PLANE-FILLING CURVES OF SMALL DEGREE OVER FINITE FIELDS

SHAMIL ASGARLI AND DRAGOS GHIOCA

ABSTRACT. A plane curve C in $\mathbb{P}^2$ defined over $\mathbb{F}_q$ is called plane-filling if C contains every $\mathbb{F}_q$-point of $\mathbb{P}^2$. Homma and Kim, building on the work of Tallini, proved that the minimum degree of a smooth plane-filling curve is $q+2$. We study smooth plane-filling curves of degree $q+3$ and higher.

1. INTRODUCTION

The study of space-filling curves in $\mathbb{R}^2$ starts with the work of Peano [Pea90] in the 19th century. About 100 years later, Nick Katz [Kat99] studied space-filling curves over finite fields and raised open questions about their existence. One version of Katz's question was the following. Given a smooth algebraic variety X over a finite field $\mathbb{F}_q$, does there always exist a *smooth* curve $C \subset X$ such that $C(\mathbb{F}_q) = X(\mathbb{F}_q)$? In other words, is it possible to pass through all of the (finitely many) $\mathbb{F}_q$-points of X using a smooth curve? Gabber [Gab01] and Poonen [Poo04] independently answered this question in the affirmative.

We will consider the special case when $X = \mathbb{P}^2$. We say that a curve $C \subset \mathbb{P}^2$ is *plane-filling* if $C(\mathbb{F}_q) = \mathbb{P}^2(\mathbb{F}_q)$. Equivalently, C is a plane-filling curve C if $\#C(\mathbb{F}_q) = q^2 + q + 1$. In a natural sense, plane-filling curves are extremal. There are other classes of extremal curves with respect to the set of $\mathbb{F}_q$-points, including blocking curves [AGY23] and tangent-filling curves [AG23].

From Poonen's work [Poo04], we know that there exist smooth plane-filling curves of degree d over $\mathbb{F}_q$ whenever d is sufficiently large with respect to q. It is natural to ask for the minimum degree of a smooth plane-filling curve over $\mathbb{F}_q$. Homma and Kim [HK13] proved that the minimum degree is $q + 2$. More precisely, by building on the work of Tallini [Tal61a, Tal61b], they showed that a plane-filling curve of the form

$$(ax + by + cz)(x^q y - xy^q) + y(y^q z - yz^q) + z(z^q x - zx^q) = 0$$

is smooth if and only if the polynomial $t^3 - (ct^2 + bt + a) \in \mathbb{F}_q[t]$ has no $\mathbb{F}_q$-roots. In a sequel paper [Hom20], Homma investigated further properties of plane-filling curves of degree $q+2$. The automorphism group of these special curves was studied by Duran Cunha [DC18]. As another direction, Homma and Kim [HK23] investigated space-filling curves in $\mathbb{P}^1 \times \mathbb{P}^1$.

In light of the aforementioned results, we aim to determine if there is a "gap" in the range of possible degrees for smooth plane-filling curves. Towards this goal, we investigate the existence of smooth plane-filling curves of degree $q + 3$ and higher. The guiding question for our paper is the following.

Question 1.1. Let q be a prime power. Does there exist a smooth plane-filling curve of degree $q + 3$ defined over $\mathbb{F}_q$?

2020 *Mathematics Subject Classification.* Primary: 14G15, 14H50; Secondary: 11G20, 14G05.
Key words and phrases. Plane curve, space-filling curve, smooth curve, finite field.

5 Feb 2024 23:34:49 PST
230706-Asgarli Version 2 - Submitted to Rocky Mountain J. Math.

More generally, one can ask about the existence of degree $q+r+1$ smooth plane-filling curves (see Theorem 1.8 for context). A positive answer to these questions would provide an effective version of Poonen's theorem in the particular case of plane-filling curves.

The three binomials $x^q y - xy^q, y^q z - yz^q$, and $z^q x - zx^q$ generate the ideal of polynomials defining plane-filling curves; see [HK13, Proposition 2.1] for proof of this assertion. Thus, any plane-filling curve of degree $q+3$ must necessarily be defined by

$$Q_1(x,y,z)\cdot(x^q y - xy^q) + Q_2(x,y,z)\cdot(y^q z - yz^q) + Q_3(x,y,z)\cdot(z^q x - zx^q) = 0$$

for some homogeneous quadratic polynomials $Q_1, Q_2, Q_3 \in \mathbb{F}_q[x,y,z]$. The difficulty is finding suitable Q_1, Q_2, Q_3 for which the corresponding curve is smooth.

