www.oeaw.ac.at

ÖAW AUSTRIAN ACADEMY OF SCIENCES

Johann Radon Institute for
Computational and Applied Mathematics
Austrian Academy of Sciences (ÖAW)

RICAM JOHANN-RADON-INSTITUTE FOR COMPUTATIONAL AND APPLIED MATHEMATICS

An application of Bertini theorem

M. Makhul, J. Schicho

RICAM-Report 2018-26

www.ricam.oeaw.ac.at

AN APPLICATION OF BERTINI THEOREM

MEHDI MAKHUL* AND JOSEF SCHICHO*

Abstract. Given an irreducible variety X over a finite field, the density of hypersurfaces of degree d of intersecting X in an irreducible subvariety tends to 1, when d goes to infinity, by a result of Charles and Poonen. In this note, we analyse the situation fixing $d = 1$ and instead extending the base field. We use this result to compute the probability that a random linear subspace of the right dimension intersects X in a given number of points.

1. Introduction

Throughout this paper, when we write $J_m = G(n-m, n)$ we mean the variety of all linear subspaces of codimension m in the projective space $\mathbb{P}^n$, the so-called *Grassmannian.*

A *Chow variety* is a variety whose points correspond to all cycles of a given projective space of given dimension and degree.

The classical Bertini theorems over an infinite field K assert that if a subscheme $X \subset \mathbb{P}^n(K)$ has a certain property (smooth, geometrically irreducible), then for almost all hyperplanes Γ, the intersection $X \cap \Gamma$ has this property too.

It has been shown that if K is a finite field, then the Bertini Theorem about irreducibility can fail, see [CP16, Theorem 1.10]. In [CP16], the authors considered the density of hypersurfaces (of sufficiently high degree) that intersect a given geometrically irreducible variety in an irreducible subvariety. More precisely: Let $\mathbb{F}_q$ be a finite field of q elements let $\mathbb{F}$ be an algebraic closure of $\mathbb{F}_q$. Let $S = \mathbb{F}_q[x_0, \ldots, x_n]$ be the homogeneous coordinate ring of $\mathbb{P}^n(\mathbb{F}_q)$, let $S_d \subset S$ be the $\mathbb{F}_q$-subspace of homogeneous polynomials of degree d. For $f \in S_d$, let H_f be the hypersurface defined by $f = 0$. Define the *density* of $\mathcal{P} \subset S_{homog} = \cup_{d=0}^{\infty} S_d$ by

$$\mu(\mathcal{P}) := \lim_{d\to\infty} \frac{|\mathcal{P} \cap S_d|}{|S_d|}.$$

Theorem 1.1 (Charles–Poonen)**.** *Let X be a geometric irreducible subscheme of $\mathbb{P}^n(\mathbb{F}_q)$. If $\dim X \geq 2$, then the density of*

$$\left\{f \in S_{homog} : H_f \cap X \text{ is geometrically irreducible}\right\}$$

is 1.

Poonen in [Poo04] proved a similar result for smoothness.

Key words and phrases. Bertini Theorem, Finite Fields.

* Supported by the Austrian Science Fund (FWF): W1214-N15, Project DK9.

Theorem 1.2 (Poonen)**.** *Let X be a smooth quasiprojective subscheme of $\mathbb{P}^n$ of dimension $m \geq 0$ over $\mathbb{F}_q$. Then there exists a homogeneous polynomial f over $\mathbb{F}_q$ for which the intersection of X and the hypersurface H_f is smooth. In fact, the set of such f has a positive density, equal to $\zeta(m+1)^{-1}$, where ζ is the zeta function.*

Recently, an analogue of this problem for plane curves was investigated in [Asg18]. In this paper, we consider an algebraic variety $X \subset \mathbb{P}^n(\mathbb{F}_q)$ of degree d and dimension m over a finite field $\mathbb{F}_q$ with q elements, where q is a prime power. Given such a variety, we can define the probability for a codimension m linear subspace in $\mathbb{P}^n(\mathbb{F}_q)$ to intersect it in exactly k points. Notice that here we consider the mere set-theoretic intersection: no multiplicities are taken into account. We can then consider the same kind of probability, keeping the same variety X, but changing the base field from $\mathbb{F}_q$ to $\mathbb{F}_{q^2}$, $\mathbb{F}_{q^3}$ and so on. In this way, for every $N \in \mathbb{N}$ we define the numbers $p_k^N(X)$, namely the probability for a codimension m linear subspace in $\mathbb{P}^n(\mathbb{F}_{q^N})$ to intersects X in exactly k points. If the limit as N goes to infinity of the sequence $\left(p_k^N(X)\right)_{N\in\mathbb{N}}$ exists, we denote this number by $p_k(X)$. We will compute the exact values $p_k(X)$ for each $k = 0, 1, \ldots d$, provided that X satisfies some geometrically properties.

