Max-Planck-Institut
für Mathematik
in den Naturwissenschaften
Leipzig

p-adic Integral Geometry

by

Avinash Kulkarni and Antonio Lerario

P–ADIC INTEGRAL GEOMETRY

AVINASH KULKARNI AND ANTONIO LERARIO

ABSTRACT. We prove a p-adic version of the Integral Geometry Formula for averaging the intersection of two p-adic projective algebraic sets. We apply this result to give bounds on the number of points in the modulo p^m reduction of a projective set (reproving a result by Oesterlé) and to the study of random p-adic polynomial systems of equations.

1. INTRODUCTION

Integral Geometry deals with "averaging" metric properties (e.g. the volume) of the intersection of two submanifolds of a homogeneous space under the action of a Lie group. This classical subject has a vast range of applications and connections to different areas of mathematics, including differential geometry [How93, San04, Ale03], representation theory [BF11, How93], convex geometry [SW08, SW93, Wei79], numerical analysis [AB15, BC13], and random geometry [EK95, BKL18]. The main goal of this paper is the adaptation of the ideas coming from this subject to the p-adic world. Before moving to the details, let us spend a few words discussing the classical framework.

1.1. **Classical Integral Geometry.** The main reference we have in mind for this section is the monograph [How93], where the spherical case is discussed; here we prefer to discuss the projective case as it offers a closer analogy with the results of this article.

Let $A, B \subset \mathbb{RP}^n$ be two compact submanifolds of dimension $\dim(A) = a$ and $\dim(B) = b$. We endow the projective space with the quotient metric from the unit sphere $S^n \subset \mathbb{R}^{n+1}$ and, restricting this metric to a submanifold Y of dimension $\dim(Y) = k$, we get a natural notion of Riemannian k-dimensional volume of Y, which we denote by $\mathrm{vol}_k(Y)$. More generally, if Y is a codimension $m - k$ submanifold of a Riemannian manifold M whose volume density is vol and $U(Y, \epsilon) = \bigcup_{x \in Y} B(x, \epsilon)$ denotes the ϵ-neighborhood of Y in M, then

$$(1.1) \qquad \mathrm{vol}_k(Y) := \lim_{\epsilon \to 0} \frac{\mathrm{vol}(U(Y, \epsilon))}{\mathrm{vol}(B_{\mathbb{R}^{m-k}}(0, \epsilon))}.$$

The volume of the projective space $\mathbb{RP}^k \subseteq \mathbb{RP}^n$ with the quotient metric is

$$\mathrm{vol}_k(\mathbb{RP}^k) = \frac{\pi^{\frac{k+1}{2}}}{\Gamma\left(\frac{k+1}{2}\right)}.$$

The group $G = O(n+1)$ acts on the projective space by isometries, and by a standard transversality argument, the intersection $A \cap gB$ is transversal and of codimension $(n - a) + (n - b)$, i.e. of dimension $k = n - (n - a) - (n - b)$, for almost every $g \in G$. The Integral Geometry Formula [How93, Corollary 3.9] then tells that:

$$(1.2) \qquad \int_G \frac{\mathrm{vol}_k(A \cap gB)}{\mathrm{vol}_k(\mathbb{RP}^k)} \, dg = \frac{\mathrm{vol}_a(A)}{\mathrm{vol}_a(\mathbb{RP}^a)} \cdot \frac{\mathrm{vol}_b(B)}{\mathrm{vol}_b(\mathbb{RP}^b)},$$

where the integral is with respect to the normalized Haar measure $\int_G dg = 1$, and the integrand is finite for almost every $g \in G$ (by transversality). The identity (1.2) is very remarkable and has many interesting applications. The spirit of this paper is much influenced by one of these applications in particular, due to [EK95], where the idea of combining (1.2) with algebraic geometry and Example 1 first appeared.

Example 1 (How many zeros of a random polynomial are real?)**.** Let $f \in \mathbb{R}[x_0, x_1]_{(d)}$ be the random polynomial given by:

$$(1.3) \qquad f(x_0, x_1) = \xi_0 x_0^d + \cdots + \xi_k \sqrt{\binom{d}{k}} x_0^{d-k} x_1^k + \cdots + \xi_d x_1^d,$$

where $\{\xi_k\}_{k=0}^d$ is a family of i.i.d. standard Gaussians. In [EK95] the authors use a nice argument from integral geometry to show that the expectation of the number of zeroes on $\mathbb{RP}^1$ of the random polynomial (1.3) is $\sqrt{d}$. The argument goes as follows. One first considers the *Veronese* embedding $\nu : \mathbb{RP}^1 \to \mathbb{RP}^d$ given by:

$$\nu : [x_0, x_1] \mapsto \left[x_0^d, \ldots, \sqrt{\binom{d}{k}} x_0^{d-k} x_1^k, \ldots, x_1^d \right].$$

Using the properties of the Gaussian distribution, one then proves that the average number of zeroes of (1.3) equals the average number of points of intersection of $\nu(\mathbb{RP}^1)$ with a randomly sampled hyperplane $g\mathbb{RP}^{n-1} \subset \mathbb{RP}^n$, with $g \in O(n+1)$ drawn from a uniform distribution. Finally, by (1.2), this expectation equals

$$(1.4) \qquad \mathbb{E}\#\{f = 0\} = \frac{\mathrm{vol}_1(\nu(\mathbb{RP}^1))}{\mathrm{vol}_1(\mathbb{RP}^1)} = \sqrt{d}.$$

In other words, by using the integral geometry formula, we see that the expectation of the number of zeros of a random polynomial with respect to a particular distribution is determined by the length of the corresponding Veronese curve. We observe, however, that computing the length of a Veronese curve is in general not trivial. In Theorem 36 we will prove the p-adic version of the results discussed in this example.

1.2. p-adic Integral Geometry.

Keeping Section 1.1 in mind, let us discuss now the content of the current paper. We begin with the geometry of the ambient space. We denote by $\mathbb{Q}_p$ the field of p-adic numbers, endowed with the standard p-adic norm, and by $\mathbb{Z}_p$ the ring of p-adic integers. The vector space $\mathbb{Q}_p^{n+1}$ is endowed with the norm:

$$\|(a_0, \ldots, a_n)\|_p = \sup_i |a_i|_p, \quad (a_0, \ldots, a_n) \in \mathbb{Q}_p^{n+1}.$$

Together with the metric structure, we also consider the standard p-adic measure μ, defined on the Borel sets of $\mathbb{Q}_p^{n+1}$ and normalized by $\mu(\mathbb{Z}_p^{n+1}) = 1$, see Section 2.4.

We also turn the p-adic projective space $\mathbb{P}^n$ into a metric measure space as follows. First we consider the Hopf fibration $\varphi : S^n \to \mathbb{P}^n$, where S^n is the open and compact subset of $\mathbb{Q}_p^{n+1}$ consisting of points $a = (a_0, \ldots, a_n) \in \mathbb{Q}_p^{n+1}$ such that $\|a\|_p = 1$ and φ is the natural projection map. Unlike the real case, the p-adic unit sphere as a p-adic analytic manifold *is not* of dimension n, but of dimension $n+1$ (see Figure 1). Nevertheless, we have decided to retain the same notation due to the strong parallels with the real case.

The metric structure on $\mathbb{P}^n$ is then defined by:

$$(1.5) \qquad d(x, y) = \|\hat{x} \wedge \hat{y}\|_p, \quad x, y \in \mathbb{P}^n,$$

where $\hat{x} \in \varphi^{-1}(x)$ and $\hat{y} \in \varphi^{-1}(y)$ are any two preimages and $\hat{x} \wedge \hat{y} \in \Lambda^2(\mathbb{Q}_p^{n+1})$. For the measure, we take the normalized pushforward $\frac{\varphi_*\mu}{1+p^{-1}}$. When there is no risk of ambiguity we will still denote this measure by μ.

The main ingredients to formulate an identity in the style of (1.2) are (1) the action on a topological space X of a topological compact group G endowed with a measure and (2) a notion of "volume" and "dimension" for subspaces of X. In this paper the group will be $G = \mathrm{GL}_{n+1}(\mathbb{Z}_p)$, which acts by isometries and measure preserving transformations on $X = \mathbb{P}^n$. For the sake of this introductory section we will take $X = \mathbb{P}^n$, but the results we will present are also valid for the p-adic sphere $S^n \subset \mathbb{Q}_p^{n+1}$ (see Section 2.2). We endow $\mathrm{GL}_{n+1}(\mathbb{Z}_p)$ with the normalized Haar measure:

$$\int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} dg = 1.$$

The class of submanifolds of $\mathbb{P}^n$ that we will consider consists of algebraic sets (but this condition can also be weakened to consider stratified $\mathbb{Q}_p$-analytic sets, see Section 2.2). In this case the *dimension* of an algebraic set $A \subseteq \mathbb{P}^n$ is the one coming from algebraic geometry; the notion of *volume* is less standard. Denoting by $B(x,r)$ the ball of radius r centered at $x \in \mathbb{P}^n$ (with respect to the metric (1.5)), for an algebraic set $Y \subseteq \mathbb{P}^n$ of dimension $\dim(Y) = k$ we define its volume, based on the work of [Ser81] and [Oes82], by:

$$(1.6) \qquad \mathrm{vol}_k(Y) := \lim_{m \to \infty} p^{m(n-k)} \cdot \mu\left(\bigcup_{x \in Y} B(x, p^{-m})\right).$$

Notice that this definition mimics the classical definition given in (1.1). The volume of the p-adic projective space equals (via Section 2.4):

$$\mathrm{vol}_k(\mathbb{P}^k) = \frac{1 - p^{-(k+1)}}{1 - p^{-1}}.$$

The main theorem around which this paper revolves is Theorem 35, restated below.

Theorem 2 (*p-adic Integral Geometry Formula*). *Let* $A, B \subset \mathbb{P}^n$ *be algebraic sets of dimensions* $\dim(A) = a, \dim(B) = b$. *Then for almost all* $g \in \mathrm{GL}_{n+1}(\mathbb{Z}_p)$ *the intersection* $A \cap gB$ *is transversal, of dimension* $k = n - (n-a) - (n-b)$, *and:*

$$(1.7) \qquad \int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \frac{\mathrm{vol}_k(A \cap gB)}{\mathrm{vol}_k(\mathbb{P}^k)} dg = \frac{\mathrm{vol}_a(A)}{\mathrm{vol}_a(\mathbb{P}^a)} \cdot \frac{\mathrm{vol}_b(B)}{\mathrm{vol}_b(\mathbb{P}^b)}.$$

Notice the exact analogy between (1.2) and (1.7). Before presenting a couple of applications, let us commentate on the notion of volume (1.6) that we use in Theorem 2.

First, since Y sits inside the metric space $\mathbb{P}^n$, it is possible to define its Hausdorff dimension, which coincides with its dimension $k = \dim(Y)$ as an algebraic set, and its k-dimensional Hausdorff measure turns out to be equal to its k-dimensional volume.

Second, a result of Oesterlé [Oes82, Theorem 2] connects the number of congruence classes of points mod p^m in Y and the volume of Y. Specifically, denoting by $N_m(Y)$ the number of points of Y in its modulo-p^m reduction (see Definition 14), we prove that:

$$\mathrm{vol}_k(Y) = \lim_{m \to \infty} \frac{N_m(Y)}{p^{mk}}.$$

In fact, if Y is smooth, then the limit above "stabilizes" for large enough m. The aforementioned result, as well as the finiteness of the limit above, were both proven by Serre in [Ser81]. We give a simplified proof of Oesterlé's result, which we state as Corollary 25 and Corollary 28.

$(-1, 1) + (3\mathbb{Z}_3)^2$	$(0, 1) + (3\mathbb{Z}_3)^2$	$(1, 1) + (3\mathbb{Z}_3)^2$
$(-1, 0) + (3\mathbb{Z}_3)^2$	$(0, 0) + (\mathbb{Z}_3)^2$	$(1, 0) + (3\mathbb{Z}_3)^2$
$(-1, -1) + (3\mathbb{Z}_3)^2$	$(0, -1) + (3\mathbb{Z}_3)^2$	$(1, -1) + (3\mathbb{Z}_3)^2$

FIGURE 1.   A depiction of the 3-adic unit circle S^1 in $\mathbb{Z}_3^2$. Each cell represents an open ball of radius $\frac{1}{3}$ centered at the indicated point. The union of all the unshaded cells is S^1. The unit $-1 \in \mathbb{Z}_3^\times$ acts by reflecting the diagram through the origin. Note that S^1 has non-zero measure inside $\mathbb{Z}_3^2$, as well as the pullback $\varphi^{-1}(U)$ of any non-empty open subset of $\mathbb{P}^1$.

Third, all this discussion on volumes and the p-adic Integral Geometry Formula is valid for open compact subsets of Y as well as for the subset of smooth points of Y. The volume of the smooth sublocus of Y and the volume of Y are equal, see Corollary 25 and Corollary 26.

