AN INTRODUCTION TO P-ADIC KAKEYA

MATTHEW BULL-WEIZEL

Abstract. The purpose of this expository article is to explain Arsovki's proof of p-adic Kakeya. The tools used in his proof are ones not often encountered alongside papers on the Kakeya conjecture: and so this article begins with providing the necessary prerequisites for Arsovki's paper. This is then followed by a highly detailed proof of the his main theorem, providing more information when needed, and extra steps.

1. Introduction and pre-requisites

Section 1 introduces motivation along with the algebraic and analytic properties of the p-adics. Section 2 states and proves Arsovski's result, Theorem 2.1.

1.1. **Introduction.** After Dvir's proof of finite field Kakeya [Dvi09], Ellenberg, Oberlin and Tao in [EOT10] noted that in order to achieve a result analogous to Euclidean Kakeya, one would require infinite *scales of length*. And so the p-adics, $\mathbb{Q}_p^n$ serve as a logical place to study Kakeya phenomena; since $\mathbb{Q}_p$, similar to $\mathbb{R}$, is a locally compact Hausdorff field. In fact, $\mathbb{R}^n$, $\mathbb{Q}_p^n$ and $\mathbb{F}_q^n((t))$, the space of formal Laurent series, along with their finite algebraic extensions, are the only such spaces. Arsovki's result [Ars24] resolves the conjecture over all n, and Salvatore [Sal23] was able to augment the method to resolve the matter over $\mathbb{F}_q((t))^n$.

Logically, we should first define $\mathbb{Q}_p$. For a rational number $q \neq 0 \in \mathbb{Q}$, we take

$$q = p^m \frac{a}{b},$$

where a and b are co-prime to p. We define the function $v_p : \mathbb{Q} \to \mathbb{Z}$ such that

$$v_p(q) = m,$$

and adopt $v_p(0) = \infty$. Later we will see this function is a *valuation* on $\mathbb{Q}$. Using v_p, we may define the p-adic norm, $|\cdot|_p$ via

$$|q|_p = p^{-v_p(q)} = p^{-m},$$

where we adopt the convention

$$|0|_p = 0. \tag{1}$$

We define the p-adic numbers as the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$, and take

$$\mathbb{Z}_p = B_{\mathbb{Q}_p}(0, 1)$$

Alternatively, one can define the ring $\mathbb{Z}_p$ as the completion of $\mathbb{Z}$ with respect to $|\cdot|_p$, and take $\mathbb{Q}_p$ as the field of fractions of $\mathbb{Z}_p$.

1.2. **Valuations.** In this subsection, we will define and discuss valuations. They are used to both construct the p-adic numbers, and extensively throughout Arsovki's proof. For a field K, We define a valuation v as a function from $K \to \mathbb{R} \cup \{\infty\}$ satisfying the following three properties.

$$v(q) = \infty \iff q = 0 \tag{2}$$

$$v(a \cdot b) = v(a) + v(b) \tag{3}$$

$$v(a + b) \geq \min\{v(a), v(b)\}. \tag{4}$$

We see that v_p, as defined in the previous subsection is a valuation from $\mathbb{Q}$ to $\mathbb{R} \cup \{\infty\}$. v_p *measures* the multiplicity of a rational q with respect to a prime p. However we can give examples of other valuations.

Consider the field of formal Laurent series over a field F, $F(t)$. For $f(t) = \sum_{n=-\infty}^{\infty} a_n t^n$, we define

$$v_t : F(t) \to \mathbb{Z} \cup \{\infty\}$$
$$v_t(f(t)) = \min\{n : a_n \neq 0\},$$

and again adopting $v_t(0) = \infty$. Note this well is defined since for all sufficiently large n, $a_{-n} = 0$.

Consider the example $F = \mathbb{F}_2$, $f_1(t) = t^2 + t^4$ and $f_2(t) = t^{100} + t^{50}$. Then if we view f_1 and f_2 as functions, and not purely algebraic objects, we can see $f_1(t) = f_2(t)$, for all t. However $v_t(f_1) = 2$ and $v_t(f_2) = 50$ and so one can see we may interpret v_t as *measuring* how fast a polynomial vanishes at $t = 0$. In fact, recalling the previous example of v_p, one can view v_p as measuring how fast a element of $\mathbb{Q}$ vanishes $\mod p$.

1.3. **Directions and Kakeya sets in $\mathbb{Q}_p$.** We define a Kakeya set $S \subseteq \mathbb{Q}_p^n$ to be a compact set such that for every direction $v \in \mathbb{Z}_p^n$, S contains a line $l_v = \{b_v + \lambda v : \lambda \in \mathbb{Z}_p\}$. One may believe we are requiring lines in too many directions, and instead should only require a line in every direction v contained in $\mathbb{P}^{n-1}(\mathbb{Z}_p)$, since this would be analogous to the euclidean definition. Indeed this definition is used in the literature, in [EOT10], however they can be show to be equivalent.

