Electronic Colloquium on Computational Complexity, Report No. 77 (2009)

From Randomness Extraction to Rotating Needles*

Zeev Dvir†

Abstract

The finite field Kakeya problem deals with the way lines in different directions can overlap in a vector space over a finite field. This problem came up in the study of certain Euclidean problems and, independently, in the search for explicit randomness extractors. We survey recent progress on this problem and describe several of its applications.

1 Overview

The geometry of finite fields has played an important role in the development of theoretical computer science in the past couple of decades. Properties of finite field polynomials have been used extensively in proving some of the seminal results of the field. Some notable examples are the PCP theorem [ALM+98, AS98], list decodable error correcting codes [Sud97, GS99, PV05, GR08], randomness extractors [TSUZ01, SU05, GUV09, DW08, DKSS09] and hardness-randomness tradeoffs [BFNW93, SU05]. These problems, while having nothing to do originally with finite fields, admit extremely elegant solutions using finite field machinery. The application of finite fields is, in many cases, in the form of constructions of certain maps with seemingly 'magical' properties that are then used as a tool to obtain the required result or, sometimes, even present the solution to the problem itself.

It occasionally happens that a certain problem attracts attention from the direction of both mathematicians working on finite field geometry and from computer scientists interested in problems such as the ones listed above. One such instance is the finite field Kakeya problem. This question, regarding the limitations of packing lines in different directions into small sets, emerged in the late 90's in connection with the famous Euclidean Kakeya conjecture and was studied by researchers interested in that problem [Wol99, Rog01, MT04, BKT04]. The exact same question, in a different

*This is a survey paper invited to appear in SIGACT news complexity column, edited by Lane A. Hemaspaandra.

†School of Mathematics, Institute for Advanced Study, Princeton, NJ 08540, USA. dvir@math.ias.edu. Research partially supported by NSF Grant CCF-0832797 (Expeditions in computing grant) and by NSF Grant DMS-0835373 (pseudorandomness grant).

ISSN 1433-8092

setting, came up independently in connection with a specific construction of randomness extractors [LRVW03, DS07] which are objects that are of interest in theoretical computer science.

In [Dvi08] the *Polynomial method* was applied to attack the finite field Kakeya problem. This technique, while not new in the context of extractors, was apparently not considered before by mathematicians working on the problem. The proof technique was developed further in subsequent works [SS08, DKSS09, EOT09] to derive stronger and more general results on Kakeya type problems in finite fields. These new techniques were applied in [DW08, DKSS09] to derive new results on randomness extractors and also lead to progress on two related problems in *Euclidean* space – the multilinear Kakeya conjecture [Gut08] and the Joints conjecture [GK08, EKS09, KSS09].

The purpose of this note is to survey the above developments and to discuss the connections between them. We will include, in some places, complete proofs or proof sketches and in others only state the results. The sections are organized as follows: In Section 2 we discuss the finite field Kakeya conjecture, the development of its proof and its generalizations. We continue in Section 3 to describe the applications to randomness extractors. Section 4 discusses the progress on related problems in Euclidean space.

2 Finite field Kakeya sets

Let $\mathbb{F}$ denote a finite field of size q. A set $K \subset \mathbb{F}^n$ is called a *Kakeya* set[1] if it contains a line in every direction. More formally, if for every (direction) $b \in \mathbb{F}^n$ there exists a point $a \in \mathbb{F}^n$ such that the set $\{a + t \cdot b \,|\, t \in \mathbb{F}\}$ is contained in K. In a survey paper, Wolff [Wol99] made a conjecture about the size of such sets.

Conjecture 1 (The finite field Kakeya conjecture [Wol99]). *Let $K \subset \mathbb{F}^n$ be a Kakeya set, then*

$$|K| \geq C_n \cdot q^n,$$

where C_n is a constant depending only on n.

This conjecture originates from the famous Euclidean Kakeya conjecture which deals with bounding the dimension of sets in $\mathbb{R}^n$ containing a unit line segment in every direction (more on this connection in Section 4). This natural question on the geometry of finite fields was posed by Wolff as a 'stripped down' version of its Euclidean sibling on which new ideas could be tested without having to deal with the technical difficulties of Euclidean geometry.

Until recently, progress on the finite field Kakeya problem and on the Euclidean problem went hand-in-hand. The best bounds for both problems were obtained using

[1] The term *Besicovitch set* is also used in the literature.

a technique of Bourgain [Bou99] (later improved in [KT02]) which uses tools from additive combinatorics. These techniques (which are beyond the scope of this survey and are still the most effective for the Euclidean problem) give a lower bound of $\approx q^{\frac{4}{7}n}$ on the size of K [Rog01, MT04]. We note that a bound of the form $|K| \geq q^{n/2}$ can be easily obtained by observing that the difference set $K - K$ is equal to the whole space. Recently, the finite field Kakeya conjecture was proved [Dvi08]. In this section we describe this proof and the improvements/generalizations that followed.

2.1 The polynomial method

We start with the first proof of the finite field Kakeya conjecture appearing in [Dvi08]. The constant C_n obtained here is not optimal and was improved in subsequent works (these will be described later). The proof uses the polynomial method, which works, in general, by interpolating a non-zero low-degree polynomial on the set in question, and then proceeds to derive a contradiction by showing that the polynomial has too many zeros and so must be identically zero. The original proof appearing in [Dvi08] gave a slightly weaker bound than the one appearing here. The improved proof, which was included in a later version of that paper, incorporates an observation made independently by N. Alon and T. Tao.

Theorem 2.1 ([Dvi08]). *Let $K \subset \mathbb{F}^n$ be a Kakeya set, then*

$$|K| \geq \frac{1}{n!} \cdot q^n.$$

The interpolation of a polynomial that vanishes on K is achieved using the following simple lemma.

