The complement of Fermat curves in the plane

Seth Dutter, Melissa Haire and Ariel Setniker
The complement of Fermat curves in the plane

Seth Dutter, Melissa Haire and Ariel Setniker

(Communicated by Bjorn Poonen)

In this paper we will examine the affine algebraic curves defined on the complement of Fermat curves of degree five or higher in the affine plane. In particular we will bound the height of integral points over an affine curve outside of an exceptional set.

1. Introduction

Let $C$ be a complete algebraic curve of genus $g$ over an algebraically closed field $k$ of characteristic 0, and $U \subset C$ be a nonempty open subset of $C$. The goal of this paper is to analyze morphisms

$$
\phi : U \to \mathbb{P}^2_k \setminus V(z(x^n + y^n - z^n)),
$$

where $V(z(x^n + y^n - z^n))$ is the zero set of the polynomial $z(x^n + y^n - z^n)$ and $[x : y : z]$ are the projective coordinates in $\mathbb{P}^2_k$. Alternatively we can think of such functions as $U$-points on the variety $\mathbb{P}^2_k \setminus V(z(x^n + y^n - z^n))$. We will call projective curves defined by equations of the form $x^n + y^n - z^n = 0$ Fermat curves of degree $n$.

A conjecture of Vojta [1987, Conjecture 3.4.3 and Proposition 4.1.2] implies that the set of integral points on the complement of a degree 4 divisor with normal crossings in $\mathbb{P}^2_k$ is not Zariski dense. Here instead of studying points over $\mathbb{Z}$ we will be looking at the split function field case of Vojta’s conjecture and studying points over $U$. Corvaja and Zannier [2008] have proven the particular case when the divisor consists of two lines and a conic section meeting only with normal crossings. This was one of the remaining borderline cases, the other two being the union of a cubic and a line, and a quartic.

The divisor defined by $(z(x^n + y^n - z^n))$ has degree $n + 1$ and normal crossings, so we should expect that the set of $U$-points is not Zariski dense for $n \geq 3$. The techniques employed in this paper are able to establish results for $n \geq 5$. A counterexample is given for the case $n = 2$, leaving the cases $n = 3$ and $n = 4$ unsettled. In particular we will establish the following theorem:


Keywords: Mason’s theorem, function field, Fermat curve.
Theorem 1.1. Let $C$ be a smooth complete algebraic curve of genus $g$ over an algebraically closed field $k$ of characteristic 0. Let $U \subset C$ be a nonempty open subset and $m = \#(C \setminus U)$. For $n \geq 5$ and any morphism $\phi : U \to \mathbb{P}_k^2 \setminus V(z(x^n + y^n - z^n))$ either
\[
h(\phi^*(x/z), \phi^*(y/z), 1) \leq \frac{3(m + \max\{2g - 2, 0\})}{n - 4},
\]
or $\text{Im}(\phi) \subset V((x^n + y^n)(x^n - z^n)(y^n - z^n))$.

Here $h$ is the height function over the function field of the curve $C$ and $\phi^* : \mathcal{O}_{\mathbb{P}_k^2 \setminus V(z(x^n + y^n - z^n))} \to \mathcal{O}_C(U)$ is the morphism of regular functions associated to $\phi$. Note that the complement of the line defined by $z = 0$ can be identified with $\mathbb{A}_k^2$. Therefore we can also interpret our main result as a height bound for $U$-points on the complement of an affine Fermat curve in $\mathbb{A}_k^2$.

In order to establish this bound we will translate the problem into one of solving a diophantine equation over $\mathcal{O}_C(U)$. Indeed, let $\phi : U \to \mathbb{P}_k^2 \setminus V(z(x^n + y^n - z^n))$; then $\phi^*((x/z)^n + (y/z)^n - 1) \in \mathcal{O}_C(U)^*$ is a unit. For convenience let $X = \phi^*(x/z)$, $Y = \phi^*(y/z)$, which after substituting gives us the equation
\[
X^n + Y^n - 1 = u
\]
for some $u \in \mathcal{O}_C(U)^*$. Therefore we can restate our main theorem as follows:

Theorem 1.2. Let $C$ be a smooth complete algebraic curve of genus $g$ over an algebraically closed field $k$ of characteristic 0. Let $U \subset C$ be a nonempty open subset and $m = \#(C \setminus U)$. If $X, Y \in \mathcal{O}_C(U)$ and $u \in \mathcal{O}_C(U)^*$ satisfy
\[
X^n + Y^n - 1 = u
\]
for some $n \geq 5$, then
\[
h(X, Y, 1) \leq \frac{3(m + \max\{2g - 2, 0\})}{n - 4} \quad (1)
\]
or $(X^n + Y^n)(X^n - 1)(Y^n - 1) = 0$.

