Mathematika 56 (2010) 1–25 © University College London
doi:10.1112/S0025579309000400

THE KAKEYA SET AND MAXIMAL CONJECTURES FOR ALGEBRAIC VARIETIES OVER FINITE FIELDS

JORDAN S. ELLENBERG, RICHARD OBERLIN AND TERENCE TAO

Abstract. Using the polynomial method of Dvir [On the size of Kakeya sets in finite fields. *Preprint*], we establish optimal estimates for Kakeya sets and Kakeya maximal functions associated to algebraic varieties W over finite fields F. For instance, given an $(n-1)$-dimensional projective variety $W \subset \mathbb{P}^n(F)$, we establish the Kakeya maximal estimate

$$\left\| \sup_{\gamma \ni w} \sum_{v \in \gamma(F)} |f(v)| \right\|_{\ell^n(W)} \leq C_{n,W,d} |F|^{(n-1)/n} \|f\|_{\ell^n(F^n)}$$

for all functions $f : F^n \to \mathbf{R}$ and $d \geq 1$, where for each $w \in W$, the supremum is over all irreducible algebraic curves in F^n of degree at most d that pass through w but do not lie in W, and with $C_{n,W,d}$ depending only on n, d and the degree of W; the special case when W is the hyperplane at infinity in particular establishes the Kakeya maximal function conjecture in finite fields, which in turn strengthens the results of Dvir.

§1. *Introduction.* Recently, Dvir [5] established the following result, first conjectured by Wolff [17].

THEOREM 1.1 (Kakeya set conjecture for F^n). *Let $n \geq 1$, let F be a finite field, and let $E \subset F^n$ be a subset of F^n that contains a line in every direction. Then $|E| \geq c_n |F|^n$, where $c_n > 0$ depends only on n.*

Remark 1.2. Dvir's original argument gave the value $c_n = 1/n!$ for the constant c_n; this was recently improved in [6, 13] to $c_n = (\frac{1}{2} + o(1))^n$, which is best possible except for possible refinement of the $o(1)$ error.

This result is the finite-field analogue of the *Kakeya set conjecture for* $\mathbf{R}^n$, which is of importance in harmonic analysis; we refer the reader to [11, 17] for further discussion. In this paper we shall obtain a stronger version of Theorem 1.1, the finite-field analogue of an analogous conjecture in $\mathbf{R}^n$ (see e.g. [2, 17].) This answers a question raised in [11].

THEOREM 1.3 (Kakeya maximal conjecture for F^n). *Let $n \geq 1$, let F be a finite field, and let $f : F^n \to \mathbf{R}$ be a function. Then*

$$\left\| \sup_{\gamma // \omega} \sum_{x \in \gamma} |f(x)| \right\|_{\ell^n(\mathbb{P}^{n-1}(F))} \leq C_n |F|^{(n-1)/n} \|f\|_{\ell^n(F^n)}. \tag{1.1}$$

Received 11 March 2009.
MSC (2000): 42B25 (primary), 11G25, 51E20 (secondary).

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

In the statement of Theorem 1.3 and throughout the paper we use the following notation.

- The space $\mathbb{P}^{n-1}(F)$ is the $(n-1)$-dimensional projective space over F, and a point ω of $\mathbb{P}^{n-1}(F)$ is interpreted as a direction in F^n.
- The space ℓ^p denotes the usual family of Lebesgue norms

$$\|G\|_{\ell^p(A)} := \left(\sum_{\omega \in A} |G(\omega)|^p\right)^{1/p}$$

with the usual modification for $p = \infty$.

The supremum on the left-hand side of (1.1) is over all lines γ with direction ω, and C_n is a constant depending only on n. In general, the bounds in this paper will all involve unspecified constants depending on geometric quantities like n or the degree and dimension of various fixed algebraic varieties; the point is that these constants are independent of $|F|$.

Remark 1.4. By interpolating (1.1) with more trivial estimates we obtain

$$\left\| \sup_{\gamma // \omega} \sum_{x \in \gamma} |f(x)| \right\|_{\ell^q(\mathbb{P}^{n-1}(F))} \leq C_n |F|^{(n-1)/q} \|f\|_{\ell^p(F^n)} \tag{1.2}$$

whenever p and q are positive real numbers satisfying $1 \leq p \leq n$ and $1 \leq q \leq (n-1)(p/(p-1))$. Various special cases of (1.2) had been established previously in the literature; see [**11**]. Except for the issue of determining the constant C_n, the various exponents in (1.1) or (1.2) are sharp, as can be seen by testing (1.1) with f equal to the indicator of a point, a line, or the whole space F^n.

Remark 1.5. It would be interesting to investigate the question of which functions f make the inequality in Theorem 1.3 a near-equality. The indicator function of a linear subspace always yields an equality in (1.1). When n is large, does the approximate equality in (1.1) indicate that f is disproportionately concentrated on a linear subspace of F^n? In contrast, the dual estimate

$$\left\| \sum_{\omega \in \mathbb{P}^{n-1}(F)} g(\omega) 1_{\gamma_\omega} \right\|_{\ell^{n/(n-1)}(F^n)} \leq C_n |F|^{(n-1)/n} \|g\|_{\ell^{n/(n-1)}(\mathbb{P}^{n-1}(F))},$$

where γ_ω is a line with direction ω for each $\omega \in \mathbb{P}^{n-1}(F)$, is essentially an equality for any non-negative g, thanks to the elementary inequality

$$\left\| \sum_{\omega \in \Omega} f_\omega \right\|_{\ell^p(A)} \geq \left(\sum_{\omega \in \Omega} \|f_\omega\|_{\ell^p(A)}^p \right)^{1/p}$$

for all $1 \leq p < \infty$ and non-negative functions $f_\omega : A \to \mathbf{R}^+$. (We will not use this dual formulation elsewhere in this paper.)

Theorem 1.1 follows immediately from Theorem 1.3 by specializing f to equal the indicator function $f = 1_E$ of the set E in Theorem 1.1.

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

In fact, the goal of this paper is to establish a still more general statement than Theorem 1.3, in which $\mathbb{P}^{n-1}(F)$ is replaced by the F-rational points of an essentially arbitrary $(n-1)$-dimensional algebraic variety of bounded degree. (See Appendix A for a review of the relevant terminology from algebraic geometry.)

THEOREM 1.6 (Kakeya maximal conjecture for algebraic varieties over F). *Let $N, d, n \geq 1$, let F be a finite field, let $V = \mathbb{P}^N$ (respectively $V = \mathbb{A}^N$), and let $W \subset V$ be a projective (respectively affine) variety of dimension $n-1$ and degree at most d. Then for any $f : V(F) \to \mathbf{R}$ we have*

$$\left\| \sup_{\gamma \ni w} \sum_{v \in \gamma(F)} |f(v)| \right\|_{\ell^n(W(F))} \leq C_{N,d,n} |F|^{(n-1)/n} \|f\|_{\ell^n(V(F))}. \tag{1.3}$$

Here, w ranges over $W(F)$, and for each $w \in W(F)$, the range of the supremum is the set of all irreducible projective (respectively affine) algebraic curves γ in V of degree at most d, which contain w but are not contained in W. The constant $C_{N,d,n} > 0$ depends only on N, d, n (and in particular is independent of F).

Remark 1.7. The observation that the polynomial method can be used to control the intersection of a specified set with curves of bounded degree (as opposed to lines) already appears in [7], in Claim 3.3 and the discussion preceding it.

Remark 1.8. The non-degeneracy requirement that γ is not contained in W is easily seen to be necessary, for instance by considering the case when $V = \mathbb{A}^n$, $W = \mathbb{A}^{n-1}$, and f is the indicator function of F^{n-1}.

Remark 1.9. Theorem 1.6 is stated for V equal to all of projective or affine space, but one can trivially restrict V to any smaller set (e.g. some intermediate subvariety between W and $\mathbb{P}^N$ or $\mathbb{A}^N$) and obtain the same estimate for $f \in \ell^n(V(F))$. Indeed, the most interesting case in practice is that where V is an n-dimensional variety containing W.

Theorem 1.3 follows immediately from Theorem 1.6 by taking $V = \mathbb{P}^n$ and W the hyperplane at infinity, and setting $d = 1$; then the set of projective lines through a given point of $W(F)$ is naturally identified with the set of lines in F^n parallel to some fixed line.

As a corollary of Theorem 1.6, we have a generalization of Theorem 1.1 to algebraic varieties.

COROLLARY 1.10 (Kakeya set conjecture for algebraic varieties over F). *Let N, d, n, F, V, W be as in Theorem 1.6. Let $w_1, \ldots, w_J \in W(F)$ be distinct F-points in W, and for each $1 \leq j \leq J$ let γ_j be an irreducible algebraic curve of degree at most d in V that passes through w_j but does not lie in W. Let $\lambda \geq 1$, and let $E \subset V(F)$ be a set of F-points in V such that $|E \cap \gamma_j(F)| \geq \lambda$ for all $1 \leq j \leq J$. Then $|E| \geq C_{N,d,n}^{-n} J \lambda^n / |F|^{n-1}$, where $C_{N,d,n}$ is the constant in Theorem 1.6.*

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

In §§2 and 3 we shall prove Theorem 1.6. The strategy will be to first establish the "flat" case $V = \mathbb{A}^n$, $W = \mathbb{A}^{n-1}$ of the theorem using (a weighted form of) Dvir's method combined with the Nikishin–Maurey–Pisier–Stein factorization trick and some real interpolation techniques. Then, using a random projection trick to flatten W, we deduce the general case from the flat case. In §4 we discuss some variants and generalizations of the above results.

