8.3 The sum-product problem in R

In Section 2.8 we considered the *sum-product problem*, where one wished to establish lower bounds on either the sum set $A + A$ or the product set $A \cdot A$ when A was an arbitrary non-empty finite subset of a field or ring. For instance, it was shown there that if the ambient field contained no proper subfields, then one had $|A + A| + |A \cdot A| = \Omega(|A|^{1+\varepsilon})$ for some explicit $\varepsilon > 0$. In the case when A is a set of integers (or more generally of real numbers), Erdős and Szemerédi conjectured the following stronger result:

Conjecture 8.13 (Erdős–Szemerédi conjecture) *[91] Let A be a finite non-empty set of integers or reals. Then for any $\varepsilon > 0$ we have*

$$|A + A| + |A \cdot A| \geq \Omega_\varepsilon(|A|^{2-\varepsilon}).$$

The condition $\varepsilon > 0$ is sharp; see Exercise 8.3.6.

In support of this conjecture, Erdős and Szemerédi [91] proved the bound $|A + A| + |A \cdot A| \geq \Omega(|A|^{1+\delta})$ for some absolute constant $\delta > 0$, when A is a set of integers. Nathanson [258] showed that one can set $\delta = 1/31$. Ford [105] improved δ to $1/15$. These proofs relied on properties of factorizations.

In 1997, Elekes [76] improved δ to $1/4$ and extended to the case of real numbers, using the Szemerédi–Trotter theorem in an ingenious way.

Theorem 8.14 *Let A be a finite non-empty set of reals. Then*

$$|A + A| \times |A \cdot A| = \Omega\big(|A|^{5/2}\big).$$

In particular

$$|A + A| + |A \cdot A| = \Omega\big(|A|^{5/4}\big).$$

Proof Let $P = \{(a, b) | a \in A + A, b \in A \cdot A\}$; P is a subset of the plane and has cardinality $|A + A||A \cdot A|$.

Consider the set L of lines of the form $\{(x, y) : y = a(x - b)\}$ where a, b are elements of A. Clearly, L has $|A|^2$ elements. Moreover, each such line contains at least $|A|$ points in P, namely the points $(b + c, ac)$ with $c \in P$. Thus $I(P, L) \geq |A|^3$. Applying the Szemerédi–Trotter theorem we conclude

$$|A|^3 \leq O\big((|A + A||A \cdot A|)^{2/3}(|A|^2)^{2/3} + |A + A||A \cdot A| + |A|^2\big),$$

and the claim follows by elementary algebra. □

Very recently, Solymosi [324] added a new twist to Elekes' argument, essentially improving ε to $3/11$.

Theorem 8.15 *[324] Let A be a finite set of real numbers with $|A| \geq 2$. Then we have $|A+A|^8|A/A|^3 = \Theta(|A|^{14})$, and $|A+A|^8|A \cdot A|^3 = \Theta(\frac{|A|^{14}}{\log^3|A|})$. Consequently*

$$|A+A| + |A \cdot A| = \Omega\big(|A|^{14/11}/\log^{3/11}|A|\big). \tag{8.3}$$

Proof We may remove zero if necessary and assume that all elements of A are non-zero. We shall need a dyadic decomposition of A/A, in order to control the multiplicity of quotients in A/A from both above and below. Let $2 \leq d \leq |A|$ be a power of two to be chosen later, and let $D_d \subseteq A/A$ be the set

$D_d := \{m \in A/A : m = a_1/a_2$ for between d and $2d$ values of $(a_1, a_2) \in A \times A\}$.

