Rice University
Department of Mathematics

A Study of Kakeya Sets

Author
Gabriel Gress

Techniques and Results in the Field
April 21, 2021

Chapter 1

Kakeya Sets in Finite Fields

This section is a reinterpretation of Dvir's paper on the size of Kakeya sets in finite fields.

We have a slightly different definition of Kakeya sets in finite fields:

Definition 1.0.1: Kakeya Set

Let $\mathbb{F}$ be a finite field of q elements. A **Kakeya set** in $\mathbb{F}^n$ is a set $K \subset \mathbb{F}^n$ such that K contains a line in every direction. That is, for every $x \in \mathbb{F}^n$, there exists a $y \in \mathbb{F}^n$ such that

$$L_{y,x} := \{y + a \cdot x \mid a \in \mathbb{F}\} \subset K.$$

Because of the structure of the lines in $\mathbb{F}^n$, a lower bound can be imposed on the size of these sets. Previously, the best lower bounds in the general case is of the form $C_n \cdot q^{\frac{4n}{7}}$. Previous results were obtained by using an additive number theory lemma– the theorem proved here is obtained via homogeneous polynomials and gets a near-optimal bound.

Theorem 1.0.1

Let $K \subset \mathbb{F}^n$ be a Kakeya set. Then

$$|K| \geq C_n \cdot q^{n-1}$$

where C_n depends only on n.

This can be improved by observing that the product of Kakeya sets is also a Kakeya set.

Corollary 1.0.1

For every integer n and every $\varepsilon > 0$, there exists a constant $C_{n,\varepsilon}$ depending only on n and ε such that any Kakeya set $K \subset \mathbb{F}^n$ satisfies

$$|K| \geq C_{n,\varepsilon} \cdot q^{n-\varepsilon}.$$

This follows from taking the Cartesian product of Kakeya sets, applying Theorem 1, then taking the r-th root to obtain the bound on K.

Definition 1.0.2

A set $K \subset \mathbb{F}^n$ is a (δ, γ)-**Kakeya set** if there exists a set $\mathcal{L} \subset \mathbb{F}^n$ of size at least $\delta \cdot q^n$ such that, for every $x \in \mathcal{L}$ there is a line in direction x that intersects K in at least $\gamma \cdot q$ points.

This broader definition will be easier to work with. We will give a lower bound on these types of Kakeya sets, and then obtain Theorem 1 by setting $\delta = \gamma = 1$.

Theorem 1.0.2

Let $K \subset \mathbb{F}^n$ be a (δ, γ)-Kakeya set. Then

$$|K| \geq \binom{d+n-1}{n-1} = \frac{(d+n-1)!}{(n-1)!d!},$$

where

$$d = \lfloor q \cdot \min\{\delta, \gamma\} \rfloor - 2.$$

1.1 Proof of Theorem 1.0.2

To prove Theorem 2, we first need a lemma on polynomials in finite fields:

Lemma 1.1.1

Let $f \in \mathbb{F}^n[x]$ be a non-zero polynomial with $\deg(f) \leq d$. Then

$$|\{x \in \mathbb{F}^n \mid f(x) = 0\}| \leq d \cdot q^{n-1}.$$

Proof of Theorem 1.0.2. Suppose for the sake of contradiction that

$$|K| < \binom{d+n-1}{n-1} = \frac{(d+n-1)!}{(n-1)!d!}.$$

Observe that there are q monomials of degree d and hence more monomials than the size of K. Thus there must exist a homogeneous polynomial g of degree d, where g is not the zero polynomial, that satisfies

$$\forall x \in K, \quad g(x) = 0.$$

In other words, because the degree of d is sufficiently high enough, we can solve a system of equations to create a polynomial that takes on zeroes on K.

We will use this to show that g has too many zeroes and hence must be identically zero, which would contradict the above. Consider the set

$$K' := \{c \cdot x \mid x \in K, \, c \in \mathbb{F}\}$$

that contains all lines that pass through zero and intersect K at some point. By the homogeneity of g, observe that

$$g(c \cdot x) = c^d \cdot g(x)$$

and so for all $x \in K'$, we must have that $g(x) = 0$.

Now recall the defintion of a (δ, γ)-Kakeya set, and let the set $\mathcal{L} \subset \mathbb{F}^n$ be given (with size $\delta \cdot q^n$).

Proposition 1.1.1

For every $y \in \mathcal{L}$, $g(y) = 0$.

Proof of Proposition. ■

Let $y \in \mathcal{L}$ be a non-zero vector. Then by definition there exists a point $z \in \mathbb{F}^n$ such that

$$L_{z,y} = \{z + a \cdot y \mid a \in \mathbb{F}\}$$

intersects K in at least $\gamma \cdot q$ points. Therefore, since $d + 2 \leq \gamma \cdot d$, there exist $d + 2$ distinct field elements $a_1, \ldots, a_{d+2} \in \mathbb{F}$ such that $z + a_i \cdot y \in K$. One a_i might be zero, but because they are distinct, this still guarantees $d + 1$ distinct non-zero field elements that lie in K.

■