Almost all non-archimedean Kakeya sets have measure zero

Xavier Caruso

Almost all non-archimedean Kakeya sets have measure zero

Xavier Caruso

August 8, 2016

Abstract

We study Kakeya sets over local non-archimedean fields with a probabilistic point of view: we define a probability measure on the set of Kakeya sets as above and prove that, according to this measure, almost all non-archimedean Kakeya sets are neglectable according to the Haar measure. We also discuss possible relations with the non-archimedean Kakeya conjecture.

Contents

At the beginning of the 20th century, Kakeya asks how small can be a subset of $\mathbb{R}^2$ obtained by rotating a needle of length 1 continuously through 360 degrees within it and returning to its original position. A set satisfying the above requirement is today known as a *Kakeya set* (or sometimes *Kakeya needle set*) in $\mathbb{R}^2$. In 1928, Besikovitch [2] constructed a subset of $\mathbb{R}^2$ with Lebesgue measure zero containing a unit length segment in each direction and derived from this the existence of Kakeya sets with arbitrary small positive Lebesgue measure. Since this, Kakeya sets have received much attention because they have connections with important questions in harmonic analysis. In particular, lower bounds on the size of a Kakeya set have been found: it

has been notably established that any Kakeya set in $\mathbb{R}^2$ must have Hausdorff dimension 2 (see [7, Theorem 2] for a short and elegant proof).

Kakeya's problem extends readily to higher dimensions: a *Besikovitch set* in $\mathbb{R}^d$ is a subset of $\mathbb{R}^d$ containing a unit length segment in each direction while a *Kakeya set* in $\mathbb{R}^d$ is a set obtained by rotating *continuously* a needle of length 1 is all directions (parametrized either by the $(d-1)$-dimensional sphere of the $(d-1)$-dimensional projective space). We refer to §1.1.1 for precise definitions. Kakeya sets in $\mathbb{R}^d$ with Lebesgue measure zero exist as well: the product of $\mathbb{R}^{d-2}$ by a neglectable Kakeya set in $\mathbb{R}^2$ makes the job. As for lower bounds, it has been proved by Wolff [9] that a Kakeya set in $\mathbb{R}^d$ has Hausdorff dimension $\geqslant \frac{d+2}{2}$. More recently Katz and Tao [8] improved the lower bound to $(2-\sqrt{2})(d-4)+3$. Experts however believe that these results are far from being optimal and actually conjecture that a Kakeya set in $\mathbb{R}^d$ should always have Hausdorff dimension d: this is the so-called Kakeya conjecture.

More recently Kakeya's problem was extended over other fields. The first case of interest was that of finite fields and was first considered in [9] by Wolff. Given a finite field $\mathbb{F}_q$, a *Besikovitch set* in $\mathbb{F}_q^d$ is a subset of $\mathbb{F}_q^d$ containing an affine line in each direction (note that the length condition has gone). Wolff wondered whether there exists a positive constant c_d depending only d such that any Besikovitch set in $\mathbb{F}_q^d$ contains at least $c_d \cdot q^d$ elements. A positive answer (leading to $c_d = \frac{1}{d!}$) was given by Dvir in his famous paper [4].

In [5], Ellenberg, Oberlin and Tao introduced Besikovitch sets over $\mathbb{F}_q[[t]]$ and asked whether there exists such a set whose Haar measure is zero. Dummit and Hablicsek addressed this question in [3] and gave to it a positive answer: they proved that, for all $d \geqslant 2$ and all finite field $\mathbb{F}_q$, there does exist a zero-measure Besikovitch set in $\mathbb{F}_q[[t]]^d$. They more generally defined Besikovitch sets over any ring R admitting a Haar measure μ for which $\mu(R)$ is finite and, for those rings, they stated a straightforward analogue of the Kakeya conjecture. Apart from $\mathbb{F}_q[[t]]$, an interesting ring R which falls within Dummit and Hablicsek's framework is $R = \mathbb{Z}_p$, the ring of p-adic integers. Dummit and Hablicsek then proved the Kakeya conjecture in dimension 2 for $R = \mathbb{F}_q[[t]]$ and $R = \mathbb{Z}_p$. The existence of zero-measure Besikovitch sets over $\mathbb{Z}_p$ was proved more recently by Fraser in [6].

The general aim of this paper is to study further the size of Kakeya/Besikovitch sets over non-archimedean local fields, *i.e.* $\mathbb{F}_q((t)) = \operatorname{Frac} \mathbb{F}_q[[t]]$, $\mathbb{Q}_p = \operatorname{Frac} \mathbb{Z}_p$ and their extensions. Our main originality is that we adopt a probabilistic point of view.

Let us describe more precisely our results. Let K be a fixed non-archimedean local field: similarly to $\mathbb{R}$, it is equipped with an absolute value which turns it into a topological locally compact field. It is thus equipped with a Haar measure μ giving a finite mass to any bounded subset. Since K is non-archimedean, the unit ball R of K is a subring of K (it is $\mathbb{F}_q[[t]]$ when $K = \mathbb{F}_q((t))$ and $\mathbb{Z}_p$ when $K = \mathbb{Q}_p$); we normalize μ so that $\mu(R) = 1$. In this setting, we provide a definition for Kakeya sets and Besikovitch sets[1] and endow the set of Kakeya sets included in R^d with a probability measure, giving this way a precise sense to the notion of random non-archimedean Kakeya set. Our main theorem is the following.

Theorem 1 (*cf* Corollary 1.19)**.** *Almost all Kakeya sets sitting in R^d have measure zero.*

We emphasize that the above theorem concerns actual Kakeya sets (and not Besikovitch sets). It then shows a clear dichotomy between the archimedean and the non-archimedean setup: in the former, Kakeya sets have necessarily positive measure (through it can be arbitrarily small) while, in the latter, almost all of them have measure zero.

We will deduce Theorem 1 from a much more accurate result providing an *exact* value for the average size of ε-neighbourhoods of Kakeya sets. Before stating (a weak version of) it, recall

[1] We emphasize that, similarly to the real setting, we make the difference between Kakeya and Besikovitch sets: basically, an additional continuity condition (corresponding to the fact that Kakeya's needle has to move continuously) is required for the former.

that the ε-neighbourhood of a subset $N \subset K^d$ consists of points whose distance to N is at most ε. Let q be the cardinality of the residue field of K, *i.e.* of $q = \operatorname{Card} R/\mathfrak{m}$ where $\mathfrak{m}$ is the open unit ball in K. When $R = \mathbb{F}_q((t))$, we can check that $\mathfrak{m} = t \cdot \mathbb{F}_q[[t]]$, so that q is indeed q. Similarly when $R = \mathbb{Q}_p$, we have $\mathfrak{m} = p\mathbb{Z}_p$ and q is equal to p.

Theorem 2 (*cf* Proposition 1.23)**.** *The expected value of the Haar measure of the ε-neighbourhood of a random Kakeya set sitting in R^d is equivalent to:*

$$\frac{2 \cdot (q^d - 1)}{(q-1)(q^{d-1} - 1)} \cdot \frac{1}{|\log_q \varepsilon|}$$

when ε goes to 0.

This refined version of Theorem 1 seems to us quite interesting because it underlines that, although Kakeya sets tend to be neglectable according to the Haar measure, they are not that small on average as reflected by the logarithmic decay with respect to ε. In particular Theorem 2 is in line with the non-archimedean Kakeya conjecture and might even be thought (with caution) as an average version of it.

Of course, beyond the mean, one would like to study further the random variables X_ε taking a random Kakeya set sitting in R^d to the Haar measure of its ε-neighbourhood. For instance, in the direction of the non-archimedean Kakeya conjecture, one may ask the following question: can one compute higher moments of the X_ε's (possibly extending the technics of this paper) and this way derive interesting informations about their minimum? In the real setting, results in related directions were obtained by Babichenko and al. [1, Theorem 1.6] in the 2-dimensional case.

This paper is organized as follows. In Section 1, we define non-archimedean Kakeya/Besikovitch sets together with the probability measure on the set of Kakeya sets we shall work with afterwards. We then state (without proof) our main theorem which is yet another refined version of Theorem 2. We then derive from it several corollaries. Section 2 provides a totally algebraic reformulation of the statements and results of Section 1. Its interest is twofold. First it allows us to extend to the torsion case the notion of Kakeya/Besikovitch sets together with the Kakeya conjecture. Second it positions the framework in which the forthcoming proof will all take place. The proof of our main theorem occupies Section 3. Section 4 contains numerical simulations whose objectives are, first, to exemplify our results and, second, to show the behaviour of the random variables X_ε's beyond their mean. Pictures of 2-adic Kakeya sets (in dimension 2 and 3) are also included.

1 Non-archimedean Kakeya sets

As just mentionned, the aim of this section is to introduce (random) Kakeya and Besikovitch sets over non-archimedean local fields (*cf* §§1.1–1.3) and then to state and comment on our main results (§1.4).

Throughout this paper, the letter K refers to a fixed discrete valuation field on which the valuation is denoted by val. We always assume that K is complete and that its residue field is finite. For our readers who are not familiar with non-archimedean geometry, we refer to Appendix A (page 30) for basic definitions and basic facts about valuation fields.

We fix in addition an integer $d \geqslant 2$: the dimension.

1.1 Besikovitch and Kakeya sets

1.1.1 The real setting

We first recall the definition and the basic properties of Kakeya sets and Besikovitch sets in the classical euclidean setting over $\mathbb{R}$. Let $\mathbb{S}^{d-1}(\mathbb{R})$ denote the unit sphere in $\mathbb{R}^d$. When $d = 2$,

Kakeya considers subsets in $\mathbb{R}^2$ that can be obtained by rotating a needle of length 1 continuously through 360 degrees within it and returning to its original position (or, depending on authors, by rotation a needle of length 1 continuously through 180 degrees within it and to its original position with reverse orientation). This notion can be extended to higher dimensions as follows.

Definition 1.1. A *Kakeya needle set* (or just a *Kakeya set*) in $\mathbb{R}^d$ is a subset N of $\mathbb{R}^d$ of the form:

$$N = \bigcup_{a \in \mathbb{S}^{d-1}(\mathbb{R})} \left[f(a) - \frac{a}{2},\ f(a) + \frac{a}{2} \right]$$

where $f : \mathbb{S}^{d-1}(\mathbb{R}) \to \mathbb{R}^d$ is a continuous function. (Here $[x, y]$ denotes the segment joining the points x and y.)

Remark 1.2. Optionally one may further require that the segments corresponding to the directions a and $-a$ coincide for all $a \in \mathbb{S}^{d-1}(\mathbb{R})$. This is equivalent to requiring that $f(a) = f(-a)$ for all $a \in \mathbb{S}^{d-1}(\mathbb{R})$, that is to requiring that f factors through the projective space $\mathbb{P}^{d-1}(R)$.

The natural question about Kakeya sets is the following: how small can be a Kakeya set? As a basic example, Kakeya first asks whether there exists a minimal area for Kakeya sets in $\mathbb{R}^2$. Besikovitch answers this question negatively and proves that there exists Kakeya sets (in any dimension) of arbitrary small measure. Besikovitch introduced a weaker version of Kakeya sets:

Definition 1.3. A *Besikovitch set* in $\mathbb{R}^d$ is a subset of $\mathbb{R}^d$ which contains a unit line segment in every direction.

Obviously a Kakeya set is a Besikovitch set. The converse is however not true. More precisely Besikovitch managed to construct Besikovitch sets of measure zero whereas one can easily show that a Kakeya set have necessarily positive measuree. The question now becomes: how small can be a Besikovitch set? A famous conjecture in this direction asks whether any Besikovitch set in $\mathbb{R}^d$ has Hausdorff dimension d? It is known to be true when $d \in \{1, 2\}$ but the question remains open for higher dimensions.

1.1.2 The non-archimedean setting

We now move to the non-archimedean setting: recall that we have fixed a complete discrete valuation field K. We denote by R its rings of integers and by k its residue field. We set $q = \mathrm{Card} k$. We fix a uniformizer $\pi \in K$ and always assume that the valuation on K is normalized so that $\mathrm{val}(\pi) = 1$. Let μ be the Haar measure on K normalized by $\mu(R) = 1$. In the sequel, we shall always work with the norm $|\cdot|$ on K defined by $|x| = q^{-\mathrm{val}(x)}$ ($x \in K$). We recall that it is compatible with the Haar measure μ on K in the sense that:

$$\mu(aE) = |a| \cdot \mu(E)$$

for all $a \in K$ and all measurable subset E of K.

We consider the K-vector space K^d and endow it with the infinite norm $\|\cdot\|_\infty$:

$$\|(x_1, \ldots, x_d)\|_\infty = \max_{1 \leqslant i \leqslant d} |x_i|.$$

Let $\mathbb{B}^d(K)$ (resp. $\mathbb{S}^{d-1}(K)$) denote the unit ball (resp. the unit sphere) in K^d. Clearly $\mathbb{B}^d(K) = R^d$ and $\mathbb{S}^{d-1}(K)$ consists of tuples $(x_1, \ldots, x_d) \in R^d$ containing at least one coordinate which is invertible in R. The latter condition is equivalent to the fact that the image of $(x_1, \ldots, x_d)$ in k^d does not vanish. This notably implies that $\mathbb{S}^{d-1}(K)$ has a large measure: precisely $\mu(\mathbb{S}^{d-1}(K)) = 1 - q^{-d}$. This contrasts with the real case.

Definition 1.4. Given $a \in \mathbb{S}^{d-1}(K)$, a *unit length segment* of direction a is a subset of K^d of the form $\{ta + b : t \in R\}$ for some $b \in R^d$.

A *Besikovitch set* in K^d is a subset of K^d containing a unit length segment in every direction.

Definition 1.5. A *Kakeya set* in K^d is a subset N of K^d of the form:

$$N = \bigcup_{a \in \mathbb{S}^{d-1}(K)} S_a \quad \text{with} \quad S_a = \{ta + f(a) \ : \ t \in R\}$$

where $f : \mathbb{S}^{d-1}(K) \to K^d$ is a continuous function.

It has been proved recently (see [6]) that Kakeya sets of measure zero exists in K^d! The main objective of this article is to prove that it is in fact the case for almost all Kakeya sets (in a sense that we will make precise later).

1.2 The projective space over K

Instead of working with $\mathbb{S}^{d-1}(K)$, it will be more convenient to use the projective space $\mathbb{P}^{d-1}(K)$. Recall that is defined as the set of lines in K^d passing through the origin. From an algebraic point of view, $P^{d-1}(K)$ is described as the quotient of $K^{d+1}\backslash\{0\}$ by the natural action by multiplication of $K^\star$. We use the standard notation $[a_1 : \cdots : a_d]$ to refer to the class in $\mathbb{P}^{d-1}(K)$ of a nonzero d-tuple $(a_1, \ldots, a_d)$ of elements of K. Geometrically $[a_1 : \cdots : a_d]$ corresponds to the line directed by the vector $(a_1, \ldots, a_d)$.

Definition 1.6. Let $a \in \mathbb{P}^{d-1}(K)$. A representative $(a_1, \ldots, a_d) \in K^d$ of a is *reduced* if it belongs to $\mathbb{S}^{d-1}(K)$.

Any element $a \in \mathbb{P}^{d-1}(K)$ admits a reduced representative: it can be obtained by dividing any representative $(a_1, \ldots, a_d)$ by a coordinate a_i for which $\|(a_1, \ldots, a_d)\|_\infty = |a_i|$. We note that two reduced representatives of a differ by multiplication by a scalar of norm 1, *i.e.* by an invertible element of R. As a consequence $\mathbb{P}^{d-1}(K)$ can alternatively be described as the quotient $\mathbb{S}^{d-1}(K)/R^\times$ where $R^\times$ stands for the group of invertible elements of R.

Canonical representatives. Although there is no canonical choice, we will need to define a particular set of representatives of the elements of $\mathbb{P}^{d-1}(K)$. The following lemma makes precise our convention.

Lemma 1.7. *Any element $a \in \mathbb{P}^{d-1}(K)$ admits a unique representative* $\mathrm{can}(a) = (a_1, \ldots, a_d) \in \mathbb{S}^{d-1}(K)$ *satisfying the following property: there exists an index* $\mathrm{piv}(a)$ *(uniquely determined) such that $a_{\mathrm{piv}(a)} = 1$ and $|a_i| < 1$ for all $i <$ piv(a).*

Proof. Let $(a'_1, \ldots, a'_d) \in \mathbb{S}^{d-1}(K)$ be any representative of a of norm 1. Define j as the smallest index i for which $|a'_i| = 1$. Then the vector $(a'_j)^{-1} \cdot (a'_1, \ldots, a'_d)$ satisfies the requirements of the lemma (with $\mathrm{piv}(a) = j$). The uniqueness is easy and left to the reader. □

Remark 1.8. The notation piv means "pivot".