Fourth, by taking $B \subset \mathbb{P}^n$ to be a subspace of complementary dimension $B = \mathbb{P}^{n-k}$, we see by the p-adic Integral Geometry formula that the volume of Y satisfies the identity:

$$\mathrm{vol}_k(Y) = \mathrm{vol}_k(\mathbb{P}^k) \cdot \int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \# \left(Y \cap g\mathbb{P}^{n-k} \right) dg.$$

This last observation allows us to prove a slightly weaker version of a result of Oesterlé [Oes82, Theorem 1], though with a substantially simpler proof. Oesterlé's result provides an estimate for the number of points in the modulo-p^m reduction of a $\mathbb{Z}_p$-algebraic set. Here again we state the projective version of this result.

Corollary 3. *Let $Y \subseteq \mathbb{P}^n$ be an algebraic set of dimension k and degree d. Then $\mathrm{vol}_k(Y) \leq d$. Moreover, if $\mathrm{vol}_k(Y) < d$, then for m large enough:*

$$N_m(Y) \leq d \cdot p^{mk}\mathrm{vol}_k(\mathbb{P}^k).$$

Proof. Note that the integrand of 1.2 is bounded by the degree for almost all $g \in \mathrm{GL}_{n+1}(\mathbb{Z}_p)$. If $\mathrm{vol}_k(Y) < d$, then the result follows immediately.   □

Remark 4. The second conclusion of the result above holds under the hypothesis that Y is equidimensional. If Y is not the union of $\deg Y$ linear subspaces, then there is a smooth point $y \in Y(\mathbb{Q}_p)$ such that the tangent space $H := T_y Y$ intersects Y with multiplicity exactly 2 at y. By perturbing H, we can construct a linear subspace H' such that $\#(H' \cap Y) < d - 2$. More precisely, such that at least two points of $H' \cap Y$ are defined over a ramified extension

of $\mathbb{Q}_p$. In particular, the interior of the subset

$$U := \{g \in \mathrm{GL}_{n+1}(\mathbb{Z}_p) : \#(Y \cap g\mathbb{P}^{n-k}) < d\}.$$

is non-empty, and thus we have that $\mathrm{vol}_k(Y) < d$. The claim then follows from Corollary 3.

Conversely, the hypothesis that Y is equidimensional is necessary. For instance, for Y the union of d lines and a points in $\mathbb{P}^2$, then $N_m(Y)$ over-estimates the volume for almost all m.

1.3. **Random p-adic polynomials.** We show how to apply the p-adic Integral Geometry Formula to study random p-adic polynomials, in a spirit similar to Example 1 above. In the paper [Eva06], Evans considers the problem of studying the expectation of the number of zeros in $\mathbb{Z}_p^n$ of a system of random p-adic polynomials. The distribution that Evans considers comes from picking Gaussian p-adic coefficients in front of the Mahler basis (see [Eva06] for more details on the notion of p-adic gaussian variable). When $n = 1$, this means considering the following random polynomial:

$$(1.8) \qquad g(t) := \zeta_0 + \zeta_1 \binom{t}{1} + \ldots + \zeta_d \binom{t}{d},$$

where $\{\zeta_k\}_{k=0}^d$ is a family of i.i.d. uniform variables in $\mathbb{Z}_p$. Evans computed the expected number of zeroes of g in $\mathbb{Z}_p$; using our techniques we recover and extend this result, computing the expectation of the number of zeroes on the whole p-adic line. More precisely, in Section 5.2 we prove the following result.

Theorem 5. *Let $g(t)$ be the random p-adic polynomial* (1.8).

(1) *The expected number of zeroes in $\mathbb{Z}_p$ of g equals* $\frac{p^{\lfloor \log_p d \rfloor}}{1+p^{-1}}$ *(this is Evans' result).*

(2) *For every $m \geq 1$ the expected number of zeroes of g in the annulus $\frac{1}{p^m}\mathbb{Z}_p \backslash \frac{1}{p^{m-1}}\mathbb{Z}_p$ equals $\frac{|d|_p}{p^m}\frac{1-p^{-1}}{1+p^{-1}}$ and in particular:*

$$\mathbb{E}\#\{g = 0\} = \frac{p^{\lfloor \log_p d \rfloor}}{1+p^{-1}} + \sum_{m \geq 1} \frac{|d|_p}{p^m}\frac{1-p^{-1}}{1+p^{-1}} = \frac{p^{\lfloor \log_p d \rfloor} + |d|_p p^{-1}}{1+p^{-1}}.$$

In this paper we also consider a different model that seems more natural over the projecive space, due to its invariance under the group $\mathrm{GL}_{n+1}(\mathbb{Z}_p)$. In the case $n = 1$, we define the random p-adic polynomial:

$$(1.9) \qquad f(x_0, x_1) = \zeta_0 x_0^d + \cdots + \zeta_k x_0^{d-k} x_1^k + \cdots + \zeta_d x_1^d,$$

where $\{\zeta_k\}_{k=0}^d$ is a family of i.i.d. uniform variables in $\mathbb{Z}_p$. This distribution is invariant under $\mathrm{GL}_2(\mathbb{Z}_p)$-change of variables – there are no preferred points or directions in the projective line $\mathbb{P}^1$. For the random polynomial (1.9) we prove the following (surprising) result.

Proposition 6. *The expected number of zeroes of the polynomial* (1.9) *in $\mathbb{P}^1$ is 1. Moreover the density of zeroes on $\mathbb{P}^1$ is uniform.*

In fact, we prove a much more general theorem which relates the expectation of the number of zeroes of a system of random p-adic equations with the volume of the image of $\mathbb{P}^n$ under an appropriate "Veronese" map (as in [EK95]). In the case of the polynomial (1.9) the Veronese map to consider is $\nu : \mathbb{P}^1 \to \mathbb{P}^d$ given by $[x_0, x_1] \mapsto [x_0^d, \cdots, x_0^{d-k}x_1^k, \ldots, x_1^d]$ and, in analogy with (1.4), we have:

$$\mathbb{E}\#\{f = 0\} = \frac{\mathrm{vol}_1(\nu(\mathbb{P}^1))}{\mathrm{vol}_1(\mathbb{P}^1)} = 1.$$

Once again, the computation of the length of the Veronese curve is an essential step to obtain the result. For us, this is given in Proposition 38.

1.4. **Applications.** We discuss some of the many interesting ties that classical integral geometry has to applied mathematics, showing some evidence on how p-adic integral geometry can be used for similar purposes. We focus on the most concrete applications, though we point out that p-adic integral expressions appear in many applied disciplines [VVZ94, DKK$^+$17].

In *numerical linear algebra*, one must generally be aware of the ill-conditioned inputs to some algorithm, such as solving a linear system or numerically finding the roots of a polynomial. If the set of ill-posed problems is defined by a variety, such as a vanishing determinant or discriminant locus, then the problems that are badly conditioned are described by a small neighbourhood of this algebraic variety. Hence, by the Weyl-tube formula, integral geometry allows one to calculate the probability that a randomly sampled problem is ill-conditioned [Dem88, BC13]. It was observed by Dixon [Dix82] that an exact solution to a linear system of equations over the rationals can be obtained by p-adic methods even when the system is numerically ill-conditioned over the reals. More precisely, that the p-adic condition number and the real condition number are not necessarily correlated. For example, the Hilbert matrix H_n, whose real condition number is $O(n^{-\frac{1}{2}}(1+\sqrt{2})^{4n})$, has a much smaller condition number over the p-adics; the inverse of H_n has integer coefficients and therefore $\|H_n^{-1}\|_p \leq 1$, so as a consequence, its p-adic condition number is $O(n)$ [Car17].

This idea of the study of the geometry of ill-conditioned samples through integral geometry is crucial in numerical algebraic geometry [BC13, Dem88, Car17, SS93] and motivates its extension to the p-adic world. Specifically this is the problem of studying the p-adic tube around the variety of ill-posed problems as a measure of the probability that an input is p-adically ill-conditioned, for instance in the sense of [CRV15, Car17, Kul19]. In the case of a linear problem, the volume of this tube depends on the volume of the set of p-adic matrices of determinant zero and operator norm 1. We intend to discuss this and related questions in future work, building on the techniques that we develop in the current paper.

Between *statistics* and integral geometry there is also a link that appears to have a p-adic analogue. In Stereology, important properties of a statistical model described by algebraic equations can be estimated via geometric quantities, and in nice cases random samples can be modeled as random subvarieties – see [Kid13, Chapter 2] for more specifics. Real integral geometry picks up on features of the statistical model apparent in the real topology. When dealing with rational equations, it is plausible that p-adic features of the statistical model capture useful information as well, and can be just as easily learned using p-adic integral geometry. We give a concrete example of the connection to statistics in Section 5, where we study properties of a model with p-adic Gaussian random variables.

Finally, p-adic integral geometry might have new applications without classical inspiration. For example, it is important in *cryptography* to quickly determine the number of points on a variety over a finite field. For a projective variety that is smooth over $\mathbb{Z}_p$, we can express its p-adic volume both in terms of the Weil canonical measure and via the integral geometry formula. Thus, we can accurately estimate the number of points on a variety over $\mathbb{F}_p$ via Monte-Carlo integration. Should a similar integral geometry formula hold for varieties over unramified extensions of $\mathbb{Q}_p$, we expect a generalization to point counting on varieties over $\mathbb{F}_q$.

2. Preliminaries

2.1. Notation.

$$
\begin{array}{rcl}
|\cdot|_p & - & \text{The } p\text{-adic absolute value, with normalization } |p|_p = p^{-1}. \\
\|\cdot\|_p & - & \text{The norm of a vector in } \mathbb{Q}_p^{n+1} \\
R_m & - & \text{The ring } \mathbb{Z}/p^m\mathbb{Z} \text{ of integers modulo } p^m. \\
\mathbb{P}^n & - & \text{Projective space over } \mathbb{Q}_p \\
B(a;p^{-m}) & - & \text{The ball in a metric space centered at } a \text{ of radius } p^{-m} \\
N_m(U) & - & \text{The minumum number of balls of radius } p^{-m} \text{ needed to cover } U \\
& & \text{(alternatively: the number of points in the modulo } p^m \text{ reduction of } U) \\
S^n & - & \text{The unit sphere in } \mathbb{Q}_p^{n+1} \\
|J_{\mathbf{f}}(a)|_p & - & \text{The absolute value of the determinant of the Jacobian matrix for} \\
& & \text{the polynomials } \mathbf{f}. \text{ (In the projective case, normalized by the norm of } a.) \\
\varphi & - & \text{The Hopf fibration } \varphi\colon S^n \dashrightarrow \mathbb{P}^n
\end{array}
$$

2.2. Affine and projective sets and their stratification.

A $\mathbb{Q}_p$-analytic manifold is defined analogously to a real or complex analytic manifold. i.e, in terms of charts and gluing maps. For the reader interested in the technical details, we refer to [Sch11, Part II]. Similarly, if $\overline{\mathbb{Q}_p}$ is an algebraic closure of $\mathbb{Q}_p$, there is the corresponding notion of $\overline{\mathbb{Q}_p}$-analytic manifold.

For a smooth projective algebraic variety X defined over $\mathbb{Q}_p$, the set of $\mathbb{Z}_p$-points of X has the structure of a $\mathbb{Q}_p$-analytic manifold. It is necessary for us to consider algebro-geometric objects whose set of $\mathbb{Z}_p$-points does not have the structure of a $\mathbb{Q}_p$-analytic manifold.

Definition 7. A *stratified $\mathbb{Q}_p$-analytic set* is a set X which admits a decomposition into finitely many subsets (called *strata*)

$$
X := \coprod_{i=1}^{k} X_i
$$

such that each X_i is a $\mathbb{Q}_p$-analytic manifold. The *dimension* of X is the maximal dimension of the strata. If X is empty we consider the empty coproduct and we set $\dim(X) = -\infty$.

The previous notion of stratified set is weaker than the usual notion coming from semialgebraic geometry, singularity theory or algebraic geometry, but all we need in this paper is to be able to decompose the sets we are working with into finitely many disjoint pieces (the strata) each one of which is a $\mathbb{Q}_p$-analytic manifold.

Note that for a stratified $\mathbb{Q}_p$-analytic set, the pieces need not be open or closed submanifolds of X, nor is the decomposition unique. Our central category of interest is the category of (analytically) open compact subsets of algebraic sets. At this point, it is convenient to define some notation we will use throught the paper.

Definition 8. Let $X \subseteq \mathbb{Q}_p^n$ be an algebraic set of codimension r, and let $a \in X$ be a smooth point. Let $\mathbf{f} := (f_1, \ldots, f_r)$ be local equations for X at a. Then we define

$$
|J_{\mathbf{f}}(a)|_p := \sup_I \left\{ |M_{\mathbf{f},I}(a)|_p : M_{\mathbf{f},I} \text{ is an } r \times r \text{ minor of } J_{\mathbf{f}}(a) \right\}.
$$

Let $X \subseteq \mathbb{P}^n$ be a projective algebraic set of codimension r, let $a \in X$ is a smooth point, and let $\mathbf{f} := (f_1, \ldots, f_r)$ be local equations for X at a. With $\delta := \sum_{i=1}^{r}(\deg(f_i) - 1)$, we define

$$
|J_{\mathbf{f}}(a)|_p := \sup_I \left\{ \frac{|M_{\mathbf{f},I}(a)|_p}{\|a\|_p^\delta} : M_{\mathbf{f},I} \text{ is an } r \times r \text{ minor of } J_{\mathbf{f}}(a) \right\}.
$$

Note in the projective definition that $|J_{\mathbf{f}}(a)|_p$ is independent of the choice of homogeneous coordinates of a. However, both definitions are sensitive to the choice of defining equations.