Our first result gives a necessary and sufficient condition for the plane-filling curve C_k to be smooth at all the $\mathbb{F}_q$-points.

Theorem 1.2. *For each $k \in \mathbb{F}_q$, consider the plane-filling curve C_k defined by*

$$x^2(x^q y - xy^q) + y^2(y^q z - yz^q) + (z^2 + kx^2)(z^q x - zx^q) = 0. \tag{1}$$

Then C_k is smooth at every $\mathbb{F}_q$-point of $\mathbb{P}^2$ if and only if the polynomial $x^7 + kx^3 - 1$ has no zeros in $\mathbb{F}_q$.

In fact, we will prove a more general theorem (namely, Theorem 1.8) which will immediately imply Theorem 1.2 as a special case.

To ensure that Theorem 1.2 is not vacuous, we need to show that there exists some $k \in \mathbb{F}_q$ such that $x^7 + kx^3 - 1$ has no zeros in $\mathbb{F}_q$.

Proposition 1.3. *There exists a value $k \in \mathbb{F}_q$ such that $x^7 + kx^3 - 1 \in \mathbb{F}_q[x]$ has no zeros in $\mathbb{F}_q$.*

Proof. When $x = 0$, there is no $k \in \mathbb{F}_q$ such that $x^7 + kx^3 - 1 = 0$. For each $x \in \mathbb{F}_q^*$, there is a *unique* value of $k \in \mathbb{F}_q$ such that $x^7 + kx^3 - 1 = 0$. Thus, there are at most $q-1$ values of $k \in \mathbb{F}_q$ such that the polynomial $x^7 + kx^3 - 1$ has a zero in $\mathbb{F}_q$. □

The next result improves Proposition 1.3.

Theorem 1.4. *There exist at least $\frac{q}{6} - 1 - \frac{28}{3}\sqrt{q}$ many values of $k \in \mathbb{F}_q$ such that $x^7 + kx^3 - 1 \in \mathbb{F}_q[x]$ has no zeros in $\mathbb{F}_q$.*

Note that Theorem 1.2 and Proposition 1.3 together yields that for each odd q, there exists at least one value $k \in \mathbb{F}_q$ for which the corresponding curve C_k has no singular $\mathbb{F}_q$-points. Note that smoothness at $\mathbb{F}_q$-points is not enough, in general, to guarantee that the curve is smooth (that is, smooth at all of its $\overline{\mathbb{F}_q}$-points). For instance, let L_1 be an $\mathbb{F}_{q^3}$-line with no $\mathbb{F}_q$-points; let L_2 and L_3 be the $\mathrm{Gal}(\mathbb{F}_{q^3}/\mathbb{F}_q)$-conjugates of L_1. Then the cubic curve $C = L_1 \cup L_2 \cup L_3$ is defined over $\mathbb{F}_q$, and yet has no $\mathbb{F}_q$-points. So, C is vacuously smooth at all of its $\mathbb{F}_q$-points but is singular at three $\mathbb{F}_{q^3}$-points. For a more involved example of this phenomenon, see Example 4.1.

However, we expect that the curves in Theorem 1.2 are smooth if and only if they are smooth at all their $\mathbb{F}_q$-points. Our main conjecture below restates this prediction.

Conjecture 1.5. *Suppose q is odd. The plane-filling curve C_k defined by (1) is smooth if and only if the polynomial $x^7 + kx^3 - 1$ has no zeros in $\mathbb{F}_q$.*

We have verified Conjecture 1.5 using Macaulay2 [GS] for all odd prime powers $q < 200$. When $q = 2^m$ is even, the curve C_k defined by (1) turns out to be singular (for *every* $k \in \mathbb{F}_q$). As

5 Feb 2024 23:34:49 PST
230706-Asgarli Version 2 - Submitted to Rocky Mountain J. Math.

a replacement, we consider another curve D_k in this case:

$$x^2(x^qy - xy^q) + y^2(y^qz - yz^q) + (z^2 + kxy)(z^qx - zx^q) = 0. \quad (2)$$

We make a similar conjecture regarding the smoothness of the curves D_k.

