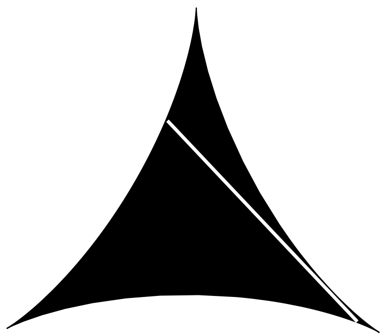
Miniature 25

Turning a Ladder Over a Finite Field

We want to turn around a ladder of length 10m inside a garden (without lifting it). What is the smallest area of a garden in which this is possible? For example, here is a garden that, area-wise, looks quite economical (the ladder is drawn as a white segment):

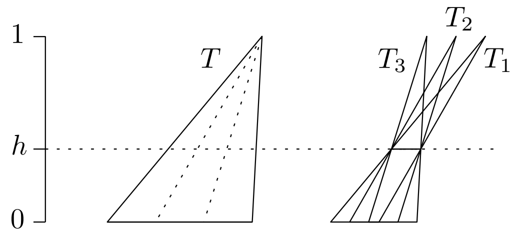


This question is commonly called the **Kakeya needle problem**; Kakeya phrased it with rotating a needle but, while I've never seen any reason for trying to rotate a needle, I did have some quite memorable experiences with turning a long and heavy ladder, so I will stick to this alternative formulation.

One of the fairly counterintuitive results in mathematics, discovered by Besicovitch in the 1920s, is that there are gardens of *arbitrarily small* area that still allow the ladder to be rotated. Let me sketch the beautiful construction, although it is not directly related to the topic of this book.

A necessary condition for turning a unit-length ladder inside a set X is that X contains a unit-length segment of every direction. An X satisfying this latter, weaker condition is called a **Kakeya set**; unlike the ladder problem, this definition has an obvious generalization to higher dimensions. We begin by constructing a planar Kakeya set of arbitrarily small area (actually, one can get a zero-measure Kakeya set with some more effort).

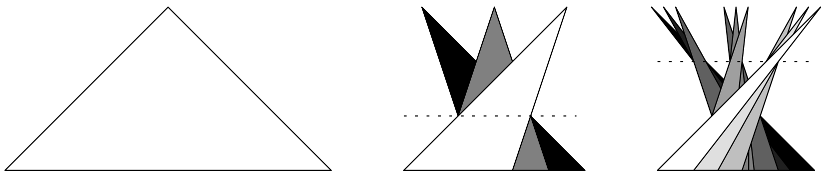
Let us consider a triangle T of height 1 with base on the x-axis, let $k \geq 2$ be an integer, and let $h \in [0, 1)$. The ***k*-thinning** of T at height h means subdividing the base of T into k equal segments, slicing T into k triangles $T_1, \ldots, T_k$ with these segments as bases, and translating each of $T_2, \ldots, T_k$ left so that it exactly overlaps with T_1 at height h. The next picture shows a 3-thinning.



More generally, k-thinning a collection of triangles at height h means k-thinning each of them separately, so from N triangles we obtain kN triangles.

We will construct a small-area set in the plane that contains segments of all directions with slope at least 1 in absolute value (more vertical than horizontal); to get a Kakeya set, we need to add another copy rotated by 90 degrees.

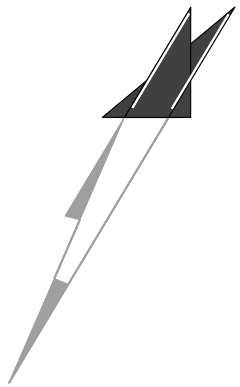
We choose a large integer m; the area of the resulting set will be bounded by $O(\frac{1}{m})$. We start with the triangle with top angle 90 degrees, perform m-thinning at height $\frac{1}{m}$, then at height $\frac{2}{m}$, and so on, up until height $\frac{m-1}{m}$. Here is an example with $m = 3$:



Let B_m denote the union of the resulting set of m^{m-1} thin triangles.

It is not hard to see that the total length of the intersection of B_m with the horizontal line at height $\frac{i}{m}$, $i = 1, 2, \ldots, m-1$, is at most $\frac{1}{m}$. Showing that the length of the intersection at all other heights is also of order $\frac{1}{m}$ is more demanding.

How can we use B_m to turn the ladder? We need to enlarge it so that the ladder can move from one thin triangle to the next. For that, we add "translation corridors" of the following kind to B_m:



The dark gray triangles are from B_i, and the lighter gray corridor can be used to transport the ladder between the two marked positions. If we are willing to walk with the ladder far enough, then the translation corridors add an arbitrarily small area.

Kakeya's conjecture. We have seen that a Kakeya set in the plane can be small—of measure zero. The Cartesian product of a zero-measure planar Kakeya set with an $(n-2)$-dimensional ball yields a zero-measure Kakeya sets in $\mathbb{R}^n$, for all $n \geq 3$. However, a statement

known as Kakeya's conjecture asserts that Kakeya sets cannot be *too* small. Namely, a Kakeya set K in $\mathbb{R}^n$ should have Hausdorff dimension n (for readers not familiar with Hausdorff dimension: roughly speaking, this means that it is not possible to cover K with sets of small diameter much more economically than the n-dimensional cube, say).