Remark 9. If $U \subseteq X$ is an open compact subset of the smooth subset of X, then there is a finite set of points $a_1, \ldots, a_k$ and open subsets $U_1, \ldots, U_k$ of U such that each $X \cap U_i$ is defined by the local equations at a_i and such that $U = \bigcup_{i=1}^{k} U_i$. In particular, the function $a \mapsto \sup_{1 \le i \le k} |J_{\mathbf{f}_i}(a)|_p$ is bounded away from 0 on U.

Proposition 10. *Let $X \subseteq \mathbb{Q}_p^n$ be an algebraic set. Then X is a stratified $\mathbb{Q}_p$-analytic set.*

Proof. Write $X := Z(f_1, \ldots, f_r)$. Let $\overline{\mathbb{Q}}_p$ denote an algebraic closure of $\mathbb{Q}_p$, and let $X(\overline{\mathbb{Q}}_p)$ be the common zero locus of $f_1, \ldots, f_r$ over $\overline{\mathbb{Q}}_p$. We may assume that $f_1, \ldots, f_r$ generate a radical ideal. The singular sublocus $Y(\overline{\mathbb{Q}}_p)) = \mathrm{Sing}(X(\overline{\mathbb{Q}}_p))$ of $X(\overline{\mathbb{Q}}_p)$ is defined by the vanishing of the maximal minors of the Jacobian matrix, and so has positive codimension in $X(\overline{\mathbb{Q}}_p)$. We may write $X(\overline{\mathbb{Q}}_p) := (X(\overline{\mathbb{Q}}_p) \backslash Y(\overline{\mathbb{Q}}_p)) \cup Y(\overline{\mathbb{Q}}_p)$, and $(X(\overline{\mathbb{Q}}_p) \backslash Y(\overline{\mathbb{Q}}_p))$ is a $\overline{\mathbb{Q}}_p$-analytic manifold. Iterating, we obtain a decomposition

$$X(\overline{\mathbb{Q}}_p) := \coprod_{i=1}^{k} X_i(\overline{\mathbb{Q}}_p).$$

Note that a point in $X(\mathbb{Q}_p)$ is smooth in the algebraic sense if and only if it is also a smooth point of $X(\overline{\mathbb{Q}}_p)$. As algebraic smoothness implies analytic smoothness, the result follows by considering the decomposition (with some strata possibly empty over $\mathbb{Q}_p$):

$$X = X(\mathbb{Q}_p) = \coprod_{i=1}^{k} X_i(\mathbb{Q}_p) \qquad \square$$

Remark 11. Note that $\mathbb{P}^n$ can be written as

$$\mathbb{P}^n := \coprod_{r=0}^{n} \mathbb{Q}_p^r$$

and that this is a stratification. In particular, if X is any projective algebraic set then each component of $X = \coprod_{r=0}^{n}(\mathbb{Q}_p^r \cap X)$ is a stratified $\mathbb{Q}_p$-analytic set. Alternatively, by restricting to affine local patches, we see the $\mathbb{Q}_p$-points of any separated scheme of finite type over $\mathbb{Q}_p$ is also a stratified $\mathbb{Q}_p$-analytic set, and the assignment $X \mapsto X(\mathbb{Q}_p)$ is functorial. However, $\mathbb{P}^n(R_m)$ is not equal to $\coprod_{r=0}^{n}(R_m)^r$ when $m > 1$, since R_m has a nontrivial ideal.

For any projective variety X over $\mathbb{Z}_p$, we have that $X(\mathbb{Z}_p) = X(\mathbb{Q}_p)$. There is a natural map defined by

$$\varphi: \quad \begin{array}{ccc} S^n & \to & \mathbb{P}^n(\mathbb{Z}_p) \\ (x_0, \ldots, x_n) & \mapsto & [x_0, \ldots, x_n] \end{array}$$

which is well-defined since $(0, \ldots, 0) \notin S^n$. Plainly, we have that φ is a surjective, $\mathbb{Q}_p$-analytic, and hence measurable map. We have $\varphi^{-1}\{[x_0, \ldots, x_n]\} = \{(\lambda x_0, \ldots, \lambda x_n) : \lambda \in \mathbb{Z}_p^{\times}\}$. Inspired by the real and complex settings, we give this map the name:

Definition 12. We call the map φ the *Hopf fibration*.

2.3. **Modulo p^m reduction.** We now discuss the relations of our models and their reductions modulo p^m. Denote

$$S^n(R_m) := \{(x_0, \ldots, x_n) : x_i \in R_m \text{ and at least one } x_i \in R_m^{\times}\}.$$

As the next result indicates, reduction modulo p^m commutes with projectivizing coordinates.

Proposition 13. *Let $m > 0$ be an integer, let $U \subseteq \mathbb{P}^n$ be any subset. The following diagram (of continuous functions) commutes:*

$$
\begin{array}{ccc}
\varphi^{-1}(U) & \xrightarrow{\ \varphi\ } & U \\
\widehat{\pi}_m \downarrow & & \downarrow \pi_m \\
\widehat{\pi}_m(\varphi^{-1}(U)) & \xrightarrow{\ \varphi_m\ } & \pi_m(U)
\end{array}
$$

The map φ_m is defined by restricting the natural map

$$
\begin{array}{rccc}
\varphi_m \colon & S^n(R_m) & \to & \mathbb{P}^n(R_m) \\
& (x_0, \ldots, x_n) & \mapsto & [x_0, \ldots, x_n].
\end{array}
$$

Moreover, for any $x \in \mathbb{P}^n(R_m)$, we have

$$(2.1) \qquad \#\varphi_m^{-1}(x) = \#R_m^\times = p^m \left(1 - \frac{1}{p} \right).$$

Proof. By definition, any $x \in U$ has at least one coordinate not in $p\mathbb{Z}_p$. Since $\pi_m(\mathbb{Z}_p^\times) = R_m^\times$ for all m, the result follows. $\square$

Definition 14 (Number of points modulo p^m). If $U \subseteq A \subseteq \mathbb{Z}_p^n$ is a subset of an algebraic set, we define $N_m(U) = \#\widehat{\pi}_m(U)$. In the projective case, if $U \subseteq A \subseteq \mathbb{P}^n$ is a subset of an algebraic set, we define $N_m(U) = \#\pi_m(U)$.

Example 15. Proposition 13 allows us to determine $N_m(\mathbb{P}^n)$ easily. We have that

$$\#S^n(R_m) = (\#R_m)^{n+1} - (\#pR_m)^{n+1} = p^{m(n+1)} - p^{(m-1)(n+1)},$$

as the maximal ideal of R_m is generated by p. In particular, using (2.1), we get:

$$\#\mathbb{P}^n(R_m) = \frac{p^{m(n+1)} - p^{(m-1)(n+1)}}{p^m - p^{m-1}} = \frac{p^{mn} - p^{m(n-1)-1}}{1 - p^{-1}}.$$

Notice that this number is *not* equal to $\#(R_m)^n + \ldots + \#R_m + 1$ in general. This explicitly demonstrates why $\mathbb{P}(R_m)$ is generally not equal to $\coprod_{r=0}^{n}(R_m)^r$.

2.4. **Measures and metrics.** On projective space, we obtain a naturally defined quotient measure and quotient metric from the unit sphere (see for instance [Cho00]).

Definition 16. We define the (normalized) pushforward measure on projective space by

$$\mu(U) := \frac{1}{\mu(\mathbb{Z}_p^\times)} \cdot \mu(\varphi^{-1}(U)).$$

Definition 17. We define the metric $d(x, y)$ for $x, y \in \mathbb{P}^n$ by

$$(2.2) \qquad d(x, y) := \| \hat{x} \wedge \hat{y} \|_p$$

for any $\hat{x} \in \varphi^{-1}(x)$ and $\hat{y} \in \varphi^{-1}(y)$.

The metric in Definition 17 is the natural quotient metric, and any subset $A \subset \mathbb{P}^n$ can be turned into a metric space by restricting the metric to A. Our normalization of the pushforward measure ensures that for any $x \in \mathbb{P}^n$ and $m > 0$, the ball $B(x; p^{-m}) \subseteq \mathbb{P}^n$ has measure p^{-mn}. When $m = 0$, we have $B(x; 1) = \mathbb{P}^n$ for any $x \in \mathbb{P}^n$, so

$$\mu(\mathbb{P}^n) = (1 - p^{-1})^{-1}\mu(S^n) = \frac{1 - p^{-(n+1)}}{1 - p^{-1}}.$$

2.5. **Hensel's lemma.** One of the main ideas in our arguments of Section 4 is to locally approximate the smooth sublocus of a stratified p-adic algebraic set by its tangent cone. In this section, we review the technical results needed to implement this idea.

Lemma 18 (Hensel's lemma). *Let* $\mathbf{f} = (f_1, \ldots, f_n) \in \mathbb{Z}_p[x_1, \ldots, x_n]^n$, *let* m *be a positive integer, let* $a \in \mathbb{Z}_p^n$, *and let* $J_{\mathbf{f}}(a)$ *be the Jacobian matrix of* $\mathbf{f}$ *at* a. *If* $\|\mathbf{f}(a)\|_p < |J_{\mathbf{f}}(a)|_p^2$, *then there is a unique* $\alpha \in \mathbb{Z}_p^n$ *such that* $\mathbf{f}(\alpha) = 0$ *and* $\alpha \equiv a \pmod{p}^m$.

Proof. See Keith Conrad's notes [Con] (unpublished) or [Fis97, Theorem 1] (published). □

The p-adic analytic implicit function theorem is the second critical tool we need. The formulation below is due to Igusa [Igu00, Theorem 2.2.1].

Theorem 19 (Implicit Function Theorem). *Denote* $\mathbb{Z}_p[\![x, y]\!] = \mathbb{Z}_p[\![x_1, \ldots, x_r, y_1, \ldots, y_{n-r}]\!]$ *the ring of formal power series in the variables* $x_1, \ldots, y_{n-r}$ *with coefficients in* $\mathbb{Z}_p$. *Then:*

(1) *If* $F_i(x, y)$ *is in* $\mathbb{Z}_p[\![x, y]\!]$ *and* $F_i(0, 0) = 0$ *for all* i *and further*

$$\frac{\partial(F_1, \ldots, F_{n-r})}{\partial(y_1, \ldots, y_{n-r})}(0, 0) \not\equiv 0 \mod p,$$

then every $f_i(x)$ *in the unique solution* $f = (f_1, \ldots, f_{n-r})$ *of* $F(x, f(x)) = 0$ *satisfying* $f_i(0) = 0$ *is in* $\mathbb{Z}_p[\![x]\!]$.

(2) *If* $a \in B(0; p^{-1})$, *then* $f(a) \in \mathbb{Z}_p^{n-r}$ *and* $F(a, f(a)) = 0$. *Furthermore, if* $(a, b) \in p\mathbb{Z}_p^r \times p\mathbb{Z}_p^{n-r}$ *satisfies* $F(a, b) = 0$, *then* $b = f(a)$.

The statement of part (2) is slightly modified from Igusa [Igu00, Theorem 2.2.1], but is equivalent (see [Igu00, p22]). In our study of embedded p-adic algebraic sets, we can give an explicit quantitative version of the Implicit Function Theorem.

Proposition 20. *Let* $X \subseteq \mathbb{Q}_p^n$ *be an algebraic set and let* $a \in X$ *be a smooth point. Let* $\mathbf{f}$ *be a set of* r *local generators for* $I(X) \cap \mathbb{Z}_p[x_1, \ldots, x_n]$ *at* a. *Let* $m \in \mathbb{N}$ *be such that* $|J_{\mathbf{f}}(a)|_p^2 \not\equiv 0$ (mod p^m). *Then there exists a bianalytic isometry* $\pi \colon (X \cap B(a; p^{-m})) \to (T_x X \cap B(a; p^{-m}))$, *which in a suitable change of coordinates is given by a projection map.*

Proof. We may assume up to translation that a is the origin. Note that we may also act on the equations by taking $\mathrm{GL}_r(\mathbb{Z}_p)$-linear combinations and act by $\mathrm{GL}_n(\mathbb{Z}_p)$-changes of coordinates on X. Thus, by using the Smith normal form of a matrix over $\mathbb{Z}_p$, we may assume that

$$J_{\mathbf{f}}(0) = \begin{bmatrix} \sigma_1 & & & \ddots & & \\ & \ddots & & & 0 & \\ & & \sigma_r & & & \ddots \end{bmatrix}$$

with $|\sigma_1|_p \geq \ldots \geq |\sigma_r|_p$. We consider the new system of equations given by

$$F_j(x) := \sigma_j^{-1}\sigma^{-1}f_j(y)$$

with $y = (\sigma x_1, \ldots, \sigma x_n)$ and $\sigma := \sigma_1 \ldots \sigma_r$. Observe:

- The constant term of each F_j is zero.
- The linear term of F_j is x_j, as the factors of σ_j, σ in the linear term cancel.
- The higher order terms are integral, as $|\sigma_j\sigma|_p \geq |\sigma|_p^2$ for all j.