The first our result remains of a similar one by Charles-Poonen. In that case, however, one considers the behaviour of the density as the degree gets larger and larger; here, instead, we fix degree and we extend the base field.

Theorem 1.3. *Let X be a geometrically irreducible variety of dimension m in $\mathbb{P}^n$. Then*

$$\mu_e(X) = \lim_{N\to\infty} \frac{\left|\left\{\Gamma \in S_1 : \Gamma \cap X \text{ is geometrically irreducible}\right\}\right|}{\left|\mathbb{P}^*(\mathbb{F}_{q^N})\right|} = 1.$$

We also consider a generalization of the following theorem proved in [MSG18].

Theorem 1.4. *Let C be an geometrically irreducible plane algebraic curve of degree d over $\mathbb{F}_q$, where q is a prime power. Suppose that C has simple tangency. Then for every $k \in \{0, \ldots, d\}$ we have*

$$p_k(C) = \sum_{s=k}^{d} \frac{(-1)^{k+s}}{s!}\binom{s}{k}.$$

In particular, $p_{d-1}(C) = 0$ and $p_d(C) = 1/d!$.

Theorem 1.5. *Let X be a geometrically irreducible variety of dimension m and degree d in projective space $\mathbb{P}^n(\mathbb{F}_q)$, where q is a prime power. Suppose that X has simple tangency property. Then for every $k \in \{0, \ldots d\}$ we have*

$$p_k(X) = \sum_{s=k}^{d} \frac{(-1)^{k+s}}{s!}\binom{s}{k}.$$

First we use Bertini Theorem and Lang-Weil Theorem [LW54, Theorem 1] to show that for a general hyperplane Γ the intersection $X \cap \Gamma$ is irreducible, provided that X is a given geometrically irreducible variety.

Sketch of proof: Given a variety X of dimension m in $\mathbb{P}^n(\mathbb{F}_{q^N})$, we want to know how the probability of the intersection between X and a random linear subvariety V of codimension m in $\mathbb{P}^n(\mathbb{F}_{q^N})$ behaves. To do this we first intersect X with a linear subspace Γ containing V. By Bertini Theorem for a hyperplane, when $N \to \infty$ we get a geometrically irreducible curve and by Lemma 2.6 it must be a curve with simple tangency. Then after some calculation we can show that the desired probability coincides with $p_k(C)$.

2. Main results

Let X be an irreducible algebraic variety over a finite field $\mathbb{F}_q$. Define

$$\mu_e(X) = \lim_{N\to\infty} \frac{\left|\left\{\Gamma \in S_1 : \Gamma \cap X \quad \text{is geometrically irreducible}\right\}\right|}{\left|\mathbb{P}^*(\mathbb{F}_{q^N})\right|}. \tag{1}$$

By applying the Bertini Theorem for an infinite field [Jou83, Theorem 6.3(4)] we show that $\mu_e(X) = 1$. In other words the intersection $X(\mathbb{F}_{q^N}) \cap \Gamma(\mathbb{F}_{q^N})$ is also geometrically irreducible, for a generic hyperplane Γ, if $N \to \infty$.

Theorem 2.1. *Let X be a geometrically irreducible variety of dimension m in $\mathbb{P}^n$. Then*

$$\mu_e(X) = \lim_{N\to\infty} \frac{\left|\left\{\Gamma \in S_1 : \Gamma \cap X \textit{ is geometrically irreducible}\right\}\right|}{\left|\mathbb{P}^*(\mathbb{F}_{q^N})\right|} = 1.$$

Proof. Let $\mathcal{H}_{d,m-1}$ be the Chow variety of cycles in $\mathbb{P}^n$ of dimension $m-1$ and degree d in $\mathbb{P}^n$. Let $\Omega \subset S_1$ be the set of hyperplanes intersection with X is reducible of dimension $m-1$. More precisely if $\Gamma \in \Omega$, then $X \cap \Gamma = X_1 \cup X_2$, where $X_i \in \mathcal{H}_{d_i,m_i}$ for $i = 1, 2$ and $\max(m_1, m_2) = m-1$ and $d_1 + d_2 = d$.