We define a Kakeya set S in $\mathbb{Z}/p^k\mathbb{Z}$ to be a set such that for every $v \in (\mathbb{Z}/p^k\mathbb{Z})^n$, there exists $l_v = \{b_v + \lambda v : \lambda \in \mathbb{Z}/p^k\mathbb{Z}\} \subset S$.

Now we prove the correspondence between Kakeya sets in $\mathbb{Z}_p^n$ and $(\mathbb{Z}/p^k\mathbb{Z})^n$ via the following proposition.

Proposition 1.1. *Consider the canonical projection $\varphi : \mathbb{Z}_p^n \to (\mathbb{Z}/p^k\mathbb{Z})^n$, then for a Kakeya set $S \subset \mathbb{Z}_p^n$, $\varphi(S)$ is a Kakeya set in $(\mathbb{Z}/p^k\mathbb{Z})^n$.*

Proof. Consider a direction $v' \in (\mathbb{Z}/p^k\mathbb{Z})^n$, and via the topological isomorphism

$$\mathbb{Z}_p/p^k\mathbb{Z}_p \cong \mathbb{Z}/p^k\mathbb{Z},$$

we take v to be some element of the coset $v' + p^k\mathbb{Z}_p^n \subset \mathbb{Z}_p^n$. Let $l_v = \{b_v + \lambda v : \lambda \in \mathbb{Z}_p\}$ be the line contained in S in the direction v. Cover l_v in p^k $\delta = p^{-k}$ balls, and note they will be disjoint since $|\cdot|_p$ is an ultrametric. Label the balls $\{B_j\}_{j=1}^{p^k}$, then we see $B_j = p^k\mathbb{Z}_p^n + \lambda_j v + b_v$ for $\lambda_j v \in l_v \cap B_j$. Since the balls are disjoint, the map

$$\varphi : \mathbb{Z}_p^n \to (\mathbb{Z}/p^k\mathbb{Z})^n,$$

restricted to the set $\lambda_j v$ is injective. Hence the image of S will contain a set of the form

$$l_{v'} = \{\varphi(b_v) + \lambda_j v' : \lambda \in \mathbb{Z}/p^k\mathbb{Z}\},$$

a line in the direction v'. Since v' was arbitrary, $\varphi(S)$ is a Kakeya set. □

Unfortunately, the relationship between Kakeya sets in $\mathbb{Z}_p$ and $\mathbb{Z}/p^k\mathbb{Z}$ does not flow in the other direction.

Proposition 1.2. *There exists a set $S \subseteq \mathbb{Z}_p^n$ such that for all $k \in \mathbb{N}$, $\varphi_k(S) \subseteq \mathbb{Z}/p^k\mathbb{Z}$ is Kakeya, but S is a not a Kakeya set in $\mathbb{Z}_p^n$.*

Proof. First note that $\mathbb{Z}^n$ is dense in $\mathbb{Z}_p^n$, and take

$$S = \bigcup_{v \in \mathbb{Z}} \{\lambda v : \lambda \in \mathbb{Z}_p\}.$$

Consider $k \in \mathbb{N}$, and $v \in (\mathbb{Z}/p^k\mathbb{Z})^n$. Then note the interior of the set $v + p^k\mathbb{Z}_p^n$ is non-empty. And so pick some $v' \in \mathbb{Z} \cap v + p^k\mathbb{Z}_p^n$. Then there exists some $l_{v'} \subset S$. By the argument presented in Proposition 1, $\varphi_k(l_{v'})$ will be a line of direction v in $(\mathbb{Z}/p^k\mathbb{Z})^n$. Since v was arbitrary, the image will be contain a unit line segment for every in the direction v, $v \in \mathbb{Z}_p^n$. Hence for every k, the projection of S will be a Kakeya set in $\mathbb{Z}/p^k\mathbb{Z}$. However S contains no line in any non-integer direction. □

Intuitively one can see why this result would hold. $\mathbb{Z} \subsetneq \mathbb{Z}_p$, however by the definition $\mathbb{Z}/p^{k+1}\mathbb{Z}$, the projection from $\mathbb{Z}_p \to \mathbb{Z}/p^k\mathbb{Z}$ restricted to $\mathbb{Z}$ will still be surjective. And so integer directions should be enough to give a Kakeya set in $\mathbb{Z}/p^k\mathbb{Z}$. This construction holds for any dense $D \subseteq \mathbb{Z}_p^n$.