Conjecture 1.6. *Suppose q is even. The plane-filling curve D_k defined by (2) is smooth if and only if the polynomial $x^7 + kx^5 + 1$ has no zeros in $\mathbb{F}_q$.*

The polynomial $x^7 + kx^5 + 1$ featured above is prominent because one can show, similar to Theorem 1.2, that a plane-filling curve D_k is smooth at all of its $\mathbb{F}_q$-points (when q is even) if and only if $x^7 + kx^5 + 1$ has no $\mathbb{F}_q$-roots. We have verified Conjecture 1.6 using Macaulay2 [GS] for $q = 2^m$ when $1 \leq m \leq 9$.

We prove the following as partial progress towards Conjecture 1.5.

Theorem 1.7. *Suppose q is odd. There exists a suitable choice of $k \in \mathbb{F}_q$ such that the plane-filling curve C_k defined by (1) is smooth at all $\mathbb{F}_{q^2}$-points.*

A similar argument as the one employed in Theorem 1.7 yields an analogous result when q is even, and the curve C_k is replaced by D_k.

To prove Theorem 1.7, we will prove that any plane-filling curve of degree $q+3$ which is smooth at $\mathbb{F}_q$-points and has no $\mathbb{F}_q$-linear component must be smooth at each of its $\mathbb{F}_{q^2}$-points.

We also investigate plane-filling curves of degree $q + r + 1$ where $r \geq 2$ is arbitrary.

Theorem 1.8. *For each $k \in \mathbb{F}_q$, consider the plane-filling curve $C_{k,r}$ defined by*

$$x^r(x^qy - xy^q) + y^r(y^qz - yz^q) + (z^r + kx^r)(z^qx - zx^q) = 0.$$

Then $C_{k,r}$ is smooth at every $\mathbb{F}_q$-point of $\mathbb{P}^2$ if and only if the polynomial $x^{r^2+r+1} + kx^{r+1} - 1 = 0$ has no zeros in $\mathbb{F}_q$.

Structure of the paper. In Section 2, we prove Theorem 1.4. We devote Section 3 to Theorem 1.7, and Section 4 to Theorem 1.8.

2. Proof of Theorem 1.4

We begin this section by noting that Theorem 1.2 is a special case of Theorem 1.8 which will be proven in Section 4. Our Theorem 1.2 provides a criterion that tests whether the plane-filling curve C_k defined by (1) is smooth at every $\mathbb{F}_q$-point.

The following technical result will be employed in our proof of Theorem 1.4.

Lemma 2.1. *The polynomial $x^3y^3(x+y)(x^2+y^2) + (x^2+xy+y^2)$ is irreducible in $\overline{\mathbb{F}_q}[x,y]$.*

Proof. The proof employs a technique seen in Eisenstein's criterion. First, suppose $p = \mathrm{char}(\mathbb{F}_q) \neq 3$. Assume, to the contrary, that $f(x,y) := x^3y^3(x+y)(x^2+y^2) + (x^2+xy+y^2)$ is reducible over the algebraic closure $\overline{\mathbb{F}_q}$. Write $f(x,y) = g(x,y) \cdot h(x,y)$, and express

$$g(x,y) = g_m(x,y) + g_{m+1}(x,y) + \cdots + g_s(x,y)$$
$$h(x,y) = h_n(x,y) + h_{n+1}(x,y) + \cdots + h_t(x,y)$$

5 Feb 2024 23:34:49 PST
230706-Asgarli Version 2 - Submitted to Rocky Mountain J. Math.

where $g_i(x,y)$ and $h_j(x,y)$ are homogeneous of degree i and j, respectively, for $m \leq i \leq s$ and $n \leq j \leq t$. From $f(x,y) = g(x,y) \cdot h(x,y)$, we see that

$$\begin{cases} g_m h_n = x^2 + xy + y^2 \\ g_s h_t = x^3y^3(x+y)(x^2+y^2) \\ \sum_{i+j=k} h_i g_j = 0 \text{ for } 2 < k < 9 \end{cases}$$

