ON SUMS AND PRODUCTS OF DISTINCT NUMBERS

Mei-Chu Chang
Department of Mathematics
University of California
Riverside, CA 92521

Abstract Let A be a set of k complex numbers, and let A^+ (respectively, $A^\times$) be the set of sums (resp. products) of distinct elements of A. Let

$$g_{\mathbb{C}}(k) = \min_{A\subset\mathbb{C}, |A|=k} \{|A^+| + |A^\times|\}.$$

Ruzsa posed the question whether $g_{\mathbb{C}}(k)$ grows faster than any power of k. In this note we give an affirmative answer to this question.

Let A be a set of k complex numbers, and let A^+ and $A^\times$ be the sets of sums and products of distinct elements of A:

$$A^+ = \left\{ \sum_{i=1}^k \varepsilon_i a_i \colon a_i \in A, \varepsilon_i = 0 \text{ or } 1 \right\},$$
$$A^\times = \left\{ \prod_{i=1}^k a_i^{\varepsilon_i} \colon a_i \in A, \varepsilon_i = 0 \text{ or } 1 \right\}.$$

In [E-S] Erdős and Szemerédi considered

$$g_{\mathbb{Z}}(k) = \min_{A\subset\mathbb{Z}, |A|=k} \{|A^+| + |A^\times|\}$$

(thus here A is a set of integers) and conjectured that $g_{\mathbb{Z}}(k)$ grows faster than any power of k. More precisely, they observed that

$$g_{\mathbb{Z}}(k) < k^{c\frac{\log k}{\log\log k}}$$

for some absolute constant $c > 0$ and conjectured that there exists an absolute constant $c' > 0$ such that

$$g_{\mathbb{Z}}(k) > k^{c' \frac{\log k}{\log \log k}}. \tag{1}$$

In [Ch1], we established (1). The argument relies heavily on factorization into primes and moment inequalities for trigonometric polynomials and does not extend beyond the integer case.

More recently, Ruzsa [R1] proposed the problem to get a nontrivial estimate for

$$g_{\mathbb{R}}(k) = \min_{A \subset \mathbb{R}, |A|=k} \{|A^+| + |A^\times|\},$$

and for

$$g_{\mathbb{C}}(k) = \min_{A \subset \mathbb{C}, |A|=k} \{|A^+| + |A^\times|\}. \tag{2}$$

Our main result is

Theorem 1. *Let $g_{\mathbb{C}}(k)$ be defined as in (2). Then*

$$\lim_{k \to \infty} \frac{\log g_{\mathbb{C}}(k)}{\log k} = \infty.$$

Hence $g_{\mathbb{C}}(k)$ (and consequently $g_{\mathbb{R}}(k) \geq g_{\mathbb{C}}(k)$) grows faster than any power of k.
We don't know if the analogue of (1) holds true for $g_{\mathbb{C}}(k)$.
The approach is substantially different from [Ch1] and our main tool is the new result on factorization in "generalized arithmetic progressions" (as defined in the following theorem) established in [Ch2].

Theorem 2 ([Ch2], Proposition 3). *Let P be a generalized arithmetic progression*

$$P = P(c_0; c_1, \ldots, c_d; J_1, \ldots, J_d) = \left\{ c_0 + \textstyle\sum_{i=1}^d k_i c_i : k_i \in [0, J_i[\right\},$$

with generators $c_1, \ldots, c_d \in \mathbb{C}$. Set $J = \max_i J_i$. Then for any $h \geq 2$ and any $n \in \mathbb{C}$ the number of representations $r_h(n) = r_h(n, P)$ of n as a product of h elements of P satisfies

$$r_h(n) < J^{\frac{C_{d,h}}{\log \log J}}.$$

The proof uses the theory of factorization in algebraic number fields.

There are two more ingredients in our argument.
The first is Freiman's theorem [F] on the structure of sets with small sumsets.

