HILBERT'S TENTH PROBLEM FOR FUNCTION FIELDS OF CHARACTERISTIC ZERO

KIRSTEN EISENTRÄGER

ABSTRACT. In this article we outline the methods that are used to prove undecidability of Hilbert's Tenth Problem for function fields of characteristic zero. Following Denef we show how rank one elliptic curves can be used to prove undecidability for rational function fields over formally real fields. We also sketch the undecidability proofs for function fields of varieties over the complex numbers of dimension at least 2.

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]), based on work by Davis, Putnam and Robinson ([DPR61]), proved that no such algorithm exists, *i.e.* Hilbert's Tenth Problem is undecidable. Since then, analogues of this problem have been studied by asking the same question for polynomial equations with coefficients and solutions in other commutative rings R. We will refer to this as *Hilbert's Tenth Problem over* R. Perhaps the most important unsolved question in this area is the case $R = \mathbb{Q}$. 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 ([Phe91]) for $k = \mathbb{F}_q(t)$with q odd, and by Videla ([Vid94]) for $\mathbb{F}_q(t)$ with q even. Shlapentokh ([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]). Kim and Roush ([KR92]) showed that the problem is undecidable for the purely transcendental function fields

$\mathbb{C}(t_1, t_2)$ and $\overline{\mathbb{F}}_p(t_1, t_2)$. In [Eis04] this was generalized to finite extensions of $\mathbb{C}(t_1, \ldots, t_n)$ with $n \geq 2$. The problem is also known to be undecidable for function fields over p-adic fields ([KR95], [Eis06], [MB05]). In Hilbert's Tenth Problem the coefficients of the equations have to be input into a Turing machine, so when we consider the problem for uncountable rings we restrict the coefficients to a subring R' of R which is finitely generated as a $\mathbb{Z}$-algebra. We say that *Hilbert's Tenth Problem for R with coefficients in R'* is undecidable if there is no algorithm that decides whether or not multivariate polynomial equations with coefficients in R' have a solution in R. In this paper we will discuss the undecidability proofs for $\mathbb{R}(t)$, and $\mathbb{C}(t_1, t_2)$. In these cases, we consider polynomials with coefficients in $\mathbb{Z}[t]$ and $\mathbb{Z}[t_1, t_2]$, respectively.

The biggest open problems for function fields are Hilbert's Tenth Problem for $\mathbb{C}(t)$ and for $\overline{\mathbb{F}}_p(t)$.

2. Approach for function fields of characteristic zero

2.1. **Preliminaries.** Before we can describe the approach that is used in characteristic zero we need the following definition. All the rings we consider are commutative with 1.

Definition 1. Let R be a ring. A subset $Q \subseteq R^k$ is *diophantine over R* if there exists a polynomial $f(x_1, \ldots, x_k, y_1, \ldots, y_m) \in R[x_1, \ldots, x_k, y_1, \ldots, y_m]$ such that

$$Q = \{\vec{x} \in R^k : \exists\, y_1, \ldots, y_m \in R : f(\vec{x}, y_1, \ldots, y_m) = 0\}.$$

Let R' be a subring of R and suppose that f can be chosen such that its coefficients are in R'. Then we say that Q is *diophantine over R with coefficients in R'*.

Example 1. The set of natural numbers $\mathbb{N}$ is diophantine over $\mathbb{Z}$. This follows from the fact that every natural number can be written as a sum of four squares, so

$$\mathbb{N} = \{a \in \mathbb{Z} : \exists\, y_1, \ldots, y_4 \in \mathbb{Z} : (y_1^2 + y_2^2 + y_3^2 + y_4^2 - a = 0)\}.$$

Example 2. The set of primes is diophantine over $\mathbb{Z}$. This follows from the proof of Hilbert's Tenth Problem for $\mathbb{Z}$, where it was shown that every recursively enumerable subset of $\mathbb{Z}$ is diophantine over $\mathbb{Z}$ ([DPR61, Mat70]). Clearly the prime numbers form a recursively enumerable subset of $\mathbb{Z}$.

