Sets with few ordinary lines, and the orchard planting problem

Ben Green and Terence Tao

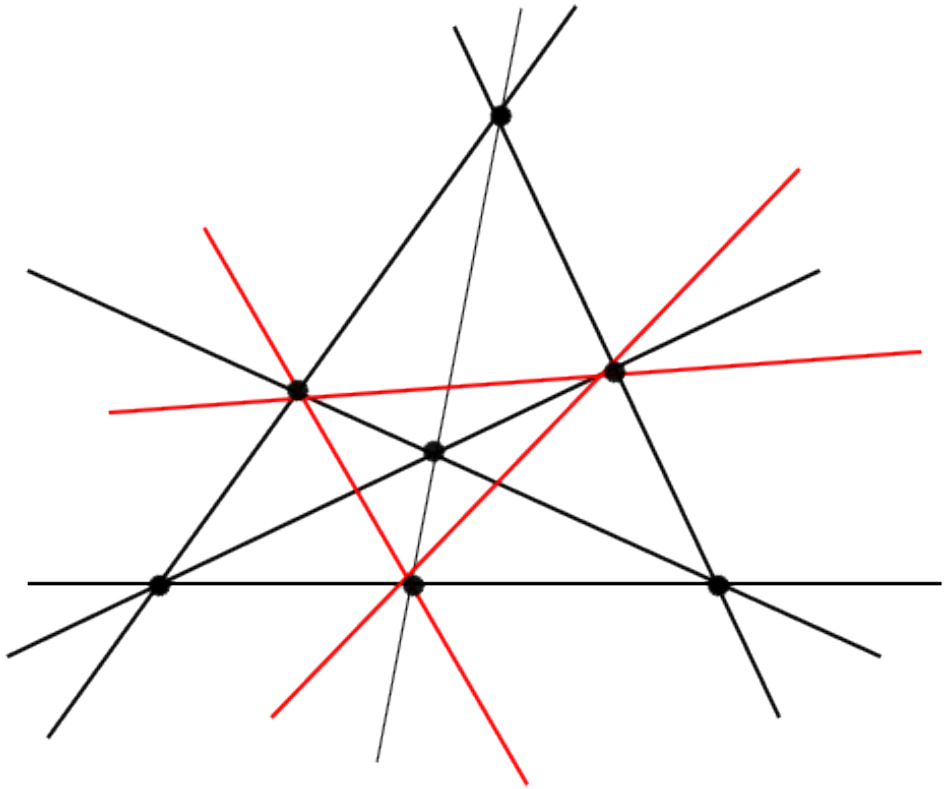
University of California, Los Angeles

Erdős Centennial Conference

Ordinary lines

- Let P be a finite set of n points in the affine plane $\mathbf{R}^2$. For any $k \geq 2$, define a k-rich line to be a line that meets exactly k points from P.
- A 2-rich line is known as an ordinary line.
- We let $N_k = N_k(P)$ denote the number of k-rich lines associated to the point set P.
- General question: for fixed n, what can we say about N_k?
- Erdős \$100: if $N_k = 0$ for $k \geq 5$, is $N_4 = o(n^2)$?
- We will focus on N_2 and N_3 in this talk.

Ordinary lines cont.



A configuration of $n = 7$ points with $N_2 = 3$ ordinary lines and $N_3 = 6$ 3-rich lines.

Projective geometry

- Note that applying a projective transformation to a point set P does not affect the number of k-rich lines. Because of this, we may pose the problem on the projective plane $\mathbf{RP}^2$ instead of the Euclidean plane and obtain the same results.
- By projective duality, we may also consider collections P^* of n lines in the projective plane $\mathbf{RP}^2$ and count k-rich points (and in particular, ordinary points that meet exactly two lines in P^*), and obtain an equivalent problem.
- For this and other reasons, it is natural to work in the projective plane instead of the affine one.

The Sylvester-Gallai theorem

Perhaps the most well known result in this area is the Sylvester-Gallai theorem:

QUESTIONS FOR SOLUTION.

11851. (Professor SYLVESTER.)—Prove that it is not possible to arrange any finite number of real points so that a right line through every two of them shall pass through a third, unless they all lie in the same right line.

Theorem (Sylvester-Gallai theorem)

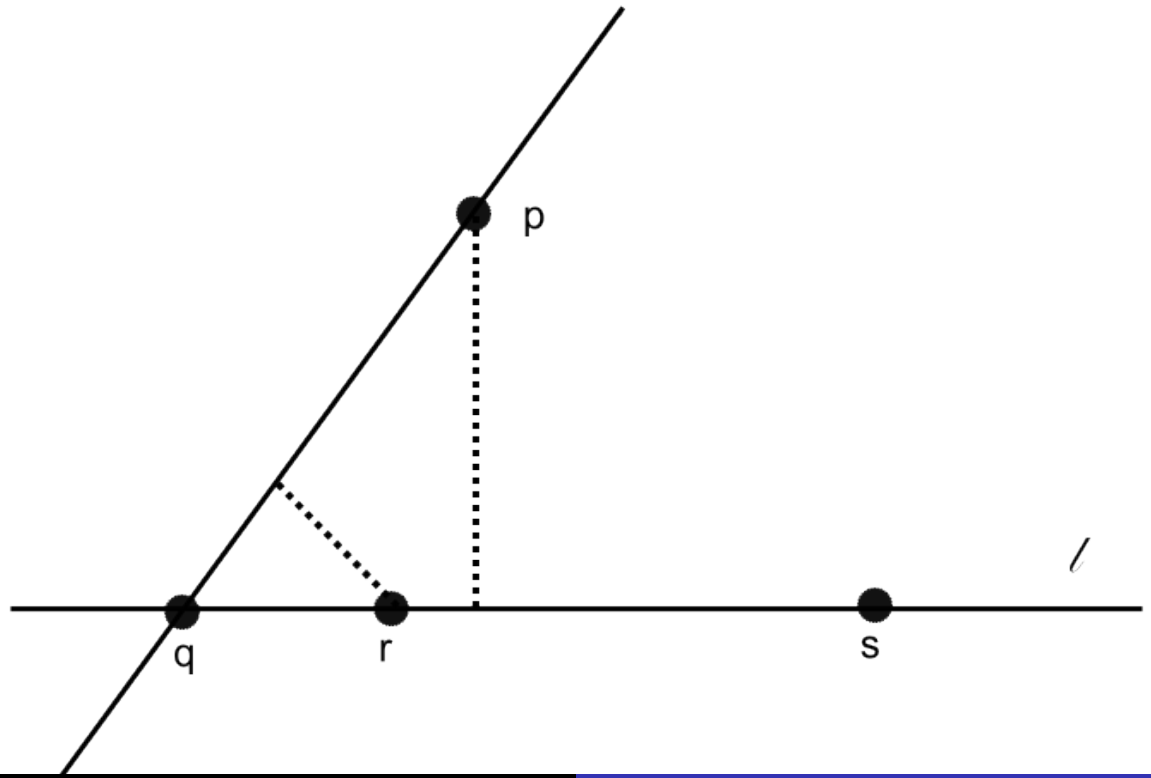
Let P be a set of points in $\mathbf{RP}^2$, not all collinear. Then there exists at least one ordinary line: $N_2 \geq 1$.