Lemma 2.2. *Let $S \subset \mathbb{F}^n$ be such that $|S| < \binom{d+n}{n}$. Then there exists a non-zero polynomial $g(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$ of degree $\leq d$ such that $g(x) = 0$ for all $x \in S$.*

Proof. The number of monomials in n variables of degree at most d is exactly $\binom{d+n}{n}$. The constraints $g(a) = 0$ for $a \in S$ are all homogeneous and linear in the coefficients of g. Therefore, since there are more coefficients than constraints, we can find a non zero solution satisfying all of these constraints. □

Another ingredient in the proof is the Schwartz-Zippel lemma, which bounds the number of zeros of a non-zero polynomial.

Lemma 2.3 ([Sch80, Zip79]). *Let $g \in \mathbb{F}[x_1, \ldots, x_n]$ be a non-zero polynomial with degree at most d. Then*

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

We are now ready to prove Theorem 2.1: Suppose in contradiction that

$$|K| < \frac{1}{n!} \cdot q^n < \binom{q-1+n}{n}.$$

Then, using Lemma 2.2, we can find a non-zero polynomial $g(x)$ of degree $d \leq q-1$ that vanishes on K. We proceed by considering the restriction of g to lines in different directions passing through K. Let $b \in \mathbb{F}^n$ be some direction and let $a \in \mathbb{F}^n$ be such that

$$\{a + t \cdot b \,|\, t \in \mathbb{F}\} \subset K.$$

The restriction of g to this line (passing through a in direction b) is a univariate polynomial given by

$$h_{a,b}(t) = g(a + t \cdot b) = g(a_1 + t \cdot b_1, \ldots, a_n + t \cdot b_n).$$

One can easily verify that the coefficient of the monomial t^d in $h_{a,b}$ is exactly $g_d(b)$, where g_d is the homogeneous part of g of highest degree. Therefore,

$$h_{a,b}(t) = g_d(b) \cdot t^d + O(t^{d-1}).$$

We now observe that $h_{a,b}(t) = 0$ for every $t \in \mathbb{F}$ (since all the points $a + tb$ are in K and g vanishes on K). This implies that $h_{a,b}$ is identically zero, since otherwise it could have at most $d \leq q-1$ zeros (this is just the fundamental theorem of algebra or the one-dimensional case of the Schwartz-Zippel lemma). Since $h_{a,b}$ is identically zero, its leading coefficient, $g_d(b)$, has to be zero. Since $b \in \mathbb{F}^n$ was arbitrary, we conclude that g_d vanishes on the entire space $\mathbb{F}^n$. This contradicts Lemma 2.3, since g_d is non-zero of degree $d \leq q-1$ and so can have at most $(q-1) \cdot q^{n-1} < q^n$ zeros. This completes the proof of Theorem 2.1.

2.2 Introducing multiplicities

In [SS08] an improvement to the constant C_n from Theorem 2.1 was derived. This was done by considering polynomials that vanish with *high multiplicity* on the Kakeya set K. This idea, of using multiplicities to enhance the polynomial method, was already used in the context of list decodable error correcting codes in [GS99] and can be traced back even to Stepanov's proof of Weil's theorem [Ste71] (via "Stepanov's Method").

The notion of multiplicities is very easy to define for univariate polynomials: a polynomial $h(t)$ vanishes with multiplicity m at a point $a \in \mathbb{F}$ iff $h(t)$ is divisible by $(t-a)^m$. This implies, in particular, that a univariate polynomial of degree d can have at most d zeros **counting multiplicities**, a fact that will be used later in the proof.

The generalization of the notion of multiplicities to the multivariate case is as follows: we say that a polynomial $g(x_1, \ldots, x_n)$ vanishes with multiplicity m at a

point $a \in \mathbb{F}^n$ if the shifted polynomial $g(x+a)$ contains only monomials of degree m and higher. We define $\mathbf{mult}(g, a)$, the multiplicity of g at a, to be the largest m such that g vanishes at a with multiplicity m. One can easily see that this definition indeed generalizes the univariate one.

We now prove the result from [SS08] (the constant 4 can be improved to 2.6 using a more clever choice of parameters).

Theorem 2.4 ([SS08]). *Let $K \subset \mathbb{F}^n$ be a Kakeya set, then*

$$|K| \geq \frac{1}{4^n} \cdot q^n.$$

We will begin the proof by interpolating a low degree polynomial (this time bounding the individual degrees instead of the total degree) that vanishes on K with high multiplicity. This is achieved using the following lemma.

Lemma 2.5. *Let $S \subset \mathbb{F}^n$ be such that*

$$|S| < \frac{q^n}{\binom{m+n-1}{n}}$$

Then there exists a non-zero polynomial $g \in \mathbb{F}[x_1, \ldots, x_n]$ such that $\mathbf{mult}(g, a) \geq m$ for all $x \in S$ and such that g has individual degrees at most $q-1$ (that is, each variable appears with degree at most $q-1$).

Proof. As before, g will be found by solving an under-determined system of homogeneous linear equations. Each condition of the form $\mathbf{mult}(g, a) \geq m$ corresponds to the $\binom{m+n-1}{n}$ homogeneous linear constraints (on the coefficients of g) requiring that the coefficients of monomials of degree less than m in $g(x+a)$ are zero (one condition per monomial). In total, we have $|S| \cdot \binom{m+n-1}{n}$ constraints, which is smaller than q^n – the number of coefficients in g (as each variable can appear with degree between 0 and $q-1$). □

The second ingredient in the proof will be the following (folklore) lemma, which will be used instead of the Schwartz-Zippel lemma.

