# HILBERT'S TENTH PROBLEM FOR FUNCTION FIELDS OF VARIETIES OVER $\mathbb{C}$

KIRSTEN EISENTRÄGER

Abstract. Let $K$ be the function field of a variety of dimension $\geq 2$ over an algebraically closed field of characteristic zero. Then Hilbert's Tenth Problem for $K$ is undecidable. This generalizes the result by Kim and Roush from 1992 that Hilbert's Tenth Problem for the purely transcendental function field $\mathbb{C}(t_1, t_2)$ is undecidable.

## 1. Introduction

Hilbert's Tenth Problem in its original form was to find an algorithm to decide, given a polynomial equation $f(x_1, \ldots, x_n) = 0$ with coefficients in the ring $\mathbb{Z}$ of integers, whether it has a solution with $x_1, \ldots, x_n \in \mathbb{Z}$. Matijasevič [Mat70] proved that no such algorithm exists, *i.e.* that Hilbert's Tenth Problem is undecidable. Since then various analogues of this problem have been studied by considering polynomial equations with coefficients and solutions over some other commutative ring $R$. Perhaps the most important unsolved question in this area is Hilbert's Tenth Problem over the field of rational numbers. However, there has been recent progress by Poonen [Poo03] who proved undecidability for large subrings of $\mathbb{Q}$. The function field analogue, namely Hilbert's Tenth Problem for the function field $k$ of a curve over a finite field, is undecidable. This was proved by Pheidas for $k = \mathbb{F}_q(t)$ with $q$ odd, and by Videla [Vid94] for $\mathbb{F}_q(t)$ with $q$ even. Shlapentokh [Shl96, Shl00] generalized Pheidas' result to finite extensions of $\mathbb{F}_q(t)$ with $q$ odd and to certain function fields over possibly infinite constant fields of odd characteristic, and the remaining cases in characteristic 2 are treated in [Eis03]. Hilbert's Tenth Problem is also known to be undecidable for several rational function fields of characteristic zero: In 1978 Denef proved the undecidability of Hilbert's Tenth Problem for rational function fields $K(T)$ over formally real fields $K$ [Den78], and he was the first to use rank one elliptic curves to prove undecidability. Kim and Roush [KR92] showed that the problem is undecidable for the purely transcendental function field $\mathbb{C}(t_1, t_2)$ and their approach also used rank one elliptic curves. In this paper we will generalize the result by Kim and Roush. We prove that Hilbert's Tenth Problem for function fields of surfaces over $\mathbb{C}$ is undecidable.

Partially supported by the National Science Foundation under agreement No. DMS-0111298. Any opinions, findings and conclusions expressed in this article are those of the author and do not necessarily reflect the views of the National Science Foundation.

More generally, in the first part of this paper we prove the following:

**Theorem 1.1.** *Let $K$ be the function field of a surface over an algebraically closed field $k$ of characteristic zero. Then Hilbert's Tenth Problem for $K$ is undecidable.*

In Hilbert's Tenth Problem we need to input the coefficients of an equation into a Turing machine, so in our situation we need to restrict the coefficients of the equations. We will show: There exist elements $z_1, z_2 \in K$ which generate an extension of transcendence degree 2 over $k$ such that Hilbert's Tenth Problem for $K$ with coefficients in $\mathbb{Z}[z_1, z_2]$ is undecidable. For simplicity we will just refer to this as Hilbert's Tenth Problem for $K$.

Theorem 1.1 can also be stated more geometrically: Let $X$ be a smooth projective surface over $k$. There is no algorithm that determines whether dominant morphisms from varieties to $X$ admit rational sections.

We will prove Theorem 1.1 by constructing a diophantine model of the integers with addition and multiplication over $K$. To do this we will construct a diophantine model of $\mathbb{Z} \times \mathbb{Z}$ with certain relations and then show that we can define the integers with addition and multiplication inside this model. In the first part of this paper we will for simplicity assume that $K$ is the function field of a surface over $\mathbb{C}$. The proof is exactly the same when we replace $\mathbb{C}$ by an arbitrary algebraically closed field of characteristic zero. We use the fact that our field has characteristic zero in the construction of rank one elliptic curves in Section 3.1, and the fact that we are working with function fields over an algebraically closed field is used in Section 4 where we apply the Tsen-Lang Theorem.

The same approach as in Theorem 1.1 also generalizes to higher transcendence degree. In Section 5 we prove:

**Theorem 1.2.** *Let $K$ be the function field of a variety of dimension $\geq 2$ over an algebraically closed field $k$ of characteristic zero. Then Hilbert's Tenth Problem for $K$ is undecidable.*

Again, we will show: There exist elements $z_1, z_2 \in K$ which generate an extension of transcendence degree 2 over $k$ such that Hilbert's Tenth Problem for $K$ with coefficients in $\mathbb{Z}[z_1, z_2]$ is undecidable.

## 2. The model

First we will define two notions that will appear frequently in the remainder of this paper.

