Probabilities of incidence between lines and a plane curve over finite fields

Mehdi Makhul[a,b,1], Josef Schicho[b,2], Matteo Gallet[c,*,3]

[a] *Johann Radon Institute for Computational and Applied Mathematics (RICAM), Austrian Academy of Sciences, Linz, Austria*
[b] *Research Institute for Symbolic Computation (RISC), Johannes Kepler University, Linz, Austria*
[c] *International School for Advanced Studies/Scuola Internazionale Superiore di Studi Avanzati (ISAS/SISSA), Via Bonomea 265, 34136 Trieste, Italy*

ABSTRACT

We study the probability for a random line to intersect a given plane curve, over a finite field, in a given number of points over the same field. In particular, we focus on the limits of these probabilities under successive finite field extensions. Supposing absolute irreducibility for the curve, we show how a variant of the Chebotarev density theorem for function fields can be used to prove the existence of these limits, and to compute them under a mildly stronger condition, known as simple tangency. Partial results have already appeared in the literature, and we propose this work as an introduction to the use of the Chebotarev theorem in the context of incidence geometry. Finally, Veronese maps allow us to compute similar probabilities of intersection between a given curve and random curves of given degree.

11R44

Keywords:
Sylvester-Gallai theorem
Galois group

[*] Corresponding author.
E-mail addresses: mmakhul@risc.jku.at (M. Makhul), jschicho@risc.jku.at (J. Schicho), mgallet@sissa.it (M. Gallet).

[1] Supported by the Austrian Science Fund (FWF): W1214-N15 Project DK9, and P30405-N32.
[2] Supported by the Austrian Science Fund (FWF): W1214-N15 Project DK9.
[3] Supported by the Austrian Science Fund (FWF): W1214-N15 Project DK9, P26607, P25652, P31061 and Erwin Schrödinger Fellowship J4253.

1. Introduction

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? More precisely, what happens if we consider a finite field with q elements as base field, and then we ask the same question for a field with $q^2, q^3, \dots, q^N$ elements, analyzing how these probabilities behave as N goes to infinity? In this work we investigate this problem by means of algebro-geometric techniques. Recently, the interplay between combinatorial problems and algebraic techniques has become more and more common, and has been revealing to be extremely fruitful. Here we refer in particular to the area called *combinatorial geometry*, which is described in the abstract of [1] as the area dealing with "*the possible range of behaviors of arbitrary finite collections of geometric objects such as points, lines, or circles with respect to geometric operations such as incidence or distance*". As Tao points out in [1], in the last decade algebraic geometry and algebraic topology helped to unriddle several important questions and conjectures in this area. Amongst the most prominent of such problems, one can mention the *distinct distance problem* (see [2]), the *Kakeya problem over finite fields* (see [3] and later improvements in [4] and [5]) and the *Dirac-Motzkin conjecture* (see [6]). For a nice survey about these topics, see [1].

A motivation for the problem we investigate in our paper comes from the famous *Sylvester-Gallai theorem*. Sylvester posed it as a question in [7], which was raised again by Erdös in [8] and later solved by Melchior (see [9]) and Gallai (see [10]). Given a set of points in the affine plane, a line is called *ordinary* if it passes through exactly two of them.

Theorem 1.1 *(Sylvester-Gallai). Suppose that P is a finite set of points in the real plane, not all on a line. Then P admits an ordinary line.*

This theorem is clearly false if we work over finite fields, since in this case we can pick P to be the whole plane. Moreover, the theorem is false also on the complex plane: in fact, in [11] Serre observed that the 9 inflection points of a cubic curve do not satisfy the requirements of Silvester-Gallai theorem; also, the so-called 3-*nets* provide other counterexamples, see [12,13].

In the same circle of ideas, in [14], Solymosi considered the following situation. Given a set P of points in the plane, a line is called *k-rich*, if it contains precisely k points of P. For example, a 2-rich line is an ordinary line. Then, Solymosi's theorem reads as:

Theorem 1.2 *(Solymosi). For any $k \geq 4$, there is a positive integer n_0 such that for $n > n_0$ there exists $P \subseteq \mathbb{R}^2$ such that there are at least $n^{2-\frac{c}{\sqrt{\log n}}}$ k-rich lines, but no $k+1$-rich lines. Here, $c = 2\log(4k+1)$.*

A recent outstanding result of Green and Tao (see [6]) gives an almost complete description of the structure of sets with few ordinary lines in the real plane. In the same paper, the authors also proved the Dirac-Motzkin conjecture and a less known problem, referred in the literature as the *orchard problem*.

Our work is inspired by these results. Here, we consider an algebraic plane curve C of degree d over a finite field $\mathbb{F}_q$ with q elements, where q is a prime power, namely the set of points in the projective plane $\mathbb{P}^2_{\mathbb{F}_q}$ that are zeros of a homogeneous trivariate polynomial of degree d. Given such a curve, we can define the probability for a line in $\mathbb{P}^2_{\mathbb{F}_q}$ 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 curve C — namely, the same trivariate polynomial — 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 $p_k^N(C)$, namely the probability for a line in $\mathbb{P}^2_{\mathbb{F}_{q^N}}$ to intersect C in exactly k points. If the limit as N goes to infinity of the sequence $\big(p_k^N(C)\big)_{N\in\mathbb{N}}$ exists, we denote this number by $p_k(C)$. The main tool we use to compute these numbers when the curve C is absolutely irreducible and with *simple tangency* is an effective version of the *Chebotarev theorem* for function fields. Here, by *absolutely irreducible* we mean that the curve is irreducible over the algebraic closure of its field of definition. By asking that the curve has *simple tangency* we require that there exists a line whose intersection with C consists of simple intersections except for one, which is a double intersection. These are the main results of our paper:

Theorem 1.3. *Let C be an absolutely irreducible plane algebraic curve of degree d over $\mathbb{F}_q$, where q is a prime power. Then the numbers $\{p_k(C)\}$ are well-defined, namely the corresponding limits exist.*

Theorem 1.4. *Let C be an absolutely 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 $p_d(C) = 1/d!$.

We approached this problem using Galois theory techniques; during a revision of our work, we have been informed[4] that some of the questions investigated in this paper (or similar ones) have already appeared in the literature, though expressed in a different language and with different purposes (see [15] and [16]). Both the two cited paper use the Chebotarev theorem for function field as a key ingredient. After studying the Chebotarev

[4] We thank two anonymous referees for pointing us to the relevant literature.

theorem, we realized that we could use it to provide a much shorter proof for our result than the one we initially used, and that our initial approach, although we were not aware of that, did not differ too much from the techniques that lead to the Chebotarev theorem. However, we still think that our initial approach could be of interest for researchers in discrete and combinatorial geometry. In fact, although it provides less information than the Chebotarev theorem, it can serve as an introduction to this technique because of its self-containedness and of the avoidance of technical aspects that are present in other works. Because of this, in the initial part of this paper we report our initial approach to the problem, and then we explain how to use the Chebotarev theorem to obtain Theorem 1.4. After that, we show how the same technique provides a formula for the probabilities of intersection between a given plane curve of degree d and a random plane curve of degree e (Proposition 5.5). Claus Diem then pointed out to us that the material we present has essentially already appeared in SGA1 [17] by Grothendieck, but it is "a bit hidden", as he said; he suggested another way of presenting the material, which we found better than the one we used, and we adopted this choice of exposition.[5]

We briefly summarize how the problem we investigate is discussed in the aforementioned literature. In [15], the focus is a variant of the so-called *Bateman-Horn conjecture* for polynomial rings of finite fields. The original Bateman-Horn conjecture concerns the frequency of prime numbers among the values of a system of polynomials at integer numbers. One of its consequences is *Schinzel conjecture*, which asks whether, given polynomials $f_1, \ldots, f_r \in \mathbb{Z}[x]$, then for infinitely many $n \in \mathbb{Z}$ we have that $f_1(n), \ldots, f_r(n)$ are all prime. Bary-Soroker and Jarden consider the situation in which $\mathbb{Z}$ is replaced by $\mathbb{F}_q[t]$ for some prime power q. More precisely, given polynomials $f_1, \ldots, f_r \in \mathbb{F}_q[t][x]$, they want to compute the number of polynomials $g \in \mathbb{F}_q[t]$ such that $f_1\bigl(t, g(t)\bigr), \ldots, f_r\bigl(t, g(t)\bigr)$ are irreducible. In particular, they focus on the case when g is linear, namely on the computation of the pairs $(a_1, a_2) \in \mathbb{F}_q^2$ such that $f_1(t, a_1 t + a_2), \ldots, f_r(t, a_1 t + a_2)$ are irreducible. In our language, this is the number of lines in the plane such that the polynomial obtained by restricting a plane curve on such a line is irreducible. The authors improve a result by Bender and Wittenberg (see [18, Theorem 1.1 and Proposition 4.1]) and show that this number goes as q^2/d. To prove this, they make use of an effective version of the Chebotarev density theorem (see the appendix of [19]). The number computed by Bary-Soroker and Jarden is similar to the quantity p_0 that we define, though it is not the same, since it can happen that a line does not intersect a curve at any point over $\mathbb{F}_q$, but the polynomial given by the restriction of the curve to the line can be reducible. Also the behavior as $d \to \infty$ of these two quantities is different: the one by Bary-Soroker and Jarden goes to zero, while p_0 tends to $1/e$.