Thus, each $F_j \in \mathbb{Z}_p[x]$, and the Jacobian matrix for the equations $\{F_1, \ldots, F_r\}$ is $\begin{bmatrix} I \mid 0 \end{bmatrix}$.

We now apply the Implicit Function Theorem; denoting $x_{\text{tail}} := (x_{r+1}, \ldots, x_n)$, we obtain power series $g_1, \ldots, g_r \in \mathbb{Z}_p[\![x_{r+1}, \ldots, x_n]\!]$ such that formally

$$F_j(g_1(x_{\text{tail}}), \ldots, g_r(x_{\text{tail}}), x_{r+1}, \ldots, x_n) = 0.$$

Furthermore, on the ball $B(0; p^{-1})$ the g_j are convergent and we have for all $b \in B(0; p^{-1})$ that $F(a, b) = 0$ implies $a = g(b)$. Finally, since the last $n - r$ coordinates are identified with the tangent space of X at 0, we have that each g_j is at least quadratic in the x_i.

Thus, each g_j is Lipschitz on $B(0; p^{-1})$ with Lipschitz constant 1. In particular, the map

$$\begin{array}{rlcc} \gamma_F\colon & B(0, p^{-1}) & \to & Z(F_1, \ldots, F_r)(\mathbb{Z}_p) \\ & x & \mapsto & (g_1(x_{\text{tail}}), \ldots, g_r(x_{\text{tail}}), x_{r+1}, \ldots, x_n) \end{array}$$

is an isometry, whose inverse is the projection.

Since each g_j is at least quadratic, we have that each $\sigma^{-1} g_j(x_{\text{tail}})$ is Lipschitz on $B(0; |\sigma|_p)$ with Lipschitz constant 1. Denoting $g_j^\flat(x) := \sigma^{-1} g(x)$ we have the isometry

$$\begin{array}{rlcc} \gamma_f\colon & B(0, |\sigma|_p) & \to & Z(f_1, \ldots, f_r)(\mathbb{Z}_p) \\ & x & \mapsto & (g_1^\flat(x_{\text{tail}}), \ldots, g_r^\flat(x_{\text{tail}}), x_{r+1}, \ldots, x_n) \end{array}$$

whose inverse is the projection. Finally, since $p^{-m} \le |J_{\mathbf{f}}(0)|_p^2 \le |\sigma|_p$, we are done. $\qquad \square$

Note that Proposition 20 holds for any choice of local equations for the algebraic set X. It is useful to fix some global set of defining equations with nice properties. For instance, we use the following elementary lemma.

Lemma 21. *Let $X \subseteq \mathbb{P}^n$ be an algebraic set, and let $I(X) \subseteq \mathbb{Q}_p[x_0, \ldots, x_n]$ be the homogeneous ideal of equations vanishing on X. Then $I(X) \cap \mathbb{Z}_p[x_0, \ldots, x_n]$ is a homogeneous ideal of $\mathbb{Z}_p[x_0, \ldots, x_n]$ saturated with respect to $\langle p \rangle$.*

Proof. If $f \in \mathbb{Z}_p[x_0, \ldots, x_n]$ such that $p^m f \in I(X)$ for some $m \ge 0$, then f vanishes at every $x \in X(\mathbb{Q}_p)$, so by definition $f \in I(X)$. $\qquad \square$

3. Volumes

3.1. The volume of an algebraic set.

Definition 22 (The volume of an algebraic set). Let $U \subset A \subseteq \mathbb{Z}_p^n$ be an open and compact subset of an algebraic set A of dimension a. We define the a-dimensional volume of U as:

$$(3.1) \qquad \mathrm{vol}_a(U) = \lim_{m \to \infty} p^{m(n-a)} \cdot \mu_n\left(\bigcup_{x \in U} B(x, p^{-m})\right).$$

In a similar way, if $U \subseteq A \subseteq \mathbb{P}^n$ is an open and compact subset of an algebraic set A of dimension $\dim(A) = a$, we define its a-dimensional projective volume by (3.1), replacing μ_n with the pushforward measure on $\mathbb{P}^n$ and taking balls with respect to the projective metric. Moreover, if $A \subseteq S^{n-1} \subset \mathbb{Q}_p^n$, again we define the volume of $U \subseteq A$ by (3.1).

For (open compact subsets of) algebraic sets, Serre [Ser81, pp148-149] observed that the limit in Definition 22 exists and is finite. He moreover observed, via an inductive argument based on resolution of singularities, that the volume of an algebraic set is a rational number. The result also appears in an article by Oesterlé [Oes82, Theorem 2], though Oesterlé's proves that the limit exists by more elementary means. Oesterlé also proves the following:

Proposition 23. *The volume of an open and compact subset $U \subseteq A$ of an algebraic set (both affine and projective) coincides with its $\dim(A)$-Hausdorff measure.*

When $U \subseteq \mathbb{Z}_p^n$ is an open set of full dimension we have $\text{vol}_n(U) = \mu_n(U)$. Additionally, the volume of $U \subseteq A \subseteq \mathbb{P}^n$ and the volume of the $(\dim(A) + 1)$-dimensional set $\varphi^{-1}(U) \subseteq \varphi^{-1}(A) \subseteq S^n$ are related by:

$$(3.2) \qquad \text{vol}_a(U) = \frac{\text{vol}_{a+1}(\varphi^{-1}(U))}{\text{vol}_1(\mathbb{Z}_p^*)} = \frac{\text{vol}_{a+1}(\varphi^{-1}(U))}{1 - \frac{1}{p}}.$$

3.2. **Volume and number of points in the modulo p^m reduction.**

Lemma 24. *We have the following two identities:*

(1) *Let $U \subseteq A \subseteq \mathbb{Z}_p^n$ be an open and compact subset of an algebraic set A of dimension $\dim(A) = a$. Then $N_m(U)$ is the minimum number of affine balls of radius p^{-m} that we need to cover U.*

(2) *Let $U \subseteq A \subseteq \mathbb{P}^n$ be an open and compact subset of an algebraic set A of dimension $\dim(A) = a$. Then $N_m(U)$ is the minimum number of projective balls of radius p^{-m} that we need to cover U. Moreover, we have that*

$$N_m(U) = \frac{N_m(\varphi^{-1}(U))}{p^m \left(1 - \frac{1}{p}\right)}$$

Proof. Both results follow from the definition of $N_m(U)$ and Proposition 13. $\qquad \square$

Corollary 25. *We have the following two identities.*

(1) *Let $U \subseteq A \subseteq \mathbb{Z}_p^n$ be an open and compact subset of an algebraic set A of dimension $\dim(A) = a$. Then:*

$$\text{vol}(U) = \lim_{m \to \infty} \frac{N_m(U)}{p^{ma}}.$$

(2) *Let $U \subseteq A \subseteq \mathbb{P}^n$ be an open and compact subset of an algebraic set A of dimension $\dim(A) = a$. Then:*

$$\text{vol}(U) = \lim_{m \to \infty} \frac{N_m(U)}{p^{ma}}.$$

Proof. In the affine case, using Lemma 24 we cover U with $N_m(U)$ disjoint balls of radius p^{-m} and centered at points $x_1, \ldots, x_{N_m(U)} \in U$. We have:

$$\text{vol}(U) = \lim_{m \to \infty} p^{m(n-a)} \cdot \mu \left(\bigcup_{x \in U} B(x, p^{-m}) \right) = \lim_{m \to \infty} p^{m(n-a)} \sum_{j=1}^{N_m(U)} \mu \left(B(x_j, p^{-m}) \right)$$

$$= \lim_{m \to \infty} \frac{N_m(U)}{p^{ma}}.$$

In the projective case, we use the result in the affine case to see that

$$\text{vol}(U) = \frac{\text{vol}(\varphi^{-1}(U))}{1 - \frac{1}{p}} = \lim_{m \to \infty} \frac{N_m(\varphi^{-1}(U))}{p^{m(a+1)} \left(1 - \frac{1}{p}\right)} = \lim_{m \to \infty} \frac{N_m(U)}{p^{ma}}. \qquad \square$$

Corollary 26. *Let $\varphi^{-1}(A) = X \subset S^n$ be the pullback of an algebraic set of dimension a. Denote by $\text{sm}(X)$ the set of analytically smooth points of X in $\mathbb{Z}_p^{n+1}$. Then $\text{vol}(X) = \text{vol}(\text{sm}(X))$.*

Proof. Let Z be the singular locus of A. Since the dimension of Z is strictly smaller than $\dim(X) = a + 1$, we have

$$\lim_{m \to \infty} p^{-m(a+1)} N_m(X) = \lim_{m \to \infty} p^{-m(a+1)} \left(N_m(\mathrm{sm}(X)) + N_m(\varphi^{-1}(Z)) \right)$$
$$= \lim_{m \to \infty} p^{-m(a+1)} N_m(\mathrm{sm}(X)). \qquad \square$$

3.3. **Quantitative estimates and the Weil canonical measure.** For an embedded p-adic analytic set, we can enhance [Oes82, Theorem 2] and give explicit quantitative estimates to compute the limit in Definition 25. Our explicit approach enables us to compute the volume of some specific algebraic sets in Section 5 (see Proposition 38 and Corollary 41).

Proposition 27. *Let $X \subset \mathbb{Z}_p^n$ be an algebraic set of dimension d and $x \in X$ be a smooth point. Then there exists $m_x > 0$ such that for all $\ell_1 \geq \ell_2 \geq m_x$ we have:*

$$N_{\ell_1}(X \cap B(x; p^{-\ell_2})) = p^{(\ell_1 - \ell_2)d}$$

Furthermore, if $\mathbf{f}$ is a set of local equations for X at x, then any $m_x \geq -\log_p |J_{\mathbf{f}}(x)|_p^2$ suffices.

Proof. By Proposition 20 there is a bianalytic isometry

$$\pi \colon X \cap B(x; p^{-m_x}) \to T_x X \cap B(x; p^{-m_x})$$

where $m_x = -\log_p |J_{\mathbf{f}}(x)|_p^2$. The result holds for the image of π, so the claim follows. $\qquad \square$

Corollary 28. *Let $X \subset \mathbb{Z}_p^n$ be a compact open set of a smooth algebraic set of dimension d, then there exists $m_0 = m_0(X) > 0$ such that for all $m \geq m_0$ we have*

$$N_m(X) = p^{(m-m_0)d} N_{m_0}(X).$$

Proof. Using Proposition 27 and compactness of X, we see that there exists $m_0(X)$ such that for every $x \in X$ and every $\ell_2 \geq \ell_1 \geq m_0(X)$, we have $N_{\ell_2}(B(x, p^{-\ell_1}) \cap X) = p^{(\ell_2 - \ell_1)d}$. Covering X with $N_{m_0}(X)$ disjoint balls of the form $B(x_i, p^{-m_0})$, with each $x_i \in X$, we see

$$N_m(X) = \sum_{i=1}^{N_{m_0}(X)} N_m(B(x_i, p^{-m_0}) \cap X) = \sum_{i=1}^{N_{m_0}(X)} p^{(m-m_0)d} = N_{m_0}(X) p^{(m-m_0)d}. \qquad \square$$

As a first application of our quantitative estimates, we have:

Theorem 29. *Let $\mathcal{X}$ be a subscheme of $\mathbb{P}^n$ which is smooth over $\mathrm{Spec}\,\mathbb{Z}_p$. Then the Weil canonical volume of $X = \mathcal{X}(\mathbb{Z}_p)$ is equal to the volume as defined above.*

Proof. The Weil canonical volume of X is $\frac{\#X(\mathbb{F}_p)}{p}$ [Wei82, Theorem 2.2.5]. However, we also have that the Jacobian matrix of the defining equations is non-zero modulo p at any point in X, so the limit in Corollary 25 stabilizes in the first term. This proves the result. $\qquad \square$

4. THE p-ADIC INTEGRAL GEOMETRY FORMULA

Lemma 30. *Let $x \in S^n$ be a point, let $B \subseteq S^n$ be a ball of radius p^{-m} containing x, with $m > 0$. Finally, let $U := \bigcup_{a \in \mathbb{Z}_p^\times} aU$, where $\mathbb{Z}_p^\times$ acts in the usual way. Then the subgroup*

$$\mathrm{Fix}(\mathrm{GL}_{n+1}(\mathbb{Z}_p), U) := \{ g \in \mathrm{GL}_{n+1}(\mathbb{Z}_p) : gU = U \}$$

is a finite index subgroup of $\mathrm{GL}_{n+1}(\mathbb{Z}_p)$ containing $\mathbb{Z}_p^\times$.