**Definition 1.** 1. If $R$ is a commutative ring, a *diophantine equation over $R$* is an equation $P(x_1, \ldots, x_n) = 0$ where $P$ is a polynomial in the variables $x_1, \ldots, x_n$ with coefficients in $R$.
2. A subset $S$ of $R^k$ is *diophantine over $R$* if there exists a polynomial $P(x_1, \ldots, x_k, y_1, \ldots, y_m) \in R[x_1, \ldots, x_k, y_1, \ldots, y_m]$ such that

$$S = \{(x_1, \ldots, x_k) \in R^k : \exists y_1, \ldots, y_m \in R,\ (P(x_1, \ldots, x_k, y_1, \ldots, y_m) = 0)\}.$$

Let $K$ be a finite extension of $\mathbb{C}(t_1, t_2)$. We will define a diophantine model of the structure $\mathcal{S} = \langle \mathbb{Z} \times \mathbb{Z}, +, |\,, \mathcal{Z}, \mathcal{W} \rangle$ in $K$. Here $+$ denotes the usual component-wise addition of pairs of integers, $|$ represents a relation which satisfies

$$(n, 1) \mid (m, s) \Leftrightarrow m = ns,$$

and $\mathcal{Z}$ is a unary predicate which is interpreted as

$$\mathcal{Z}(n, m) \Leftrightarrow m = 0.$$

The predicate $\mathcal{W}$ is interpreted as

$$\mathcal{W}((m, n), (r, s)) \Leftrightarrow m = s \wedge n = r.$$

A *diophantine model* of $\mathcal{S}$ over $K$ is a diophantine subset $S \subseteq K^n$ equipped with a bijection $\phi : \mathbb{Z} \times \mathbb{Z} \to S$ such that under $\phi$, the graphs of addition, $|$, $\mathcal{Z}$, and $\mathcal{W}$ in $\mathbb{Z} \times \mathbb{Z}$ correspond to diophantine subsets of $S^3, S^2, S$, and $S^2$, respectively.

In this section we will show that constructing such a model is sufficient to prove undecidability of Hilbert's Tenth Problem for $K$.

First we can show the following

**Proposition 2.1.** *The relation $\mathcal{W}$ can be defined entirely in terms of the other relations.*

*Proof.* It is enough to verify that

$$\mathcal{W}((a, b), (x, y)) \Leftrightarrow (1, 1) \mid ((x, y) + (a, b)) \wedge (-1, 1) \mid ((x, y) - (a, b)).$$

□

As Pheidas and Zahidi [PZ00] point out we can existentially define the integers with addition and multiplication inside $\mathcal{S} = \langle \mathbb{Z} \times \mathbb{Z}, +, |\,, \mathcal{Z}, \mathcal{W} \rangle$, so $\mathcal{S}$ has an undecidable existential theory:

**Proposition 2.2.** *The structure $\mathcal{S}$ has an undecidable existential theory.*

*Proof.* We interpret the integer $n$ as the pair $(n, 0)$. The set $\{(n, 0) : n \in \mathbb{Z}\}$ is existentially definable in $\mathcal{S}$ through the relation $\mathcal{Z}$. Addition of integers $n, m$ corresponds to the addition of the pairs $(n, 0)$ and $(m, 0)$. To define multiplication of the integers $m$ and $r$, note that $n = mr$ if and only if $(m, 1) \mid (n, r)$, hence $n = mr$ if and only if

$$\exists\, a, b\ : ((m, 0) + (0, 1)) \mid ((n, 0) + (a, b)) \wedge \mathcal{W}((a, b), (r, 0)).$$

Since the positive existential theory of the integers with addition and multiplication is undecidable, $\mathcal{S}$ has an undecidable existential theory as well. □

The above proposition shows that in order to prove Theorem 1.1 it is enough to construct a diophantine model of $\mathcal{S}$ over $K$. In Sections 3 and 4 we will construct this model.

## 3. An existentially definable set isomorphic to $\mathbb{Z} \times \mathbb{Z}$

3.1. **Generating elliptic curves of rank one.** Let $K$ be a finite extension of $\mathbb{C}(t_1, t_2)$.

Our first task is to find a diophantine set $A$ over $K$ which is isomorphic to $\mathbb{Z} \times \mathbb{Z}$ as a set. In their undecidability proof for $\mathbb{C}(t_1, t_2)$ [KR92] Kim and Roush obtain such a set by using the $\mathbb{C}(t_1, t_2)$-rational points on two elliptic curves which have rank one over $\mathbb{C}(t_1, t_2)$. We need to construct two elliptic curves which have rank one over $K$.

These can be obtained from a theorem by Moret-Bailly [MB03]. In his theorem he uses the following notation: Let $k$ be a field of characteristic zero. Let $C$ be a smooth projective geometrically connected curve over $k$ with function field $F$. Let $Q$ be a finite nonempty set of closed points of $C$. Let $E : y^2 = x^3 + ax + b$ be an elliptic curve over $k$ with $b \neq 0$. In [MB03] Moret-Bailly also introduces another curve $\Gamma$, but for our application of his theorem we only have to consider the special case where $\Gamma = E$.

**Definition 2.** Let $k, C, F, E, Q$ be as above. Let $g : C \to \mathbf{P}^1_k$ be a non-constant $k$-morphism corresponding to an injection $k(T) \hookrightarrow F$ sending $T$ to $g$. We say that $g$ is *admissible* for $E$ (and $Q$) if

(1) $g$ has only simple branch points.
(2) $g$ is étale above 0 and the branch points of $E$.
(3) Every point of $Q$ is a pole of $g$.

*Remark.* In [MB03] Moret-Bailly asserts that, given $C, E, Q$, we can always find an admissible morphism $g$. If $g$ is admissible for $E$, then for all but finitely many $\lambda \in k^*$, $\lambda g$ is still admissible.

Now we can state Moret-Bailly's theorem.