Notation 1.11. We use the notation $X \ll Y$, $Y \gg X$, or $X = O(Y)$ to denote an estimate of the form $X \leq CY$ where C is a constant that is allowed to depend on parameters such as the dimension n (but is always independent of the field F). We sometimes use subscripts to draw attention to additional parameters on which the implied constants depend; for example, $X \ll_{C_0} Y$ means that $X \leq CY$ where C depends not only on n but also some constant C_0 which is local to the argument. We write $X \asymp Y$ for $X \ll Y \ll X$.

Unless otherwise specified, all varieties are defined over the fixed finite field F; so that when we refer to "a curve of degree d in $\mathbb{A}^n$", for instance, we mean a curve defined over F.

§2. *The flat case.* To prove Theorem 1.6, we first establish a model case when $V = \mathbb{A}^n$ (thus $V(F) = F^n$) and W is the standard hyperplane $W = \mathbb{A}^{n-1}$ of $\mathbb{A}^n$ embedded in $\mathbb{A}^n$ in the usual manner; the reason for treating this case first is that it enjoys a very useful translation-invariance symmetry that can be exploited to obtain good estimates. In the next section we shall use a random projection trick to reduce the general case to this case.

The main result of this section is following.

THEOREM 2.1 (Kakeya maximal conjecture for curves in F^n). *Let $d, n \geq 1$. For any $f : F^n \to \mathbf{R}$, let $f^* : F^{n-1} \to \mathbf{R}$ be the maximal function*

$$f^*(w) := \sup_{\gamma \ni w} \sum_{v \in \gamma(F) \setminus F^{n-1}} |f(v)| \tag{2.1}$$

where the supremum is over all irreducible algebraic curves γ in F^n of degree at most d that pass through w. Then we have

$$\|f^*\|_{\ell^n(F^{n-1})} \ll |F|^{(n-1)/n} \|f\|_{\ell^n(F^n)},$$

where the implied constants can depend on d and n.

Remark 2.2. It is easy to see that the $d = 1$ case of Theorem 2.1 implies Theorem 1.3, by applying a projective transformation to move F^{n-1} to the plane at infinity (cf. [**16**]). (Strictly speaking, this transformation will leave out a codimension-one set of directions, and also a codimension-one set of points, but one can easily erase this omission by rotating the estimate a bounded number of times and using the triangle inequality; we omit the details. In any case, Theorem 1.3 will also be deduced from the stronger Theorem 1.6, proven in the next section.)

Theorem 2.1 will follow from the following distributional estimate.

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

PROPOSITION 2.3 (Kakeya distributional estimate for curves in F^n). *Let d, $n \geq 1$. Then there exists $K = K_{d,n}$ such that for any $A > 0$, any $f : F^n \to \{0\} \cup [A, +\infty)$, and every $K\|f\|_{\ell^n(F^n)} \leq \lambda \leq A|F|$, we have*

$$|\{w \in F^{n-1} : f^*(w) \geq \lambda\}| \ll \frac{|F|^{n-2}}{A\lambda^{n-1}} \|f\|^n_{\ell^n(F^n)},$$

where the supremum and implied constants are as in Theorem 2.1.

Proof of Theorem 2.1 assuming Proposition 2.3. We will use a variant of the real interpolation method. We may of course take f to be non-negative and not identically zero. We normalize $\|f\|_{\ell^n(F^n)} = 1$. Using the identity

$$\|f^*\|^n_{\ell^n(F^{n-1})} = n \int_0^\infty |\{w \in F^{n-1} : f^*(w) \geq \alpha\}| \alpha^{n-1}\, d\alpha \tag{2.2}$$

it suffices to show that

$$\int_0^\infty |\{w \in F^{n-1} : f^*(w) \geq \alpha\}| \alpha^{n-1}\, d\alpha \ll |F|^{n-1}.$$

The crude bound $|\{w \in F^{n-1} : f^*(w) \geq \alpha\}| \leq |F|^{n-1}$ allows one to dispose of the region $\alpha \leq C_0$, where $C_0 = O(1)$ is a large constant to be chosen later. So it remains to show that

$$\int_{C_0}^\infty |\{w \in F^{n-1} : f^*(w) \geq \alpha\}| \alpha^{n-1}\, d\alpha \ll |F|^{n-1}. \tag{2.3}$$

Fix $\alpha > C_0$. For each positive integer j we define a function $f_{j,\alpha} : F^n \to \mathbf{R}$ by

$$f_{j,\alpha}(v) = \begin{cases} f(v) & \text{if } 100^{n(j-1)} \dfrac{\alpha}{C_0^{1/2}|F|} \leq f(v) < 100^{nj} \dfrac{\alpha}{C_0^{1/2}|F|} \\ 0 & \text{otherwise.} \end{cases}$$

We similarly define $f_{0,\alpha}(v)$ to be equal to $f(v)$ when $f(v) < (\alpha/(C_0^{1/2}|F|))$ and 0 otherwise. Finally, we define $f_\alpha(v)$ to be equal to $f(v)$ when $f(v) \geq 100^{n(j_\alpha-1)}(\alpha/(C_0^{1/2}|F|))$ and 0 otherwise, where j_α is the largest integer satisfying $\alpha/2^{j_\alpha+1} \geq K$, where K is the quantity in Proposition 2.3. Then f decomposes as

$$f = f_\alpha + f_{0,\alpha} + \sum_{j=1}^{j_\alpha-1} f_{j,\alpha}.$$

From Lemma A.3 and the bound $f_{0,\alpha}(v) < (\alpha/(C_0^{1/2}|F|))$ we have

$$f^*_{0,\alpha}(w) \ll \frac{\alpha}{C_0^{1/2}}$$

and thus (if C_0 is large enough)

$$f^*(w) \leq f^*_\alpha(w) + \sum_{j=1}^{j_\alpha-1} f^*_{j,\alpha}(w) + \frac{\alpha}{2}$$

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

and hence

$$|\{w \in F^{n-1} : f^*(w) \geq \alpha\}| \leq |\{w \in F^{n-1} : f_\alpha^*(w) \geq K\}| + \sum_{j=1}^{j_\alpha - 1} |\{w \in F^{n-1} : f_{j,\alpha}^*(w) \geq \alpha/2^{j+1}\}|.$$

On the other hand, we have

$$\max(\|f_\alpha\|_{\ell^n(F^n)}, \|f_{j,\alpha}\|_{\ell^n(F^n)}) \leq \|f\|_{\ell^n(F^n)} = 1.$$

Applying Proposition 2.3 with $A := 100^{n(j_\alpha - 1)}(\alpha/(C_0^{1/2}|F|))$ and $\lambda := K$ we obtain

$$|\{w \in F^{n-1} : f_\alpha^*(w) \geq K\}| \ll_{C_0} 100^{-nj_\alpha}|F|^{n-1} \ll \alpha^{-2n}|F|^{n-1}$$

where the last inequality follows from the maximality of j_α. It follows that

$$\int_{C_0}^{\infty} |\{w \in F^{n-1} : f_\alpha^*(w) \geq K\}|\alpha^{n-1}\, d\alpha \ll_{C_0} |F|^{n-1}.$$

For each $j < j_\alpha$, we now apply Proposition 2.3 with

$$A := 100^{n(j-1)}\frac{\alpha}{C_0^{1/2}|F|} \quad \text{and} \quad \lambda := \min(\alpha/2^{j+1}, A|F|);$$

note by the choice of j_α and the hypothesis $\alpha \geq C_0$, that $\lambda \geq K$ if C_0 is large enough. Using the fact that

$$A|F| \gg \frac{\alpha}{2^{j+1}C_0^{1/2}}$$

we obtain

$$|\{w \in F^{n-1} : f_{j,\alpha}^*(w) \geq \alpha/2^{j+1}\}| \ll_{C_0} 100^{-nj}2^{(n-1)j}\frac{|F|^{n-1}}{\alpha^n}\|f_{j,\alpha}\|_{\ell^n(F^n)}^n$$

where the subscript $\ll_{C_0}$ indicates that the implied constant can depend on C_0. Putting this all together, one finds that

$$\int_{C_0}^{\infty} |\{w \in F^{n-1} : f^*(w) \geq \alpha\}|\alpha^{n-1}\, d\alpha \ll_{C_0} |F|^{n-1} + \sum_{j=1}^{\infty} 100^{-nj}2^{(n-1)j}|F|^{n-1}\int_{C_0}^{\infty}\sum_{v \in \Sigma_{j,\alpha}} f(v)^n\,\frac{d\alpha}{\alpha}$$

where $\Sigma_{j,\alpha} \subset F^n$ denotes the support of $f_{j,\alpha}$.

Now interchange the α integration and v summation; for each fixed v, the function of α to be integrated against $d\alpha/\alpha$ is the product of $f(v)^n$ with the

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

characteristic function of an interval of the form $[A, 100^n A]$. The size of this integral is a constant multiple of $f(v)^n$; so we arrive at the inequality

$$\int_{C_0}^{\infty} |\{w \in F^{n-1} : f^*(w) \geq \alpha\}| \alpha^{n-1}\, d\alpha \ll_{C_0} \sum_{j=1}^{\infty} 100^{-nj} 2^{(n-1)j} |F|^{n-1} \sum_{v \in F^n} f(v)^n$$

and (2.3) now follows from the normalization $\|f\|_{\ell^n(F^n)} = 1$. □

It remains to prove Proposition 2.3. We first rewrite that proposition in an equivalent form. We may first normalize by dividing f and λ by A; thus, it suffices to prove Proposition 2.3 with $A = 1$. Let us enumerate the set $\{w \in F^{n-1} : f^*(w) \geq \lambda\}$ as $w_1, \ldots, w_J$, and for each $1 \leq j \leq J$, let γ_j be the curve attaining the supremum used to define $f^*(w_j)$ in (2.1). (Note that as there are only finitely many possible choices for γ_j, the supremum here is attainable.) Our task is now to show the following.

