



Sharp Bertini Theorem for Plane Curves over Finite Fields

Shamil Asgarli

Abstract. We prove that if C is a reflexive smooth plane curve of degree d defined over a finite field \mathbb{F}_q with $d \leq q + 1$, then there is an \mathbb{F}_q -line L that intersects C transversely. We also prove the same result for non-reflexive curves of degree $p + 1$ and $2p + 1$ when $q = p^r$.

1 Introduction

A classical theorem of Bertini states that if X is a smooth quasi-projective variety in \mathbb{P}^n defined over an infinite field k , then a general hyperplane section of X is smooth. Specializing to the case when $C \subseteq \mathbb{P}^2$ is a smooth plane curve, it follows that there exists a line L (defined over k) such that L intersects C transversely, meaning that $C \cap L$ consists of d distinct geometric points where $d = \deg(C)$. But when $k = \mathbb{F}_q$ is a finite field, it is possible to have a smooth plane curve $C \subseteq \mathbb{P}^2$ such that every line L defined over \mathbb{F}_q is tangent to the curve C (see Example 2.2). Moreover, Poonen's Bertini Theorem [8, Theorem 1.2] guarantees that such smooth curves, where all the \mathbb{F}_q -lines are tangent, do exist in every sufficiently large degree (see Example 2.3). With a view toward an effective version of Poonen's theorem, one can ask the following question.

Question 1.1 *Suppose $C \subseteq \mathbb{P}^2$ is a smooth plane curve defined over \mathbb{F}_q . Let $d = \deg(C)$. What conditions on q and d will ensure that there is a line $L \subseteq \mathbb{P}^2$ defined over \mathbb{F}_q such that L meets C transversely?*

Let us call L a *good line* if L meets C transversely. We expect that if q is large with respect to d , then good lines will exist. Indeed, if $q \geq d(d - 1)$, then the dual curve C^* cannot be space-filling, i.e., $C^*(\mathbb{F}_q) \neq (\mathbb{P}^2)^*(\mathbb{F}_q)$. This is because $\deg(C^*) \leq d(d - 1) \leq q$ and a curve of degree of at most q cannot go through all the points of $(\mathbb{P}^2)^*(\mathbb{F}_q)$. Any point in $(\mathbb{P}^2)^*(\mathbb{F}_q) \setminus C^*(\mathbb{F}_q)$ represents a good line $L \subseteq \mathbb{P}^2$ defined over \mathbb{F}_q . A generalization of this observation to higher dimensions is proved by Ballico [1, Theorem 1].

In this paper, we improve the quadratic bound $q \geq d(d - 1)$ to the linear bound $q \geq d - 1$.

Received by the editors April 17, 2018.

Published electronically May 18, 2018.

AMS subject classification: 14H50, 11G20, 14N05.

Keywords: Bertini theorem, transversality, finite field.

Theorem 1.2 *If C is a smooth reflexive plane curve defined over \mathbb{F}_q with $\deg(C) \leq q + 1$, then there is an \mathbb{F}_q -line L such that L intersects C transversely.*

The theorem is sharp in a sense that the statement cannot be improved to $q \geq d - 2$. There is a counter-example when $q = d - 2$ (see Example 2.2). The “reflexive” assumption on C is same as saying that C has finitely many flex points (see Section 2). As a natural follow-up, we can ask the following question.

Question 1.3 *Does Theorem 1.2 hold when C is non-reflexive?*

In Section 3, we prove a partial result in this direction.

Theorem 1.4 *Let C be a smooth non-reflexive plane curve of degree $p + 1$ or $2p + 1$ defined over \mathbb{F}_q where $q = p^r$ with $r \geq 2$. Then there is an \mathbb{F}_q -line L such that L intersects C transversely.*

Finally, in the last section of the paper (Section 4), we focus exclusively on Frobenius non-classical curves, which are non-reflexive curves of a special kind. As we will see, Question 1.3 in this case is equivalent to a statement about collinear \mathbb{F}_q -points on the curve.

Conventions In order to avoid various pathologies, we will assume throughout the paper that the characteristic of the field is $p > 2$.