In [16], the author focuses on the complexity of computation of the so-called *discrete logarithm* in the group of divisors of degree 0 of a nonsingular curve. Given two elements a and b in a group G, the discrete logarithm $\log_b a$ is an integer k such that $b^k = a$. On a smooth curve C, one can consider formal integer sums of points of C, and define an

[5] We thank Claus Diem for his careful description of the alternative way of presenting the material.

equivalence relation on them in order to obtain the class group of C. One can therefore try to compute discrete logarithms in the class group of a curve, and in particular for those formal integer sums of points whose coefficients add up to zero, namely the ones of degree 0; this has important applications in cryptography. In [16, Theorem 2], Diem proves that computing the discrete logarithm has an expected time of $\widetilde{O}(q^{2-\frac{2}{d-2}})$ for those curves over $\mathbb{F}_q$ that admit a birational plane model D of degree d such that there exists a line in the plane intersecting D in d distinct points over $\mathbb{F}_q$. Then the author computes the number of lines in the plane intersecting D in exactly d points over $\mathbb{F}_q$ (see [16, Theorem 3]), namely the quantity $p_d(D)$ in our language. As in the previous paper, this is done using an effective version of the Chebotarev density theorem (see [20]).

Recently, a new paper [21] appeared dealing with the same problem we investigate in our work, but allowing the given curve to be constituted of several irreducible components. We have been informed by Kaloyan Slavov that also Birch and Swinnerton-Dyer investigated in [22] this topic, providing a formula for the quantity $p_1(C) + \cdots + p_d(C)$ in our language. We thank him for pointing out to us this reference, and for useful suggestions.

The rest of the paper is structured as follows. Section 2 introduces some preliminary results, namely the Lang-Weil bound for the number of points of a variety over a finite field (Subsection 2.1) and some known facts about Galois groups of plane curves (Subsection 2.2). Sections 3 and 4 present our initial approach to the problem, which provides less information than the one obtained via the Chebotarev theorem, but uses more elementary tools (namely, some basic facts about étale maps). Section 5 shows how to use the Chebotarev density theorem in order to prove Theorems 1.3 and 1.4 and Proposition 5.5.

2. Preliminaries

2.1. Lang-Weil bound

One of the main tools we use in our work is the so-called *Lang-Weil bound* for the number of points of a variety over a finite field (see [23, Theorem 1]). For a nice exposition of this result, see Terence Tao's blog.[6] Let $\mathbb{F}$ be a field and consider an affine algebraic variety V over $\mathbb{F}$. This means that we are given finitely many polynomials $P_1, \ldots, P_r \in \mathbb{F}[x_1, \ldots, x_n]$, which generate the so-called ideal of V, denoted $I(V)$. For any extension of fields $\mathbb{F} \subseteq \mathbb{K}$, we denote by $V(\mathbb{K})$ the set of common zeros in $\mathbb{K}^n$ of the polynomials in the ideal $I(V)$, considered now as an ideal in $\mathbb{K}[x_1, \ldots, x_n]$. One says that a variety V is *irreducible* if $I(V)$ is prime in $\mathbb{F}[x_1, \ldots, x_n]$. For our considerations we will need a stronger notion of irreducibility, which we introduce in the following definition.

[6] https://terrytao.wordpress.com/2012/08/31/the-lang-weil-bound/.

Definition 2.1. We say that an affine variety V over a field $\mathbb{F}$ is *absolutely irreducible* if the ideal $I(V)$ is prime in $\overline{\mathbb{F}}[x_1,\dots,x_n]$, where $\overline{\mathbb{F}}$ is an algebraic closure of $\mathbb{F}$.

Definition 2.2. We say that an affine variety $V \subseteq \mathbb{F}^n$ defined by polynomials $P_1,\dots,P_r$ has *complexity* M if $n, r \leq M$ and $\deg(P_i) \leq M$ for all $i \in \{1,\dots r\}$.

Theorem 2.3 *(Lang-Weil bound). Let V be an absolutely irreducible variety over a finite field $\mathbb{F}$ of complexity at most M. Then*

$$|V(\mathbb{F})| = \left(1 + O_M(|\mathbb{F}|^{-\frac{1}{2}})\right)|\mathbb{F}|^{\dim(V)}.$$

By writing $O_M(|\mathbb{F}|^{-\frac{1}{2}})$ we mean that there exists a nonnegative constant δ_M depending on M, but not on V, such that

$$\left(1 - \delta_M|\mathbb{F}|^{-\frac{1}{2}})\right)|\mathbb{F}|^{\dim(V)} \leq |V(\mathbb{F})| \leq \left(1 + \delta_M|\mathbb{F}|^{-\frac{1}{2}})\right)|\mathbb{F}|^{\dim(V)}.$$

Using an inclusion-exclusion argument, one obtains by induction on the dimension:

Corollary 2.4. *Let V be a variety over a finite field $\mathbb{F}$ of complexity at most M. Then*

$$|V(\mathbb{F})| = \left(c + O_M(|\mathbb{F}|^{-\frac{1}{2}})\right)|\mathbb{F}|^{\dim(V)},$$

where c is the number of irreducible components of V that are absolutely irreducible.

All the considerations and results we stated so far hold also for projective varieties over finite fields. By a *projective variety* over a field $\mathbb{F}$ we mean a variety in the projective space $\mathbb{P}^n_{\mathbb{F}}$ given by finitely many *homogeneous* polynomials $P_1,\dots,P_r \in \mathbb{F}[x_0,\dots,x_n]$. From now on, all the varieties we consider are projective, or are open subsets of projective varieties.

2.2. Galois group of a plane curve

The aim of this section is to recall a construction (see [24]) which associates a Galois group to a plane algebraic curve. We will see in the following sections that this group determines the irreducibility of certain surfaces; this will be the key to derive a formula for the probabilities we are interested in.

Let q be a prime power, namely $q = p^r$ for some prime number p. We denote by $\mathbb{F}_q$ the finite field with q elements. Let C be an absolutely irreducible algebraic curve in $\mathbb{P}^2_{\mathbb{F}_q}$. Define X_1 to be the unique subvariety of $C \times \check{\mathbb{P}}^2_{\mathbb{F}_q}$ — here $\check{(\cdot)}$ denotes the *dual projective plane* — such that, for every extension field K of $\mathbb{F}_q$,

$$X_1(K) = \left\{(w, [\ell]) \in C(K) \times \check{\mathbb{P}}^2(K) : w \in \ell\right\} \quad \text{and} \quad X_0 := \check{\mathbb{P}}^2_{\mathbb{F}_q}.$$

For a line $\ell \subseteq \mathbb{P}^2_K$, we write $[\ell]$ for the corresponding point in $\check{\mathbb{P}}^2(K)$. The correspondence is given by

$$\check{\mathbb{P}}^2(K) \ni (a:b:c) \quad \longleftrightarrow \quad \big\{(x:y:z) \in \mathbb{P}^2(K) \,:\, ax+by+cz=0\big\}.$$

Definition 2.5. Using the notation we have already introduced, we define the map $\pi\colon X_1 \longrightarrow X_0$ to be the projection onto the second component.