Throughout the literature there are different notions of Kakeya sets in $\mathbb{Z}_p^n$ and $(\mathbb{Z}/p^k\mathbb{Z})^n$. Some definitions require lines in all directions, while others only require lines in directions contained in $\mathbb{P}(\mathbb{Z}_P)^{n-1}$ and $\mathbb{P}(\mathbb{Z}/p^k\mathbb{Z})^{n-1}$ respectively. In this section we define the aforementioned objects, and prove the equivalence of Kakeya sets defined using either.

As in euclidean space, we define $S^{d-1}(\mathbb{Q}_p)$ to be the set of elements with norm 1 contained in $\mathbb{Q}_p^n$. By the definition of the norm we can see these are exactly the elements with at least one component of norm 1, and the rest having norm less than or equal to 1. It follows that

$$S^{d-1}(\mathbb{Q}_p) = S^{d-1}(\mathbb{Z}_p).$$

Recalling $\mathbb{Z}_p$ is the unit ball in $\mathbb{Q}_p$, we see that by the non-degeneracy and absolute homogenity of the norm $|\cdot|_p$, if $|x|_p = 1$, x^{-1} exists in $\mathbb{Q}_p$ and $|x^{-1}|_p = 1$. And so we can see $x^{-1} \in \mathbb{Z}_p$. Using this argument, we can equivlantly define $S^{d-1}(\mathbb{Z}_p)$ to be the set of x having one component invertible in $\mathbb{Z}_p$.

Somewhat naturally, we define

$$S^{d-1}(\mathbb{Z}/p^k\mathbb{Z}) = \{x \in (\mathbb{Z}/p^k\mathbb{Z})^d : x_i \text{ is a unit for some } 1 \leq i \leq d\}.$$

Analogous to $\mathbb{P}(\mathbb{R})^{n-1}$ we define

$$\mathbb{P}(\mathbb{Z}_p)^{n-1} = S^{n-1}(\mathbb{Z}_p)/\mathbb{Z}_p^\times$$
$$\mathbb{P}(\mathbb{Z}/p^k\mathbb{Z})^{n-1} = S^{n-1}(\mathbb{Z}/p^k\mathbb{Z})/(\mathbb{Z}/p^k\mathbb{Z})^\times,$$

where in both definitions, we quotient out by the relation

$$b \sim b' \iff b = \lambda b,\ \lambda \in R^{\times}.$$

For sake of clarity, we call a set $S \subset \mathbb{Z}_p^n$ $p-$Kakeya if S contains a unit line l_v for every $v \in S^{n-1}(\mathbb{Z}_p)$

Proposition 1.3. *A set $S \subset \mathbb{Z}_p^n$ is Kakeya if and only if it is $p-$Kakeya.*

Proof. We can see that if a set is Kakeya, it is automatically $p-$Kakeya. Now we prove the other implication.

Consider a $p-$Kakeya set S, and a direction $v \neq 0$ contained in $\mathbb{Z}_p^n \setminus S^{n-1}(\mathbb{Z}_p)$. Then

$$v = (v_1, \dots, v_n) = (p^{e_1}k_1, \dots p^{e_n}k_n),$$

where $(k_j, p) = 1$ and $e_j > 0$ for all $1 \leq j \leq n$. Then let $e_i = \min_{1 \leq j \leq n}\{e_j\}$. Then we can see

$$p^{e_i}k_i(p^{e_1-e_i}\frac{k_1}{k_i}, \dots, p^{e_{i-1}-e_i}\frac{k_{i-1}}{k_i}, 1, p^{e_{i+1}e_i}\frac{k_{i+1}}{k_i}, \dots, p^{e_n-e_i}\frac{k_n}{k_i}) = v.$$

Let

$$b = (p^{e_1-e_i}\frac{k_1}{k_i}, \dots, p^{e_{i-1}-e_i}\frac{k_{i-1}}{k_i}, 1, p^{e_{i+1}e_i}\frac{k_{i+1}}{k_i}, \dots, p^{e_n-e_i}\frac{k_n}{k_i}) \in S^{d-1}(\mathbb{Z}_p).$$

Then we can see any line in direction b will contain a line of direction v. And so any $p-$Kakeya set will contain a Kakeya set, and therefore is Kakeya. □

Corollary 1.4. *The Kakeya conjecture is equivalent to the proving every $p-$Kakeya set has full Hausdorff dimension.*

Remark 1.5. *One can use the same method to show the parallel result for Kakeya sets in $\mathbb{Z}/p^k\mathbb{Z}$.*

Now when working with $\mathbb{P}^{n-1}(\mathbb{Z}/p^k\mathbb{Z})$ we will have to pick a set of representatives that is consistent. Consider a equivalence class contained in projective space, $[x]$. Then let n_x be a natural such that the n_x^{th} coordinate of x is the first which is a unit. It is important to note that n_x is independent of our choice of representative of $[x]$. Then choose the unique scalar such that $\lambda x_{n_x} = 1$. Then this representative is unique for each class in $\mathbb{P}^{n-1}(\mathbb{Z}/p^k\mathbb{Z})^n$. Proceeding, when we work with projective space over these rings, we will treat directions as simply these representatives, unless for some unforeseen reason, it is easy to choose another.