**Theorem 3.1.** [MB03, Theorem 1.5] *Let $k, C, F, E, Q$ be as above. Let $f \in F$ be admissible for $E, Q$. Let $\mathcal{E}_{\lambda f}$ be the elliptic curve*

$$\mathcal{E}_{\lambda f} : ((\lambda f)^3 + a(\lambda f) + b)\, y^2 = x^3 + ax + b.$$

*Then the natural homomorphism $\mathcal{E}(k(T)) \hookrightarrow \mathcal{E}_{\lambda f}(F)$ induced by the inclusion $k(T) \hookrightarrow F$ that sends $T$ to $\lambda f$ is an isomorphism for infinitely many $\lambda \in \mathbb{Z}$.*

If we assume in addition that $E$ has no complex multiplication, then by a theorem of Denef [Den78], $\mathcal{E}(k(T))$ has rank one with generator $(T, 1)$ (modulo 2-torsion). So Theorem 3.1 gives us infinitely many elliptic curves that have rank one over $F$: Given $f$ and $\lambda$ as in the theorem we obtain an elliptic curve $\mathcal{E}_{\lambda f}$ which has rank one over $F$ with generator $(\lambda f, 1)$ (modulo 2-torsion).

We can use Moret-Bailly's theorem to prove the following theorem:

**Theorem 3.2.** *Let $K$ be a finite extension of $\mathbb{C}(t_1, t_2)$. Let $E : y^2 = x^3 + ax+b$ be an elliptic curve with $a, b \in \mathbb{C}$, $b \neq 0$, and no complex multiplication. There exist $z_1, z_2 \in K$ such that $\mathbb{C}(z_1, z_2)$ has transcendence degree 2 over $\mathbb{C}$*

*and such that the two elliptic curves* $\mathcal{E}_1 : (z_1^3 + az_1 + b)\, y^2 = x^3 + ax + b$ *and* $\mathcal{E}_2 : (z_2^3 + az_2 + b)\, y^2 = x^3 + ax + b$ *have rank one over* $K$ *with generators* $(z_1, 1)$ *and* $(z_2, 1)$*, respectively (modulo 2-torsion).*

*Proof.* Let $k$ be the algebraic closure of $\mathbb{C}(t_2)$ inside $K$. There exists a smooth, projective, geometrically connected curve $C$ over $k$ whose function field is $K$. Let $Q$ be a finite nonempty set of closed points of $C$, and choose an $f \in K$ that is admissible for $E$ and $Q$. Since $f$ is non-constant, $f$ is transcendental over $\mathbb{C}(t_2)$. Now we can apply Theorem 3.1 with $F = K$ and $k, C, E, Q, f$ as defined above. By Theorem 3.1 there exists a nonzero $\lambda \in \mathbb{Z}$ such that

$$\mathcal{E}_{\lambda f} : ((\lambda f)^3 + a(\lambda f) + b)y^2 = x^3 + ax + b$$

has rank one with generator $(\lambda f, 1)$ (modulo 2-torsion). By the remark, some integer multiple of $t_2 \cdot \lambda f$ will still be admissible for $E$. Let $g$ be such an integer multiple. By Theorem 3.1 applied to $g$ there exists a nonzero integer $\mu$ such that

$$\mathcal{E}_{\mu g} : ((\mu g)^3 + a(\mu g) + b)y^2 = x^3 + ax + b$$

has rank one with generator $(\mu g, 1)$ (modulo 2-torsion). Let $z_1 := \lambda f$, and let $z_2 := \mu g$. To complete the proof it remains to show that $\mathbb{C}(z_1, z_2)$ has transcendence degree 2 over $\mathbb{C}$. Since $z_2 = \nu z_1 t_2$ for some nonzero integer $\nu$, it follows that $t_2 \in \mathbb{C}(z_1, z_2)$. As pointed out above, the element $f$ is transcendental over $\mathbb{C}(t_2)$, and hence the same is true for $\lambda f = z_1$. This shows that the transcendence degree of $\mathbb{C}(z_1, z_2)$ over $\mathbb{C}$ is at least 2, and since $\mathbb{C}(z_1, z_2) \subseteq K$, which is algebraic over $\mathbb{C}(t_1, t_2)$, the transcendence degree must equal 2. □

3.2. **Diophantine definition of $A$.** In the following let $E : y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbb{C}$, $b \neq 0$, no complex multiplication and such that the point $(0, \sqrt{b})$ has infinite order. Such a curve exists: the curve $E : y^2 = x^3 + x + 1$ (496A1 in [Cre97]) has the required properties. The condition that $(0, \sqrt{b})$ has infinite order will be needed in the proof of Theorem 4.1. Let $\mathcal{E}_1$ and $\mathcal{E}_2$ be as above. To be able to define a suitable set $A$ which is isomorphic to $\mathbb{Z} \times \mathbb{Z}$ we need to work in an algebraic extension $L$ of $K$. Let $L := K(h_1, h_2)$, where $h_i$ is defined by $h_i^2 = z_i^3 + az_i + b$, for $i = 1, 2$. To prove undecidability for $K$ it is enough to prove that the existential theory of $L$ in the language $\langle\, L, +, \cdot\ ; 0, 1, z_1, z_2, h_1, h_2, S\,\rangle$ is undecidable, where $S$ is a predicate for the elements of the subfield $K$ [PZ00, Lemma 1.9]. So from now on we will work with equations over $L$.