Since X_0 is irreducible, we can define its *function field*, denoted $K(X_0)$. This is the field of equivalence classes of morphisms $\varphi\colon U \longrightarrow \mathbb{A}^1_{\mathbb{F}_q}$, where U is any (Zariski) open subset of X_0; two morphisms are considered equivalent if they agree on a non-empty open subset. Consider the projection $\rho\colon X_1 \longrightarrow C$ on the first component: its fibers are lines in the dual projective space. Hence all these fibers are irreducible varieties of the same dimension. This implies that X_1 is irreducible by [25, Exercise 11.4.C]; its function field is denoted $K(X_1)$.

Lemma 2.6 *(see [24, Definition 1.3]). The projection $\pi\colon X_1 \longrightarrow X_0$ is a quasi-finite dominant separable morphism of degree d.*

Because of Lemma 2.6, the induced map $\pi^*\colon K(X_0) \longrightarrow K(X_1)$ between fields of rational functions realizes $K(X_1)$ as a finite separable extension of $K(X_0)$ of degree d. By the primitive element theorem, the field $K(X_1)$ is generated over $K(X_0)$ by a single rational function $h \in K(X_1)$ satisfying $P(h) = 0$ for an irreducible monic polynomial P over $K(X_0)$ of degree d.

Definition 2.7 *(Galois group, see [24, Definition 1.3]).* Using the notation just introduced, we define the *Galois group* $\mathrm{Gal}(C)$ of C to be the Galois group of a splitting field of the polynomial P over $K(X_0)$. In other words, $\mathrm{Gal}(C)$ is the Galois group of a Galois closure (see [26, Remark 4.77]) of the field extension $K(X_0) \hookrightarrow K(X_1)$. The group $\mathrm{Gal}(C)$ is independent of the choice of h and it can be regarded as a subgroup of the permutation group S_d of the roots of P.

Definition 2.8 *(Simple tangency).* Let C be an absolutely irreducible curve of degree d in $\mathbb{P}^2_{\mathbb{F}_q}$. 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.

Remark 2.9. A general curve $C \subseteq \mathbb{P}^2_{\mathbb{F}_q}$ of degree d has simple tangency. In fact, notice that having simple tangency is an open condition, therefore it is enough to exhibit a single example in order to obtain the claim. To do that, consider the curve of equation

$$x^2\, P(x,y) + z\, Q(x,y,z) = 0,$$

where P is a homogeneous polynomial with $d-2$ distinct roots in $\overline{\mathbb{F}}_q$ and Q is a homogeneous polynomial of degree $d-1$.

Proposition 2.10 *([24, Proposition 2.1]). Let $C \subseteq \mathbb{P}^2_{\mathbb{F}_q}$ be an absolutely irreducible plane curve of degree d with simple tangency. Then the Galois group* $\mathrm{Gal}(C)$ *of C is the whole symmetric group S_d.*

Claus Diem pointed out to us that in the original proof of Proposition 2.10 it is written that "*For $k = 2$ the variety U_2 is a $\mathbb{P}^{n-2}$-bundle over C and therefore irreducible*". He explained us that this is impossible for dimension reasons. A first attempt for a fix would be to replace C by $C \times C$. It turns out that then the fibers are not (always) proper, and then one cannot conclude that U_2 is irreducible. A correct argument has already been given by Ballico and Hafez in [27].

3. Galois theory for étale maps

In this section we associate a Galois group to a morphism (satisfying certain conditions) between two irreducible smooth varieties. We show that this concept admits a geometric counterpart, and we use this characterization in the next section. As we pointed out in the Introduction, the results of this and the following section are subsumed by the ones of Section 5. Nevertheless, we believe that the approach presented in these sections can be useful to help understanding the setting that is used also in the Chebotarev theorem to solve this kind of problems. Claus Diem pointed out that the material in this section is essentially already present in SGA1 [17]; moreover, he suggested us a clearer and shorter way to present the material about Galois closures of étale maps. We follow his suggestions, and we thank him for sharing with us this material.

For technical reasons, we develop the theory for a special class of morphisms, namely the one of *étale* maps. They model, in the algebraic setting, the notion of "local isomorphism" for the analytic topology. Recall that, in differential geometry, a smooth map between two smooth manifolds is a *local diffeomorphism* if it induces an isomorphism at the level of tangent spaces. For an affine variety X cut out by polynomials $P_1, \ldots, P_r$, one defines the *tangent cone* $C_O(X)$ of X at the origin as the variety defined by the homogeneous parts of minimal degree of each of the polynomials $P_1, \ldots, P_r$; the tangent cone at any other point is obtained by translating it to the origin and by applying the previous definition. The tangent cone plays for étale morphisms the role played by the tangent space for local diffeomorphisms. A morphism $f \colon X \longrightarrow Y$ between varieties over an algebraically closed field is *étale at a point $x \in X$* if it induces an isomorphism between the tangent cones $C_x(X)$ and $C_{f(x)}(Y)$. A map is called *étale* if it is étale at every point (see [28, Chapter 2]). For more general varieties, one adopts the definition of an étale map as a morphism which is flat and unramified (see [29, Chapter 1]).

We are going to define a notion of Galois closure for étale maps.

Remark 3.1. Consider a separable extension of fields $K \subseteq L$. We can define the *Galois closure* of this extension as the minimal extension M of L which is Galois over K. In the language of schemes, the extension $K \subseteq L$ corresponds to a connected étale map. The two varieties of this map have each a single point, but the structure of schemes still allows to encode the field extension. We can hence consider the classical notion of Galois closure for field extensions as the "toy" case of the notion of Galois closure of étale maps.

We mimic the classical notion of Galois closure for field extensions in the context of maps. The Galois closure of a map, then, is defined as a map satisfying a universal property similar to the one satisfied by the Galois closure of a field extension.

Definition 3.2. Let $g\colon Z \longrightarrow X$ be a connected étale map, namely both Z and X are connected. We say that Z is *Galois* over X if the group of automorphisms of Z is transitive on the geometric fibers of g.

Definition 3.3. Let $f\colon X \longrightarrow Y$ be a connected étale morphism. A *Galois closure* of f is an étale morphism $Z \longrightarrow X$ such that Z is Galois over Y and such that $Z \longrightarrow X$ is minimal under this condition. The latter sentence means that if $Z \longrightarrow X$ factors as $Z \longrightarrow Z' \longrightarrow X$, where Z' is Galois and connected, then actually $Z = Z'$.

We now provide a characterization of Galois closures of étale maps, showing that the Galois closure always exists.

Definition 3.4. Let $f\colon X \longrightarrow Y$ be a finite étale map of degree d between two irreducible smooth varieties. We define the *Galois scheme* (see [30, Section 3]) of f as the scheme $\mathrm{GS}(f)$ such that for any extension K of the ground field of X and Y, we have

$$\mathrm{GS}(f)(K) = \bigl\{(x_1, \ldots, x_d) \in X^d(K) \,:\, f(x_1) = \cdots = f(x_d),\ x_i \neq x_j \text{ for all } i \neq j\bigr\}.$$

Notice that the Galois scheme is the fiber product of d copies of the map f minus $\binom{d}{2}$ small diagonals. Because of this, and since f is a finite map, we have

$$\dim \mathrm{GS}(f) \,=\, \dim X \,=\, \dim Y. \qquad (1)$$

There is an induced map $F\colon \mathrm{GS}(f) \longrightarrow Y$, sending $(x_1, \ldots, x_d)$ to $f(x_1)$, which is dominant, and each point $y \in Y$ has $d!$ preimages. Notice that $\mathrm{GS}(f)$ is Galois over Y.