2.2. **Combining diophantine equations.** If K is a formally real field and $P_1 = 0$, $P_2 = 0$ are two diophantine equations over $K(t)$ with coefficients in $\mathbb{Z}[t]$, then $P_1 = 0 \wedge P_2 = 0$ and $P_1 = 0 \vee P_2 = 0$ are also diophantine with coefficients in $\mathbb{Z}[t]$: we have

$$P_1 = 0 \wedge P_2 = 0 \leftrightarrow P_1^2 + tP_2^2 = 0$$

and

$$P_1 = 0 \vee P_2 = 0 \leftrightarrow P_1 P_2 = 0.$$

The same holds for diophantine equations over $\mathbb{C}(t_1, t_2)$ with coefficients in $\mathbb{Z}[t_1, t_2]$:

$$P_1 = 0 \wedge P_2 = 0 \leftrightarrow P_1^2 + t_1 P_2^2 = 0 \text{ and } P_1 = 0 \vee P_2 = 0 \leftrightarrow P_1 P_2 = 0.$$

An argument similar to the one above can be made for many other rings whose quotient field is not algebraically closed, provided that the ring of coefficients is large enough.

The above argument shows that proving undecidability of Hilbert's Tenth Problem for $K(t)$ with coefficients in $\mathbb{Z}[t]$ is the same as proving that the positive existential theory of $K(t)$ in the language $\langle +, \cdot\, ; 0, 1, t\rangle$ is undecidable. Similarly, Hilbert's Tenth Problem for $\mathbb{C}(t_1, t_2)$ with coefficients in $\mathbb{Z}[t_1, t_2]$ is undecidable if and only if the positive existential theory of $\mathbb{C}(t_1, t_2)$ in the language $\langle +, \cdot\, ; 0, 1, t_1, t_2\rangle$ is undecidable.

2.3. **Approach in characteristic zero.** We can use a reduction argument to prove undecidability for a ring R of characteristic zero if we can give a diophantine definition of $\mathbb{Z}$ inside R. We have the following proposition:

Proposition 2.1. *Let R be an integral domain of characteristic zero. Let R' be a subring of R, which is finitely generated as a $\mathbb{Z}$-algebra and such that the fraction field of R does not contain an algebraic closure of R'. Assume that $\mathbb{Z}$ is a diophantine subset of R with coefficients in R'. Then Hilbert's Tenth Problem for R with coefficients in R' is undecidable.*

Proof. Given a polynomial equation $f(x_1, \dots, x_n) = 0$ over $\mathbb{Z}$ we can construct a system of polynomial equations over R with coefficients in R' by taking the original equation together with, for each $i = 1, \dots, n$ an equation $g_i(x_i, \dots) = 0$ involving x_i and a new set of variables, such that in any solution over R of the system, $g_i = 0$ forces x_i to be in $\mathbb{Z}$. In other words, the new system of equations has a solution over R if and only $f(x_1, \dots, x_n)$ has a solution in $\mathbb{Z}$. Also, since the quotient field of R does not contain the algebraic closure of R', the system over R with coefficients in R' is equivalent to a single polynomial equation with coefficients in R' ([PZ00, p. 51]). □

Sometimes we cannot give a diophantine definition of the integers inside a ring R, but we might be able to construct a model of the integers inside R.

Definition 2. A *diophantine model* of $\langle \mathbb{Z}, 0, 1; +, \cdot \rangle$ over R is a diophantine subset $S \subseteq R^m$ equipped with a bijection $\phi : \mathbb{Z} \to S$ such that under ϕ, the graphs of addition and multiplication correspond to diophantine subsets of S^3.

Let R' be a subring of R. A *diophantine model* of $\langle \mathbb{Z}, 0, 1; +, \cdot \rangle$ over R *with coefficients in* R' is a diophantine model of $\langle \mathbb{Z}, 0, 1; +, \cdot \rangle$, where in addition S and the graphs of addition and multiplication are diophantine over R with coefficients in R'.

