C_{z'_Q}| > |B|^{\delta_1 - 3(1+\epsilon)\delta}. \tag{1.30}$$

Proof. The same as Claim 6.

Remark 9.1. Denoting $C_{z'_Q}$ by C_Q, we have

$$C_Q = B_Q \cap z'(B \cap Q_0)(B \cap Q_0)^{-1}, \tag{1.31}$$

and

$$C_Q^{-1} C_Q \subset (B \cap Q_0)(B \cap Q_0)^{-1}(B \cap Q_0)(B \cap Q_0)^{-1}. \tag{1.32}$$

Moreover, Remark 6.1 and (1.31) give

$$C_Q - C_Q \subset 2(B \cap Q_0) - 2(B \cap Q_0). \tag{1.33}$$

Proof of Theorem 2. For any $Q \in \mathcal{P}_2$ and for any $z \neq z' \in C_Q$, (1.33) implies that there are $z_1, \dots, z_4 \in B \cap Q_0$, such that

$$z' - z = z_1 + z_2 - z_3 - z_4, \tag{1.34}$$

and (1.32) implies that there are $z_5, \dots, z_8$, such that

$$z^{-1} z' = z_5\, z_6^{-1} z_7\, z_8^{-1}. \tag{1.35}$$

Therefore, given $(z_1, \dots, z_8) \in (B \cap Q_0) \times \cdots \times (B \cap Q_0)$, (1.34) and (1.35) determine z, z' uniquely.

$$\begin{aligned} z &= (z_1 + z_2 - z_3 - z_4)(z_5\, z_6^{-1} z_7\, z_8^{-1} - 1)^{-1} \\ z' &= (z_1 + z_2 - z_3 - z_4)\big((z_5\, z_6^{-1} z_7\, z_8^{-1} - 1)^{-1} + 1\big). \end{aligned} \tag{1.36}$$

Namely, (1.34) and (1.36) define a map on $(B \cap Q_0) \times \cdots \times (B \cap Q_0)$ whose image contains $C_Q \times C_Q$. Thus, we have

$$|B \cap Q_0|^8 \geq \sum_{Q \in \mathcal{P}_2} |C_Q|^2 \gtrsim |B|^{1+\delta_1 - 6(1+\epsilon)\delta}. \tag{1.37}$$

The last inequality follows from (1.29) and (1.30).

Now, the theorem follows from (1.5) and (1.37).

Remark. *To prove Theorem 3, we observe that*

$$z(z_5z_6^{-1}z_7z_8^{-1}-1)=z_1+z_2-z_3-z_4\in V\setminus\{0\}.$$

Hence $(z_5z_6^{-1}z_7z_8^{-1}-1)^{-1}$ *exists for* $z_5,\cdots,z_8\in B\cap Q_0$.

Section 2. The General Case.

In this section we will use Theorem 2 to prove Theorem 1.

First, according to (1.1), we may assume that

$$A\subset\{\ z:\ 1<|z|\ \}.$$

We define, for any $k\in\mathbb{N}$,

$$A_k=\{z\in A:\ 2^{k-1}<|z|\ \le 2^k\}. \tag{2.1}$$

Claim 1. *There is a set* $K\subset\mathbb{N}$ *such that for any* $k\in K$, *we have*

$$|A_k|>\frac{|A|}{2|K|\ \log_2|A|}, \tag{2.2}$$

where $\log_2|A|\equiv\lceil\log_2|A|\rceil$.

Proof. For $l=1,\cdots,\log_2|A|$, we define

$$K_l=\{k\ \mid\ 2^{l-1}\le\ |A_k|<2^l\}. \tag{2.3}$$

Therefore,

$$\sum_l 2^l|K_l|>|A|,$$

and there is $\bar{l}$ such that

$$2^{\bar{l}}|K_{\bar{l}}|>\frac{|A|}{\log_2|A|}.$$

Let $K=K_{\bar{l}}$. Then for any $k\in K$,

$$|A_k|\ge 2^{\bar{l}-1}>\frac{|A|}{2|K|\ \log_2|A|}.$$

Claim 2. *To estimate* $|2A_k|$ *and* $|A_k^2|$*, we may assume that* A_k *is contained in one of the quadrants, and*

$$|A_k| > \frac{|A|}{2^3|K| \ \log_2 |A|}. \tag{2.4.}$$

Furthermore, for any $z_1, z_2 \in A_k$*,*

$$|z_1 + z_2| \geq \max\{|z_1|, |z_2|\}. \tag{2.5}$$

Proof. One of the four quadrants contains at least $\frac{1}{4}|A_k|$ elements of A_k. To see (2.5), we note that $\sqrt{(\Re z_1 + \Re z_2)^2 + (\Im z_1 + \Im z_2)^2} \geq \sqrt{(\Re z_i^2 + \Im z_i^2)}$, because z_1, z_2 are in the same quadrant implies that $|\Re z_1 + \Re z_2|^2 \geq \max\{|\Re z_1|^2, |\Re z_2|^2\}$ and $|\Im z_1 + \Im z_2|^2 \geq \max\{|\Im z_1|^2, |\Im z_2|^2\}$.