Lemma 2.6. *Let $g \in \mathbb{F}[x_1, \ldots, x_n]$ be a non-zero polynomial with individual degrees at most $q-1$. Then there exists a point $a \in \mathbb{F}^n$ such that $g(a) \neq 0$.*

We now turn to prove Theorem 2.4. Assuming

$$|K| < \frac{q^n}{4^n} \leq \frac{q^n}{\binom{2n-1}{n}},$$

we can find, using Lemma 2.5, a non-zero polynomial $g(x)$ with individual degrees bounded by $q-1$ such that $\mathbf{mult}(g, a) \geq n$ for every $a \in K$. As before, we fix some $b \in \mathbb{F}^n$ and let $a \in \mathbb{F}^n$ be such that the set $\{a + t \cdot b \,|\, t \in \mathbb{F}\}$ is contained in K. The

polynomial $h_{a,b}(t) = g(a+t\cdot b)$ now has q zeros of multiplicity at least n (one needs to verify that the restriction operation can only increase multiplicities). As the degree of $h_{a,b}$ is at most $(q-1)\cdot n$ (the sum of individual degrees of g) we conclude that $h_{a,b}$ is identically zero. This implies, as before, that $g_d(b) = 0$. Using Lemma 2.6 we derive the required contradiction (g_d cannot vanish everywhere). This completes the proof.

2.3 More multiplicities

As we saw in the previous section, using polynomials of higher degree (total degree $(q-1)n$ instead of $q-1$) resulted in a tighter bound on the size of Kakeya sets. It is natural to wonder whether we can push this idea further. At first glance it seems that we cannot, since a non-zero polynomial with individual degrees larger than $q-1$ can potentially vanish on the entire space (e.g the polynomial $x_1^q - x_1$). The solution is to use a more general form of the Schwartz-Zippel lemma that is useful also for polynomials of degree higher than the field size. This is done, again, by considering the more general case of zeros with multiplicities.

Lemma 2.7 ([DKSS09]). *Let $g \in \mathbb{F}[x_1, \ldots, x_n]$ be a non-zero polynomial of degree at most d. Then*

$$\sum_{a\in\mathbb{F}^n} \mathbf{mult}(g,a) \leq d\cdot q^{n-1}.$$

Using this lemma we can improve the value on C_n in the Kakeya bound to $1/2^n$. This improvement brings the lower bound on the size of Kakeya sets to within a factor of 2 of the known upper bounds (these are described in the next section).

Theorem 2.8 ([DKSS09]). *Let $K \subset \mathbb{F}^n$ be a Kakeya set. Then*

$$|K| \geq \frac{1}{2^n}\cdot q^n.$$

We will not give the complete proof but rather sketch the idea. As in the previous proofs we first interpolate a non-zero degree d polynomial that vanishes on K with multiplicity m (d and m will be chosen later). An argument similar to the one used in Lemma 2.5 tells us that this is possible as long as

$$|K| < \frac{\binom{d+n}{n}}{\binom{m+n-1}{n}}. \tag{1}$$

Next, we consider the restrictions $h_{a,b}(t)$ to lines through K. In the previous proofs, each restriction gave us a simple (multiplicity one) zero of g_d. We will modify this step so that we will derive a zero *of high multiplicity* of g_d at b. That is, we will show that $\mathbf{mult}(g,b) \geq m/2$ for every b. This part of the proof (which uses Hasse

derivatives and is omitted due to its technicality) goes through as long as

$$d < \frac{m}{2} \cdot q \tag{2}$$

Using Lemma 2.7 and the above argument (carried out for each $b \in \mathbb{F}^n$) we have that

$$\frac{m}{2} \cdot q^n \leq \sum_{b \in \mathbb{F}^n} \mathbf{mult}(g_d, b) \leq d \cdot q^{n-1},$$

which is a contradiction, by Equation. 2.

We complete the proof by picking d and m as follows: d will go to infinity in multiples of q. That is, $d = q \cdot R$, with R an integer tending to infinity. We then pick

$$m = 2 \cdot \frac{d}{q} + 1$$

so that Eq. 2 is satisfied. Observing Eq. 1 we see that this choice of parameters (when taking R to infinity) results in a bound of

$$|K| \geq \frac{\binom{d+n}{n}}{\binom{m+n-1}{n}} \to \frac{d^n}{m^n} \approx \frac{q^n}{2^n},$$

as was required.

2.4 A construction of small Kakeya sets

We now turn to describing the smallest known Kakeya sets which are of size

$$|K| \leq \frac{q^n}{2^{n-1}} + O(q^{n-1}),$$

which is, asymptotically as q tends to infinity, to within a factor of 2 of the lower bound obtained in [DKSS09]. The construction for the case $n = 2$ was given by [MT04] and the generalization for larger n was observed by the author for odd characteristic and by [SS08] for even characteristic. We give here the construction for odd characteristic.

We will only worry about lines in directions $b = (b_1, \ldots, b_n)$ with $b_n = 1$. The rest of the lines can be added using an additional q^{n-1} points, which is swallowed by the low order term. Our set is defined as follows:

$$K = \left\{ \left(v_1^2/4 + v_1 \cdot t, \ldots, v_{n-1}^2/4 + v_{n-1} \cdot t, t \right) \;\middle|\; v_1, \ldots, v_{n-1}, t \in \mathbb{F} \right\}.$$

Let $b = (b_1, \ldots, b_{n-1}, 1)$ be some direction. Then K clearly contains the line in direction b through the point $(b_1^2/4, \ldots, b_{n-1}^2/4, 0)$. We now turn to showing that $|K| \leq \frac{q^n}{2^{n-1}}$. Notice that the sum of the first coordinate of K and the square of the last one is equal to

$$v_1^2/4 + v_1 \cdot t + t^2 = (v_1/2 + t)^2$$

and so is a square in $\mathbb{F}$. Since $\mathbb{F}$ has odd characteristic it contains at most $\approx q/2$ squares. Let $x_1, \ldots, x_n$ denote the coordinates of the set K. Fixing the last coordinate we get that the first coordinate x_1 can take at most $\approx q/2$ values. The same holds for $x_2, \ldots, x_{n-1}$ and so we get a bound of $\approx \frac{q^n}{2^{n-1}}$ on the size of K.