Theorem (Freiman) [N, Theorem 8.1]. *Let G be a torsion free abelian group and let $A \subset G$ be a finite subset. If α is a real number such that $|2A| < \alpha|A|$, then there exist real $C_1 = C_1(\alpha)$ and $C_2 = C_2(\alpha)$ (depending only on α) and a generalized progression P as defined above, such that $A \subset P$, with*

$$d \leq C_1$$

and

$$|P| \leq C_2|A|.$$

Finally, use Plünnecke-Ruzsa sumset estimate; see [R3] or [N, Theorem 7.8].

Lemma 3 (Ruzsa's Inequality) [R3]. *Let ρ be a real number and let M and N be finite subsets of an abelian group such that*

$$|M + N| \leq \rho|M|.$$

Let $h \geq 1$ and $\ell \geq 1$. Then

$$|hN - \ell N| \leq \rho^{h+\ell}|M|.$$

Proof of Theorem 1. For brevity we write $g(k)$ rather than $g_{\mathbb{C}}(k)$.

Fix a positive real number c (so that all constants depending on c will also be considered fixed) and suppose that there exists $A \subset \mathbb{C}$ of arbitrarily large cardinality $k = |A|$ such that $|A^+| + |A^\times| \leq k^c$.

We split A into $\lfloor\sqrt{k}\rfloor$ disjoint subsets $B_1, B_2, \cdots$, each of cardinality at least $\lfloor\sqrt{k}\rfloor$. Let

$$\rho = 1 + k^{-1/5}$$

and

$$A_s = \bigcup_{i=1}^{s} B_i.$$

If $|A^+_{s+1}| > \rho\,|A^+_s|$ for all $s \leq \sqrt{k} - 1$ then

$$|A^+| \;>\; \rho^{\lfloor\sqrt{k}\rfloor - 1}|A^+_1| \;>\; \rho^{\sqrt{k}} \;=\; \left((1 + k^{-\frac{1}{5}})^{k^{\frac{1}{5}}}\right)^{k^{\frac{1}{2}-\frac{1}{5}}} \;>\; e^{k^{\frac{1}{4}}},$$

contradicting the assumption; thus there exists $1 \leq s \leq \sqrt{k} - 1$ such that $|A^+_{s+1}| \leq \rho\,|A^+_s|$.

Let $B = B_{s+1}$ and let $\ell = \lceil k^{\frac{1}{5}} \rceil$; we claim then that

$$|\ell B| \;<\; 3\,k^c. \tag{3}$$

Indeed, we have

$$|A_s^+ + B| \;\le\; |A_s^+ + B^+| = |A_{s+1}^+| \;\le\; \rho\, |A_s^+|\,,$$

which by Lemma 3 implies

$$|\ell B| \le |(\ell+1)B - B| \;\le\; \rho^{\ell+2}\, |A_s^+|.$$

As $\rho^{\ell+2} = (1+k^{-\frac{1}{5}})^{\lceil k^{\frac{1}{5}}\rceil+2} < 3$ for sufficiently large k, we obtain

$$|\ell B| \;<\; 3\,|A^+| \;\le\; 3\,k^c. \tag{4}$$

Put

$$c_1 \;=\; 2^{10c}$$

and suppose that

$$|2^{j+1}B| \;>\; c_1|2^jB| \tag{5}$$

for all positive integers $j \le \log_2 \ell$. Then by (5) we have

$$\begin{aligned} |\ell B| \;&\ge\; c_1^{\lfloor \log_2\,\ell\rfloor}|B| \\ &>\; c_1^{\log_2\,\ell} \\ &=\; \ell^{\log_2\,c_1} \\ &=\; \ell^{10c} \\ &\ge\; k^{2c}. \end{aligned}$$

(The second inequality holds since $|B| > \sqrt{k} - 1 > c_1$.)

Now by (4) we get

$$k^c \;>\; \frac{1}{3}\,|\ell B| \;>\; \frac{1}{3}\,k^{2c},$$

which is a contradiction.