Proposition 3.5. *Let $f\colon X \longrightarrow Y$ be a finite connected étale map of degree d between two irreducible smooth varieties. Pick a point $y_0 \in Y$ and let $(x_1, \ldots, x_d)$ be a fixed permutation of the (geometric) fiber of f over y_0. Let Z be the connected component of $\mathrm{GS}(f)$ containing $(x_1, \ldots, x_d)$. Then $F|_Z\colon Z \longrightarrow Y$ is a Galois closure of $f\colon X \longrightarrow Y$.*

Proof. We have to prove that Z is Galois over Y and that Z is minimal with respect to this property. Since $\mathrm{GS}(f)$ is Galois over Y, also the restriction of F to any of its connected components is so, hence Z is Galois over Y. Suppose now that we have a factorization $Z \longrightarrow Z' \longrightarrow X$ with Z' Galois over Y. This induces a factorization of the inclusion $Z \hookrightarrow \mathrm{GS}(f)$ as $Z \longrightarrow Z' \hookrightarrow \mathrm{GS}(f)$, and this implies that $Z = Z'$. □

Remark 3.6. Note that the permutation group S_d of d elements is a group of automorphisms of $\mathrm{GS}(f)$ over Y acting transitively on the fibers of F. Hence the stabilizer of Z under this group is a group of automorphisms of $F|_Z$ acting transitively on the fibers (which shows that Z is Galois over Y). It follows that the number of irreducible components of the Galois scheme $\mathrm{GS}(f)$ coincides with the number of cosets of this stabilizer.

We notice that, if we consider the étale map of varieties induced by a separable extension of fields $K \subseteq L$, then the spectrum of a Galois closure (in the field sense) of $K \subseteq L$ satisfies the universal property of the Galois closure (in the map sense, namely as in Definition 3.3).

Definition 3.7. Let $f\colon X \longrightarrow Y$ be a finite étale morphism between irreducible smooth varieties. Since f is dominant, it determines a field extension $K(Y) \hookrightarrow K(X)$. We define the *Galois group* $\mathrm{Gal}(f)$ of f to be the Galois group of the extension $K(Y) \hookrightarrow E$, where E is a Galois closure (see [26, Remark 4.77]) of $K(Y) \hookrightarrow K(X)$.

Proposition 3.8. *For every finite étale morphism $f\colon X \longrightarrow Y$ of smooth irreducible varieties the Galois group of f is the stabilizer of the Galois closure Z of f in the Galois scheme* $\mathrm{GS}(f)$*.*

Proof. The proof follows if we can show that the base change of a Galois closure is still a Galois closure if it is connected. In fact, if this is true, given a Galois closure $Z \longrightarrow Y$ of f, we can consider its base change at the generic point of Y. The base change of $Z \longrightarrow X \longrightarrow Y$ under this map is $\operatorname{Spec} K(Z) \longrightarrow \operatorname{Spec} K(X) \longrightarrow \operatorname{Spec} K(Y)$. We then know that $K(Z)$ is a Galois closure of $K(Y) \subseteq K(X)$, and so $\mathrm{Gal}\big(K(Z)/K(Y)\big)$ is $\mathrm{Gal}(f)$. However, $\mathrm{Gal}\big(K(Z)/K(Y)\big)$ coincides with the stabilizer of Z in $\mathrm{GS}(f)$, because base change preserves the group of automorphism lying over the base and permuting the fibers (which makes the corresponding map Galois over the base).

Hence, we need to show that the base change of a Galois closure is still a Galois closure if it is connected. Suppose that $g\colon W \longrightarrow Y$ is a morphism. Then the map $f'\colon X \times_Y W \longrightarrow W$ is étale by [31, Lemma 38.34.4]. Assume that $X \times_Y W$ is connected; then by base change $Z \times_Y W$ is a union of connected components of $\mathrm{GS}(f')$. Therefore $Z \times_Y W$ is a Galois closure of f' when it is itself connected. □

Now we cast the notions defined so far into the framework of Galois schemes of morphisms (Corollary 3.12). After that, we recall the notion of simple tangency for a curve and highlight its consequences on Galois groups.

Definition 3.9. For an absolutely irreducible curve $C \subseteq \mathbb{P}^2_{\mathbb{F}_q}$ of degree d, define $\mathcal{V}_C$ to be the set of points in $X_0 = \check{\mathbb{P}}^2_{\mathbb{F}_q}$ such that the restriction of the map $\pi\colon X_1 \longrightarrow X_0$ from Definition 2.5 to $\mathcal{U}_C := \pi^{-1}\big(\mathcal{V}_C\big)$ is étale.

Remark 3.10. Notice that the set $\mathcal{V}_C$ is open and non-empty. In fact, since the map $\pi\colon X_1 \longrightarrow X_0$ is separable, the general point of X_0 belongs to $\mathcal{V}_C$. Moreover, by Lemma 2.6 the map π is quasi-finite, and since both X_0 and X_1 are projective varieties, it is finite, hence closed. The locus of point in X_1 where π is ramified is closed (since it is locally defined by the vanishing of the minors of a Jacobian matrix), so its image under π is closed, too. Therefore the locus in X_0 over which π is unramified is open and non-empty. It is then enough to ensure that $\pi\colon \mathcal{U}_C \longrightarrow \mathcal{V}_C$ is flat. Now, the locus in the domain where a map is flat is open (see [31, Tag 0398, Theorem 36.15.1,]), and flat maps are open morphisms (see [31, Tag 01U2, Lemma 28.24.9]), so this shows that $\mathcal{V}_C$ is open. The fact that $\mathcal{V}_C$ is non-empty is ensured by the generic flatness result (see [31, Tag 0529, Proposition 28.26.1]).

Lemma 3.11. *Let C be an absolutely irreducible curve of degree d over $\mathbb{F}_q$. Then the restriction to $\mathcal{U}_C := \pi^{-1}\big(\mathcal{V}_C\big)$ of the map $\pi\colon X_1 \longrightarrow X_0$ from Definition 2.5 is a finite separable dominant étale morphism between smooth absolutely irreducible varieties.*

Proof. We know from Section 2.2 that both X_0 and X_1 are smooth and absolutely irreducible. Since $\mathcal{V}_C$ and $\mathcal{U}_C$ are open and non-empty, the same is true for them. Moreover, π is a quasi-finite separable dominant morphism between projective varieties (Lemma 2.6) and so it is finite. Hence, the same holds for its restriction $\pi_{|\mathcal{U}_C}$. By Remark 3.10, the map is étale, and this concludes the proof. □

By unravelling the definitions, in the light of Lemma 3.11 we obtain:

Corollary 3.12. *For an absolutely irreducible projective plane curve C over $\mathbb{F}_q$, we have* $\mathrm{Gal}(C) \cong \mathrm{Gal}\big(\pi_{|\mathcal{U}_C}\big)$.

The interpretation of the Galois group of a curve provided by Corollary 3.12 allows to use Proposition 3.8 and hence to deduce the irreducibility of the Galois scheme when the Galois group is the full symmetric group.

Corollary 3.13. *Suppose that C is an absolutely irreducible curve in $\mathbb{P}^2_{\mathbb{F}_q}$ of degree d with simple tangency. Then, the Galois group $\mathrm{Gal}\big(\pi_{|\mathcal{U}_C}\big)$ is the full symmetric group, and so the Galois scheme $\mathrm{GS}\big(\pi_{|\mathcal{U}_C}\big)$ is irreducible.*

Proof. This follows from Corollary 3.12 and Proposition 3.8. □

4. Probabilities of incidence

In this section we define probabilities of intersection between a random line and a given curve in the projective plane over a finite field (Definition 4.1). We then prove the main result of our paper, namely Theorems 1.3 and 1.4, by showing that its counterpart for morphisms hold (Theorems 4.5 and 4.7). We will re-prove these results in Section 5 by using the Chebotarev density theorem.

Definition 4.1 *(Probabilities of intersection).* Let q be a prime power and let C be a plane projective absolutely irreducible curve of degree d 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

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

Notice that $q^{2N} + q^N + 1$ is the number of lines in $\mathbb{P}^2_{\mathbb{F}_{q^N}}$.

The aim of this paper is to prove that the limit as N goes to infinity of the quantities $p_k^N(C)$ exists for every k, and to give a formula for these limits, provided that some conditions on the curve C are fulfilled.

The following result is a direct consequence of Definitions 4.1 and 2.5.

Lemma 4.2. *Let C be a plane projective absolutely irreducible curve of degree d over $\mathbb{F}_q$. For every $k \in \{0, \ldots, d\}$ we have*

$$p_k^N(C) = \frac{\left|\left\{[\ell] \in \check{\mathbb{P}}^2(\mathbb{F}_{q^N}) \,:\, |\pi^{-1}([\ell])(\mathbb{F}_{q^N})| = k\right\}\right|}{q^{2N} + q^N + 1}.$$

Via Lemma 4.3 and Definition 4.4 we reduce the problem of computing intersection probabilities for curves to the analogous problem for morphisms.

