A FINITE VERSION OF THE KAKEYA PROBLEM

SIMEON BALL, AART BLOKHUIS, AND DIEGO DOMENZAIN

Abstract. Let $L$ be a set of lines of an affine space over a field and let $S$ be a set of points with the property that every line of $L$ is incident with at least $N$ points of $S$. Let $D$ be the set of directions of the lines of $L$ considered as points of the projective space at infinity. We give a geometric construction of a set of lines $L$, where $D$ contains an $N^{n-1}$ grid and where $S$ has size $2(\frac{1}{2}N)^n$, given a starting configuration in the plane. We provide examples of such starting configurations for the reals and for finite fields. Following Dvir’s proof of the finite field Kakeya conjecture and the idea of using multiplicities of Dvir, Kopparty, Saraf and Sudan, we prove a lower bound on the size of $S$ dependent on the ideal generated by the homogeneous polynomials vanishing on $D$. This bound is maximised as $(\frac{1}{2}N)^n$ plus smaller order terms, for $n \geq 4$, when $D$ contains the points of a $N^{n-1}$ grid.

1. Introduction

Let $AG_n(\mathbb{K})$ denote the $n$-dimensional affine space over the field $\mathbb{K}$ and let $PG_n(\mathbb{K})$ denote the $n$-dimensional projective space over the field $\mathbb{K}$.

Let $L$ be a set of lines of $AG_n(\mathbb{K})$ and let $D$ be the set of directions of the lines of $L$, viewed as points of the projective space $PG_{n-1}(\mathbb{K})$ at infinity. Let $S$ be a set of points of $AG_n(\mathbb{K})$ with the property that every line of $L$ is incident with at least $N$ points of $S$.

In the case that $\mathbb{K} = \mathbb{F}_q$ and $N = q$, Dvir [1] proved that if $L$ contains a line in every direction then $|S| > q^n/n!$, answering a question posed by Wolff in [7]. Dvir, and subsequently Saraf and Sudan [4], provided examples of set of lines $L$ containing a line with every direction and sets of points $S$ for which $|S| = 2(\frac{1}{2}q)^n$ plus smaller order terms. The lower bound on $|S|$ was improved for $n \geq 4$ to $|S| \geq (\frac{1}{2}q)^n + c(n)q^{n-1}$ for some $c(n)$, by Dvir, Kopparty, Saraf and Sudan in [2].

We define a $N^{n-1}$ grid in $PG_{n-1}(\mathbb{K})$ as a point set, which with respect to a suitable basis, has the form

$$\{(a_1, \ldots, a_{n-1}, 1) \mid a_i \in A_i\},$$

where $A_i$ is a subset of $\mathbb{K}$ of size $N$ for all $i = 1, \ldots, n-1$.

The aim of this article is reformulate the problem in a far more general setting. There are a couple of recent articles by Slavov in which he formulates the Kakeya problem in an algebraic geometric setting, see [5] and [6]. Here we consider any arbitrary finite set of
lines in an affine space over any fixed field \( K \). We prove lower bounds on the size of \( S \) that depend on \( I(D) \), the ideal generated by the homogeneous polynomials of \( K[X_1, \ldots, X_n] \) which are zero at all points of \( D \). Firstly, we will give a geometric construction of set of \( N^{n-1} \) lines, whose directions contain a \( N^{n-1} \) grid and a set \( S \) of roughly \( 2(\frac{1}{2}N)^n \) points with the property that every line of \( L \) is incident with at least \( N \) points of \( S \).

2. A geometric construction of Kakeya sets

For any two non-intersecting subspaces \( x \) and \( y \) of a projective space we denote by \( x \oplus y \) the subspace that they span.