Since the characteristic $p \neq 3$, the polynomial $x^2 + xy + y^2$ factors into distinct linear factors in $\overline{\mathbb{F}_q}[x,y]$. Let $x + \lambda y$ be one of those linear factors with $\lambda \in \overline{\mathbb{F}_q}$. Then $x^2 + xy + y^2$ is divisible by $x + \lambda y$ but not by $(x+\lambda y)^2$. Thus, exactly one of g_m or h_n is divisible by $x + \lambda y$. Without loss of generality, assume $x + \lambda y$ divides g_m, and not h_n. Then using $\sum_{i+j=k} h_i g_j = 0$ for $2 < k < 9$, we inductively see that $x + \lambda y$ divides g_j for each $m \leq j \leq s$. In particular, $x + \lambda y$ divides $g_s h_t$. This is a contradiction because $x + \lambda y$ does not divide $x^3y^3(x+y)(x^2+y^2)$. Indeed, $x^2 + xy + y^2$ and $x^3y^3(x+y)(x^2+y^2)$ are relatively prime.

When $p = 3$, a similar argument works from the other end of the polynomial: the leading term $x^3y^3(x+y)(x^2+y^2)$ is divisible by $x+y$ but not by $(x+y)^2$. We deduce that $f(x,y)$ is irreducible over $\overline{\mathbb{F}_q}$ for every prime power q. □

Proof of Theorem 1.4. Our goal is to give a lower bound on the number of $k \in \mathbb{F}_q$ such that the polynomial $x^7 + kx^3 - 1$ has no roots in $\mathbb{F}_q$. As x ranges in $\mathbb{F}_q^*$ (note that there is no $k \in \mathbb{F}_q$ for which $x = 0$ would be a root of $x^7 + kx^3 - 1$), the number of "bad" choices of k are parametrized by $\frac{1-x^7}{x^3}$. We will show that there are many choices of x and y such that $\frac{1-x^7}{x^3}$ and $\frac{1-y^7}{y^3}$ give rise to the same value of k. Setting these expressions equal to each other, we obtain the following.

$$\frac{1-x^7}{x^3} = \frac{1-y^7}{y^3} \quad \Rightarrow \quad x^7y^3 - y^3 = y^7x^3 - x^3$$

After rearranging and dividing both sides by $x - y$, we obtain an affine curve $\mathcal{C} \subset \mathbb{A}^2$ defined by

$$x^3y^3(x+y)(x^2+y^2) + x^2 + xy + y^2 = 0,$$

for $x, y \in \mathbb{F}_q^*$ *and* $x \neq y$. Let G be a graph whose vertex set is $\mathbb{F}_q^*$, and there is an edge between x and y if (x,y) lies on the affine curve $\mathcal{C}$. We consider undirected edges, so the pairs (x,y) and (y,x) correspond to the same edge.

Claim 1. The number of edges of G is at least $\frac{q}{2} - 6 - 28\sqrt{q}$.

Let $\tilde{\mathcal{C}} \subset \mathbb{P}^2$ be the projectivization of $\mathcal{C}$. By Lemma 2.1, the curve $\tilde{\mathcal{C}}$ is geometrically irreducible. By Hasse-Weil inequality for geometrically irreducible curves [AP96, Corollary 2.5], $\#\tilde{\mathcal{C}}(\mathbb{F}_q) \geq q + 1 - 56\sqrt{q}$. Since the line at infinity $z = 0$ can contain at most 5 distinct $\mathbb{F}_q$-points, we have $\#C(\mathbb{F}_q) \geq q - 4 - 56\sqrt{q}$; furthermore, we exclude the points for which $xy = 0$ and there is only one such point $[0:0:1] \in \tilde{\mathcal{C}}$. We also need to rule out the points on the diagonal, namely $x = y$; in this case, $4x^9 + 3x^2 = 0$ which contributes at most 7 additional points with $x \neq 0$. Thus, the number of $(x,y) \in C(\mathbb{F}_q)$ with $x \neq y$ is at least $q - 12 - 56\sqrt{q}$. The claim follows since the edges are undirected.

Claim 2. Every connected component of G is a complete graph K_n where $n \in \{1,2,3,4,5,6\}$.

If (x,y) and (x,z) are both edges of G, then $\frac{1-x^7}{x^3} = \frac{1-y^7}{y^3}$ and $\frac{1-x^7}{x^3} = \frac{1-z^7}{z^3}$. Consequently, $\frac{1-y^7}{y^3} = \frac{1-z^7}{z^3}$ and (y,z) lies on the curve $\mathcal{C}$, so (y,z) is an edge in G too. Thus, each connected component of G is a clique. In addition, from the equation of $\mathcal{C}$, the degree of each vertex $x \in G$ is at most 6.

