such that the orthogonal projection of A on P has $\min(\Omega(D^{1/3}n^{2/3}), n/4)$ elements.

8.4.5 [326] (Beck's lemma for homogeneous sets in $\mathbf{R}^3$) There is a positive constant K such that the following holds. Let B be a homogeneous set of s points in $\mathbb{R}^3$ and F be a set of f pairs of points of B. At least $f/2$ pairs of F are on lines incident to at most $K\frac{s}{f^{1/2}}$ points of B.

8.4.6 Let n be a large number, and let $P \subset \mathbf{R}^2$ be the set $A := [1, \sqrt{n}] \times [1, \sqrt{n}]$. Show that $|P| = \Theta(n)$ and $g_2(P) = o(n)$. (Hint: for primes $p = 3 \pmod 4$, any number divisible by p but not by p^2 cannot be written as the sum of two integer squares. Use this fact for all small p (say $p < \log\log n$) and the Chinese remainder theorem to improve upon the trivial bound of $g_2(P) = O(n)$.) Conclude in particular that $g_2(n) = o(n)$.

8.4.7 The purpose of this exercise is to sketch an alternative proof of the Szemerédi–Trotter theorem via *cell decomposition*. Let P, L be collections of points and lines, and let $1 \leq r \leq |L|/2$. Choose r lines from L at random; show that this divides the plane into $O(r^2)$ regions (known as "cells"), and that all the other lines in L intersect at most $O(r)$ of these cells. Show that there are at most $O(r|L|)$ of incidences (p, l) with p lying on the boundary of one or more cells. By applying (8.2) to the points and lines incident to the interior of each cell, and then summing using the Cauchy–Schwarz inequality, show that there are at most $O(r|L| + r^{-1/2}|P||L|^{1/2})$ incidences (p, l) with p in the interior of one of the cells. Optimize this in r to conclude the Szemerédi–Trotter theorem up to an absolute constant.

8.5 The sum-product problem in other fields

A natural extension of the sum-product problem is to consider sets from fields and rings other than $\mathbf{R}$. One example (when $\mathbf{R}$ is replaced by $\mathbf{Z}_p$ for a prime p) was consider in an earlier chapter. In this section, we consider the case when $\mathbf{R}$ is replaced by the set of complex numbers.

One way to attack the problem is to prove a complex version of Szemerédi–Trotter theorem and then repeat the proofs of Theorems 8.14 and 8.15. While it is believed that the statement of Szemerédi–Trotter theorem holds for complex lines and points, proving it is not easy as the technique using the crossing number no longer applies (see however the recent announcement by Tóth [368]).

In the following, we show that using a clever double counting argument, one can extend Elekes's result for complex numbers. In fact, the argument, which is

due to Solymosi [325], is effective for several other number fields as well. (See the remark at the end of the proof.)

Theorem 8.24 *[325] For any finite non-empty sets of complex numbers A, B, and Q,*

$$|A+B|\cdot|A\cdot Q| = \Omega\big(|A|^{3/2}|B|^{1/2}|Q|^{1/2}\big).$$

By setting $Q = B = A$, it follows immediately that

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

and

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

thus this theorem generalizes Theorem 8.14.

Proof We may assume $|A| \geq 2$ and $0 \neq Q$. From elementary algebra we observe that the map

$$(a, a', b, q) \mapsto (a+b, a'+b, aq, a'q)$$

is one-to-one from $A\times A\times B\times Q$ to $(A+B)\times(A+B)\times(A\cdot Q)\times(A\cdot Q)$ provided that we exclude the diagonal $a = a'$. This observation by itself is only enough to obtain the trivial bound $|A+B|\cdot|A\cdot Q| = \Omega(|A||B|^{1/2}|Q|^{1/2})$. However we can do better by exploiting the intuitive observation that if a' is close to a, then $a'+b$ is close to $a+b$ and aq is close to $a'q$.