Let $P := A \times A$, and let L denote all the lines $\{(x, y) : y = mx + b\}$ with slope m in D_d, and which contain at least one point in P. Observe that L is finite, and that each point $p \in P$ is incident to $|D_d|$ lines in L. Thus by Corollary 8.5 we have

$$|A|^2 = |P| = O\left(\frac{|L|}{|D_d|} + \frac{|L|^2}{|D_d|^3}\right);$$

since $|D_d| \leq |A/A| \leq |A|^2$, this implies a lower bound on $|L|$:

$$|L| = \Omega\big(|A||D_d|^{3/2}\big). \tag{8.4}$$

Now let $P' := (A+A) \times (A+A)$. Observe that if $l \in L$, then l has some slope $m \in D_d$ and contains a point (a_1, a_2) in P. In particular, $l \cap P'$ contains the set $\{(a_1 + a_3, a_2 + a_4) : a_3, a_4 \in A; a_3/a_4 = m\}$, which has cardinality at least d by definition of D_d. Thus each line in L contains at least d points in P'; by Corollary 8.5 again, we conclude that

$$|L| = O\left(\frac{|P'|}{d} + \frac{|P'|^2}{d^3}\right) = O\left(\frac{|P'|^2}{d^3}\right),$$

where the latter bound follows since $d \leq |A|$ and $|P'| \geq |A|^2$. Inserting (8.4) and $|P'| = |A+A|^2$ we obtain after some algebra

$$|D_d| = O\left(\frac{|A+A|^{8/3}}{|A|^{2/3}d^2}\right). \tag{8.5}$$

In particular, by definition of D_d,

$$|\{(a_1, a_2) \in A \times A : a_1/a_2 \in D_d\}| = O\left(\frac{|A+A|^{8/3}}{|A|^{2/3}d}\right).$$

Summing this over d equal to all powers of two greater than $C|A+A|^{8/3}/|A|^{18/3}$ for some large absolute constant C, we obtain

$$\big|\big\{(a_1, a_2) \in A \times A : a_1/a_2 \in D_d \text{ for some } d \geq C|A+A|^{8/3}/|A|^{8/3}\big\}\big| \leq \frac{1}{2}|A|^2$$

and hence

$$\left|\left\{(a_1, a_2) \in A \times A : a_1/a_2 \in D_d \text{ for some } d < C|A+A|^{8/3}/|A|^{8/3}\right\}\right| \geq \frac{1}{2}|A|^2.$$

But for d as above, each $m \in D_d$ has at most $O(d) = O(|A+A|^{8/3}/|A|^{14/3})$ representations of the form a_1/a_2, and so we can conclude that $|A/A| = \Omega(|A|^2/(|A+A|^{8/3}/|A|^{8/3}))$ which gives the first inequality.

To prove the second inequality, we observe from (8.5) that

$$|\{(a_1, a_2, a_3, a_4) \in A \times A : a_1/a_2 = a_3/a_4 \in D_d\}| = O\left(\frac{|A+A|^{8/3}}{|A|^{2/3}}\right);$$

note that while the above argument was only for $d \geq 2$, the estimate here also holds for $d = 1$ by crudely bounding the left-hand side by $|A|^2$ and bounding $|A + A|$ from below by $|A|$. Summing this over d equal to all powers of 2 between 1 and $|A|$, we obtain

$$|\{(a_1, a_2, a_3, a_4) \in A \times A : a_1/a_2 = a_3/a_4\}| = O\left(\frac{|A+A|^{8/3}}{|A|^{2/3}} \log |A|\right).$$

On the other hand, by a simple double counting argument (cf. (2.8)) we have

$$|\{(a_1, a_2, a_3, a_4) \in A \times A : a_1/a_2 = a_3/a_4\}| \geq |A|^4/|A \cdot A|,$$

and the claim follows. □

A special case which draws lots of attention is when either $|A + A|$ or $|A \cdot A|$ is small. Elekes and Ruzsa [80] proved the following theorem.

Theorem 8.16 *Let A be a finite set of real numbers with $|A| \geq 2$. Then*

$$|A+A|^4 |A \cdot A| = \Omega\left(\frac{|A|^6}{\log |A|}\right).$$

In particular, if $|A + A| = O(|A|)$, then $|A \cdot A| = \Omega(|A|^2/\log |A|)$.