First we show that Ω is a closed set. To do this, consider the rational map

$$\Phi_X : S_1 \dashrightarrow \mathcal{H}_{d,m-1} \quad \Gamma \mapsto \Gamma \cap X.$$

Indeed $\Omega = \bigcup_{d_1,d_2,d_1+d_2=d} \Phi^{-1}(\mathcal{H}_{d_1,m_1} \times \mathcal{H}_{d_2,m_2})$. Hence Ω is an algebraic variety. By Bertini Theorem $\dim \Omega < \dim S_1 = n+1$. Hence the probability that an element in S_1 is in Ω tends to 0. More precisely, by the Lang-Weil Theorem this probability is bounded by

$$\frac{(q^N)^{\dim \Omega}}{(q^N)^{\dim S_1}} \to 0 \quad \text{for } N \to \infty. \qquad \square$$

Let X be a variety in projective space $\mathbb{P}^n(K)$, where K is an algebraically closed perfect field. We define the *conormal* variety of X as the Zariski closure of the set

$$\operatorname{con}(X) := \left\{(p, \Gamma) \in X \times (\mathbb{P}^n)^* : T_p(X) \subset \Gamma\right\}.$$

Let π_2 be the second projection $\operatorname{con}(X) \to \pi_2(\operatorname{con}(X)) := X^*$, which is called the conormal map. If $\operatorname{con}(X)$ and $\operatorname{con}(X^*)$ are isomorphic by the map which flips the two entries of a pair in a product variety, then we say that X is *reflexive*.

It is known that if the field K has zero characteristic, then every variety is reflexive; this is not true in characteristic $p > 0$. The following theorem is useful for checking if a given projective variety is reflexive or not. see [Wal56].

Theorem 2.2 (Monge-Segre-Wallace)**.** *A projective variety X is reflexive if and only if the conormal map π_2 is separable.*

In [HK85] the authors proved the following result, called the Generic Order of Contact Theorem:

Theorem 2.3. *A projective curve Z is non-reflexive if and only if for a general point p of Z and a general tangent hyperplane H to Z at p, we have*

$$[K(\mathrm{con}(Z)) : K(Z^*)]_{isep} = I(p, Z.H).$$

Where $I(p, Z.H)$ is the intersection multiplicity of Z and H at p, and $[K(\mathrm{con}(Z)) : K(Z^*)]_{isep}$ is the inseparable degree extension.

A combination of these two theorems implies

Corollary 2.4. *If C is a geometrically irreducible reflexive curve of degree d in $\mathbb{P}^n(\overline{\mathbb{F}_q})$, then there exists a hyperplane $H \subset \mathbb{P}^n(\overline{\mathbb{F}_q})$ intersecting C in $d-1$ smooth points of C such that H intersects C transversely at $d-2$ points and has intersection multiplicity 2 at the remaining point. We say C has simple tangency.*

Definition 2.5. *Let X be a geometrically irreducible variety in $\mathbb{P}^n(K)$ of dimension m. We say that X has the simple tangency property if there exist a linear subspace $\Gamma \in J_{m-1}$ such that the curve $X \cap \Gamma$ has simple tangency.*

Lemma 2.6. *Suppose that X is a geometrically irreducible variety of degree d and dimension m in $\mathbb{P}^n(K)$ with simple tangency property. Then for a general linear subspace $\Gamma \in J_{m-1}$ the intersection $X \cap \Gamma$ is a curve with simple tangency.*

Proof. Let $\mathcal{H}_{d,m}$ be the Chow variety. Let $\mathcal{H}'_{d,1}$ be the set of all curves in $\mathbb{P}^n(K)$ of degree d and without simple tangency. Define

$$\Phi_X\colon J_{m-1} \dashrightarrow \mathcal{H}_{d,1}, \qquad (X, \Gamma) \mapsto X \cap \Gamma.$$