PROPOSITION 2.4 (Distributional estimate, again). *Let $d, n \geq 1$, and let $w_1, \ldots, w_J$ be distinct points in F^{n-1}. For each $1 \leq j \leq J$, let γ_j be an irreducible algebraic curve in $\mathbb{A}^n$ of degree at most d that passes through w_j but does not lie in $\mathbb{A}^{n-1}$. Let $f : F^n \to \{0\} \cup [1, +\infty)$ and $K\|f\|_{\ell^n(F^n)} \leq \lambda \leq |F|$ for some sufficiently large K depending only on d, n, and suppose that*

$$\sum_{v \in \gamma_j(F) \setminus F^{n-1}} f(v) \geq \lambda \tag{2.4}$$

for all $1 \leq j \leq J$. Then

$$J \ll \frac{|F|^{n-2}}{\lambda^{n-1}} \sum_{v \in F^n} f(v)^n. \tag{2.5}$$

The hypothesis and conclusion of this proposition are invariant under translations of F^n by vectors in F^{n-1}. We take advantage of this translation invariance to make a standard reduction (cf. [**2, 12, 15**]) to the case of small λ (or equivalently, for large J).

PROPOSITION 2.5 (Nikishin–Maurey–Pisier–Stein factorization reduction). *To prove Proposition 2.4, it suffices to do so in the special case $\lambda = K_0\|f\|_{\ell^n(F^n)} \leq |F|$ for some sufficiently large K_0 depending on n and d.*

Proof. Let $d, n, w_1, \ldots, w_J, \gamma_1, \ldots, \gamma_J, f, \lambda$ be as in Proposition 2.4. Let K_0 be as in Proposition 2.5, and assume K sufficiently large depending on d, n, K_0. Let M be the greatest integer less than or equal to $\lambda^n/(K_0^n \|f\|^n_{\ell^n(F^n)})$; thus $M \geq 1$ if K is large enough.

We use a probabilistic method. Let $u_1, \ldots, u_M \in F^{n-1}$ be selected independently and uniformly at random, and let $\Omega := \{w_j + u_m : 1 \leq j \leq J,$

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

$1 \le m \le M\}$, thus Ω is a random subset of F^{n-1}. Observe that every $w \in F^{n-1}$ lies in Ω with probability

$$1 - \left(1 - \frac{J}{|F|^{n-1}}\right)^M \asymp \min\left(\frac{MJ}{|F|^{n-1}}, 1\right).$$

The expected size of Ω is thus

$$\mathbb{E}|\Omega| \asymp \min(MJ, |F|^{n-1}),$$

and so we may select $u_1, \dots, u_M$ such that

$$|\Omega| \gg \min(MJ, |F|^{n-1}). \tag{2.6}$$

Fix these $u_1, \dots, u_M$, and define

$$f_M(v) := \left(\sum_{m=1}^{M} f(v - u_m)^n\right)^{1/n}.$$

Then f_M clearly takes values in $\{0\} \cup [1, +\infty)$, and

$$\|f_M\|_{\ell^n(F^n)}^n = \sum_{m=1}^{M} \|f(\cdot - u_m)\|_{\ell^n(F^n)}^n = M\|f\|_{\ell^n(F^n)}^n \tag{2.7}$$

and thus (by construction of M)

$$K_0\|f_M\|_{\ell^n(F^n)} \le \lambda \ll K_0\|f_M\|_{\ell^n(F^n)}.$$

On the other hand, since $f_M(v) \ge f(v - u_m)$ for every $1 \le m \le M$, we also have

$$\sum_{v \in \gamma_j(F) + u_m \setminus F^{n-1}} f_M(v) \ge \lambda$$

for all $1 \le j \le J$ and $1 \le m \le M$. Applying Proposition 2.5 with f replaced by f_M, λ replaced by $K_0\|f_M\|_{\ell^n(F^n)}$, and $w_1, \dots, w_J$ replaced by an enumeration of Ω, we conclude that

$$|\Omega| \ll \frac{|F|^{n-2}}{(K_0\|f_M\|_{\ell^n(F^n)})^{n-1}} \sum_{v \in F^n} f_M(v)^n \ll \frac{|F|^{n-2}}{\lambda^{n-1}} \sum_{v \in F^n} f_M(v)^n$$

and hence by (2.6), (2.7) we have

$$\min(MJ, |F|^{n-1}) \ll \frac{|F|^{n-2}}{\lambda^{n-1}} M\|f\|_{\ell^n(F^n)}^n.$$

If $MJ \le |F|^{n-1}$, then we obtain (2.5) as required. If instead $MJ > |F|^{n-1}$, then we have

$$|F|^{n-1} \ll \frac{|F|^{n-2}}{\lambda^{n-1}} M\|f\|_{\ell^n(F^n)}^n.$$

Using the definition of M, we conclude that

$$\lambda \gg K_0^n |F|.$$

However, this contradicts the hypothesis $\lambda \le |F|$, if K_0 is large enough. □

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

It remains to prove Proposition 2.4 in the case $\lambda = K_0 \|f\|_{\ell^n(F^n)}$ for some large $K_0 = K_0(n, d)$.

We begin with some simple reductions. Rounding f down to the nearest integer (modifying λ and K_0 appropriately) we may now assume that f is integer-valued. Since $\lambda \leq |F|$, we may replace f with $\min(f, |F|)$ without affecting the property (2.4). So we have reduced to the case where f takes values in the set $\{0, 1, \ldots, |F|\}$. Our task is to show that

$$J \ll |F|^{n-2} \|f\|_{\ell^n(F^n)}. \tag{2.8}$$

To establish this, we use the polynomial method of Dvir [5] (or more precisely the weighted refinement of this method as used in [6, 13]). Let $1 \leq D < |F|$ be an integer to be chosen later, and consider the F-vector space $\mathcal{P}_D$ of polynomials on F^n of degree at most d. Then

$$\dim_F \mathcal{P}_D = \binom{n+D}{D} \asymp d^n.$$

Now let V_f be the subspace of polynomials P in $\mathcal{P}_D$ such that for every $v \in F^n$, P vanishes to order at least $f(v)$ at v (i.e. the multivariate Taylor expansion of P at v contains no non-zero terms of degree less than $f(v)$ in the coordinates $x - v$). The condition at each v imposes $O(f(v)^n)$ linear conditions on $\mathcal{P}_D$; thus, summing over v, we find that

$$\dim_F \mathcal{P}_D - \dim_F V_f \ll \sum_{v \in F^n} f(v)^n = \|f\|^n_{\ell^n(F^n)}.$$

In particular, if we choose D equal to a suitably large multiple of $\|f\|_{\ell^n(F^n)}$, the dimension of V_f is positive, so we can choose a non-zero P in V_f.

Let x_n be the defining function of F^{n-1} in F^n. We can factor $P = x_n^j Q$ for some $j \geq 0$, where Q is a polynomial which does not contain x_n as a factor. Of course, Q also has degree at most d, and vanishes with degree at least $f(v)$ for any $v \in F^n \backslash F^{n-1}$.

Now let γ_j be one of the curves in Proposition 2.4. We claim that this curve is contained in the algebraic hypersurface $\{Q = 0\}$. We emphasize that we have the geometric, not the combinatorial notion of containment in mind; that is, we are asserting that the restriction of Q to γ_j is the zero function on the algebraic curve γ_j, not merely that it vanishes on every F-rational point of γ_j.

Suppose on the contrary that γ_j is not contained in the vanishing locus of Q. Then the algebraic set $\{v \in \gamma_j : Q(v) = 0\}$ would have dimension zero, and by Bezout's theorem (Lemma A.5) would have degree $O(d) = O(\|f\|_{\ell^n(F^n)})$. On the other hand, by construction this set contains v with multiplicity at least $f(v)$ for each $v \in \gamma_j(F) \backslash F^{n-1}$, thus

$$\sum_{v \in \gamma_j(F) \backslash F^{n-1}} f(v) \ll \|f\|_{\ell^n(F^n)}.$$

However, this contradicts (2.4) and the choice of λ, if K_0 is large enough, and the claim follows.

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

We have shown that the hypersurface $\{Q = 0\}$ contains γ_j for each $1 \leq j \leq J$, and in particular contains the points $w_1, \ldots, w_J$. Thus,

$$|\{w \in F^{n-1} : Q(w) = 0\}| \geq J.$$

On the other hand, by construction, Q restricts to a non-trivial polynomial on F^{n-1} of degree at most d. By Lemma A.3 we have

$$J \ll |F|^{n-2} D$$

and (2.8) follows by our choice of d. The proof of Proposition 2.4 and (thus Theorem 2.1) is now complete.

§3. *The general case.* We now prove Theorem 1.6.

Proof of Theorem 1.6. As in the statement of the theorem, all implied constants are allowed to depend on N, d, n. The case $n = 1$ is trivial (note that $|W(F)| = O(1)$ in this case), so we shall assume $n \geq 2$. We may also assume that $|F|$ is large compared with N, n, d, as the claim is trivial otherwise.

We begin with the simple observation that the projective case of Theorem 1.6 follows from the affine case by a random covering argument, as follows. Let $T : \mathbb{P}^N \to \mathbb{P}^N$ be a random projective transformation (with coefficients in F). Applying T to all the quantities in Theorem 1.6, restricting from projective space $\mathbb{P}^N$ to affine space $\mathbb{A}^N$ and then applying the affine case of that theorem, we see that

$$\left\| \sup_{T\gamma \ni Tw} \sum_{v \in T\gamma(F) \cap F^N} |f \circ T^{-1}(v)| \right\|_{\ell^n(TW(F) \cap F^N)} \ll |F|^{(n-1)/n} \|f \circ T^{-1}\|_{\ell^n(F^N)},$$

which we rearrange as

$$\left\| \sup_{\gamma \ni w} \sum_{v \in \gamma(F) \cap T^{-1}F^N} |f(v)| \right\|^n_{\ell^n(W(F) \cap T^{-1}F^N)} \ll |F|^{n-1} \|f\|^n_{\ell^n(T^{-1}F^N)}.$$

Taking expectations over all T, we conclude that the projective case of Theorem 1.6 does indeed follow from the affine case as claimed.