Consider the following maps

$$\varphi_k : \mathbb{P}^{n-1}(\mathbb{Z}/p^k\mathbb{Z}) \to \mathbb{P}^{n-1}(\mathbb{Z}/p^{k-1}\mathbb{Z}),$$

which determined by $(x_1, \dots, 1 \dots, x_n) \mapsto (x_1, \dots, 1 \dots, x_n) \mod p^k$. Then we can see this map is indeed surjective.

And so we have the sequence

$$\dots \overset{\varphi_{k+2}}{\to} \mathbb{P}^{n-1}(\mathbb{Z}/p^{k+1}\mathbb{Z}) \overset{\varphi_{k+1}}{\to} \mathbb{P}^{n-1}(\mathbb{Z}/p^k\mathbb{Z}) \overset{\varphi_k}{\to} \mathbb{P}^{n-1}(\mathbb{Z}/p^{k-1}\mathbb{Z}) \overset{\varphi_{k-1}}{\to} \cdots .$$

One can verify that indeed $\mathbb{P}^{n-1}(\mathbb{Z}_p)$ is the inverse limit of the above sequence and further using the argument presented in Proposition 1.1, that if S is p-Kakeya as a subset of $\mathbb{Z}_p^n$, then all of it's projections are p-Kakeya in $(\mathbb{Z}/p^k\mathbb{Z})^n$.

1.4. **Acknowledgement.** The author was partially supported by an Undergraduate Student Research Award (USRA) and by Discovery Grant 22R80520 from the National Sciences and Engineering Research Council of Canada." The author would also like to acknowledge the advice of his supervisor, Dr. Izabella Łaba, and graduate mentor Paige Bright.

2. Arsovki's proof of p-adic Kakeya

2.1. **Theorem statements and Proof sketch.** For $A \subset \mathbb{Q}_P^n$ we define the Hausdorff s measure of A as

$$\mathcal{H}^s(A) = \lim_{\delta \searrow 0} \inf\{\sum_{i=1}^{\infty} |U_i|^s : \bigcup_{i=1}^{\infty} U_i \supset A,\ |U_i| \leq \delta\}.$$

And further we define the Hausdorff dimension as

$$\dim_{\mathcal{H}}(A) = \inf\{s : \mathcal{H}^s(A) < \infty\}.$$

This is well defined for every Borel subset of $\mathbb{Q}_p$. Arsovki's was able to prove the p-adic Kakeya conjecture with the following theorem.

Theorem 2.1. *Every Kakeya set $A \subset \mathbb{Q}_p^n$ satisfies $\dim_{\mathcal{H}}(A) = n$.*

We now give a proof sketch and the intermediate results Arsovski uses to prove Theorem 2.1.

Arsovski's proof of the p-adic Kakeya conjecture relies precisely on the idea that the projection of a Kakeya set contained in $\mathbb{Z}_p^n$ to $(\mathbb{Z}/p^k\mathbb{Z})^n$, is a Kakeya set. To show $\dim_{\mathcal{H}} S = n$, we show $\mathcal{H}^s(S) > 0$ for all $s < n$. To do this, we show that for every δ, $\mathcal{H}^s_\delta(S)$ is sufficiently large: and to accomplish this, he exploits the fact that the projective image of a *nice enough* covering of a Kakeya set in $\mathbb{Z}_p^n$ will form a Kakeya set in $(\mathbb{Z}/p^k\mathbb{Z})^n$. And so to lower bound the cardinality of any $\delta = p^{-k}$ covering on a Kakeya set in $\mathbb{Z}_p^n$, we find lowerbounds to the size of Kakeya sets in $\mathbb{Z}/p^k\mathbb{Z}$. This what we call as The Covering Theorem.