A similar argument as for Proposition 2.1 can be used to prove the following

Proposition 2.2. *Let R, R' be as in Proposition 2.1. If we have a diophantine model of $\langle \mathbb{Z}, 0, 1; +, \cdot \rangle$ over R with coefficients in R', then Hilbert's Tenth Problem for R with coefficients in R' is undecidable.*

3. Fields of rational functions over formally real fields

In this section we will give an outline of Denef's theorem:

Theorem 3.1 ([Den78])**.** *Let K be a formally real field, i.e. -1 is not the sum of squares. Hilbert's Tenth Problem for $K(t)$ with coefficients in $\mathbb{Z}[t]$ is undecidable.*

We follow Denef's proof and use elliptic curves to construct a model of $\langle \mathbb{Z}, 0, 1; +, \cdot \rangle$ in $K(t)$. Denef actually gives a diophantine definition of $\mathbb{Z}$ inside $K(t)$, but we will construct a model of the integers, because this approach is slightly shorter and it is used in subsequent papers ([KR92],[KR95], [Eis06]).

To construct the diophantine model of the integers we first have to obtain a set S which is diophantine over $K(t)$ and which has a natural bijection to $\mathbb{Z}$.

3.1. **Obtaining S.** Let E be an elliptic curve defined over $\mathbb{Q}$ without complex multiplication and with Weierstrass equation

$$y^2 = x^3 + ax + b. \tag{1}$$

The points (x, y) satisfying equation (1) together with the point at infinity form an abelian group, and the group law is given by equations. We will now look at a twist of E, the elliptic curve $\mathcal{E}$, which is defined to be the smooth projective model of

$$(t^3 + at + b)Y^2 = X^3 + aX + b.$$

This is an elliptic curve defined over the rational function field $\mathbb{Q}(t)$. An obvious point on $\mathcal{E}$ which is defined over $\mathbb{Q}(t)$ is the point $P_1 := (t, 1)$. Denef proved:

Theorem 3.2. [Den78, p. 396] *The point P_1 has infinite order and generates the group $\mathcal{E}(K(t))$ modulo points of order 2.*

The elliptic curve $\mathcal{E}$ 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

$$\mathcal{E}(K(t)) = \{(X, Y) : X, Y \in K(t) \wedge (t^3+at+b)Y^2 = X^3+aX+b\} \cup \{\mathbf{O}\}$$

is diophantine over $K(t)$, since we can take care of the point at infinity $\mathbf{O}$ of $\mathcal{E}$.

We can express by polynomial equations that a point on the elliptic curve is of the form $2 \cdot P$, where P is another point on the curve. Hence the set

$$\begin{aligned} S' =& \{(X_{2n}, Y_{2n}) : n \in \mathbb{Z}\} \\ =& \{(x, y) \in (K(t))^2 : \\ & \exists\, u, v \in K(t) : (u, v) \in \mathcal{E}(K(t)) \wedge (x, y) = 2(u, v)\} \end{aligned}$$

is diophantine over $K(t)$ with coefficients in $\mathbb{Z}[t]$. Then the set

$$\begin{aligned} S'' &= \{(X_n, Y_n) : n \in \mathbb{Z}\} \\ &= \{(x, y) \in (K(t))^2 : \exists\, n \in \mathbb{Z} : \\ &\quad ((x, y) = (X_{2n}, Y_{2n}) \vee (x, y) = (X_{2n}, Y_{2n}) + P_1)\} \end{aligned}$$

is diophantine over $K(t)$ with coefficients in $\mathbb{Z}[t]$ as well.

Let $P_n := n \cdot (t, 1) = (X_n, Y_n)$ for $n \in \mathbb{Z} - \{0\}$, and let $P_0 := \mathbf{O}$. The set $S' \cup S''$ is equal to the set $\{P_n : n \in \mathbb{Z}\}$. Let $Z_n := \frac{X_n}{tY_n}$ for $n \in \mathbb{Z} - \{0\}$, and let $Z_0 := 0$. We define S to be the set

$$S = \{Z_n : n \in \mathbb{Z}\}.$$

Then S is diophantine over $K(t)$. Since $Z_n \in \mathbb{Q}(t)$, we can consider Z_n as a function on the projective line $\mathbf{P}^1_{\mathbb{Q}} = \mathbb{Q} \cup \{\infty\}$. Denef ([Den78, p. 396]) proved the following proposition:

Proposition 3.3. *Considered as a function on $\mathbf{P}^1_{\mathbb{Q}}$, Z_n takes the value n at infinity.*

For $n \neq m$, we have $Z_n \neq Z_m$, and so by associating the point Z_n to an integer n we obtain an obvious bijection between $\mathbb{Z}$ and S. This is the set that we will use for the diophantine model of $\langle \mathbb{Z}, 0, 1; +, \cdot \rangle$.

3.2. **Existentially defining multiplication and addition.** The bijection $\phi : \mathbb{Z} \to S$ given by $\phi(n) = Z_n$ induces multiplication and addition laws on the set S, and it remains to show that the graphs of addition and multiplication on S are diophantine over $K(t)$. This means that we have to show that the sets

$$S_{add} := \{(Z_n, Z_m, Z_\ell) \in S^3 : n + m = \ell\}$$

and

$$S_{mult} := \{(Z_n, Z_m, Z_\ell) \in S^3 : n \cdot m = \ell\}$$

are diophantine over $K(t)$. Since addition of points on the elliptic curve is given by equations involving rational functions of the coordinates of the points, it follows easily that the set S_{add} is diophantine over $K(t)$:

$$Z_n + Z_m = Z_\ell \leftrightarrow \exists (X, Y), (X', Y'), (X'', Y'') \in \mathcal{E}(K(t)) :$$
$$\left(Z_n = \frac{X}{tY}, Z_m = \frac{X'}{tY'}, Z_\ell = \frac{X''}{tY''} \wedge (X, Y) + (X', Y') = (X'', Y'') \right).$$

The difficult part is showing that S_{mult} is diophantine.

3.3. **Defining multiplication.** We define the discrete valuation $\mathrm{ord}_{t^{-1}} : K(t) \to \mathbb{Z} \cup \{\infty\}$ by $\mathrm{ord}_{t^{-1}} u = -\deg f + \deg g$, for $u \in K(t)^*$, $u = f/g$ with $f, g \in K[t]$. We let $\mathrm{ord}_{t^{-1}}(0) = \infty$. Proposition 3.3 implies that for $n \neq 0$, $\mathrm{ord}_{t^{-1}}(Z_n) = 0$ and $\mathrm{ord}_{t^{-1}}(Z_n - n) > 0$.

The discrete valuation $\mathrm{ord}_{t^{-1}}$ has the following properties: For $u \in K(t)$ we have

(1) $\mathrm{ord}_{t^{-1}}(u) = 0$ if and only if u takes a nonzero value $a \in K$ at infinity.
(2) $\mathrm{ord}_{t^{-1}}(u) > 0$ if and only if u takes the value zero at infinity.
(3) $\mathrm{ord}_{t^{-1}}(u) < 0$ if and only if u takes the value infinity at infinity.

We will use the discrete valuation $\mathrm{ord}_{t^{-1}}$ to existentially define multiplication of elements of S. This is done in the following theorem.

Theorem 3.4. *Assume that the set $T' := \{u \in K(t) : \mathrm{ord}_{t^{-1}}(u) > 0\}$ is diophantine over $K(t)$. Then the set S_{mult} is diophantine over $K(t)$, i.e. we can existentially define multiplication of elements of S.*

Proof. The theorem follows immediately from the following claim.
Claim: Given $n, m, \ell \in \mathbb{Z}$ we have $n \cdot m = \ell$ if and only if $Z_n \cdot Z_m - Z_\ell \in T'$, *i.e.*

$$\mathrm{ord}_{t^{-1}}(Z_n \cdot Z_m - Z_\ell) > 0.$$

Proof of Claim: If $n \cdot m = \ell$, then by Proposition 3.3, $Z_n \cdot Z_m - Z_\ell$ takes the value $n \cdot m - \ell = 0$ at infinity, and hence $\mathrm{ord}_{t^{-1}}(Z_n \cdot Z_m - Z_\ell) > 0$.