Let \( x_0, x_1, \ldots, x_n \) be projective points in general position and let

\[
\Sigma_i = x_0 \oplus x_1 \oplus \cdots \oplus x_n,
\]

and let

\[
\pi_i = x_1 \oplus x_2 \oplus \cdots \oplus x_n.
\]

Let \( y_i \) be a third point on the line \( x_{i-1} \oplus x_i \), for \( i = 1, \ldots, n \), so

\[
(x_i \oplus y_i) \cap \pi_{i-1} = x_{i-1}.
\]

Let \( L \) be a set of lines of \( \Sigma_2 \) incident with distinct points of \( \pi_1 \), or in other words, by interpreting \( \pi_1 \) as the line at infinity, distinct directions. Note that if \( K \) is infinite then we can always find a line which intersects the lines of a finite set of lines in distinct points. More generally for a set of lines in \( \text{AG}_n(K) \), we can always find a hyperplane which intersects the lines of a finite set of lines in distinct points. After a suitable change of basis this line (hyperplane) can be assumed to be the line (hyperplane) at infinity.

Let \( (\ell_1, \ldots, \ell_{n-1}) \) be an \((n-1)\)-tuple of distinct lines of \( L \) and let

\[
p_i = \ell_i \cap \pi_1.
\]

By assumption, \( p_1, \ldots, p_{n-1} \) are distinct points.

We now construct a set \( L' \) of \(|L|(|L|-1)\cdots(|L|-n+2)\) lines in \( \Sigma_n \) with distinct directions, i.e. distinct intersections with the hyperplane \( \pi_{n-1} \) of \( \Sigma_n \). See Figure 1 for a pictorial representation of this construction in the three dimensional case.

Define a line of \( \Sigma_n \) by

\[
\ell_{1,\ldots,n-1} = (x_n \oplus \ell_{1,\ldots,n-3,n-2}) \cap (y_n \oplus \ell_{1,\ldots,n-3,n-1}).
\]

This line intersects \( \pi_n \) in the point

\[
p_{1,\ldots,n-1} = (x_n \oplus p_{1,\ldots,n-3,n-2}) \cap (y_n \oplus p_{1,\ldots,n-3,n-1}),
\]

By induction, the points \( p_{1,\ldots,n-2} \) are distinct for distinct \((n-2)\)-tuples of lines \((\ell_1, \ldots, \ell_{n-2})\), so the points \( p_{1,\ldots,n-1} \) are all distinct.
Let \( m \) be a line of \( \Sigma_2 \) incident with the point \( x_2 \). For each occurrence that we can find lines \( \ell_n, \ldots, \ell_{2n-2} \in L \) such that there are points

\[
z_i = \ell_i \cap \ell_{n-1+i} \cap m,
\]

for all \( i = 1, \ldots, n-1 \), we construct a point of \( S' \) incident with the line \( \ell_{1,\ldots,n-1} \) inductively by

\[
z_{1,\ldots,n-1} = (x_n \oplus z_{1,\ldots,n-3,n-2}) \cap (y_n \oplus z_{1,\ldots,n-3,n-1}).
\]

Proof. Observe that we construct the same point \( z_{1,\ldots,n-1} \) in the same way if we choose \( \ell_{i+n-1} \) instead of \( \ell_i \). This implies that each point of \( S' \) is incident with \( 2^{n-1} \) points of \( L' \).

The set \( S' \) contains

\[
\sum_{i=1}^{N} \left( \frac{1}{2}N - \epsilon_i \right) \left( \frac{1}{2}N - \epsilon_i - 1 \right) \cdots \left( \frac{1}{2}N - \epsilon_i - n + 2 \right)
\]

points, so we have constructed \( N^n - c(n)N^{n-1} \) incidences between lines of \( L' \) and points of \( S' \).

The set \( L' \) contains \( N(N-1) \ldots (N-n+2) \) lines and we would like each line to be incident with \( N \) points of \( S' \). Therefore we are missing less than \( c(n)N^{n-1} \) incidences. No
line of \( L' \) is incident with more than \( N \) points of \( S' \), so we can add less than \( c(n)N^{n-1} \) points to \( S' \) so that every line of \( L' \) is incident with at least \( N \) points of \( S' \). This does not affect the first order term of \( |S'| \), which is \( N^n/2^{n-1} \).