Proof. The action of $\mathrm{GL}_{n+1}(\mathbb{Z}_p)$ on S^n commutes with reduction to R_m. The result is immediate since $\mathrm{GL}_{n+1}(R_m)$ is a finite group. $\qquad \square$

The following technical lemma is simply the result that if X, Y are random linear subspaces of complementary codimension, the probability densities

$$P(\{x\} = X \cap Y \mid x \in X), \qquad P(\{y\} = X \cap Y \mid y \in Y)$$

are uniform on X and Y (resp.), and furthermore are independent.

Lemma 31. *Let $X, Y, H \subseteq \mathbb{P}^n$ be linear varieties such that* $\operatorname{codim} X + \operatorname{codim} Y + \operatorname{codim} H = n$. *Let $U_x \subseteq X, U_y \subseteq Y$ be relatively open balls (i.e, open balls of the subspaces X, Y). Then*

$$\int_{\operatorname{GL}_{n+1}(\mathbb{Z}_p)} \int_{\operatorname{GL}_{n+1}(\mathbb{Z}_p)} \#(g_x U_x \cap g_y U_y \cap H) dg_y dg_x = \frac{\operatorname{vol}(U_x)}{\operatorname{vol}(X)} \cdot \frac{\operatorname{vol}(U_y)}{\operatorname{vol}(Y)}.$$

Proof. The strategy of the proof is to replace the integrand with a constant function by using the fact that X (resp. Y) is the disjoint union of finitely many copies of U_x (resp. U_y).

Let $G_X := \operatorname{Fix}(\operatorname{GL}_{n+1}(\mathbb{Z}_p), X)$ and let $G_Y = \operatorname{Fix}(\operatorname{GL}_{n+1}(\mathbb{Z}_p), Y)$. Furthermore, let $A := \operatorname{Fix}(G_X, U_x)$ and $B := \operatorname{Fix}(G_Y, U_y)$. Note that G_X acts on X through $\operatorname{GL}_{\dim X+1}(\mathbb{Z}_p)$, so we have the commutative diagram

$$
\begin{array}{ccc}
G_X & \longrightarrow & \operatorname{GL}_{\dim X+1}(\mathbb{Z}_p) \\
\uparrow & & \uparrow \\
\operatorname{Fix}(G_X, U_x) & \longrightarrow & \operatorname{Fix}(\operatorname{GL}_{\dim X+1}(\mathbb{Z}_p), U_x)
\end{array}
\quad.
$$

In particular, A has finite index in G_X by the previous lemma. Denote $a := [G_X : A]$, $b := [G_Y : B]$ and let $g_{x,1}, \ldots, g_{x,a}$ and $g_{y,1}, \ldots, g_{y,b}$ be coset representatives for $A \subseteq G_X$ and $B \subseteq G_Y$ respectively.

Note that $X = \coprod_{j=1}^{a} g_{x,j} U_x$. As G_X acts transitively on the balls in H of a fixed radius, we have for any i, j that

$$\int_{G_X} \#(g_x U_x \cap g_y U_y \cap H) dg_y dg_x = \int_{G_X} \#(g_x g_{x,j} U_x \cap g_y g_{y,i} U_y \cap H) dg_y dg_x.$$

In particular, if $\#(X \cap Y \cap H) = 1$, we have

$$
ab \int_{G_X} \int_{G_Y} \#(g_x U_x \cap g_y U_y \cap H) dg_y dg_x = \sum_{j=1}^{a} \sum_{i=1}^{b} \int_{G_X} \int_{G_Y} \#(g_x g_{x,j} U_x \cap g_y g_{y,i} U_y \cap H) dg_y dg_x
$$

$$
= \int_{G_X} \int_{G_Y} \#(g_x X \cap g_y Y \cap H) dg_y dg_x
$$

$$
= \int_{G_X} \int_{G_Y} \#(X \cap Y \cap H) dg_y dg_x
$$

$$
= \int_{G_X} \int_{G_Y} dg_y dg_x
$$

We now write $\operatorname{GL}_{n+1}(\mathbb{Z}_p) \cong G_X \times (G_X \backslash \operatorname{GL}_{n+1}(\mathbb{Z}_p))$ as a product measure space, with corresponding differential $dg_x = ds_x dt_x$, using the orbit-stabilizer theorem. Thus, by Fubini's

theorem we have

$$ab \int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \#(g_x U_x \cap g_y U_y \cap H) dg_y dg_x$$

$$= ab \int_{G_X \backslash \mathrm{GL}_{n+1}(\mathbb{Z}_p)} \int_{G_X} \int_{G_Y \backslash \mathrm{GL}_{n+1}(\mathbb{Z}_p)} \int_{G_Y} \#(g_x U_x \cap g_y U_y \cap H) ds_y dt_y ds_x dt_x$$

$$= ab \int_{G_X \backslash \mathrm{GL}_{n+1}(\mathbb{Z}_p)} \int_{G_Y \backslash \mathrm{GL}_{n+1}(\mathbb{Z}_p)} \int_{G_X} \int_{G_Y} \#(g_x U_x \cap g_y U_y \cap H) ds_y ds_x dt_y dt_x$$

$$= \int_{G_X \backslash \mathrm{GL}_{n+1}(\mathbb{Z}_p)} \int_{G_Y \backslash \mathrm{GL}_{n+1}(\mathbb{Z}_p)} \left(ab \int_{G_X} \int_{G_Y} \#(g_x U_x \cap g_y U_y \cap H) ds_y ds_x \right) dt_y dt_x$$

Since the set of (g_x, g_y) in $\mathrm{GL}_{n+1}(\mathbb{Z}_p)$ where $g_x X, g_y Y, H$ do not meet transversely has measure zero, we have that our expression above equals

$$\int_{G_X \backslash \mathrm{GL}_{n+1}(\mathbb{Z}_p)} \int_{G_Y \backslash \mathrm{GL}_{n+1}(\mathbb{Z}_p)} \int_{G_X} \int_{G_Y} ds_y ds_x dt_y dt_x = 1.$$

Finally, since the disjoint union of a copies of U_x is X, we have that $\frac{1}{a} = \frac{\mathrm{vol}(U_x)}{\mathrm{vol}(X)}$ □

Corollary 32. *Let* $X, H \subseteq \mathbb{P}^n$ *be linear varieties such that* $\mathrm{codim}\, X + \mathrm{codim}\, H = n$. *Let* $U_x \subseteq X$ *be a relatively open ball. Then*

$$\int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \#(g_x U_x \cap H) dg_x = \frac{\mathrm{vol}(U_x)}{\mathrm{vol}(X)}.$$

Proof. Let $Y := \mathbb{P}^n$ and $U_y := Y$. By Lemma 4.1 we have that

$$\int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \#(g_x U_x \cap g_y U_y \cap H) dg_y dg_x = \frac{\mathrm{vol}(U_x)}{\mathrm{vol}(X)} \cdot \frac{\mathrm{vol}(U_y)}{\mathrm{vol}(Y)} = \frac{\mathrm{vol}(U_x)}{\mathrm{vol}(X)}.$$

But we see that the inner integral is constant in g_y and equal to $\#(U_x \cap H)$ since $g_y U_y = \mathbb{P}^n$. □

We define some notation to state the next lemma. Let $\mathbf{f}_1, \mathbf{f}_2 \subseteq \mathbb{Z}_p[x_0, x_1, \ldots, x_n]$ be sets of homogeneous polynomials of size $n - r$, n respectively, and let $x, y \in \mathbb{P}^n$. We define

$$J(\mathbf{f}_1(x), \mathbf{f}_2(y)) := \begin{bmatrix} J_{\mathbf{f}_1}(x) \\ J_{\mathbf{f}_2}(y) \end{bmatrix} \qquad \text{and} \qquad |J(\mathbf{f}_1(x), \mathbf{f}_2(y))|_p = \frac{|\det J(\mathbf{f}_1(x), \mathbf{f}_2(y))|_p}{\|x\|_p^{\delta_1} \|y\|_p^{\delta_2}}$$

where $\delta_j = \sum_{f \in \mathbf{f}_j} \deg f$. Additionally, if $g \in \mathrm{GL}_{n+1}(\mathbb{Z}_p)$ and $\mathbf{f} = (f_1, \ldots, f_{n-r})$, we denote $\mathbf{f}^g := (f_1 \circ g, \ldots, f_{n-r} \circ g)$.

Lemma 33 (Linear Approximation Lemma). *Let* $X, Y \subseteq \mathbb{P}^n$ *be algebraic sets of complementary codimension. Let* $x \in X, y \in Y$ *be smooth points, contained in open balls* U_x, U_y *of* $\mathbb{P}^n$ *of radius* p^{-m}, *with local equations* $\mathbf{f}_x, \mathbf{f}_y$ *(respectively). If*

$$|J(\mathbf{f}_x(x), \mathbf{f}_y(y))|_p^2 > p^{-m} \qquad or \qquad U_x \cap U_y = \emptyset,$$

then $\#(X \cap U_x \cap Y \cap U_y) = \#(T_x X \cap U_x \cap T_y Y \cap U_y)$.

Proof. If $U_x \cap U_y = \emptyset$, we have $\#(X \cap U_x \cap Y \cap U_y) = \#(T_x X \cap U_x \cap T_y Y \cap U_y) = 0$.

Otherwise, note that U_x, U_y are balls of radius p^{-m} with nontrivial intersection, so $U_x = U_y$. In particular, $\pi_m(x) = \pi_m(y)$. Choosing representatives on S^n for x, y, we have

$$J(\mathbf{f}_x(x), \mathbf{f}_y(y)) \equiv J(\mathbf{f}_x(x), \mathbf{f}_y(x)) \pmod{p^{-m}}.$$

The right hand side is just the Jacobian matrix for $\mathbf{f}_x \cup \mathbf{f}_y$ at x. By Hensel's lemma, there is a unique projective solution to the system $\mathbf{f}_x \cup \mathbf{f}_y$ which is contained in $U_x = U_y$. On the other

hand, the equations defining the two tangent spaces $T_x X, T_y X$ also satisfy the conditions of Hensel's lemma, and have the common interesction point $x \equiv y \pmod{p^{-m}}$. Thus, the conclusion of the lemma holds in this case as well. $\square$

Theorem 34. *Let $A \subset S^n$ be a homogeneous algebraic set of dimension $\dim(A) = a + 1$ and let $X \subset \mathbb{P}^n$ be its projectivization. If $U \subseteq X$ is a compact open subset and $L \subset \mathbb{P}^n$ is a projective subspace of dimension $n - a$, then for almost all $g \in \mathrm{GL}_{n+1}(\mathbb{Z}_p)$ the intersection $U \cap gL$ is transversal and:*

$$\mathrm{vol}(\varphi^{-1}(U)) = \mathrm{vol}(\mathbb{P}^a) \cdot \int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \#\left(U \cap gL\right) dg.$$

Proof. Let $Z \subset \mathrm{GL}_{n+1}(\mathbb{Z}_p)$ be the set defined by:

$$Z = \{g : gL \text{ is not transversal to } X\}.$$

and denote $Z_\ell := \bigcup_{g \in Z} B(g, p^{-\ell})$. Since Z is contained in a proper algebraic set, by Corollary 25 there is a constant $C > 0$ such that

$$\mu\left(\bigcup_{g \in Z} B(g, p^{-\ell})\right) \leq C p^{-\ell \dim(Z)}.$$

With ℓ fixed, we have for every $u \in U$ there exists $m_{u,\ell} > 0$ such that for all $g \in \mathrm{GL}_{n+1}(\mathbb{Z}_p) \backslash Z_\ell$ and for every $m \geq m_{u,\ell}$:

$$(4.1) \qquad \#\left(gL \cap U \cap B(u, p^{-m}))\right) = \#\left(gL \cap T_u U \cap B(u, p^{-m}))\right).$$

Observe that $Z_1 \supset Z_2 \supset \ldots$ and that $\bigcap_{\ell \in \mathbb{N}} Z_\ell = Z$. Since Z has measure zero, we see from the Monotone Convergence Theorem that

$$\int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} f(g) dg = \lim_{\ell \to \infty} \int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p) \backslash Z_\ell} f(g) dg$$

for every measurable function $f : \mathrm{GL}_{n+1}(\mathbb{Z}_p) \to \mathbb{R}$. With this in mind, we evaluate now:

$$\int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \#\left(U \cap gL\right) dg = \lim_{\ell \to \infty} \int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p) \backslash Z_\ell} \#\left(U \cap gL\right) dg$$

$$= \lim_{\ell \to \infty} \int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p) \backslash Z_\ell} \sum_{i=1}^{N_m(U)} \#\left(U_i \cap gL\right) dg = (*),$$

where we have covered $U = \bigcup_{i=1}^{N_m(U)} \left(B(u_i, p^{-m}) \cap U\right)$ with $N_m(U)$ disjoint subsets of the form $U_i = B(u_i, p^{-m}) \cap U$, with

$$m = m_\ell \geq \sup_{u \in U} m_{u,\ell} \geq 0$$

large enough (such an m exists by compactness of U).