Over $L$ both $\mathcal{E}_1$ and $\mathcal{E}_2$ are isomorphic to $E$. There is an isomorphism between $\mathcal{E}_1$ and $E$ that sends $(x, y) \in \mathcal{E}_1$ to the point $(x, h_1 y)$ on $E$. Under this isomorphism the point $(z_1, 1)$ on $\mathcal{E}_1$ corresponds to the point $P_1 := (z_1, h_1)$ on $E$. Similarly there is an isomorphism between $\mathcal{E}_2$ and $E$ that sends the point $(z_2, 1)$ on $\mathcal{E}_2$ to the point $P_2 := (z_2, h_2)$ on $E$.

The elliptic curve $E$ is a projective variety, but any projective algebraic set can be partitioned into finitely many affine algebraic sets, which can then be embedded into a single affine algebraic set. This implies that the set $E(L)$ is diophantine over $L$, since we can take care of the point at infinity $\mathbf{O}$ of $E$.

We will show that the set of points $\mathbb{Z}P_1 \times \mathbb{Z}P_2 \subseteq E(L)$ is existentially definable in our language, because we have a predicate for the elements of $K$: Since $\mathcal{E}_1$ has 2-torsion, we first give a diophantine definition of $2 \cdot \mathbb{Z}P_1$:

$$P \in 2 \cdot \mathbb{Z}P_1 \Leftrightarrow \exists\, x, y \in K \ (z_1^3 + az_1 + b)\, y^2 = x^3 + ax + b \wedge P = 2 \cdot (x, h_1 y)$$

This set is diophantine, because we can express that $P = 2 \cdot Q$ by diophantine equations. Then $\mathbb{Z}P_1$ can be defined as

$$P \in \mathbb{Z}P_1 \Leftrightarrow (P \in 2 \cdot \mathbb{Z}P_1) \text{ or } (\exists\, Q \in 2 \cdot \mathbb{Z}P_1 \text{ and } P = Q + P_1)$$

Similarly we have a diophantine definition for $\mathbb{Z}P_2$. Hence the cartesian product $\mathbb{Z}P_1 \times \mathbb{Z}P_2 \subseteq E(L)$ is existentially definable, since addition on $E$ is existentially definable.

3.3. **Existential definition of $+$ and $\mathcal{Z}$.** The unary relation $\mathcal{Z}$ is existentially definable, since this is the same as showing that the set $\mathbb{Z}P_1$ is diophantine, which was done above. Addition of pairs of integers corresponds to addition on the cartesian product of the elliptic curves $\mathcal{E}_i$ (as groups), hence it is existentially definable. Since $\mathcal{W}$ can be defined in terms of the other relations, it remains to define the divisibility relation $\mid$. This is done in the next section.

## 4. Existential definition of $(m, 1) \mid (n, r)$

Now we will show how to existentially define the relation $\mid$ among pairs of integers in $L$. In the following $x(P)$ will denote the $x$-coordinate of a point $P$ on $E$, and $y(P)$ will denote the $y$-coordinate of $P$. Let $\alpha := [L : \mathbb{C}(z_1, z_2, h_1, h_2)]$. To give an existential definition of $\mid$ we will use the fact that $(m, 1) \mid (n, r) \Leftrightarrow (m, 1) \mid (kn, kr)$ for $k \neq 0$.

**Theorem 4.1.** *There exists a finite set $U \subseteq \mathbb{Z}$ such that for all $m \in \mathbb{Z} - U$ we have: for all $n, r \in \mathbb{Z}$*

$$\begin{aligned} &(m, 1) \mid (n, r) \Leftrightarrow \\ &\quad (\exists\, y_0, z_0 \in L^* \ \ x(nP_1 + rP_2)\, y_0^2 + x(mP_1 + P_2)\, z_0^2 = 1 \\ &\wedge \exists\, y_1, z_1 \in L^* \ \ x(2nP_1 + 2rP_2)\, y_1^2 + x(mP_1 + P_2)\, z_1^2 = 1 \\ &\qquad\qquad \cdots \\ &\wedge \exists\, y_\alpha, z_\alpha \in L^* \ \ x(2^\alpha nP_1 + 2^\alpha rP_2)\, y_\alpha^2 + x(mP_1 + P_2)\, z_\alpha^2 = 1\,). \end{aligned}$$

*Proof.* For the first implication, assume that $(m, 1) \mid (n, r)$, *i.e.* $n = mr$. Then both $x(nP_1 + rP_2) = x(r(mP_1 + P_2))$ and $x(mP_1 + P_2)$ are elements of $\mathbb{C}(x(mP_1 + P_2), y(mP_1 + P_2))$, which has transcendence degree one over $\mathbb{C}$. This means that we can apply the Tsen-Lang Theorem (Theorem 6.3 in the appendix) to the quadratic form

$$x(nP_1 + rP_2)y^2 + x(mP_1 + P_2)z^2 - w^2$$

to conclude that there exists a nontrivial zero $(y, z, w)$ over $\mathbb{C}(x(mP_1 + P_2), y(mP_1 + P_2))$. From the theory of quadratic forms it follows that there exists a nontrivial zero $(y, z, w)$ with $y \cdot z \cdot w \neq 0$. The same can be done for the other equations.

For the other direction, suppose that $n \neq mr$ and assume by contradiction that all $\alpha + 1$ equations are satisfied. We will proceed with the proof in four steps.

**Claim 1.** There exists a finite set $U \subseteq \mathbb{Z}$ such that for all $m \in \mathbb{Z} - U$ there exists a discrete valuation $w_m : L^* \twoheadrightarrow \mathbb{Z}$ such that $w_m(x(mP_1 + P_2)) = 1$ and such that $w_m(x(knP_1 + krP_2)) = 0$ for $k = 1, 2, 4, \ldots, 2^\alpha$.