Finally, we add lines to \( L' \) and \( N \) points to \( S' \) for each of these lines, so that we have a line with every direction of the \( N^{n-1} \) grid. Thus far we have constructed \( \binom{N}{n-1}(n-1)! \) lines in \( L' \), so we add less than \( c'N^{n-2} \) lines to \( L' \) to complete the grid and add at most \( c'N^{n-1} \) points to \( S' \), for some \( c' = c'(n) \). Again, this does not affect the first order term of \( |S'| \).

\[ \square \]

Example 2. If \( K = \mathbb{F}_q \) and \( N = q \) then we can take \( L \) to be the lines dual to a conic (or any oval), where one the lines is \( \pi_1 \). If \( q \) is even then \( \epsilon_i = 0 \) for \( i = 1, \ldots, q-1 \) and \( \epsilon_q = 0 \). If \( q \) is odd then \( \epsilon_i = \frac{1}{2} \) for \( i = 1, \ldots, q \).

Example 3. If \( K = \mathbb{R} \) then we can take \( L \) to be the set of lines dual to a regular \( N \)-gon. If \( N \) is even then \( \epsilon_i = 0 \) for \( i = \frac{1}{2}N, \ldots, N \) and \( \epsilon_i = 1 \) for \( i = \frac{1}{2}N + 1, \ldots, N \). If \( N \) is odd then \( \epsilon_i = \frac{1}{2} \) for \( i = 1, \ldots, N \).

In [3], Guth and Katz prove that if \( L \) is a set of lines in \( \text{AG}_3(\mathbb{R}) \), no \( N \) of which are contained in a plane, and if \( S \) is a set of points with the property that every line of \( L \) is incident with at least \( N \) points of \( S \), then \( |S| > cN^3 \) for some (very small) constant \( c \).

Example 3, together with Theorem 1, provide an example of such a set of lines for which \( |S| = \frac{1}{4}N^3 \) plus smaller order terms.

3. A lower bound for \( |S| \)

Let \( J = (\mathbb{Z}_{\geq 0})^n \) be the set \( n \)-tuples of non-negative integers. For any \( j, c \in J \), we define the \( j \)-Hasse derivative of \( X^c = \prod_{i=1}^n X_i^{c_i} \) as

\[
\partial^j(X^c) = \prod_{i=1}^n \binom{c_i}{j_i} X_i^{c_i-j_i}.
\]

This definition extends to polynomials by linearity.

For any \( j \in J \), let \( \text{wt}(j) = \sum_{i=1}^n j_i \). We say that a polynomial \( f \in \mathbb{K}[X_1, \ldots, X_n] \) has a zero of multiplicity \( m \) at a point \( u \) of \( \text{AG}_n(\mathbb{K}) \) if \( u \in V(\partial^j f) \) for all \( j \in J \), where \( \text{wt}(j) \leq m - 1 \).

If \( u \) is a zero of multiplicity \( m \) of \( f \) and \( \text{wt}(j) = r \) then \( u \) is a zero of multiplicity at least \( m - r \) of \( \partial^j f \), see [2].

Let \( I_r(D) \) be the ideal of homogeneous polynomials of \( \mathbb{K}[X_1, \ldots, X_n] \) which have zeros of multiplicity at least \( r \) at all points of \( D \).

For any \( f \in \mathbb{K}[X_1, \ldots, X_n] \), let \( f^* \) denote the polynomial consisting of the terms of \( f \) of highest degree.
Theorem 4. If $U$ is a subspace of $\mathbb{K}[X_1, \ldots, X_n]$ of polynomials of degree at most $rN - 1$ with the property that for all non-zero $f \in U$, $f^* \not\in I_r(D)$ then

$$\binom{2r + n - 2}{n} |S| \geq \dim U.$$ 

Proof. Suppose that $\binom{2r + n - 2}{n} |S| < k$, where $\dim U = k$. Let $f(X)$ be a polynomial of $U$, so