The above construction defines two mappings piv : $\mathbb{P}^{d-1}(K) \to \{1, \ldots, d\}$ and can : $\mathbb{P}^{d-1}(K) \to \mathbb{S}^{d-1}(K)$ and the latter is a section of the projection $\mathbb{S}^{d-1}(K) \to \mathbb{P}^{d-1}(K)$. In the sequel, we shall often consider can as a function from $\mathbb{P}^{d-1}(K)$ to R^d.

A distance on $\mathbb{P}^{d-1}(K)$. Recall that we have seen that $\mathbb{P}^{d-1}(K) = \mathbb{S}^{d-1}(K)/R^\times$. The natural distance on $\mathbb{S}^{d-1}(K)$ (inherited from that on K^d) then defines a distance dist on $\mathbb{P}^{d-1}(K)$ by:

$$\mathrm{dist}(a,b) = \inf_{\hat{a},\hat{b}} |\hat{a} - \hat{b}|$$

where the infimum is taken over all representatives $\hat{a}$ and $\hat{b}$ of a and b respectively *lying in* $\mathbb{S}^{d-1}(K)$. One easily proves that dist takes its values in the set $\{0, 1, q^{-1}, q^{-2}, q^{-3}, \ldots\}$ and remains non-archimedean in the sense that

$$\mathrm{dist}(a,c) \leqslant \max\big(\mathrm{dist}(a,b), \mathrm{dist}(b,c)\big)$$

for all $a, b, c \in \mathbb{P}^{d-1}(K)$. Moreover $\mathbb{P}^{d-1}(K)$ equipped with the topology induced by dist is a compact space since there is a continuous map $\mathbb{S}^{d-1}(K) \to \mathbb{P}^{d-1}(K)$ with compact domain.

Proposition 1.9. *For all $a, b \in \mathbb{P}^{d-1}(K)$, we have:*

$$\mathrm{dist}(a,b) = |\mathrm{can}(a) - \mathrm{can}(b)|.$$

Proof. Clearly $\mathrm{dist}(a,b) \leqslant |\mathrm{can}(a) - \mathrm{can}(b)|$.

Hence, we just need to prove that $|\mathrm{can}(a) - \mathrm{can}(b)| \leqslant \mathrm{dist}(a,b)$. Let us first assume that $\mathrm{piv}(a) < \mathrm{piv}(b)$ and let $\hat{a} = (\hat{a}_1, \ldots, \hat{a}_d)$ and $\hat{b} = (\hat{b}_1, \ldots, \hat{b}_d)$ be two vectors in $\mathbb{S}^{d-1}(K)$ lifting a and b respectively. Set $j = \mathrm{piv}(a)$. The coordinate $\hat{a}_j$ has necessarily norm 1 while $|\hat{b}_j| < 1$. Therefore $|\hat{a}_j - \hat{b}_j|$ has norm 1 and $\mathrm{dist}(a,b)$ is equal to 1 as well. We conclude similarly when $\mathrm{piv}(a) > \mathrm{piv}(b)$.

Assume now that $\mathrm{piv}(a) = \mathrm{piv}(b)$. Set $j = \mathrm{piv}(a)$ and write $\mathrm{can}(a) = (a_1, \ldots, a_d)$ and $\mathrm{can}(b) = (b_1, \ldots, b_d)$, so that $a_j = b_j = 1$. We notice that any representative $\hat{a} \in \mathbb{S}^{d-1}(K)$ of a can be written $\hat{a} = \lambda \cdot \mathrm{can}(a)$ for some $\lambda \in R^\times$. Similarly we can write $\hat{b} = \mu \cdot \mathrm{can}(b)$ with $\mu \in R^\times$ for any representative $\hat{b}$ of b. We are then reduced to show that:

$$|\lambda \cdot \mathrm{can}(a) - \mu \cdot \mathrm{can}(b)| \geqslant |\mathrm{can}(a) - \mathrm{can}(b)| \tag{1}$$

for any λ and μ of norm 1. Set $r = |\mathrm{can}(a) - \mathrm{can}(b)|$. Observe that the j-th coordinate of the vector $\lambda \cdot \mathrm{can}(a) - \mu \cdot \mathrm{can}(b)$ is $\lambda - \mu$. The inequality (1) then holds if $|\lambda - \mu| \geqslant r$. Otherwise, let j' be an index such that $r = |a_{j'} - b_{j'}|$. For this particular j', write $\lambda a_{j'} - \mu b_{j'} = \lambda(a_{j'} - b_{j'}) + (\lambda - \mu) b_{j'}$. Moreover $|\lambda(a_{j'} - b_{j'})| = r$ while $|(\lambda - \mu) b_{j'}| \leqslant |\lambda - \mu| < r$. Thus $|\lambda a_{j'} - \mu b_{j'}| = r$ and (1) follows. □

Corollary 1.10. *Let $a, b \in \mathbb{P}^{d-1}(K)$. Let $(a_1, \ldots, a_d)$ and $(b_1, \ldots, b_d)$ in $\mathbb{S}^{d-1}(K)$ be some representatives of a and b respectively. Then* $\mathrm{dist}(a,b)$ *is the maximal norm of a 2×2 minor of the matrix*

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_d \\ b_1 & b_2 & \cdots & b_d \end{pmatrix}. \tag{2}$$

Proof. Since two representatives of a differ by multiplication by an element of norm 1, we may safely assume that $(a_1, \ldots, a_d) = \mathrm{can}(a)$. Similarly we assume that $(b_1, \ldots, b_d) = \mathrm{can}(b)$. If $\mathrm{piv}(a) \neq \mathrm{piv}(b)$, the determinant of the submatrix of (2) composed by the $\mathrm{piv}(a)$-th and $\mathrm{piv}(b)$-th columns is congruent to ± 1 modulo $\mathfrak{m}$. It thus has norm 1 and the corollary is proved in this case. Suppose now that $\mathrm{piv}(a) = \mathrm{piv}(b)$ and assume further for simplicity that they are equal to 1. The matrix (2) is then equivalent to:

$$\begin{pmatrix} 1 & a_2 & \cdots & a_d \\ 0 & b_2 - a_2 & \cdots & b_d - a_d \end{pmatrix}.$$

It is now clear that the maximal norm of a 2×2 minor is equal to $\|\mathrm{can}(b) - \mathrm{can}(a)\|_\infty$. The corollary then follows from Proposition 1.9. □

Projective Kakeya sets. Following Remark 1.2, one may define non-archimedean Kakeya sets using the projective space instead of the sphere.

Definition 1.11. A *projective Kakeya set* in K^d is a subset N of K^d of the form:

$$N = \bigcup_{a \in \mathbb{P}^{d-1}(K)} S_a \quad \text{with} \quad S_a = \big\{ t \cdot \mathrm{can}(a) + f(a) \ : \ t \in R \big\}$$

where $f : \mathbb{P}^{d-1}(K) \to K^d$ is a continuous function.

Proposition 1.12. *(a) Any projective Kakeya set is a Kakeya set.*

(b) Any Kakeya set contains a projective Kakeya set.

Proof. *(a)* The projective Kakeya set attached to a function $f : \mathbb{P}^{d-1}(K) \to K^d$ is equal to the Kakeya set attached to the compositum of f with the natural map $\mathbb{S}^{d-1}(K) \to \mathbb{P}^{d-1}(K)$ sending a vector to the line it generates.

(b) The Kakeya set attached to a function $f : \mathbb{S}^{d-1}(K) \to K^d$ contains the projective Kakeya set attached to $f \circ \mathrm{can}$. (Notice that can is continuous by Proposition 1.9.) □

In what follows, we will mostly work with projective Kakeya sets.

1.3 The universe

To each continuous function $f : \mathbb{P}^{d-1}(K) \to K^d$, we attach the (projective) Kakeya set $N(f)$ defined by:

$$N(f) = \bigcup_{a \in \mathbb{P}^{d-1}(K)} S_a(f) \quad \text{with} \quad S_a(f) = \big\{ t \cdot \mathrm{can}(a) + f(a) \ : \ t \in R \big\}.$$

Observe that $N(f)$ is compact. Indeed it appears as the image of the compact space $\mathbb{P}^{d-1}(K) \times R$ under the continuous mapping $(a, t) \mapsto t \cdot \mathrm{can}(a) + f(a)$. In particular, it is closed in K^d.

We would like to define random Kakeya sets, that is to turn N into a random variable on a certain probability space Ω. Of course, the whole set $C^0(\mathbb{P}^{d-1}(K), K^d)$ of all continuous functions $\mathbb{P}^{d-1}(K) \to K^d$ cannot be endowed with a nice probability measure because K itself cannot. We then need to restrict the codomain and a second natural candidate for Ω is then $C^0(\mathbb{P}^{d-1}(K), R^d)$. Unfortunately, we were not able to find a reasonable definition of a probability measure on it[2]. Nevertheless our intuition is that $C^0(\mathbb{P}^{d-1}(K), R^d)$ would be in any case too large to be relevant for the application we have in mind; indeed, we believe that any reasonable probability measure on it (if it exists) would eventually lead to $N(f) = R^d$ almost surely.

Instead, we propose to define Ω as the set of 1-Lipschitz functions from $\mathbb{P}^{d-1}(K)$ to R^d. The addition on R^d turns Ω into a commutative group. We endow Ω with the infinite norm $\| \cdot \|_\infty$ defined by the usual formula:

$$\|f\|_\infty = \sup_{a \in \mathbb{P}^{d-1}(K)} \|f(a)\|_\infty \quad (f \in \Omega).$$

The induced topology is then the topology of uniform convergence. The Arzelà–Ascoli theorem implies that Ω is compact. It is thus endowed with its Haar measure, which is a probability measure.

[2] By the way, it would be interesting to define a nice probability measure on $C^0(R, R^d)$ and then investigate what could be the non-archimedean analogue of the Brownian motion.

Remark 1.13. More generally, one could also have considered r-Lipschitz functions $\mathbb{P}^{d-1}(K) \to R^d$ for some positive *fixed* real number r. This would actually lead to similar qualitative behaviours (although of course precise numerical values would differ). Moreover the technics introduced in this paper extends more or less easily to the general case — and the reader is invited to write it down as an exercise! We have chosen to restrict ourselves to the case $r = 1$ in order to avoid many technicalities and be able to focus on the heart of the argumentation.

In the rest of this paragraph (which can be skipped on first reading), we give a more explicit description of the universe Ω as a probability space. We fix a complete set of representatives of classes modulo $\mathfrak{m}$ and call it S. We denote by S_n the set of elements that can be written as

$$s_0 + s_1\pi + s_2\pi^2 + \cdots + s_{n-1}\pi^{n-1}$$

where the s_i's lie in S and we recall that $\pi \in R$ denotes a fixed uniformizer of K. Then S_n forms a complete set of representatives of classes modulo $\mathfrak{m}^n$. Observe in particular that $S_1 = S$.
We now introduce special "step functions" that will be useful for approximating functions in Ω.

Definition 1.14. For a positive integer n, let Ω_n^{an} denote the subset of Ω consisting of functions taking their values in S_n and which are constant of each closed ball of radius q^{-n}.

Remark 1.15. The exponent "an" refers to "analytic" and recalls that we are here giving an analytic description of Ω. Later on, in §2.3, we will revisit the constructions of this subsection in a more algebraic fashion and notably define an algebraic version of Ω_n^{an}.

Note that $\Omega_n^{\mathrm{an}} \subset \Omega_m^{\mathrm{an}}$ as soon as $n \leqslant m$. Moreover Ω_n^{an} is a finite set. Indeed S_n is finite and the set of closed balls of radius q^{-n} is in bijection with $\mathbb{P}^{d-1}(S_n)$ and thus is finite as well.

Proposition 1.16. *Given $n \geqslant 1$ and $f \in \Omega$ there exists a unique function $\psi_n^{\mathrm{an}}(f) \in \Omega_n^{\mathrm{an}}$ such that:*

$$\|f - \psi_n^{\mathrm{an}}(f)\|_\infty \leqslant q^{-n}.$$

Proof. Let $a \in \mathbb{P}^{d-1}(K)$. Set $f(a) = (x_1, \ldots, x_d)$ where the x_i's lie in R. For any i, let y_i be the unique element of S_n which is congruent to x_i modulo $\mathfrak{m}^n$. We define $\psi_n^{\mathrm{an}}(f)(a) = (y_1, \ldots, y_d)$. Remembering that $\|x-y\|_\infty \leqslant q^{-n}$ (with $x, y \in R^d$) if and only if x and y are congruent modulo $\mathfrak{m}^n$ coordinate-wise, we deduce that $\psi_n^{\mathrm{an}}(f)(a)$ is the unique element of S_n with the property that:

$$\|f(a) - \psi_n^{\mathrm{an}}(f)(a)\|_\infty \leqslant q^{-n}.$$

This construction then defines a function $\psi_n^{\mathrm{an}}(f) : \mathbb{P}^{d-1}(K) \to S_n$ such that $\|f-\psi_n^{\mathrm{an}}(f)\|_\infty \leqslant q^{-n}$. and we have shown in addition that $\psi_n^{\mathrm{an}}(f)$ is the unique function satisfying the above condition.

It then remains to prove that $\psi_n^{\mathrm{an}}(f) \in \Omega_n^{\mathrm{an}}$, *i.e.* that (1) $\psi_n^{\mathrm{an}}(f)$ is constant on each closed ball of radius q^{-n} and (2) is 1-Lipschitz. Let us first prove (1). Let $a, b \in \mathbb{P}^{d-1}(K)$ such that $\mathrm{dist}(a, b) \leqslant q^{-n}$. By the Lipschitz condition, we get $\|f(a) - f(b)\|_\infty \leqslant q^{-n}$ as well. In other words, $f(a)$ and $f(b)$ are congruent modulo $\mathfrak{m}^n$ coordinate-wise. By construction of $\psi_n^{\mathrm{an}}(f)$, we then derive that $\psi_n^{\mathrm{an}}(f)(a) = \psi_n^{\mathrm{an}}(f)(b)$ and (1) is proved.

We now move to (2). Pick $a, b \in \mathbb{P}^{d-1}(K)$. If $\mathrm{dist}(a, b) \leqslant q^{-n}$, then we have just seen that $\psi_n^{\mathrm{an}}(a) = \psi_n^{\mathrm{an}}(b)$. Consequently we clearly have $\|\psi_n^{\mathrm{an}}(a) - \psi_n^{\mathrm{an}}(b)\|_\infty \leqslant \mathrm{dist}(a, b)$. Otherwise, we can write:

$$\|\psi_n^{\mathrm{an}}(a) - \psi_n^{\mathrm{an}}(b)\|_\infty \leqslant \max\big(\|\psi_n^{\mathrm{an}}(a) - f(a)\|_\infty, \|f(a) - f(b)\|_\infty, \|\psi_n^{\mathrm{an}}(b) - f(b)\|_\infty\big).$$

Now remark that $\|\psi_n^{\mathrm{an}}(a) - f(a)\|_\infty$ and $\|\psi_n^{\mathrm{an}}(b) - f(b)\|_\infty$ are both not greater than q^{-n} by construction. They are then *a fortiori* both less than $\mathrm{dist}(a, b)$ by assumption. Moreover since f is 1-Lipschitz, we have $\|f(a) - f(b)\|_\infty \leqslant \mathrm{dist}(a, b)$. Putting all together we finally derive $\|\psi_n^{\mathrm{an}}(a) - \psi_n^{\mathrm{an}}(b)\|_\infty \leqslant \mathrm{dist}(a, b)$ as wanted. □

Proposition 1.16 just above shows that the union of all Ω_n^{an} are dense in Ω. Moreover, there is a projection $\psi_n^{\mathrm{an}} : \Omega \to \Omega_n^{\mathrm{an}}$ for any $n \geqslant 1$. For $m \geqslant n$, let $\psi_{m,n}^{\mathrm{an}} : \Omega_m^{\mathrm{an}} \to \Omega_n^{\mathrm{an}}$ denote the restriction of ψ_n^{an} to Ω_m^{an}.