The logarithmic factor is necessary; if one has $A := [1, n]$ then it is known that $|A \cdot A| = O(\frac{n^2}{\log^c n})$ for some positive constant c. (See also Exercise 8.3.6.)

Proof It is easy to reduce to the case when the elements of A are positive. Let $P := ((A + A) \cup A) \times ((A + A) \cup A)$; thus P is a collection of points of cardinality $O(|A + A|^2)$. We shall apply the double counting method to the number of collinear triples in P. On the one hand, Corollary 8.9 shows that the number of such triples is $O(|A + A|^2 \log |A|)$. On the other hand, a standard Cauchy–Schwarz argument (cf. (2.8)) shows that

$$|\{(a, b, c, d) \in A \times A \times A \times A : ab = cd\}| \geq \frac{|A|^4}{|A \cdot A|}.$$

We may assume $|A \cdot A| \le \frac{1}{2}|A|^2$ since the claim is trivial otherwise. We can then remove the $a = d$ contribution from the right-hand side and conclude

$$|\{(a, b, c, d) \in A \times A \times A \times A : ab = cd; a \neq d\}| = \Omega\left(\frac{|A|^4}{|A \cdot A|}\right).$$

For any (a, b, c, d) in the above set and $e, f \in A$, observe that the three points (e, f), $(e + a, f + c)$, $(e + b, f + d)$ form a collinear triple in P. The number of triples obtained in this manner is $\Omega(\frac{|A|^6}{|A \cdot A|}$. Combining this with the upper bound, the claim follows. □

The above results show that if $|A + A|$ is close to $|A|$, then $|A \cdot A|$ is close to $|A|^2$. In the other direction, the best known results are due to Chang [49], who has established that if $|A \cdot A| \le K|A|$ then $|A + A| \ge 36^{-K}|A|^2$, and more generally $|hA| \ge (2h^2 - h)^{-hK}|A|^h$ for all $h \ge 2$. Those arguments are not as elementary as those presented here, relying instead on a result of Freiman (Theorem 5.13) and the machinery of $\Lambda(p)$ constants from Section 4.5 in order to get good lower bounds on $|hA|$. See [49] for further details and some history of the problem.

Exercises

8.3.1 Show that the Erdős–Szemerédi conjecture for sets of integers is equivalent to the corresponding conjecture for sets of rationals. Show that the conjecture for sets of reals is equivalent to the conjecture for sets of *algebraic* integers. It is not known whether the conjecture for reals is equivalent to the conjecture for (rational) integers.

8.3.2 Let A, B be additive sets of real numbers with $|A|, |B| \ge 2$. Show that $|\frac{A-A}{(B-B)\backslash 0}| = \Omega(|A||B|)$. (Hint: apply Beck's theorem to $P = A \times B$.) In particular, in the notation of Section 2.8 we have $|Q[A]| = \Omega(|A|^2)$; compare this with Corollary 2.51 and Corollary 2.52.

8.3.3 Let A, B, C be additive sets of real numbers. Show that $|A + B \cdot C| = \Omega(|A|^{1/2}|B|^{1/2}|C|^{1/2})$. (Hint: if $|B| \le |C|$, apply the Szemerédi–Trotter theorem with $P := B \times (A + B \cdot C)$ and L equal to those lines with slope in C and y-intercept in A.) Conclude that $|h(B \cdot C)| = \Omega((|B||C|)^{1-1/2^h})$ for all $h \ge 1$.

8.3.4 Generalize Theorem 8.14 by demonstrating the inequality $|A + B||B \cdot C| = \Omega(\min(|A||B||C|, |A|^{1/2}|B|^{1/2}|C|^{3/2}))$.

8.3.5 [79] Let $f : \mathbf{R} \to \mathbf{R}$ be any strictly convex function, and let A be an additive set of reals. Show that $|A + A||f(A) + f(A)| = \Theta(|A|^{5/2})$. (Hint: note that Theorem 8.14 addresses the case when $f(x) = \log x$; this should suggest a proof for the general case.)