2.5 The Kakeya maximal function estimate

The finite field Kakeya conjecture tells us that we cannot hope to pack lines in *all* directions into a small set. But perhaps there is some large family of directions such that lines in *these* directions *can* be packed efficiently? Another question one might ask is what if we only require each line to intersect our set in many points, instead of being contained in it completely? When perused further, this line of inquiry bring us to the Kakeya *maximal function estimate*, which gives a highly precise statement on the way lines in different directions can be packed together.

In order to state this result we require some notations. Let $\mathbb{P}^{n-1}(\mathbb{F})$ denote the set of directions of lines in $\mathbb{F}^n$ (this is simply the $n-1$ dimensional projective space over $\mathbb{F}$). For a direction $w \in \mathbb{P}^{n-1}(\mathbb{F})$ and for a point $a \in \mathbb{F}^n$, let $\ell_{a,w} \subset \mathbb{F}^n$ denote the line through a in direction w. For every function $f : \mathbb{F}^n \mapsto \mathbb{R}$ we define its *Kakeya maximal function*, $f^* : \mathbb{P}^{n-1}(\mathbb{F}) \mapsto \mathbb{R}$, as follows

$$f^*(w) = \max_{a \in \mathbb{F}^n} \sum_{x \in \ell_{a,w}} |f(x)|.$$

In other words, $f^*(w)$ is equal to the maximum, over all lines in direction w, of the sum of absolute values of f along this line. In particular, if f is the indicator function of a Kakeya set, then $f^*(w) = q$ for every w. Similarly, if f is the indicator function of a set which is 'close' to being a Kakeya set (e.g it contains many partial lines in many directions) then the ℓ_1 norm of f^* will be large, since for many w's there exists an a for which the sum of absolute values of f on $\ell_{a,w}$ is large. In general, there is no reason to limit f to be an indicator function – f can be an arbitrary measure on the space $\mathbb{F}^n$.

We are now ready to state the Kakeya maximal estimate in its full generality. This estimate, which was recently proved in [EOT09], was first conjectured in [MT04] and corresponds to a similar estimate in the Euclidean domain, generalizing the Euclidean Kakeya conjecture. Its proof (which is too technical to fit here) builds on the polynomial method while introducing several new ideas.

Theorem 2.9 ([EOT09]). *Let $f : \mathbb{F}^n \mapsto \mathbb{R}$ be a function and let $f^* : \mathbb{P}^{n-1}(\mathbb{F}) \mapsto \mathbb{R}$ be its corresponding Kakeya maximal function. Then*

$$\sum_{w \in \mathbb{P}^{n-1}(\mathbb{F})} |f^*(w)|^n \leq C_n \cdot q^{n-1} \cdot \sum_{x \in \mathbb{F}^n} |f(x)|^n,$$

where C_n depends only on n.

In order to demonstrate the strength of this theorem we consider a special case. Suppose $K \subset \mathbb{F}^n$ is a set intersecting m lines (with different directions) in at least k points each. Intuitively, we expect K to have size roughly $\approx mk$. Let f be the indicator function of K. Then, $|f^*(w)| \geq k$ for at least m different values of w. Plugging this information into the estimate in Theorem 2.9 we get

$$m \cdot k^n \leq C_n \cdot q^{n-1} \cdot |K|.$$

Rearranging, we get that

$$|K| \geq C_n^{-1} \cdot \left(\frac{k}{q}\right)^{n-1} \cdot mk,$$

which is $\Omega_n(mk)$ whenever, say, $k = \Omega_n(q)$.

In fact, a more general estimate, involving curves instead of lines, was proved in [EOT09]. The idea to use the polynomial method to control the intersections of curves was first used in [DW08] in the context of randomness extractors. This leads us to the second part of this survey which deals with the application of Kakeya type estimates to the construction of randomness extractors.

3 Application to randomness extractors

As was mentioned before, the finite field Kakeya problem originated independently in the quest for constructing functions with 'special' properties used in theoretical computer science. These functions, called randomness extractors (or just extractors for short), play an important role in the proofs of many results on a large number of topics including de-randomization (the relation between deterministic and randomized algorithms), error correcting codes, cryptography and many others.

Roughly speaking, an extractor is a function that 'extracts' randomness from arbitrary random distributions, with the help of a short random seed. More formally, an extractor is a function

$$E : \{0,1\}^n \times \{0,1\}^d \mapsto \{0,1\}^m$$

such that for every random variable X on $\{0,1\}^n$ with min-entropy[2] at least k, the random variable $E(X, U_d)$ is close, in statistical distance, to the uniform distribution, where U_d is uniform on $\{0,1\}^d$ and independent of X. We think of d as being much smaller than k and m and so E can be said to 'extract' the entropy of X (and not that of U_d). In the definition above, k is said to be the *entropy threshold* of the extractor and X is said to be an extractor for sources of entropy k.

Another useful way to view an extractor is as an unbalanced bipartite graph with 2^n left vertices and 2^m right vertices and with left-degree 2^d. The fact that E is an

[2]A random variable X has min entropy at least k if $\mathbf{Pr}[X = x] \leq 2^{-k}$ for every $x \in \{0,1\}^n$.

extractor, say for sources of min-entropy k, means that every set of left vertices of size at least 2^k is mapped almost uniformly to the right hand side of the graph. Naturally, we wish to maximize m (the amount of entropy extracted) and to minimize d and the statistical error (it can be shown that the need for an independent random seed is unavoidable).

One important thing to keep in mind when talking about extractors is that picking E at random will give, with overwhelming probability, an extractor with the best possible parameters. The challenge is therefore, not to show that good extractors exists, but rather to give explicit (efficiently computable) constructions, matching the parameters of a random construction. This type of challenge is similar to the one arising in the construction of good error correcting codes, expander graph, Ramsey graphs and other combinatorial objects.