2 Reflexive Curves

In this section we review the theory of reflexive plane curves and prove Theorem 1.2. If C is a plane curve defined over a field k , we can consider the Gauss map $\varphi: C \rightarrow (\mathbb{P}^2)^*$ that associates with each smooth point p of C its tangent line. The dual curve C^* is defined to be the closure of $\varphi(C)$ inside $(\mathbb{P}^2)^*$. By looking at the Gauss map for the dual curve, we get $\varphi': C^* \rightarrow C^{**}$. In what follows, we will identify \mathbb{P}^2 and $(\mathbb{P}^2)^{**}$.

Definition 2.1 The curve C is called *reflexive* if $C = C^{**}$ and $\varphi' \circ \varphi: C \rightarrow C^{**}$ is the identity map.

A theorem of Wallace [9] asserts that C is reflexive if and only if φ is separable. As a result, all smooth plane curves in characteristic zero are reflexive. Recall that a point P of C is called a *flex point* if the tangent line at P meets the curve C at P with multiplicity at least 3. When $\text{char}(k) = p > 2$, we have the following characterization: C is reflexive if and only if C has finitely many flex points [7, Proposition 1.5].

Before we prove Theorem 1.2, here are some counter-examples of smooth curves C where all the lines defined over \mathbb{F}_q are tangent to C (so that no good line exists).

Example 2.2 Let C be a smooth plane curve with $\deg(C) = q + 2$ such that $\#C(\mathbb{F}_q) = \#\mathbb{P}^2(\mathbb{F}_q)$. Such curves exist, and have been extensively studied by Homma and Kim [6]. For such a curve C , every \mathbb{F}_q -line L intersects C at $q + 2$ points (counted with multiplicity). But $q + 1$ of these points are already accounted by the points of $L(\mathbb{F}_q) =$

$\mathbb{P}^1(\mathbb{F}_q)$. Thus, the residual intersection multiplicity results from L being tangent to C at one of the \mathbb{F}_q -points.

Example 2.3 Fix a finite field \mathbb{F}_q . Let $\{L_1, \dots, L_{q^2+q+1}\}$ be all the \mathbb{F}_q -lines in the plane. Pick distinct (geometric) points $P_i \in L_i$ for each i . The condition that C is tangent to L_i at P_i is a statement about vanishing of the first few coefficients in the Taylor expansion at these finitely many points. By applying Poonen’s Bertini theorem with Taylor conditions [8, Theorem 1.2], there exists some d_0 such that for every $d \geq d_0$, there exists a smooth plane curve $C \subseteq \mathbb{P}^2$ of degree d such that L_i is tangent to C at P_i . In particular, all \mathbb{F}_q -lines $L \subseteq \mathbb{P}^2$ are tangent to C . A closer inspection of the proof reveals that the integer d_0 is in the order of q^2 (essentially because we imposed $q^2 + q + 1$ local conditions).

We will now prove the main theorem of this paper.

Theorem 1.2 *If C is a smooth reflexive plane curve defined over \mathbb{F}_q with $\deg(C) \leq q + 1$, then there is an \mathbb{F}_q -line L such that L intersects C transversely.*

Proof Let Φ be the Frobenius map, defined on points by

$$\Phi([X:Y:Z]) = [X^q:Y^q:Z^q].$$

We will write $T_P(C)$ for the tangent line to C at a (geometric) point P . Set

$$N = \#\{P \in C(\overline{\mathbb{F}_q}) : \Phi(P) \in T_P(C)\},$$

which is finite, because C is reflexive [4]. Let $d = \deg(C)$. The following inequality is proved in [5, Theorem 8.41]:

$$(*) \quad 2 \cdot \#C(\mathbb{F}_q) + N \leq d(q + d - 1)$$

under the assumption that C has finitely many flex points and that characteristic of the field is $p > 2$. This is the step where we use the hypothesis that C is reflexive.