Using (4.1), we can continue with:

$$(*) = \lim_{\ell \to \infty} \int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)\setminus Z_\ell} \sum_{i=1}^{N_m(U)} \# \left(B(u_i, p^{-m}) \cap T_{u_i} U_i \cap gL \right) dg$$

$$= \lim_{\ell \to \infty} \left(\int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \sum_{i=1}^{N_m(U)} \# \left(B(u_i, p^{-m}) \cap T_{u_i} U_i \cap gL \right) dg + O(p^{-\ell \dim(Z)}) \right)$$

$$= \lim_{\ell \to \infty} \int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \sum_{i=1}^{N_m(U)} \# \left(B(u_i, p^{-m}) \cap T_{u_i} U_i \cap gL \right) dg$$

$$= \lim_{\ell \to \infty} N_m(U) \cdot \frac{\mathrm{vol}_a(B(u, p^{-m}) \cap \mathbb{P}^a)}{\mathrm{vol}_a(\mathbb{P}^a)}$$

$$= \lim_{m \to \infty} N_m(U) \cdot \frac{\mathrm{vol}_a(B(u, p^{-m}) \cap \mathbb{P}^a)}{\mathrm{vol}_a(\mathbb{P}^a)} \quad = \frac{\mathrm{vol}(U)}{\mathrm{vol}(\mathbb{P}^a)} \qquad \text{by Corollary 25.}$$

The conclusion follows now from the definition (3.2). □

Theorem 35 (The p-adic Integral Geometry Formula). *Let $U, V \subset \mathbb{P}^n$ be open and compact subsets of algebraic sets of dimensions $\dim(U) = a, \dim(V) = b$. Then for almost all $g \in \mathrm{GL}_{n+1}(\mathbb{Z}_p)$ the intersection $U \cap gV$ is transversal, of dimension $c = n - (n-a) - (n-b)$, and:*

$$\int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \frac{\mathrm{vol}(U \cap gV)}{\mathrm{vol}(\mathbb{P}^c)} dg = \frac{\mathrm{vol}(U)}{\mathrm{vol}(\mathbb{P}^a)} \cdot \frac{\mathrm{vol}(V)}{\mathrm{vol}(\mathbb{P}^b)}.$$

Proof. The proof proceeds similarly to the previous one. We observe first that, whenever the intersection $U \cap gV$ is transversal, picking $L \simeq \mathbb{P}^c \subset \mathbb{P}^n$ and using Theorem 34, we can write:

$$\frac{\mathrm{vol}(U \cap gV)}{\mathrm{vol}(\mathbb{P}^c)} = \int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \# (U \cap gV \cap g_2 L) \, dg_2,$$

and consequently:

$$(4.2) \qquad \int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \frac{\mathrm{vol}(U \cap gV)}{\mathrm{vol}(\mathbb{P}^c)} dg = \int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \# (U \cap g_1 V \cap g_2 L) \, dg_2 dg_1.$$

Denote by $G = \mathrm{GL}_{n+1}(\mathbb{Z}_p)$ and consider the set:

$$Z = \{(g_1, g_2) \in G \times G : U \cap g_1 V \cap g_2 L \text{ is not transversal}\}.$$

Given $\ell > 0$, for every $y = (u, v) \in U \times V$ there exists $m_{y,\ell} > 0$ such that for all $(g_1, g_2) \in G \times G \setminus \left(\bigcup_{z \in Z} B(z, p^{-\ell}) \right)$ and for all $m \geq m_{y,\ell}$ we have:

$$\#(\quad U \cap B(u, p^{-m}) \quad \cap \quad g_1 (V \cap B(v, p^{-m})) \quad \cap \quad g_2 L)$$

$$= \#(\quad T_u U \cap B(u, p^{-m}) \quad \cap \quad g_1 (T_v V \cap B(v, p^{-m})) \quad \cap \quad g_2 L).$$

As in the proof of Theorem 34, since Z is contained in a proper algebraic set, we also have:

$$\mu \left(\bigcup_{z \in Z} B(z, p^{-\ell}) \right) \leq O(p^{-\ell}).$$

As before, we denote $Z_\ell = \bigcup_{z \in Z} B(z, p^{-\ell})$.

By compactness of $U \times V$, we choose some $m = m_\ell \geq \sup_{y \in U \times V} m_{y,\ell} > 0$. We cover now

$$U = \bigcup_{i=1}^{N_m(U)} \left(B(u_i, p^{-m}) \cap U \right), \qquad V = \bigcup_{i=1}^{N_m(V)} \left(B(v_i, p^{-m}) \cap V \right)$$

with $N_m(U)$ (resp. $N_m(V)$) disjoint projective balls of radius p^{-m}. In the sequel we denote $U_{i,m} = B(u_i, p^{-m}) \cap U$ and $V_{i,m} = B(v_i, p^{-m}) \cap V$; we will also write $TU_{i,m} = B(u_i, p^{-m}) \cap T_{u_i} U$ and $TV_{j,m} = B(v_j, p^{-m}) \cap T_{v_j} V$.

We proceed now to evaluate the integral in the statement, using (4.2):

$$\int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \frac{\mathrm{vol}\,(U \cap gV)}{\mathrm{vol}\,(\mathbb{P}^c)} dg = \int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \int_{\mathrm{GL}_{n+1}(\mathbb{Z}_p)} \#\left(U \cap g_1 V \cap g_2 L \right) dg_2 dg_1$$

$$= \lim_{\ell \to \infty} \int_{G \times G \setminus Z_\ell} \#\left(U \cap g_1 V \cap g_2 L \right) dg_2 dg_1$$

$$= \lim_{\ell \to \infty} \int_{G \times G \setminus Z_\ell} \sum_{i=1}^{N_m(U)} \sum_{j=1}^{N_m(V)} \#\left(U_{i,m} \cap g_1 V_{j,m} \cap g_2 L \right) dg_2 dg_1$$

$$= \lim_{\ell \to \infty} \int_{G \times G \setminus Z_\ell} \sum_{i=1}^{N_m(U)} \sum_{j=1}^{N_m(V)} \#\left(TU_{i,m} \cap g_1 TV_{j,m} \cap g_2 L \right) dg_2 dg_1$$

$$= \lim_{\ell \to \infty} \left(\int_{G \times G} \sum_{i=1}^{N_m(U)} \sum_{j=1}^{N_m(V)} \#\left(TU_{i,m} \cap g_1 TV_{j,m} \cap g_2 L \right) dg_2 dg_1 + O(p^{-\ell}) \right)$$

$$= \lim_{\ell \to \infty} \int_{G \times G} \sum_{i=1}^{N_m(U)} \sum_{j=1}^{N_m(V)} \#\left(TU_{i,m} \cap g_1 TV_{j,m} \cap g_2 L \right) dg_2 dg_1 = (*)$$

We use now Lemma 31 and continue with:

$$(*) = \lim_{\ell \to \infty} N_m(U) \frac{\mathrm{vol}_a(B(u, p^{-m}) \cap \mathbb{P}^a)}{\mathrm{vol}_a(\mathbb{P}^a)} \cdot N_m(V) \frac{\mathrm{vol}_b(B(v, p^{-m}) \cap \mathbb{P}^b)}{\mathrm{vol}_b(\mathbb{P}^b)}$$

$$= \lim_{m \to \infty} N_m(U) \frac{\mathrm{vol}_a(B(u, p^{-m}) \cap \mathbb{P}^a)}{\mathrm{vol}_a(\mathbb{P}^a)} \cdot N_m(V) \frac{\mathrm{vol}_b(B(v, p^{-m}) \cap \mathbb{P}^b)}{\mathrm{vol}_b(\mathbb{P}^b)}$$

$$= \frac{\mathrm{vol}_a(U)}{\mathrm{vol}_a(\mathbb{P}^a)} \cdot \frac{\mathrm{vol}_b(V)}{\mathrm{vol}_b(\mathbb{P}^b)}. \qquad \qquad \Box$$

5. How many zeroes of a random p-adic polynomial are in $\mathbb{Z}_p$?

Theorem 36. *Let $\{f_0, \ldots, f_\ell\}$ be a basis for $\mathbb{Q}_p[x_0, \ldots, x_n]_{(d)}$ and for every $i = 1, \ldots, n$ consider the random polynomial:*

$$F_i(x) = \sum_{k=0}^{\ell} \xi_{i,k} f_k(x)$$

where $\{\xi_{i,k}\}_{i=1,\ldots,n,k=0,\ldots,\ell}$ is a family of independent uniformly distributed random variables in $\mathbb{Z}_p$. Let $\nu(\mathbb{P}^n) \subset \mathbb{P}^\ell$ be the image of the "Veronese map" $\nu : \mathbb{P}^n \to \mathbb{P}^\ell$

(5.1) $$\nu([x]) = [f_0(x), \ldots, f_\ell(x)].$$

Then, the expectation of the number of solution of the random system of equations $F_1 = \cdots = F_n = 0$ in $\mathbb{P}^n$ equals:

$$\mathbb{E}\#\{F_1 = \cdots = F_n = 0\} = \frac{\text{vol}(\nu(\mathbb{P}^n))}{\text{vol}(\mathbb{P}^n)}.$$

Proof. The result is an easy consequence of the Integral Geometry Formula. We use the fact that $\{f_0, \ldots, f_\ell\}$ is a linearly independent and spanning set to ensure that the map ν is an embedding and that $\nu(\mathbb{P}^n)$ is a smooth algebraic subset. Now for every $i = 1, \ldots, n$ we can consider the random hyperplane $L_i \subset \mathbb{P}^\ell$:

$$L_i = \left\{ \sum_{k=0}^{\ell} \xi_{i,k} y_i = 0 \right\}.$$

The distribution of this hyperplane is invariant under the group $\text{GL}_{\ell+1}(\mathbb{Z}_p)$ and can be alternatively described as fixing a hyperplane $L_0 \subset \mathbb{P}^\ell$, sampling $g_i \in \text{GL}_{\ell+1}(\mathbb{Z}_p)$ uniformly and setting $L_i = g_i L_0$. Consequently:

$$\begin{aligned}
\mathbb{E}\#\{F_1 = \cdots = F_n = 0\} &= \mathbb{E}\#\nu(\mathbb{P}^n) \cap L_1 \cdots \cap L_n \\
&= \mathbb{E}\#\nu(\mathbb{P}^n) \cap g_1 L_0 \cdots \cap g_n L_n \\
&= \mathbb{E}_{g_1,\ldots,g_{n-1}} \left(\mathbb{E}_{g_n} \#\nu(\mathbb{P}^n) \cap g_1 L_0 \cdots \cap g_n L_0 \right) \\
&= \mathbb{E}_{g_1,\ldots,g_{n-1}} \left(\int_{\text{GL}_{\ell+1}(\mathbb{Z}_p)} \#\nu(\mathbb{P}^n) \cap g_1 L_0 \cdots \cap g_n L_0 \, dg_n \right) \\
&= \mathbb{E}_{g_1,\ldots,g_{n-1}} \left(\frac{\text{vol}(\nu(\mathbb{P}^n) \cap g_1 L_0 \cdots \cap g_{n-1} L_0)}{\text{vol}(\mathbb{P}^1)} \right) = (*),
\end{aligned}$$

where in the last step we have used the Integral Geometry Formula from Theorem 35. Repeating this process iteratively we get:

$$\begin{aligned}
(*) &= \mathbb{E}_{g_1,\ldots,g_{n-2}} \left(\frac{\text{vol}(\nu(\mathbb{P}^n) \cap g_1 L_0 \cdots \cap g_{n-1} L_0)}{\text{vol}(\mathbb{P}^2)} \right) \\
&= \cdots \\
&= \mathbb{E}_{g_1} \left(\frac{\text{vol}(\nu(\mathbb{P}^n) \cap g_1 L_0)}{\text{vol}(\mathbb{P}^{n-1})} \right) = \frac{\text{vol}(\nu(\mathbb{P}^n))}{\text{vol}(\mathbb{P}^n)}. \qquad \square
\end{aligned}$$

The previous theorem reduces the question of the expected number of zeros of a random polynomial systerm to computing the volume of the "Veronese variety" $\nu(\mathbb{P}^n) \subset \mathbb{P}^\ell$ (i.e. the image of ν from (5.1)).

In order to actually calculate the volume of the image of the Veronese, it is tremendously convienient to have available a coarea formula. Specifically, a statement which allows us to calculate the 1-dimensional volume of a curve in S^d.

