On sum-sets and product-sets of complex numbers

par JÓZSEF SOLYMOSI

RéSUMÉ. On donne une preuve simple que pour tout ensemble fini de nombres complexes $A$, la taille de l’ensemble de sommes $A + A$ ou celle de l’ensemble de produits $A \cdot A$ est toujours grande.

Abstract. We give a simple argument that for any finite set of complex numbers $A$, the size of the sum-set, $A + A$, or the product-set, $A \cdot A$, is always large.

1. Introduction

Let $A$ be a finite subset of complex numbers. The sum-set of $A$ is $A + A = \{a + b : a, b \in A\}$, and the product-set is given by $A \cdot A = \{a \cdot b : a, b \in A\}$. Erdős conjectured that for any $n$-element set the sum-set or the product-set should be close to $n^2$. For integers, Erdős and Szemerédi [7] proved the lower bound $n^{1+\varepsilon}$.

$$\max(|A + A, |A \cdot A|) \geq |A|^{1+\varepsilon}.$$  

Nathanson [9] proved the bound with $\varepsilon = 1/31$, Ford [8] improved it to $\varepsilon = 1/15$, and the best bound is obtained by Elekes [6] who showed $\varepsilon = 1/4$ if $A$ is a set of real numbers. Very recently Chang [3] proved $\varepsilon = 1/54$ to finite sets of complex numbers. For further results and related problems we refer to [4, 5] and [1, 2].

In this note we prove Elekes’ bound for complex numbers.

Theorem 1.1. There is a positive absolute constant $c$, such that, for any finite sets of complex numbers $A, B,$ and $Q$,

$$c|A|^{3/2}|B|^{1/2}|Q|^{1/2} \leq |A + B| \cdot |A \cdot Q|,$$

whence $c|A|^{5/4} \leq \max(|A + A|, |A \cdot A|)$. 

Manuscrit reçu le 26 aout 2003.

This research was supported by NSERC and OTKA grants.
2. Proof

For the proof we need some simple observations and definitions. For each \( a \in A \) let us find "the closest" element, an \( a' \in A \) so that \( a' \neq a \) and for any \( a'' \in A \) if \( |a - a'| > |a - a''| \) then \( a = a'' \). If there are more then one closest elements, then let us select any of them. This way we have \(|A|\) ordered pairs, let us call them neighboring pairs.

**Definition.** We say that a quadruple \((a, a', b, q)\) is good if \((a, a')\) is a neighboring pair, \(b \in B\) and \(q \in Q\), moreover

\[
\left| \{u \in A + B : |a + b - u| \leq |a - a'| \} \right| \leq \frac{28|A + B|}{|A|}
\]

and

\[
\left| \{v \in A \cdot Q : |aq - v| \leq |aq - a'|q| \} \right| \leq \frac{28|A \cdot Q|}{|A|}.
\]

When a quadruple \((a, a', b, q)\) is good, then it means that the neighborhoods of \(a + b\) and \(aq\) are not very dense in \(A + B\) and in \(A \cdot Q\).

**Lemma 2.1.** For any \(b \in B\) and \(q \in Q\) the number of good quadruples \((a, a', b, q)\) is at least \(|A|/2\).

**Proof.** Let us consider the set of disks around the elements of \(A\) with radius \(|a - a'|\) (i.e. for every \(a \in A\) we take the largest disk with center \(a\), which contains no other elements of \(A\) in it’s interior). A simple geometric observation shows that no complex number is covered by more then \(7\) disks. Therefore

\[
\sum_{a \in A} \left| \{u \in A + B : |a + b - u| \leq |a - a'| \} \right| \leq 7|A + B|
\]

and

\[
\sum_{a \in A} \left| \{v \in A \cdot Q : |aq - v| \leq |aq - a'|q| \} \right| \leq 7|A \cdot Q|
\]

providing that at least half of the neighboring pairs form good quadruples with \(b\) and \(q\). Indeed, if we had more then a quarter of the neighboring pairs so that, say,

\[
\left| \{v \in A \cdot Q : |aq - v| \leq |aq - a'|q| \} \right| > \frac{28|A \cdot Q|}{|A|}
\]

then it would imply

\[
7|A \cdot Q| \geq \frac{|A|}{4} \left| \{v \in A \cdot Q : |aq - v| \leq |aq - a'|q| \} \right| > 7|A \cdot Q|.
\]

\(\square\)
Proof of Theorem 1 To prove the theorem, we count the good quadruples \((a, a', b, q)\) twice. For the sake of simplicity let us suppose that \(0 \notin Q\). Such a quadruple is uniquely determined by the quadruple \((a + b, a' + b, aq, a'q)\). Now observe that there are \(|A + B|\) possibilities for the first element, and given the value of \(a + b\), the second element \(a' + b\) must be one of the nearest element of the sum-set \(A + B\). We make the same argument for the third and fourth component to find that the number of such quadruples is at most
\[
|A + B| \frac{28|A + B|}{|A|} \frac{|A \cdot Q|}{|A|} 28|A \cdot Q| .
\]
On the other hand, by Lemma 1 the number of such quadruples is at least
\[
\frac{|A|}{2} |B| |Q|
\]
that proves the theorem.

A similar argument works for quaternions and for other hypercomplex numbers. In general, if \(T\) and \(Q\) are sets of similarity transformations and \(A\) is a set of points in space such that from any quadruple \((t(p_1), t(p_2), q(p_1), q(p_2))\) the elements \(t \in T, q \in Q, \) and \(p_1 \neq p_2 \in A\) are uniquely determined, then
\[
c|A|^{3/2} |T|^{1/2} |Q|^{1/2} \leq |T(A)| \cdot |Q(A)|,
\]
where \(c\) depends on the dimension of the space only.

References

József SOLY MOSI
Department of Mathematics,
University of British Columbia
1984 Mathematics Road, Vancouver,
Colombie-Britannique, Canada V6T 1Z2
E-mail: solymosi@math.ubc.ca