It is this version of the theorem that we will prove. After some background material is introduced in the next section, Theorem 1.2 will be proved in Section 3.

2. Preliminaries

The main theorems we will need in order to prove (1) are Mason’s theorem and its generalization by Masser and Brownawell. Before introducing these theorems, however, we will need to define some terms.

For each point $p$ on a complete algebraic curve $C$ there exists a discrete valuation $v_p : \mathcal{O}_{C,p} \to \mathbb{Z} \cup \{\infty\}$, which maps a function that is regular at $p$ to its order of vanishing at $p$. Such valuations naturally extend to the function field $K$ of $C$. 

We will use these valuations to define heights which will generalize the notion of degree to a set of rational functions on an algebraic curve.

**Definition 2.1.** The height of any finite collection \( u_1, u_2, \ldots, u_n \in K \), not all identically 0, is defined by

\[
h(u_1, u_2, \ldots, u_n) = -\sum_{p \in C} \min_{1 \leq j \leq n} v_p(u_j)
\]

and has the following properties:

(i) For any nonzero \( \alpha \in K \),

\[
h(\alpha u_1, \alpha u_2, \ldots, \alpha u_n) = h(u_1, u_2, \ldots, u_n).
\]

(ii) For any \( j \),

\[
h(u_1, \ldots, u_j, \ldots, u_n) \geq h(u_1, \ldots, u_{j-1}, u_{j+1}, \ldots, u_n).
\]

(iii) For any positive integer \( q \),

\[
h(u_1^q, u_2^q, \ldots, u_n^q) = q h(u_1, u_2, \ldots, u_n).
\]

**Remark 2.2.** Without note we will use the fact that replacing any function in the collection with its negative does not change the height. Likewise any permutation of the collection of functions will not change their height.

When the \( u_i \) are polynomials without any common zero, their height is simply the maximum of their degrees. In this sense height generalizes the notion of degree.

**Definition 2.3.** For \( \{u_1, u_2, \ldots, u_n\} \subseteq K \) we define the support to be

\[
\text{Supp}\{u_1, u_2, \ldots, u_n\} = \{p \in C : v_p(u_i) \neq 0 \text{ for some } 1 \leq i \leq n\},
\]

that is, the set of points where at least one \( u_i \) has a zero or pole.

Mason’s theorem and its generalizations give an inequality between the height of a set of linearly dependent rational functions and their support. The particular version that we will need is this:

**Theorem 2.4 [Brownawell and Masser 1986, Theorem B].** Let \( u_1, u_2, \ldots, u_n \in K \) be such that \( u_1 + u_2 + \cdots + u_n = 0 \) with no nonempty proper subset of the \( u_i \) adding to 0, and define \( \gamma_s = \frac{1}{2} (s - 1)(s - 2) \) for \( s \geq 1 \) and 0 otherwise. Then

\[
h(u_1, u_2, \ldots, u_n) \leq \gamma_n \max\{2g - 2, 0\} + \sum_{p \in C} (\gamma_n - \gamma_r(p)),
\]

where \( r(p) \) is the number of \( u_i \) not supported at \( p \).

The specialization of this result to the case of three rational functions will be convenient to have:
Theorem 2.5 (Mason’s theorem). Let $n = 3$ and assume the hypothesis and notation of Theorem 2.4. Then
\[ h(u_1, u_2, u_3) \leq \max\{2g - 2, 0\} + \# \text{Supp}\{u_1, u_2, u_3\}. \]

3. Main results

Throughout this section we will assume that $C$ is a smooth complete curve of genus $g$ over an algebraically closed field of characteristic 0, $U \subset C$ is a nonempty open subset, $m = \#(C \setminus U)$, and $X, Y \in \mathbb{C}(U)$ are regular functions on $U$.

As noted in Section 1 it suffices to study the solutions to the equation
\[ X^n + Y^n - 1 = u, \]
where $u \in \mathbb{C}(U)^*$. By Theorem 2.4 we can bound the height, $h(X^n, Y^n, -1, -u)$, in terms of an expression involving the number of points in the support of each of these functions. For convenience define
\[ S_1 = \text{Supp}\{X\} \cap \text{Supp}\{Y\} \cap U, \]
\[ S_2 = (\text{Supp}\{X, Y\} \setminus S_1) \cap U. \]

Then we have the following cases:

(i) If $p \in S_1$, precisely 2 of the functions are not supported at $p$, so $r(p) = 2$. Hence $\gamma_4 - \gamma_{r(p)} = \gamma_4 - \gamma_2 = 3 - 0 = 3$.