Sylvester-Gallai cont.

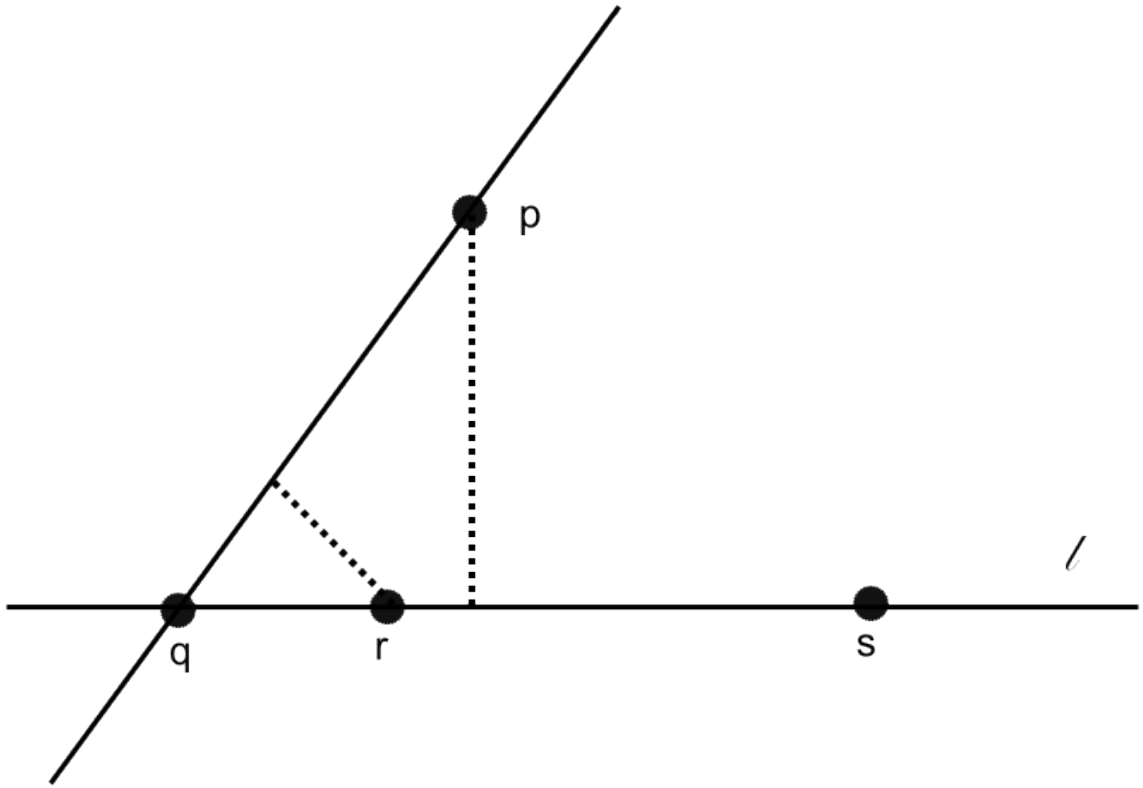
- Posed first by Sylvester (1893), and then by Erdős (1943). Has many proofs, including Melchior (1940), Gallai (1944), and Kelly (1948). Kelly's proof is the most well known, but Melchior's is the most relevant for our work.
- Depends crucially on the properties of the real line $\mathbf{R}$. The Sylvester-Gallai theorem fails over finite fields $\mathbf{F}$ of order greater than two (just take $P = \mathbf{F}^2$) and over the complex numbers (the Hesse configuration - see below).

Kelly's proof of Sylvester-Gallai

Suppose for contradiction that we have a set of points P, not all collinear, with no ordinary lines. Consider all pairs p, ℓ where $p \in P$ and ℓ meets at least two points of P, but does not meet p. Among all such pairs, take a pair where the distance between p and ℓ is shortest:



Kelly cont.