If $n \cdot m \neq \ell$, then $Z_n \cdot Z_m - Z_\ell$ takes the value $n \cdot m - \ell \neq 0$ at infinity. Hence $\mathrm{ord}_{t^{-1}}(Z_n \cdot Z_m - Z_\ell) = 0$. This proves the claim.

Since we assumed that the set T' of all elements with positive valuation at t^{-1} was diophantine over $K(t)$ this proves the theorem. □

Remark 1. We can modify the set T' and still make the proof of Theorem 3.4 work. What we needed in the proof was a diophantine set T with the following properties:

(1) If $Z \in \mathbb{Q}(t)$ and $\mathrm{ord}_{t^{-1}}(Z) > 0$, then $Z \in T$.
(2) If $Z \in K(t)$ and $Z \in T$, then $\mathrm{ord}_{t^{-1}}(Z) > 0$.

This is enough because the functions Z_n are elements of $\mathbb{Q}(t)$.

3.4. **How to obtain a diophantine definition for T.** We will now define the set T that has the properties in Remark 1. By Theorem 3.4 this is enough to finish the proof of Theorem 3.1.

Consider the relation $\mathrm{Com}(y)$ defined by

$$\mathrm{Com}(y) \leftrightarrow y \in K(t) \wedge \exists\, x \in K(t) : y^2 = x^3 - 4.$$

Since $y^2 = x^3 - 3$ is a curve of genus 1, it does not admit a rational parameterization, and so if an element y satisfies $\mathrm{Com}(y)$, then y lies in K. Also, Denef ([Den78]) showed that for every rational number z, there exists a rational number $y > z$ satisfying $\mathrm{Com}(y)$. We are now ready to define the set T.

Theorem 3.5. *Define the set T by*

$$\begin{aligned} Z \in T \leftrightarrow\ & \exists\, X_1, \ldots, X_5, y \in K(t) : \\ & (\mathrm{Com}(y) \wedge \\ & (y - t)Z^2 + 1 = X_1^2 + X_2^2 + \cdots + X_5^2\big)\,. \end{aligned} \tag{2}$$

Then T has the properties as in Remark 1.

Proof. We follow the proof in [Den78]: We will first show that every element $Z \in T$ has positive order at t^{-1}.

Suppose there exist $X_1, \ldots, X_5, y$ in $K(t)$ as in Equation (2), and assume by contradiction that $\mathrm{ord}_{t^{-1}}(Z) \leq 0$. Then $\deg Z \geq 0$, where $\deg Z$ denotes the degree of the rational function Z. Since y satisfies $\mathrm{Com}(y)$, we have $y \in K$, which implies that $\deg(y - t) = 1$, and so $\deg((y - t)Z^2 + 1)$ is positive and odd. But the degree of the rational function $X_1^2 + \ldots X_5^2$ is even, since in a formally real field, a sum of squares is zero if and only if each term is zero, and hence there is no cancellation of the coefficients of largest degree. Hence the left-hand-side of (2) has odd degree, while the right-hand-side has even degree, contradiction.

To show that the set T satisfies the second property, let $Z \in \mathbb{Q}(t)$, and assume $\mathrm{ord}_{t^{-1}}(Z) > 0$. We want to show that $Z \in T$. Since $\mathrm{ord}_{t^{-1}}(Z) > 0$, we have $\mathrm{ord}_{t^{-1}}(tZ^2) > 0$, and so $tZ^2(r) \to 0$ as $|r| \to \infty$ ($r \in \mathbb{R}$). Hence we can find a natural number n, such that for real numbers r with $|r| > n$, we have $|tZ^2(r)| \leq 1/2$. Pick a rational number y with $y > n > 0$ and satisfying $\mathrm{Com}(y)$. Such a y exists by the discussion before Theorem 3.5. Then

$$\left((y-t)Z^2+1\right)(r) = yZ^2(r) - tZ^2(r) + 1 \geq yZ^2(r) - 1/2 + 1 > 0$$

for all $r \in \mathbb{R}$. By Pourchet's theorem, every positive definite rational function over $\mathbb{Q}$ can be written as a sum of five squares in $\mathbb{Q}(t)$. Hence there exist $X_1, \ldots, X_5 \in K(t)$ as desired. □

4. Function fields over the complex numbers in two variables

Unfortunately, the diophantine definition of the set T which defined the elements of positive order at t^{-1} and which was crucial for the proof of Theorem 3.1 only works for formally real fields.