More precisely, for each $a\in A$, define the *nearest neighbor* a' of a to be an element of $A\backslash a$ which minimizes the distance $|a-a'|$. (If there is more than one candidate for nearest neighbor, choose arbitrarily.) We refer to (a, a') as a *neighboring pair*, thus there are $|A|$ neighboring pairs. We caution that if (a, a') is a neighboring pair then (a', a) is not necessarily a neighboring pair also.

Call a quadruple (a, a', b, q) *good* if (a, a') is a neighboring pair, $b\in B$ and $q\in Q$, and one has the closeness properties

$$|\{u\in A+B : |a+b-u| \leq |a-a'|\}| \leq \frac{28|A+B|}{|A|} \tag{8.7}$$

and

$$|\{v\in A\cdot Q : |aq-v| \leq |aq-a'q|\}| \leq \frac{28|A\cdot Q|}{|A|}. \tag{8.8}$$

Informally, (8.7) and (8.8) assert that $a'+b$ is a fairly close neighbor of $a+b$ in $A+B$, and similarly $a'q$ is a fairly close neighbor of aq in $A\cdot Q$. We will apply a double counting argument to N, the number of good quadruples.

First we establish a lower bound. For each $a \in A$ let $D_a := \{z \in \mathbf{C} : |z-a| \leq |a'-a|\}$ be the disk of radius $|a'-a|$ centered at a. A simple geometric argument (which we leave as an exercise) shows that any complex number z can be contained in at most seven of these disks. In particular for any $b \in B$ we have

$$\sum_{a\in A} |\{u \in A+B : |a+b-u| \leq |a-a'|\}| = \sum_{z\in A+B-b} |\{a \in A : z \in D_a\}| \leq 7|A+B|$$

and similarly for any $q \in Q$

$$\sum_{a\in A} |\{v \in A\cdot Q : |aq-v| \leq |aq-a'q|\}| = \sum_{z\in A\cdot Q/q} |\{a \in A : z \in D_a\}| \leq 7|A\cdot Q|.$$

If we thus fix b and q and choose $a \in A$ uniformly at random, a simple application of Markov's inequality then shows that (a, a', b, q) will be good with probability at least $1/2$. This shows that

$$N \geq |B||Q|\frac{|A|}{2}.$$

Now we establish an upper bound. Recall that the quadruple (a, a', b, q) is uniquely determined by the quadruple $(a+b, a'+b, aq, a'q)$. There are $|A+B|$ choices for $a+b$ and $|A\cdot Q|$ choices for aq. For fixed $a+b$, we see from (8.7) that there are at most $\frac{28|A+B|}{|A|}$ elements of $A+B$ which are closer to or equally distant from $a+b$ than $a'+b$, and thus there are at most $\frac{28|A+B|}{|A|}$ values of $a'+b$. Similarly there are at most $\frac{28|A\cdot Q|}{|A|}$ values of $a'q$. This gives the upper bound

$$N \leq |A+B|\frac{28|A+B|}{|A|}|A\cdot Q|\frac{28|A\cdot Q|}{|A|}.$$

Combining this with the lower bound, we obtain the claim. □

Remark 8.25 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.

To conclude this section, let us describe a recent result of Chang, who investigates the sum-product problem for matrices [51].

Theorem 8.26 *There is a function $\Phi(n)$ tending to infinity with n such that the following holds. Let d be a fixed integer and A be a finite set of $d\times d$ real matrices such that for any two different elements M and M' of A, $\det(M-M') \neq 0$. Then*

$$|A+A| + |A\cdot A| \geq \Phi(|A|)|A|.$$

Theorem 8.27 *For every d there is a positive constant $\epsilon = \epsilon(d)$ such that the following holds. Let A be a finite set of $d \times d$ real, symmetric, matrices. Then*

$$|A + A| + |A \cdot A| \geq |A|^{1+\epsilon}.$$

The proofs of these theorems are more complicated than those presented here and we refer the readers to [51] for details.

Exercise

8.5.1 With the notation in the proof of Theorem 8.24, show that every complex number is contained in at most seven of the disks D_a. (Hint: show that if z is contained in both D_a and $D_{a'}$ with a, a', z distinct, then a, a' subtend an angle of at least 60° with respect to z.)