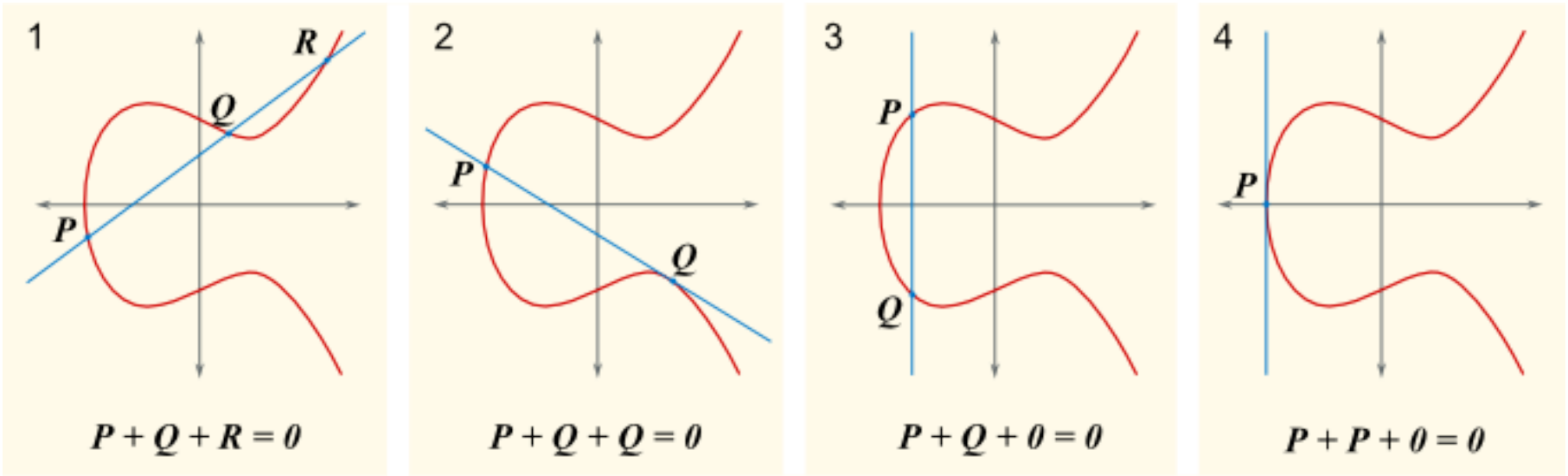
By hypothesis, ℓ contains at least three points q, r, s in P. One can then use p, q, r, s to create another point-line pair that are closer to each other than p and ℓ, a contradiction.

Hesse example

An elliptic curve is a curve which (up to projective transformation) takes the Weierstrass normal form

$$C = \{(x, y) : y^2 = x^3 + ax + b\}$$

for some a, b with $4a^3 + 27b^2 \neq 0$. There is an abelian group law $\oplus$ on C, with $p \oplus q \oplus r = 0$ if and only if p, q, r are collinear (image from Wikipedia):



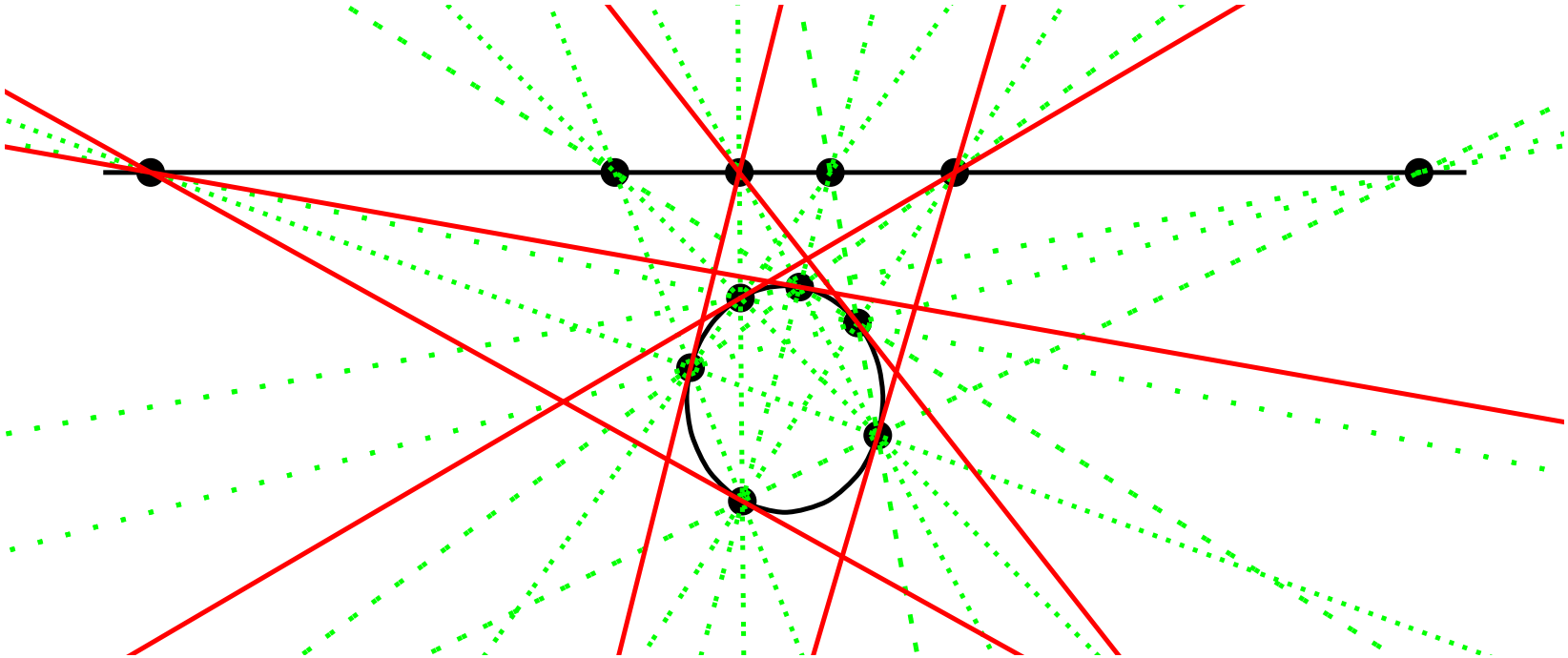
Hesse cont.

- Over the complex numbers $\mathbf{C}$, an elliptic curve C is isomorphic as an abelian group to the two-torus $\mathbf{R}^2/\mathbf{Z}^2$.
- In particular, it contains a nine-element subgroup isomorphic to $(\mathbf{Z}/3\mathbf{Z})^2$ (the points of 3-torsion, or more geometrically the inflection points of the elliptic curve).
- This set of nine points is not collinear, but contains no ordinary lines: any line through two of these points passes through a third, thanks to the elliptic curve group law.
- Thus the Sylvester-Gallai theorem fails in the complex plane.