It remains to establish the case when $W \subset \mathbb{A}^N$ is an affine variety. For each irreducible curve γ in $\mathbb{A}^N$ of degree d, we can write

$$\sum_{v \in \gamma(F)} f(v) = \sum_{v \in \gamma(F) \setminus W(F)} f(v) + \sum_{v \in \gamma(F) \cap W(F)} f(v).$$

To control the latter sum, observe from Bezout's theorem (Lemma A.5) that $\gamma(F) \cap W(F)$ has cardinality $O(1)$ (note that we assume γ does not lie in W), and thus

$$\sum_{v \in \gamma(F) \cap W(F)} f(v) \ll \|f\|_{\ell^n(F^N)}.$$

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

Applying Lemma A.3, we have $|W(F)| \ll |F|^{n-1}$ and so we see that the contribution of this term to is negligible.

It remains to show that

$$\left\| \sup_{\gamma \ni w} \sum_{v \in \gamma(F) \backslash W(F)} |f(v)| \right\|_{\ell^n(W(F))} \leq C_{N,d,n} |F|^{(n-1)/n} \|f\|_{\ell^n(F^N)}.$$

Clearly we may now drop the assumption that γ is not contained in W.

By Lemma A.4 we may write

$$W = \{v \in \mathbb{A}^N : P_1(v) = \cdots = P_K(v) = 0\}$$

for $O(1)$ polynomials $P_1, \ldots, P_K$ on $\mathbb{A}^N$ of degree $O(1)$, such that each locus $\{P_k = 0\}$ is a hypersurface containing W. It will suffice to show for each k that

$$\left\| \sup_{\gamma \ni w} \sum_{v \in \gamma(F) \backslash \{P_k = 0\}} |f(v)| \right\|_{\ell^n(W(F))} \ll |F|^{(n-1)/n} \|f\|_{\ell^n(F^N)}$$

since the desired claim then follows from the triangle inequality.

Next, we can reduce to the case when P_k is the vertical coordinate function x_N. Indeed, given any P_k, we can realize W, γ as subvarieties of $\mathbb{A}^{N+1}$ by composing the given inclusion in $\mathbb{A}^N$ with the "graphing" map $\mathbb{A}^N \to \mathbb{A}^{N+1}$ defined by $x \mapsto (x, P_k(x))$. Since P_k has degree $O(1)$, it is clear that the images of W, γ in $\mathbb{A}^{N+1}$ are again varieties of degree $O(1)$. Incrementing N by 1, we may now assume that $W \subset \mathbb{A}^{N-1}$.

It thus suffices to show that

$$\|g\|_{\ell^n(W(F))} \ll |F|^{(n-1)/n} \|f\|_{\ell^n(F^N)} \tag{3.1}$$

where W is contained in $\mathbb{A}^{N-1}$, and $g : W(F) \to \mathbf{R}^+$ is the function

$$g(w) := \sup_{\gamma \ni w} \sum_{v \in \gamma(F) \backslash F^{N-1}} |f(v)|. \tag{3.2}$$

We now apply another random projection trick; the idea is to "flatten" the $(n-1)$-dimensional variety W by a linear projection $F^{N-1} \to F^{n-1}$, thus returning us to the situation of the previous section. The main point is that a sufficiently generic projection from $W(F)$ to F^{n-1} will have, in a sense, bounded fibers on average.

Let $T : F^{N-1} \to F^{n-1}$ be a random surjective linear map; we extend this map (by abuse of notation) to the linear map $T : F^N \to F^n$ by defining $T(w, v_N) := (Tw, v_N)$ for $w \in F^{N-1}$ and $v_N \in F$. We introduce the functions $f_T : F^n \to \mathbf{R}^+$ and $g_T : F^{n-1} \to \mathbf{R}^+$ by the formulae

$$f_T(x) := \left(\sum_{v \in F^N : T(v) = x} |f(v)|^n \right)^{1/n} \tag{3.3}$$

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

and

$$g_T(y) := \sup_{w \in W(F): T(w)=y} g(w) \tag{3.4}$$

for all $y \in F^{n-1}$ and $x \in F^n$, with the convention that the supremum over w in (3.4) is zero if no w of the required form exist.

LEMMA 3.1. *For all T, we have*

$$\|g_T\|_{\ell^n(F^{n-1})} \ll |F|^{(n-1)/n} \|f_T\|_{\ell^n(F^n)} \tag{3.5}$$

for all T.

Proof. In view of Theorem 2.1, it suffices to establish the pointwise estimate

$$g_T(y) \ll f_T^*(y)$$

for all $y \in F^{n-1}$, where the degree d appearing in the definition of f_T^* is $O(1)$.

Fix y. We may of course assume that g_T is non-zero, which implies by (3.4) that there exists $w \in W(F)$ with $T(w) = y$ and an irreducible curve γ in $\mathbb{A}^N$ passing through w of degree at most d, such that

$$\sum_{v \in \gamma(F) \setminus F^{N-1}} |f(v)| = g_T(y).$$

Since g_T is non-zero, we see that $\gamma(F)$ is not contained in F^{N-1}. Since γ contains $w \in F^{N-1}$, we see that the image of $\gamma(F)$ in F^n contains at least two distinct points; in particular, it is not constant. It follows from Bezout's theorem (Lemma A.5) that

$$|\gamma \cap T^{-1}(y')| \ll 1$$

for any $y' \in F^n$. From this and (3.3) we see that

$$\sum_{v \in \gamma(F) \setminus F^{N-1}} |f(v)| \ll \sum_{x \in T(\gamma(F)) \setminus F^{n-1}} |f_T(x)|.$$

By Lemma A.6, $T(\gamma(F))$ is contained in an irreducible algebraic curve in $\mathbb{A}^n$ of degree $O(1)$; this curve passes through y, and the claim follows.

We raise (3.5) to the nth power and take expectations to conclude

$$\mathbb{E}\|g_T\|^n_{\ell^n(F^{n-1})} \ll |F|^{n-1} \mathbb{E}\|f_T\|^n_{\ell^n(F^n)}.$$

By construction, $\|f_T\|_{\ell^n(F^n)} = \|f\|_{\ell^n(F^N)}$, and so to show (3.1) we only need to show that

$$\|g\|^n_{\ell^n(W(F))} \ll \mathbb{E}\|g_T\|^n_{\ell^n(F^{n-1})}.$$

By using distributional formulae such as (2.2) and linearity of expectation, it suffices to show that

$$|\{w \in W(F) : g(w) \geq \lambda\}| \ll \mathbb{E}|\{y \in F^{n-1} : g_T(y) \geq \lambda\}|$$

for each $\lambda > 0$.

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

Fix λ. If we denote the set on the left-hand side as Ω, then the set on the right-hand side is $T(\Omega)$. It thus suffices to show that $|T(\Omega)| \gg |\Omega|$ with probability p for some $p \gg 1$. From the Cauchy–Schwarz inequality we have

$$|\{(w, w') \in \Omega \times \Omega : T(w) = T(w')\}| \gg \frac{|\Omega|^2}{|T(\Omega)|}$$

and so it suffices by Markov's inequality to show that

$$\mathbb{E}|\{(w, w') \in \Omega \times \Omega : T(w) = T(w')\}| \ll |\Omega|.$$

The contribution of the diagonal case $w = w'$ is clearly acceptable, so we may impose the condition $w \neq w'$. However, for any $w \neq w'$, the probability that $T(w) = T(w')$ is just the probability that $w - w'$ is in the kernel of T, which is $O(|F|^{1-n})$. So, by linearity of expectation, the contribution of the non-diagonal pairs (w, w') is $O(|\Omega|^2|F|^{1-n})$, which is acceptable since $|W(F)| \ll F^{n-1}$. The proof of Theorem 1.6 is complete. □

Remark 3.2. One can also apply Dvir's polynomial method directly to the algebraic variety W without performing the flattening trick. This suffices to establish results such as Corollary 1.10 when the number J of curves is large (e.g. $J \asymp |F|^{n-1}$), but does not seem to give optimal results when J is small. In case $W = \mathbb{A}^{n-1}$, we made critical use of the large automorphism group of W in Proposition 2.5 in order to reduce the small J case to the large J case by superimposing many translations of f by random elements of $\mathrm{Aut}(W)$. When W is a more general variety, its automorphism group is typically trivial, and we do not know of any substitute for the method of Proposition 2.5.

We remark that this is not so different from Lemma A.3. In general, the estimation of the number of F-rational points on a variety W over F is a very difficult problem, requiring some knowledge of the cohomology of W with its Frobenius action. However, in cases where W has a large automorphism group—for instance, when W is a homogeneous space, or in particular affine space—it can be quite easy to compute $W(F)$ exactly. So if we are content to compute $W(F)$ up to a multiplicative constant, as in Lemma A.3, we need only flatten W down to affine space and do our combinatorics on the latter, much simpler variety.

§4. *Variants.* We now consider some variants and generalizations of the above results. We will not always strive for maximal generality here, instead giving a sample of possible directions in which the above methods can be pushed. As a consequence, some details will be omitted in the discussion.

4.1. *Reducibility.* In Theorem 1.6, W was assumed to be a variety, and thus irreducible. However, one can clearly generalize to the case when W is the union of a bounded number of varieties of bounded degree, with the irreducible components of W having dimension $n - 1$.

One cannot, of course, relax the requirement that the curve γ be irreducible. If we did so, reducible curves of the form $\gamma \cup \gamma_0$ for each $w \in W(F)$, where γ

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

goes through w and γ_0 is a fixed curve independent of w on which f is large, would easily contradict (1.3).