Theorem 2.2. *The Covering Theorem Let p be a prime number, and n, k be positive integers, then a Kakeya set in $\mathbb{Z}_P^n$ cannot be covered by fewer than*

$$\binom{p^k/pnk + n - 1}{n} \gtrsim \frac{p^{kn}}{3kn}.$$

To prove The Covering Theorem, take ζ to be a primitive p^kth root of unity, and lift our Kakeya set from $(\mathbb{Z}/p^k\mathbb{Z})^n$ to $(\mathbb{Q}_p[\zeta])^n$ via the isomorphism $\zeta^{\mathbb{Z}} \cong \mathbb{Z}/p^k\mathbb{Z}$. We then find a polynomial f, vanishing on the image of our Kakeya set in $(\mathbb{Q}_p[\zeta])^n$ of small degree, and examine it's reduction in $\mathbb{Z}/p^k\mathbb{Z}$. Heuristically it is at this point that Dvir's and Arsovki's proof follow in the same manner. For Dvir's proof of finite field Kakeya, he takes a polynomial of small degree vanishing on his Kakeya set, and shows the homogenization vanishes at the hyperspace at infinity, which is in bijection with the set of directions of the finite field vector space. This in turn forces the homogenous component of the original polynomial to vanish in every direction. Applying the Schwartz-Zippel Lemma yields a contradiction.

Here we are not so fortunate that we can show the homogeneous component of our f vanishes at every direction. However we can show it has large v_t-valuation at every $x \in \overline{C}^n$, which corresponds with the set of directions in $(\mathbb{Z}/p^k\mathbb{Z})^n$. Then

we apply the DVR Schwartz-Zippel Lemma which yields a contradiction in the same spirit as the original Schwartz-Zippel Lemma did in Dvir's paper. Now we proceed with Arsovski's proof, by formally introducing the The DVR Schwartz-Zippel Lemma and proving the Covering Theorem implies Theorem 2.1.

Lemma 2.3. *(Discrete Valutation Schwartz-Zippel). Let the coefficient of* $z_1^{m_1} z_2^{m_2} \cdots z_n^{m_n}$ *of* $f \in \overline{T}[z_1, \dots z_n]$ *be* $c \neq 0$*, and any monomimal that is larger in lexicographic order than* $z_1^{m_1} z_2^{m_2} \cdots z_n^{m_n}$ *be* 0*, and* $\gamma \in (0, 1]$*. Then the number of* $s \in \overline{C}^n$ *such that* $v_t(f(s)) \geq v_t(c) + \gamma n p^k$ *is at most* $pkp^{(n-1)k}(m_1 + \cdots m_n)/\gamma$*.*

2.2. **Proofs.** In this subsection, we prove first that the Theorem 2.2 proves Theorem 2.1. And then we prove Theorem 2.1 and Lemma 2.3.

Proof. **Theorem 2.2 implies Theorem 2.1**

To see this, we first show the implication of the Kakeya conjecture over $\mathbb{Z}_p^n$. Consider $\delta > 0$ and $0 \leq s < n$. Since we are working over $\mathbb{Z}_p^n$, $\delta = p^{-k}$ for some $k \in \mathbb{Z}$. From Theorem 2.2, we know we require $\gtrsim \frac{p^{nk}}{k^{3n}}$ δ balls to cover our set. And so

$$\mathcal{H}_\delta^s(S) \gtrsim \frac{p^{kn}}{k^{3n}} \cdot p^{-ks} = p^{k(n-s)} k^{-3n} \gtrsim_{n,p} 1.$$

Since this bound is uniform in k, when we take $\delta \searrow 0$, we see $\mathcal{H}^s(S) > 0$. Since $s < n$ was arbitrary, we see $\dim_{\mathcal{H}} S = n$. And so this resolves the case over $\mathbb{Z}_p^n$. To See how this applies to the case of $\mathbb{Q}_p^n$, we note that a Kakeya set is compact by definition, and hence can be covered in finitely many disjoint δ balls. Partition S by intersecting with these balls, then translate and superimpose them to form a Kakeya set $\tilde{S}$ in the unit ball $\mathbb{Z}_p^n$. We know $\mathcal{H}_\delta^s(\tilde{S}) > 0$ uniformly in δ and $s < n$. $\tilde{S}$ is the union and translation of finitely many subsets of S, and so at least one of those subsets must have $\mathcal{H}^s > 0$. This proves the desired result. □

Proof. **Proof of Theorem 2.2**

We will show the any kakeya set in $(\mathbb{Z}/p^k\mathbb{Z})^n$ has cardinality at least $\binom{p^k/pnk + n - 1}{n}$. Too see this suppose not and that there is some counter example S. Consider the set

$$S_c = \{(\zeta^{s_1}, \zeta^{s_2}, \dots, \zeta^{s_n}) \subset (\mathbb{Z}_p[\zeta])^n : (s_1, \dots, s_2) \in S\}.$$