Claim 3. *Every element of* $2A$ *lies in at most two of the sets* $2A_k$*, and every element of* A^2 *lies in exactly one of the sets* A_k^2*.*

Proof. Let $z_1, z_2 \in A_k$. Then

$$2^{k-1} < |z_1 + z_2| \leq 2^{k+1}, \tag{2.6}$$

and

$$4^{k-1} < |z_1 z_2| \leq 4^k. \tag{2.7}$$

The first inequality in (2.6) follows from (2.5). Let z be an element with norm between 2^{k-1} and 2^k for some k. Then z can only be in $2A_{k-1}$ and $2A_k$.

Claim 4. *Let* δ *be the absolute constant given in Theorem 2. Then*

$$|2A| + |A^2| > \frac{|A|^{1+\delta}}{2^{4+3\delta}|K|^\delta(\log_2 |A|)^{1+\delta}}. \tag{2.8}$$

Proof. Claim 3 gives the following inequalities.

$$|2A| > |\bigcup_{k\in K} 2A_k| \geq \frac{1}{2}\sum_{k\in K} |2A_k|, \tag{2.9}$$

$$|A^2| > |\bigcup_{k\in K} A_k^2| \geq \sum_{k\in K} |A_k^2|. \tag{2.10}$$

Adding (2.9) and (2.10) together, and applying Theorem 2 to A_k, we have

$$|2A| + |A^2| > \frac{1}{2}\sum_{k\in K} |A_k|^{1+\delta} > \frac{|A|^{1+\delta}}{2^{4+3\delta}|K|^\delta(\log_2 |A|)^{1+\delta}}. \tag{2.11}$$

The last inequality follows from (2.4).

We divide the proof into two cases.

Case 1. $|K| < |A|^{\frac{1}{2}+\epsilon}$.

Then from (2.11)

$$|2A| + |A^2| \gtrsim \frac{|A|^{1+\delta-(\frac{1}{2}+\epsilon)\delta}}{(\log_2 |A|)^{1+\delta}} \gtrsim |A|^{1+(\frac{1}{2}-2\epsilon)\delta}. \tag{2.12}$$

Case 2. $|K| > |A|^{\frac{1}{2}+\epsilon}$.

For each $k \in K$, we pick $z_k \in A_k$. We may assume that there is $K_1 \subset K$ with $|K_1| > \frac{1}{2}|K|$ such that

$$\frac{1}{\sqrt{2}}\, 2^{k-1} < \Re z_k < 2^k, \text{ for all } k \in K_1. \tag{2.13}$$

Hence,

$$\begin{aligned} |2A| &\geq |\{\ z_k + z_{k'} : k, k' \in K_1\}| \\ &\geq |\ \{\ \Re z_k + \Re z_{k'} : k, k' \in K_1\}| \\ &> \frac{1}{3}|K_1|^2 \\ &\gtrsim |A|^{1+2\epsilon} \\ &> |A|^{1+(\frac{1}{2}-2\epsilon)\delta}. \end{aligned} \tag{2.14}$$

The third inequality is by the same reasoning as that in Claim 1 in Section 1. The last inequality follows from our assumption (0.7).

Finally, (2.12), (2.14), and (0.7) conclude the proof of the theorem.

Remark 5. *If $A \subset \mathbb{K}$, then in (2.4), (2.8), and (2.11), 2^3 and $2^{4+3\delta}$ are replaced by 2^5 and $2^{6+5\delta}$. Also in (2.13), $\frac{1}{\sqrt{2}}2^{k-1}$ and $|K_1| > \frac{1}{2}|K|$ are replaced by $\frac{1}{\sqrt{4}}2^{k-1}$ and $|K_1| > \frac{1}{4}|K|$. For the normed space V, we have $2^{m+1}, 2^{(m+1)(\delta+1)+1}$, $\frac{1}{\sqrt{m}}2^{k-1}$, $\frac{1}{m}|K|$ instead.*

Acknowledgement. *The author would like to thank J. Stafney for helpful discussions.*

References

[1]. J. Bourgain, N. Katz, and T. Tao, *A sum-product estimate in finite fields, and applications*, preprint.

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

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

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

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

[6]. G. Elekes, J. Ruzsa, *Product sets are very large if sumsets are very small*, preprint.

[7]. P. Erdős and E. Szemerédi, *On sums and products of integers*, in Studies in Pure Mathematics, Birkhauser, Basel, 1983, pp. 213-218.

[8]. 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.

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

[10]. M. Nathanson and G. Tenenbaum, *Inverse theorems and the number of sums and products*, in Structure Theory of Set Addition, Astérisque 258 (1999).

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

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

[13]. J. Solymosi, *On the number of sums and products,*, (preprint) (2003).