Dirac-Motzkin conjecture

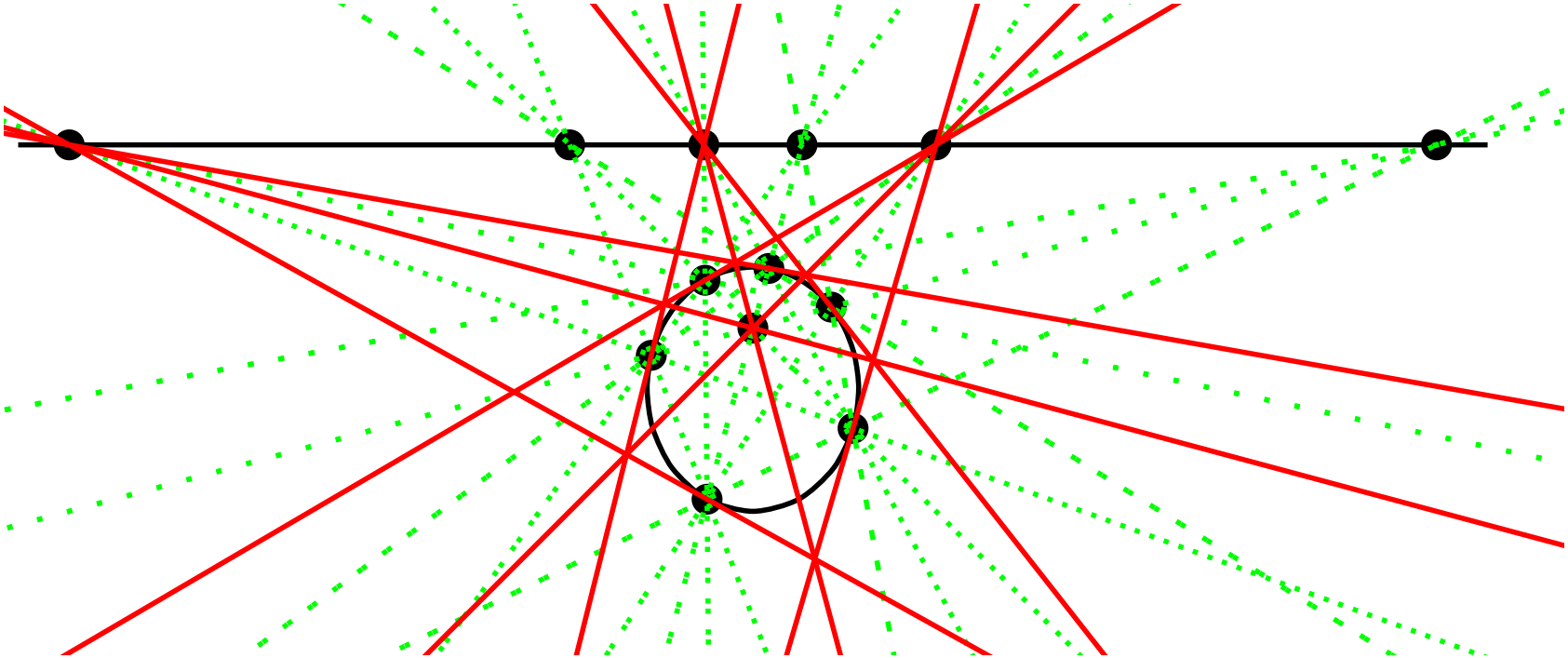
- Let P be a set of n points in $\mathbf{RP}^2$, not all collinear. The Sylvester-Gallai theorem tells us that N_2 is positive. But how small can N_2 be?
- When n is even, a basic example of Böröczky (1968) involving $n/2$ equally spaced points on the unit circle, and $n/2$ points on the line at infinity, shows that N_2 can be as small as $n/2$.
- For odd n, a modification of this constriction shows N_2 can be as small as $3\lfloor n/4 \rfloor$.
- One also has examples in which $N_2 = 3$ when $n = 7$ (Kelly-Moser, 1958), or $N_2 = 6$ when $n = 13$ (Crowe-McKee, 1968).

Böröczky example



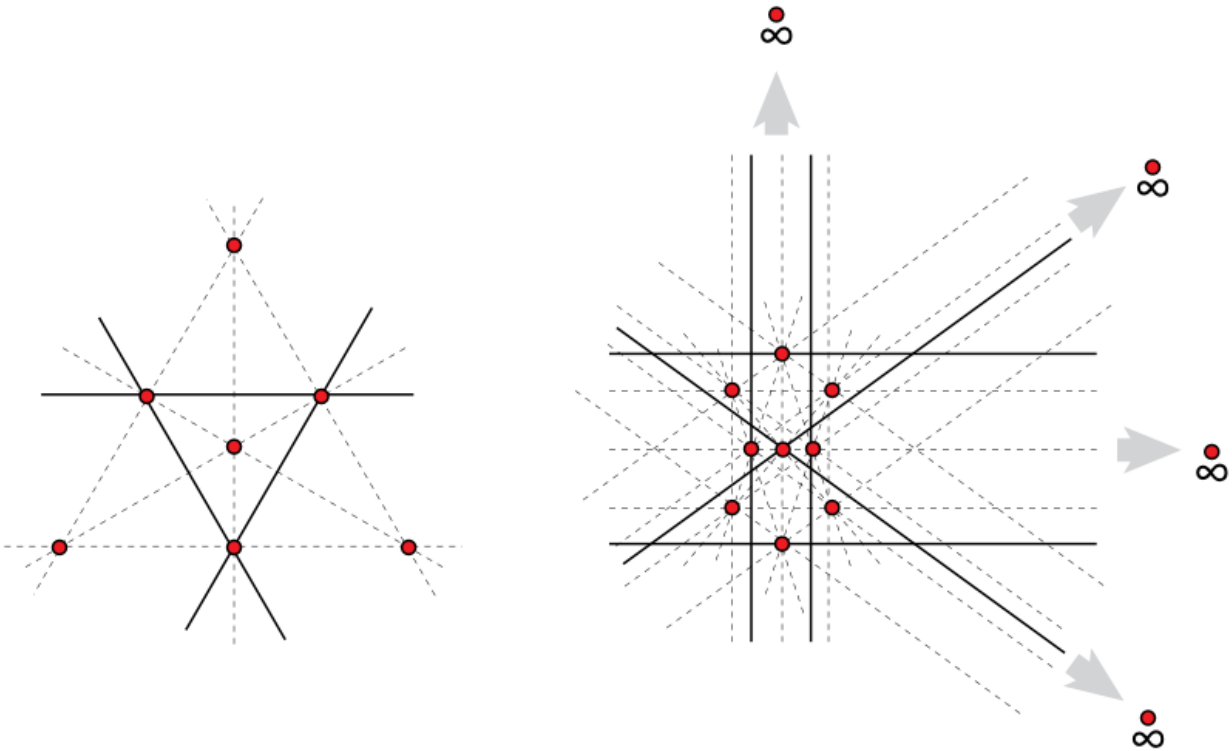
A Böröczky example with $n = 12$ and $N_2 = 6$, consisting of $n/2 = 6$ points on the unit circle and $n/2 = 6$ points on the line at infinity; a projective transformation has been applied to bring the line at infinity into view.