Lemma 37 (Arc length formula). *Let $U \subset \mathbb{Q}_p$ be an open and compact set and $\gamma : U \to \mathbb{Q}_p^n$ be an analytic embedding such that for all $u \in U$ we have $|J\gamma(u)| = p^b$ for some $b \in \mathbb{Z}$, then $\text{vol}_1(\gamma(U)) = p^b \text{vol}_1(U)$.*

Proof. Using Taylor's formula for every $u \in U$ and $\epsilon \in \mathbb{Q}_p$ sufficiently small, we have:

$$\gamma(u + \epsilon) - \gamma(u) = J\gamma(u)\epsilon + O(\|\epsilon\|_p^2).$$

Because $\mathbb{Q}_p^n$ is an ultrametric space, this implies that for ϵ small enough:

$$\|\gamma(u + \epsilon) - \gamma(u)\|_p = |J\gamma(u)|_p \|\epsilon\|_p.$$

In particular, denoting $|J\gamma(u)| = p^b$, for every $u \in U$ there is $m_u \in \mathbb{N}$ such that for all $m \geq m_0$

(5.2) $$\gamma(B(u, p^{-m})) = \gamma(U) \cap B(\gamma(u), p^{b-m}).$$

Since U is assumed to be compact, then there exists $m_0 > 0$ such that for all $m \geq m_0$ equation (5.2) is true for all $u \in U$. Now, covering U with N_m disjoint balls

$$B(u_{m,1}, p^{-m}), \ldots, B(u_{m,N_m}, p^{-m}),$$

we can write $\mathrm{vol}_1(U) = p^{-m} N_m$ for m large enough:

At the same time the balls $B(\gamma(u_{m,1}), p^{b-m}), \ldots, B(\gamma(u_{m,N_m}), p^{b-m})$ cover $\gamma(U)$ and for large enough m are disjoint. In particular,

$$p^b \mathrm{vol}_1(U) = p^b \lim_{m\to\infty} \frac{N_m}{p^m} = \lim_{m\to\infty} \frac{N_{m-b}(\gamma(U))}{p^{m-b}} = \lim_{m'=m-b\to\infty} \frac{N_{m'}(\gamma(U))}{p^{m'}} = \mathrm{vol}(\gamma(U)). \quad \square$$

5.1. The standard Veronese random model.

Proposition 38. *Let $\mathbb{P}^\ell$ be the projectivization of the space of homogeneous polynomials with coefficients in $\mathbb{Q}_p$, of degree d and in $n+1$ variables (so that $\ell = \binom{n+d}{d} - 1$). Let $\nu : \mathbb{P}^n \to \mathbb{P}^\ell$ be the Veronese map*

$$\nu_{n,d} : [x_0, \ldots, x_n] \mapsto [(x_0^{\alpha_0} \cdots x_n^{\alpha_n})_{|\alpha|=d}].$$

Then $\mathrm{vol}(\nu(\mathbb{P}^n)) = \mathrm{vol}(\mathbb{P}^n)$.

Proof. We will prove that ν is an isometry onto its image: from this the result will follow, since Proposition 23 establishes that the volume in our sense is a metric invariant.

Observe first that the linear representation $\rho : \mathrm{GL}_{n+1}(\mathbb{Z}_p) \to \mathrm{GL}_\ell(\mathbb{Q}_p)$ by change of variables has image in $\mathrm{GL}_\ell(\mathbb{Z}_p)$, hence for every $g \in \mathrm{GL}_{n+1}(\mathbb{Z}_p)$, the map $\rho(g) : \mathbb{P}^\ell \to \mathbb{P}^\ell$ acts by isometries (as well as the map $g : \mathbb{P}^n \to \mathbb{P}^n$).

Let now $x, y \in \mathbb{P}^n$ be any two points. Pick an element $g \in \mathrm{GL}_{n+1}(\mathbb{Z}_p)$ such that:

$$g[x] = [1, 0, \ldots, 0] \quad \text{and} \quad g[y] = [a_0, a_1, 0, \ldots, 0]$$

with $(a_0, a_1, 0, \ldots, 0) \in S^n$. Then, because g is an isometry, using the definition (2.2) of the distance in projective spaces:

(5.3) $$d_{\mathbb{P}^n}([x], [y]) = d_{\mathbb{P}^n}([1, 0, \ldots, 0], [a_0, a_1, 0, \ldots, 0]) = |a_1|_p.$$

Let us evaluate now the distance $d([\nu(x)], [\nu(y)])$:

$$\begin{aligned} d_{\mathbb{P}^\ell}([\nu(x)], [\nu(y)]) &= d_{\mathbb{P}^\ell}(\rho(g)[\nu(x)], \rho(g)[\nu(y)]) \\ &= d_{\mathbb{P}^\ell}([\nu(gx)], [\nu(gy)]) \\ &= d_{\mathbb{P}^\ell}([1, 0, \ldots, 0], \nu[a_0, a_1, 0, \ldots, 0]). \end{aligned}$$

Since $(a_0, a_1, 0, \ldots, 0)$ was in the unit sphere, the vector $\nu(a_0, a_1, 0, \ldots, 0) \in \mathbb{Q}_p^{\ell+1}$ is also on the unit sphere and its components are (in lexicographic order):

$$\nu(a_0, a_1, 0, \ldots, 0) = (a_0{}^d, a_0{}^{d-1}a_1, \ldots, a_0 a_1{}^{d-1}, a_1{}^d, 0, \ldots, 0).$$

As a consequence, using again the definition (2.2), we see that $d_{\mathbb{P}^\ell}([1, 0, \ldots, 0], \nu[a_0, a_1, 0, \ldots, 0])$ equals the p-adic norm of the vector:

$$\begin{aligned} (a_0{}^{d-1}a_1, \ldots, a_0 a_1{}^{d-1}, a_1{}^d, 0, \ldots, 0) &= a_1(a_0{}^{d-1}, \ldots, a_0 a_1{}^{d-2}, a_1{}^{d-1}, 0, \ldots) \\ &= a_1(\underbrace{\nu_{1,d-1}(a_0, a_1)}_{\in \mathbb{Q}_p{}^d}, \underbrace{0, \ldots, 0}_{\in \mathbb{Q}_p^{\ell-1-d}}). \end{aligned}$$

But $\|\nu_{1,d-1}(a_0,a_1)\|_p = 1$, so using (5.3) we see:

$$
\begin{aligned}
d_{\mathbb{P}^\ell}([1,0,\ldots,0],\nu[a_0,a_1,0,\ldots,0]) &= \|a_1(\nu_{1,d-1}(a_0,a_1),0,\ldots,0)\|_p \\
&= \|a_1(\nu_{1,d-1}(a_0,a_1))\|_p \\
&= d_{\mathbb{P}^n}([x],[y]) \qquad \square
\end{aligned}
$$

Corollary 39. *Let $\{\xi_{1,\alpha}\}_{i=1,\ldots,n,|\alpha|=d}$ be a family of independent uniformly distributed random variables in $\mathbb{Z}_p$ and for every $i=1,\ldots,n$ define the random polynomial:*

$$
g_i(x) = \sum_{|\alpha|=d} \xi_{i,\alpha} x_0^{\alpha_0} \cdots x_n^{\alpha_n}.
$$

Then $\mathbb{E}\#\{g_1 = \cdots = g_n = 0\} = 1$.

Proof. Proposition 38 gives the volume of the standard Veronese. We apply Theorem 36. $\square$

5.2. **Evans' result and the Mahler Veronese.** The *Mahler basis* for the space of (nonhomoegeneous) polynomials of degree d in n variables is defined as follows. For every $k_1,\ldots,k_n$ with $k_1 + \cdots + k_n \leq d$ consider the polynomial:

$$
T_{k_1,\ldots,k_n}(t_1,\ldots,t_n) := \binom{t_1}{k_1} \cdots \binom{t_n}{k_n} = \frac{t_1 \cdots (t_1 - k_1 + 1)}{k_1!} \cdots \frac{t_n \cdots (t_n - k_n + 1)}{k_n!}.
$$

The family $\{T_{k_1,\ldots,k_n}\}$ forms a basis for $\mathbb{Q}_p[t_1,\ldots,t_n]_d$. Evans considers the random system of equations:

$$
(5.4) \quad f_1 = \ldots = f_n = 0, \qquad \text{where} \qquad f_i(t_1,\ldots,t_n) = \sum_{k_1+\cdots k_n \leq d} \xi_{i,k} \cdot T_{k_1,\ldots k_n}(t_1,\ldots,t_n)
$$

and proves [Eva06, Theorem 1.2] that the expected number of solutions of (5.4) in $\mathbb{Z}_p^n$ is

$$
\mathbb{E}\#\{f_1 = \ldots = f_n = 0\} \cap \mathbb{Z}_p^n = p^{n\lfloor \log_p d \rfloor}(1 + p^{-1} + \cdots + p^{-n})^{-1}.
$$

We give a proof of Evans' result for the expected number of zeros in $\mathbb{Z}_p$ using the integral geometry formula in the univariate case. We also extend Evans' result and compute the expected number of zeros in $\mathbb{Q}_p \backslash \mathbb{Z}_p$. The argument for both results follow the same pattern. First, we will prove an elementary technical lemma regarding the size of binomial expressions. Next, we use the Arc length formula to compute the image of the appropriate Veronese map on the unit sphere and also the image in projective space. Finally, we apply the Integral Geometry formula to obtain results about the random model.

Lemma 40. *Let $a \in \mathbb{Z}_p$ and let $F\colon (t,1) \to \left(1, \binom{t}{1}, \ldots, \binom{t}{d}\right)$ be the affine Mahler Veronese map. Then the image of $F\colon \mathbb{Z}_p \to \mathbb{Q}_p^{d+1}$ is contained in the unit sphere, and*

$$
|J_F(a)|_p = \max_{1 \leq k \leq d} |k|_p^{-1} = p^{\lfloor \log_p d \rfloor}.
$$

Proof. Since $\mathbb{Z}$ is dense in $\mathbb{Z}_p$ and $\mathbb{Z}_p$ is a discrete valuation domain, we may assume that $a \in \mathbb{Z}$. The first claim is obvious since the first coordinate of $F(a)$ is a unit, and binomial coefficients are integers. Next, let

$$
g(t) := \frac{d}{dt}\binom{t}{k} = \sum_{j=0}^{k-1} \frac{1}{t-j}\binom{t}{k}
$$

and note each term of $g(t)$ is a polynomial. Let α be the largest (in the archimedean sense) p-th power in $\{1, \ldots, k\}$ and let $\beta \in \{a - k + 1, \ldots, a\}$ be an element which is maximally p-divisible. Since both intervals of integers have length k, we have that $|\beta|_p \leq |\alpha|_p$. Furthermore,

$$\prod_{\substack{x=1 \\ x \neq \alpha}}^{k} |x|_p \geq \prod_{\substack{y=a-k+1 \\ y \neq \beta}}^{a} |y|_p .$$

If follows for each $a \in \mathbb{Z}$ and $j \in \{0, \ldots, k-1\}$ that

$$\left| \frac{1}{a-j} \binom{a}{k} \right|_p = \left| \frac{1}{\alpha} \right|_p \left(\prod_{\substack{y=a-k+1 \\ y \neq a-j}}^{a} |y|_p \right) \left(\prod_{\substack{x=1 \\ x \neq \alpha}}^{k} |x|_p \right)^{-1} \leq |\alpha|_p^{-1}$$

since the left hand side is maximal when ommiting the factor $a - j = \beta$ of minimal size. Thus, each term of the k-th entry of $J_F(a)$ is bounded by $|\alpha|_p^{-1} \leq p^{\lfloor \log_p d \rfloor}$.

To demonstrate equality, we let α be the largest p-th power in $\{1, \ldots, d\}$ and we consider the $(\alpha + 1)$-th entry of $J_F(a)$. In this case, we have the equality

$$\prod_{\substack{x=1 \\ x \neq \alpha}}^{\alpha} |x|_p = \prod_{\substack{y=a-\alpha+1 \\ y \neq \beta}}^{a} |y|_p .$$

since both sets $\{1, \ldots, \alpha\}$, $\{a - \alpha + 1, \ldots, a\}$ are a complete set of representatives of the integers modulo the p-th power α. Thus,

$$\frac{d}{dt} \binom{t}{\alpha} (a) = \sum_{j=0}^{\alpha-1} \frac{1}{a-j} \binom{a}{\alpha}$$

has a unique term of maximal size $|\alpha|_p^{-1} = p^{\lfloor \log_p d \rfloor}$. $\square$

Corollary 41. *The length of the image of the affine Mahler Veronese map $F \colon (\mathbb{Z}_p \times \{1\}) \to S^d$*

$$F \colon (t, 1) \to \left(1, \binom{t}{1}, \ldots, \binom{t}{d} \right)$$

is exactly $p^{\lfloor \log_p d \rfloor}$. Furthermore, with $\varphi \colon S^d \to \mathbb{P}^d$, we have that

$$\mathrm{vol}_1(F(\mathbb{Z}_p)) = \mathrm{vol}_1(\varphi(F(\mathbb{Z}_p))).$$

Proof. The first part of the statement, follows immediately from Lemma 37 (with the choice $U = \mathbb{Z}_p$ and $\gamma(t) = F(1, t)$) and Lemma 40:

$$\mathrm{vol}_1(F(\mathbb{Z}_p)) = p^{\lfloor \log_p d \rfloor} \mathrm{vol}_1(\mathbb{Z}_p) = p^{\lfloor \log_p d \rfloor}.$$

We now prove the second part of the claim. In fact, we prove that the Hopf map restricted to the affine Mahler Veronese $F(\mathbb{Z}_p)$ is an isometry. Let $a, b \in F(\mathbb{Z}_p) \subseteq S^d$, and write

$$a := (1, a_1, \ldots, a_d)$$
$$b := (1, b_1, \ldots, b_d).$$

We have that the standard metric distance $d(a, b)$ is $\max_{1 \leq i \leq n} |a_i - b_i|_p$. On the other hand, the distance between the projective points $\varphi(a), \varphi(b)$ is given by the maximum absolute value of the 2×2 minors of $\begin{bmatrix} 1 & a_1 & \ldots & a_d \\ 1 & b_1 & \ldots & b_d \end{bmatrix}$. The maximum absolute value of the minors is invariant under $\mathrm{GL}_{d+1}(\mathbb{Z}_p)$, so substracting integral multiples of the first column from the others yields

the matrix $\begin{bmatrix} 1 & 0 & \cdots & 0 \\ 1 & b_1 - a_1 & \cdots & b_d - a_d \end{bmatrix}$. From which it is clear that $d(\varphi(a), \varphi(b)) = \|a \wedge b\|_p = d(a, b)$, showing that the Hopf map restricted to $F(\mathbb{Z}_p)$ is an isometry. $\qquad\square$

We now turn our attention to the complement of $\mathbb{Z}_p$ in $\mathbb{Q}_p$. We will make extensive use of the simple observation that if $|t|_p > 1$, then $|t - j|_p = |t|_p$ for all $j \in \mathbb{Z}$.