Assume, to the contrary, that every \mathbb{F}_q -line is tangent to the curve C at some (geometric) point. Let us divide these lines into two groups: if L is tangent to C at an \mathbb{F}_q -rational point, we will call L a *rational tangent*. Otherwise, we will call L a *special tangent*. Since every \mathbb{F}_q -line is tangent to C , and there are $q^2 + q + 1$ lines defined over \mathbb{F}_q , we get

$$\#\{\text{rational tangents}\} + \#\{\text{special tangents}\} = q^2 + q + 1$$

and

$$\#\{\text{rational tangents}\} \leq \#C(\mathbb{F}_q)$$

Now, if L is a special tangent, it is tangent to the curve C at a non- \mathbb{F}_q -point P . Then L is also tangent to C at $P, \Phi(P), \Phi^2(P), \dots, \Phi^{e-1}(P)$ where $e = [k(P):\mathbb{F}_q]$ is the degree of the point P . Since $e \geq 2$, the line L contributes at least 2 elements to N . As a result,

$$2 \cdot \#\{\text{special tangents}\} \leq N.$$

Combining all the inequalities above, we obtain that

$$\begin{aligned} q^2 + q + 1 &= \#\{\text{rational tangents}\} + \#\{\text{special tangents}\} \\ &\leq \#C(\mathbb{F}_q) + \frac{N}{2} \leq \frac{1}{2}d(q + d - 1) \quad (\text{using } (*)) \\ &\leq \frac{1}{2}(q + 1)(q + (q + 1) - 1) = \frac{1}{2}(q + 1)(2q) = q^2 + q, \end{aligned}$$

which is a contradiction. \blacksquare

When $q = p$ is a prime, every smooth curve of degree at most p is reflexive. Moreover, Pardini [7, Proposition] has shown that every smooth non-reflexive curve of degree $p + 1$ (over any field of characteristic p) is projectively equivalent to the curve given by the equation $xy^p + yz^p + zx^p = 0$. For this curve, many good lines exist. For instance, take two \mathbb{F}_p -points on the curve, and join them with a line L . Then L will intersect C transversely.

Consequently, we deduce the result for all smooth plane curves over \mathbb{F}_p where p is prime.

Corollary 2.4 *If C is a smooth plane curve defined over \mathbb{F}_p with $\deg(C) \leq p + 1$, where p is a prime, then there is an \mathbb{F}_p -line L such that L intersects C transversely.*

3 Non-reflexive Curves

In this section, we will restrict attention to non-reflexive curves and prove Theorem 1.4.

Let $C \subseteq \mathbb{P}^2$ be a smooth non-reflexive curve defined over \mathbb{F}_q with $q = p^r$ where $r \geq 2$. Pardini [7, Corollary 2.4] has shown that C is defined by an equation of the form:

$$a^p x + b^p y + c^p z = 0$$

where $a, b, c \in \mathbb{F}_q[x, y, z]$ are homogeneous polynomials of degree $t \geq 1$. In particular, $\deg(C) = tp + 1$.

We establish a Bertini-type theorem for the case $t = 1$ and $t = 2$.

Theorem 1.4 *Let C be a smooth non-reflexive plane curve of degree $p + 1$ or $2p + 1$ defined over \mathbb{F}_q where $q = p^r$ with $r \geq 2$. Then there is an \mathbb{F}_q -line L such that L intersects C transversely.*

Proof If $\deg(C) = p + 1$, then C is projectively equivalent to the curve given by the equation $xy^p + yz^p + zx^p = 0$, for which many good lines L exist (see the discussion before Corollary 2.4). For the rest of the proof, we will assume that $\deg(C) = 2p + 1$. Since C is non-reflexive, by [7, Corollary 4.3] the degree of the dual curve is

$$\deg(C^*) = \frac{d(d-1)}{p} = \frac{(2p+1)(2p)}{p} = 4p + 2.$$

For $p \geq 5$, we observe that $\deg(C^*) = 4p + 2 \leq p^2 \leq q$, so C^* cannot contain all of $(\mathbb{P}^2)^*(\mathbb{F}_q)$, and hence any point $L \in (\mathbb{P}^2)^*(\mathbb{F}_q) \setminus C^*(\mathbb{F}_q)$ will be a desired line that intersects C transversely.

When $p = 3$, the inequality $\deg(C^*) = 4p + 2 = 14 \leq p^r = q$ still holds for $r \geq 3$. The only case that requires a separate analysis is $(p, r) = (3, 2)$, which corresponds to degree $2 \cdot 3 + 1 = 7$ curve defined over $\mathbb{F}_{3^2} = \mathbb{F}_9$. The rest of the proof is devoted to studying this remaining case.