4.2. *Restricted Kakeya maximal functions.* As we saw in Remark 1.8, the condition that each curve γ is not contained in W is an ingredient necessary to obtain the full range of estimates. By examining the argument in §3, one sees that if this non-degeneracy condition is further strengthened then we can slightly relax the condition that W is an algebraic set while preserving the full range of estimates.

THEOREM 4.3. *Let $N, d, n \geq 1$, let F be a finite field, let $V = \mathbb{P}^N$ (respectively $V = \mathbb{A}^N$), let $U \subset V$ be a projective (respectively affine) variety of any dimension and of degree at most d, and let W be any subset of $U(F)$. Then for any $f : V(F) \to \mathbf{R}$ we have*

$$\left\| \sup_{\gamma \ni w} \sum_{v \in \gamma(F)} |f(v)| \right\|_{\ell^n(W)} \leq C_{N,d,n} \max(|W|, |F|^{n-1})^{1/n} \|f\|_{\ell^n(V(F))}. \quad (4.1)$$

Here, w ranges over W, and for each $w \in W$, the range of the supremum is the set of all irreducible projective (respectively affine) algebraic curves γ in V of degree at most d, which contain w but are not contained in U. The constant $C_{N,d,n} > 0$ depends only on N, d, n.

4.4. *Nikodym sets and maximal functions.* It is well known (see e.g. [**16**]) that Kakeya-type estimates imply "Nikodym-type" analogues, in which the $(n-1)$-dimensional variety W is replaced by the n-dimensional variety V. For instance, we have the following analogue of Theorem 1.1, first observed in [**10**].

THEOREM 4.5 (Nikodym set conjecture for F^n). *Let $n \geq 1$, let F be a finite field, and let $E \subset F^n$ be a subset of F^n such that for every $x \in F^n \backslash E$, there exists a line γ passing through x such that $\gamma \backslash \{x\} \subset E$. Then $|E| \gg |F|^n$.*

To see the connection with Theorem 1.1, note that after applying a projective transformation to a set E of the form in Theorem 4.5, one gets something very close to a set E of the form in Theorem 1.1. The same projective transformation trick allows us to deduce the following maximal function estimate from Theorem 1.3.

THEOREM 4.6 (Nikodym maximal conjecture for F^n). *Let $n \geq 1$, let F be a finite field, and let $f : F^n \to \mathbf{R}$ be a function. Then*

$$\left\| \sup_{\gamma \ni x} \sum_{x' \in \gamma} |f(x')| \right\|_{\ell^n(F^n)} \ll |F| \|f\|_{\ell^n(F^n)}$$

where the implied constant depends on n, and γ ranges over lines through x.

The deduction of Theorem 4.6 from Theorem 1.3 was established in the Euclidean case in [**16**]; the proof for finite fields is identical and is omitted.

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

Alternatively, one can deduce Theorem 4.6 from Theorem 2.1 (or Theorem 1.6), which implies in particular that

$$\Big\| \sup_{\gamma \ni x} \sum_{x' \in \gamma \setminus W} |f(x')| \Big\|_{\ell^n(W)}^n \ll |F|^{n-1} \|f\|_{\ell^n(F^n)}^n$$

for all hyperplanes W in F^n. Averaging this over all W (cf. the Calderón–Zygmund method of rotations [4]) yields the claim. The same argument also yields the following Nikodym-type variant of Theorem 2.1.

THEOREM 4.7 (Nikodym maximal conjecture for curves in F^n). *Let d, $n \geq 1$. For any $f : F^n \to \mathbf{R}$, we have*

$$\Big\| \sup_{\gamma \ni x} \sum_{x' \in \gamma(F)} |f(x')| \Big\|_{\ell^n(F^n)} \ll |F| \|f\|_{\ell^n(F^n)},$$

where the supremum is over all irreducible algebraic curves γ in F^n of degree at most d that pass through x, and the implied constant depends on both n and d.

One can also establish this theorem directly by repeating the arguments in §2 with some minor changes (for instance, it is no longer necessary to factor out all factors of x_n from the polynomial P); we leave the details as an exercise for the interested reader.

The following is a Nikodym-type variant of Theorem 1.6. Since, in the Nikodym problem, there is no longer a natural non-degeneracy condition for the curves γ, the requirement that W is an algebraic set may be dropped entirely.

THEOREM 4.8 (Nikodym maximal conjecture for subsets of $\mathbb{P}^N(F)$). *Let N, d, $n \geq 1$, let F be a finite field, and let W be any subset of $\mathbb{P}^N(F)$. Then for any $f : \mathbb{P}^N(F) \to \mathbf{R}$ we have*

$$\Big\| \sup_{\gamma \ni v} \sum_{v' \in \gamma(F)} |f(v')| \Big\|_{\ell^n(W)} \ll \max(|W|, |F|^n)^{1/n} \|f\|_{\ell^n(\mathbb{P}^N(F))},$$

where for each $v \in W$, the supremum is over all irreducible projective (respectively affine) algebraic curves γ of degree at most d in $\mathbb{P}^N(F)$ that pass through v, and the implied constants depend on N, d, n.

To deduce this from Theorem 4.7, it is necessary to slightly modify the arguments in §3. First, the random surjective linear map $T : F^{N-1} \to F^{n-1}$ is replaced by a random surjective linear map $T : F^N \to F^n$. We are then no longer able to guarantee, in Lemma 3.1, that the image under T of each relevant curve $\gamma(F)$ contains at least two points. To remedy this, we define a function $h_T(y)$ identically to $g(y)$ except excluding in each sup the curves γ mapped to only one point by T. Redefining $g_T(y) = \sup_{w \in W : T(w) = y} h_T(w)$, we prove the lemma with the new g_T. Setting $\Omega_T = \{y \in \Omega : h_T(y) = g(y)\}$ one observes that with probability greater than or equal to 0.6 we have $|\Omega_T| \gg |\Omega|$ (here we must delete from Ω the points corresponding to curves with $|\gamma(F)| = 1$, but these

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

have negligible contribution to the final estimate as before). Since $|\{(w, w') \in \Omega_T \times \Omega_T : T(w) = T(w')\}| \ll |\Omega| \max(1, |W|/|F|^n)$ with probability greater than or equal to 0.6, we conclude that $|T(\Omega_T)| \gg |\Omega| \min(1, |F|^n/|W|)$ with probability greater than or equal to 0.2.

4.9. *Kakeya for blowups.* The methods of this paper also apply to the case where our Kakeya maximal function is defined not on the set of points $W(F)$ but on the set of *tangent directions* to points of $W(F)$, so that our supremum is not over all curves passing through a particular point w but rather over all curves tangent at w to a given line through w.

For simplicity, take $W \subset V = \mathbb{P}^N$ to be a smooth projective variety of dimension $n - k$, and let E be a rank k subbundle of the projectivized normal bundle $\mathbb{P}N_V W := \mathbb{P}(TV|_W/TW)$ of W in V. We can think of E as a way of specifying, for each point w of W, a k-dimensional subspace of the $(N - n + k)$-dimensional space of tangent vectors at w which are normal to W. (We also require that these subspaces "vary algebraically" with w.)

Then the *blowup* of V along W is a variety $\tilde{V}$ endowed with a map $\pi : \tilde{V} \to V$ which is an isomorphism away from $\tilde{W} := \pi^{-1}(W)$. Moreover, $\tilde{W}$ has dimension $N - 1$ and is naturally identified with $\mathbb{P}N_V(W)$. In particular, E determines a closed subvariety of $\tilde{W}$ of dimension $n - 1$. For the basic facts about blowups used here, see [**8**, §II.7].

If $\gamma \subset V$ is an irreducible curve not contained in W, the preimage $\pi^{-1}(\gamma)$ is a union of some number of copies of $\tilde{W}$ with an irreducible curve $\tilde{\gamma} \subset \tilde{V}$, called the *strict transform* of γ. If $w \in \gamma \cap W$, then the lifted point $\tilde{w} \in \tilde{\gamma} \cap \tilde{W}$ is essentially the tangent vector $\gamma'(w) \in T_w V$ of γ at w, projected onto $\mathbb{P}N_V(W) \equiv \tilde{W}$ by the obvious map from $TV|_W$ to $\mathbb{P}N_V(W)$.

The variety $\tilde{V}$ can be embedded in some large projective space $\mathbb{P}^M$ in such a way that the strict transform of a curve of degree $O(1)$ again has degree $O(1)$. (It suffices to observe that there is a very ample line bundle on $\tilde{V}$ of degree $O(1)$; this follows, for instance, from the explicit construction of a very ample line bundle in [**8**, Proposition II.7.10].)

If e is a point of E, we say that a curve γ passes through e if its strict transform in $\tilde{V}$ passes through e, interpreted as a point of $\mathbb{P}^M$. Without reference to the blowup, we can think of e as a tangent direction to some point w of W, and to say γ passes through e is to say it passes through w along the given tangent direction.

Applying Theorem 1.6 to the pair $(\mathbb{P}^M, E)$, we obtain the following high-codimension variant.

THEOREM 4.10 (Kakeya maximal conjecture for algebraic varieties over F, blowup version). *Let $N, d, n, k \geq 1$, let F be a finite field, let $W \subset \mathbb{P}^N$ be a smooth projective variety of dimension $n - k$ and degree at most d, and let E be a rank k subbundle of the normal bundle of W in $\mathbb{P}^N$. Then for any $f : V \to \mathbf{R}$ we have*

$$\left\| \sup_{\gamma // e} \sum_{v \in \gamma(F)} |f(v)| \right\|_{\ell^n(E(F))} \ll |F|^{(n-1)/n} \|f\|_{\ell^n(V(F))},$$

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

where for each $e \in E(F)$ with base point $w \in W(F)$, the supremum is over all irreducible projective algebraic curves γ in V of degree at most d in $\mathbb{P}^N$ that pass through w with projective tangent vector e but are not contained in W, and the implied constants depend only on N, d, n, k.