5 Feb 2024 23:34:49 PST
230706-Asgarli Version 2 - Submitted to Rocky Mountain J. Math.

For each $1 \le i \le 6$, let m_i denote the number of cliques of size i in G. Counting the number of edges in G leads to the following equality.

$$\#E(G) = \sum_{i=1}^{6} \frac{i(i-1)}{2} \cdot m_i.$$

Each clique of size i in G increases the number of "good" values of k by an additive factor of $i-1$ because each clique corresponds to one "bad" value of k, i.e., a value $k \in \mathbb{F}_q$ for which the equation $x^7 + kx^3 - 1 = 0$ is solvable for some $x \in \mathbb{F}_q$. More precisely,

$$\begin{aligned}
&\#\{k \in \mathbb{F}_q \mid x^7 + kx^3 - 1 \text{ has no zeros in } \mathbb{F}_q\} \\
&= q - \sum_{i=1}^{6} m_i \\
&= 1 + (q-1) - \sum_{i=1}^{6} m_i \\
&= 1 + \sum_{i=1}^{6} i \cdot m_i - \sum_{i=1}^{6} m_i \\
&= 1 + \sum_{i=1}^{6} (i-1) \cdot m_i \\
&\ge 1 + \frac{1}{3} \sum_{i=1}^{6} \frac{(i-1)i}{2} \cdot m_i \ge 1 + \frac{1}{3}\#E(G) \ge 1 + \frac{1}{3}\left(\frac{q}{2} - 6 - 28\sqrt{q}\right)
\end{aligned}$$

as desired. □

3. Smoothness at $\mathbb{F}_{q^2}$-points

In this section, we show that a plane-filling curve C of degree $q+3$ has the following special property: being smooth at $\mathbb{F}_q$-points implies being smooth at $\mathbb{F}_{q^2}$-points under a mild condition.

Proposition 3.1. *Suppose C is a plane-filling curve of degree $q+3$ such that*

(i) The curve C is smooth at all the $\mathbb{F}_q$-points.
(ii) The curve C has no $\mathbb{F}_q$-linear component.

Then C is smooth at each $\mathbb{F}_{q^2}$-point.

Proof. Assume, to the contrary, that C is singular at some $\mathbb{F}_{q^2}$-point Q. Then Q is not an $\mathbb{F}_q$-point due to the hypothesis (i). Let Q^σ denote the Galois conjugate of Q under the Frobenius automorphism. More explicitly, if $Q = [x : y : z] \in \mathbb{P}^2$, then $Q^\sigma = [x^q : y^q : z^q]$. Note that Q^σ is also contained in C (since C is defined over $\mathbb{F}_q$). Moreover, Q^σ is also a singular point of C.

Consider the line L joining Q and Q^σ, which is an $\mathbb{F}_q$-line by Galois theory. By hypothesis (ii), the line L must intersect C in exactly $q+3$ points (counted with multiplicity). However, L already contains $q+1$ distinct $\mathbb{F}_q$-points of C (because C is plane-filling), and passes through the two singular points Q and Q^σ, each contributing intersection multiplicity at least 2. Thus, the total intersection multiplicity between L and C is at least $(q+1)+2+2 = q+5$, a contradiction. □

5 Feb 2024 23:34:49 PST
230706-Asgarli Version 2 - Submitted to Rocky Mountain J. Math.

Remark 3.2. We can weaken the hypothesis of Proposition 3.1 by replacing the condition $\deg(C) = q+3$ with $\deg(C) \leq q+4$. Indeed, the same proof works verbatim.

Next, we show that the plane-filling curves C_k of degree $q+3$ considered in equation (1) indeed satisfy condition (ii) when q is odd.

Proposition 3.3. *The curve C_k defined by (1) has no $\mathbb{F}_q$-linear components when q is odd.*

Proof. There are three types of $\mathbb{F}_q$-lines in $\mathbb{P}^2$.

Type I. The line L is given by $z = 0$.

The curve C_k meets the line $\{z = 0\}$ at finitely many points determined by $x^2(x^q y - xy^q) = 0$. In particular, $\{z = 0\}$ is not a component of C.

Type II. The line L is given by $x = az$ for some $a \in \mathbb{F}_q$.