While the Kakeya needle problem has a somewhat recreational flavor, Kakeya's conjecture is regarded as a fundamental mathematical question, mainly in harmonic analysis, and it is related to several other serious problems. Although many partial results have been achieved, by the effort of many great mathematicians, the conjecture still seems far from solution (it has been proved only for $n = 2$).

Kakeya for finite fields. Recently, however, an analogue of Kakeya's conjecture, with the field $\mathbb{R}$ replaced by a finite field $\mathbb{F}$, has been settled by a short algebraic argument (after previous, weaker results involving *much* more complicated mathematics). A set K in the vector space $\mathbb{F}^n$ is a **Kakeya set** if it contains a "line" in every possible "direction"; that is, for every nonzero $\mathbf{u} \in \mathbb{F}^n$ there is $\mathbf{a} \in \mathbb{F}^n$ such that $\mathbf{a} + t\mathbf{u}$ belongs to K for all $t \in \mathbb{F}$.

Theorem (Kakeya's conjecture for finite fields)**.** *Let $\mathbb{F}$ be a q-element field. Then any Kakeya set K in $\mathbb{F}^n$ has at least $\binom{q+n-1}{n}$ elements.*

For n fixed and q large, $\binom{q+n-1}{n}$ behaves roughly like $q^n/n!$, so a Kakeya set occupies at least about $\frac{1}{n!}$ of the whole space. Hence, unlike in the real case, a Kakeya set over a finite field occupies a substantial part of the "n-dimensional volume" of the whole space.

The binomial coefficient enters through the following easy lemma.

Lemma. *Let $\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_N$ be points in $\mathbb{F}^n$, where $N < \binom{d+n}{n}$. Then there exists a nonzero polynomial $p(x_1, x_2, \ldots, x_n)$ of degree at most d such that $p(\mathbf{a}_i) = 0$ for all i.*

Proof. A general polynomial of degree at most d in variables $x_1, x_2, \ldots, x_n$ can be written as $p(\mathbf{x}) = \sum_{\alpha_1+\cdots+\alpha_n \leq d} c_{\alpha_1,\ldots,\alpha_n} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, where the sum is over all n-tuples of nonnegative integers $(\alpha_1, \ldots, \alpha_n)$ summing to at most d, and the $c_{\alpha_1,\ldots,\alpha_n} \in \mathbb{F}$ are coefficients.

We claim that the number of the n-tuples $(\alpha_1, \ldots, \alpha_n)$ as above is $\binom{d+n}{n}$. Indeed, we can think of choosing $(\alpha_1, \ldots, \alpha_n)$ as distributing d identical balls into $n+1$ numbered boxes (the last box is for the $d - \alpha_1 - \cdots - \alpha_n$ "unused" balls). A simple way of seeing that the number of distribution is as claimed is to place the d balls in a row, and then insert n separators among them defining the groups:

○ | ○ ○ ○ | | ○ | ○ ○ |

So among $n+d$ positions for balls and separators, we choose the n positions that will be occupied by separators, and the count follows.

A requirement of the form $p(\mathbf{a}) = 0$ translates to a *homogeneous* linear equation with the $c_{\alpha_1,\ldots,\alpha_n}$ as unknowns. Since $N < \binom{n+d}{d}$, we have fewer equations than unknowns, and such a homogeneous system always has a nonzero solution. So there is a polynomial with at least one nonzero coefficient. □

Proof of the theorem. We proceed by contradiction, assuming $|K| < \binom{q+n-1}{n}$. Then by the lemma, there is a nonzero polynomial p of degree $d \le q-1$ vanishing at all points of K.

Let us consider some nonzero $\mathbf{u} \in \mathbb{F}^n$. Since K is a Kakeya set, there is $\mathbf{a} \in \mathbb{F}^n$ with $\mathbf{a} + t\mathbf{u} \in K$ for all $t \in \mathbb{F}$. Let us define $f(t) := p(\mathbf{a} + t\mathbf{u})$. This is a polynomial in the single variable t of degree at most d. It vanishes for all the q possible values of t, and since a univariate polynomial of degree d over a field has at most d roots, it follows that $f(t)$ is the zero polynomial. In particular, the coefficient of t^d in $f(t)$ is 0.

Now let us see what the meaning is of this coefficient in terms of the original polynomial p: It equals $\overline{p}(\mathbf{u})$, where $\overline{p}$ is the *homogeneous part* of p, i.e., the polynomial obtained from p by omitting all monomials of degree strictly smaller than d. Clearly, $\overline{p}$ is also a nonzero polynomial, for otherwise, the degree of p would be smaller than d.

Hence $\overline{p}(\mathbf{u}) = 0$, and since $\mathbf{u}$ was arbitrary, $\overline{p}$ is 0 on all of $\mathbb{F}^n$. But this contradicts the Schwartz–Zippel theorem from Miniature 24, which implies that a nonzero polynomial of degree d can vanish on at most $dq^{n-1} \le (q-1)q^n < |\mathbb{F}^n|$ points of $\mathbb{F}^n$. The resulting contradiction proves the theorem. □