Let C be a smooth non-reflexive curve of degree 7 defined over \mathbb{F}_9 . Assume, to the contrary, that all the lines defined over \mathbb{F}_9 are tangent to C . Following the same terminology used in the proof of Theorem 1.2, we call L a *rational tangent* if L is tangent to C at some \mathbb{F}_9 -point. Otherwise, L is called a *special tangent*. Since C is non-reflexive, each tangent line L must intersect the curve at the tangency point with multiplicity at least 3 ([7, Proposition 1.5]). Then the following hold.

- (i) If L is a rational tangent, then $L \cap C$ contains at most five \mathbb{F}_9 -points.
- (ii) If L is a special tangent, then $L \cap C$ contains a conjugate pair of \mathbb{F}_{81} -points and a single \mathbb{F}_9 -point. In symbols, $L \cap C = \{Q, Q^\sigma, P\}$, where $Q \in \mathbb{P}^2(\mathbb{F}_{81}) \setminus \mathbb{P}^2(\mathbb{F}_9)$ and $P \in \mathbb{P}^2(\mathbb{F}_9)$.

Consider the following incidence correspondence of points and lines:

$$\mathcal{J} = \{ (P, L) : L \in (\mathbb{P}^2)^*(\mathbb{F}_9) \text{ and } P \in (C \cap L)(\mathbb{F}_9) \}.$$

Each $P \in C(\mathbb{F}_9)$ is contained in $q + 1 = 10$ different \mathbb{F}_9 -lines. Therefore, $\#\mathcal{J} = \#C(\mathbb{F}_9) \cdot 10$. On the other hand, using (i) and (ii) above, each special tangent L contributes 1 point, while each rational tangent L contributes at most 5 points to $\#\mathcal{J}$. Thus, $\#\mathcal{J} \leq S + 5R$ where S and R are the number of special and rational tangents, respectively. We deduce that $\#C(\mathbb{F}_9) \cdot 10 \leq S + 5R$. Since $\#C(\mathbb{F}_9) \geq R$, we get $10R \leq S + 5R$, which implies $5R \leq S$. Since $S + R = 9^2 + 9 + 1 = 91$, we have $5(91 - S) \leq S$, so that $S \geq \frac{5 \cdot 91}{6} = 75.8333 \dots$. Thus, $S \geq 76$.

Next, take any rational tangent L_0 . Every special tangent line intersects L_0 in one of its ten \mathbb{F}_9 -points. Since $\frac{S}{10} \geq \frac{76}{10} > 7$, there exists $P_0 \in L_0(\mathbb{F}_9)$ such that there are at least 8 special tangent lines that pass through P_0 . By looking at the ten \mathbb{F}_9 -lines passing through P_0 , we can estimate $\#C(\mathbb{F}_9)$ as follows. Each of the 8 special tangents will contribute at most 1 rational point, while the remaining (at most 2) rational tangents will contribute at most 5 rational points. Thus, one gets $\#C(\mathbb{F}_9) \leq 8 + 2 \cdot 5 = 18$. Consider the incidence correspondence

$$\mathcal{J} = \{ (P, L) : L \text{ is a special tangent and } P \in (C \cap L)(\mathbb{F}_9) \}.$$

By (i) above, every special tangent contains exactly one \mathbb{F}_9 -point of C , so that $\#\mathcal{J} = S$. As a result,

$$S = \#\mathcal{J} = \sum_{P \in C(\mathbb{F}_9)} \#\{\text{special tangents passing through } P\}.$$

Since

$$\frac{S}{\#C(\mathbb{F}_9)} \geq \frac{76}{18} > 4,$$

there exists a point $P \in C(\mathbb{F}_9)$ such that at least 5 special tangents pass through P . Consider the corresponding line P^* in the dual space $(\mathbb{P}^2)^*$, which consists of all lines passing through P . Let us look at the intersection of the line P^* and the dual curve C^* inside $(\mathbb{P}^2)^*$. The intersection has all the ten \mathbb{F}_9 -points of P^* , since all the \mathbb{F}_9 -lines are tangent to C . However, each of the special tangents is bitangent to C , so it

is a node in C^* , and hence will contribute 2 to the intersection. It follows that $P^* \cap C^*$ has at least $5 \cdot 2 + 5 = 15$ intersections, contradicting the fact that $\deg(C^*) = 14$. ■