The curve C_k meets the line $\{x = az\}$ at finitely many points determined by

$$(az)^2((az)^q y - (az)y^q) + y^2(y^q z - yz^q) + (z^2 + k(az)^2)(z^q(az) - z(az)^q) = 0.$$

After simplifying and using $a^q = a$, the last term cancels and we obtain:

$$a^3 z^{q+2} y - a^3 z^3 y^q + y^{q+2} z - y^3 z^q = 0$$

In particular, $\{x = az\}$ is not a component of C.

Type III. The line L is given by $y = ax + bz$ for some $a, b \in \mathbb{F}_q$.

If $a = 0$ or $b = 0$, then $y = bz$ or $y = ax$, and the analysis is very similar to the previous case. We will assume that $a \neq 0$ and $b \neq 0$. We substitute $y = ax + bz$ into the equation (1) and collect terms to obtain:

$$\begin{aligned}&(b + a^3 - k)x^{q+2}z + (2a^2 b)x^{q+1}z^2 + (b^2 a - 1)x^q z^3 + \\ &(-b - a^3 + k)x^3 z^q + (-2ab)x^2 z^{q+1} + (-ab^2 + 1)xz^{q+2} = 0\end{aligned}$$

The coefficient of $x^{q+1}z^2$ is $2a^2 b$, which is nonzero since q is odd (so $2 \neq 0$), $a \neq 0$ and $b \neq 0$. Thus, L is not a component of C_k. ☐

We are now in a position to prove Theorem 1.7 on the existence of $k \in \mathbb{F}_q$ such that the plane-filling curve C_k is smooth at all its $\mathbb{F}_{q^2}$-points.

Proof of Theorem 1.7. The result follows immediately from Proposition 1.3, Proposition 3.1, and Proposition 3.3. ☐

4. Higher degree plane-filling curves

We begin by establishing Theorem 1.8, which provides a necessary and sufficient condition for the plane-filling curve $C_{k,r}$ to be smooth at all the $\mathbb{F}_q$-points.

Proof of Theorem 1.8. We consider the curve $C_{k,r}$ given by the equation:

$$x^r \cdot (x^q y - xy^q) + y^r \cdot (y^q z - yz^q) + (z^r + kx^r) \cdot (z^q x - zx^q) = 0. \tag{3}$$

We analyze the singular locus of $C_{k,r}$ and get the equations:

$$rx^{r-1} \cdot (x^q y - xy^q) + x^r \cdot (-y^q) + krx^{r-1} \cdot (z^q x - zx^q) + (z^r + kx^r) \cdot z^q = 0 \tag{4}$$

$$x^r \cdot x^q + ry^{r-1} \cdot (y^q z - yz^q) + y^r \cdot (-z^q) = 0 \tag{5}$$

$$y^r \cdot y^q + rz^{r-1} \cdot (z^q x - zx^q) + (z^r + kx^r) \cdot (-x^q) = 0. \tag{6}$$

We next analyze the possibility that we have a singular point when $xyz = 0$.

If $x = 0$, then equation (4) yields $z = 0$, which is then employed in (6) to derive $y = 0$, contradiction.

If $y = 0$, then equation (5) yields $x = 0$ and then equation (4) yields $z = 0$, contradiction.

If $z = 0$, then equation (5) yields $x = 0$ and then equation (6) yields $y = 0$, contradiction.

So, the only possible singular points are of the form $[x : 1 : z]$.

We search for possible singular points $[x : 1 : z] \in \mathbb{P}^2(\mathbb{F}_q)$. Then equations (4), (5) and (6) read:

$$-x^r + z^{r+1} + kx^r z = 0 \tag{7}$$

$$x^{r+1} - z = 0 \tag{8}$$

$$1 - z^r x - kx^{r+1} = 0. \tag{9}$$

Substituting $z = x^{r+1}$ from equation (8) into equations (7) and (9), we obtain

$$-x^r + x^{r^2+2r+1} + kx^{2r+1} = 0 \text{ and } 1 - x^{r^2+r+1} - kx^{r+1} = 0,$$

that is, there exists a singular $\mathbb{F}_q$-rational point on $C_{k,r}$ if and only if there exists $x \in \mathbb{F}_q^*$ such that

$$x^{r^2+r+1} + kx^{r+1} - 1 = 0, \tag{10}$$

as desired.