**Proof of Claim 1:** Fix $m \in \mathbb{Z}$. Let $P_2' = mP_1 + P_2 = (z_2', h_2')$. Let $F := \mathbb{C}(z_1, z_2, h_1, h_2)$. Then

$$F = \mathbb{C}(z_1, z_2, h_1, h_2) = \mathbb{C}(z_1, h_1, z_2', h_2') = \mathbb{C}(x(P_1), y(P_1), x(P_2'), y(P_2')),$$

since $z_2 = x(P_2' - mP_1)$ and $z_2' = y(P_2' - mP_1)$. Let $v_m : F^* \twoheadrightarrow \mathbb{Z}$ be a discrete valuation which extends the discrete valuation $v$ of $\mathbb{C}(z_1, h_1)(z_2')$ associated to $z_2'$. The valuation $v$ is the discrete valuation that satisfies $v(\gamma) = 0$ for all $\gamma \in \mathbb{C}(z_1, h_1)$ and $v(z_2') = 1$. In $F$ the element $z_2'$ is still a uniformizer. Suppose $v_m$ does not ramify in $L$. Let $w_m$ be an extension of $v_m$ to $L$. We can consider $L/F$ as an extension of algebraic function fields of transcendence degree one by taking the constant field of $F$ to be $\mathbb{C}(z_1, h_1)$, and $v_m$ is a valuation which is trivial on $\mathbb{C}(z_1, h_1)$. We can apply Theorem 6.1 to conclude that only finitely many $v_m$ ramify in $L$. Let

$$U := \{m \in \mathbb{Z} : v_m \text{ ramifies in } L\}.$$

Then $U$ is a finite set. Let $m \in \mathbb{Z} - U$, and let $\ell$ be the residue field of $w_m$. Since the residue field of $v_m$ is just $\mathbb{C}(z_1, h_1)$, it follows that $\ell$ is a finite extension of $\mathbb{C}(z_1, h_1)$ with $[\ell : \mathbb{C}(z_1, h_1)] \leq \alpha$. Let $s := n - mr$. By assumption $s \neq 0$. The equations, rewritten in terms of $P_2'$ and $s$ become

$$\begin{aligned} &\exists\, y_0, z_0 \in L^* \;\; x(sP_1 + rP_2')\, y_0^2 + x(P_2')\, z_0^2 = 1 \\ \wedge\, &\exists\, y_1, z_1 \in L^* \;\; x(2sP_1 + 2rP_2')\, y_1^2 + x(P_2')\, z_1^2 = 1 \\ &\qquad\cdots \\ \wedge\, &\exists\, y_\alpha, z_\alpha \in L^* \;\; x(2^\alpha sP_1 + 2^\alpha rP_2')\, y_\alpha^2 + x(P_2')\, z_\alpha^2 = 1. \end{aligned}$$

By our choice of $w_m$, we have $w_m(x(P_2')) = 1$. The residue field $\ell$ of $w_m$ is an extension of $\mathbb{C}(z_1, h_1)$ and the image of $x(sP_1 + rP_2')$ in the residue field $\ell$ is $x(s(z_1, h_1) + r(0, \pm\sqrt{b}))$. We can show that this $x$-coordinate cannot be zero, which will imply that $w_m(x(nP_1 + rP_2)) = w_m(x(sP_1 + rP_2')) = 0$: The point $(z_1, h_1) \in E(\mathbb{C}(z_1, h_1))$ has infinite order, $z_1$ is transcendental over $\mathbb{C}$, and all points of $E$ whose $x$-coordinate is zero are defined over $\mathbb{C}$. Since $s \neq 0$, this implies that $x(s(z_1, h_1) + r(0, \pm\sqrt{b})) \neq 0$.

The same argument shows that $w_m(x(knP_1 + krP_2)) = w_m(x(ksP_1 + krP_2')) = 0$ for $k = 1, 2, 4, \ldots, 2^\alpha$ for all $m \in \mathbb{Z} - U$.

**Claim 2.** Denote by $x_{s,r}$ the image of $x(sP_1 + rP_2') = x(nP_1 + rP_2)$ in the

residue field $\ell$. The elements $x_{s,r}$ , $x_{2s,2r}$ , ..., $x_{2^\alpha s,2^\alpha r}$ are squares in $\ell$.
**Proof of Claim 2:** This follows immediately from Lemma 6.2 in the appendix.
**Claim 3.** The elements $x_{s,r}$ , ..., $x_{2^\alpha s\,,\,2^\alpha r}$ are not squares in $\mathbb{C}(z_1, h_1)$.
**Proof of Claim 3:** Since $x_{s,r}$ , $x_{2s,2r}$ , $\cdots$ , $x_{2^\alpha s,2^\alpha r} \in \mathbb{C}(z_1, h_1)$, which is the function field of $E$, we can consider them as functions $E \to \mathbf{P}^1_{\mathbb{C}}$. Then $x_{s,r}$ corresponds to the function on $E$ which can be obtained as the composition $P \mapsto sP + r(0, \sqrt{b}) \mapsto x(sP + r(0, \sqrt{b}))$. The $x$-coordinate map is of degree 2 and has two distinct zeros, namely $(0, \sqrt{b})$ and $(0, -\sqrt{b})$. The map $E \to E$ which maps $P$ to $(sP + r(0, \sqrt{b}))$ is unramified since it is the multiplication-by-$s$ map followed by a translation. Hence the composition of these two maps has $2s^2$ simple zeros. The same argument works for the other functions $x_{ks,kr}$. So each of the functions $x_{ks,kr}$, for $k = 1, 2, 4, \dots, 2^\alpha$ has only simple zeros. In particular, none of these functions is a square in $\mathbb{C}(z_1, h_1)$.
**Claim 4.** The images of $x_{s,r}, \dots, x_{2^\alpha s,2^\alpha r}$ in

$$V := [(\ell^*)^2 \cap \mathbb{C}(z_1, h_1)^*]/(\mathbb{C}(z_1, h_1)^*)^2 \text{ are distinct.}$$