As seen in Guth's book, there is a non-zero Polynomial $f \in \mathbb{Q}_p(\zeta)[z_1, z_2, \dots z_n]$ vanishing on S_c, with degree strictly less than p^k/pnk. We may take $f \in \mathbb{Z}_p[\zeta][z_1, z_2, \dots, z_n]$ since one can multiply f by $(1-\zeta)^m$ for the minimum m such that each coefficient of f has non-negative v_p-valuation: taking the minimum m insures at least one coefficient of f remains non-zero under the reduction via $\mathfrak{m}$, the maximal ideal $(\zeta - 1)$ in $\mathbb{Z}_p[\zeta]$. Proceeding with the proof, we can can see by the definition of f if we take l_v as defined previously, to be the line in direction v, contained in S, we see for all $v = (v_1, \dots, v_n) \in (\mathbb{Z}/p^k\mathbb{Z})^n$, $b_v = ((b_v)_1, \dots (b_v)_n)$, and $\lambda \in \mathbb{Z}/p^k\mathbb{Z}$, we have

$$f(\zeta^{(b_v)_1 + \lambda v_1}, \dots, \zeta^{(b_v)_n + \lambda v_n}) = f(\zeta^{(b_v)_1} \zeta^{[v_1]}, \dots, \zeta^{(b_v)_n} \zeta^{[v_n]}) = 0,$$

where we take $[v_k] = v_k \mod p^k$. We define a polynomial $g_v \in \mathbb{Z}_p[\zeta][z]$, indexed on v such that

$$g_v(z) = f(\zeta^{(b_v)_1} z^{\lambda[v_1]}, \dots, \zeta^{(b_v)_1} z^{\lambda[v_n]}).$$

Consequentially, we see g_v vanishes at ζ^λ for all $\lambda \in \mathbb{Z}/p^k\mathbb{Z}$, hence

$$\prod_{\lambda \in \mathbb{Z}/p^k\mathbb{Z}} (z - \zeta^\lambda) | \, g_v(z).$$

And so if we take $\overline{g_v}$ to be the reduction of g_v via $\mathfrak{m}$, we have

$$(z-1)^{p^k} = \prod_{\lambda \in \mathbb{Z}/p^k\mathbb{Z}} (z-1) | \, \overline{g_v}(z).$$

It follows that

$$v_t(\overline{g_v}((1+t))) = v_t(\overline{f}((1+t)^{[v_1]}, \ldots, (1+t)^{[v_2]})) \geq p^k, \tag{5}$$

where the λ's disappeared because they are mapped to 1 under the reduction by $\mathfrak{m}$. And so by (5), we see for all

$$s \in D = \{(1+t)^{[v_1]}, \ldots (1+t)^{[v_n]}\} \subseteq \overline{C}^n$$

, we have $v_t(\overline{f}(s)) \geq p^k$: importantly, $|D| = (p^k)^n$. f was constructed in such a way that it would have non-zero reduction in $\overline{T}[z_1, \ldots, z_n]$ and to be of degree at most $p^k/pnk < p^k$ with coefficients in $\mathbb{F}_p$. Noting Lemma 2.3, and since all of the coefficients of f have v_t-valuation equal to 0, taking $\gamma = 1/n$ we have

$$p^{kn} = |D| < (pkp^{k^{n-1}})/(p^k/pnk)(n) = p^{kn},$$

a contradiction, and so all Kakeya sets in $(\mathbb{Z}/p^k\mathbb{Z})^n$ have size at least

$$\binom{p^k/pnk + n - 1}{n} \gtrsim_{n,p} \frac{p^{kn}}{k^{3n}}.$$

□

Proof. **Proof of Lemma 2.3**

We will prove this inductivly, beginning with the base case $n = 1$. Suppose for sake of contradiction we have a $S \subseteq \overline{C}$ such that $|S| > pkm_1/\gamma$ where f has v_t valuation at least $v_t(c) + \gamma p^k$. Take

$$S = \{(1+t)^l : l \in L\},$$

such that $l \in \{0, 1, \ldots, p^k - 1\}$, $|L| = |S|$. Define d such tat

$$k \geq d = \lceil \log_p(k/\gamma) \rceil \geq 1.$$

Then we can see L modulo p^{k-d} has an image of size greater than

$$p^{-d}|L| = p^{\lceil \log_p(k/\gamma) \rceil} pkm_1/\gamma > m_1.$$

Choose an element from the pre-image of the coset under $\mod p^{k-d}$ to form the set $L_0 \subseteq L$. Then we can see that $|L_0| \geq m_1 + 1$, and the difference between any two elements in L_0 is not divisible by p^{k-d}. Let S_0 be the subset of S associated to L_0. By Lagrange interpolation in the field $\mathbb{F}_p(t)$, we see we have the Lagrange Polynomial generated by

$$\sum_{s \in S_0} \left(\prod_{u \in S_0 \setminus \{s\}} \frac{z-u}{s-u} \right) f(s) = f(z),$$

for $z \in S_0$. By construction, the polynomial has degree m_1. And so we may recover c by looking at the coefficient of maximum degree, indeed

$$c = \sum_{s \in S_0} \left(\prod_{u \in S_0 \setminus \{s\}} \frac{1}{s-u} \right) f(s).$$

