The Finite Field Kakeya Problem

Keith McKenzie Rogers

The Kakeya problem, in its various guises, has been around for many years. In 1917, the Japanese mathematician S. Kakeya asked:

> *In the class of figures in which a segment of length one can be turned around through* 360°, *remaining always in the figure, which has the smallest area?*

Surprisingly there exist figures with arbitrarily small area that fulfill Kakeya's conditions. This was discovered soon after A. S. Besicovitch constructed a set, containing a line segment in every direction, of zero Lesbesgue measure. Such a construction can be found in [**1**] or [**5**].

It was subsequently conjectured that a *Kakeya set in* $\mathbb{R}^n$ (a compact set in $\mathbb{R}^n$ containing a line segment in every direction) has fractal dimension n. In the plane, this has been proved in the affirmative and a proof can be found in [**5**]. For higher dimensions however, the problem is still open, and only in the last seven years has much progress been made. Recent work of Bourgain [**2**] and Katz and Tao [**3**] revealed a lower bound of $4n/7 + 3/7$ on the Minkowski dimension of Kakeya sets in $\mathbb{R}^n$. This, when n is large, is an improvement on Wolff's bound of $n/2 + 1$ in [**4**].

The conjecture has important links to harmonic analysis and number theory; see [**5**] for a survey. It plays a significant role in the theory of oscillatory integrals and is of relevance to questions related to the distribution of Dirichlet series.

In [**5**] Wolff introduced finite field Kakeya sets and posed the corresponding Kakeya conjecture. This reduction removes much of the technicality (there is no use of measure or fractal dimension), while preserving the essence of the problem. We apply the ideas of Bourgain, Katz, and Tao to the finite field version of the problem.

Let $\mathbb{F}$ be a field with q elements. A *Kakeya set in* $\mathbb{F}^n$ is a set $E \subset \mathbb{F}^n$ containing a line in every direction; thus for all $e \in \mathbb{F}^n \backslash \{0\}$ there is an $a \in \mathbb{F}^n$ such that $a + te \in E$ for all $t \in \mathbb{F}$.

It seems reasonable to conjecture that finite field Kakeya sets have bounded cardinality:

$$|E| \geq C_n q^n,$$

where C_n is a constant independent of q.

In [**5**] Wolff showed that there is a constant C_n such that

$$|E| \geq C_n q^{\frac{n}{2}+1}.$$

The purpose of this note is to prove the following bound, which improves Wolff's result when n is greater than 8.

Theorem 1. *If E is a Kakeya set in $\mathbb{F}^n$ and the characteristic of $\mathbb{F}$ is greater than 3, then*

$$|E| \geq C_n q^{\frac{4n}{7}+\frac{3}{7}},$$

where C_n is a constant independent of $q = |\mathbb{F}|$.

Our proof of Theorem 1 uses the following two trivial facts.

Fact 1. Any two distinct lines intersect in at most one point.

Fact 2. There are $(q^n - 1)/(q - 1)$ distinct directions in $\mathbb{F}^n$.

As in the Euclidean Kakeya problem, for the case $n = 2$, the finite field Kakeya conjecture is proved in the affirmative and Facts 1 and 2 allow proof by a simple counting argument.

Proposition 2. *If E is a Kakeya set in $\mathbb{F}^2$ then*

$$|E| \geq q^2/2.$$

Proof. There are $q + 1$ distinct lines $\{l_j\}_{j=1}^{q+1}$ contained in E, each containing q elements. If we consider the worst case scenario in which these elements are the only elements in E, and each line l_j intersects each preceding line l_i, $i \leq j$, then if we count the new elements contributed by each l_j we see that

$$\begin{aligned} |E| &\geq \overset{(l_1)}{q} + \overset{(l_2)}{q-1} + \cdots + \overset{(l_q)}{1} + \overset{(l_{q+1})}{0} \\ &= q^2 - \sum_{i=1}^{q-1} i = q^2 - \frac{q(q-1)}{2} = \frac{q^2+q}{2} \geq \frac{q^2}{2}. \end{aligned}$$ ■

Proof of Theorem 1. Let $\mathbb{F}$ be a field with q elements. Let E be a Kakeya set in $\mathbb{F}^n$. We apply the following result from [**3**].