**Proof of Claim 4:** By Claim 2 all elements $x_{ks,kr}$ are in $(\ell^*)^2$. If $x_{s,r}(P) = 0$ for some point $P$ on $E$, then

$$sP + r(0, \sqrt{b}) = (0, \sqrt{b}) \text{ or } sP + r(0, \sqrt{b}) = (0, -\sqrt{b}).$$

But that implies that

$$2[sP + r(0, \sqrt{b})] \neq \mathbf{O}, (0, \sqrt{b}), (0, -\sqrt{b}),$$

since we picked our curve $E : y^2 = x^3 + ax + b$ such that the point $(0, \sqrt{b})$ has infinite order. Hence neither $2(0, \sqrt{b})$ nor $2(0, -\sqrt{b})$ can equal $\mathbf{O}$, $(0, \sqrt{b})$ or $(0, -\sqrt{b})$. This implies that $P$ is neither a zero nor a pole of $x_{2s,2r}$ and similarly neither a zero nor a pole of $x_{2^k s,2^k r}$. The same argument shows that a zero of $x_{2^i s,2^i r}$ is neither a zero nor a pole of $x_{2^j s,2^j r}$ for $j > i$. This implies that it cannot happen that $x_{2^i s,2^i r} = f^2 \cdot x_{2^j s,2^j r}$ with $f \in \mathbb{C}(z_1, h_1)$, because if, say, $j > i$ and $P$ is a zero of the left-hand-side, then the left-hand-side has a zero of order 1 at $P$ while the right-hand-side has a zero of even order at $P$. Hence all the elements are different in $V = (\ell^{*2} \cap \mathbb{C}(z_1, h_1)^*)/(\mathbb{C}(z_1, h_1)^*)^2$. This proves the claim.

But now we have obtained a contradiction: since $[\ell : \mathbb{C}(z_1, h_1)] \leq \alpha$, the size of $V$ is bounded by $\alpha$ by Theorem 6.4, so it cannot contain $\alpha+1$ distinct elements. This means that for all $m \in \mathbb{Z} - U$ the solvability of the $\alpha + 1$ equations implies that $n = mr$. □

We have seen above that the relation $\mathcal{W}$ can be defined in terms of the other relations. It turns out that it is convenient to give an existential definition of $\mathcal{W}$ now and then use it to give a short proof that $|$ has an existential definition.

**Proposition 4.2.** *The relation $\mathcal{W}$ is existentially definable.*

*Proof.* Let $m_0 \in \mathbb{Z} - U$. Then

$$\begin{aligned}&\mathcal{W}((m,n),(r,s))\\ &\Leftrightarrow (1,1) \mid (m+r, n+s) \wedge (-1,1) \mid (m-r, n-s)\\ &\Leftrightarrow (m_0,1) \mid (m_0(m+r), n+s) \wedge (m_0,1) \mid (-m_0(m-r), n-s).\end{aligned}$$

Since $m_0$ is a fixed element of $\mathbb{Z}-U$, and since $\mathbb{Z}P_1$ and $\mathbb{Z}P_2$ are diophantine, the expression

$$(m_0,1) \mid (m_0(m+r), n+s) \wedge (m_0,1) \mid (-m_0(m-r), n-s)$$

is diophantine in $(m,n)$ and $(r,s)$ by Theorem 4.1. □

**Theorem 4.3.** *The relation $(m,1) \mid (n,r)$ is existentially definable in $(m,1)$ and $(n,r)$.*

*Proof.* Let $m_0$ be as in the above proposition, and let $d$ be a positive integer such that $U \subseteq (m_0-d, m_0+d)$. Since $n = mr \Leftrightarrow dn + m_0 r = dmr + m_0 r = (dm+m_0)r$, we have

$$(m,1) \mid (n,r) \Leftrightarrow (dm+m_0,1) \mid (dn+m_0r, r),$$

and we can just work with that formula instead. So

$$(m,1) \mid (n,r) \Leftrightarrow \exists\, a,b\, (dm+m_0,1) \mid ((dn,r)+m_0(a,b)) \wedge \mathcal{W}((a,b),(0,r)).$$

This last expression is existentially definable in $(m,1)$ and $(n,r)$. Since $m_0 \in \mathbb{Z}-U$, and by our choice of $d$, we have $(dm+m_0) \in \mathbb{Z}-U$, and we can apply Theorem 4.1. □

## 5. Hilbert's Tenth Problem for function fields of transcendence degree $\geq 2$

In this section we will generalize Theorem 1.1 to function fields of transcendence degree $\geq 2$ and prove Theorem 1.2. Again, for simplicity of notation, we will prove Theorem 1.2 for $k = \mathbb{C}$ . The proof still works word for word the same when we replace $\mathbb{C}$ by an arbitrary algebraically closed field of characteristic zero.