Since this is not a survey on extractors (the curious reader is referred to [Sha02, GUV09, DW08, DKSS09] and references within) we will not delve into all the intricacies surrounding them, but rather concentrate on their connection to the finite field Kakeya problem. In order to make clear this connection we have to introduce the notion of *mergers*. Mergers are similar to extractors in the sense that they are functions that extract randomness from weak distributions. However, unlike extractors, they relax two of the conditions on the input and output distributions. The first relaxation is a structural condition on the input X. Instead of being an arbitrary distribution (with high min entropy), X is now divided into s blocks $X_1, \ldots, X_s$, each of length n bits, and we are guaranteed that one of these blocks is uniform (the dependencies between the blocks can be arbitrary). This type of source is referred to in the literature as a 'somewhere-random source'. The second relaxation is that, instead of requiring the output, another n-bit string, to be close to uniform, we only require it to have very high min-entropy (say, at least $\frac{9}{10}n$). As is the case with extractors, mergers have to rely on an additional short random seed.

Stated more formally, a merger is a function

$$M : (\{0,1\}^n)^s \times \{0,1\}^d \mapsto \{0,1\}^n$$

such that if $X = (X_1, \ldots, X_s)$ is a random variable on $(\{0,1\}^n)^s$ for which one of the X_i's is uniform, then $M(X, U_d)$ has (up to some small statistical error) min entropy at least $\frac{9}{10}n$ (the choice of constant $\frac{9}{10}$ is arbitrary). It was shown in [TS96, NTS99] that explicit constructions of good mergers (for a large number of blocks) imply good constructions of extractors and so the task of building good mergers became one of equal interest to that of building extractors.

3.1 Mergers using finite fields

The connection to the finite field Kakeya problem arose in an attempt to analyze a specific, very natural, construction of mergers [3]. This construction, given by [LRVW03], is the following: pick a finite field $\mathbb{F}$ of size q and interpret each block $X_i \in \{0,1\}^n$ as an element of $\mathbb{F}^r$ for $r \approx n/\log_2(q)$. Now, use the seed U_d to pick s field elements $a_1, \ldots, a_s$ and output the linear combination $\sum_{i=1}^{s} a_i X_i$. In other words, the merger picks a uniform element in the span of the blocks $X_1, \ldots, X_s$. The question is whether this construction can be called a merger?

In order to to see how this question leads to the Kakeya problem we will consider the simplest case of merging just two blocks. This boils down to bounding the entropy of a random variable of the form

$$a_1 X_1 + a_2 X_2,$$

with either X_1 or X_2 uniform in $\mathbb{F}^r$ and with a_1, a_2 uniform and independent of X_1, X_2. Suppose there was a Kakeya set $K \subset \mathbb{F}^r$ such that

$$|K| \ll q^{\frac{9}{10}r} \approx 2^{\frac{9}{10}n}.$$

Then, we could define a function $f_K : \mathbb{F}^r \mapsto \mathbb{F}^r$ such that for every $x \in \mathbb{F}^r$ and for every $t \in \mathbb{F}$ we would have

$$f_K(x) + t \cdot x \in K$$

(the line through $f_K(x)$ in direction x is contained in K). Now, consider the pair of random variables (X_1, X_2) with X_1 uniform on $\mathbb{F}^r$ and $X_2 = f_K(X_1)$. The random variable

$$Z = \frac{a_1}{a_2} \cdot X_1 + X_2 = \frac{a_1}{a_2} \cdot X_1 + f_K(X_1)$$

(we assume $a_2 \neq 0$ for simplicity) is now supported on the set K and so has entropy at most

$$\log_2 |K| \ll \frac{9}{10} n.$$

Multiplying Z by a_2 cannot increase its entropy by much (since $\log_2(q)$ is relatively small compared to n) and so we get that the merger fails on the input X_1, X_2. In other words, if we show that the merger output has high entropy then we also show that there are no small Kakeya sets! Of course, there is a direct connection between the fraction of entropy extracted by the merger and the minimum size of Kakeya sets. The analog to the finite field Kakeya conjecture would be to show that the merger outputs a string with entropy close to n.

Even though the reduction above, converting merger bounds to Kakeya bounds, is one-way, it is not surprising that results can be usually translated also in the

[3] This demonstrates a recurring theme in theoretical computer science, when constructions using finite fields are often the most natural.

reverse direction. The proof method of [Dvi08], for example, can be used to show that the merger of [LRVW03] has output entropy very close to n. This result, while interesting in its own right, does not lead to progress on extractors due to the fact that the seed length, d, grows linearly with the number of blocks (this makes the reduction to extractors outlined in [TS96, NTS99] practically useless). The situation can be remedied, however, by replacing lines with curves.

3.2 Curves instead of lines

In [DW08] a new merger was constructed that makes use of the fact that the polynomial method can be applied just as efficiently to control intersections of low degree *curves* instead of lines. roughly speaking, the merger passes a low degree curve through the s points $X_1, \ldots, X_s \in \mathbb{F}^r$ and outputs a random point on this curve. More formally, we find (using interpolation) an r-tuple of univariate polynomials

$$\phi(t) = (\phi_1(t), \ldots, \phi_r(t)) \in (\mathbb{F}[t])^r$$

of degree at most $s-1$ such that

$$\phi(1) = X_1, \ldots, \phi(s) = X_s,$$

where we assume for simplicity that $\mathbb{F}$ is prime and so contains the elements $1, 2, \ldots, s$. The output of the merger is $\phi(U_d)$, where we need to take $d \approx \log_2(q)$ so that U_d will have enough bits to sample a uniform element in $\mathbb{F}$ (the exact choice of field size will be discussed below).