Proposition 1.17. *Let n be a positive integer and $f_n \in \Omega_n^{\mathrm{an}}$. The fibre of $\psi_{n+1,n}^{\mathrm{an}}$ over f_n consists exactly of functions of the shape:*

$$f_n + \pi^n g$$

where $g : \mathbb{P}^{d-1}(K) \to S_1^d$ is any function which is constant on each closed ball of radius $q^{-(n+1)}$.

Proof. We notice first that any function f_{n+1} of the form $f_n + \pi^n g$ clearly lies in $\Omega_{n+1}^{\mathrm{an}}$ and maps to f_n under $\psi_{n+1,n}^{\mathrm{an}}$ because

$$\|f_{n+1} - f_n\|_\infty = \|\pi^n g\|_\infty = q^{-n} \cdot \|g\|_\infty \leqslant q^{-n}.$$

Pick now $f_{n+1} \in \Omega_{n+1}^{\mathrm{an}}$ such that $\psi_{n+1,n}^{\mathrm{an}}(f_{n+1}) = f_n$. Then $\|f_{n+1} - f_n\|_\infty \leqslant q^{-n}$, meaning that f_{n+1} is congruent to f_n modulo $\mathfrak{m}^n$, *i.e.* that there exists a function $g : \mathbb{P}^{d-1}(K) \to R^d$ such that $f_{n+1} = f_n + \pi^n g$. Looking at the shape of the elements of S_n and S_{n+1}, we deduce that g must take its values in S_1^d. □

Let G^{an} be the set of functions $\mathbb{P}^{d-1}(K) \to S_1^d$ which are constant on each closed ball of radius q^{-i}. Applying repeatedly Proposition 1.17, we find that the functions in Ω_n^{an} are exactly those that can be written as $\sum_{i=1}^n g_i \pi^{i-1}$ with $g_i \in G_i^{\mathrm{an}}$. Moreover this writing is unique. Passing to the limit, we find that the functions in Ω can all be written uniquely as an inifinite converging sum $\sum_{i=1}^\infty g_i \pi^{i-1}$ with $g_i \in G_i^{\mathrm{an}}$ as above. In other words there is a bijection:

$$\begin{array}{ccc} \prod_{i=1}^\infty G_i^{\mathrm{an}} & \xrightarrow{\sim} & \Omega \\ (g_1, g_2, \ldots) & \mapsto & \sum_{i=1}^\infty g_i \pi^{i-1} \end{array} \tag{3}$$

Furthermore, if we endow G_i^{an} with the discrete topology, the above bijection is an homeomorphism. Since the G_i^{an}'s are all finite, we recover that Ω is compact. Finally, the Haar measure on Ω can be described as follows: it corresponds under the bijection (3) to the product measure on $\prod_{i=1}^\infty G_i^{\mathrm{an}}$ where each factor is endowed with the uniform distribution (it may be seen directly but it is also a consequence of Proposition 2.16 below). In other words picking a random element in Ω amounts to picking each "coordinate" g_i in G_i^{an} uniformly and independantly.

1.4 Average size of a random Kakeya set

For $f \in \Omega$, recall that we have defined a Kakeya set $N(f)$. Recall that $N(f)$ is closed and remark in addition that $N(f) \subset R^d$ since f takes its values in R^d. Given an auxiliary positive integer n, we introduce the (q^{-n})-neighbourhood $N_n(f)$ of $N(f)$, that is:

$$N_n(f) = \left\{ x \in R^d \;\middle|\; \inf_{y \in N(f)} |x - y| \leqslant q^{-n} \right\}$$

and let $X_n(f)$ denote its measure. This defines a collection of random variables $X_n : \Omega \to \mathbb{N}$ that measures the size of $N(f)$. Our main theorem provides an explicit formula for their mean. Before stating it, let us recall that q denotes the cardinality of the residue field k.

Theorem 1.18. *Let $(u_n)_{n \geqslant 0}$ be the sequence defined by the recurrence:*

$$u_0 = 1 \quad ; \quad u_{n+1} = 1 - \left(1 - \frac{u_n}{q^{d-1}}\right)^{q^{d-1}}.$$

Then:

$$\mathbb{E}[X_n] = 1 - (1 - u_n)^{1 + q^{-1} + \cdots + q^{-(d-1)}}.$$

This theorem will be proven in Section 3. For now, we would like to comment on it a bit and derive some corollaries. The first one justifies the title of this article.

Corollary 1.19. *The set $N(f)$ has measure zero almost surely.*

Proof. The sequence $(X_n)_{n\geqslant 1}$ defines a nonincreasing sequence of bounded random variables and therefore converges when n goes to infinity. Set $X = \lim_{n\to\infty} X_n$. Noting that the X_n's are all bounded by 1, it follows from the dominated convergence theorem that $\mathbb{E}[X] = \lim_{n\to\infty} \mathbb{E}[X_n]$. Observing that

$$\forall x > 0, \quad \left(1 - \frac{x}{q^{d-1}}\right)^{q^{d-1}} > 1 - x$$

we deduce that the sequence $(u_n)_{n\geqslant 1}$ of Theorem 1.18 is decreasing and therefore converges. Furthermore, its limit is necessarily 0. This implies that $\mathbb{E}[X] = 0$. Since $X \geqslant 0$, we deduce that $X = 0$ almost surely. Moreover, for a fixed $f \in \Omega$, $X(f)$ is the volume of the $\bigcap_n N_n(f)$ which is equal to $N(f)$ because the latter is closed. Therefore $N(f)$ has measure zero almost surely. □

Around Kakeya conjecture. In the real setting, the classical Kakeya conjecture asks whether any Besikovitch set in $\mathbb{R}^d$ has maximal Hausdorff dimension. In the non-archimedean setting, the analogue of the Kakeya conjecture can be formulated as follows.

Conjecture 1.20 (Kakeya Conjecture)**.** *Let B be a bounded Besikovitch set in K^d. For any positive integer n, let B_n be the (q^{-n})-neighbourhood of B:*

$$B_n = \left\{ x \in K^d \;\middle|\; \inf_{y\in B} |x - y| \leqslant q^{-n} \right\}$$

and μ_n be its Haar measure. Then $|\log\ \mu_n| = o(n)$ when n goes to infinity.

Remark 1.21. Using the fact the the balls of radius q^{-n} are pairwise disjoint in the non-archimedean setting, one derives that the minimal number of balls needed to cover B_n is $q^{nd}\mu_n$. The Hausdorff dimension of B is then defined by the limit of the sequence:

$$\frac{\log(q^{nd}\mu_n)}{n\ \log q} = d + \frac{\log\ \mu_n}{n\ \log q}$$

and thus is equal to d if and only if $|\log\ \mu_n| = o(n)$.

The non-archimedean Kakeya conjecture is known in dimension 2 thanks to the works of Dummit and Hablicsek [3, Theorem 1.2]. It is contrariwise widely open in higher dimensions (to our knowledege). Before going further, we state a slight improvement of Dummit and Hablicsek's result.

Theorem 1.22. *Let B be a bounded Besikovitch set in K^2. For any positive integer n, let B_n be the (q^{-n})-neighbourhood of B and let μ_n be its Haar measure. Then:*

$$\mu_n \geqslant \frac{1}{\frac{q-1}{q+1}\, n + 1}.$$

We postpone the proof of this theorem to §3.1 because it will be convenient to write it down using the algebraic framework on which we will elaborate later on. Instead let us go back to random non-archimedean Kakeya sets. Studying further the asymptotic behaviour of the sequence (u_n) defined in Theorem 1.18, one can determine an equivalent of the mean of the random variable X_n.

Proposition 1.23. *We have the equivalent:*

$$\mathbb{E}[X_n] \sim \frac{2 \cdot (q^d - 1)}{(q-1)(q^{d-1} - 1)} \cdot \frac{1}{n}$$

when n goes to infinity.

Proof. A simple computation shows that $u_{n+1} = u_n - c \cdot u_n^2 + o(u_n^2)$ with $c = \frac{q^{d-1}-1}{2q^{d-1}}$. For $n \geqslant 0$, define $w_n = \frac{1}{u_n}$, so that we have:

$$w_{n+1} - w_n = \frac{u_n - u_{n+1}}{u_n u_{n+1}} = \frac{cu_n^2 + o(u_n^2)}{u_n u_{n+1}} = \frac{cu_n^2 + o(u_n^2)}{u_n^2 - cu_n^3 + o(u_n^3)} = c + o(1).$$

Thus $w_n \sim cn$ and $u_n \sim \frac{1}{cn}$. The claimed result then follows from Theorem 1.18. □

It follows from Proposition 1.23 that:

$$-\log \mathbb{E}[X_n] = \log n + \log\left(\frac{(q-1)(q^{d-1}-1)}{2 \cdot (q^d - 1)}\right) + o(1).$$

In particular $|\log \mathbb{E}[X_n]| = o(n)$. Proposition 1.23 then might be thought as an *average* strong version of Conjecture 1.20. We remark in addition that the lower bound given by Theorem 1.22 is rather close to the expected value of X_n provided by Proposition 1.23: roughly the differ by a factor 2. We then expect the random variables X_n to be quite concentrated around their mean. We refer to Section 4 for numerical simulations supporting further this expectation.

2 Algebraic reformulation

The aim of this section is merely to rephrase the constructions, theorems and conjectures of Section 1 in the more abstract framework of algebra in which the proofs of Section 3 will be written.

For any positive integer n, set $R_n = R/\mathfrak{m}^n = R/\pi^n R$. It is a finite ring of cardinality q^n. Concretely if $S \subset R$ is a set of representatives of the quotient $R/\mathfrak{m} = k$, any class in R_n is uniquely represented by an element of the shape:

$$s_0 + s_1\pi + s_2\pi^2 + \cdots + s_{n-1}\pi^{n-1} \tag{4}$$

where the s_i's lie in S and we recall that π is a fixed uniformizer of R (that is a generator of $\mathfrak{m}$). Let $p_n : R^d \to R_n^d$ denote the canonical projection taking a tuple $(x_1, \ldots, x_d)$ to its class modulo $\mathfrak{m}^n$ (obtained by taking the class modulo $\mathfrak{m}^n$ of each coordinate separatedly).

Proposition 2.1. *Let E be a subset of R^d and E_n denote its (q^{-n})-neighbourhood, that is:*

$$E_n = \left\{ x \in K^d \;\middle|\; \inf_{y \in E} |x - y| \leqslant q^{-n} \right\}.$$

Then $E_n = p_n^{-1}(p_n(E))$ and the volume of E_n is:

$$\mu(E_n) = q^{-nd} \cdot \text{Card}\, p_n(E).$$

Proof. Notice that, given $x = (x_1, \ldots, x_d)$ and $y = (y_1, \ldots, y_d)$ in R^d, $\|x - y\|_\infty \leqslant q^{-n}$ if and only if $x_i \equiv y_i \pmod{\mathfrak{m}^n}$ for all i. As a consequence, the closed ball of radius q^{-n} and centre x is exactly $B_x = p_n^{-1}(p_n(x))$. This gives the first assertion of the proposition.

To establish the second assertion, it is enough to prove that each B_x has volume q^{-nd}. Observe that $B_x = B_y + (y - x)$. By the properties of the Haar measure, we then must have $\mu(B_x) = \mu(B_y)$. Finally we note that the B_x's are pairwise distinct and cover the whole space R^d when x runs over the tuples $(x_1, \ldots, x_d)$ where each x_i has the shape (4). Since there are q^{nd} such elements, we are done. □

2.1 The torsion Kakeya Conjecture

Recall that the sphere $\mathbb{S}^{d-1}(K)$ — or equivalenty $\mathbb{S}^{d-1}(R)$ — consists of tuples $(x_1, \dots, x_d) \in R^d$ having one invertible coordinate. This algebraic description makes sense for more general rings and allows us to define $\mathbb{S}^{d-1}(R_n)$ as the set of tuples $(x_1, \dots, x_d) \in R_n^d$ for which x_i is invertible in R_n for some i. Note that an element $x \in R_n$ is invertible if and only if its image in $R/\mathfrak{m} = k$ does not vanish, *i.e.* if and only if $x \not\equiv 0 \pmod{\mathfrak{m}}$.

We can now extend the definition of a Besikovitch set (*cf* Definition 1.4) and the Kakeya conjecture (*cf* Conjecture 1.20) over R_n.

Definition 2.2. Let n be a positive integer and let $\ell \in [\![0, n]\!]$. Given $a \in \mathbb{S}^{d-1}(R_n)$, a *segment of length* $q^{-\ell}$ of direction a is a subset of R_n^d of the form $\{ta + b : t \in \mathfrak{m}^\ell\}$ for some $b \in R_n^d$.
A *ℓ-Besikovitch set* in R_n^d is a subset of R_n^d containing a segment of length $q^{-\ell}$ in every direction.

Conjecture 2.3 (Torsion Kakeya Conjecture)**.** *There exists a sequence*[3] *of positive real numbers $(\varepsilon_n)_{n\geqslant 1}$ converging to 0 satisfying the following property: for any $n \geqslant 1$, any $\ell \in [\![0, n]\!]$ and any ℓ-Besikovitch set B in R_n^d, we have:*

$$\log_q \text{Card } B \geqslant n \cdot (d - \varepsilon_n)$$

where $\log_q$ stands for the logarithm in q-basis.

Theorem 1.22 admits an analogue in the torsion case as well; it can be formulated as follows.

Theorem 2.4. *For any positive integer n, any integer $\ell \in [\![0, n]\!]$ and any ℓ-Besikovitch set B in R_n^2, we have:*

$$\text{Card } B \geqslant q^{2(n-\ell)} \cdot \frac{1}{\frac{q-1}{q+1}\, n + 1}.$$

Again, we postpone the proof of this theorem to §3.1. Let us however notice here that it implies Theorem 1.22. Indeed, let B be a bounded Besikovitch set in R^2. Let ℓ be an integer for which B is included in the ball of centre 0 and radius q^ℓ. Then $\pi^\ell B \subset R$ and $p_n(\pi^{-\ell} B)$ is a ℓ-Besikovitch set in R_n^2. Therefore, according to the above theorem, one must have:

$$\text{Card } p_n(\pi^\ell B) > q^{2(n-\ell)} \cdot \frac{1}{\frac{q-1}{q+1}\, n + 1}.$$

Combining this with Proposition 2.1, we get the result.

2.2 Algebraic description of the projective space

The projective space $\mathbb{P}^{d-1}(K)$ — considered as a metric space — which has been introduced in §1.2 admits an algebraic description as well. In order to explain it, let us first recall that $\mathbb{P}^{d-1}(K) = \mathbb{S}^{d-1}(K)/R^\times$. This allows us to define a specialization map:

$$\begin{array}{rccc} \text{sp}_1 : & \mathbb{P}^{d-1}(K) & \longrightarrow & \mathbb{P}^{d-1}(k) \\ & [a_1 : \cdots : a_d] & \mapsto & [\bar{a}_1 : \cdots : \bar{a}_d] \end{array}$$

where $(a_1, \dots, a_d) \in \mathbb{S}^{d-1}(K)$ and $\bar{a}_i$ denotes the image of a_i in k. With these notations, the index $\text{piv}(a)$ (defined in §1.2) appears as the first index of a non-vanishing coordinate of $\text{sp}_1(a)$. We notice that the mapping sp_1 is surjective and that the preimage of any point in $\mathbb{P}^{d-1}(k)$ is in bijection with R^{d-1}. Indeed let us define $\text{piv}_1(\bar{a})$ as the smallest index of a non-vanishing coordinate of $\bar{a}$ and consider the unique representative $(\bar{a}_1, \dots, \bar{a}_d)$ of a such that $\bar{a}_{\text{piv}_1(\bar{a})} = 1$.

[3] This sequence may a priori depend on K, d and ℓ.

Choose moreover a lifting $a \in R^d$ of $(\bar{a}_1, \dots, \bar{a}_d)$ whose $\mathrm{piv}_1(\bar{a})$-th coordinate is 1. We can then define a bijection:

$$\begin{array}{ccc} H_{\mathrm{piv}_1(\bar{a})} & \longrightarrow & \mathrm{sp}_1^{-1}(\bar{a}) \\ x & \mapsto & [a + \pi x] \end{array}$$

where $H_{\mathrm{piv}_1(\bar{a})}$ denote the coordinate hyperplane of R^d defined by the equation $x_{\mathrm{piv}_n(\bar{a})} = 0$. We remark moreover that the vectors $a + \pi x$ appearing above are all canonical representatives.