Theorem 3. *Let A and B be finite subsets of an abelian group, and let $G \subset A \times B$ be such that each of*

$$|A|,\ |B|,\ |\{a + b : (a, b) \in G\}|, \text{ and } |\{a + 2b : (a, b) \in G\}|$$

is not greater than N. Then

$$|\{a - b : (a, b) \in G\}| \leq N^{\frac{7}{4}}.$$

We consider four 'slices' $E \cap \{x = (x_1, \ldots, x_n) : x_n = k\}$ of E. Let $\underbrace{1 + \cdots + 1}_{r}$ be denoted by r, where 1 is the identity in $\mathbb{F}$. Define

$$S_k = \{x : x_n = k\} \cup \{x : x_n = k + 1\} \cup \{x : x_n = k + 2\} \cup \{x : x_n = k + 3^{-1}4\}.$$

Clearly

$$|E| = \frac{1}{4} \sum_{k \in \mathbb{F}} |E \cap S_k|,$$

so the pigeonhole principle ensures that there is some $k_0 \in \mathbb{F}$ such that

$$|E \cap S_{k_0}| \leq \frac{4|E|}{q}. \tag{1}$$

For each direction $e \in \mathbb{F}^n \backslash 0$ with $e_n = 1$, we choose a line l_e in E with direction e. We denote this set of lines by L. This excludes the lines in a hyperplane $\{x : x_n = k\}$. Each line in L intersects each hyperplane $\{x : x_n = k\}$ so we can define

$$a_e = l_e \cap \{x : x_n = k_0\}, \ b_e = l_e \cap \{x : x_n = k_0 + 2\}.$$

In the notation of Theorem 3,

$$A = \{a_e : l_e \in L\}, \quad B = \{b_e : l_e \in L\}, \quad G = \{(a_e, b_e) : l_e \in L\}.$$

By (1) we see that both $|A|$ and $|B|$ are not greater than $4|E|/q$. Define

$$f : E \cap \{x : x_n = k_0 + 1\} \rightarrow \mathbb{F}^n; x \rightarrow 2x.$$
$$g : E \cap \{x : x_n = k_0 + 3^{-1}4\} \rightarrow \mathbb{F}^n; x \rightarrow 3x.$$

Since

$$a_e + b_e = a_e + a_e + 2e = 2(a_e + e) \in range(f)$$

and

$$a_e + 2b_e = a_e + 2(a_e + 2e) = 3a_e + 4e = 3(a_e + 3^{-1}4e) \in range(g),$$

we have

$$|\{a + b : (a, b) \in G\}|, \ |\{a + 2b : (a, b) \in G\}| \leq \frac{4|E|}{q}.$$

Thus Theorem 3 ensures that

$$|\{a - b : (a, b) \in G\}| \leq \left(\frac{4|E|}{q}\right)^{\frac{7}{4}}.$$

On the other hand, Facts 1 and 2 ensure that

$$|\{a - b : (a, b) \in G\}| = |\{2e : l_e \in L\}| = \frac{q^n - 1}{q - 1} - \frac{q^{n-1} - 1}{q - 1} \geq C_n q^{n-1}.$$

Hence

$$C_n q^{n-1} \leq \left(\frac{4|E|}{q}\right)^{\frac{7}{4}},$$

which is the desired inequality. ■

Katz and Tao suggest in [3] that it may be possible to improve the bound in Theorem 3 by including more conditions of the form

$$|\{a + kb : (a, b) \in G\} \leq N.$$

This corresponds to more slices of the Kakeya set and would enable an improvement of our bound with little further trouble.

ACKNOWLEDGEMENT. Thanks to A. Carbery and W. T. Gowers for all their invaluable help.

REFERENCES

1. A. S. Besicovitch, The Kakeya Problem, *Amer. Math. Monthly* **70** (1963) 697–706.
2. J. Bourgain, On the dimension of Kakeya sets and related maximal inequalities, *Geom. Funct. Anal.* **9** (1999) 256–282.
3. N. H. Katz and T. Tao, Bounds on arithmetic projections, and applications to the Kakeya conjecture, *preprint*.
4. T. Wolff, An improved bound for Kakeya type maximal functions, *Rev. Mat. Iberoamericana* **11** (1995) 651–674.
5. T. Wolff, Recent work connected with the Kakeya problem, in *Prospects in Mathematics: Invited Talks on the Occasion of the 250th Aniversity of Princeton University March 17–21, 1996 Princeton University*, Hugo Rossi, ed., American Mathematical Society, Providence, RI, 1998, pp. 129–162.

Cambridge University, DPMMS, 16 Mill Lane, Cambridge, CB2 1SB, U.K.
kmrogers123@hotmail.com

The Fundamental Theorem of Algebra Revisited

Airton von Sohsten de Medeiros

We present a proof based upon the Lefschetz Fixed-point Theorem of the

Fundamental Theorem of Algebra. Every nonconstant polynomial with complex coefficients has a (complex) zero.

We recall the

Lefschetz Fixed-Point Theorem. Let X be a compact polyhedron and let $f: X \to X$ be a continuous mapping. If the Lefschetz number of f is not zero, then f has a fixed point.

All we need to know about the Lefschetz number is that homotopic mappings have the same Lefschetz number and that, for the identity mapping, this number coincides with the Euler characteristic of the polyhedron [**2**, pp. 194–195].

The main idea, which allows us to make use of the Lefschetz Theorem, is that a linear isomorphism A of the complex n-space $\mathbb{C}^n$ induces (in the obvious way) a continuous mapping $\tilde{A}$ on the complex projective $(n-1)$-space $\mathbb{C}P(n-1)$, viewed