Lemma 4.3. *Let C be a plane projective absolutely irreducible curve of degree d over $\mathbb{F}_q$. Let $\mathcal{V}_C \subseteq \check{\mathbb{P}}^2_{\mathbb{F}_q}$ be as in Definition 3.9. For every $N \in \mathbb{N}$ and for every $k \in \{0, \ldots, d\}$, define*

$$\widetilde{p}_k^N(C) := \frac{\left|\left\{[\ell] \in \mathcal{V}_C(\mathbb{F}_{q^N}) \,:\, |\pi^{-1}([\ell])(\mathbb{F}_{q^N})| = k\right\}\right|}{|\mathcal{V}_C(\mathbb{F}_{q^N})|}.$$

Then $\lim\limits_{N\to\infty} p_k^N(C)$ exists if and only if $\lim\limits_{N\to\infty} \widetilde{p}_k^N(C)$ exists, in which case the two numbers coincide.

Proof. It is enough to show that the probability for a point to lie in $\mathbb{P}^2(\mathbb{F}_{q^N}) \setminus \mathcal{V}_C(\mathbb{F}_{q^N})$ goes to zero as N goes to infinity. This is a consequence of the Lang-Weil bound (Theorem 2.3). In fact, since the complement of $\mathcal{V}_C$ has dimension at most 1:

$$\frac{\left|\mathbb{P}^2_{\mathbb{F}_{q^N}}(\mathbb{F}_{q^N}) \setminus \mathcal{V}_C(\mathbb{F}_{q^N})\right|}{q^{2N} + q^N + 1} \sim \frac{\left(c + O(q^{-N/2})\right) q^N}{q^{2N}} \to 0\,,$$

where the constant c is the number of irreducible components of the complement of $\mathcal{V}_C$. □

Definition 4.4. Let $f\colon X \longrightarrow Y$ be a finite étale morphism of degree d, where q is a prime power, between smooth irreducible varieties over $\mathbb{F}_q$. For every $N \in \mathbb{N}$ and for every $k \in \{0, \ldots, d\}$, we define the *k-th preimage probability* $p_k^N(f)$ to be

$$p_k^N(f) := \frac{\left|\left\{y \in Y(\mathbb{F}_{q^N}) \,:\, |f^{-1}(y)(\mathbb{F}_{q^N})| = k\right\}\right|}{|Y(\mathbb{F}_{q^N})|}\,.$$

Notice that if C is an absolutely irreducible algebraic plane curve of degree d, then for every $N \in \mathbb{N}$ and for every $k \in \{0, \ldots, d\}$ we have $\widetilde{p}_k^N(C) = p_k^N\left(\pi_{|\mathcal{U}_C}\right)$. Hence, by Lemma 4.3, in order to show the existence of the limits of k-th probabilities of intersections for a curve, it is enough to show the existence of k-th preimage probabilities for morphisms over $\mathbb{F}_q$.

Theorem 4.5. *Let $f\colon X \longrightarrow Y$ be a finite étale morphism of degree d, where q is a prime power, between smooth irreducible varieties over $\mathbb{F}_q$. Then for every $k \in \{0, \ldots, d\}$ the limit as N goes to infinity of the sequence $\left(p_k^N(f)\right)_{N \in \mathbb{N}}$ exists.*

Proof. We generalize the construction of the Galois scheme of the morphism f. For every $k \in \{0, \ldots, d\}$, define $G_k(f)$ to be the scheme such that for every extension K of $\mathbb{F}_q$, we have

$$\begin{aligned} G_k(f)(K) := \big\{(x_1, \ldots, x_k) \in X^k(K) \,:\, & f(x_1) = \ldots = f(x_k), \\ & x_i \neq x_j \text{ for all } i \neq j\big\}. \end{aligned}$$

In particular $G_d(f) = \mathrm{GS}(f)$. As we showed for the Galois scheme, see Equation (1), for every k the variety $G_k(f)$ has the same dimension of X and Y. There is a natural finite morphism $F_k\colon G_k(f) \longrightarrow Y$, the fiber product of f with itself k times. A general $\overline{\mathbb{F}}_q$-valued point of Y has $d(d-1)\cdots(d-k+1)$ preimages under the map F_k. The main idea of the proof is to compute, in two different ways, the expected cardinality $\mu_k^N(f)$ of the set of $\mathbb{F}_{q^N}$-rational points of the fiber $F_k^{-1}(y)$, where y is a uniformly distributed random element in $Y(\mathbb{F}_{q^N})$. On one hand,

$$\mu_k^N(f) = \frac{\bigl|G_k(f)(\mathbb{F}_{q^N})\bigr|}{\bigl|Y(\mathbb{F}_{q^N})\bigr|}\,.$$

On the other hand, we can express $\mu_k^N(f)$ in terms of the preimage probabilities:

$$\mu_k^N(f) = \sum_{s=k}^{d} s(s-1)\cdots(s-k+1)\,p_s^N(f)\,. \tag{2}$$

In matrix form:

$$\begin{pmatrix} \mu_0^N(f) \\ \vdots \\ \mu_d^N(f) \end{pmatrix} = \begin{pmatrix} 1 & * & \cdots & & \cdots & * \\ 0 & 1 & * & & & \vdots \\ \vdots & & \ddots & & & \vdots \\ 0 & \cdots & 0 & k! & * & * \\ \vdots & & & & \ddots & \vdots \\ 0 & \cdots & & & \cdots & d! \end{pmatrix} \begin{pmatrix} p_0^N(f) \\ \vdots \\ p_d^N(f) \end{pmatrix}. \tag{3}$$

Since the matrix in Equation (3) has non-zero determinant, we can write

$$p_k^N(f) = \sum_{s=0}^{d} \alpha_{k,s}\,\mu_s^N(f) \tag{4}$$

for some numbers $(\alpha_{k,s})_{k,s}$. Using the Lang-Weil bound on Equation (2), we have

$$\mu_k^N(f) \sim \frac{\delta_k\, q^{N\cdot\dim G_k(f)}}{q^{N\cdot\dim Y}} \qquad \text{as } N \to \infty\,, \tag{5}$$

where δ_k is the number of irreducible components of $G_k(f)$ that are absolutely irreducible. Since $\dim G_k(f) = \dim Y$, we conclude that the limit in Equation (5) exists, and so by Equation (4) also $\lim\limits_{N\to\infty} p_k^N(f)$ exists. □

Remark 4.6. Theorem 1.3 holds. In fact, the map $\pi_{|\mathcal{U}_C}$ satisfies the hypotheses of Theorem 4.5, so the numbers $p_k\bigl(\pi_{|\mathcal{U}_C}\bigr)$ exist, and we have already proved that this implies that the limits $p_k(C)$ exist.

Theorem 4.7. *Let $f\colon X \longrightarrow Y$ be a finite étale morphism of degree d, where q is a prime power, between smooth irreducible varieties over $\mathbb{F}_q$. Suppose that* Gal(f) *is the full symmetric group S_d. Then for every $k \in \{0,\dots,d\}$ we have*

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

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

Proof. Since $\mathrm{Gal}(f)$ is the full symmetric group, the Galois scheme $\mathrm{GS}(f)$ is absolutely irreducible. Hence, using the notation of the proof of Theorem 4.5, for all $k \in \{0, \dots, d\}$ we have

$$\lim_{N\to\infty} \mu_k^N(f) = \lim_{N\to\infty} \frac{q^{N\cdot \dim G_k(f)}}{q^{N\cdot \dim Y}} = 1. \tag{6}$$

In fact, every variety $G_k(f)$ is an image (under a projection) of $\mathrm{GS}(f) = G_d(f)$, thus is absolutely irreducible and so Equation (6) follows from Equation (5). Again using the notation as in Theorem 4.5, we get

$$\lim_{N\to\infty} p_k^N(f) = \sum_{s=0}^{d} \alpha_{k,s}. \tag{7}$$

Therefore, the statement is proved once we are able to explicitly compute the coefficients $(\alpha_{k,s})_{k,s}$. Recall that $\alpha_{k,s}$ is the (k,s)-entry of the inverse of the matrix M_d appearing in Equation (3). A direct inspection of the matrices M_d shows that they admit the following structure:

$$M_d = \left(\begin{array}{ccc|c} & & & 1 \\ & M_{d-1} & & \vdots \\ & & & d!/1! \\ \hline 0 & \cdots & 0 & d!/0! \end{array}\right).$$