The way to argue about the min-entropy of this merger's output is as follows (we only give a rough sketch of the argument): Suppose that $M(X, U_d)$ has entropy smaller than k. Then, we can find a small set K of size roughly 2^k such that for 'many' fixings of $X = x$ we have

$$\mathbf{Pr}[M(x, U_d) \in K] \geq 1/10.$$

In other words, the set K intersects 'many' curves (each curve corresponding to a fixing of $X = x$) in at least $q/10$ points. The fact that we have many curves follows from the fact that one of the X_i's is uniform (and so the curves 'cover' the entire space). We can thus use the polynomial method (as was done in [DW08]) or the polynomial method with multiplicities (as in [DKSS09]) to derive a contradiction. The argument is a straightforward generalization of the one used for lines – we first find a polynomial vanishing (with high multiplicity) on the set K and then consider its restrictions to all the relevant curves passing through K. As long as the degree of the vanishing polynomial is chosen to be sufficiently small, we get that this polynomial must vanish identically on *all* of these curves, and so (since the curves cover the space uniformly) must have many zeros (or many zeros with high multiplicities). We then use the Schwartz-Zippel lemma (with multiplicities) to get a contradiction. This final result is described by the following theorem.

Theorem 3.1 ([DKSS09]). *The output of the merger described above is ϵ-close (in statistical distance) to having min entropy at least $(1-\delta)\cdot n$, whenever*

$$q \geq \left(\frac{2\cdot s}{\epsilon}\right)^{\frac{1}{\delta}}.$$

This theorem improves a weaker bound obtained in [DW08] (without the use of multiplicities) in which the bound on the field size included also the *length* of each block. In [EOT09] a more general Kakeya-type result for curves was obtained using an even more sophisticated application of the polynomial method. The setting studied in [EOT09] deals with sets *inside varieties* that intersect many curves in many points and proves a more refined *maximal estimate* for this setting (this however, does not seem to strengthen the merger analysis in any significant way).

As a result of the merger analysis of Theorem 3.1, a new extractor construction was given in [DKSS09] with parameters that were not obtainable using previous methods (we refer the interested reader to [DKSS09] for more details on this result).

4 The polynomial method in Euclidean space

Let us go back now and consider the original motivation, given by Wolff [Wol99], for studying finite field Kakeya sets – namely, the Euclidean Kakeya problem. Let $K \subset \mathbb{R}^n$ be a compact set containing a unit line segment in every direction. Such sets are called Kakeya (or Besicovitch) sets and, surprisingly enough, can have Lebesgue measure equal to zero [Bes28]. The simplest formulation of the Euclidean Kakeya problem uses the notion of Minkowski (or covering) dimension, which provides a more refined way to argue about the 'size' of such sets. For every $\epsilon > 0$ let $N_\epsilon(K)$ denote the minimal number of balls of radius ϵ needed to cover K. We are interested in the way $N_\epsilon(K)$ grows as ϵ goes to zero. It is clear that $N_\epsilon(K) \leq O(1/\epsilon^n)$, where all hidden constants depend on n, since K is compact and is thus contained in a ball of finite radius. Roughly speaking, the Minkowski dimension of K is defined to be the smallest d such that $N_\epsilon(K) \leq O(1/\epsilon^d)$. Notice that d is a number (not necessarily integer) between 0 and n. It is not hard to see that this notion of dimension agrees with our intuition regarding 'simple' sets such as bounded 'chunks' of vector spaces or varieties.

The Euclidean Kakeya conjecture states that a Kakeya set in $\mathbb{R}^n$ must have Minkowski dimension equal to n. In other words, in order to cover K with balls of radius ϵ, we need at least $\Omega(1/\epsilon^n)$ balls (asymptotically, as ϵ tends to zero). When comparing this with the finite field setting we see that the quantity $1/\epsilon$ corresponds to the field size q and that the dimension corresponds to $\log_q |K|$. With this correspondence in mind, it is not hard to see that a bound of $\approx n/2$ on the dimension of Kakeya sets is relatively easy to obtain. The first bound of the form $(1/2+\delta)n$ was given by Bourgain [Bou99] using tools from additive combinatorics. This proof method was

subsequently improved by [KT02] where a bound of $\approx 0.596n$ was obtained. Proving the Euclidean Kakeya conjecture (in the form described above or in one of its more general formulations) is considered to be a major open problem and is connected to many other unanswered questions in various areas of mathematics (see the surveys [Wol99, Tao01, Bou00] for more information).

Even though the recent progress on the finite field Kakeya problem did not yet lead to new bounds on the Euclidean Kakeya conjecture, it did lead to progress on two related problems in Euclidean space. These are described below.

4.1 The multilinear Kakeya conjecture

The multilinear Kakeya conjecture, stated by [BCT06], is a restricted version of the general Kakeya conjecture. This version of the problem requires, essentially, that the line segments passing trough a 'typical' point of K cannot be 'close' to being contained in a hyperplane. A nearly complete proof of this conjecture was given in [BCT06] using Heat-Flow arguments. Recently, a simpler proof, with a better (indeed, optimal) result, was given by Guth [Gut08]. Guth's proof is based on an adaptation of the polynomial method of [Dvi08] to the Euclidean setting. This is made possible via the Polynomial Ham Sandwich theorem, which replaces Lemma 2.2 in the argument of [Dvi08].

Theorem 4.1 (The Polynomial Ham-Sandwich theorem [Gro03]). *Let*

$$U_1, \ldots, U_s \subset \mathbb{R}^n$$

be bounded open sets with

$$s < \binom{d+n}{n}.$$

Then, there exists a non-zero polynomial $g \in \mathbb{R}[x_1, \ldots, x_n]$, of degree at most d, such that the sets $\{g(x) < 0\}$ and $\{g(x) > 0\}$ bisect each of the sets U_i into two equal parts.