For $\mathbb{C}(t_1, t_2)$ and finite extensions we will do something else that avoids defining order.

4.1. **Hilbert's Tenth for the rational function field $\mathbb{C}(t_1, t_2)$.** In this section we will outline the proof of the following

Theorem 4.1 ([KR92])**.** *Hilbert's Tenth Problem for $\mathbb{C}(t_1, t_2)$ with coefficients in $\mathbb{Z}[t_1, t_2]$ is undecidable.*

To prove undecidability of Hilbert's Tenth Problem for $K := \mathbb{C}(t_1, t_2)$ we will construct a diophantine model of the structure

$$\mathcal{S} := \langle \mathbb{Z} \times \mathbb{Z}, +, |, \mathcal{Z}, \mathcal{W} \rangle$$

in K (with coefficients in $\mathbb{Z}[t_1, t_2]$). 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 ϕ, 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.

A *diophantine model* of $\mathcal{S}$ over K with coefficients in $\mathbb{Z}[t_1, t_2]$ is a model, where in addition S and the graphs of addition, $|$, $\mathcal{Z}$, and $\mathcal{W}$ are diophantine over K with coefficients in $\mathbb{Z}[t_1, t_2]$.

We will now 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 4.2. ([Eis04]) *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 positive existential theory:

Proposition 4.3. *The structure $\mathcal{S}$ has an undecidable positive 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 positive existential theory as well. □

The above proposition shows that in order to prove Theorem 4.1 it is enough to construct a diophantine model of $\mathcal{S}$ over K with coefficients in $\mathbb{Z}[t_1, t_2]$. In the next section we will construct this model.

4.2. **Generating Elliptic Curves of Rank One.** As before, let $K := \mathbb{C}(t_1, t_2)$. Our first task is to find a diophantine set A over K which is isomorphic to $\mathbb{Z} \times \mathbb{Z}$ as a set. Following Kim and Roush ([KR92]) we will obtain such a set by using the K-rational points on two elliptic curves which have rank one over K. The same argument as in Theorem 3.2 shows that the following proposition holds:

Proposition 4.4. *Let E be an elliptic curve over $\mathbb{Q}$ without complex multiplication and with Weierstrass equation $y^2 = x^3 + ax + b$, where $a, b \in \mathbb{Q}$ and $b \neq 0$. Consider the twists $\mathcal{E}_1, \mathcal{E}_2$ of E defined by*

$$\mathcal{E}_1 : (t_1^3 + at_1 + b)Y^2 = X^3 + aX + b$$

and

$$\mathcal{E}_2 : (t_2^3 + at_2 + b)Y^2 = X^3 + aX + b.$$

The point $(t_i, 1) \in \mathcal{E}_i(K)$ has infinite order for $i = 1, 2$, and $(t_i, 1)$ generates $\mathcal{E}_i(K)$ modulo points of order 2.

To be able to define a suitable set S which is isomorphic to $\mathbb{Z} \times \mathbb{Z}$ we need to work in an algebraic extension F of K. Let $F := \mathbb{C}(t_1, t_2)(h_1, h_2)$, where h_i is defined by $h_i^2 = t_i^3 + at_i + b$, for $i = 1, 2$.

To prove that the positive existential theory of K in the language $\langle +, \cdot\, ; 0, 1, t_1, t_2 \rangle$ is undecidable, it is enough to prove that the positive existential theory of F in the language $\langle +, \cdot\, ; 0, 1, t_1, t_2, h_1, h_2, \mathcal{P} \rangle$ is undecidable, where $\mathcal{P}$ is a predicate for the elements of the subfield K ([PZ00, Lemma 1.9]). So from now on we will work with equations over F.