A direct computation shows that

$$M_d^{-1} = \left(\begin{array}{ccc|c} & & & \frac{(-1)^d}{d!}\cdot\binom{d}{0} \\ & M_{d-1}^{-1} & & \vdots \\ & & & \frac{(-1)}{d!}\cdot\binom{d}{d-1} \\ \hline 0 & \cdots & 0 & \frac{1}{d!}\cdot\binom{d}{d} \end{array}\right).$$

Hence

$$\alpha_{k,s} = \frac{(-1)^{k+s}}{s!}\binom{s}{k} \qquad \text{for all } k, s \in \{0, \dots, d\}.$$

It follows from Equation (7) that for all $k \in \{0, \dots, d\}$,

$$p_k(f) = \sum_{s=0}^{d} \frac{(-1)^{k+s}}{s!}\binom{s}{k} = \sum_{s=k}^{d} \frac{(-1)^{k+s}}{s!}\binom{s}{k}$$

and so the statement is proved. □

As a consequence of Proposition 2.10 and Theorem 4.7, Theorem 1.4 holds.

5. Probabilities of intersection via the Chebotarev theorem

In this section, we show how to use an effective version of the Chebotarev density theorem for function fields as exposed in [19, Appendix A]—and used in [15] and [16] to prove the results reported in the Introduction—to show Theorems 1.3 and 1.4. We recall the setting and the results of the paper [19], and specialize the Chebotarev theorem to our case. We refer to the cited appendix for the proofs of the claims we make in this section regarding the objects introduced to state the Chebotarev theorem (Theorem 5.1).

We start by considering an integrally closed finitely generated $\mathbb{F}_q$-algebra R and a monic polynomial $\mathcal{F} \in R[T]$ such that the discriminant of $\mathcal{F}$ is invertible in R. In our case, we take R to be the $\mathbb{F}_q$-algebra

$$R := \frac{\mathbb{F}_q[a,b,u]}{\mathrm{Disc}_x\big(F(x,ax+b)\big)\cdot u - 1} \cong \mathbb{F}_q[a,b]_{(f)} \quad \text{with } f := \mathrm{Disc}_x\big(F(x,ax+b)\big),$$

where the last ring is the localization of the polynomial ring $\mathbb{F}_q[a,b]$ at the element f. In geometric terms, R is the coordinate ring of the open subset of the dual projective plane parameterizing lines in the plane that intersect the curve $\{F=0\}$ in d distinct points over the algebraic closure of $\mathbb{F}_q$. We then take the polynomial $\mathcal{F}$ to be $F(T,aT+b)$. Then by construction, its discriminant is invertible in R.

Starting from R and $\mathcal{F}$, we consider K, the quotient field of R, and we define L to be the splitting field of $\mathcal{F}$ over K. In other words, if $\{y_1,\dots,y_d\}$ are the roots of $\mathcal{F}$, we set $L := K(y_1,\dots,y_d)$. In our situation, we have

$$L = \frac{K[t_1,\dots,t_d]}{\big(F(t_i,at_i+b) \text{ for } i\in\{1,\dots,d\}\big)}\,.$$

Then we define S to be the integral closure of R in L, namely $S = R[y_1,\dots,y_d]$. Geometrically, S is the coordinate ring of an open subset of the unique variety $X_d \subset C^d \times \check{\mathbb{P}}^2_{\mathbb{F}_q}$ such that for every extension M of $\mathbb{F}_q$ we have

$$X_d(M) = \big\{(x_1,\dots,x_d,[\ell]) \in C^d(M)\times\check{\mathbb{P}}^2(M) :\ x_i\in\ell\big\}\,.$$

The strategy we adopt to compute probabilities of intersections is the following: our goal is to count the number of lines ℓ in $\mathbb{P}^2$ such that the intersection $\ell(\mathbb{F}_{q^N})\cap C(\mathbb{F}_{q^N})$ is constituted of exactly k points, and we interpret this as the number of lines such that the univariate polynomial $F_{|\ell}$ has exactly k linear factors over $\mathbb{F}_{q^N}$. Notice that every univariate polynomial H of degree d over $\mathbb{F}_q^N$ determines a partition π_H of d, namely a tuple $\pi_H = (\alpha_1,\dots,\alpha_s)$ such that $\alpha_1+\cdots+\alpha_s = d$ and $\alpha_1\le\cdots\le\alpha_s$. Such partition is obtained by factoring H over $\mathbb{F}_{q^N}$ into irreducible factors $H_1,\dots,H_s$ and then setting $\alpha_i = \deg(H_i)$. Then, the number of lines we are interested in can be computed as the sum, over the set of partitions π of d with exactly k ones, of the number of lines ℓ such that the partition associated to $F_{|\ell}$ is π. The Chebotarev theorem provides a formula for the probability for a line to determine a given partition.

We set G to be the Galois group of the field extension $K \subseteq L$. By definition, this coincides with the Galois group of the curve C as in Definition 2.7. Notice that, in our situation, the intersection $L \cap \mathbb{F}$, where $\mathbb{F}$ is an algebraic closure of $\mathbb{F}_q$, coincides with $\mathbb{F}_q$. This implies that the subgroup

$$G_0 := \left\{ g \in G :\ g_{|\mathbb{F}_q}(x) = x \text{ for all } x \in \mathbb{F}_q \right\}$$

coincides with G. Similarly, if for every $\nu \geq 1$ we set

$$G_\nu := \left\{ g \in G :\ g_{|\mathbb{F}_q}(x) = x^{q^\nu} \text{ for all } x \in \mathbb{F}_q \right\},$$

then G_ν, which in general is a coset of G_0 in G, coincides with G.

As one can see from the definition of X_d, its points are intimately related to the probabilities we are interested in. From an algebraic point of view (see [32, Section II.6]) these points correspond to $\mathbb{F}_q$-homomorphisms from S to $\mathbb{F}$. Moreover, a homomorphism $\Phi \in \mathrm{Hom}_{\mathbb{F}_q}(S, \mathbb{F})$ such that $\Phi(R) = \mathbb{F}_{q^\nu}$ corresponds to a point $(x_1, \ldots, x_d, [\ell])$ in X_d such that the line ℓ is defined over $\mathbb{F}_{q^\nu}$. Given such a homomorphism Φ there always exists an element in G, called the *Frobenius element* and denoted $\left[\frac{S/R}{\Phi}\right]$ such that the following diagram is commutative:

$$\begin{tikzcd} S \arrow[r, "\left[\frac{S/R}{\Phi}\right]"] \arrow[d, "\Phi"'] & S \arrow[d, "\Phi"] \\ \mathbb{F} \arrow[r, "\alpha \mapsto \alpha^{q^\nu}"] & \mathbb{F} \end{tikzcd} \tag{8}$$

In other words, we have the relation

$$\Phi\left(\left[\frac{S/R}{\Phi}\right] x \right) = \Phi(x)^{q^\nu} .$$

One then can show that $\left[\frac{S/R}{\Phi}\right] \in G_\nu$.