Let $K$ be a finite extension of $\mathbb{C}(t_1, t_2, \dots, t_n)$. We want to prove that Hilbert's Tenth Problem for $K$ is undecidable. In our proof we will use the following approach. Let $R$ be the algebraic closure of $\mathbb{C}(t_3, \dots, t_n)$ in $K$. Then $K$ is a finite extension of $R(t_1,t_2)$. Our argument will follow the proof of the transcendence degree 2 case with $\mathbb{C}$ replaced by $R$. The only difference is that we are now working with a transcendence degree 2 extension over a ground field that is no longer algebraically closed. We only have to modify the parts of the proof of Theorem 1.1 that used the fact that the ground field was algebraically closed. Theorem 4.1 needed this assumption, because we used the Tsen-Lang Theorem (Theorem 6.3) in its proof, but this theorem is the only part of the proof which relied on the assumption that we are over an algebraically closed ground field. As in the proof of Theorem 1.1 we will construct a diophantine model of the structure $\mathcal{S} = \langle\, \mathbb{Z}\times\mathbb{Z}, +, \mid, \mathcal{Z}, \mathcal{W}\,\rangle$ in $K$.

To set up some notation we will state Theorem 3.2 for higher transcendence degree.

**Theorem 5.1** (Theorem 3.2 for higher transcendence degree)**.** *Let $K$ be a finite extension of $\mathbb{C}(t_1, t_2, \dots, t_n)$, and let $R$ be as above. Let $E : y^2 = x^3 + ax+b$ be an elliptic curve with $a, b \in \mathbb{C}$, $b \neq 0$, and no complex multiplication. There exist $z_1, z_2 \in K$ such that $R(z_1, z_2)$ has transcendence degree 2 over $R$ and such that the two elliptic curves $\mathcal{E}_1 : (z_1^3 + az_1 + b)\, y^2 = x^3 + ax + b$ and $\mathcal{E}_2 : (z_2^3 + az_2 + b)\, y^2 = x^3 + ax + b$ have rank one over $K$ with generators $(z_1, 1)$ and $(z_2, 1)$, respectively (modulo 2-torsion).*

*Proof.* The proof goes through word for word as the proof of Theorem 3.2 with $\mathbb{C}$ replaced by $R$. □

As before, we let $L := K(h_1, h_2)$, where $h_i^2 = z_i^3 + az_i + b$, and we will work with the two points $P_1 := (z_1, h_1)$ and $P_2 := (z_2, h_2)$ on $E$. To prove undecidability for $K$ it is enough to prove that the existential theory of $L$ in the language $\langle\, L, +, \cdot\ ; 0, 1, z_1, z_2, h_1, h_2, S\,\rangle$ is undecidable, where $S$ is a predicate for the elements of the subfield $K$ [PZ00, Lemma 1.9]. So from now on we will work in this language. We can use the same argument as in Section 3.2 to show that the set of points $\mathbb{Z}P_1 \times \mathbb{Z}P_2 \subseteq E(L)$ is existentially definable in our language. The argument from Section 3.3 implies that the relations $+$ and $\mathcal{Z}$ are existentially definable. The only remaining part of the proof is to show that the divisibility relation $|$ is existentially definable in our language. For this we only have to prove the analogue of Theorem 4.1.

**Theorem 5.2** (Theorem 4.1 for higher transcendence degree)**.** *There exists a finite set $U \subseteq \mathbb{Z}$ such that for all $m \in \mathbb{Z} - U$ we have: for all $n, r \in \mathbb{Z}$*

$$
\begin{aligned}
&(m, 1) \mid (n, r) \Leftrightarrow \\
&\quad (\,\exists\, y_0, z_0 \in L^*\ \ x(nP_1 + rP_2)\, y_0^2 + x(mP_1 + P_2)\, z_0^2 = 1 \\
&\quad \wedge\ \exists\, y_1, z_1 \in L^*\ \ x(2nP_1 + 2rP_2)\, y_1^2 + x(mP_1 + P_2)\, z_1^2 = 1 \\
&\qquad\qquad\qquad \dots \\
&\quad \wedge\ \exists\, y_\alpha, z_\alpha \in L^*\ \ x(2^\alpha nP_1 + 2^\alpha rP_2)\, y_\alpha^2 + x(mP_1 + P_2)\, z_\alpha^2 = 1\,)\,.
\end{aligned}
$$

*Proof.* For the first implication, assume that $(m, 1) \mid (n, r)$, *i.e.* $n = mr$. Let $K' := \mathbb{C}(x(mP_1 + P_2), y(mP_1 + P_2))$. As in the proof of Theorem 4.1, both $x(nP_1 + rP_2) = x(r(mP_1 + P_2))$ and $x(mP_1 + P_2)$ are elements of $K'$, which has transcendence degree one over $\mathbb{C}$. This means that we can apply the Tsen-Lang Theorem (Theorem 6.3 in the appendix) with $K = K'$ to the quadratic form

$$x(nP_1 + rP_2)y^2 + x(mP_1 + P_2)z^2 - w^2$$

to conclude that there exists a nontrivial zero $(y, z, w)$ over $K'$ and hence that there exists a nontrivial zero $(y, z, w)$ in $K'$ with $y \cdot z \cdot w \neq 0$. Since $K' \subseteq L$, this produces the desired solution over $L^*$ for the first equation. The same can be done for the other equations.

The other implication in the proof of Theorem 4.1 does not use the fact that we have a function field over an algebraically closed field, so we can just work with our finite extension $K$ of $R(z_1, z_2)$ and with $L$ as defined above, and repeat this part of the proof word for word with $\mathbb{C}$ replaced by $R$. □

The rest of the proof is word for word the same as in the transcendence degree 2 case showing that the relation $|$ is existentially definable and thus completing the proof of Theorem 1.2.