More generally, for any positive integer n, we define:

$$\mathbb{P}^{d-1}(R_n) = \mathbb{S}^{d-1}(R_n)/R_n^\times$$

Given $a \in \mathbb{P}^{d-1}(R_n)$, let $\mathrm{piv}_n(a)$ be the index of the first invertible coordinate of a and $\mathrm{can}_n(a) \in \mathbb{S}^{d-1}(R_n)$ be the unique representative of a whose $\mathrm{piv}_n(a)$-th coordinate is 1. We have a specialization map of level n:

$$\begin{array}{rccc} \mathrm{sp}_n : & \mathbb{P}^{d-1}(K) & \longrightarrow & \mathbb{P}^{d-1}(R_n) \\ & [a_1 : \cdots : a_d] & \mapsto & [a_1 \bmod \mathfrak{m}^n : \cdots : a_d \bmod \mathfrak{m}^n]. \end{array}$$

Again sp_n is surjective and the preimage of any point $a \in \mathbb{P}^{d-1}(R_n)$ is isomorphic to R^{d-1} *via*

$$\begin{array}{ccc} H_{\mathrm{piv}_n(a)} & \longrightarrow & \mathrm{sp}_n^{-1}(a) \\ x & \mapsto & [\mathrm{can}_n(a) + \pi^n x] \end{array}$$

Similarly, given a second integer $m \geqslant n$, the reduction modulo $\mathfrak{m}^n$ defines a map $\mathrm{sp}_{m,n} : \mathbb{P}^{d-1}(R_m) \to \mathbb{P}^{d-1}(R_n)$. This map is surjective and its fibres are all in bijection with R_{m-n}^{d-1}. It notably follows from this that:

$$\mathrm{Card}\, \mathbb{P}^{d-1}(R_n) = q^{(d-1)(n-1)} \cdot \frac{q^d - 1}{q - 1}. \tag{5}$$

Proposition 2.5. *The collection of applications* sp_n *induces a bijection:*

$$\mathrm{sp} : \mathbb{P}^{d-1}(K) \longrightarrow \varprojlim_n \mathbb{P}^{d-1}(R_n)$$

where the codomain is by definition the set of all sequences $(x_n)_{n\geqslant 1}$ *with* $x_n \in \mathbb{P}^{d-1}(R_n)$ *and* $\mathrm{sp}_{n+1,n}(x_{n+1}) = x_n$ *for all* n.

Proof. We define a function φ in the opposite direction as follows. Let $(x_n)_{n\geqslant 1}$ be a sequence in $\varprojlim_n \mathbb{P}^{d-1}(R_n)$. The compatibility condition implies that $\mathrm{piv}_n(x_n)$ is constant and that $\mathrm{can}_n(x_n)$ is the reduction modulo $\mathfrak{m}^n$ of $\mathrm{can}_{n+1}(x_{n+1})$. Therefore the sequence $(\mathrm{can}_n(x_n))_{n\geqslant 1}$ defines an element $x \in R^d$. The $\mathrm{piv}_1(x_1)$-th coordinate of x is 1, so that $x \in \mathbb{S}^{d-1}(K)$. Let define $\varphi((x_n)_{n\geqslant 1})$ as the class of x in the projective space $\mathbb{P}^{d-1}(K)$. It is clear that $\varphi \circ \mathrm{sp}$ and $\mathrm{sp} \circ \varphi$ are both the identity, implying that sp is a bijection as claimed. □

Algebraic version of the distance. For $a, b \in \mathbb{P}^{d-1}(K)$, define $v(a, b)$ as the supremum in $\mathbb{N} \cup \{+\infty\}$ of the set consisting of 0 and the positive integers n for which $\mathrm{sp}_n(a) = \mathrm{sp}_n(b)$. Thanks to Proposition 2.5, $v(a, b) = +\infty$ if and only if $a = b$.

Proposition 2.6. *Given* $a, b \in \mathbb{P}^{d-1}(K)$*, we have* $\mathrm{dist}(a, b) = q^{-v(a,b)}$.

Proof. Note that $\mathrm{sp}_n(a) = \mathrm{sp}_n(b)$ if and only if a and b have the same image in $\mathbb{P}^{d-1}(S_n)$, *i.e.* if and only if $\mathrm{can}(a) \equiv \mathrm{can}(b) \pmod{\mathfrak{m}^n}$. The proposition now follows from Proposition 1.9. □

More generally, given $a, b \in \mathbb{P}^{d-1}(S_n)$, we define $v_n(a, b)$ as the biggest integer $v \in \{0, 1, \dots, n\}$ for which $\mathrm{sp}_{n,v}(a) = \mathrm{sp}_{n,v}(b)$ (with the convention that $v = 0$ always satisfies the above requirement). As above $v_n(a, b) = n$ if and only if $a = b$. A torsion analogue of Proposition 1.9 then holds.

Proposition 2.7. *For $a, b \in \mathbb{P}^{d-1}(R_n)$, we can write:*

$$\mathrm{can}_n(b) - \mathrm{can}_n(a) = \pi^{v_n(a,b)} \cdot u$$

where u lies in R_n^d and has at least one invertible coordinate.

Proof. It is a simple adaptation of the proof of Proposition 1.9. □

2.3 Algebraic description of the universe

Recall that we have defined in §1.3 the set Ω (our universe) consisting of 1-Lipschitz functions $\mathbb{P}^{d-1}(K) \to R^d$. The aim of this subsection is to revisit constructions and results of §1.3 with an algebraic point of view. We recall that we have defined specialization maps $\mathrm{sp}_n : \mathbb{P}^{d-1}(K) \to \mathbb{P}^{d-1}(S_n)$ in §1.2 and, similarly, that we have introduced previously the projections $p_n : R^d \to R_n^d$ taking a tuple to its reduction modulo $\mathfrak{m}^n$.

The algebraic analogue of the existence of $\psi_n^{\mathrm{an}}(f)$ can be formulated as follows.

Proposition 2.8. *Let $f \in \Omega$. For all positive integer n, there exists a unique function $\psi_n(f) : \mathbb{P}^{d-1}(R_n) \to R_n^d$ making the following diagram commutative:*

$$\begin{array}{ccc} \mathbb{P}^{d-1}(K) & \xrightarrow{f} & R^d \\ \Big\downarrow{\scriptstyle \mathrm{sp}_n} & & \Big\downarrow{\scriptstyle p_n} \\ \mathbb{P}^{d-1}(R_n) & \xrightarrow{\psi_n(f)} & R_n^d \end{array} \tag{6}$$

Remark 2.9. Roughly speaking, the function $\psi_n(f)$ encodes the action of $\psi_n^{\mathrm{an}}(f)$ on closed balls of radius q^{-n}.

Proof of Proposition 2.8. The proposition can be derived from Proposition 1.16. We nevertheless prefer giving an independant and completely algebraic proof.

Let $a, b \in \mathbb{P}^{d-1}(K)$ with $\mathrm{sp}_n(a) = \mathrm{sp}_n(b)$. By definition $\mathrm{dist}(a, b) \leqslant q^{-n}$. Thus $|f(a) - f(b)| \leqslant q^{-n}$ because f is assumed to be 1-Lipschitz. Thus $f(a)$ and $f(b)$ lie in the same ball of radius q^{-n} or, equivalently, $p_n \circ f(a) = p_n \circ f(b)$. In other words, for $x \in \mathbb{P}^{d-1}(K)$, $p_n \circ f(x)$ depends only on $\mathrm{sp}_n(x)$. This implies the existence of the required mapping f_n. The unicity follows from the surjectivity of sp_n. □

We emphasize that, we have not proved yet that $\psi_n(f)$ is 1-Lipschitz. Indeed this notion has not been defined yet. Here is the definition we will use.

Definition 2.10. A function $f : \mathbb{P}^{d-1}(S_n) \to R_n^d$ is 1-Lipschitz if for all $a, b \in \mathbb{P}^{d-1}(S_n)$:

$$f(a) \equiv f(b) \pmod{\mathfrak{m}^{v_n(a,b)}}$$

where the above condition means that all the coordinates of $f(b_n) - f(a_n)$ lie in $\mathfrak{m}^{n - v_n(a,b)}$.

We denote by Ω_n their set.

We notice that Ω_1 is the of *all* set theoretical functions $\mathbb{P}^{d-1}(k) \to k^d$. Moreover, two integers $m \geqslant n$ together with a function $f_m \in \Omega_m$, it is easily checked that there exists a unique function $\psi_{m,n}(f_{n+1}) \in \Omega_n$ making the diagram below commutative:

$$\begin{array}{ccc} \mathbb{P}^{d-1}(R_m) & \xrightarrow{f_m} & R_m^d \\ \Big\downarrow{\scriptstyle \mathrm{sp}_{m,n}} & & \Big\downarrow{\scriptstyle p_{m,n}} \\ \mathbb{P}^{d-1}(R_n) & \xrightarrow{\psi_{m,n}(f_m)} & R_n^d \end{array}$$

Lemma 2.11. *The function ψ_n takes its values in Ω_n.*

Proof. Let $f \in \Omega$. Let $a_n, b_n \in \mathbb{P}^{d-1}(S_n)$. If $a_n = b_n$, we have $v_n(a_n, b_n) = n$ and there is nothing to prove. Otherwise, pick $a, b \in \mathbb{P}^{d-1}(K)$ such that $\mathrm{sp}_n(a) = a_n$ and $\mathrm{sp}_n(b) = b_n$. Then $\psi_n(f)$ maps a_n and b_n to $p_n(f(a))$ and $p_n(f(b))$ respectively. We then need to prove that $p_n(f(a)) - p_n(f(b)) = p_n(f(a) - f(b))$ has all its coordinates in $\mathfrak{m}^{v_n(a_n,b_n)}$. But, using that f is 1-Lipschitz, we get:

$$\|f(a) - f(b)\|_\infty \leqslant \mathrm{dist}(a, b) = q^{-v(a,b)} = q^{-v_n(a_n,b_n)}$$

and we are done. □

One important benefit of working with Ω_n instead of Ω_n^{an} is that the former is naturally endowed with algebraic structures. Precisely, one easily checks that Ω_n is a R-module for the usual operations (addition and scalar multiplication) on functions and that the projection maps $\psi_n : \Omega \to \Omega_n$ and $\psi_{m,n} : \Omega_m \to \Omega_n$ are all R-linear.

The $\psi_{m,n}$'s are actually the exact algebraic analogue of the functions $\psi_{m,n}^{\mathrm{an}}$'s introduced in §1.3. In order to state an analogue of Proposition 1.17, we introduce the additive group G_{n+1} consisting of functions $\mathbb{P}^{d-1}(R_{n+1}) \to k^d$ and let it act on Ω_{n+1} by

$$\forall g_{n+1} \in \mathcal{G}_{n+1}, \quad \forall f_{n+1} \in \mathcal{L}_{n+1}, \quad g_{n+1} \bullet f_{n+1} = f_{n+1} + \pi^n g_{n+1}.$$

Proposition 2.12. *The map $\psi_{n+1,n} : \Omega_{n+1} \to \Omega_n$ is surjective. Moreover the action of G_{n+1} stabilizes each fibre of $\psi_{n+1,n}$ and induces on it a free and transitive action.*

Remark 2.13. Recall that an action of a group G over a space X is free and transitive if, given two any points $x, y \in X$, there always exists a unique element $g \in G$ such that $y = gx$. This notably implies that, for all $x \in X$, the map $h_x : G \to X$, $g \mapsto gx$ is a bijection. In particular X is either empty or in bijection with G.

Proof of Proposition 2.12. The surjectivity of $\psi_{n+1,n}$ comes from that of $\mathrm{sp}_{n+1,n}$ while the claimed properties on the action of G_{n+1} are easily checked. □

Corollary 2.14. *The set Ω_n has cardinality:*

$$\mathrm{Card}\ \Omega_n = q^{d \cdot \frac{q^d - 1}{q-1} \cdot \frac{q^{n(d-1)} - 1}{q^{d-1} - 1}}.$$

Proof. Proposition 2.12 implies:

$$\mathrm{Card}\ \Omega_n = \mathrm{Card}\ \Omega_{n-1} \cdot \mathrm{Card}\ G_n = \mathrm{Card}\ \Omega_{n-1} \cdot q^{d\ \mathrm{Card}\ \mathbb{P}^{d-1}(S_n)}.$$

The claimed formula follows by induction using Eq. (5). □

Proposition 2.15. *The mapping $\psi : f \mapsto (\psi_n(f))_{n \geqslant 1}$ induces a bijection between Ω and $\varprojlim_n \Omega_n$ where the latter is by definition the set of all sequences $(f_n)_{n \geqslant 1}$ with $f_n \in \Omega_n$ and $\psi_{n+1,n}(f_{n+1}) = f_n$ for all n.*

Proof. We define the inverse bijection of ψ. Let $(f_n)_{n \geqslant 1}$ be a sequence in $\varprojlim_n \Omega_n$. Let $a \in \mathbb{P}^{d-1}(K)$. The sequence of $f_n \circ \mathrm{sp}_n(a)$ defines an element in $\varprojlim_n R_n^d$, *i.e.* an element $f(a)$ in R^d by completeness of R. This yields a function $f : \mathbb{P}^{d-1}(K) \to R^d$ making all the diagrams

$$\begin{array}{ccc} \mathbb{P}^{d-1}(K) & \xrightarrow{f} & R^d \\ {\scriptstyle \mathrm{sp}_n}\downarrow & & \downarrow{\scriptstyle p_n} \\ \mathbb{P}^{d-1}(R_n) & \xrightarrow{f_n} & R_n^d \end{array}$$

commutative. One derives from this that f is 1-Lipschitz, *i.e.* $f \in \Omega$. Moreover it is apparently an antecedent by ψ of the sequence $(f_n)_{n\geqslant 1}$. Finally, starting with $f \in \Omega$, the above construction applied with $f_n = \psi_n(f)$ clearly rebuilds f. This concludes the proof. □

Proposition 2.16. *For all n and all subset $E \subset \Omega_n$, we have:*

$$\mathbb{P}[\psi_n(\omega) \in E] = \frac{\text{Card } E}{\text{Card } \Omega_n}.$$

In other words the map ψ_n sends the probability measure on Ω to the uniform distribution on Ω_n.

Proof. Let $f_n, g_n \in \Omega_n$. Pick $h \in \Omega$ mapping to $g_n - f_n$ under ψ_n. Taking advantage of the fact that ψ_n is a group homomorphism, we derive that the translation by h sends the fibre over f_n to the fibre over g_n. The properties of the Haar measure consequently implies that all the fibres of ψ_n have the same measure. The proposition follows from this. □

2.4 Reformulation of the main Theorem

We fix a positive integer n. Following the construction of Section 1, given a function $f \in \Omega_n$, we define a Besikovitch set $N(f) \subset R_n^d$ by:

$$N(f) = \bigcup_{a \in \mathbb{P}^{d-1}(S_n)} S_a(f) \quad \text{with} \quad S_a(f) = \big\{t \cdot \text{can}_n(a) + f(a) \ : \ t \in R_n\big\}.$$

where we recall that $\text{can}_n(a) \in R^d$ denote the unique representative of a whose first invertible coordinate is equal to 1 (see §2.2). The relationship between the above construction and that of Section 1 is made precise by the following lemma.

Lemma 2.17. *With the notations of §1.4, we have:*

$$X_n(f) = q^{-nd} \cdot \text{Card } N(\psi_n(f))$$

for all $f \in \Omega$.

Proof. Set $f_n = \psi_n(f)$. Proposition 2.1 shows that:

$$X_n(f) = q^{-nd} \cdot \text{Card } p_n(N(f)).$$

It is then enough to show that $N(f_n)$ and $p_n(N(f))$ have the same cardinality. We will actually show that these two sets are equal.

Pick first $x \in N(f)$. Thus $x \in S_a(f)$ for some $a \in \mathbb{P}^{d-1}(K)$ from what we derive that $p_n(x) \in S_{\text{sp}_n(a)}(f_n)$. Therefore $p_n(x) \in N(f_n)$ and we have proved that $p_n(N(f)) \subset N(f_n)$. Conversely, take $x_n \in N(f_n)$, so that $x_n = t_n \cdot \text{can}_n(a_n) + f_n(a)$ for some $a_n \in \mathbb{P}^{d-1}(S_n)$ and some $t_n \in R_n$. Consider now $a \in \mathbb{P}^{d-1}(K)$ and $t \in R$ such that $\text{sp}_n(a) = a_n$ and $p_n(t) = t_n$. Clearly $x = t \cdot \text{can}_n(a) + f(a)$ sits in $N(f)$ and, coming back to the definition of ψ_n (*cf* Proposition 2.8), we observe that $p_n(x) = x_n$. Thus $x_n \in p_n(N(f))$ and we have proved the reverse inclusion. □

Combining the above lemma with Proposition 2.16, we find that our main theorem can then be rephrased as follows.