There is of course an obvious affine counterpart to this theorem, in which all projective varieties are replaced by affine ones; we omit the details.

Example 4.11. If γ is a non-degenerate affine conic

$$ax^2 + bxy + cy^2 + dx + ey + g = 0$$

and ℓ is a line defined by the vanishing of some linear form $mx + ny - p$ (which we also denote by ℓ) we say γ has ℓ as an asymptote if γ can be written

$$\ell\ell' + D = 0$$

for some other linear form ℓ' and some constant D. If ω is a point on the line at infinity—that is, a direction in $\mathbb{A}^2$—then γ has an asymptote in direction ω precisely when γ intersects the line at infinity at ω.

Let f be a function $\mathbb{P}^2(F) \to \mathbf{R}$. For each conic γ we define

$$F(\gamma) = \sum_{v \in \gamma(F)} |f(v)|.$$

Then we can define a function f^* on the space of directions in $\mathbb{A}^2$ by setting $f^*(\omega)$ to be the supremum of $F(\gamma)$ as γ ranges over the space of conics with an asymptote in direction ω. Thus, the norm of f^* is controlled by Theorem 1.6 applied with $V = \mathbb{P}^2$ and W the line at infinity.

Now let W be the point $[0 : 1 : 0]$ on the line at infinity, corresponding to the horizontal direction. Applying Theorem 1.6 directly yields the trivial inequality

$$|f^*(\omega)| < C\|f\|_{\ell^1}.$$

We can define a more interesting maximal operator using the blowup formalism of this section, as follows. Let f^* be a function on the space of horizontal lines ℓ, defined by setting $f^*(\ell)$ to be the supremum of $F(\gamma)$ as γ ranges over the space of conics having ℓ as asymptote. The horizontal lines in $\mathbb{A}^2$ are in bijection with the directions through the point $[0 : 1 : 0]$ in $\mathbb{P}^2$, apart from the direction of the line at infinity, and the condition that γ has ℓ as asymptote implies that the projective closure of γ passes through $[0 : 1 : 0]$ with tangent direction corresponding to ℓ. Now applying Theorem 4.10 with $V = \mathbb{P}^2$ and $W = [0 : 1 : 0]$ yields an upper bound on the norm of f^*.

4.12. *Higher-dimensional averages.* In the preceding discussion, all averages were over one-dimensional curves γ. It is natural to ask what happens if we instead average over k-dimensional subvarieties π for some $k > 1$. To simplify the discussion we focus on one concrete case, that of the *k-plane maximal operator* $T_{n,k}$ for fixed $1 \le k \le n$, which maps functions $f : F^n \to \mathbf{R}$ to

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

functions $T_{n,k} : \mathrm{Gr}(F^n, k) \to \mathbf{R}^+$ defined on the Grassmannian of k-dimensional subspaces π of F^n, and is defined by the formula

$$T_{n,k} f(\pi) := \sup_{a \in F^n} \sum_{v \in \pi + a} |f(v)|.$$

CONJECTURE 4.13 (k-plane maximal operator estimate in finite fields). *For any $n, k \geq 1$ and $f : F^n \to \mathbf{R}$, we have*

$$\| T_{n,k} f \|_{\ell^q(\mathrm{Gr}(F^n,k))} \ll |\mathrm{Gr}(F^n, k)|^{1/q} \| f \|_{\ell^p(F^n)}$$

whenever $1 \leq p \leq n/k$ and $q \leq (n-k)(p/(p-1))$; the implied constant can depend on n and k.

Remark 4.14. Note that the $k = 1$ case of this inequality is just (1.2). The various exponents here are sharp, as can be seen by testing f equal to the indicator function of a point, a k-plane, or all of F^n. For the best known prior progress towards this result, see [3].

Although not able to verify the conjecture above, we prove a related estimate where the ℓ^q norm is replaced by a certain normalized mixed norm, defined as follows. For any $1 \leq k \leq n$, any n-dimensional vector space V and any exponents $q_1, \ldots, q_k$, we define the norm $\| \cdot \|_{\tilde{\ell}^{q_1,\ldots,q_k}(\mathrm{Gr}(V,k))}$ for $k = 1$ by the formula

$$\| h \|_{\tilde{\ell}^{q_1}(\mathrm{Gr}(V,1))} = \left(\frac{1}{|\mathrm{Gr}(V,\ 1)|} \sum_{\pi \in \mathrm{Gr}(V,1)} |h(\pi)|^{q_1} \right)^{1/q_1}$$

and then recursively for $k > 1$ by the formula

$$\| g \|_{\tilde{\ell}^{q_1,\ldots,q_k}(\mathrm{Gr}(V,k))} = \left(\frac{1}{|\mathrm{Gr}(V,\ 1)|} \sum_{\pi \in \mathrm{Gr}(V,1)} \| g(\pi + \cdot) \|^{q_1}_{\tilde{\ell}^{q_2,\ldots,q_k}(\mathrm{Gr}(\pi^c,k-1))} \right)^{1/q_1},$$

where for every subspace of π of V, we arbitrarily pick a complementary subspace π^c (thus $\pi^c + \pi = V$ and $\pi^c \cap \pi = \{0\}$). If any $q_i = \infty$ above, the corresponding sum is replaced by a supremum in the usual way.

Using an iteration method of Bourgain's [2] and the bound (1.1), we now obtain the following theorem.

THEOREM 4.15. *For any $n, k \geq 1$ and $f : F^n \to \mathbf{R}$, we have*

$$\| T_{n,k} f \|_{\tilde{\ell}^{q_1,\ldots,q_k}(\mathrm{Gr}(F^n,k))} \ll \| f \|_{\ell^{n/k}(F^n)}$$

with $q_i = ((n-i)(n-i+1))/(n-k)$; the implied constant can depend on n and k.

Since $(1/k)(1/q_1 + \cdots + 1/q_k) = 1/n$, one would like to switch the order of the mixed norm and interpolate to deduce Conjecture 4.13 from the theorem above; this is unfortunately not possible because the exponents q_i are in decreasing order.

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

Proof of Theorem 4.15. For $k = 1$ the bound is identical to (1.1). Suppose that the bound holds for $k-1$ and all n, and that $\pi \in \mathrm{Gr}(F^n, k-1)$, and $\xi \in \mathrm{Gr}(\pi^c, 1)$. Note that

$$T_{n,k} f(\xi + \pi) \leq T_{n-k+1,1}\left(\sum_{x \in \pi} |f(x + \cdot)|\right)(\xi).$$

Applying (1.1) to the function $g_\pi(y) = \sum_{x \in \pi} |f(x+y)|$ defined on π_c, we obtain

$$\|T_{n,k} f\|_{\tilde{\ell}^{r_1,\ldots,r_{k-1},n-k+1}(\mathrm{Gr}(F^n,k))} \ll \|\|g_\pi\|_{\ell^{n-k+1}(\pi^c)}\|_{\tilde{\ell}^{r_1,\ldots,r_{k-1}}(\mathrm{Gr}(F^n,k-1))} \tag{4.2}$$

for any exponents $r_1, \ldots, r_{k-1}$ where, on the right side above, π is variable summation in the outer norm. Interpolating† the hypothesized bound

$$\|\|g_\pi\|_{\ell^\infty(\pi^c)}\|_{\tilde{\ell}^{(n(n-1))/(n-k+1),\ldots,n-k+2}(\mathrm{Gr}(F^n,k-1))} \ll \|f\|_{\ell^{n/(k-1)}(F^n)}$$

with the trivial bound

$$\|\|g_\pi\|_{\ell^1(\pi^c)}\|_{\tilde{\ell}^{\infty,\ldots,\infty}(\mathrm{Gr}(F^n,k-1))} \ll \|f\|_{\ell^1(F^n)}$$

we see that the right side of (4.2) is bounded up to constants by $\|f\|_{\ell^{n/k}(F^n)}$ provided that each $r_i = (n-i)(n-i+1)/(n-k)$. □

The situation is more satisfactory if we restrict our attention to the analogue of the Kakeya set conjecture. We say a subset $E \subset F^n$ is a *k-plane Kakeya set* if it contains a k-plane parallel to any given k-plane. (Such sets are also called *(n,k)-sets.*) Of course, a k-plane Kakeya set is also a Kakeya set in the usual sense, so one has $|E| > c_n |F|^n$ by Theorem 1.1. However, the k-plane Kakeya condition in fact implies a much better lower bound on $|E|$ when $k > 1$.

PROPOSITION 4.16. *Let n, k be integers with $2 \leq k < n$. Let E be a subset of F^n which contains a k-plane in every direction, and let $q = |F|$. Then*

$$|E| \geq q^n (1 - q^{1-k})^{\binom{n}{2}}.$$

for all q sufficiently large relative to n.

Proof. We use the method of Dvir together with the "method of multiplicities", as in the proof of Proposition 2.5. Let m be a positive integer and let $\mathcal{P}_{mq-1}$ be the space of polynomials in $x_1, \ldots, x_n$ of degree at most $mq-1$. Then

$$\dim_F \mathcal{P}_{mq-1} = \binom{mq+n-1}{n}.$$

We want to find a non-zero polynomial P in $\mathcal{P}_{mq-1}$ such that P vanishes to order m at each point of E. The vanishing conditions at each point impose $\binom{m+n-1}{n}$ linear conditions on $\mathcal{P}_{mq-1}$, so we can choose such a P as long as

$$\binom{mq+n-1}{n} > \binom{m+n-1}{n}|E|. \tag{4.3}$$

† One can for instance use the complex interpolation method here, which works perfectly well in the mixed-norm setting, see e.g. [1].