(ii) If $p \in S_2$, precisely 3 of the functions are not supported at $p$ so $\gamma_4 - \gamma_{r(p)} = 2$.

(iii) If $p \in C \setminus U$ we have $\gamma_4 - \gamma_{r(p)} \leq 3$, since $\gamma_{r(p)} \geq 0$ by definition for any $p$.

(iv) For all remaining points, $p \notin \text{Supp}\{X, Y, u\}$, so $\gamma_4 - \gamma_{r(p)} = 0$.

Thus, provided no nonempty proper subset of $\{X^n, Y^n, -1, -u\}$ adds to 0, we have
\[ h(X^n, Y^n, -1, -u) \leq 3 \max\{2g - 2, 0\} + 3\#S_1 + 2\#S_2 + 3\#(C \setminus U). \]

By definition $\#(C \setminus U) = m$, which is fixed by the choice of $U$. In order to bound the height it suffices to establish bounds on $\#S_1$ and $\#S_2$. Rather than directly bounding the size of these sets we will instead bound the quantity $2\#S_1 + \#S_2$. In particular we will show that $2\#S_1 + \#S_2 \leq 2h(X, Y, 1)$. It is necessary to first establish a theorem on the addition of heights. We begin with a fact about minimums.

Lemma 3.1. For any real numbers $x_1, x_2, \ldots, x_n, y_1, y_2, \ldots, y_m$,
\[ \min_{1 \leq i \leq n} \{x_i\} + \min_{1 \leq j \leq m} \{y_j\} = \min_{1 \leq i \leq n, 1 \leq j \leq m} \{x_i + y_j\}. \]
Proof. Let \( x \) be the minimum of the \( x_i \)'s, \( y \) be the minimum of the \( y_j \)'s, and \( x_p + y_q \) be the minimum of the \( (x_i + y_j) \)'s. Then \( x \leq x_p \) and \( y \leq y_q \), so \( x + y \leq x_p + y_q \). On the other hand, \( x + y \in \{x_i + y_j\} \). Therefore \( x + y \geq x_p + y_q \), and equality holds.

We are now able to come up with an alternate interpretation for the addition of heights.

**Corollary 3.2.** Let \( f_1, \ldots, f_n \) and \( g_1, \ldots, g_m \) be rational functions on an algebraic curve \( C \) where at least one \( f_i \) and one \( g_j \) are not identically 0. Then

\[
\begin{align*}
\h(f_1, f_2, \ldots, f_n) + \h(g_1, g_2, \ldots, g_m) &= -\sum_{p \in C} \min_{1 \leq i \leq n, 1 \leq j \leq m} \{v_p(f_i) + v_p(g_j)\}.
\end{align*}
\]

**Proof.** Immediate by Lemma 3.1 and the definition of the height function.

The utility of Corollary 3.2 comes from interpreting it as a type of distributive property. We can see this by noting \( v_p(f_i) + v_p(g_j) = v_p(f_i g_j) \). The particular case that we are interested in is

\[
\h(X, Y, 1) + \h(X, Y, 1) = \h(X^2, XY, X, Y^2, Y, 1).
\]

(4)

We can now proceed to bound the quantity \( 2\#S_1 + \#S_2 \).

**Proposition 3.3.** Suppose that neither \( X \) nor \( Y \) is identically 0. Then

\[
2\#S_1 + \#S_2 \leq 2h(X, Y, 1).
\]

**Proof.** As a result of Corollary 3.2 and Equation (4),

\[
2h(X, Y, 1) = h(X^2, XY, X, Y^2, Y, 1).
\]

By property (i) of heights (Definition 2.1) we can multiply through by \( (XY)^{-1} \), giving

\[
2h(X, Y, 1) = h\left(\frac{X}{Y}, 1, \frac{1}{Y}, \frac{Y}{X}, \frac{1}{X}, \frac{1}{XY}\right).
\]

Now by the definition of height, this is equal to

\[
-\sum_{p \in C} \min\{v_p\left(\frac{X}{Y}\right), v_p\left(\frac{1}{Y}\right), v_p\left(\frac{Y}{X}\right), v_p\left(\frac{1}{X}\right), v_p\left(\frac{1}{XY}\right), 0\}.
\]

After distributing the negative, we get

\[
\sum_{p \in C} \max\{v_p\left(\frac{Y}{X}\right), v_p(Y), v_p\left(\frac{X}{Y}\right), v_p(X), v_p(XY), 0\}.
\]

For each \( p \in S_1 \) we have \( v_p(XY) \geq 2 \) and for each \( p \in S_2 \) either \( v_p(X) \geq 1 \) or \( v_p(Y) \geq 1 \). Since every term of the sum is nonnegative and \( S_1 \cap S_2 \) is empty, it follows that \( 2\#S_1 + \#S_2 \leq 2h(X, Y, 1) \).
The previous proposition required the assumption that neither $X$ nor $Y$ was identically 0. This is necessary as $\#\text{Supp}\{0\} = \infty$. However, Theorem 1.2 still holds if either $X$ or $Y$ is 0. In fact a stronger bound holds.