Theorem 2.18. *Let $(u_n)_{n\geqslant 0}$ be the sequence defined by the recurrence:*

$$u_0 = 1 \quad ; \quad u_{n+1} = 1 - \left(1 - \frac{u_n}{q^{d-1}}\right)^{q^{d-1}}.$$

and set:

$$u'_n = 1 - (1 - u_n)^{1+q^{-1}+\cdots+q^{-(d-1)}}.$$

Then, for any position integer n:

$$\frac{1}{\text{Card } \Omega_n} \cdot \sum_{f_n \in \Omega_n} \text{Card } N(f_n) = q^{nd} u'_n.$$

3 Proofs

In this section, we give complete proofs of Theorem 1.18 and Theorem 1.22 or, more precisely, of their algebraic analogues, namely Theorem 2.4 and Theorem 2.18 respectively. The strategy of the proof of Theorem 2.4 follows closely that of the real case (see [7, Theorem 2] or [1, Proposition 6.4]): a clever use of the Cauchy–Schwartz inequality reduces the proof to finding good estimations of the size of the intersections of two segments. This is achieved by counting the number of solutions of some affine congruences.

The proof of Theorem 2.18 basically follows the same idea of understading the size of the intersections of unit length segments. Several complications nonetheless occur. The most significant one is that we cannot restrict ourselves to 2 by 2 intersections but need to study s by s intersections for any integer $s \geqslant 2$. Roughly speaking, using the inclusion-exclusion principle, we will write X_n as an alternating sum:

$$X_n = X_{n,1} - X_{n,2} + X_{n,3} - \cdots + (-1)^s X_{n,s} + \cdots . \tag{7}$$

We will then compute the mean of $X_{n,s}$ for all s, put it into the above formula and end up this way with the value of $\mathbb{E}[X_n]$. We would like to insist on the fact that, although X_n is rather small (at least less than 1), the random variables $X_{n,s}$'s — and their mean — may take very large values when n is large. For instance $\mathbb{E}[X_{n,2}]$ goes to infinity when n grows up. There are then many compensations and the miracle is that we will be able to keep *exact* values during all the computation and then simplify the result.

3.1 Kakeya conjecture in dimension 2

We fix a positive integer n and an integer $\ell \in [\![0, n]\!]$. Let B be a ℓ-Besikovitch set in R_n^2. Our aim is to prove that:

$$\text{Card } B \geqslant q^{2(n-\ell)} \cdot \frac{1}{\frac{q-1}{q+1}\, n + 1} \tag{8}$$

By definition B contains a segment S_a of length $q^{-\ell}$ and direction a for each $a \in \mathbb{P}^1(S_n)$. Let ψ_a be the indicator function of S_a. Set $\psi = \sum_{a \in \mathbb{P}^1(S_n)} \psi_a$. Note that ψ vanishes outside B. Applying the Cauchy–Schwarz inequality with ψ and the indicator function of B, we then get:

$$\left(\sum_{x \in R_n^2} \psi(x) \right)^2 \leqslant \text{Card } B \cdot \sum_{x \in R_n^2} \psi(x)^2.$$

Noting that $\psi_a^2 = \psi_a$ and $\sum_{x \in R_n^2} \psi_a(x) = \text{Card } S_a$, the above inequality rewrites:

$$\Big(\sum_a \text{Card } S_a \Big)^2 \leqslant \text{Card } B \cdot \sum_{a,b} \text{Card } (S_a \cap S_b) \tag{9}$$

where a and b run over $\mathbb{P}^1(R_n)$. Recall that, given $a, b \in \mathbb{P}^1(R_n)$, we have defined in §2.2 an integer $v_n(a, b)$ between 0 and n.

Lemma 3.1. *(a) For $a \in \mathbb{P}^1(R_n)$, we have* Card $S_a = q^{n-\ell}$.

(b) For $a, b \in \mathbb{P}^1(R_n)$, we have Card $(S_a \cap S_b) \in \{0, q^{\min(n-\ell, v_n(a,b))}\}$.

Proof. *(a)* Recall that S_a consists of points $m_t = t \cdot \text{can}_n(a) + a'$ where t runs over $\pi^\ell R_n$ and $a' \in R_n^2$ is fixed. We claim that these points are pairwise distinct. Indeed remember the $\text{piv}_n(a)$-th coordinate of $\text{can}_n(a)$ is equal to 1. Consequently the $\text{piv}_n(a)$-th coordinate of m_t is $t + c$ where $c \in R_n$ is some constant. Our claim then becomes clear and it follows from it that the map $\pi^\ell R_n \to S_a$, $t \mapsto m_t$ is bijective. Hence Card $S_a = q^{n-\ell}$.

(b) Thanks to what we have just explained, there exists $a', b' \in R_n$ for which the cardinality of $S_a \cap S_b$ is equal to the number of solutions of the equation:

$$u \cdot \mathrm{can}_n(a) + a' = v \cdot \mathrm{can}_n(b) + b'$$

where the unknown are u and v and run over $\pi^\ell R_n$. The number of solutions of this affine system is either 0 or equal to the number of solutions of the associated homogeneous system, namely:

$$\begin{pmatrix} u & v \end{pmatrix} \cdot \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix} = 0$$

where $\mathrm{can}(a) = (a_1, a_2)$ and $\mathrm{can}(b) = (b_1, b_2)$. Thanks to (a direct adaptation of) Corollary 1.10, the above square matrix is equivalent to the diagonal matrix $\mathrm{Diag}(1, \pi^{v_n(a,b)})$. In other words there exists a linear change of basis $(u, v) \mapsto (u', v')$ after which our system rewrites:

$$\begin{cases} u' = 0 \\ \pi^{v_n(a,b)} v' = 0 \end{cases} \qquad \textit{i.e.} \qquad \begin{cases} u' = 0 \\ \pi^{n - v_n(a,b)} \text{ divides } v' \end{cases}$$

It is now clear that this system has $q^{\min(n-\ell, v_n(a,b))}$ solutions in $(\pi^\ell R_n)^2$. □

Coming back to the inequality (9), we obtain:

$$\mathrm{Card}\, B \geqslant \frac{\left(\mathrm{Card}\, \mathbb{P}^1(R_n) \cdot q^{n-\ell}\right)^2}{\sum_{a,b} q^{v_n(a,b)}} = \frac{q^{4n-2\ell-2} \cdot (q+1)^2}{\sum_{a,b} q^{v_n(a,b)}} \tag{10}$$

where a and b run over $\mathbb{P}^1(R_n)$. Now fix $a \in \mathbb{P}^1(R_n)$ and observe that the set of b's in $\mathbb{P}^1(R_n)$ for which $v_n(a,b) \geqslant v$ is a fibre of $\mathrm{sp}_{n,v}$. Thanks to the results of §2.2, there are q^{n-v} of them if $v > 0$ and, according to our convention, there are $\mathrm{Card}\, \mathbb{P}^1(R_n) = q^{n-1}(q+1)$ of them when $v = 0$. Therefore, when a remains fixed, we obtain:

$$\begin{aligned} \sum_b q^{v_n(a,b)} &= 2q^n + \sum_{v=1}^{n-1} q^v \cdot (q^{n-v} - q^{n-v-1}) \\ &= (n+1)\, q^n - (n-1)\, q^{n-1} = n\, q^{n-1}(q-1) + q^{n-1}(q+1) \end{aligned}$$

Summing up over all a, we get:

$$\begin{aligned} \sum_{a,b} q^{v_n(a,b)} &= \mathrm{Card}\, \mathbb{P}^1(R_n) \cdot \left(n\, q^{n-1}(q-1) + q^{n-1}(q+1)\right) \\ &= q^{n-1}(q+1) \cdot \left(n\, q^{n-1}(q-1) + q^{n-1}(q+1)\right) \end{aligned}$$

and injecting this in (10), we end up with Eq. (8) and the proof is complete.

3.2 Average size of a random Kakeya set

We now focus on the proof of Theorem 2.18 (which is equivalent to Theorem 1.18 thanks to the results of §2.4). We fix a positive integer n and endow Ω_n with the uniform distribution. Recall that to any function $f \in \Omega_n$, we have attached the Kakeya set:

$$N(f) = \bigcup_{a \in \mathbb{P}^{d-1}(S_n)} S_a(f) \quad \text{with} \quad S_a(f) = \left\{ t \cdot \mathrm{can}_n(a) + f(a) \ : \ t \in R_n \right\}.$$

Set $C(f) = \mathrm{Card}\, N(f)$ and, given in addition a subset A of $\mathbb{P}^{d-1}(S_n)$, define:

$$C_A(f) = \mathrm{Card} \bigcap_{a \in A} S_a(f). \tag{11}$$

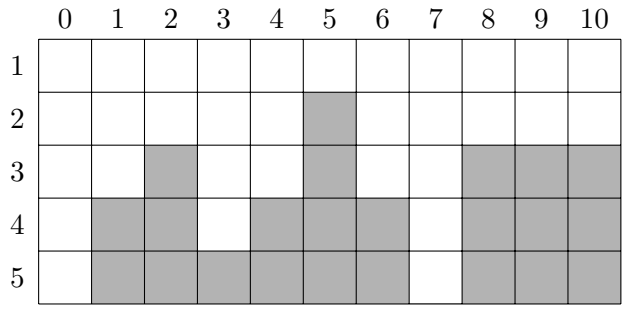


Figure 1: Representation of a height function (with $n = 5$ and $\ell = 10$)

This defines a family of random variables on Ω_n and the value we want to compute is the mean of C. The inclusion-exclusion principle readily implies:

$$C(f) = \sum_{A \subset \mathbb{P}^{d-1}(S_n)} (-1)^{1+\text{Card } A} \cdot C_A(f)$$

from what we get:

$$\mathbb{E}[C] = \sum_{A \subset \mathbb{P}^{d-1}(S_n)} (-1)^{1+\text{Card } A} \cdot \mathbb{E}[C_A]. \tag{12}$$

Remark 3.2. The random variables $X_{n,s}$ considered in the introduction of the Section 3 are related to the C_A's as follows:

$$X_{n,s} = q^{-nd} \cdot \sum_{\substack{A \subset \mathbb{P}^{d-1}(S_n) \\ \text{Card } A = s}} C_A.$$

Our strategy is now clear: first, we compute the expected values of the C_A's and second, we inject the obtained result in Eq. (12). The first step is achieved in §3.2.2 while the second is reached in §3.2.3. The first paragraph (§3.2.1) is devoted to work out one important notion on which the rest of the proof will be based.

3.2.1 The height function

For $i \in \{1, \dots, n\}$, choose and fix a total order on $\mathbb{P}^{d-1}(S_i)$ in such a way that the implication:

$$a < b \quad \Longrightarrow \quad \text{sp}_{i,i-1}(a) < \text{sp}_{i,i-1}(b) \tag{13}$$

holds for $i \geqslant 2$ and $a, b \in \mathbb{P}^{d-1}(S_i)$. (We recall that the specialization maps $\text{sp}_{i,i-1}$ were defined in §2.2.) These orders can be built inductively on i. Indeed first choose any total order on $\mathbb{P}^{d-1}(S_1)$. Then choose any total order on each fibre of $\text{sp}_{2,1}$ and glue them together in order to build a total order on $\mathbb{P}^{d-1}(S_2)$ making the implication (13) true for $i = 2$. Now continue this way with $i = 3, \dots, n$.

Definition 3.3. Let A be a subset of $\mathbb{P}^{d-1}(S_n)$ of cardinality $\ell + 1$. The *height function* of A is the function:

$$\begin{array}{rccc} h_A : & [\![1, \ell]\!] & \to & [\![1, n]\!] \\ & j & \mapsto & n - v_n(a_j, a_{j-1}) \end{array}$$

where the a_j's ($0 \leqslant j \leqslant \ell$) are the elements of A sorted by increasing order.

It is sometimes convenient to extend the function h_A by setting $h_A(0) = n$. We will often represent a height function as a table with n rows (labeled from 1 to n) and ℓ columns (labeled

from 1 to ℓ), where the cell (i,j) is tinted in gray when $i > h(j)$. Sometimes we will add a 0-th column on the left with all cells left white, in agreement with our convention $h_A(0) = n$. Figure 1 gives an example of such a representation. It turns out that interesting informations can be read off immediately on this representation. For example, the numbers of white cells on the i-th row (including that on the 0-th column) indicates the number of different values taken by the $\mathrm{sp}_{n,n+1-i}(a_j)$'s (for $0 \leqslant j \leqslant n$). More precisely, if $j < j'$, the equality $\mathrm{sp}_{n,n+1-i}(a_j) = \mathrm{sp}_{n,n+1-i}(a_{j'})$ holds if and only if the cells $(i,j+1),(i,j+2),\ldots,(i,j')$ are all left white. This remark notably implies that:

$$v_n(a_j, a_{j'}) = n - \max\big(h(j+1), h(j+2), \ldots, h(j')\big) \tag{14}$$

provided that $j < j'$. In order to visualize even better the above properties, it can be helpful to fill the table of Figure 1 by writing the value $\mathrm{sp}_{n,n+1-i}(a_j)$ is the cell (i,j). The three following properties then hold:

(i) each cell contains an element which lies in the fibre of the element written just below (or, equivalently, each element of the table specializes to the element written just above),

(ii) each gray cell contains the same element as the cell immediately on the left,

(iii) on each line, the elements are sorted in increasing order.

Conversely remark that any filling of the table which satisfies the three above requirements corresponds to one unique choice of A: it suffices to read the a_j's on the first line. As we are going to explain now, this point of view will be particularly suitable for counting the number of subsets A having a fixed height function.

Definition 3.4. Let $h : [\![1,\ell]\!] \to [\![1,n]\!]$ be any function.
The *multiplicity function* of h is the function $M(h) : [\![1,\ell]\!] \to \mathbb{N}$ taking an integer $j \in [\![1,\ell]\!]$ to the number of indices $j' \in [\![1,j]\!]$ for which:

$$h(j') = h(j) \quad \text{and} \quad h(x) \leqslant h(j) \text{ for all } x \in [\![j,j']\!].$$

The *weight function* of h is the function $W(h) : [\![1,\ell]\!] \to \mathbb{R}$ defined by:

$$W(h)(j) = \frac{1}{q^{d-1}} \cdot \frac{q^{d-1} - M(h)(j)}{M(h)(j)+1}.$$

The *modified weight function* of h is the function $W'(h) : [\![1,\ell]\!] \to \mathbb{R}$ defined by:

$$W'(h)(j) = \begin{cases} \dfrac{1}{q^{d-1}} \cdot \dfrac{q^{d-1} - M(h)(j)}{M(h)(j)+1} & \text{if } h(j) \neq n \\[2ex] \dfrac{1}{q^{d-1}} \cdot \dfrac{1 + q + \cdots + q^{d-1} - M(h)(j)}{M(h)(j)+1} & \text{if } h(j) = n. \end{cases}$$

We emphasize that $j' = j$ is allowed in the definition of the multiplicity function, so that $M(h)(j)$ is always at least 1. As an example, the values of the multiplicity function attached to the function h_A represented on Figure 1 are:

j	1	2	3	4	5	6	7	8	9	10
$h_A(j)$	3	2	4	3	1	3	5	2	2	2
$M(h_A)(j)$	1	1	1	1	1	2	1	1	2	3

Proposition 3.5. *Let $h : [\![1,\ell]\!] \to [\![1,n]\!]$ be a function. The number of subset A of $\mathbb{P}^{d-1}(S_n)$ (necessarily of cardinality $\ell+1$) whose height function is h is:*

$$\big(1 + q^{-1} + q^{-2} + \cdots + q^{-(d-1)}\big) \cdot q^{(d-1)n} \cdot \prod_{j=1}^{\ell} W'(h)(j) \cdot q^{(d-1)\cdot h(j)}. \tag{15}$$

Proof. Let us first explain that the value (15) can be easily read off on the representation by cells (see Figure 1) we have introduced before. To do this, write $1+q+\cdots+q^{d-1}$ in the cell $(0,n)$, write the number $q^{d-1}W'(h)(j)$ in the cell $(h(j),j)$ $(0\leqslant j\leqslant \ell)$ and q^{d-1} in all other *white* cells. In the example of Figure 1, we get:

	0	1	2	3	4	5	6	7	8	9	10
1	A	A	A	A	A	$\frac{A-1}{2}$	A	A	A	A	A
2	A	A	$\frac{A-1}{2}$	A	A		A	A	$\frac{A-1}{2}$	$\frac{A-2}{3}$	$\frac{A-3}{4}$
3	A	$\frac{A-1}{2}$		A	$\frac{A-1}{2}$		$\frac{A-2}{3}$	A			
4	A			$\frac{A-1}{2}$				A			
5	P							$\frac{P-1}{2}$			

where we have set $A=q^{d-1}$ (A for "affine") and $P=1+q+\cdots+q^{d-1}$ (P for "projective"). It can then be easily checked that the quantity (15) equals the product of all the numbers written in the above table.