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

Now let X be a k-plane contained in E. Then P vanishes to degree m on each point of X, and thus must vanish identically on X thanks to the following lemma, a variant of the Schwarz–Zippel lemma.

LEMMA 4.17. *Let Q be a polynomial on F^k of degree less than mq which vanishes to order m at each point of F^k. Then $Q = 0$.*

Proof. The statement is clear when $k = 1$. Then proceed by induction; if k is the smallest integer where the lemma does not hold, then Q must restrict to 0 on each of the $(q^{k+1} - q)/(q - 1)$ F-rational hyperplanes in F^k. Write Π for the product of all the F-rational linear forms on F^k. Then we can write

$$Q = Q_0 \Pi^M$$

for some $M > 0$, and some Q_0 not a multiple of Π. Now Π vanishes at each point of F^k to order $(q^k - 1)/(q - 1)$, and the degree of Π is $(q^{k+1} - q)/(q - 1)$. Thus Q_0 vanishes at each point to order $m_0 = m - M(q^k - 1)/(q - 1)$ and has degree less than $mq - M(q^{k+1} - q)/(q - 1) = m_0 q$. However, Q_0 is not a multiple of Π, so Q_0 restricts to a non-zero polynomial on some F-rational hyperplane, which contradicts the induction hypothesis. □

Let $\bar{P}$ be the leading term of P, a homogeneous polynomial of degree at most $mq - 1$. Since P vanishes identically on a k-plane in every direction, $\bar{P}$ must vanish identically on every (projective) $(k - 1)$-plane in $\mathbb{P}^{n-1}(F)$. The following lemma now bounds $\deg P$ from below.

LEMMA 4.18. *Let Q be a non-zero homogeneous polynomial in n variables which restricts to 0 on every F-rational $(k - 1)$-plane on $\mathbb{P}^{n-1}$. Then* $\deg Q \geq (q^{k+1} - 1)/(q - 1)$.

Proof. Choose a homogeneous form Q, and let k be the smallest integer such that Q restricts to 0 on every F-rational $(k - 1)$-plane. Let X be an F-rational k-plane on which Q does not vanish. Then the restriction of Q to X is a homogeneous form in $k + 1$ variables which is a multiple of $(q^{k+1} - 1)/(q - 1)$ distinct linear forms; thus Q must have degree at least $(q^{k+1} - 1)/(q - 1)$. The statement in the lemma follows, since $(q^{k+1} - 1)/(q - 1)$ increases with k. □

To sum up, we have proven that the inequality (4.3) can hold only when

$$mq - 1 \geq (q^{k+1} - 1)/(q - 1).$$

We note that the negation of this condition forces $m = 1$ when $k = 1$; but for larger k it allows substantially more freedom in m. In particular, we can take $m = q^{k-1}$ and conclude that

$$|E| \geq \binom{q^k + n - 1}{n} \binom{q^{k-1} + n - 1}{n}^{-1}$$

and one easily verifies that the latter quantity is bounded below by $q^n(1 - q^{1-k})^{\binom{n}{2}}$ once q is large relative to n. □

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

Remark 4.19. Suppose that $1 < k < n$. Then, by [13, Theorem 2], F^{n-k+1} contains a Kakeya set of size $2^{-n+k}q^{n-k+1} + O(q^{n-k})$. Embedding this Kakeya set in F^n, and then also adding the set $F^n \setminus F^{n-k+1}$, we obtain a k-plane Kakeya set of size $q^n(1 - (1 - 2^{-n+k})q^{1-k} + O(q^{-k}))$. Comparing this with the upper bound of $q^n(1 - \binom{n}{2}q^{1-k} + O(q^{-k}))$ from Proposition 4.16, we see that the latter is nearly sharp, missing at most by a constant in the q^{1-k} term.

4.20. *Kakeya problems over more general rings.* The analogy between Kakeya problems over $\mathbf{R}$ and their finite-field analogues is deficient in the very important respect that the latter do not admit multiple scales. That is, there is no natural notion of "distance" in F^n more refined than the trivial distance, in which any two distinct points are separated by distance 1.

The problem of multiple scales interferes with any attempt to mimic the proofs of finite-field results in the Euclidean setting, and indeed, some facts which hold over finite fields are not true over $\mathbf{R}$. For instance, the construction of Besicovitch sets depends crucially on the existence of multiple scales, and as a result they have no analogue over finite fields; Dvir's theorem shows that a subset of F^n containing a line in every direction has measure bounded below by an absolute constant (where measure is normalized so that F^n has measure 1).

It is thus an interesting problem to reintroduce multiple scales in an algebraic setting. One might, for instance, ask about Kakeya problems over the finite Artinian rings $F[x]/x^k$ or $\mathbf{Z}/p^k\mathbf{Z}$. These rings have precisely k scales, rather than the infinite scales available in $\mathbf{R}$; so they should stand as a good "baby case" for understanding the role played by the interplay between different scales in Kakeya problems. Better still would be to use results on the finite rings above to derive results in the limit rings $F[[x]]$ and $\mathbf{Z}_p$, which are closer still to $\mathbf{R}$.

Let R be the ring $F[x]/x^k$, and let $\mathfrak{m} = (x)$ be the maximal ideal of R. By a line in R^n we mean a subset of R^n of the form $a + bR$, with $a \in R^n$ and $b \in \mathbf{R}^n - \mathfrak{m}^n$. The line determines b up to scalar multiplication by the group of units $R^* = R - \mathfrak{m}$; so by the *direction* of a line we mean an element of $(R^n - \mathfrak{m}^n)/R^* = \mathbb{P}^{n-1}(R)$.

Dvir's theorem almost immediately implies a lower bound on the size of Kakeya sets in R^n.

PROPOSITION 4.21. *Let R be the ring $F[x]/x^k$, and let $E \subset R^n$ be a subset containing a line in every direction. Then*

$$|E| \geq c^{nk}|R|^n$$

for some c in $(0, 1)$.

Proof. Choose an isomorphism $\phi : R^n \to F^{nk}$ of F-vector spaces. Then ϕ carries multiplication by x to an endomorphism X of F^{nk} satisfying $X^k = 0$.

Let ω be a direction in $\mathbb{P}^{nk-1}(F)$, and let v be a point of F^{nk} lying over ω. Let v_0 be an element of $R^n - \mathfrak{m}^n$ such that $\phi^{-1}(v) \in Rv_0$. (If v does not lie in the image of X, we can take v_0 to be $\phi^{-1}(v)$ itself.)

By hypothesis, there is some $x \in R^n$ such that $x + Rv_0 \subset E$. However, applying ϕ, this certainly implies that $\phi(x) + Fv \subset \phi(E)$. So $\phi(E)$ is a Kakeya

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

set, and we conclude [6, 13] that

$$|E| = |\phi(E)| < c^{nk}|F|^{nk}$$

for some $c \in (0, 1)$ (which in fact can be taken to be slightly larger than $1/2$ as in [6]). □

Proposition 4.21 shows that, when k is held fixed and F varies, the analogue of the Kakeya conjecture holds for $R = F[x]/x^k$. However, when F is fixed and k grows, the situation is different. The natural analogue of Minkowski dimension for a subset E of R^n is

$$\log|E|/\log|R|.$$

So the bound supplied by Proposition 4.21 shows only that the Minkowski dimension is bounded below by $1 + \log c/\log|F|$. This gives the desired lower bound of 1 only when $|F|$ is allowed to grow.

This leads us to several natural questions.

- Can the lower bound in Proposition 4.21 be improved to something of the form
$$|E| \geq c_n|R|^n?$$
More modestly, is there a bound
$$|E| \geq c_{n,\varepsilon}|R|^{n-\varepsilon}$$
for any $\varepsilon > 0$?
- Let E be a subset of $F[[x]]^n$ containing a line in every direction, and write E_k for the image of E under the projection $F[[x]]^n \to (F[x]/x^k)^n$. Are there Besicovitch phenomena in $F[[x]]^n$? That is, is it possible that
$$\lim|E_k||F|^{-nk} = 0?$$
Of course, such a sequence of E_n would give a negative answer to the first question above.
- What can be said in the cases $R = \mathbf{Z}/p^k\mathbf{Z}$, or $R = \mathbf{Z}_p$? The simple argument of Proposition 4.21 does not work, since R^n is no longer an F-vector space. One might try identifying $Z/p^k\mathbf{Z}$ with $\mathbf{F}_p^k$ via the Witt construction [14, II.6].

Acknowledgements. The first author is partially supported by NSF-CAREER grant DMS-0448750 and a Sloan Research Fellowship. The third author is supported by a grant from the MacArthur Foundation, and by NSF grant DMS-0649473. We are indebted to the anonymous referee for useful comments and corrections.

A. *Appendix. Review of algebraic geometry.* We now quickly review some basic concepts and results in algebraic geometry which are relevant to this paper. All the material here is found in standard textbooks, e.g. [8].

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

Throughout this appendix, F is a fixed finite field, and $\overline{F}$ is its algebraic closure. For any $n \geq 1$, we define *affine space*

$$\mathbb{A}^n := \{(x_1, \ldots, x_n) : x_1, \ldots, x_n \in \overline{F}\}$$

and *projective space*

$$\mathbb{P}^n := \{[x_1, \ldots, x_{n+1}] : (x_1, \ldots, x_{n+1}) \in \mathbb{A}^{n+1} \backslash 0\}$$

where $[x_1, \ldots, x_{n+1}]$ is the equivalence class of $(x_1, \ldots, x_{n+1})$ modulo dilations. (More precisely, $\mathbb{A}^n$ and $\mathbb{P}^n$ are *schemes* whose $\overline{F}$-points are the sets given above; for the purpose of this paper, the distinction between a scheme and its set of $\overline{F}$-points can be safely ignored by non-experts.)