Remark 3.1 As we saw above, the hardest part of the proof is the case $p = 3$. This answers a question of Felipe Voloch, who asked, in a private communication, whether or not there exists a transverse line for a degree 7 smooth non-reflexive curve defined over \mathbb{F}_9 . The small primes still persist when we try to extend Theorem 1.3 to non-reflexive curves of degree $3p + 1$. Indeed, if C is a smooth non-reflexive curve of degree $3p + 1$, then

$$\deg(C^*) = \frac{(3p+1)(3p)}{p} = 9p + 3 \leq p^2 \leq q$$

for $p \geq 11$; the usual argument shows that $(C^*)(\mathbb{F}_q) \neq (\mathbb{P}^2)^*(\mathbb{F}_q)$, implying that good lines exist for $p \geq 11$. However, the main difficulty lies with the primes $p = 3, 5, 7$.

4 Connection to Frobenius Non-classical Curves

In this section, we observe the implications of a Bertini-type theorem for a special class of non-reflexive curves, known as Frobenius non-classical curves.

Definition 4.1 Let $C \subseteq \mathbb{P}^2$ be a smooth plane curve defined over \mathbb{F}_q . Then C is called *Frobenius non-classical* if $\Phi(P) \in T_P(C)$ for every P , where $T_P(C)$ is the tangent line to C at the point P , and $\Phi: \mathbb{P}^2 \rightarrow \mathbb{P}^2$ is the q -th power Frobenius map.

We should remark that the usual definition of Frobenius non-classical is stated differently (by looking at the order sequence of C), but the definition given above is equivalent in the case of smooth plane curves [4, Proposition 1].

Example Let C be the curve defined over \mathbb{F}_{q^2} by the equation

$$x^{q+1} + y^{q+1} + z^{q+1} = 0.$$

It can be checked that C is a smooth Frobenius non-classical curve for \mathbb{F}_{q^2} .

If C is a smooth Frobenius non-classical plane curve of degree d defined over \mathbb{F}_q where $q = p^r$, then it is known that C is non-reflexive [4, Proposition 1] and $\sqrt{q} + 1 \leq d \leq \frac{q-1}{q'-1}$, where q' is the generic order of contact of the curve with a tangent line [4, Propositions 5 and 6]. In particular, $\deg(C) \leq q - 1$ always holds. So Question 1.3 is equivalent to the following.

Question 4.2 If C is a smooth Frobenius non-classical plane curve defined over \mathbb{F}_q , does there exist an \mathbb{F}_q -line L such that L intersects C transversely?

The existence of such a line L can be verified for the curve $x^{q+1} + y^{q+1} + z^{q+1} = 0$, and more generally, for the curve given by the equation

$$x^{q^{n-1}+\dots+q+1} + y^{q^{n-1}+\dots+q+1} + z^{q^{n-1}+\dots+q+1} = 0,$$

where $n \geq 2$. These curves are indeed smooth and Frobenius non-classical with respect to the field \mathbb{F}_{q^n} [4, Theorem 2].

If the Question 4.2 has an affirmative answer, then it implies that there is a line L defined over \mathbb{F}_q such that $L \cap C$ consists of $d = \text{deg}(C)$ distinct \mathbb{F}_q -rational points. Indeed, if L contains a non- \mathbb{F}_q -point Q , then we observe that $Q, \Phi(Q) \in T_Q(C)$ (since C is Frobenius non-classical) and $Q, \Phi(Q) \in L$ (as L is defined over \mathbb{F}_q), implying that $L = T_Q(C)$ is a tangent line. Thus, any good (transverse) line L intersects C at $\text{deg}(C)$ distinct \mathbb{F}_q -points. This allows us to reformulate Question 4.2 as follows.