By properties of the valuation v_t and the definition of S_0, we have

$$\begin{aligned} v_t(c) &\geq \min_{s \in S_0} \left(v_t(f(s)) + v_t \left(\prod_{u \in S_0 \setminus \{s\}} \frac{1}{s-u} \right) \right) \\ \implies 0 &\geq \min_{s \in S_0} \left(\gamma p^k + v_t \left(\prod_{u \in S_0 \setminus \{s\}} \frac{1}{s-u} \right) \right) \\ \implies \max_{s \in S_0} v_t &\left(\prod_{u \in S_0 \setminus \{s\}} (s-u) \right) \geq \gamma p^k \end{aligned}$$

And so there must exist some $s \in S_0$ such that

$$v_t \left(\prod_{u \in S_0 \setminus \{s\}} (s-u) \right) \geq \gamma p^k.$$

Then we take

$$L_0 = \{l_0, \ldots, l_{m_1}\},$$

where $(1+t)^{l_0} = s$. Take $l_i \neq l_0$ in L_0, then we see we have

$$v_t\left((1+t)^{l_i} - (1+t)^{l_0}\right) = v_t\left((1+t)^{l_0}((1+t)^{l_i - l_0} - 1)\right) = v_t\left((1+t)^{l_0}\right) + v_t\left((1+t)^{l_i-l_0} - 1)\right).$$

Since $v_t\left((1+t)^{l_0}\right) = 0$, we see we have

$$v_t\left((1+t)^{l_i} - (1+t)^{l_0}\right) = v_t\left((1+t)^{l_i-l_0} - 1)\right). \tag{6}$$

Since

$$(1+t)^{l_i - l_0} - 1 = \sum_{n=1}^{l_i - l_0} \binom{l_i - l_0}{n} t^n,$$

the valuation in (6) will be the least n such that $\binom{l_i - l_0}{n}$ is non-zero. One can deduce from Kummer's theorem for binomial coefficients $\mod p$ that $\binom{l}{w}$ is non-zero in $\mathbb{F}_p$ if and only if every p-adic digit of w is at most the corresponding p-adic digit of l. Note here that $p^{v_p(l_i - l_0)}$ is the largest power of p dividing $l_i - l_0$. Expanding $l_i - l_0$, one can see that for every $k < v_p(l_i - l_0)$, $l_i - l_0$ has a p-adic digit of 0, and and in the $v_p(l_i - l_0)^{th}$ place, a p-adic digit of at least 1. And since $p^{v_p(l_i - l_0)}$ has a p-adic digit of 0 for every place other than the $v_p(l_i - l_0)$, where it has a one; we can see $\binom{l_i - l_0}{p^{v_p(l_i - l_0)}}$ is the least non-zero (in terms of monomial degree) coefficient of $(1+t)^{l_i - l_0}$. Hence

$$\gamma p^k \leq \sum_{i=1}^{m_1} v_t((1+t)^{l_i - l_0} - 1) = \sum_{i=1}^{m_1} p^{v_p(l_i - l_0)}.$$

Hence

$$\gamma p^k \leq v_t\left(\prod_{u\in S_0\setminus\{s\}}(s-u)\right) = \sum_{i=1}^{m_1} v_t\left((1+t)^{l_i}-(1+t)^{l_0}\right)$$
$$= \sum_{i=1}^{m_1} p^{v_p(l_i-l_0)}.$$

Define

$$N_j = |\{l_i \in L_0 : v_p(l_i - l_0) \geq j\}|$$
$$r = \lceil \log_p(m_1)\rceil.$$

Then if we sum over the possible values of $v_p(l_i - l_0)$, and count multiplicities,

$$\gamma p^k \leq \sum_{i=1}^{m_1} p^{v_p(l_i-l_0)} = N_0 + \sum_{j=1}^{k-d-1} N_j(p^j - p^{j-1}). \tag{7}$$