Böröczky cont.



A Böröczky example with $n = 13$ and $N_2 = 9$, consisting of $(n-1)/2 = 6$ points on the unit circle, $(n-1)/2 = 6$ points on the line at infinity, and the origin.

Kelly-Moser and Crowe-McKee examples



The examples of Kelly-Moser ($n = 7, N_2 = 3$) and Crowe-McKee ($n = 13, N_2 = 6$). (From Wikipedia.)

Dirac-Motzkin conjecture

Dirac-Motzkin conjecture

If $n > 13$, and P is a set of n points in $\mathbf{RP}^2$, not all collinear, then $N_2 \geq n/2$.

Stated as "likely" by Dirac (1951).

Strong Dirac-Motzkin conjecture

If $n > 13$, and P is a set of n points in $\mathbf{RP}^2$, not all collinear, then $N_2 \geq n/2$ if n is even and $N_2 \geq 3\lfloor n/4 \rfloor$ when n is odd.

Partial results

- The Sylvester-Gallai theorem gives $N_2 \geq 1$.
- Melchior's proof (1940) of Sylvester-Gallai gives $N_2 \geq 3$.
- Motzkin (1951) showed $N_2 \gg \sqrt{n}$.
- Kelly-Moser (1958) showed $N_2 \geq 3n/7$.
- Csima-Sawyer (1993) showed $N_2 \geq 6n/13$ when $n > 7$.

First main theorem

Our first main result is that the strong Dirac-Motzkin conjecture holds for sufficiently large n.

Theorem

There exists a constant n_0 such that if $n > n_0$ and P is a set of n points in $\mathbf{RP}^2$, not all collinear, then $N_2 \geq n/2$ if n is even and $N_2 \geq 3\lfloor n/4 \rfloor$ when n is odd.

The value we get for n_0 is effective, but huge (double exponential in size).

The orchard planting problem

2. Fain would I plant a grove in rows,
But how must I its form compose
With three trees in each row;
To have as many rows as trees;
Now tell me, artists, if you please;
'Tis all I want to know.

- The orchard planting problem asks to maximise N_3 as P ranges over all configurations of n points in $\mathbf{RP}^2$.
- Asked (poetically) by Jackson (1821) and by Sylvester (1868).

Orchard planting cont.

Since every two points determine a k-rich line for some $k \geq 2$, we have the double-counting identity

$$\sum_{k=2}^{n} \binom{k}{2} N_k = \binom{n}{2}$$

which gives the trivial upper bound

$$N_3 \leq \frac{1}{6}n^2 - \frac{1}{6}n.$$

Orchard planting cont.

As observed by Burr, Grunbaum, Sloane (1974), lower bounds on N_2 can be used to improve this upper bound. For instance, the Dirac-Motzkin conjecture implies that

$$N_3 \leq \frac{1}{6}n^2 - \frac{1}{3}n$$

for $n > 13$ (with some small further improvements possible using the fact that the N_k are integers).

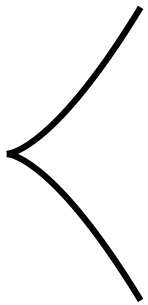
Orchard planting cont.

- In the converse direction, sets with large N_3 may be constructed using elliptic curves (Sylvester 1868, Burr-Grunbaum-Sloane 1974).
- Over $\mathbf{R}$, an elliptic curve C is either isomorphic as a group to $\mathbf{R}/\mathbf{Z}$ (if connected) or $\mathbf{R}/\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ (if disconnected). In either case, it will contain a subgroup P of order n for any $n \geq 1$.
- Elementary combinatorics then tells us that there are $\lfloor \frac{1}{6}n^2 - \frac{1}{2}n \rfloor + 1$ triples $\{a, b, c\}$ of distinct elements in P that sum to zero, and so

$$N_3 = \lfloor \frac{1}{6}n^2 - \frac{1}{2}n \rfloor + 1.$$

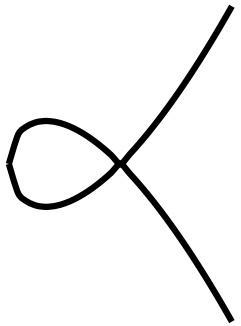
Orchard planting cont.

- Similarly if one shifts P within the group C by an element of order three (i.e. one works with a coset of P rather than P itself).
- The construction also works for an acnodal cubic curve such as $\{(x, y) : y^2 = x^3 - x\}$ (which, as a group, is isomorphic to $\mathbf{R}/\mathbf{Z}$ away from the singular point.



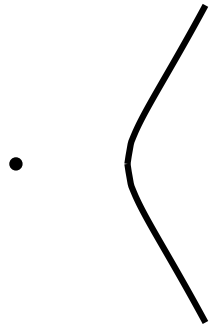
$y^2 = x^3$

cuspidal



$y^2 = x^2(x+1)$

nodal



$y^2 = x^2(x-1)$

acnodal

Second main theorem

Our second main theorem shows that the elliptic curve examples are sharp for sufficiently large n:

Theorem

There exists a constant n_0 such that if $n > n_0$ and P is a set of n points, then $N_3 \leq \lfloor \frac{1}{6}n^2 - \frac{1}{2}n \rfloor + 1$.

Structure theorems

- The proof of both of our main theorems rely on structure theorems that describe classify the sets of n points P that have few ordinary lines ($N_2 = O(n)$).
- It turns out that sets with few ordinary lines are very restricted in structure, and are all closely tied to cubic curves such as elliptic curves, or the union of a conic section and a line. (This is already suggested by several of the previous examples.)
- Note that counterexamples to either of our two theorems would have few ordinary lines (large N_3 implies small N_2).