If we fix a line in $\mathbb{P}^2$, namely, if we fix an $\mathbb{F}_q$-homomorphism $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(R, \mathbb{F})$, we can consider all points in X_d "lying over" this line. In other terms, we can consider all homomorphisms $\Phi \in \mathrm{Hom}_{\mathbb{F}_q}(S, \mathbb{F})$ prolonging φ. Their corresponding Frobenius elements form one key object in the statement of the Chebotarev theorem. For $\varphi \in \mathrm{Hom}_{\mathbb{F}_q}(R, \mathbb{F})$, we set

$$\left(\frac{S/R}{\varphi}\right) := \left\{ \left[\frac{S/R}{\Phi}\right] \ :\ \Phi \text{ prolongs } \varphi \right\} .$$

In our setting, since $G_0 = G$ one can show that $\left(\frac{S/R}{\varphi}\right)$ is a conjugacy class in G. Now we are ready to state the Chebotarev theorem (see [19, Theorem A.4]):

Theorem 5.1. *Let $Z \subseteq G$ be a conjugacy class and let $\nu \geq 1$; define*

$$P_{\nu,Z} := \frac{\left|\left\{\varphi \in \operatorname{Hom}_{\mathbb{F}_q}(R, \mathbb{F}) \text{ such that } \varphi(R) = \mathbb{F}_{q^\nu} \text{ and } \left(\frac{S/R}{\varphi}\right) = Z\right\}\right|}{\left|\left\{\varphi \in \operatorname{Hom}_{\mathbb{F}_q}(R, \mathbb{F}) \text{ such that } \varphi(R) = \mathbb{F}_{q^\nu}\right\}\right|}\,.$$

Then there exists a constant δ independent of q such that, as $q \to \infty$,

$$P_{\nu,Z} \sim \frac{|Z|}{|G|} + \frac{\delta}{\sqrt{q}}\,.$$

In order to use the Chebotarev theorem for our purposes, we have to understand what does the condition $\left(\frac{S/R}{\varphi}\right) = Z$ correspond to in our setting. Suppose that C has simple tangency. Then we know by Proposition 2.10 that G is the symmetric group S_d. Notice that to every conjugacy class Z of S_d we can associate a partition π_Z of d, obtained from the cycle structure of permutations belonging to Z. On the other hand, given a line $\ell = \{y = ax + b\}$, we can consider the restriction of the equation F of C to ℓ, namely the univariate polynomial $F_\ell = F(x, ax + b)$. This polynomial defines a partition π_ℓ of d by considering its factorization over $\mathbb{F}_{q^\nu}$: the partition π_ℓ has as many 1 as the linear factors of F_ℓ, as many 2 as the quadratic factors of F_ℓ, and so on.

Lemma 5.2. *If $Z \subseteq S_d$ is a conjugacy class of permutations, then the set*

$$I_{\nu,Z} := \left\{\varphi \in \operatorname{Hom}_{\mathbb{F}_q}(R, \mathbb{F}) \text{ such that } \varphi(R) = \mathbb{F}_{q^\nu} \text{ and } \left(\frac{S/R}{\varphi}\right) = Z\right\}$$

corresponds to the set of lines in $\mathbb{P}^2_{\mathbb{F}_{q^\nu}}$ such that $\pi_\ell = \pi_Z$.

Proof. Let $\varphi \in I_{\nu,Z}$ and let $\Phi \in \operatorname{Hom}(S, \mathbb{F})$ be a homomorphism prolonging φ. Let $\ell = \{y = \bar{a}x + \bar{b}\}$ be the line in $\mathbb{P}^2_{\mathbb{F}_{q^\nu}}$ corresponding to φ. Then from the explicit description of K and L we provided at the beginning of the section, it follows that $M := \Phi(S)$ is a splitting field of the polynomial $F_\ell = F(x, \bar{a}x + \bar{b})$. By definition of the Frobenius element, we have the commutative diagram

$$\begin{tikzcd}
L = \frac{K[t_1,\ldots,t_d]}{(F(t_i,at_i+b) \text{ for } i\in\{1,\ldots,d\})} \arrow[r, "\left[\frac{S/R}{\Phi}\right]"] \arrow[d] & L = \frac{K[t_1,\ldots,t_d]}{(F(t_i,at_i+b) \text{ for } i\in\{1,\ldots,d\})} \arrow[d] \\
M = \frac{K[u_1,\ldots,u_d]}{(F(u_i,\bar{a}u_i+\bar{b}) \text{ for } i\in\{1,\ldots,d\})} \arrow[r, "\alpha\mapsto\alpha^{q^\nu}"] & M = \frac{K[u_1,\ldots,u_d]}{(F(u_i,\bar{a}u_i+\bar{b}) \text{ for } i\in\{1,\ldots,d\})}
\end{tikzcd}$$

which is just the extension to L of the diagram in Equation (8). From the commutativity of this diagram, we see that the permutation action of $\left[\frac{S/R}{\Phi}\right]$ on the classes $[t_1], \dots, [t_d]$ is the same as the action of the map $\alpha \mapsto \alpha^{q^\nu}$ on the classes $[u_1], \dots, [u_d]$. Since the $\{[u_i]\}$ are the roots of $F(x, \bar{a}x + \bar{b})$, and the latter is a polynomial with coefficients in $\mathbb{F}_{q^\nu}$, which are hence preserved by the map $\alpha \mapsto \alpha^{q^\nu}$, it follows that the structure of factors of F_ℓ over $\mathbb{F}_{q^{nu}}$ is the same as the cycle structure of $\left[\frac{S/R}{\Phi}\right]$. This concludes the proof. □

As a corollary, we obtain that the set of lines in $\mathbb{P}^2_{\mathbb{F}_{q^\nu}}$ intersecting C in exactly k points corresponds to the set

$$\bigcup_{Z \text{ has exactly } k \text{ fixed points}} I_{\nu,Z} \,.$$

The number of permutations having exactly k fixed points is given by the so-called *rencontres numbers*, see [33]. We have hence:

$$\left| \bigcup_{Z \text{ has exactly } k \text{ fixed points}} Z \right| = d! \sum_{s=k}^{d} \frac{(-1)^{k+s}}{s!} \binom{s}{k} \,.$$

Using the Chebotarev theorem we then conclude the proof of Theorem 1.4.

As the reader can see, there is nothing particularly special in considering the setting of plane curves. In fact, the concept of simple tangency (see Definition 2.8) is applicable to curves in arbitrary projective space: an absolutely irreducible curve C in $\mathbb{P}^n$ has simple tangency if there exists a hyperplane $H \subseteq \mathbb{P}^n_{\overline{\mathbb{F}}_q}$ 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. Also the concepts of Galois group of a curve and probabilities of intersections generalize similarly by considering hyperplanes instead of lines.

The generalized statement for the situation of irreducible curves is the following.

Proposition 5.3. *Let C be an absolutely irreducible algebraic curve of degree d in $\mathbb{P}^n_{\mathbb{F}_q}$, where q is a prime power. Suppose that C has simple tangency. Then for every $k \in \{0, \dots, d\}$ 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 $p_d(C) = 1/d!$.

Using Proposition 5.3, we can compute the probabilities of intersection of a given plane curve C with a random plane curve E of degree e. In fact, via the *Veronese map* we can reduce this situation to the one of Proposition 5.3. Let us start by defining the probabilities of intersection of a given curve C with a random curve E in the plane in exactly k points, for $k \in \{0, \dots, de\}$:

$$p_k^N(C,e) := \frac{\left|\left\{\text{curves } E \subseteq \mathbb{P}^2_{\mathbb{F}_{q^N}} \text{ of degree } e \,:\, |E(\mathbb{F}_{q^N}) \cap C(\mathbb{F}_{q^N})| = k\right\}\right|}{q^{\binom{e+2}{2}N} + \cdots + q^{2N} + q^N + 1},$$
$$p_k(C,e) := \lim_{N\to\infty} p_k^N(C,e) \quad \text{when the limit exists}.$$

Recall now that for every $r \in \mathbb{N}$, the Veronese map of degree e is an algebraic morphism embedding $\mathbb{P}^r$ into a larger projective space, so that hypersurfaces of degree e get mapped to hyperplane sections of the image of the map. In this sense, the Veronese map operates a sort of "linearization" of the problem. In the case of $\mathbb{P}^2$, which is the one that interests us, it is given by

$$\begin{array}{cccc} v_e\colon & \mathbb{P}^2 & \longrightarrow & \mathbb{P}^{\binom{e+2}{2}-1} \\ & (x:y:z) & \mapsto & \left(\{x^a y^b z^c\}_{a+b+c=e}\right) \end{array}.$$

The following lemma ensures that if we start from a plane curve that has simple tangency and we apply the Veronese map, we obtain a curve that has simple tangency.