Thus, there exists some $j \le \log_2 \ell$ such that

$$|2^jB + 2^jB| \;=\; |2^{j+1}B| \;\le\; c_1\,|2^jB|. \tag{6}$$

Inequality (3) gives

$$|2^jB| \;\le\; 3\,k^c. \tag{7}$$

Applying Freiman's Theorem to (6) we find two positive constants C_1 and C_2, depending only on c, and a generalized arithmetic progression P of dimension $d < C_1$ such that

$$2^jB \;\subset\; P, \tag{8}$$

and

$$|P| \leq C_2 \, |2^j B|.$$

From (7) we get

$$|P| \leq c_2 \, k^c$$

(where c_2 depends only on c). Also, (8) implies that

$$B \subset x + P$$

for any fixed $x \in -(2^j - 1)B$.

Note that Theorem 2 gives

$$r_h(n, x+P) < |P|^{\frac{c(h)}{\log \log |P|}} = e^{c(h) \frac{\log |P|}{\log \log |P|}},$$

for any $n \in \mathbb{C}$ and $h \geq 2$, where $c(h)$ is a constant dependent on c and h.

It follows that the number of representations of n as a product of h elements of B is at most

$$\begin{aligned} r_h(n, x+P) &< e^{c(h) \frac{\log(c_2 k^c)}{\log \log (c_2 k^c)}} \\ &< e^{c_1(h) \frac{\log k}{\log \log k}} \\ &= k^{\frac{c_1(h)}{\log \log k}} \\ &< k^{\epsilon}, \end{aligned}$$

for any fixed $\epsilon > 0$ and h, and for k large enough.

Next, using the Stirling formula in the form

$$\left(\frac{n}{e}\right)^n \sqrt{2\pi n} < n! < 2 \left(\frac{n}{e}\right)^n \sqrt{2\pi n}$$

we find a lower bound on $\binom{|B|}{h}$ in terms of k. Let $b = |B|$ (which is $> k^{\frac{1}{2}} - 1$). Then there exists an absolute constant h_0 such that for $h_0 < h < k^{1/5} - 1$ we have

$$\begin{aligned} \binom{|B|}{h} &> \frac{1}{4\sqrt{2\pi}} \left(\frac{b}{h}\right)^h \left(\frac{b}{b-h}\right)^{b-h+\frac{1}{2}} \frac{1}{\sqrt{h}} \\ &> \frac{1}{4\sqrt{2\pi}} \left(\frac{b}{h}\right)^h \frac{1}{\sqrt{h}} \\ &> \frac{1}{4\sqrt{2\pi}} \, k^{(\frac{1}{2} - \frac{1}{5})h - \frac{1}{10}} \\ &> k^{\frac{h}{4}}. \end{aligned}$$

We conclude that for any h as above holds

$$|B^\times| > k^{-\epsilon} \binom{|B|}{h} > k^{-\epsilon} k^{\frac{h}{4}},$$

and thus

$$k^c > |A^\times| > |B^\times| > k^{\frac{h}{4}-\epsilon}.$$

Appropriate choice of h gives the contradiction. $\square$

Acknowledgement The author would like to thank the referee for various helpful comments.

References

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

[Ch1]. M. Chang, *Erdös-Szemerédi problem on sum set and product set*, Annals of Math. **157** (2003), 939-957.

[Ch2]. M. Chang, *Factorization in generalized arithmetic progressions and applications to the Erdös-Szemerédi sum-product problems*, Geom. Funct. Anal. (to appear).

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

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

[N]. M.B. Nathanson, *Additive Number Theory: Inverse Problems and the Geometry of Sumsets, Springer (1996)..*

[R1]. I. Ruzsa, *Private Communication.*

[R2]. I. Ruzsa, *An analog of Freiman's theorem in groups*, in 'Structure Theory of Set Addition', Astérisque 258 (1999).

[R3]. I. Ruzsa, *Sums of finite sets*, Number Theory: New York Seminar (D. V. Chudnovsky, G. V. Chudnovsky, M. B. Nathanson, eds.), Springer-Verlag, 1996.