**Proposition 3.4.** Suppose that $X^n + Y^n - 1$ is a unit on $U$ for some $n \geq 3$ and that at least one of $X$ or $Y$ is 0; then

$$h(X, Y, 1) \leq \frac{m + \max\{2g - 2, 0\}}{n - 2}.$$

**Proof.** If both $X$ and $Y$ are 0 the inequality trivially holds. Without a loss of generality we may assume $X \neq 0$ and $Y = 0$, in which case $X$ satisfies the equation $X^n - 1 - u = 0$ for some unit $u \in \mathcal{O}_C(U)^*$. Applying Theorem 2.5 we get the inequality

$$h(X^n, -1, -u) \leq \max\{2g - 2, 0\} + \#\text{Supp}\{X, 1, u\}.$$

By an argument similar to the proof of Proposition 3.3, $(\#(\text{Supp}\{X\} \cap U) \leq 2h(X, 1)$. Therefore we have

$$h(X^n, -1, -u) \leq \max\{2g - 2, 0\} + m + 2h(X, 1).$$

By properties (ii) and (iii) of heights (Definition 2.1),

$$(n - 2)h(X, -1) \leq \max\{2g - 2, 0\} + m.$$

Since $h(X, 0, -1) = h(X, -1)$ and $Y = 0$,

$$h(X, Y, 1) \leq \frac{m + \max\{2g - 2, 0\}}{n - 2},$$

as claimed. \qed

Now that we have bounds established we are able to give a proof of Theorem 1.2, from which Theorem 1.1 immediately follows.

**Proof of Theorem 1.2.** We only need to demonstrate the case where neither $X$ nor $Y$ is 0, since otherwise Proposition 3.4 gives a stronger inequality. If some nonempty proper subset of $\{X^n, Y^n, -1, -u\}$ adds to 0 then $(X^n + Y^n)(X^n - 1)(Y^n - 1) = 0$. Therefore we suppose that no nonempty proper subset adds to 0 and apply Theorem 2.4 to get (3):

$$h(X^n, Y^n, -1, -u) \leq 3 \max\{2g - 2, 0\} + 3\#S_1 + 2\#S_2 + 3\#(C \setminus U).$$

Next we simplify this inequality by applying properties (ii) and (iii) of heights:

$$nh(X, Y, 1) \leq 3 \max\{2g - 2, 0\} + 3\#S_1 + 2\#S_2 + 3\#(C \setminus U).$$
Since $3\#S_1 + 2\#S_2 \leq 2(2\#S_1 + \#S_2)$ we can apply Proposition 3.3 to get

$$nh(X, Y, 1) \leq 3 \max\{2g - 2, 0\} + 4h(X, Y, 1) + 3m.$$  

Provided $n \geq 5$ we can solve for $h(X, Y, 1)$ and get

$$h(X, Y, 1) \leq \frac{3(m + \max\{2g - 2, 0\})}{n - 4}.$$  

\[\square\]

4. Discussion

In Theorem 1.1 we were able to get a height bound provided $n \geq 5$ and that the image of the curve is not contained within a certain set. In this section we will give a geometric interpretation of this exceptional set as well as a proof that no bound can exist when $n = 2$.

Recall that a flex of an algebraic curve is a simple point where the tangent line intersects with multiplicity three or higher. Flexes can be computed by finding the zeroes of the Hessian of the defining function in the projective plane (see [Kunz 2005, Theorem 9.7] for details). In the case of Fermat curves the Hessian is

$$\begin{vmatrix} n(n-1)x^{n-2} & 0 & 0 \\ 0 & n(n-1)y^{n-2} & 0 \\ 0 & 0 & -n(n-1)z^{n-2} \end{vmatrix},$$

which is equal to $-n^3(n-1)^3x^{n-2}y^{n-2}z^{n-2}$. Therefore all of the flexes lie along the lines $x = 0$, $y = 0$, and $z = 0$. Substituting each of these into the Fermat equation gives us $y^n - z^n = 0$, $x^n - z^n = 0$, and $x^n + y^n = 0$ respectively. Each of these equations in turn determines $n$ flexes on the Fermat curve for a total of $3n$ flexes. Additionally each of these three equations defines the union of $n$ lines in projective space with each line being tangent to a flex. Returning to the statement of Theorem 1.1 we can see that the exceptional set $V((x^n + y^n)(x^n - z^n)(y^n - z^n))$ is just the union of the lines tangent to the $3n$ flexes of the curve.