We end the proof by mentioning that some care is needed to treat the case when the characteristic p of the field divides the degree of the curve (i.e., p divides $r+1$ in this setting). Indeed, the singular locus of any projective curve $\{f = 0\}$ is defined by $\{f = \frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = \frac{\partial f}{\partial z} = 0\}$. When p divides $\deg(f)$, it is *not* enough to consider the points in the locus $\{\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = \frac{\partial f}{\partial z} = 0\}$. Fortunately, in our case, the $\mathbb{F}_q$-point $[x : 1 : z]$ is automatically on the curve $C_{k,r}$ because $C_{k,r}$ is plane-filling. □

It may be natural to make a prediction identical to Conjecture 1.5 for higher-degree curves. However, some care is needed, as the following two examples show. We found these examples using Macaulay2 [GS].

Example 4.1. Let $r = 5$, $q = 11$, and $k = 9$. The plane-filling curve $C_{9,5}$ over $\mathbb{F}_{11}$ is smooth at all the $\mathbb{F}_{11}$-points because the polynomial $x^{31} + 9x^6 - 1$ is an irreducible polynomial over $\mathbb{F}_{11}$. However, $C_{9,5}$ is singular at two Galois-conjugate $\mathbb{F}_{11^2}$-points.

In the previous example, the curve $C_{9,5}$ is irreducible over $\mathbb{F}_{11}$. Thus, $C_{9,5}$ satisfies the two conditions of Theorem 3.1 and yet it is singular at two $\mathbb{F}_{11^2}$-points. Since $\deg(C_{9,5}) = q + 6$, we see that Remark 3.2 is close to being sharp.

Example 4.2. Let $r = 7$, $q = 5$. In this case, the plane-filling curve $C_{k,7}$ defined over $\mathbb{F}_5$ is singular for each $k \in \mathbb{F}_5$. Indeed, the associated polynomial $x^{57}+kx^8-1$ has an $\mathbb{F}_5$-root for $k \in \{0, 2, 3, 4\}$. For these values of k, the curve $C_{k,r}$ is singular at an $\mathbb{F}_5$-point. For $k = 1$, the curve $C_{1,7}$ is singular at four points, namely, two pairs of Galois-conjugate $\mathbb{F}_{5^2}$-points.

The two examples above illustrate that Conjecture 1.5 needs to be modified for plane-filling curves of degree $q+r+1$ when r is arbitrary. We propose two related conjectures on the smoothness of the curve $C_{k,r}$ from Theorem 1.8. Recall that $C_{k,r} \subset \mathbb{P}^2$ is defined by

$$x^r(x^q y - xy^q) + y^r(y^q z - yz^q) + (z^r + kx^r)(z^q x - zx^q) = 0$$

where $r \geq 2$ is a positive integer and $k \in \mathbb{F}_q$.

Conjecture 4.3. *Let $r \geq 2$. There exists an integer $m := m(r)$ with the following property. For all finite fields $\mathbb{F}_q$ with cardinality $q > m$ and characteristic not dividing r, there exists some $k \in \mathbb{F}_q$ such that the curve $C_{k,r}$ is smooth.*

Using Macaulay2 [GS], we enumerated through values of r in the range $[2, 17]$ and q in the range $[2, 100]$ with $\gcd(r, q) = 1$. We found only the following pairs (r, q) for which $C_{k,r}$ is singular for *every* $k \in \mathbb{F}_q$: $(r, q) = (7, 5)$, $(13, 3)$, $(16, 9)$, and $(17, 7)$.

Conjecture 4.4. *Let $r \geq 2$. There exists an integer $s := s(r)$ with the following property. For all finite fields $\mathbb{F}_q$ with characteristic not dividing r, and for all $k \in \mathbb{F}_q$, if $C_{k,r}$ is smooth at all of its $\mathbb{F}_{q^s}$-points, then $C_{k,r}$ is smooth.*

As a motivation for Conjecture 4.4, we mention the following general fact about pencils of plane curves. The family of plane curves C_k forms a *pencil* of plane curves since the parameter $k \in \mathbb{F}_q$ appears linearly in the defining equation. If $\mathcal{L}$ is a pencil of plane curves in $\mathbb{P}^2$ parametrized by $\mathbb{A}^1$, then $\mathbb{F}_q$-members of $\mathcal{L}$ are defined by $f(x, y, z) + kg(x, y, z) = 0$ where $k \in \mathbb{F}_q$ is arbitrary. We will use X_k to denote this plane curve in the following proposition.