Giving a complete account of Guth's proof is beyond the scope of this survey. We will, however, attempt to describe the way in which the above theorem appears in the argument. Suppose $N_\epsilon(K) = s \ll 1/\epsilon^n$ and let $B_1, \ldots, B_s$ be balls of radius ϵ covering K. Applying Theorem 4.1 we can find a non-zero polynomial $g \in \mathbb{R}[x_1, \ldots, x_n]$ of degree $d \ll 1/\epsilon$ that bisects each of these balls into two equal parts. The main part of the argument uses this property together with the multilinearity condition to argue that the hyper-surface $H = \{g(x) = 0\}$ intersects many of the lines passing through the points of K. Here we use the fact that H looks locally like a hyperplane and, therefore, the lines through a typical point cannot all avoid it. Finally, this information is used to find a single line that intersects the interior of H in more than d points. The restriction of g to this line is identically zero, since each intersection with H is a zero and the number of intersections is larger than the degree. By slightly

perturbing this line we get a family of lines, on which g vanishes, whose union forms a set of positive measure. This is a contradiction since a non-zero polynomial cannot vanish on a set of positive measure.

4.2 The joints conjecture

Another Euclidean problem, related to Kakeya, on which recent progress was made using the polynomial method is the Joints Conjecture of Sharir [Sha94]. This is a problem which originated from the area of computational geometry and was observed later to be related to the Euclidean Kakeya problem by Wolff [Wol99]. In this problem we consider a set of M lines in $\mathbb{R}^3$. We say that a point $a \in \mathbb{R}^3$ is a *joint* if it is the intersection of at least three lines which are not co-planar. The joints conjecture states that there could be at most $O(M^{3/2})$ joints. This is seen to be the optimal bound using a trivial arrangement of lines in a lattice of side length $\sqrt{M}$. Using a variant of the polynomial method, Guth and Katz [GK08] proved this conjecture, improving the previously best bound of $M^{1.6232}$ due to Feldman and Sharir [FS05].

Theorem 4.2 ([GK08]). *M lines in $\mathbb{R}^3$ can create at most $O(M^{3/2})$ joints.*

The proof of this theorem was simplified in [EKS09] and generalized to n dimensions in [KSS09]. The definition of a joint in n dimensions is an intersection of n lines in n linearly independent directions.

Theorem 4.3 ([KSS09]). *M lines in $\mathbb{R}^n$ can create at most $O_n(M^{\frac{n}{n-1}})$ joints, where the implied constant depends on n only.*

Proof. Let J denote the set of joints created by M lines in $\mathbb{R}^n$. W.l.o.g. we can assume that each line passes through at least $|J|/2M$ joints (we can through away all other lines at negligible cost). Suppose in contradiction that

$$|J| > A \cdot M^{\frac{n}{n-1}},$$

with A a constant (depending on n) to be determined later. Let $g \in \mathbb{R}[x_1, \ldots, x_n]$ be a non-zero polynomial of *minimal degree* vanishing on J. Using Lemma 2.2 (which holds, of course, also over the reals) we have that

$$d = \deg(g) \leq O_n(|J|^{1/n}).$$

If we restrict g to one of the M lines we see that the restriction has at least $|J|/2M$ zeros, which is, by our assumption, larger than d (as long as we pick the constant A to be sufficiently large). Therefore, g vanishes identically on each of the M lines. We will now show that all of the n partial derivatives $\frac{\partial g}{\partial x_i}$ of g vanish on J, which will be a contradiction, since one of them will be non-zero and of degree lower than that of g.

Let $a \in J$ be a joint and let $v_1, \ldots, v_n$ be the linearly independent directions of n lines passing through a. Since g vanishes identically on each of these lines we have

$$h_i(t) = g(a + t \cdot v_i) \equiv 0$$

for every $i \in [n]$. Let

$$\nabla g(a) = \left(\frac{\partial g}{\partial x_1}(a), \ldots, \frac{\partial g}{\partial x_n}(a) \right)$$

denote the gradient of g. A simple calculation shows that the coefficient of the monomial t in $h_i(t)$ is equal to $\langle \nabla g(a), v_i \rangle$. Since $h_i(t)$ is identically zero we have that $\langle \nabla g(a), v_i \rangle = 0$ for every $i \in [n]$. Since the set $v_1, \ldots, v_n$ is a basis of $\mathbb{R}^n$ we get that $\nabla g(a) = 0$. Since a was arbitrary, we have that ∇g vanishes on the entire set J, which is a contradiction to the minimality of the degree of g. □

We note that the proof above can be made to work also in the setting of finite fields. One difference is that, in a finite field, a non-constant polynomial can have all of its partial derivatives equal to zero (e.g x^q in $\mathbb{F}_q$). However, one can show that this can only happen if the polynomial is itself a power of another polynomial and that this power is divisible by the characteristic. This clearly cannot be the case for g in the proof due to the minimality of its degree.

References

[ALM+98] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and the hardness of approximation problems. *J. ACM*, 45(3):501–555, 1998.

[AS98] S. Arora and S. Safra. Probabilistic checking of proofs: a new characterization of NP. *J. ACM*, 45(1):70–122, 1998.

[BCT06] J. Bennett, A. Carbery, and T. Tao. On the multilinear restriction and Kakeya conjectures. *Acta Mathematica*, 196:261–302, 2006.

[Bes28] A. Besicovitch. On Kakeya's problem and a similar one. *Mathematische Zeitschrift*, (27):312–320, 1928.

[BFNW93] L. Babai, L. Fortnow, N. Nisan, and A. Wigderson. BPP has subexponential time simulations unless EXPTIME has publishable proofs. *Complexity Theory*, 3:307–318, 1993.

[BKT04] J. Bourgain, N. Katz, and T. Tao. A sum-product estimate in finite fields, and applications. *Geom. Funct. Anal.*, 14(1):27–57, 2004.

[Bou99] J. Bourgain. On the dimension of Kakeya sets and related maximal inequalities. *Geom. Funct. Anal.*, 9(2):256–282, 1999.