$$f(X) = \sum_{i=1}^{k} a_i h_i(X),$$

where $\{h_1, \ldots, h_k\}$ is a basis for $U$, for some $a_i \in \mathbb{K}$. Suppose that $f$ has a zero of multiplicity at least $2r - 1$ at all points $x \in S$. For every $x \in S$, $\partial^j f$ has a zero of multiplicity $2r - 1 - \deg(j)$ at $x$. Therefore, for each $j \in J$, where $\deg(j) \leq 2r - 2$, $\partial^j f(x) = 0$ is a linear equation with unknowns $a_1, \ldots, a_k$. Thus we get a system of $\binom{n+2r-2}{n} |S|$ linear equations and $k$ unknowns. Since $\binom{n+2r-2}{n} |S| < k$ there must be a non-trivial solution and so there is an $f \in U$ such that $f$ has a zero of multiplicity at least $2r - 1$ at all points $x \in S$.

By hypothesis, for any $\langle v \rangle \in D$ there is a line with direction $v$ incident with at least $N$ points of $S$. Therefore, for any $\langle v \rangle \in D$ there is a $u \in \text{AG}_n(\mathbb{K})$ and $N$ distinct values $\lambda \in \mathbb{K}$ with the property that $u + \lambda v$ is a zero of $f$ of multiplicity at least $2r - 1$. For any $j \in J$ with $\deg(j) \leq r - 1$, $u + \lambda v$ is a zero of $\partial^j f$ of multiplicity at least $r$. Since $d = \deg f \leq rN - 1$, it follows that $\partial^j f(u + \lambda v)$ is identically zero as a polynomial in $\lambda$. The coefficient of $\lambda^d$ of $\partial^j f$ is $\partial^j f(\langle v \rangle)$. Hence, $\partial^j f(\langle v \rangle) = 0$ for all $j \in J$, where $\deg(j) \leq r - 1$. This implies $f^*$ has a zero of multiplicity $r$ at all points of $D$ and so $f^* \in I_r(D)$, which is a contradiction, since $f \in U$ implies $f^* \not\in I_r(D)$.

Theorem 4 allows us to give an explicit lower bound for $|S|$ if $D$ contains an $N^{n-1}$ grid.

Recall that we defined a $N^{n-1}$ grid in $\text{PG}_{n-1}(\mathbb{K})$ as

$$\{(a_1, \ldots, a_{n-1}, 1) \mid a_i \in A_i\},$$

where $A_i$ is a subset of $\mathbb{K}$ of size $N$ for all $i = 1, \ldots, n - 1$.

Theorem 5. If $D$ contains an $N^{n-1}$ grid then, for any $r \in \mathbb{N}$,

$$\binom{2r + n - 2}{n} |S| \geq \binom{rN + n - 1}{n}.$$ 

Proof. The ideal $I_r(D)$ is generated by products of $r$ (not necessarily distinct) polynomials from the set $\{g_1, \ldots, g_{n-1}\}$, where

$$g_i(X) = \prod_{a \in A_i} (X_i - aX_n).$$

Any non-zero polynomial in $I_r(D)$ has degree at least $rN$, so we can set $U$ to be the subspace of all polynomials in $\mathbb{K}[X_1, \ldots, X_n]$ of degree at most $rN - 1$. 

$\square$
Theorem 6. If $D$ contains an $N^{n-1}$ grid then
$$|S| \geq \binom{N+n-1}{n}.$$}

Proof. Put $r = 1$ in Theorem 5. 

The following theorem improves on the lower bound in Theorem 6 for $n \geq 4$.

Theorem 7. If $D$ contains an $N^{n-1}$ grid then $|S| \geq \left( \frac{1}{2}N \right)^n$.

Proof. By Theorem 5 we have
$$|S| \geq \frac{(rN+n-1)(rN+n-2)\ldots(rN)}{(2r+n-2)(2r+n-3)\ldots(2r-1)}.$$This gives $|S| \geq \left( \frac{1}{2}N \right)^n$ if we choose $r$ large enough.

References