PROBABILITIES OF INCIDENCE BETWEEN LINES AND A PLANE CURVE OVER FINITE FIELDS

Mehdi Makhul

Radon Institute For Computation and Applied Mathematics

June 19, 2019

Definition

Let X be an algebraic curve over a field K. We say that X is *geometrically irreducible* if X is irreducible over $\overline{K}$. Here $\overline{K}$ denotes the algebraic closure of K.

Example (non-geometrically irreducible curve)

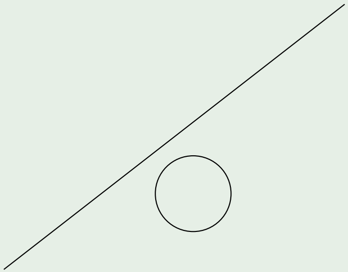
Consider the curve C given by

$$C := x^2 + y^2 = 0,$$

C is irreducible over real numbers but it is not irreducible over complex numbers. i.e $x^2 + y^2 = (x + iy)(x - iy) = 0$.

If C is an irreducible algebraic curve of degree d, by Bézout's theorem every line intersects C in d points (over an algebraically closed field). We can see that if the base field is not algebraically closed then we can get less than d intersection points.

Example



Incidence over finite fields

Given an algebraic curve C over a finite field $\mathbb{F}_q$ we would like to study the behaviour of the number of k-rich lines determined by the set of points corresponding to the some algebraic plane curve from a probabilistic point of view.

What is the probability that a random line in the (affine or projective) plane intersects a curve of given degree in a given number of points? What happens when we extend the base field to $\mathbb{F}_{q^2}$, $\mathbb{F}_{q^3}$,...,$\mathbb{F}_{q^N}$, and in particular what happens to the probabilities as $N \to \infty$.

Example

Let C be an irreducible quadratic curve in $\mathbb{P}^2(\mathbb{F}_q)$. It is known that C contains exactly $q+1$ $\mathbb{F}_q$-points. Hence the number of lines that meets C in exactly two points is

$$\binom{q+1}{2}.$$

On the other hand every tangent line touches C in exactly one point, hence there are $q+1$ lines in $\mathbb{P}^2(\mathbb{F}_q)$ that intersects C in exactly one point. By a straight forward calculation since the total number of lines in the projective plane is q^2+q+1, we expect that the number of lines that do not meet C to be

$$\frac{q(q-1)}{2}.$$

Now if we replace $\mathbb{F}_q$ with $\mathbb{F}_{q^N}$ for $N = 1, 2, 3, \ldots$, then we have

$$t_2 = \frac{q^N(q^N+1)}{2},\ t_1 = q^N + 1,\ t_0 = \frac{q^N(q^N-1)}{2}.$$

Since the total number of lines in $\mathbb{P}^2(\mathbb{F}_{q^N})$ is $q^{2N} + q^N + 1.$ We conclude

$$p_2(C) = \frac{1}{2},\ p_1 = 0,\ p_0 = \frac{1}{2}.$$

We would like to control this behaviour for an arbitrary curve.

Definition (Probabilities of intersection)

Let q be a prime power and let $C \subseteq \mathbb{P}^2(\mathbb{F}_q)$ be a geometrically irreducible curve of degree d defined over $\mathbb{F}_q$. For every $N \in \mathbb{N}$ and for every $k \in \{0, \ldots, d\}$, the *k-th probability of intersection* $p_k^N(C)$ of lines with C over $\mathbb{F}_{q^N}$ is

$$p_k^N(C) := \frac{\left|\{\text{lines } \ell \subseteq \mathbb{P}^2(\mathbb{F}_{q^N}) \ : \ |\ell(\mathbb{F}_{q^N}) \cap C(\mathbb{F}_{q^N})| = k\}\right|}{q^{2N} + q^N + 1}.$$

Notice that $q^{2N} + q^N + 1$ is the number of lines in $\mathbb{P}^2(\mathbb{F}_{q^N})$. We define $p_k(C)$ to be the limit of $(p_k^N(C))$ if it exists.

Theorem (M, Gallet-Schicho)

Let C be a geometrically irreducible plane algebraic curve of degree d over $\mathbb{F}_q$, where q is a prime power. Then the limit $p_k(C)$ exists for $0 \leq k \leq d$. Furthermore,

$$p_0(C) + p_1(C) + \cdots + p_d(C) = 1.$$

Definition (Simple tangency)

Let C be a geometrically irreducible curve of degree d in $\mathbb{P}^2(\overline{\mathbb{F}_q})$. We say that C has *simple tangency* if there exists a line $\ell \subseteq \mathbb{P}^2(\overline{\mathbb{F}_q})$ intersecting C in $d-1$ smooth points of C such that ℓ intersects C transversely at $d-2$ points and has intersection multiplicity 2 at the remaining point.

Theorem (M, Gallet-Schicho)

Let C be a geometrically irreducible plane algebraic curve of degree d over $\mathbb{F}_q$. 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 $p_d(C) = 1/d!$.

Incidences in higher dimension

Finally we generalize the intersection between a given curve and a random line to a given variety of dimension m in $\mathbb{P}^n$ with a random linear subspace of codimension m.

Definition

In projective space $\mathbb{P}^n$, we denote $J_m = G(n-m, n)$ to be the variety of all linear subspaces of codimension m in the projective space $\mathbb{P}^n$, the so-called *Grassmannian*.

Definition

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.

Theorem (M-Schicho)

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

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

Thank you for your attention.