Lemma 5.4. *Let C be a plane curve of degree d with simple tangency and let $e \in \mathbb{N}$. Then the image $\widetilde{C} = v_e(C)$ of C under the Veronese map of degree e has also simple tangency.*

Proof. Let ℓ_1 be a line witnessing simple tangency for C. Select lines $\ell_2, \dots, \ell_e$ in $\mathbb{P}^2$ such that each of them intersects C in d distinct points and $\ell_i \cap \ell_j \cap C$ is empty for all $i \neq j$. Define E as the zero set of the product $\ell_1 \cdots \ell_e$. The Veronese map sends E to a hyperplane section of the Veronese surface; let $\widetilde{H}$ be the corresponding hyperplane. Then, by construction, $\widetilde{H}$ witnesses simple tangency for $\widetilde{C}$. □

Since the Veronese map of degree e defines a bijection between plane curves of degree e and hyperplanes in $\mathbb{P}^{\binom{e+2}{2}-1}$, determining the probabilities $p_k(C,e)$ of intersection of a given plane absolutely irreducible curve C with a random curve of degree e in k points is equivalent to compute the corresponding probabilities of intersection of the image $\widetilde{C}$ of C under the Veronese map with hyperplanes. We sum up what we obtained in the following:

Proposition 5.5. *Let C be an absolutely irreducible algebraic curve of degree d in $\mathbb{P}^2_{\mathbb{F}_q}$, where q is a prime power. Suppose that C has simple tangency. Let $e \in \mathbb{N}$ be a natural number. Then for every $k \in \{0, \dots, de\}$ we have*

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

Acknowledgments

We thank all the anonymous referees for very useful comments and suggestions. We also thank Claus Diem who shared with us a better strategy to prove the results in Section 3, and gave us several other important suggestions to improve significantly the paper. We also thank Kaloyan Slavov for several useful suggestions and corrections to our paper. Matteo Gallet has been supported by the Austrian Science Fund (FWF): W1214-N15 Project DK9, P26607, P25652, and P31061, and is supported by the Austrian Science Fund (FWF): Erwin Schrödinger Fellowship J4253. Mehdi Makhul has been supported by the Austrian Science Fund (FWF): W1214-N15 Project DK9, and is supported by the Austrian Science Fund (FWF): P30405-N32. Josef Schicho is supported by the Austrian Science Fund (FWF): W1214-N15 Project DK9.

References

[1] T. Tao, Algebraic combinatorial geometry: the polynomial method in arithmetic combinatorics, incidence combinatorics, and number theory, EMS Surv. Math. Sci. 1 (1) (2014) 1–46, https://doi.org/10.4171/EMSS/1.

[2] L. Guth, N.H. Katz, On the Erdös distinct distances problem in the plane, Ann. Math. (2) 181 (1) (2015) 155–190, https://doi.org/10.4007/annals.2015.181.1.2.

[3] Z. Dvir, On the size of Kakeya sets in finite fields, J. Am. Math. Soc. 22 (4) (2009) 1093–1097, https://doi.org/10.1090/S0894-0347-08-00607-3.

[4] S. Saraf, M. Sudan, An improved lower bound on the size of Kakeya sets over finite fields, Anal. PDE 1 (3) (2008) 375–379, https://doi.org/10.2140/apde.2008.1.375.

[5] Z. Dvir, S. Kopparty, S. Saraf, M. Sudan, Extensions to the method of multiplicities, with applications to Kakeya sets and mergers, SIAM J. Comput. 42 (6) (2013) 2305–2328, https://doi.org/10.1137/100783704.

[6] B. Green, T. Tao, On sets defining few ordinary lines, Discrete Comput. Geom. 50 (2) (2013) 409–468, https://doi.org/10.1007/s00454-013-9518-9.

[7] J.J. Sylvester, Mathematical question 11851, Educ. Times 59 (1893) 385–394.

[8] P. Erdös, R. Bellman, H.S. Wall, J. Singer, V. Thébault, Problem 4065, Am. Math. Mon. 50 (1943) 65–66.

[9] E. Melchior, Über Vielseite der projektiven Ebene, Dtsch. Math. 5 (1941) 461–475.

[10] T. Gallai, Solution to problem 4065, Am. Math. Mon. 51 (1944) 169–171.

[11] S.A. Naimpally, R.G. Buschman, K. Koh, B.R. Toskey, P.M. Weichsel, K.E. Whipple, D. Rearick, H.F. Mattson, E.F. Assmus Jr., J.-P. Serre, Problems and solutions: advanced problems: 5350-5359, Am. Math. Mon. 73 (1) (1966) 87–89, https://doi.org/10.2307/2313941.

[12] G. Korchmáros, G.P. Nagy, N. Pace, k-nets embedded in a projective plane over a field, Combinatorica 35 (1) (2015) 63–74, https://doi.org/10.1007/s00493-011-3055-z.

[13] S. Yuzvinsky, Realization of finite Abelian groups by nets in $\mathbb{P}^2$, Compos. Math. 140 (6) (2004) 1614–1624, https://doi.org/10.1112/S0010437X04000600.

[14] J. Solymosi, M. Stojaković, Many collinear k-tuples with no $k+1$ collinear points, Discrete Comput. Geom. 50 (3) (2013) 811–820, https://doi.org/10.1007/s00454-013-9526-9.

[15] L. Bary-Soroker, M. Jarden, On the Bateman-Horn conjecture about polynomial rings, Münster J. Math. 5 (2012) 41–57.

[16] C. Diem, On the discrete logarithm problem for plane curves, J. Théor. Nr. Bordx. 24 (3) (2012) 639–667.

[17] A. Grothendieck, Revêtements étales et groupe fondamental (SGA 1): Séminaire de géométrie algébrique du Bois Marie 1960–61 (Algebraic Geometry Seminar of Bois Marie 1960-61), Documents Mathématiques (Paris) (Mathematical Documents (Paris)), vol. 3, Société Mathématique de France, Paris, 2003, Directed by A. Grothendieck, With two papers by M. Raynaud, Updated and annotated reprint of the 1971 original [Lecture Notes in Math., 224, Springer, Berlin].

[18] A.O. Bender, O. Wittenberg, A potential analogue of Schinzel's hypothesis for polynomials with coefficients in $\mathbb{F}_q[t]$, Int. Math. Res. Not. 36 (2005) 2237–2248, https://doi.org/10.1155/IMRN.2005.2237.

[19] J.C. Andrade, L. Bary-Soroker, Z. Rudnick, Shifted convolution and the Titchmarsh divisor problem over $\mathbb{F}_q[t]$, Philos. Trans. R. Soc. A 373 (2040) (2015), https://doi.org/10.1098/rsta.2014.0308.

[20] V. Kumar Murty, J. Scherk, Effective versions of the Chebotarev density theorem for function fields, C. R. Acad. Sci. Paris Sér. I Math. 319 (6) (1994) 523–528.

[21] A. Entin, Monodromy of hyperplane sections of curves and decomposition statistics over finite fields, Available at https://arxiv.org/abs/1805.05454.

[22] B. Birch, H. Swinnerton-Dyer, Note on a problem of Chowla, Acta Arith. 5 (4) (1959) 417–423, http://eudml.org/doc/206420.

[23] S. Lang, A. Weil, Number of points of varieties in finite fields, Am. J. Math. 76 (1954) 819–827, https://doi.org/10.2307/2372655.

[24] J. Rathmann, The uniform position principle for curves in characteristic p, Math. Ann. 276 (4) (1987) 565–579, https://doi.org/10.1007/BF01456986.

[25] R. Vakil, Schubert induction. Available at http://math.stanford.edu/~vakil/216blog/FOAGnov1817public.pdf.

[26] L. Rowen, Graduate Algebra: Commutative View, American Mathematical Society, Providence, RI, 2006.

[27] E. Ballico, A. Hefez, On the Galois group associated to a generically étale morphism, Commun. Algebra 14 (5) (1986) 899–909, https://doi.org/10.1080/00927878608823344.

[28] J.S. Milne, Lectures on étale cohomology (v2.21), available at www.jmilne.org/math/, 2013.

[29] J.S. Milne, Étale Cohomology, Princeton Mathematical Series, vol. 33, Princeton University Press, Princeton, N.J., 1980.

[30] R. Vakil, Schubert induction, Ann. Math. (2) 164 (2) (2006) 489–512, https://doi.org/10.4007/annals.2006.164.489.

[31] T. Stacks Project Authors, Stacks project, http://stacks.math.columbia.edu, 2017.

[32] D. Mumford, The Red Book of Varieties and Schemes, Lecture Notes in Mathematics, vol. 1358, Springer-Verlag, Berlin, 1999.

[33] J. Riordan, An Introduction to Combinatorial Analysis, Dover Publications, Inc., 2002, reprint of the 1958 original [Wiley, New York].