Proposition 4.5. *Let $\mathcal{L}$ be a pencil of plane curves $\{X_k\}_{k \in \mathbb{F}_q}$ of degree d defined over a finite field $\mathbb{F}_q$. Suppose that for every $s \geq 1$, there exists some $k \in \mathbb{F}_q$ such that X_k is smooth at all of its $\mathbb{F}_{q^s}$-points. Then there exists some $\ell \in \mathbb{F}_q$ such that X_ℓ is smooth.*

Proof. Assume, to the contrary, that X_k is singular for each $k \in \mathbb{F}_q$. For each $k \in \mathbb{F}_q$, let $n_k \in \mathbb{N}$ such that the curve X_k is singular at some $\mathbb{F}_{q^{n_k}}$-point. Let $N := \prod_{k \in \mathbb{F}_q} n_k$. By construction, no X_k is smooth at all of its $\mathbb{F}_{q^N}$-points, contradicting the hypothesis. □

Proposition 4.5 asserts that to find a smooth member of any pencil $\mathcal{L}$ defined over $\mathbb{F}_q$, it is sufficient to find a member which is smooth at all points of an (arbitrary) finite degree. Conjecture 4.4 strengthens the conclusion by predicting that for a pencil of plane-filling curves, one finds a smooth member by only checking smoothness at all points of *fixed* finite degree.

Acknowledgements

The authors are grateful to the anonymous referee for the valuable comments.

References

[AG23] Shamil Asgarli and Dragos Ghioca, *Tangent-filling plane curves over finite fields*, Bull. Aust. Math. Soc. (2023), published online on May 2, 2023, available at https://arxiv.org/abs/2302.13420.

[AGY23] Shamil Asgarli, Dragos Ghioca, and Chi Hoi Yip, *Plane curves giving rise to blocking sets over finite fields*, Des. Codes Cryptogr. **91** (2023), no. 11, 3643–3669.

[AP96] Yves Aubry and Marc Perret, *A Weil theorem for singular curves*, Arithmetic, geometry and coding theory (Luminy, 1993), 1996, pp. 1–7.

[DC18] Gregory Duran Cunha, *Curves containing all points of a finite projective Galois plane*, J. Pure Appl. Algebra **222** (2018), no. 10, 2964–2974.

[Gab01] O. Gabber, *On space filling curves and Albanese varieties*, Geom. Funct. Anal. **11** (2001), no. 6, 1192–1200.

[Hom20] Masaaki Homma, *Fragments of plane filling curves of degree $q + 2$ over the finite field of q elements, and of affine-plane filling curves of degree $q + 1$*, Linear Algebra Appl. **589** (2020), 9–27.

[HK13] Masaaki Homma and Seon Jeong 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.

[HK23] ———, *Filling curves for $\mathbb{P}^1 \times \mathbb{P}^1$*, Comm. Algebra **51** (2023), no. 6, 2680–2687.

[Kat99] Nicholas M. Katz, *Space filling curves over finite fields*, Math. Res. Lett. **6** (1999), no. 5-6, 613–624.

5 Feb 2024 23:34:49 PST
230706-Asgarli Version 2 - Submitted to Rocky Mountain J. Math.

[GS] Daniel R. Grayson and Michael E. Stillman, *Macaulay2, a software system for research in algebraic geometry*. http://www.math.uiuc.edu/Macaulay2/.

[Pea90] Giuseppe Peano, *Sur une courbe, qui remplit toute une aire plane*, Math. Ann. **36** (1890), no. 1, 157–160.

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

[Tal61a] Giuseppe Tallini, *Le ipersuperficie irriducibili d'ordine minimo che invadono uno spazio di Galois*, Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Nat. (8) **30** (1961), 706–712.

[Tal61b] ______, *Sulle ipersuperficie irriducibili d'ordine minimo che contengono tutti i punti di uno spazio di Galois* $S_{r,q}$, Rend. Mat. e Appl. (5) **20** (1961), 431–479.

Department of Mathematics and Computer Science, Santa Clara University, 500 El Camino Real, USA 95053

Email address: sasgarli@scu.edu

Department of Mathematics, University of British Columbia, 1984 Mathematics Road, Canada V6T 1Z2

Email address: dghioca@math.ubc.ca

5 Feb 2024 23:34:49 PST
230706-Asgarli Version 2 - Submitted to Rocky Mountain J. Math.