And so we have

$$N_j \leq p^{k-d-j} \tag{8}$$
$$N_j \leq p^r, \tag{9}$$

where (8) follows from requiring the quotient by p^{k-d} to be injective on L_0. Hence we may bound (7) by

$$\gamma p^k \leq p^r + \sum_{j=1}^{k-d-r} p^r(p^j - p^{j-1}) + \sum_{j=k-d-r+1}^{k-d} p^{k-d-j}(p^j - p^{j-1}),$$

where we used (9) in the first summation, and (8) in the second summation. Proceeding, we have

$$p^r + \sum_{j=1}^{k-d-r} p^{k-d-j}(p^j - p^{j-1}) + \sum_{j=k-d-r+1}^{k-d} p^r(p^j - p^{j-1}) \leq p^{k-d} + \sum_{j=k-d-r+1}^{k-d} p^r(p^j - p^{j-1})$$
$$\leq p^{k-d} + rp^{k-d} = (r+1)p^{k-d}.$$

By assumption, we have $r + 1 \leq k$, hence

$$\gamma p^k < kp^{-\lceil \log_p(k/\gamma)\rceil} p^k \leq \gamma p^k.$$

This gives us a contradiction, so we must have $|S| \leq pkm_1/\gamma$. Now we proceed with the inductive argument. For $n > 1$, we write

$$f(z_1, \ldots, z_n) = z_1^{m_1} g(z_2, \ldots, z_n) + h(z_1, \ldots, z_n),$$

where h is of degree less than m_1 in z_1. We use the probabilistic method to find the probability that f has large valuation on a given point in $\overline{C}$. Since we are working over a finite probability space, this probability will give us the exact proportion of $\overline{C}^n$ where f has large v_t valuation, and further, multiplying by $|\overline{C}|^n$ we find the cardinality of the subset where f is large in v_t.

Forging ahead, we see define the events

$$F = v_t(f) \geq v_t(c) + \gamma n p^k$$
$$G_< = v_t(g) < v_t(c) + \gamma(n-1)p^k$$
$$G_\geq = v_t(g) \geq v_t(c) + \gamma(n-1)p^k.$$

Evaluating at$z_1, \dots z_n$, uniformly and independently over $\overline{C}$ at random, we see

$$\begin{aligned}\mathbb{P}(F) &= \mathbb{P}(F|G_<)\mathbb{P}(G_<) + \mathbb{P}(F|G_\geq)\mathbb{P}(G_\geq) \\ &\leq \mathbb{P}(F|G_<) + \mathbb{P}(G_\geq).\end{aligned}$$

We can see the event $G_{\geq 0}$ is a reduction to the case of $n-1$, and so we know $\mathbb{P}(G_\geq) \leq pk(m_2 + m_3 + \cdots + m_n)/\gamma p^k$.

Now considering the case $\mathbb{P}(F|G_<)$. We consider g now as a function in 1 variable $y \in \overline{C}^{n-1}$. Since we are working with conditional probabilities, we fix y' satisfying $G_<$. Now for a fixed y, if we assume F to also be true, we see

$$v_t(g(y)) < v_t(c) + \gamma(n-1)p^k \implies v_t(f) > v_t(g(y)) + \gamma p^k \implies v_t(f) \geq v_t(g(y)) + \gamma p^k.$$

The *event* of the inequality on the right of the above has probability $pkm_1/p^k\gamma$ by inductive assumption, and so

$$\mathbb{P}(F) \leq pkm_1/p^k\gamma + pk(m_2 + m_3 + \cdots + m_n)/\gamma p^k) = pk(m_1 + \cdots + m_n)/\gamma p^k.$$

Noting $|\overline{C}^n| = p^{nk}$, we prove the lemma.

□

Remark 2.4. *The result in* [Ars24] *is more general than Theorem 2.1, where Arsovski resolves the* $(\delta, \varepsilon)-$*Kakeya conjecture, which seeks bounds on the Hausdorff Dimension of fragmented Kakeya sets. Theorem 2.1 is the special case of the* $(\delta, \varepsilon)-$*Kakeya conjecture, where both* $\delta, \varepsilon = 1$*. The proofs are essentially the same, and the above exposition should lend the reader guidance on reading* [Ars24].

References

[Ars24] Bodan Arsovski, *The p-adic Kakeya conjecture*, J. Amer. Math. Soc. **37** (2024), no. 1, 69–80. MR 4654608

[Dvi09] Zeev Dvir, *On the size of Kakeya sets in finite fields*, J. Amer. Math. Soc. **22** (2009), no. 4, 1093–1097. MR 2525780

[EOT10] Jordan S. Ellenberg, Richard Oberlin, and Terence Tao, *The Kakeya set and maximal conjectures for algebraic varieties over finite fields*, Mathematika **56** (2010), no. 1, 1–25. MR 2604979

[Sal23] Alejo Salvatore, *The Kakeya conjecture on local fields of positive characteristic*, Mathematika **69** (2023), no. 1, 1–16. MR 4516796