Lemma 42. *For a fixed $|t|_p > 1$, the function $g(k) := \left|\binom{t}{k}\right|_p$ is strictly increasing for $k \in \mathbb{N}$.*

Proof. For $k > 0$, we have that

$$\left|\binom{t}{k}\right|_p = \left|\frac{1}{k}\right|_p \cdot \left|\frac{1}{(k-1)!}\right|_p \cdot \left|\prod_{j=0}^{k-1}(t-j)\right|_p = \left|\frac{t-k+1}{k}\right|_p \cdot \left|\binom{t}{k-1}\right|_p.$$

Since $|k|_p \leq 1$ and $|t|_p > 1$, we are done. $\qquad\square$

Define for $m \geq 1$ the m-th annulus $A_m := B(0; p^m) \backslash B(0; p^{m-1})$ in $\mathbb{Z}_p$. We show how to map A_m to the unit sphere using a scaling of the Mahler Veronese map and we calculate the volume of the image.

Definition 43. We extend the affine Mahler Veronese to all of $\mathbb{Q}_p$ by

$$\begin{array}{rcc} F \colon \mathbb{Q}_p \backslash \mathbb{Z}_p & \to & S^d \\ (t, 1) & \mapsto & \left(\binom{t}{d}^{-1}, \binom{t}{1}\binom{t}{d}^{-1}, \ldots, 1\right). \end{array}$$

By Lemma 42, we have that the image of F is contained in S^d, so the map is well-defined. We also have that F is injective, since it the $(d-1)$-th component is invertible on $\mathbb{Q}_p \backslash \mathbb{Z}_p$. By our choice of scaling, the map F, together with the previously defined affine Mahler Veronese descends to a well-defined morphism $\nu_{\mathrm{mahler}} \colon \mathbb{P}^1 \to \mathbb{P}^d$.

Lemma 44. *If $0 \leq j < d$, then*

$$\frac{d}{dt}\binom{t}{j}\binom{t}{d}^{-1} = \frac{d!}{j!} \cdot \prod_{r=j}^{d-1}\frac{1}{t-r} \cdot \left(\sum_{r=j}^{d-1}\frac{1}{t-r}\right).$$

Proof. We observe that for $0 \geq j < d$ that

$$\binom{t}{j}\binom{t}{d}^{-1} = \frac{d!}{j!} \cdot \frac{\prod_{r=j}^{d-1}(t-r)}{\prod_{r=0}^{d-1}(t-r)} = \frac{d!}{j!} \cdot \prod_{r=j}^{d-1}\frac{1}{t-r}.$$

The result follows from the product rule. $\qquad\square$

Corollary 45. *If $t \in A_m$, then $|J_F(t)|_p = |d|_p \cdot p^{-2m}$.*

Proof. We see that the d-th component of the Jabobian is 0, and for $j < d$ that

$$|(J_F(t))_j|_p = \left|\frac{d!}{j!}\right|_p \cdot \left|\prod_{r=j}^{d-1}\frac{1}{t-r}\right|_p \cdot \left|\sum_{r=j}^{d-1}\frac{1}{t-r}\right|_p.$$

We see that each of the three factors is maximal when $j = d - 1$, so the maximum is attained when $j = d - 1$ and equals $|d|_p \cdot \left|t^{-1}\right|_p \cdot \left|t^{-1}\right|_p$. $\qquad\square$

Corollary 46. *For $m \geq 1$, the image of $F \colon A_m \to S^d$ has volume*

$$(p^m - p^{m-1}) \cdot |d|_p \cdot p^{-2m} = \frac{|d|_p}{p^m}(1 - p^{-1})$$

and the image of $F \colon \mathbb{Q}_p \backslash \mathbb{Z}_p \to S^d$ has volume $\frac{|d|_p}{p}$. Finally, the Hopf fibration restricted to $F(\mathbb{Q}_p \backslash \mathbb{Z}_p)$ is an isometry.

Proof. Since F is injective on A_m, and the Jacobian has constant absolute value, the first claim follows from Lemma 37. For the second, we have

$$\mathrm{vol}_1\left(F(\mathbb{Q}_p \backslash \mathbb{Z}_p)\right) = \mathrm{vol}_1\left(\bigcup_{m \geq 1} F(A_m)\right) = |d|_p\,(1 - p^{-1}) \cdot \sum_{m=1}^{\infty} \frac{1}{p^m} = \frac{|d|_p}{p}.$$

Finally, as the last coordinate of $F(t)$ is 1 for any $t \in \mathbb{Q}_p \backslash \mathbb{Z}_p$, we see as before that the Hopf fibration restricts to an isometry on $F(\mathbb{Q}_p \backslash \mathbb{Z}_p)$. $\qquad\square$

With all of the calculation details in place, we can give several results at once about the expected number of zeros of random polynomials in the Mahler random model.

Theorem 47. *Let $f(t)$ be the random polynomial $f(t) = \sum_{k=0}^{d} \xi_k \binom{t}{k}$ with $\{\xi_k\}_{k=0,\ldots,d}$ a family of i.i.d. random variable uniformly distributed on $\mathbb{Z}_p$. Then:*

(1) *(Evans:)* $\mathbb{E}\#\{f = 0\} \cap \mathbb{Z}_p = \frac{p^{\lfloor \log_p d \rfloor}}{1 + p^{-1}}$.

(2) $\mathbb{E}\#\{f = 0\} = \frac{p^{\lfloor \log_p d \rfloor} + |d|_p p^{-1}}{1 + p^{-1}}$.

Proof. Reasoning as in the proof of Theorem 36, we see that, through the p-adic Integral Geometry Formula and the calculation of Corollary 41 we have:

$$\mathbb{E}\#\{f = 0\} \cap \mathbb{Z}_p = \frac{\mathrm{vol}_1\left(\varphi(F(\mathbb{Z}_p))\right)}{\mathrm{vol}_1(\mathbb{P}^1)} = \frac{p^{\lfloor \log_p d \rfloor}}{1 + p^{-1}}.$$

For the second part, we use the calculation from Corollary 46 in a similar argument, and combine the result with part (1). $\qquad\square$

REFERENCES

[AB15]   Dennis Amelunxen and Peter Bürgisser. Probabilistic analysis of the Grassmann condition number. *Found. Comput. Math.*, 15(1):3–51, 2015.

[Ale03]   Semyon Alesker. Hard Lefschetz theorem for valuations, complex integral geometry, and unitarily invariant valuations. *J. Differential Geom.*, 63(1):63–95, 2003.

[BC13]   Peter Bürgisser and Felipe Cucker. *Condition*, volume 349 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer, Heidelberg, 2013. The geometry of numerical algorithms.

[BF11]   Andreas Bernig and Joseph H. G. Fu. Hermitian integral geometry. *Ann. of Math. (2)*, 173(2):907–945, 2011.

[BKL18]   Paul Breiding, Khazhgali Kozhasov, and Antonio Lerario. On the Geometry of the Set of Symmetric Matrices with Repeated Eigenvalues. *Arnold Math. J.*, 4(3-4):423–443, 2018.

[Car17]   Xavier Caruso. Computations with p-adic numbers, 2017. arXiv:1701.06794.

[Cho00]   Kwok-Kwong Choi. On the distribution of points in projective space of bounded height. *Trans. Amer. Math. Soc.*, 352(3):1071–1111, 2000.

[Con]   Keith Conrad. A multivariable hensel's lemma. Available at https://kconrad.math.uconn.edu/blurbs/gradnumthy/multivarhensel.pdf.

[CRV15]   Xavier Caruso, David Roe, and Tristan Vaccon. p-adic stability in linear algebra. In *ISSAC'15—Proceedings of the 2015 ACM International Symposium on Symbolic and Algebraic Computation*, pages 101–108. ACM, New York, 2015.

[Dem88]   James W. Demmel. The probability that a numerical analysis problem is difficult. *Math. Comp.*, 50(182):449–480, 1988.

[Dix82]   John D. Dixon. Exact solution of linear equations using p-adic expansions. *Numer. Math.*, 40(1):137–141, 1982.

[DKK$^+$17]   B. Dragovich, A. Yu. Khrennikov, S. V. Kozyrev, I. V. Volovich, and E. I. Zelenov. p-adic mathematical physics: the first 30 years. *p-Adic Numbers Ultrametric Anal. Appl.*, 9(2):87–121, 2017.

[EK95]   Alan Edelman and Eric Kostlan. How many zeros of a random polynomial are real? *Bull. Amer. Math. Soc. (N.S.)*, 32(1):1–37, 1995.

[Eva06]   Steven N. Evans. The expected number of zeros of a random system of p-adic polynomials. *Electron. Comm. Probab.*, 11:278–290, 2006.

[Fis97]   Benji Fisher. A note on Hensel's lemma in several variables. *Proc. Amer. Math. Soc.*, 125(11):3185–3189, 1997.

[How93]   Ralph Howard. The kinematic formula in Riemannian homogeneous spaces. *Mem. Amer. Math. Soc.*, 106(509):vi+69, 1993.

[Igu00]   Jun-ichi Igusa. *An introduction to the theory of local zeta functions*, volume 14 of *AMS/IP Studies in Advanced Mathematics*. American Mathematical Society, Providence, RI; International Press, Cambridge, MA, 2000.

[Kid13]   Markus Kiderlen. Introduction into integral geometry and stereology. In *Stochastic geometry, spatial statistics and random fields*, volume 2068 of *Lecture Notes in Math.*, pages 21–48. Springer, Heidelberg, 2013.

[Kul19]   A. Kulkarni. Solving p-adic polynomial systems via iterative eigenvector algorithms. arXiv preprint https://arxiv.org/abs/1907.03740, 2019.

[Oes82]   Joseph Oesterlé. Réduction modulo p^n des sous-ensembles analytiques fermés de $\mathbf{Z}_p^N$. *Invent. Math.*, 66(2):325–341, 1982.

[San04]   Luis A. Santaló. *Integral geometry and geometric probability*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, second edition, 2004. With a foreword by Mark Kac.

[Sch11]   Peter Schneider. *p-adic Lie groups*, volume 344 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer, Heidelberg, 2011.

[Ser81]   Jean-Pierre Serre. Quelques applications du théorème de densité de Chebotarev. *Inst. Hautes Études Sci. Publ. Math.*, (54):323–401, 1981.

[SS93]   M. Shub and S. Smale. Complexity of Bezout's theorem. II. Volumes and probabilities. In *Computational algebraic geometry (Nice, 1992)*, volume 109 of *Progr. Math.*, pages 267–285. Birkhäuser Boston, Boston, MA, 1993.

[SW93]   Rolf Schneider and John A. Wieacker. Integral geometry. In *Handbook of convex geometry, Vol. A, B*, pages 1349–1390. North-Holland, Amsterdam, 1993.

[SW08]   Rolf Schneider and Wolfgang Weil. *Stochastic and integral geometry*. Probability and its Applications (New York). Springer-Verlag, Berlin, 2008.

[VVZ94]   V. S. Vladimirov, I. V. Volovich, and E. I. Zelenov. *p-adic analysis and mathematical physics*, volume 1 of *Series on Soviet and East European Mathematics*. World Scientific Publishing Co., Inc., River Edge, NJ, 1994.

[Wei79]   Wolfgang Weil. Kinematic integral formulas for convex bodies. In *Contributions to geometry (Proc. Geom. Sympos., Siegen, 1978)*, pages 60–76. Birkhäuser, Basel-Boston, Mass., 1979.

[Wei82]   André Weil. *Adeles and algebraic groups*, volume 23 of *Progress in Mathematics*. Birkhäuser, Boston, Mass., 1982. With appendices by M. Demazure and Takashi Ono.

Max Planck Institute MIS Leipzig

E-mail address: avinash@mis.mpg.de

SISSA (Trieste)

E-mail address: lerario@sissa.it