We can also see that the exclusion of this exceptional set is necessary. For example, let $\zeta \in k$ be such that $\zeta^n = 1$. Then for each positive integer $q$ the morphism

$$\phi_q : \mathbb{P}_k^1 \setminus \{0, \infty\} \rightarrow \mathbb{P}_k^2 \setminus V(z(x^n + y^n - z^n))$$

given by $[u : v] \mapsto [u^q : \zeta^q : v^q]$ is well-defined and has its image contained within the zero set of $y^n - z^n$. Since $q$ can be any positive integer there cannot be a bound on the height. A similar argument holds for the other components of the exceptional set.

Finally we will show that such height bounds cannot exist if $n = 2$. Let $C = \mathbb{P}_k^1$ and $U = C \setminus \{\infty, 0\}$ with coordinate ring $\mathcal{O}_C(U) = k[t, t^{-1}]$. Consider the
diophantine equation

\[ X^2 + Y^2 - 1 = t^q, \]

where \( X, Y \in k[t, t^{-1}] \) and \( q \) is any odd positive integer. We can rewrite this as

\[ (X + iY)(X - iY) = 1 + t^q. \]

We then set

\[ X + iY = 1 + t \quad \text{and} \quad X - iY = \sum_{j=0}^{q-1} (-1)^j t^j. \]

Solving for \( X \) and \( Y \) gives

\[ X = \frac{1}{2} \left( 1 + t + \sum_{j=0}^{q-1} (-1)^j t^j \right) \quad \text{and} \quad Y = -i \frac{1}{2} \left( 1 + t - \sum_{j=0}^{q-1} (-1)^j t^j \right). \]

Since \( q \) can be arbitrarily large, \( h(X, Y, 1) \) is unbounded. Moreover the family of rational curves defined by \( (X, Y) \) as \( q \) varies is not contained in any proper closed subset of \( \mathbb{A}^2_k \). Therefore no similar result can hold for \( n = 2 \).

Acknowledgements

We wish to acknowledge the support of the University of Wisconsin-Stout. We also thank Christopher Bendel for comments on an earlier version of this manuscript and the referee for pointing out a simplification to the proof of the main theorem. This research was funded in part by NSF grant 1062403.

References


Received: 2012-08-31 Revised: 2013-01-20 Accepted: 2013-01-21
dutters@uwstout.edu Department of Mathematics, Statistics and Computer
Science, University of Wisconsin-Stout,
Menomonie, WI 54751, United States

Melissa.Haire@gordon.edu Department of Mathematics and Computer
Science, Gordon College, Wenham, MA 01984, United States

asetniker09@wou.edu Mathematics Department, Western Oregon University,
Monmouth, OR 97361, United States
Infinite cardinalities in the Hausdorff metric geometry
ALEXANDER ZUPAN
585
Computing positive semidefinite minimum rank for small graphs
STEVEN OSBORNE AND NATHAN WARNBERG
595
The complement of Fermat curves in the plane
SETH DUTTER, MELISSA HAIRE AND ARIEL SETNIKER
611
Quadratic forms representing all primes
JUSTIN DEBENEDETTO
619
Counting matrices over a finite field with all eigenvalues in the field
LISA KAYLOR AND DAVID OFFNER
627
A not-so-simple Lie bracket expansion
JULIE BEIER AND MCCABE OLSEN
647
On the omega values of generators of embedding dimension-three numerical monoids generated by an interval
SCOTT T. CHAPMAN, WALTER PUCKETT AND KATY SHOUR
657
Matrix coefficients of depth-zero supercuspidal representations of GL(2)
ANDREW KNIGHTLY AND CARL RAGSDALE
669
The sock matching problem
SARAH GILLIAND, CHARLES JOHNSON, SAM RUSH AND DEBORAH WOOD
691
Superlinear convergence via mixed generalized quasilinearization method and generalized monotone method
VINCHENCIA ANDERSON, COURTNEY BETTIS, SHALA BROWN, JACQKIS DAVIS, NAEEM TULL-WALKER, VINODH CHELLAMUTHU AND AGHALAYA S. VATSALA
699