Question 4.3 *If C is a smooth Frobenius non-classical plane curve defined over \mathbb{F}_q , then does C have $d = \text{deg}(C)$ many \mathbb{F}_q -rational points on a line?*

Question 4.3 is motivated by the fact that Frobenius non-classical curves have many \mathbb{F}_q -points. In fact, the \mathbb{F}_q -points on these curves have been used in [2, 3] to construct certain complete arcs in the plane. Moreover, the following theorem due to Hefez and Voloch [4, Theorem 1] gives the exact the number of \mathbb{F}_q -points on any smooth Frobenius non-classical plane curve.

Theorem 4.4 (Hefez–Voloch) *If $C \subseteq \mathbb{P}^2$ is a smooth Frobenius non-classical curve of degree d defined over \mathbb{F}_q , then $\#C(\mathbb{F}_q) = d(q - d + 2)$.*

We can apply Theorem 4.4 directly to get an estimate on the number of collinear points of C . Consider the incidence correspondence $\{(P, L) : L \in (\mathbb{P}^2)^*(\mathbb{F}_q) \text{ and } P \in (L \cap C)(\mathbb{F}_q)\}$. Since each \mathbb{F}_q -point P is contained in $q + 1$ lines,

$$\#C(\mathbb{F}_q)(q + 1) = \sum_{P \in C(\mathbb{F}_q)} (q + 1) = \sum_L \#(L \cap C)(\mathbb{F}_q).$$

The sum on the right runs over all $q^2 + q + 1$ lines. Thus, an \mathbb{F}_q -line on average contains

$$\frac{\#C(\mathbb{F}_q)(q + 1)}{q^2 + q + 1} = \frac{d(q - d + 2)(q + 1)}{q^2 + q + 1} > \frac{d(q - d + 2)}{q + 1} > d\left(1 - \frac{d}{q + 1}\right)$$

\mathbb{F}_q -points of C . As q gets larger, this number approaches d . This heuristic suggests that Question 4.3 may have an affirmative answer.

Acknowledgements I would like to thank my advisor Brendan Hassett for the unwavering support and constant encouragement. I am especially grateful to Felipe Voloch for suggesting to investigate the case of degree 7 non-reflexive curves over \mathbb{F}_9 , which led to Theorem 1.4. I also thank Dan Abramovich, Dori Bejleri, Herivelto Borges, Pol van Hoften, and Giovanni Inchiostro for insightful discussions and useful comments on the manuscript.

References

- [1] E. Ballico, *An effective Bertini theorem over finite fields*. Adv. Geom. 3(2003), no. 4, 361–363. <http://dx.doi.org/10.1515/advg.2003.020>
- [2] H. Borges, *On complete (N, d) -arcs derived from plane curves*. Finite Fields Appl. 15(2009), no. 1, 82–96. <http://dx.doi.org/10.1016/j.ffa.2008.08.003>
- [3] M. Giulietti, F. Pambianco, F. Torres, and E. Ughi, *On complete arcs arising from plane curves*. Des. Codes Cryptogr. 25(2002), no. 3, 237–246. <http://dx.doi.org/10.1023/A:1014979211916>

- [4] A. Hefez and J. F. Voloch, *Frobenius nonclassical curves*. Arch. Math. 54(1990), no. 3, 263–273.
<http://dx.doi.org/10.1007/BF01188523>
- [5] J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field*. Princeton Series in Applied Mathematics, Princeton University Press, Princeton, NJ, 2008.
- [6] M. Homma and S. J. Kim, *Nonsingular plane filling curves of minimum degree over a finite field and their automorphism groups: supplements to a work of Tallini*. Linear Algebra Appl. 438(2013), no. 3, 969–985. <http://dx.doi.org/10.1016/j.laa.2012.08.032>
- [7] R. Pardini, *Some remarks on plane curves over fields of finite characteristic*. Compositio Math. 60(1986), no. 1, 3–17.
- [8] B. Poonen, *Bertini theorems over finite fields*. Ann. of Math. 160(2004), no. 3, 1099–1127.
<http://dx.doi.org/10.4007/annals.2004.160.1099>
- [9] A. H. Wallace, *Tangency and duality over arbitrary fields*. Proc. London Math. Soc. 6(1956), 321–342. <http://dx.doi.org/10.1112/plms/s3-6.3.321>

Department of Mathematics, Brown University, Providence, RI 02912, USA

e-mail: shamil_asgarli@brown.edu