[Bou00] J. Bourgain. Harmonic analysis and combinatorics: How much may they contribute to each other? *IMU/Amer. Math. Soc.*, pages 13–32, 2000.

[DKSS09] Z. Dvir, S. Kopparty, S. Saraf, and M. Sudan. Extensions to the method of multiplicities, with applications to kakeya sets and mergers. In *FOCS 09 (to appear)*, 2009.

[DS07] Z. Dvir and A. Shpilka. An improved analysis of linear mergers. *Comput. Complex.*, 16(1):34–59, 2007. (Extended abstract appeared in RANDOM 2005).

[Dvi08] Z. Dvir. On the size of Kakeya sets in finite fields. *J. AMS (to appear)*, 2008.

[DW08] Z. Dvir and A. Wigderson. Kakeya sets, new mergers and old extractors. In *FOCS '08: Proceedings of the 2008 49th Annual IEEE Symposium on Foundations of Computer Science*, pages 625–633, Washington, DC, USA, 2008. IEEE Computer Society.

[EKS09] G. Elekes, H. Kaplan, and M. Sharir. On lines, joints, and incidences in three dimensions, 2009. Manuscript.

[EOT09] J. Ellenberg, R. Oberlin, and T. Tao. The Kakeya set and maximal conjectures for algebraic varieties over finite fields, 2009. Manuscript.

[FS05] S. Feldman and M. Sharir. An improved bound for joints in arrangements of lines in space. *Discrete Comput. Geom.*, 33(2):307–320, 2005.

[GK08] L. Guth and N. H. Katz. Algebraic methods in discrete analogs of the Kakeya problem, 2008. Manuscript.

[GR08] V. Guruswami and A. Rudra. Explicit codes achieving list decoding capacity: Error-correction with optimal redundancy. *IEEE Transactions on Information Theory*, 54(1):135–150, 2008.

[Gro03] M. Gromov. Isoperimetry of waists and concentration of maps. *Geom. Funct. Anal.*, 13(1):178–215, 2003.

[GS99] V. Guruswami and M. Sudan. Improved decoding of Reed-Solomon and algebraic-geometry codes. *IEEE Transactions on Information Theory*, 45(6):1757–1767, 1999.

[Gut08] L. Guth. The endpoint case of the Bennett-Carbery-Tao multilinear Kakeya conjecture, 2008. Manuscript.

[GUV09] V. Guruswami, C. Umans, and S. Vadhan. Unbalanced expanders and randomness extractors from Parvaresh–Vardy codes. *J. ACM*, 56(4):1–34, 2009.

[KSS09] H. Kaplan, M. Sharir, and E. Shustin. On lines and joints, 2009. Manuscript.

[KT02] N. Katz and T. Tao. New bounds for Kakeya problems. *Journal d'Analyse de Jerusalem*, 87:231–263, 2002.

[LRVW03] C. Lu, O. Reingold, S. Vadhan, and A. Wigderson. Extractors: Optimal up to constant factors. In *FOCS 03: Proceedings of the 35th Annual ACM Symposium on Theory of Computing*, 2003.

[MT04] G. Mockenhaupt and T. Tao. Restriction and Kakeya phenomena for finite fields. *Duke Math. J.*, 121:35–74, 2004.

[NTS99] N. Nisan and A. Ta-Shma. Extracting randomness: A survey and new constructions. *Journal of Computer and System Sciences*, 58, 1999.

[PV05] F. Parvaresh and A. Vardy. Correcting errors beyond the Guruswami-Sudan radius in polynomial time. In *FOCS '05: Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science*, pages 285–294, Washington, DC, USA, 2005. IEEE Computer Society.

[Rog01] K.M Rogers. The finite field Kakeya problem. *Amer. Math. Monthly 108*, (8):756–759, 2001.

[Sch80] J. T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *J. ACM*, 27(4):701–717, 1980.

[Sha94] M. Sharir. On joints in arrangements of lines in space and related problems. *J. Combin. Theory Ser. A*, 67(1):89–99, 1994.

[Sha02] R. Shaltiel. Recent developments in explicit constructions of extractors. *Bulletin of the EATCS*, 77:67–95, 2002.

[SS08] S. Saraf and M. Sudan. Improved lower bound on the size of Kakeya sets over finite fields. *Analysis and PDE*, 1(3):375–379, 2008.

[Ste71] S.A. Stepanov. On the number of points of a hyperelliptic curve over a finite prime field. *Math. USSR, Izv.*, 3:1103–1114, 1971.

[SU05] R. Shaltiel and C. Umans. Simple extractors for all min-entropies and a new pseudorandom generator. *J. ACM*, 52(2):172–216, 2005.

[Sud97] M. Sudan. Decoding of Reed Solomon codes beyond the error-correction bound. *J. Complex.*, 13(1):180–193, 1997.

[Tao01] T. Tao. From rotating needles to stability of waves: emerging connections between combinatorics, analysis, and PDE. *Notices Amer. Math. Soc.*, 48(3):294–303, 2001.

[TS96] A. Ta-Shma. *Refining Randomness*. PhD thesis, The Hebrew Univerity, Jerusalem, Israel, 1996.

[TSUZ01] A. Ta-Shma, C. Umans, and D. Zuckerman. Loss-less condensers, unbalanced expanders, and extractors. In *STOC '01: Proceedings of the thirty-third annual ACM symposium on Theory of computing*, pages 143–152, New York, NY, USA, 2001. ACM.

[Wol99] T. Wolff. Recent work connected with the Kakeya problem. *Prospects in mathematics (Princeton, NJ, 1996)*, pages 129–162, 1999.

[Zip79] R. Zippel. Probabilistic algorithms for sparse polynomials. In *Proceedings of the International Symposiumon on Symbolic and Algebraic Computation*, pages 216–226. Springer-Verlag, 1979.

ECCC ISSN 1433-8092

http://eccc.hpi-web.de