Now recall that we have previously defined a bijection between the set of all A's such that $h_A=h$ and the fillings of the table corresponding to h obeying to the requirements (i)–(iii) listed on page 20. We are going to show that the number of such fillings of the m last rows is exactly the product of the numbers appearing on the m last rows. This will conclude the proof. We proceed by induction on m. For $m=1$, we have to count the number of strictly increasing sequences of elements of $\mathbb{P}^{d-1}(k)$ of length c where c is the number of white cells located on the last row. The data of such a sequence is obviously equivalent to the data of the set of its values. Since furthermore Card $\mathbb{P}^{d-1}(k)=P$, there are then $\binom{P}{c}$ such sequences and we are done for $m=1$. More generally, going from m to $m+1$ is obtained in a similar fashion once we have noticed that the fibres of $\mathrm{sp}_{n-m+1,n-m}$ all have cardinality A (see the discussion just below Eq. (5), page 13). □

3.2.2 Directional expected values

Throughout this paragraph, we fix a subset A of $\mathbb{P}^{d-1}(S_n)$. We write $A=\{a_0,a_1,\dots,a_\ell\}$ with $a_0<a_1<\cdots<a_\ell$ and denote by h_A the height function of A. Recall that we have defined a random variable C_A on Ω_n by Eq. (11). The aim of this paragraph is to compute its mean. In order to do so, we consider the following evaluation mapping:

$$\begin{array}{rccc}\mathrm{ev}_A: & \Omega_n & \to & (R_n^d)^{\ell+1}\\ & f & \mapsto & \big(f(a_0),f(a_1),\dots,f(a_\ell)\big).\end{array}$$

Clearly, $C_A(f)$ only depends on $\mathrm{ev}_A(f)$ for $f\in\Omega_n$. Moreover ev_A is a group homomorphism, which notably implies that the fibres of ev_A all have the same cardinality. As a consequence, letting $\mathcal{B}_A$ denote the image of ev_A, we get:

$$\mathbb{E}[C_A]=\frac{1}{\mathrm{Card}\,\mathcal{B}_A}\cdot\sum_{b\in\mathcal{B}_A}\mathrm{Card}\bigcap_{j=1}^{\ell}\Sigma_{a_j}(b_j) \tag{16}$$

where $\Sigma_{a_j}(b_j)=\big\{t\cdot\mathrm{can}_n(a_i)+b_i\ :\ t\in R_n\big\}$.

Lemma 3.6. *The set $\mathcal{B}_A$ consists of tuples $(b_0,b_1,\dots,b_{\ell+1})\in(R_n^d)^{\ell+1}$ such that $b_{j+1}\equiv b_j \pmod{\mathfrak{m}^{n-h(j)}}$ for all $j\in[\![1,\ell]\!]$.*

Proof. By definition of h_A, we have $v_n(a_j,a_{j+1})=n-h_A(j)$ for all j. Going back to the definition of Ω_n, we deduce that, for any $f\in\Omega_n$ and $j\in[\![1,\ell]\!]$, we must have $f(a_{j+1})\equiv f(a_j) \pmod{\mathfrak{m}^{n-h_A(j)}}$. In other words, ev_A takes its values in $\mathcal{B}_A$.

Conversely pick $(b_0, b_1, \dots, b_{\ell+1}) \in \mathcal{B}_A$. Given $a \in \mathbb{P}^{d-1}(S_n)$, let $j(a)$ be the smallest index for which $v_n(a, a_{j(a)})$ is maximal and set $f(a) = b_{j(a)}$. This defines a function $f : \mathbb{P}^{d-1}(S_n) \to R_n^d$ satisfying $f(a_j) = b_j$ for all j. It remains to prove that $f \in \Omega_n$, *i.e.* that f is 1-Lipschitz. Let $a, a' \in \mathbb{P}^{d-1}(S_n)$ and set for simplicity $j = j(a)$ and $j' = j(a')$. Up to swapping a and a', we may assume that $j \leqslant j'$. If $j = j'$ there is nothing to prove. Otherwise, it follows from Eq. (14) and the definition of $\mathcal{B}_A$ that $b_j \equiv b_{j'} \pmod{\mathfrak{m}^{v_n(a_j, a_{j'})}}$. This readily implies the 1-Lipschitz condition under the extra assumption $v_n(a, a') \leqslant v_n(a_j, a_{j'})$ since then $\mathfrak{m}^{v_n(a_j,a_{j'})} \subset \mathfrak{m}^{v_n(a,a')}$. Let us now examine the case where $v_n(a, a') > v_n(a_j, a_{j'})$. Put $\nu = v_n(a, a')$. From the assumption $v_n(a, a_j) \geqslant \nu$, we would derive:

$$v_n(a', a_{j'}) \geqslant v_n(a', a_j) \geqslant \min(v_n(a', a), v_n(a, a_j)) \geqslant \nu$$

and would deduce:

$$v_n(a_j, a_{j'}) \geqslant \min(v_n(a_j, a), v_n(a, a'), v_n(a', a_{j'})) = \nu$$

which is a contradiction. Hence $v_n(a, a_j) < \nu$ and similarly $v_n(a', a_{j'}) < \nu$. Noting that $v_n(x, z) = \min(v_n(x, y), v_n(y, z))$ as soon as $v_n(x, y) \neq v_n(y, z)$ (which comes from the very first definition of v_n), we find:

$$v_n(a', a_j) = v_n(a, a_j) \geqslant v_n(a, a_{j'}) = v_n(a', a_{j'}).$$

Now we conclude by remarking that the above inequality cannot be true since it contradicts the minimality of j' (remember that we had assumed $j < j'$). □

Corollary 3.7. *We have:*

$$\text{Card } \mathcal{B}_A = q^{nd} \cdot \prod_{j=1}^{\ell} q^{d \cdot h_A(j)}. \tag{17}$$

Proof. There are q^{nd} possibilities for the choice of b_0. Once this choice has been made, b_1 must satisfy $b_1 \equiv b_0 \pmod{\mathfrak{m}^{n-h_A(1)}}$, which leads to $q^{d \cdot h_A(1)}$ possibilities. Repeating this reasoning, we end up with the announced formula. □

Proposition 3.8. *We have:*

$$\mathbb{E}[C_A] = q^n \cdot \prod_{j=1}^{\ell} q^{-(d-1) \cdot h_A(j)}.$$

Proof. Fix a point $c \in R_n^d$. We are going to count the number of parameters $(b_0, b_1, \dots, b_\ell) \in \mathcal{B}_A$ for which c lies on all lines $\Sigma_{a_j}(b_j)$ $(0 \leqslant j \leqslant \ell)$. Call N_c this number.

We first focus on b_0. By definition $c \in \Sigma_{a_0}(b_0)$ if and only if there exists $t_0 \in R_n$ such that $t_0 \cdot \text{can}(a_0) + b_0 = c$. Since one of the coordinates of $\text{can}(a_0)$ is equal to 1, the mapping $t \mapsto t \cdot \text{can}(a_0) + b_0$ is injective and there is then exactly Card $R_n = q^n$ acceptable values for b_0.

Suppose now that we are given $b_0, \dots, b_j$ satisfying the above condition and let us count the number of possibilities for completing the sequence with an extra term b_{j+1}. This b_{j+1} has to satisfy the two following conditions:

$$\begin{aligned} \exists t_{j+1} \in R_n, \quad & t_{j+1} \cdot \text{can}(a_{j+1}) + b_{j+1} = c \\ & b_{j+1} \equiv b_j \pmod{\mathfrak{m}^{n-h_A(j)}} \end{aligned}$$

Our problem then amounts to counting the number of values $t_{j+1} \in R_n$ such that:

$$t_{j+1} \cdot \text{can}(a_{j+1}) + b_j \equiv c \pmod{\mathfrak{m}^{n-h_A(j)}}. \tag{18}$$

Since $c \in \Sigma_{a_j}(b_j)$, we know that there exists some $t_j \in R_n$ such that $t_j \cdot \text{can}(a_j) + b_j = c$. By Proposition 2.7, we know moreover that $\text{can}(a_j) \equiv \text{can}(a_{j+1}) \pmod{\mathfrak{m}^{n-h_A(j)}}$. Thus $t_{j+1} = t_j$

is a solution of (18) and, using again that can(a_{j+1}) has one coordinate equal to 1, we find that Eq. (18) rewrites $t_{j+1} \equiv t_j \pmod{\mathfrak{m}^{n-h_A(j)}}$. There are thus $q^{h_A(j)}$ possibilities for t_{j+1}.

As a consequence of the previous discussion, we find that $N_c = q^n \cdot q^{h_A(1)} \cdot q^{h_A(2)} \cdots q^{h_A(\ell)}$ (independantly on c). Finally notice that:

$$\sum_{b \in \mathcal{B}_A} \text{Card} \bigcap_{j=1}^{\ell} \Sigma_{a_j}(b_j) = \sum_{c \in R_n^d} N_c = q^{nd} \cdot q^n \cdot q^{h_A(1)} \cdot q^{h_A(2)} \cdots q^{h_A(\ell)}$$

and conclude by injecting this equality together with Eq. (17) in Eq. (16). □

3.2.3 Summing up all contributions

Let $\mathcal{H}_n$ be the set of all functions $h : [\![1, \ell]\!] \to [\![1, n]\!]$ for ℓ varying in $[\![0, +\infty[\![$ (agreeing as usual that there exists a unique function $h : \emptyset \to [\![1, n]\!]$). For $h \in \mathcal{H}_n$, denote $\ell(h)$ its ℓ. Combining Proposition 3.5 and Proposition 3.8, we find that the expected value of C is:

$$\mathbb{E}[C] = \left(1 + q^{-1} + q^{-2} + \cdots + q^{-(d-1)}\right) \cdot q^{nd} \cdot \sum_{h \in \mathcal{H}_n} (-1)^{\ell(h)} \prod_{i=1}^{\ell(h)} W'(h)(i) \tag{19}$$

Recall that we have defined a sequence $(u_n)_{n \geqslant 0}$ by:

$$u_0 = 1 \quad ; \quad u_n = 1 - \left(1 - \frac{u_{n-1}}{q^{d-1}}\right)^{q^{d-1}}. \tag{20}$$

Proposition 3.9. *The following formula holds:*

$$u_n = \sum_{h \in \mathcal{H}_n} (-1)^{\ell(h)} \prod_{i=1}^{\ell(h)} W(h)(i).$$

Proof. For simplicity, we set $w(h) = \prod_{i=1}^{\ell(h)} W(h)(i)$. The key observation is the following: to each $h \in \mathcal{H}_n$, one can attach a finite sequence $h_0, h_1, \ldots, h_m$ of functions in $\mathcal{H}_{n-1}$ as follows. Let $j_1 < j_2 < \cdots < j_m$ be the integers for which $h(j_i) = n$, set $j_0 = 0$ and $j_{m+1} = \ell(h) + 1$ and, for $i \in [\![0, m]\!]$, define:

$$\begin{aligned} h_i : [\![1, j_{i+1} - j_i - 1]\!] &\to [\![1, n-1]\!] \\ j &\mapsto h(j + j_i). \end{aligned}$$

On the representation of Figure 1, the functions h_i's then correspond to the bands (with last row erased) located between two white columns. This construction clearly defines a bijection between $\mathcal{H}_n$ and the set of finite sequences of elements of $\mathcal{H}_{n-1}$. This bijection is moreover compatible with the length and the weight functions in the following sense: if h corresponds to $(h_0, h_1, \ldots, h_m)$ then $\ell(h) = m + \ell(h_1) + \ell(h_2) + \cdots + \ell(h_m)$ and

$$\begin{aligned} W(h)(j) &= W(h_i)(j - j_i) \qquad \text{for } j_i < j < j_{i+1} \\ W(h)(j_i) &= \frac{1}{q^{d-1}} \cdot \frac{q^{d-1} - i}{i + 1} \end{aligned}$$

Hence $w(h) = q^{-(d-1)(m+1)} \cdot \binom{q^{d-1}}{m+1} \cdot w(h_1) \cdot w(h_2) \cdots w(h_m)$. Taking the sum over all $h \in \mathcal{H}_n$, we

find the relation:

$$\begin{aligned}
\sum_{h\in\mathcal{H}_n}(-1)^{\ell(h)}w(h) &= \sum_{m=0}^{\infty}(-1)^m\cdot\binom{q^{d-1}}{m+1}\cdot\Big(\frac{1}{q^{d-1}}\Big)^{m+1}\sum_{\substack{h_0,\dots,h_m\\\in\mathcal{H}_{n-1}}}\prod_{i=0}^{m}(-1)^{\ell(h_i)}w(h_i)\\
&= \sum_{m=0}^{\infty}(-1)^m\cdot\binom{q^{d-1}}{m+1}\cdot\Big(\frac{1}{q^{d-1}}\Big)^{m+1}\cdot\Big(\sum_{h\in\mathcal{H}_{n-1}}(-1)^{\ell(h)}w(h)\Big)^{m+1}\\
&= 1\ -\ \sum_{m'=1}^{q^{d-1}}\binom{q^{d-1}}{m'}\cdot\Big(-\frac{1}{q^{d-1}}\Big)^{m'}\cdot\Big(\sum_{h\in\mathcal{H}_{n-1}}(-1)^{\ell(h)}w(h)\Big)^{m'}\\
&= 1\ -\ \Big(1-\frac{1}{q^{d-1}}\sum_{h\in\mathcal{H}_{n-1}}(-1)^{\ell(h)}w(h)\Big)^{q^{d-1}}.
\end{aligned}$$

The proposition now follows by comparing the above relation with Eq. (20). □

Slightly adapting the arguments of the above proof, we get:

$$\begin{aligned}
\big(1+q^{-1}+q^{-2}+\cdots+q^{-(d-1)}\big)\cdot\sum_{h\in\mathcal{H}_n}(-1)^{\ell(h)}\prod_{i=1}^{\ell(h)}W'(h)(i)&\\
= 1-\Big(1-\frac{u_{n-1}}{q^{d-1}}\Big)^{1+q+\cdots+q^{d-1}} &= u'_n
\end{aligned}$$

where u'_n is defined in the statement of Theorem 2.18 (page 16). Using Eq. (19), we end up with $\mathbb{E}[C]=q^{nd}u'_n$ and Theorem 2.18 is proved.

4 Numerical simulations

We recall that the main objects studied in this paper are the random Kakeya sets and especially the random variables X_n (defined in §1.4) that measure their size. In this last section, We present several numerical simulations showing the behaviour of the X_n's beyond their mean.

All our experiments have been done over the field of 2-adic numbers $\mathbb{Q}_2$. We recall briefly that $\mathbb{Q}_2$ is the completion of $\mathbb{Q}$ for the 2-adic norm $|\cdot|_2$ defined, for two integers n and m, by:

$$\begin{aligned}
&|n|_2 = 2^{-v} \quad \text{if } 2^v \text{ is the highest power of 2 dividing } n\\
\text{and}\quad &\big|\tfrac{n}{m}\big|_2 = \tfrac{|n|_2}{|m|_2}.
\end{aligned}$$

The unit ball of $\mathbb{Q}_2$ is the so-called ring of 2-adic integers $\mathbb{Z}_2$. Any element x in it can be uniquely written as a convergent series

$$x = s_0 + 2s_1 + 2^2s_2 + 2^3s_3 + \cdots + 2^ns_n + \cdots$$

where the s_i's all lie in $S=\{0,1\}$ (decomposition in 2-basis). The s_i's define mutually independent Bernoulli variables of parameter $\frac{1}{2}$ on $\mathbb{Z}_2$. In other words, generating a random element in $\mathbb{Z}_2$ reduces to pick each digit s_i uniformly in S and independently.