Notice that Φ_X in general is a rational map but we can consider the restriction Φ_X to $\mathrm{dom}(\Phi_X)$ if necessary to Φ_X be a morphism. For a fixed $X \in \mathcal{H}_{d,m}$,

$$\Omega_X = \Big\{\Gamma \in J_{m-1} : \quad X \cap \Gamma \quad \text{does not have simple tangency}\Big\}.$$

Indeed $\{X\} \times \Omega_X \cong \Omega_X$, by the definition we have $\Omega_X \subset \Phi^{-1}(\mathcal{H}'_{d,1})$. Since X is a variety with simple tangency property there exists a linear subspace $\Gamma \in J_{m-1}$ such that $\Gamma \cap X$ is a curve with simple tangency, hence $\Phi^{-1}(\mathcal{H}'_{d,1})$ is a proper set. We need to only show that $\Phi^{-1}(\mathcal{H}'_{d,1})$ is a close set. The proof of the lemma is a consequence of the following claim.

Claim. $\mathcal{H}'_{d,1}$ is a closed set in $\mathcal{H}_{d,1}$.

Proof of the claim. By Theorem 2.2 a curve C is in $\mathcal{H}'_{d,1}$ if and only if its conormal map is not separable. This is the case if and only if the Jacobian of the conormal map vanishes identically. This can be expressed as algebraic equations in the curve, hence the set $\mathcal{H}'_{d,1}$ is closed. □

Let us first formulate the definition of the probabilities that we want to compute.

Definition 2.7 (Probabilities of intersection)**.** *Let q be a prime power and let $X \subset \mathbb{P}^n(\mathbb{F}_q)$ be a geometrically irreducible variety of dimension m and degree d defined over $\mathbb{F}_q$. For every $N \in \mathbb{N}$ and for every $k \in \{0, \dots, d\}$, the k-th* probability of intersection *$p_k^N(X)$ of varieties of codimension m with X over $\mathbb{F}_{q^N}$ is*

$$p_k^N(X) := \frac{\Big|\big\{V \in J_m \,:\, |X(\mathbb{F}_{q^N}) \cap V(\mathbb{F}_{q^N})| = k\big\}\Big|}{|J_m(\mathbb{F}_{q^N})|}.$$

Theorem 2.8. *Let X be a geometrically irreducible variety of dimension m and degree d in projective space $\mathbb{P}^n(\mathbb{F}_q)$, where q is a prime power. Suppose that X has the simple tangency property. Then for every $k \in \{0, \dots d\}$ we have*

$$p_k(X) = \sum_{s=k}^{d} \frac{(-1)^{k+s}}{s!}\binom{s}{k}.$$

Proof. Define

$$I = \big\{(V, W) \in J_m \times J_{m-1} : V \subset W\big\}.$$

From Definition 2.7, we have

$$p_k^N(X) = \frac{\big|\{V \in J_m : |X(\mathbb{F}_{q^N}) \cap V(\mathbb{F}_{q^N})| = k\}\big|}{|J_m|} = \frac{\big|\{(V,W) \in I : |X(\mathbb{F}_{q^N}) \cap V(\mathbb{F}_{q^N})| = k\}\big|}{|I|}.$$

By extending this formula over all $W \in J_{m-1}$ we obtain

$$\sum_{W \in J_{m-1}} \frac{\big|\{(V,W) \in I : |V \cap X \cap W| = k\}\big|}{|I|}. \tag{2}$$

Where for a generic W the intersection $X \cap W$ must be geometrically irreducible curve by Theorem 1.3. Since any two linear subspaces have same number of points over a finite field we can write:

$$\sum_{W \in J_{m-1}} \frac{\big|\{V \subset W : |V \cap X \cap W| = k\}\big|}{\big|\{V : V \subset W\}\big|} \Bigg/ \frac{|I|}{\big|\{V : V \subset W_0\}\big|} \tag{3}$$

But the denominator of Equation (3) is $|J_{m-1}|$. Let us write $J_{m-1} = A \sqcup B$, where

$$A = \big\{W \in J_{m-1} : X \cap W \quad \text{is irreducible and has simple tangency}\big\},$$

and

$$B = \big\{W \in J_{m-1} : X \cap W \quad \text{is reducible or without simple tangency}\big\}.$$