First structure theorem

In fact we prove several structure theorems, in increasing order of difficulty (and with increasingly worse constants). This structure theorem is the easiest to prove:

Theorem (First structure theorem)

Let P be a set of n points with at most Kn ordinary lines. Then P can be covered by at most $500K$ cubic curves.

Second structure theorem

Here is a harder one:

Theorem (Second structure theorem)

Let P be a set of n points with at most Kn ordinary lines. Suppose that $n \geq \exp\exp(CK^C)$ for some large absolute constant C. Then all but at most $O(K^{O(1)})$ points of P lie on a single curve of degree at most three.

Third structure theorem

Here is our strongest theorem:

Theorem (Third structure theorem)

Let P be a set of n points with at most Kn ordinary lines. Suppose that $n \geq \exp\exp(CK^C)$ for some large absolute constant C. Then, after applying a projective transformation and adding and deleting at most $O(K)$ points, P is either

- *collinear;*
- *a Böröczky example (equally spaced points on the unit circle and on the line at infinity); or*
- *a subgroup or coset of an elliptic curve (or the acnodal singular cubic curve $y^2 = x^3 - x$).*

Third structure theorem cont.

From this strongest structure theorem it is straightforward to establish our first two main theorems, basically by checking all the cases explicitly. It also shows that there are no other extremisers for these theorems beyond the ones already given.

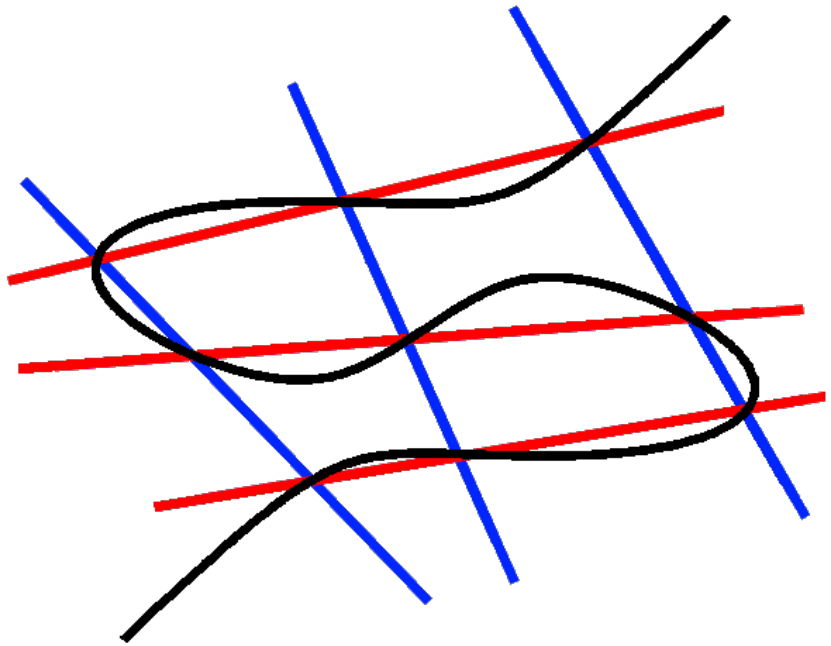
Why cubic curves?

Why are cubic curves so fundamentally tied to the property of having few ordinary lines: the answer lies in the Cayley-Bacharach theorem, or more precisely a version of this theorem due to Chasles (1885):

Theorem (Cayley-Bacharach theorem)

Suppose that two sets of three lines in $\mathbf{RP}^2$ *meet in nine distinct points. Then any cubic curve that passes through eight of these nine points, necessarily passes through the ninth.*

Cubic curves cont.



This classical theorem contains as special cases Pappus's theorem (when the cubic curve consists of three lines), Pascal's theorem (when the cubic curve is the union of a conic section and a line), and the associative law for elliptic curves (when the cubic curve is an elliptic curve).

Melchior's argument

- To see how the Cayley-Bacharach theorem can actually be used, we need to first review Melchior's proof of the Sylvester-Gallai theorem.
- The first step is to pass to the dual configuration P^* of n lines in $\mathbf{RP}^2$, rather than n points. If the points in P were not all collinear, then this partitions the projective plane into a certain number of vertices, edges, and faces. In particular we have Euler's formula

$$V - E + F = 1$$

in the projective plane.

Melchior cont.

Double counting reveals that

$$V = \sum_{k=2}^{n} N_k; \quad E = \sum_{k=2}^{n} kN_k; \quad F = \sum_{s=3}^{n} M_s; \quad 2E = \sum_{s=3}^{n} sM_s,$$

where M_s is the number of faces with s sides. After some rearranging, Euler's formula $V - E + F = 1$ then becomes Melchior's formula

$$N_2 = 3 + \sum_{k=4}^{n} (k-3)N_k + \sum_{s=4}^{n} (s-3)M_s$$

which gives Melchior's bound $N_2 \geq 3$.

Inverting Melchior

Melchior's identity

$$N_2 = 3 + \sum_{k=4}^{n}(k-3)N_k + \sum_{s=4}^{n}(s-3)M_s$$

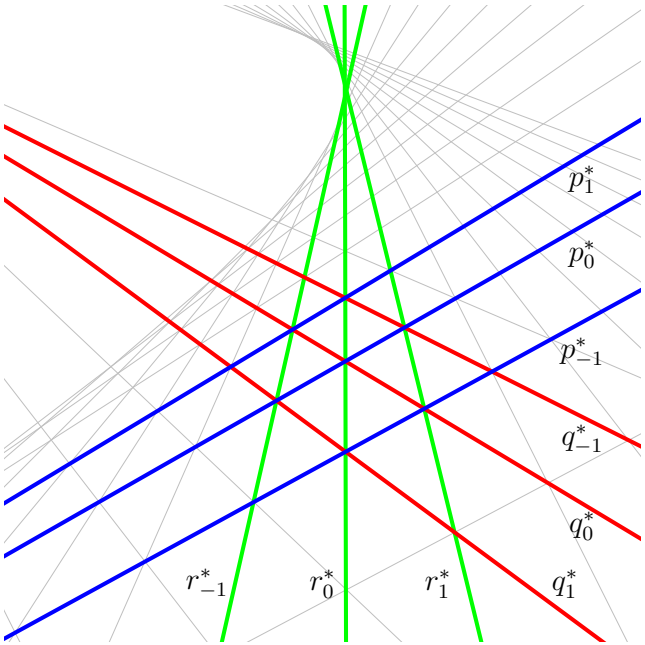
reveals important information about sets with few ordinary lines (N_2 small); it says that