We can embed $\mathbb{A}^n$ in $\mathbb{P}^n$ by identifying $(x_1, \ldots, x_n)$ with $[x_1, \ldots, x_n, 1]$. We also define the set of F-points of $\mathbb{A}^n$ and of $\mathbb{P}^n$ by the formulae

$$\mathbb{A}^n(F) := F^n = \{(x_1, \ldots, x_n) : x_1, \ldots, x_n \in F\}$$

and

$$\mathbb{P}^n(F) := \mathbb{P}F^n = \{[x_1, \ldots, x_{n+1}] : (x_1, \ldots, x_{n+1}) \in F^{n+1} \backslash 0\}.$$

Definition A.1 (Varieties). A *projective algebraic set* (respectively *affine algebraic set*) is a subset V of a projective space $\mathbb{P}^N$ (respectively affine space $\mathbb{A}^N$) of the form

$$V = \{x \in \mathbb{P}^N : P_1(x) = \cdots = P_J(x) = 0\}$$

where $P_1, \ldots, P_J$ are homogeneous polynomials (respectively polynomials). A projective (respectively affine) algebraic set is called *irreducible* if it cannot be written as the union of two proper projective (respectively affine) algebraic subsets, in which case we refer to the algebraic set as a *variety*.

The *dimension* of an algebraic set V is the smallest integer d such that intersections of V with generic codimension-d subspaces of $\mathbb{P}^N$ or $\mathbb{A}^N$ are finite. If V is a projective variety of dimension d, then generic codimension-d subspaces of $\mathbb{P}^N$ intersect V in a constant number of points, known as the *degree* of V. Every affine variety can be embedded in a unique projective variety of the same dimension (the projective *closure* of the affine variety); we define the degree of the affine variety to be that of its projective closure.

Remark A.2. The definitions given here are classical in style, and thus subject to certain pathologies; for instance, one might expect the vanishing locus of a degree-d polynomial in 2 variables to be a curve of degree d, and this is generically the case: but if the polynomial is, for instance, $(x + y)^d$, then the vanishing locus is (according to our definition) a curve of degree one. Problems of this kind will change degrees at worst by bounded multiplicative constants, so we will systematically ignore them; in any event, all proofs in the paper work when the better-behaved scheme-theoretic definitions of dimension and degree are used.

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

Given a projective (respectively affine) algebraic set V, we define its set of *F-points* $V(F)$ to be the set $V(F) = V \cap \mathbb{P}^n(F)$ (respectively $V(F) = V \cap \mathbb{A}^n(F)$).

An *irreducible curve* is an algebraic variety of dimension one. A *hypersurface* in an algebraic variety V of degree n is a subvariety of V whose dimension is $n - 1$.

LEMMA A.3 (Size estimate). *Let $V \subset \mathbb{P}^N$ be a projective variety of dimension n and degree d. Then $|V(F)| \leq d(|F| + 1)^n$.*

We note that Lemma A.3 is essentially the same as the Schwarz–Zippel theorem.

Proof. The statement is clear for $n = 0$. We may thus suppose inductively that $n > 0$ and that V is not contained in any hyperplane of $\mathbb{P}^N$. Then consider a pencil of hyperplanes through some fixed subspace of $\mathbb{P}^N$ of dimension $N - 2$, and write $V_0, V_1, \ldots, V_{|F|+1}$ for the intersection of V with each of the hyperplanes in this pencil. Each of these is a projective variety (or union of varieties) of dimension $n - 1$ and degree d. By induction, $|V_j(F)| \leq d(|F| + 1)^{n-1}$ for all j, and the claim follows. □

LEMMA A.4 (Degree bounds complexity). *Let $V \subset \mathbb{A}^N$ be an affine variety of degree d. Then there exists a set of polynomials $P_1, \ldots, P_J$ in $\mathbb{A}^N$ with $1 \leq J \leq C_{N,d}$, with degree at most $C_{N,d}$, such that*

$$V = \{v \in \mathbb{A}^N : P_1(v) = \cdots = P_J(v) = 0\}.$$

Here $C_{N,d}$ is a constant depending only on N and d.

Proof. This is Corollary 6.11 of Kleiman's article [**9**] in SGA6. (In concrete terms, one may think of Kleiman's theorem as saying that the n-dimensional subvarieties of $\mathbb{A}^N$ of degree d fall into finitely many continuous families, on each one of which the invariants like "minimal number and degree of polynomials needed to cut out V" is controlled.) □

Our main algebro-geometric tool is Bezout's theorem.

LEMMA A.5 (Bezout's theorem). *If $\gamma \subset \mathbb{P}^N$ is an irreducible algebraic curve of degree d, and V is a projective or algebraic set of degree d' that does not contain γ, then $\gamma \cap V$ is a zero-dimensional algebraic variety of degree at most dd'; in particular, the cardinality of $\gamma(F) \cap V(F)$, counting multiplicity, is at most dd'.*

For details, including a precise definition of multiplicity, see [**8**, I.7].

LEMMA A.6 (Projection lemma). *Let $\gamma \subset \mathbb{A}^N$ be an irreducible affine curve of degree d, and let $T : \mathbb{A}^N \to \mathbb{A}^n$ be a linear map. Then $T(\gamma)$ is contained in an irreducible affine curve of degree at most d.*

Proof. First of all, we can write $\mathbb{A}^N = \mathbb{A}^{N-n} \times \mathbb{A}^n$ in such a way that T is projection onto the second factor. Then $\mathbb{A}^N$ is an open subvariety of $\mathbb{P}^{N-n} \times \mathbb{A}^n$,

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press

and T extends to a projection $\overline{T}$ from $\mathbb{P}^{N-n} \times \mathbb{A}^n$ to $\mathbb{A}^n$. Write $\overline{\gamma}$ for the closure of γ in $\mathbb{P}^{N-n} \times \mathbb{A}^n$; then $\overline{T}(\overline{\gamma})$ is a closed subvariety of $\mathbb{A}^n$, since $\overline{T}$ is a proper morphism. Now $T(\gamma)$ is an open dense subvariety of $\overline{T}(\gamma)$, so it is the complement of a finite set of points in an affine curve in $\mathbb{A}^n$.

Let P be a generic hyperplane in $\mathbb{A}^n$; in particular we choose P to avoid the finite set $\overline{T}(\overline{\gamma}) \backslash T(\gamma)$. Then

$$\overline{T}(\overline{\gamma}) \cap P = T(\gamma) \cap P = T(\gamma \cap T^{-1}(P)).$$

Since P does not contain $T(\gamma)$, we know that γ is not contained in the hyperplane $T^{-1}(P)$; so $\gamma \cap T^{-1}(P)$ is finite of degree at most d. This implies that $\overline{T}(\overline{\gamma})$ has degree at most d, as required. □

References

1. J. Bergh and J. Löfström, *Interpolation Spaces: An Introduction*, Springer (Berlin, 1976).
2. J. Bourgain, Besicovitch-type maximal operators and applications to Fourier analysis. *Geom. Funct. Anal.* **22** (1991), 147–187.
3. J. Bueti, An incidence bound for k-planes in F^n and a planar variant of the Kakeya maximal function. *Preprint*.
4. A. Calderón and A. Zygmund, On singular integrals. *Amer. J. Math.* **78** (1956), 289–309.
5. Z. Dvir, On the size of Kakeya sets in finite fields. *Preprint*.
6. Z. Dvir, S. Kopparty, S. Saraf and M. Sudan, Extensions to the method of multiplicities, with applications to Kakeya sets and mergers. *Preprint*.
7. Z. Dvir and A. Wigderson, Kakeya sets, new mergers, and old extractors. *Proceedings of the 49th Annual IEEE Symposium on Foundations of Computer Science*, IEEE Computer Society (2008).
8. R. Hartshorne, *Algebraic Geometry* (*Graduate Texts in Mathematics* **52**), Springer (New York, 1977).
9. S. L. Kleiman, Les théorèmes du finitude pour le foncteur de Picard. In *Théorie des intersections et théorème de Riemann–Roch (SGA6), expose XIII* (*Lecture Notes in Mathematics* **225**), Springer (Berlin, 1971), 616–666.
10. L. Li, On the size of Nikodym sets in finite fields. *Preprint*.
11. G. Mockenhaupt and T. Tao, Kakeya and restriction phenomena for finite fields. *Duke Math. J.* **121** (2004), 35–74.
12. G. Pisier, Factorization of operators through $L^{p,\infty}$ or $L^{p,1}$ and noncommutative generalizations. *Math. Ann.* **276** (1986), 105–136.
13. S. Saraf and M. Sudan, Improved lower bound on the size of Kakeya sets over finite fields. *Preprint*.
14. J. P. Serre, *Local Fields* (*Graduate Texts in Mathematics* **67**), Springer (New York, 1979).
15. E. Stein, Limits of sequences of operators. *Ann. of Math.* (2) **74** (1961), 140–170.
16. T. Tao, The Bochner–Riesz conjecture implies the Restriction conjecture. *Duke Math J.* **96** (1999), 363–376.
17. T. Wolff, Recent work connected with the Kakeya problem. In *Prospects in Mathematics (Princeton, NJ, 1996)*, American Mathematical Society (Providence, RI, 1999), 129–162.

Jordan S. Ellenberg,
Department of Mathematics,
University of Wisconsin,
Madison WI 53706,
U.S.A.
E-mail: ellenber@math.wisc.edu

Terence Tao,
UCLA Department of Mathematics,
Los Angeles, CA 90095-1555,
U.S.A.
E-mail: tao@math.ucla.edu

Richard Oberlin,
UCLA Department of Mathematics,
Los Angeles, CA 90095-1555,
U.S.A.
E-mail: oberlin@math.ucla.edu

https://doi.org/10.1112/S0025579309000400 Published online by Cambridge University Press