Over F 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 $(t_1, 1)$ on $\mathcal{E}_1$ corresponds to the point $P_1 := (t_1, h_1)$ on E. Similarly there is an isomorphism between $\mathcal{E}_2$ and E that sends the point $(t_2, 1)$ on $\mathcal{E}_2$ to the point $P_2 := (t_2, h_2)$ on E.

So the element $(n, m) \in \mathbb{Z} \times \mathbb{Z}$ corresponds to the point $nP_1 + mP_2 \in E(F)$. As in Section 3.1, we can take care of the point at ∞ on the curve E.

The set of points $\mathbb{Z}P_1 \times \mathbb{Z}P_2 \subseteq E(F)$ 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 $2 \cdot \mathbb{Z}P_1$ as in Section 3.1:

$$P \in 2 \cdot \mathbb{Z}P_1 \Leftrightarrow \exists\, x, y \in K\ (t_1^3 + at_1 + b)\, y^2 = x^3 + ax + b \wedge P = 2 \cdot (x, h_1 y)$$

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 $\mathbb{Z}P_1 \times \mathbb{Z}P_2 \subseteq E(F)$ is existentially definable, since addition on E is existentially definable.

4.3. **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 $|$.

4.4. **Existential Definition of $(m,1) \mid (n,r)$.** 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. The following theorem gives the existential definition of $|$:

Theorem 4.5.

$$\begin{aligned} &\forall m \in \mathbb{Z}, n, r \in \mathbb{Z} - \{0\} : \\ (m,1) \mid (n,r) \Leftrightarrow \\ &(\exists\, z, w \in F^* \;\; x(nP_1 + rP_2)\, z^2 + x(mP_1 + P_2)\, w^2 = 1) \end{aligned}$$

Clearly this definition is existential in $(m,1)$ and (n,r). It is enough to give an existential definition of $|$ for $n, r \in \mathbb{Z} - \{0\}$, because we can handle the cases when n or r are zero separately.

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 6.2 from the appendix) to the quadratic form

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

to conclude that there exists a nontrivial zero (z,w,v) 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 (z,w,v) with $z \cdot w \cdot v \neq 0$.

For the other direction, suppose that $n \neq mr$ and assume by contradiction that there exist $z, w \in F^*$ with

$$x(nP_1 + rP_2)\, z^2 + x(mP_1 + P_2)\, w^2 = 1. \tag{3}$$

Claim: There exists a discrete valuation $w_m : F^* \twoheadrightarrow \mathbb{Z}$ such that $w_m(x(mP_1 + P_2)) = 1$ and such that $w_m(x(nP_1 + rP_2)) = 0$.
Proof of Claim: Let $P_2' = mP_1 + P_2 = (t_2', h_2')$. Remember that $F = \mathbb{C}(t_1, t_2, h_1, h_2)$. Then

$$F = \mathbb{C}(t_1, t_2, h_1, h_2) = \mathbb{C}(t_1, h_1, t_2', h_2') = \mathbb{C}(x(P_1), y(P_1), x(P_2'), y(P_2')),$$

since $t_2 = x(P_2' - mP_1)$ and $h_2 = y(P_2' - mP_1)$.

Now let $w_m : F^* \twoheadrightarrow \mathbb{Z}$ be a discrete valuation which extends the discrete valuation w of $\mathbb{C}(t_1, h_1)(t_2')$ associated to t_2'. The valuation w is the discrete valuation that satisfies $w(\gamma) = 0$ for all $\gamma \in \mathbb{C}(t_1, h_1)$ and $w(t_2') = 1$.

Let $s := n - mr$. By assumption $s \neq 0$. We have $nP_1 + rP_2 = sP_1 + rP_2'$. The residue field of w_m is $\mathbb{C}(t_1, h_1)$. Let $x_{s,r}$ denote the image of $x(sP_1 + rP_2')$ in the residue field of w_m. Then $x_{s,r} = x\left(s(t_1, h_1) + r(0, \pm\sqrt{b})\right)$. 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 $(t_1, h_1) \in E(\mathbb{C}(t_1, h_1))$ has infinite order, t_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 $x\left(s(t_1, h_1) + r(0, \pm\sqrt{b})\right) \neq 0$. This proves the claim.