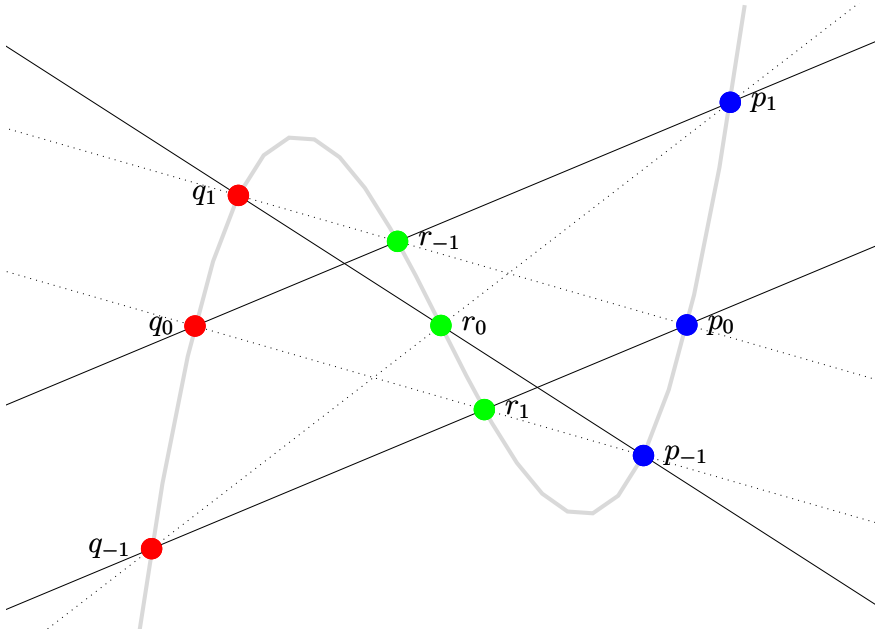
- N_k is small for most $k \geq 4$ (thus most lines are 3-rich, and most vertices in the dual configuration have degree six); and
- M_s is small for most $s \geq 4$ (thus most faces in the dual configuration are triangles).

This implies that the dual configuration usually has the local combinatorial structure of a triangular grid.

Triangular grids and Cayley-Bacharach

Key fact: triangular grids are dual to Cayley-Bacharach configurations!





First structure theorem

By Melchior, if P has few ordinary lines, then P^* contains many triangular grids, so P contains many Cayley-Bacharach configurations, and so many points lie on the same cubic curve. This is basically how our first structure theorem is proven:

Theorem (First structure theorem)

Let P be a set of n points with at most Kn ordinary lines. Then P can be covered by at most $500K$ cubic curves.

Linear and nonlinear cases

A refined version of the above analysis can also exclude cases in which the cubic curves that cover P contain two or more irreducible nonlinear curves (i.e. irreducible conic sections, or irreducible cubic curves), basically because Bezout's theorem prevents these curves from "interacting" much with each other. A more difficult situation to eliminate is the linear case when a large portion of P is covered by a small number of lines. There are three model subcases:

(i) (Triangular case) P is covered by three non-concurrent lines.

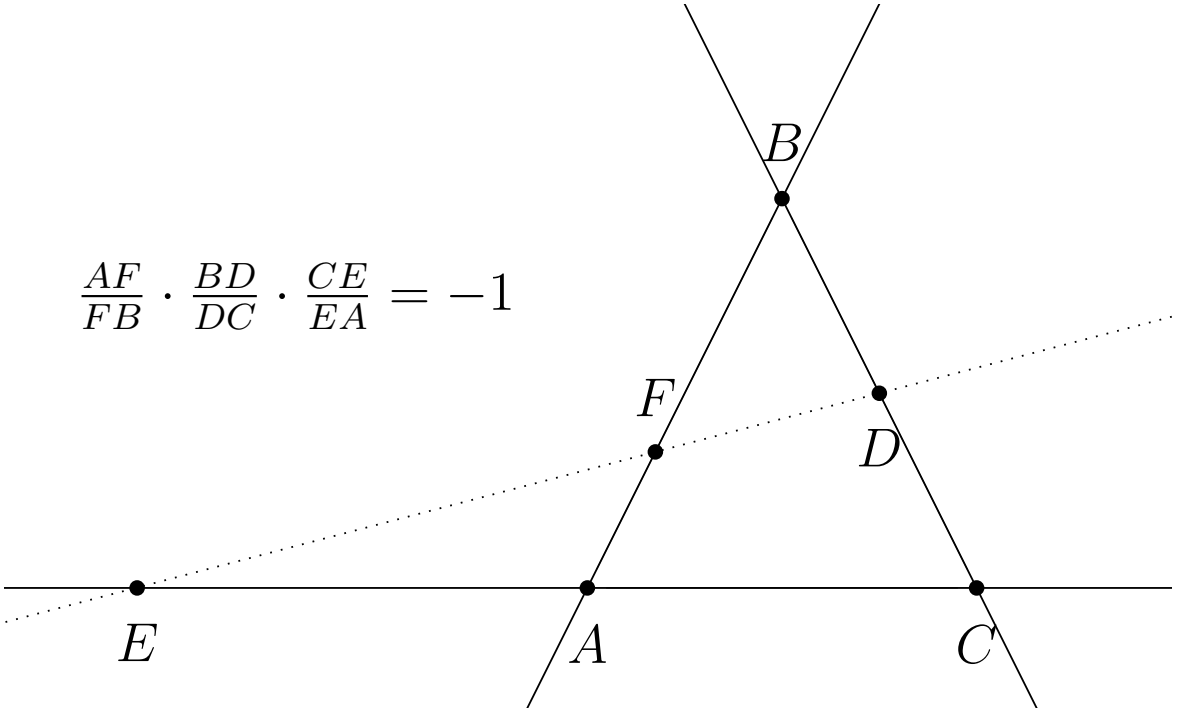
(ii) (Non-concurrent case) P is covered by k lines, no three of which are concurrent.