4.1 Empirical distribution of the variables X_n

We recall that our universe Ω is the set of 1-Lipschitz functions $\mathbb{P}^{d-1}(K)\to R^d$. By the results of §1.3, Ω comes equipped with projection maps $\Omega\to\Omega_n^{\text{an}}$ where Ω_n^{an} was defined as the subset

```
def random_lipschitz_iter(d,n):
    if n == 1:
        # Run over elements a ∈ P^{d-1}(Z/2Z) according to the position of the first nonzero coordinate
        for piv in range(d):
            for a in xmrange_iter(piv*[[0]] + [[1]] + (d-1-piv)*[[0,1]]):
                # Gererate a random image b ∈ (Z/2Z)^d of a
                b = [ randint(0,1) for _ in range(d) ]
                yield(piv, vector(a), vector(b))
    else:
        # Run over elements a ∈ P^{d-1}(Z/2^{n-1}Z) and call b the image of a
        for (piv,a,b) in random_lipschitz_iter(d,n-1):
            q = 2**(n-1)
            # Run over the elements a + a' of the fibre of sp_{n,n-1} above a
            for aprime in xmrange_iter(piv*[[0,q]] + [[0]] + (d-1-piv)*[[0,q]]):
                # Generate a random image b + b' ∈ (Z/2Z)^d (with 2^{n-1} divides b') of a + a'
                bprime = [ q*randint(0,1) for _ in range(d) ]
                yield(piv, a+vector(aprime), b+vector(bprime))
```

Figure 2: SAGEMATH function generating a random element in Ω_n^{an} for $K = \mathbb{Q}_2$

n	5	6	7	8	9	10	11
$\mathbb{E}[X_n]$ (theoretical value)	0.534	0.487	0.448	0.415	0.386	0.362	0.340
$\mathbb{E}[X_n]$ (empirical value)	0.534	0.487	0.448	0.415	0.386	0.362	0.340
$\sigma[X_n]$ (empirical value)	0.0316	0.0229	0.0169	0.0126	0.0097	0.0076	0.0061

Figure 3: Expected value and standard deviation of X_n for $K = \mathbb{Q}_2$ and $d = 2$

of Ω consisting of functions which are constant on each closed ball of radius q^{-n} and takes their values in $[\![0, 2^n-1]\!]^d$. Alternatively functions in Ω_n^{an} can be viewed as mapping $\mathbb{P}^{d-1}(S_n) \to S^d$ satisfying an extra condition (see §2.3). Two other interesting features of Ω_n^{an} are the following: (1) the measure induces on Ω_n^{an} by the projection $\Omega \to \Omega_n^{\mathrm{an}}$ is the uniform distribution and (2) the random variable X_n factors through Ω_n^{an}.

We recall also that one can furthermore decompose any function in Ω_n^{an} as a sum:

$$(g_1 \circ \mathrm{sp}_1) + 2 \cdot (g_2 \circ \mathrm{sp}_2) + 2^2 \cdot (g_3 \circ \mathrm{sp}_3) + \cdots + 2^{n-1} \cdot (g_n \circ \mathrm{sp}_n) \tag{21}$$

where $g_i : \mathbb{P}^{d-1}(S_i) \to S^d$ is any function and conversely that any function of the shape (21) lies in Ω_n^{an}. Generating a random function in Ω_n^{an} then reduces to pick the g_i's ($1 \leqslant i \leqslant n$) uniformly and independently. Picking each g_i is also easy: we enumerate the elements of $\mathbb{P}^{d-1}(S_i)$ (this can be done using the results of §2.2) and choose their image randomly and independantly in S^d. The SAGEMATH function presented in Figure 2 generates a random element $f_n \in \Omega_n^{\mathrm{an}}$ according to the uniform distribution. More precisely, it returns an iterator over the sequence of triples $(\mathrm{piv}(a), a, f_n(a))$ where a runs over $\mathbb{P}^{d-1}(S_n)$. (Note that the first coordinate $\mathrm{piv}(a)$ is useful for the recursion but may be then omitted.) One nice feature of this implementation is its memory cost which (almost) does not grow with n.

The tables of Figure 3 (page 25) and Figure 4 (page 26) show the expected value and the standard deviation of some of X_n's observed on a sample (renewed for each value of n) of $100,000$ random Kakeya sets in dimension 2 and 3 respectively. We note in particular that:

- the empirical mean agrees with the theoretical one (given by Theorem 1.18) up to 10^{-3},

n	3	4	5	6	7	8	9
$\mathbb{E}[X_n]$ (theoretical value)	0.628	0.551	0.490	0.442	0.402	0.369	0.341
$\mathbb{E}[X_n]$ (empirical value)	0.628	0.551	0.490	0.442	0.402	0.369	0.341
$\sigma[X_n]$ (empirical value)	0.0502	0.0371	0.0286	0.0227	0.0187	0.0155	0.0132

Figure 4: Expected value and standard deviation of X_n for $K = \mathbb{Q}_2$ and $d = 3$

- the standard deviation is quite small and seems to converge to 0 faster than the mean, *i.e.* faster than $\frac{1}{n}$ (although this phenomenon is less apparent in dimension 3).

Going further one can draw the empirical "density"[4]: we subdivise $\mathbb{R}$ into small intervals and count, for each of them, the proportion of sample points (renormalized by the size of the interval) leading to a point in it. The results are displayed in Figure 5 (page 27) and Figure 6 (page 28) in dimension 2 and 3 respectively. The red and green vertical lines (which actually always collapse) in these pictures indicate the theoretical mean and the empirical mean of X_n respectively.

For a fixed dimension, the density curves (for various n) all have a similar shape. This may suggest that the law of X_n — correctly renormalized — converges to some limit. We believe that it would be very interesting to investigate further this question. For example if one can compute this limit and check that it is zero until some point, it would eventually imply the Kakeya conjecture for almost all non-archimedean Kakeya sets.

We finally remark that, on the first diagram of Figure 5, one can clearly separate two curves. This reflects a parity phenomenon: $q^{nd}X_n = 2^{10}X_5$ is even with probability $\approx 73\%$ and odd with probability $\approx 27\%$. The curve below then corresponds to odd values of X_5 while the curve above corresponds to even values. This phenomenon tends to disappear rapidly when n grows up.

4.2 Visualizing a random 2-adic Kakeya set

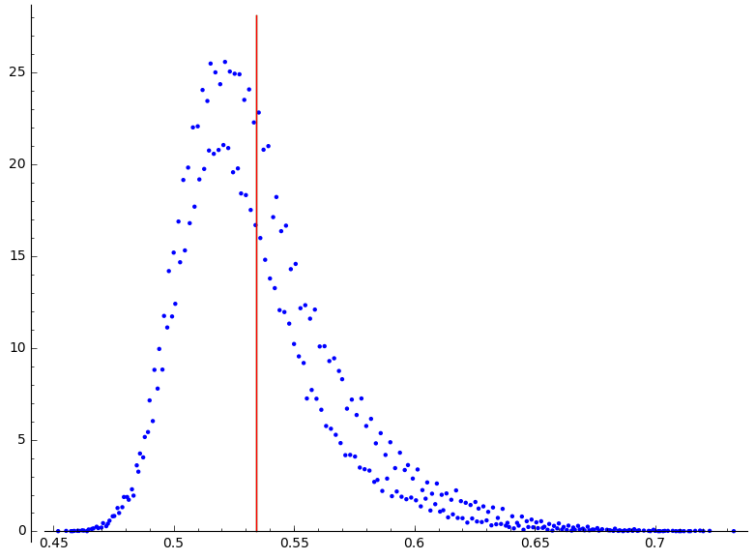
In order to draw a 2-adic Kakeya set sitting naturally in $\mathbb{Z}_2^d$, we will necessarily need to relate $\mathbb{Z}_2$ and $\mathbb{R}$. In order to do so, we use the "reverse" function $r : \mathbb{Z}_2 \to [0,1]$ mapping the 2-adic integer $\sum_{i=0}^{\infty} 2^i s_i$ (with $s_i \in \{0,1\}$) to the real number $\sum_{i=0}^{\infty} 2^{-i-1} s_i$.

Note that r is continuous (it is actually 1-Lipschitz) but not injective since the binary representation of a real number fails to be unique in general. For instance $\frac{1}{2}$ has two preimages which are $1 \in \mathbb{Z}_2$ and $-2 \in \mathbb{Z}_2$. The closed intervals $[0, \frac{1}{2}]$ and $[\frac{1}{2}, 1]$ correspond to the disjoint cosets $2\mathbb{Z}_2$ and $2\mathbb{Z}_2 + 1$ respectively. Note that the latter are open and closed in $\mathbb{Z}_2$. More generally all real number of the form $\frac{a}{2^n}$ have two distinct preimages in $\mathbb{Z}_2$ and there always exist two closed interval meeting $\frac{a}{2^n}$ corresponding to two open closed subsets of $\mathbb{Z}_2$.

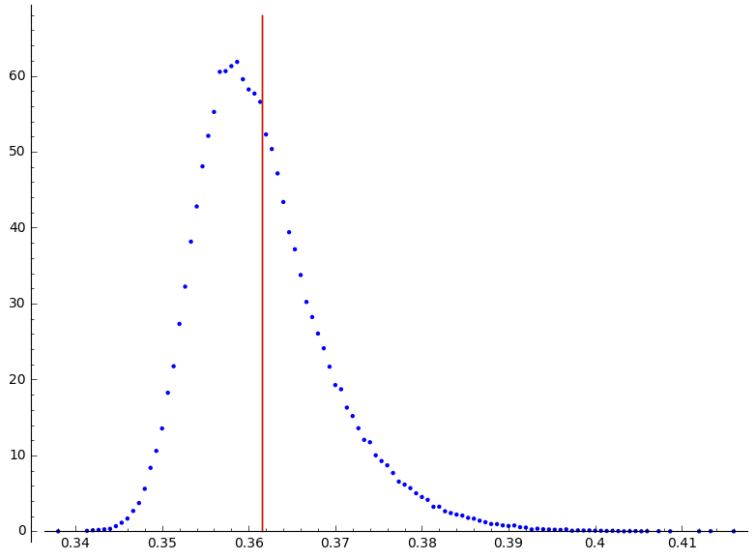
Remark 4.1. There actually exist closed embeddings $\mathbb{Z}_2 \to \mathbb{R}$; an example of it is the Cantor mapping C taking $\sum_{i=0}^{\infty} 2^i s_i \in \mathbb{Z}_2$ to $2 \cdot \sum_{i=0}^{\infty} 3^{-i-1} s_i$. The image of C is the usual triadic Cantor set and C induces an homeomorphism between it and $\mathbb{Z}_2$. We nevertheless preferred to use r because it maps $\mathbb{Z}_2$ to an interval whereas C maps $\mathbb{Z}_2$ to a null set. Working with C has then two disadvantages: it would lead to undrawable pictures on the one hand and would not reflect properly the properties we want to emphasize on the other hand.

[4] It is not actually a density in the usual sense because the variables X_n's take their values in a *discrete* subset of $\mathbb{R}$.

$n = 5$:



$n = 10$:



$n = 11$:

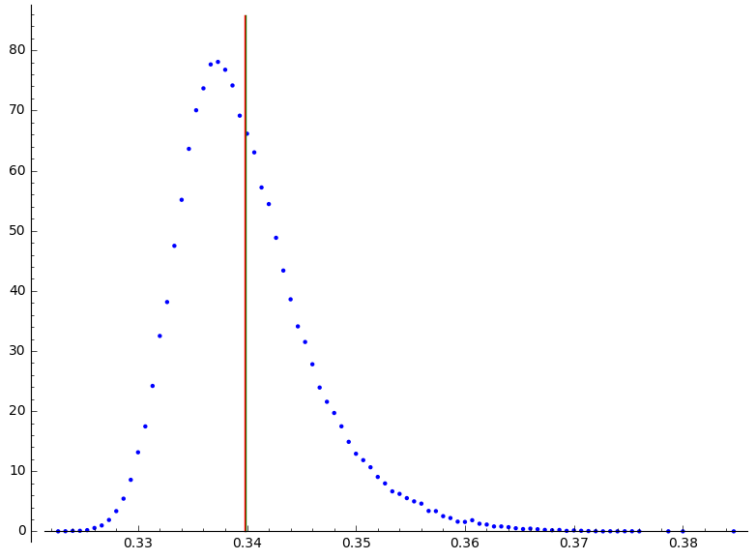
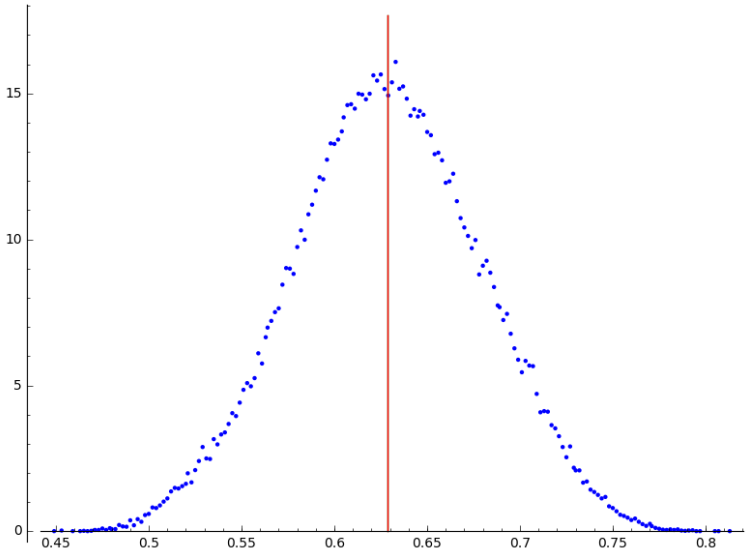
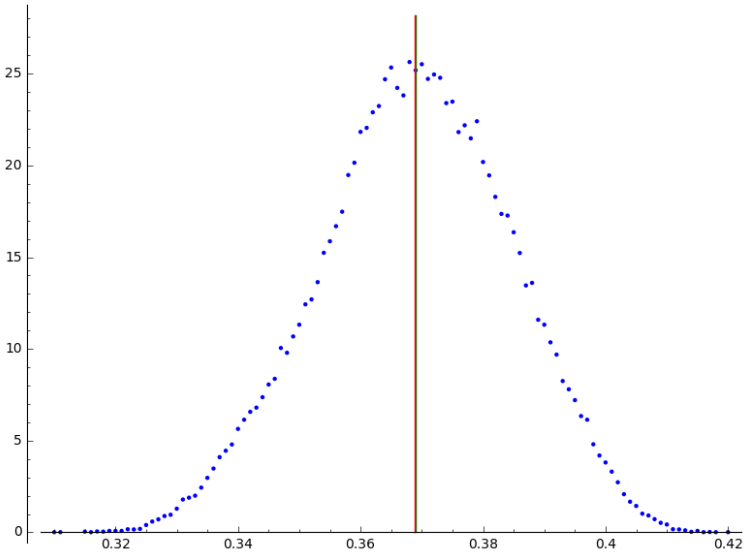


Figure 5: Empirical density of X_n for $K = \mathbb{Q}_2$ and $d = 2$

$n = 3$:



$n = 8$:



$n = 9$:

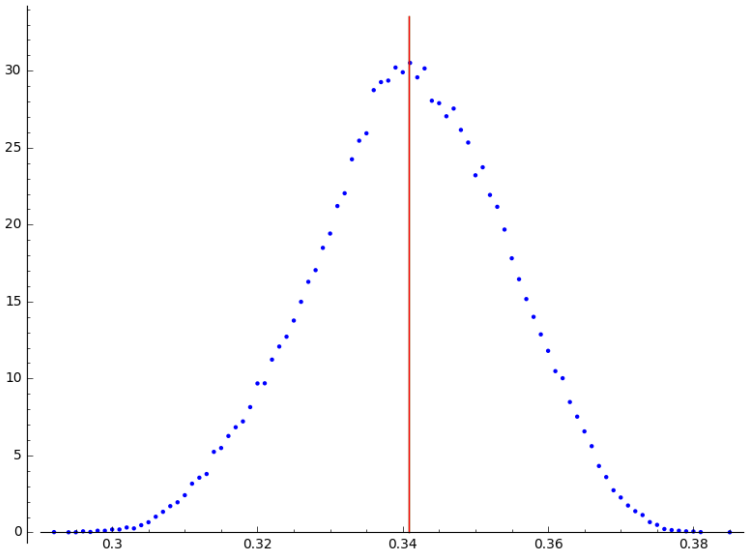


Figure 6: Empirical density of X_n for $K = \mathbb{Q}_2$ and $d = 3$

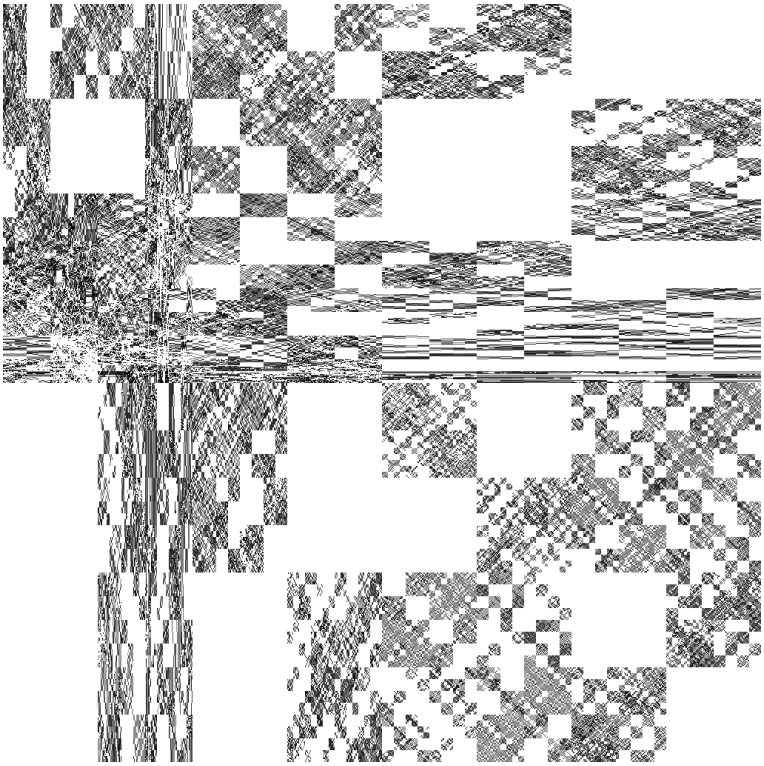


Figure 7: A 2-dimensional random Kakeya set over $\mathbb{Q}_2$

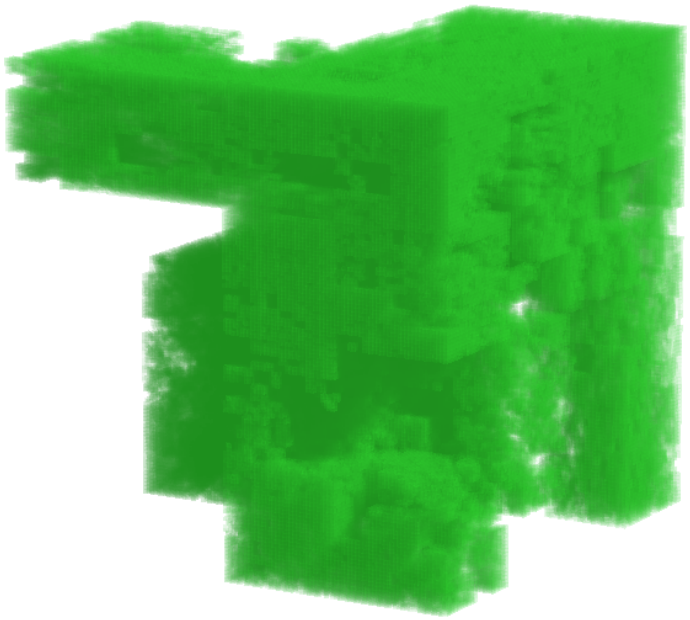


Figure 8: A 3-dimensional random Kakeya set over $\mathbb{Q}_2$

Viewing $\mathbb{Z}_2^2$ in $\mathbb{R}^2$ through the map (r, r), the picture of Figure 7 (page 29) represents a random Kakeya set — or more precisely its (2^{-13})-neighbourhood — in $\mathbb{Z}_2^2$. An animation showing a 2-adic needle moving continuously in the 2-adic plane and filling a 2-adic Kakeya set is available at the URL:

http://xavier.toonywood.org/papers/publis/kakeya/kakeya-2d.gif

Finally, a 3-dimensional 2-adic Kakeya set is displayed on Figure 8 and a movie showing it on different angles can be found at:

http://xavier.toonywood.org/papers/publis/kakeya/kakeya-3d.mp4

A Appendix: Discrete valuation fields

This appendix is dedicated to readers who are not familiar with non-archimedean geometry. It presents a quick summary of the most important basic definitions and facts of the domain. All the material presented below is very classical.

Definitions

A *discrete valuation field* is a field K equipped with a map $\mathrm{val} : K \to \mathbb{Z} \cup \{+\infty\}$ (the so-called *valuation*) satisfying the following axioms:

(i) $\mathrm{val}(x) = +\infty$ if and only if $x = 0$,

(ii) $\mathrm{val}(xy) = \mathrm{val}(x) + \mathrm{val}(y)$,

(iii) $\mathrm{val}(x + y) \geqslant \min(\mathrm{val}(x), \mathrm{val}(y))$

for all x and y in K. The valuation val is *non trivial* if there exists an element $x \in K^\star$ with $\mathrm{val}(x) \neq 0$. Under this additional assumption, the set $\mathrm{val}(K^\star)$ is a subgroup of $\mathbb{Z}$ and therefore is equal to $n\mathbb{Z}$ for some positive integer n. An element $\pi \in K$ of valuation n is called a *uniformizer* of K. One can always renormalize the valuation (by dividing it by n) in order to ensure $n = 1$.

The valuation on K readily defines a family of absolute values $|\cdot|_a$ $(a > 1)$ on K by:

$$\forall a \in (1, \infty), \forall x \in K, \quad |x|_a = a^{-\mathrm{val}(x)}$$

with the convention that $a^{-\infty} = 0$. Each of these absolute values defines a distance d_a on K by the usual formula $d_a(x, y) = |x - y|_a$. It is easily seen that all these distances define the same topology on K. We underline that d_a is ultrametric in the sense that:

$$\forall x, y, z \in K, \qquad d_a(x, z) \leqslant \max\big(d_a(x, y), d_a(y, z)\big). \tag{22}$$

This stronger version of the triangle inequalities has unexpected and important consequences. For instance it implies that $d_a(x, z) = \max\big(d_a(x, y), d_a(y, z)\big)$ as soon as $d_a(x, y) \neq d_a(y, z)$, showing then that every triangle in K is isosceles. Similarly if two balls B_1 and B_2 of K meet, we necessarily have $B_1 \subset B_2$ or $B_2 \subset B_1$.

Let R be the closed unit ball of K (this does not depend on the parameter a); alternatively R is the subset of K consisting of elements x with nonnegative valuation. An important remark following from axioms (ii) and (iii) is that R is a subring of K; it is usually called the *ring of integers* of K. The invertible elements in R are clearly exactly the elements of norm 1 (since the norm is multiplicative). On the contrary, the open unit ball $\mathfrak{m}$ is an ideal of R. It is actually the unique maximal ideal of R (showing that R is a local ring). It is moreover principal and generated by any uniformizer of K. The quotient $k = R/\mathfrak{m}$ is a field which is called the *residue field* of K.

Examples

1. Let p be a prime number. Recall that the *p-adic valuation* of a nonzero integer n is defined as the greatest integer v such that p^v divides n; it is often denoted by $v_p(n)$. This construction defines a function $v_p : \mathbb{Z}\backslash\{0\} \to \mathbb{N}$. We extend it to a function $\mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$ by setting:

$$v_p(0) = +\infty \quad \text{and} \quad v_p(\tfrac{a}{b}) = v_p(a) - v_p(b)$$

for $a, b \in \mathbb{Z}$. One checks that v_p satisfies the axioms of a valuation, turning then $\mathbb{Q}$ into a discrete valuation field. A uniformizer of $(\mathbb{Q}, v_p)$ is p. Its rings of integers is the ring $\mathbb{Z}_{(p)}$ consisting of fractions $\frac{a}{b}$ where b is not divisible by p. Its residue field is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

2. Let k be any field and $K = k(t)$ be the field of univariate rational fractions over k. Given $f \in K$, $f \neq 0$, let $\mathrm{ord}(f)$ denote the order of vanishing of f at 0, *i.e.* $\mathrm{ord}(f)$ is the unique integer for which one can write $f = t^{\mathrm{ord}(f)} \cdot g$ where $g \in k(t)$ is defined and does not vanish at 0. This defines a function $\mathrm{ord} : K^\star \to \mathbb{Z}$ that we extend to K by letting $\mathrm{ord}(0) = +\infty$. One then checks that (K, ord) is a discrete valuation field. Its ring of integers consists of fractions $\frac{f}{g}$ where f and g are polynomials with $g(0) \neq 0$. A uniformizer of (K, ord) is t and its residue field is canonically isomorphic to k.

Completeness

A discrete valuation field (K, val) is said *complete* is it complete[5] with respect to one (or equivalently all) d_a. Using the ultrametric triangle inequality (22), we easily check that, assuming that K is complete, a series $\sum_{n\geqslant 0} u_n$ (with $u_n \in K$) converges if and only if the sequence $(u_n)_{n\geqslant 0}$ converges to 0.

Let (K, val) be a discrete valuation field and let $\hat{K}_a$ be the completion of the metric space (K, d_a). One checks that $\hat{K}_a$ does not depend on a, so that we can denote it safely simply $\hat{K}$. Observe that the ring operations extend uniquely to $\hat{K}$, turning then it into a field. Similarly the continuous map $\mathrm{val} : K \to \mathbb{Z} \cup \{+\infty\}$ extends uniquely to $\hat{K}$, turning then $\hat{K}$ into a discrete valuation field. By construction $\hat{K}$ is moreover complete. The ring of integers $\hat{R}$ of $\hat{K}$ can be seen as the completion of R or, alternatively, as the topological closure of R in $\hat{K}$. Note moreover that a uniformizer of K remains a uniformizer of $\hat{K}$ (since the valuation on $\hat{K}$ extends that on K) and that the residue field of $\hat{K}$ is canonical isomorphic to that of K.

Elements in complete discrete valuation fields can be explicitely described as the values at a fixed uniformizer of particular power series.

Proposition A.1. *Let K be a complete discrete valuation field. Let R be its ring of integers, k be its residue field and π be a fixed uniformizer. Let $S \subset R$ be a fixed complete system of representatives of k and assume $0 \in S$. Then:*

(1) any element $x \in R$ can be written uniquely as a converging sum:

$$x = s_0 + s_1\pi + s_2\pi^2 + \cdots + s_n\pi^n + \cdots \tag{23}$$

with $s_n \in S$ for all $n \geqslant 0$

(2) any element $x \in K$ can be written uniquely as a converging sum:

$$x = s_v\pi^v + s_{v+1}\pi^{v+1} + s_{v+2}\pi^{v+2} + \cdots + s_n\pi^n$$

with $v \in \mathbb{Z}$, $s_n \in S$ for all $n \geqslant v$. We can moreover require that $s_v \neq 0$, in which case we have $v = \mathrm{val}(x)$.

[5] In the sense that all Cauchy sequences converge.

Proof. We only prove the first statement, the second being totally similar. We first remark that the series (23) converges since its general term $s_n\pi^n$ goes to 0 when n goes to infinity.

Assume first that we are given a decomposition (23). Then s_0 has to be congruent to x modulo π and therefore is uniquely determined since S is by definition a complete set of representatives of $k = R/\pi R$. Substrating s_0, dividing by π and applying the same reasoning, we find that s_1 is uniquely determined as well. Repeating this argument again and again, we get the unicity of the decomposition (23).

Now pick $x \in R$. Define s_0 as the unique element of S which is congruent to x modulo π. Then $r_1 = \frac{x-s_0}{\pi}$ lies in R. We can thus repeat the construction and define s_1 as the unique element of S which is congruent to r_1 modulo π. We construct this way an infinite sequence $(s_n)_{n\geqslant 0}$ of elements of S with the property that $x \equiv s_0 + s_1\pi + s_2\pi^2 + \cdots + s_{n-1}\pi^{n-1} \pmod{\pi^n}$ for all n. Passing to the limit (and noting that π^n goes to 0), we get (23). □

Examples

1. The field $\mathbb{Q}$ equipped with the p-adic valuation v_p is *not* complete. Its completion is the field of p-adic numbers $\mathbb{Q}_p$. A uniformizer of $\mathbb{Q}_p$ is p and its residue field is $\mathbb{Z}/p\mathbb{Z}$. The ring of integers of $\mathbb{Q}_p$ is usually denoted by $\mathbb{Z}_p$; its elements are the so-called p-adic integers. According to Proposition A.1, any p-adic integer can be uniquely written as a sum:

$$s_0 + s_1 p + s_2 p^2 + \cdots + s_n p^n + \cdots$$

with $s_n \in \{0, 1, \ldots, p-1\}$. It is the decomposition in p-basis of a p-adic integer.

2. Similarly, the field $k(t)$ equipped with the valuation ord is *not* complete. Thanks to Proposition A.1, its completion consists of series of the shape:

$$s_v t^v + s_{v+1} t^{v+1} + s_{v+2} t^{v+2} + \cdots + s_n t^n + \cdots$$

with $v \in \mathbb{Z}$ and $s_n \in k$. It is therefore nothing but the field of univariate Laurent series over k, usually referred to as $k((t))$. Its rings of integers is the ring of power series over k, namely $k[[t]]$. Again its rings of integers is canonically isomorphic to k.

The Haar measure

Let (K, val) be a *complete* discrete valuation ring with ring of integers R and residue field k. From now and until the end of this appendix, *we assume that k is finite*.

The first part of Proposition A.1 shows that R is homeomorphic to $k^{\mathbb{N}}$ (*i.e.* the set of all sequences with coefficients in k) and therefore is compact. Since R carries in addition a group structure, it is endowed with a unique Haar measure μ normalized by $\mu(R) = 1$. This measure extends uniquely to a Haar measure on K. Be careful nevertheless that $\mu(K)$ is infinite.

Under the additional assumptions of this paragraph, it is quite convenient to normalize the norm $|\cdot|$ on K by $|\pi| = \frac{1}{\mathrm{Card}\, k}$ where π is any uniformizer. (If the valuation is normalized so that it takes the value 1, the above norm is the norm $|\cdot|_{\mathrm{Card}\, k}$ we have introduced before.) The above convention leads to the expected relation:

$$\mu(aE + b) = |a| \cdot \mu(E)$$

for all $a, b \in K$ and all measurable subset E of K (and where $aE+b$ denotes of course the image of E under the affine transformation $x \mapsto ax + b$).

References

[1] Y. Babichenko, Y. Peres, R. Peretz, P. Sousi, P. Winkler, *Hunter, Cauchy Rabbit, and Optimal Kakeya Sets*, Trans. Amer. Math. Soc. **366** (2014), 5567–5586

[2] A. Besicovitch, *On Kakeya's problem and a similar one*, Math. Z. **27** (1928), 312–320

[3] E. Dummit, M. Hablicsek, *Kakeya sets over non-archimedean local rings*, Mathematika **59** (2013), 257–266

[4] Z. Dvir, *On the size of Kakeya sets in finite fields*, J. Amer. Math. Soc. **22** (2009), 1093–1097

[5] J. Ellenberg, R. Oberlin, T. Tao, *The Kakeya set and maximal conjectures for algebraic varieties over finite fields*, Mathematika **56** (2010), 1–25

[6] R. Fraser, *Kakeya-Type Sets in Local Fields with Finite Residue Field*, Mathematika **62** (2016), 614–629

[7] B. Green, *Restriction and Kakeya Phenomena*, lecture notes from a course at Cambridge, http://people.maths.ox.ac.uk/greenbj/papers/rkp.pdf

[8] N. Katz, T. Tao, *New bounds for Kakeya problems*, J. Anal. Math. **87** (2002), 231–263

[9] T. Wolff, *An improved bound for Kakeya type maximal functions*, Rev. Mat. Iberoamericana **11** (1995), 651–674

[10] T. Wolff, *Recent work connected with the Kakeya problem*, in *Prospects in mathematics* (Princeton, NJ, 1996), pp. 129–162, Amer. Math. Soc., Providence, RI (1999)