## 6. Appendix

In this section we will state and prove some general theorems which were used to prove that the relation $|$ is diophantine.

**Theorem 6.1.** *Let $L$ and $K$ be function fields of one variable with constant fields $C_L$ and $C_K$, respectively, such that $L$ is an extension of $K$. If $L$ is separably algebraic over $K$, then there are at most a finite number of places of $L$ which are ramified over $K$.*

*Proof.* This theorem is proved on p. 111 of [Deu73] when $C_L \cap K = C_K$, and the general theorem also follows. □

We also need the following easy lemma.

**Lemma 6.2.** *Let $k$ be a field, and let $v : k^* \twoheadrightarrow \mathbb{Z}$ be a discrete valuation on $k$. Let $a, b \in k$ with $v(a) = 0$ and $v(b)$ odd. Suppose that $ax^2 + by^2 = 1$ has a solution in $k^*$. Then $a$ is a square in the residue field of $k$.*

*Proof.* The equation $ax^2 + by^2 = 1$ implies that $v(ax^2 + by^2) = 0$. The condition $v(a) = 0$ implies that $v(ax^2)$ is even. Since $v(b)$ is odd, it follows that $v(by^2)$ is odd. Hence $v(ax^2) = 0$ and $v(by^2) > 0$. So in the residue field our equation becomes $\bar{a} \cdot \bar{x}^2 + 0 \equiv 1 \mod v$. This implies that $a$ is a square in the residue field. □

**Theorem 6.3.** *Tsen-Lang Theorem. Let $K$ be a function field of transcendence degree $j$ over an algebraically closed field $k$. Let $f_1, \cdots, f_r$ be forms in $n$ variables over $K$, of degrees $d_1, \cdots, d_r$. If*

$$n > \sum_{i=1}^{r} d_i^j$$

*then the system $f_1 = \cdots = f_r = 0$ has a non-trivial zero in $K^n$.*

*Proof.* This is proved in Proposition 1.2 and Theorem 1.4 in Chapter 5 of [Pfi95]. □

**Lemma 6.4.** *Let $F, G$ be fields of characteristic $\neq 2$, and let $G/F$ be a field extension of degree $r$. Then the cardinality of $V := [(G^*)^2 \cap F^*]/(F^*)^2$ is bounded by $r$.*

*Proof.* The set $V$ is a vector space over $\mathbb{F}_2$. If we have $s$ elements of $(G^*)^2 \cap F^*$ whose images in $V$ are linearly independent, then by a theorem of Kummer theory ([Lan93], Theorem 8.1, p. 294) the square roots of these elements will generate a field extension of degree $2^s$. This extension is contained in $G$. So $\operatorname{card}(V) = 2^{\dim V} \leq r$. □

## References

[Cre97] J. E. Cremona. *Algorithms for modular elliptic curves.* Cambridge University Press, Cambridge, second edition, 1997.

[Den78] Jan Denef. The Diophantine problem for polynomial rings and fields of rational functions. *Trans. Amer. Math. Soc.*, 242:391–399, 1978.

[Deu73] Max Deuring. *Lectures on the theory of algebraic functions of one variable.* Springer-Verlag, Berlin, 1973. Lecture Notes in Mathematics, Vol. 314.

[Eis03] Kirsten Eisenträger. Hilbert's Tenth Problem for algebraic function fields of characteristic 2. *Pacific J. Math.*, (210):261–281, 2003.

[KR92] K. H. Kim and F. W. Roush. Diophantine undecidability of $\mathbf{C}(t_1, t_2)$. *J. Algebra*, 150(1):35–44, 1992.

[Lan93] Serge Lang. *Algebra.* Springer-Verlag, New York, third edition, 1993.

[Mat70] Yu. V. Matijasevič. The Diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*, 191:279–282, 1970.

[MB03] Laurent Moret-Bailly. Elliptic curves and Hilbert's Tenth Problem for function fields of characteristic zero. Preprint. December 4, 2003.

[Pfi95] Albrecht Pfister. *Quadratic forms with applications to algebraic geometry and topology*, volume 217 of *London Mathematical Society Lecture Note Series.* Cambridge University Press, Cambridge, 1995.

[Poo03] Bjorn Poonen. Hilbert's tenth problem and Mazur's conjecture for large subrings of $\mathbb{Q}$. *J. Amer. Math. Soc.*, 16(4):981–990 (electronic), 2003.

[PZ00] Thanases Pheidas and Karim Zahidi. Undecidability of existential theories of rings and fields: a survey. In *Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999)*, pages 49–105. Amer. Math. Soc., Providence, RI, 2000.

[Shl96] Alexandra Shlapentokh. Diophantine undecidability over algebraic function fields over finite fields of constants. *J. Number Theory*, 58(2):317–342, 1996.

[Shl00] Alexandra Shlapentokh. Hilbert's tenth problem for algebraic function fields over infinite fields of constants of positive characteristic. *Pacific J. Math.*, 193(2):463–500, 2000.

[Vid94] Carlos R. Videla. Hilbert's tenth problem for rational function fields in characteristic 2. *Proc. Amer. Math. Soc.*, 120(1):249–253, 1994.

School of Mathematics, Institute for Advanced Study, Einstein Drive, Princeton, NJ 08540, USA

*E-mail address*: eisentra@ias.edu