(iii) (Parallel case) P is covered by k parallel lines.

Triangular case

The key geometric tool to deal with the triangular case is Menelaus' theorem:

$$\frac{AF}{FB} \cdot \frac{BD}{DC} \cdot \frac{CE}{EA} = -1$$



This theorem reduces the question to one in additive combinatorics (or more precisely, multiplicative combinatorics).

Triangular case cont.

Roughly speaking, the triangular case is deduced from the following assertion:

Theorem

Let $A \subset \mathbf{R}^\times$ be a set of cardinality n for some large n. Then there are $\gg n^2$ pairs $(a, b) \in A \times A$ such that $ab \notin A$.

Informally, this is a robust version of the assertion that the multiplicative group $\mathbf{R}^\times$ does not contain large finite subgroups. It can be proven by standard tools from additive combinatorics.

Non-concurrent case

The non-concurrent case is a generalisation of the triangular case, but in addition to simple products as in Menelaus's theorem, fractional linear transformations also begin to appear. To deal with this, we use (among other things) the following result of Elekes, Nathanson, and Ruzsa (2000), stated somewhat informally:

Theorem

Let A be a finite set of real numbers, and let $f : \mathbf{RP}^1 \to \mathbf{RP}^1$ be a fractional linear transformation that is not a dilation. Then at least one of the sets $A \cdot A$ and $f(A) \cdot f(A)$ is large.

Parallel case

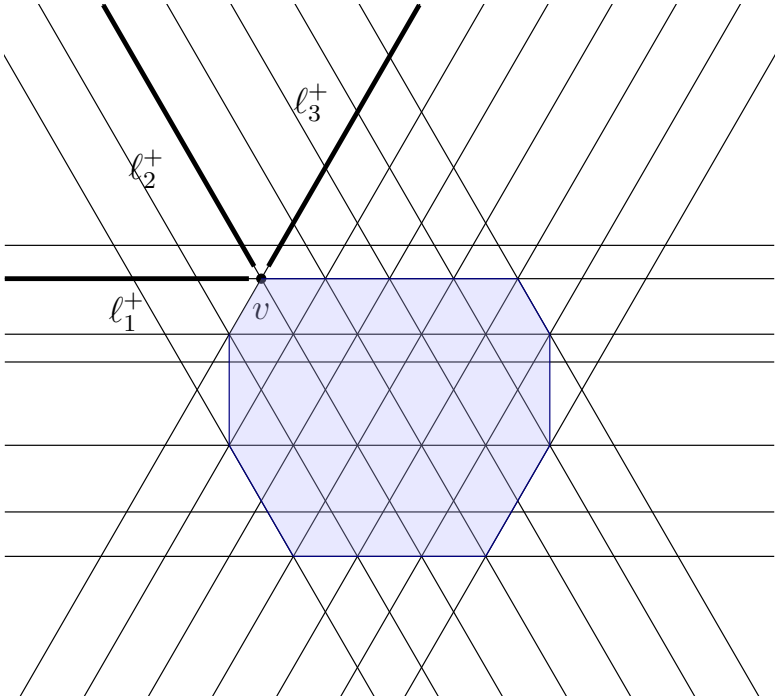
A nice treatment of the parallel case was worked out for us by Luke Betts (an undergraduate at Cambridge). After projective duality, the key claim is the following:

Theorem

Let P^* be a collection of n lines that point in only $O(1)$ different directions, not all concurrent. Then there are $\gg n^2$ ordinary points (points that meet only two lines).

Parallel case cont.

The key trick is to take an extreme point of the convex hull of the non-ordinary points, and find rays from that point that contain many ordinary points. Then remove the lines going through that extreme point and iterate.



Combining the non-concurrent case and the parallel case together to cover the general linear case requires an iteration argument based on the pigeonhole principle. Unfortunately, this iteration is the main reason why there are double exponentials in the final bounds. Ultimately we obtain

Theorem (Second structure theorem)

Let P be a set of n points with at most Kn ordinary lines. Suppose that $n \geq \exp\exp(CK^C)$ for some large absolute constant C. Then all but at most $O(K^{O(1)})$ points of P lie on a single curve of degree at most three.

Once one has most of the points on a single curve, one can use additional tools to finish off the structural classification. Firstly, one can arrange most of these points in a subgroup or a coset of the cubic curve, using the following tool from additive combinatorics:

Lemma

Let A be a finite subset of an abelian group G of order n, such that there are only $O(n)$ pairs $a, b \in A$ for which $a + b \notin A$. Then after adding or deleting $O(1)$ elements, A is equal to a coset of a finite subgroup of G.

Using this lemma, one can place most of P in something like a subgroup of an elliptic curve, or the roots of unity on the unit circle.

To finish up and get the full structure theorem, results such as the following result of Poonen and Rubinstein (1998) are useful:

Theorem (Poonen-Rubinstein theorem)

Let p be a point in the interior of the unit circle that is not the origin. Then p lies on at most seven chords connecting two roots of unity.

Actually we also need variants of this result in the exterior of the circle, and also for subgroups of elliptic curves instead of roots of unity.

Theorem (Third structure theorem)

Let P be a set of n points with at most Kn ordinary lines. Suppose that $n \geq \exp\exp(CK^C)$ for some large absolute constant C. Then, after applying a projective transformation and adding and deleting at most $O(K)$ points, P is either

- *collinear;*
- *a Böröczky example (equally spaced points on the unit circle and on the line at infinity); or*
- *a subgroup or coset of an elliptic curve (or the acnodal singular cubic curve $y^2 = x^3 - x$).*

Open questions

- Are there structure theorems over the complex numbers? Euler formula does not seem to be available.
- What about other curves than lines? Cayley-Bacharach does not seem to be available.
- We understand the $N_2 = O(n)$ case, but what about $N_2 = o(n^2)$ or something in between?
- Get better constants (no double exponentials!). Maybe one can finish off all cases of the Dirac-Motzkin and orchard problems?
- Erdős \$100: if $N_k = 0$ for $k \geq 5$, is $N_4 = o(n^2)$?