From these and Equation (3) we obtain

$$p_k^N(X) = \frac{\sum_{W \in A} p_k^N(X \cap W) + \sum_{W \in B} \delta_B}{|J_{m-1}|},$$

where $\delta_B = \delta$ is a number in interval $[0, 1]$. Hence

$$\frac{|p_k^N(X \cap W_0)||A| + \delta|B|}{|J_{m-1}|}.$$

By Lemma 2.6 we know that $\frac{|B|}{|J_{m-1}|} \to 0$, when $q \mapsto \infty$. This implies

$$p_k^N(X \cap W_0) = \frac{p_k^N(X \cap W_0)|A|}{|J_{m-1}|}.$$

Note that $X \cap W_0$ is a curve of degree d. Hence the result is a consequence of the [MSG18, Proposition 5.2]. □

It is natural to consider the probabilities of intersection of a variety X of degree d and dimension m in $\mathbb{P}^n$ with a random variety Y of degree e and codimension m in $\mathbb{P}^n$. If X is a hypersurface and Y is a curve, via the *Veronese map* we can reduce this situation to the one of [MSG18, Proposition 5.2]. This motivates us to pose the following conjecture.

Conjecture 2.9. *Let X be a geometrically irreducible variety of dimension m and degree d in $\mathbb{P}^n(\mathbb{F}_q)$, where q is a prime power. Suppose that X has the simple tangency property. Let $e \in \mathbb{N}$ be a natural number. Then for every $k \in \{0, 1, \dots ek\}$ the probability that a random irreducible variety of degree e and codimension m intersects X in exactly k points is given by*

$$p_k(X, e) = \sum_{s=k}^{de} \frac{(-1)^{k+s}}{s!}\binom{s}{k}.$$

If we removed the word "irreducible" in the conclusion above, then the conjecture would be false: the set of varieties in $\mathbb{P}^n$ of degree d and codimension m is bijective to the set of points in a Zariski-dense and open set of a Chow variety. The Chow variety has several components of maximal dimension; the smallest case for which this happens is $m = e = 2$ and $n = 3$. Here there is an 8-dimensional set of irreducible conics and an 8-dimensional set of reducible conics (pairs of lines). One can show that the probability that an irreducible conic intersect X in k points is as stated in the conjecture, but for the reducible conics, the probabilities differ. The total probabilities would be the arithmetic means of both, which would then also differ from the statement above.

Acknowledgements. We are grateful to Herwig Hauser, who informed us about theorem of Bertini. Also we would like to thank Matteo Gallet for helpful discussions.

References

[Asg18] Shamil Asgarli, *Sharp Bertini theorem for plane curves over finite fields*, Available at https://arxiv.org/abs/1804.01569.

[CP16] François Charles and Bjorn Poonen, *Bertini irreducibility theorems over finite fields*, J. Amer. Math. Soc. **29** (2016), no. 1, 81–94. MR 3402695

[HK85] Abramo Hefez and Steven L. Kleiman, *Notes on the duality of projective varieties*, Geometry today (Rome, 1984), Progr. Math., vol. 60, Birkhäuser Boston, Boston, MA, 1985, pp. 143–183. MR 895153

[Jou83] Jean-Pierre Jouanolou, *Théorèmes de Bertini et applications*, Progress in Mathematics, vol. 42, Birkhäuser Boston, Inc., Boston, MA, 1983. MR 725671

[LW54] Serge Lang and André Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827.

[MSG18] Mehdi Makhul, Josef Schicho, and Matteo Gallet, *Probabilities of incidence between lines and a plane curve over finite fields*, Available at https://arxiv.org/abs/1711.06021.

[Par86] Rita Pardini, *Some remarks on plane curves over fields of finite characteristic*, Compositio Math. **60** (1986), no. 1, 3–17. MR 867952

[Poo04] Bjorn Poonen, *Bertini theorems over finite fields*, Ann. of Math. (2) **160** (2004), no. 3, 1099–1127. MR 2144974

[Wal56] Andrew H. Wallace, *Tangency and duality over arbitrary fields*, Proc. London Math. Soc. (3) **6** (1956), 321–342. MR 0080354

(Mehdi Makhul) Johann Radon Institute for Computational and Applied Mathematics (RICAM), Austrian Academy of Sciences, Linz and Research Institute for Symbolic Computation (RISC), Johannes Kepler University, Linz

(Josef Schicho) Research Institute for Symbolic Computation (RISC), Johannes Kepler University, Linz

Email address: {mmakhul,jschicho}@risc.jku.at