Since z, w satisfy Equation (3) it easily follows that $x_{s,r}$ is a square in the residue field. This will give us a contradiction:

We have $x_{s,r} = x\left(s(t_1, h_1) + r(0, \pm\sqrt{b})\right)$. Since the residue field of w_m is $\mathbb{C}(t_1, h_1)$, which is the function field of E, we can consider $x_{s,r}$ as a function $E \to \mathbf{P}^1_{\mathbb{C}}$. 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. In particular, it is not a square in $\mathbb{C}(t_1, h_1)$. This completes the proof of the theorem. □

5. Generalization to finite extensions of $\mathbb{C}(t_1, t_2)$

In [Eis04] we proved the following theorem.

Theorem 5.1. *Let L be the function field of a surface over the complex numbers. There exist $z_1, z_2 \in L$ that generate an extension of transcendence degree 2 of $\mathbb{C}$ and such that Hilbert's Tenth Problem for L with coefficients in $\mathbb{Z}[z_1, z_2]$ is undecidable.*

Remark 2. This theorem also holds for transcendence degree ≥ 2, *i.e.* for finite extensions of $\mathbb{C}(t_1, \ldots, t_n)$, with $n \geq 2$, and the proof of the more general theorem can also be found in [Eis04]. To make our exposition as short as possible and to avoid extra notation, we will only discuss the transcendence degree 2 case here.

Our proof will proceed as the proof for $\mathbb{C}(t_1, t_2)$, *i.e.* we will construct a diophantine model of $\langle \mathbb{Z} \times \mathbb{Z}, +, |, \mathcal{Z}, \mathcal{W} \rangle$ in L. We will now give an outline of the steps that are needed in the proof.

5.1. **Finding suitable elliptic curves of rank one.** In the above undecidability proof for $\mathbb{C}(t_1, t_2)$ ([KR92]) we obtained a set that was in bijection with $\mathbb{Z} \times \mathbb{Z}$ by using the $\mathbb{C}(t_1, t_2)$-rational points on two elliptic curves which have rank one over $\mathbb{C}(t_1, t_2)$. However, the two elliptic curves that we used in Section 4.2 could have a rank higher than one over L, so we need to construct two new elliptic curves which will have rank one over L.

To do this we use a theorem by Moret-Bailly ([MB05, Theorem 1.8]):

Theorem 5.2. *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 be an elliptic curve over k with Weierstrass equation $y^2 = x^3 + ax + b$ where $a, b \in k$ and $b \neq 0$. Let $f \in F$ be admissible for E, Q. For $\lambda \in k^*$ consider the twist $\mathcal{E}_{\lambda f}$ of E which is defined to be the smooth projective model of*

$$\left((\lambda f)^3 + a(\lambda f) + b\right) y^2 = x^3 + ax + b.$$

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 λf is an isomorphism for infinitely many $\lambda \in \mathbb{Z}$.

We will not define here what it means to be admissible, but we will only state that given C, E, Q as above, admissible functions exists, and if f is admissible for C, E, Q, then for all but finitely many $\lambda \in k^*$, λf is still admissible.

Now we can state our theorem that allows us to obtain two suitable elliptic curves of rank one over L:

Theorem 5.3. *Let L be a finite extension of $\mathbb{C}(t_1, t_2)$. Let $E/\mathbb{C}$ be an elliptic curve with Weierstrass equation*

$$y^2 = x^3 + ax + b,$$

where $a, b \in \mathbb{C}$, $b \neq 0$. Assume that E does not have complex multiplication. There exist $z_1, z_2 \in L$ such that $\mathbb{C}(z_1, z_2)$ has transcendence degree 2 over $\mathbb{C}$ and such that the two elliptic curves $\mathcal{E}_1, \mathcal{E}_2$ given by the affine equations $\mathcal{E}_1 : (z_1^3 + az_1 + b)\, y^2 = x^3 + ax + b$ and $\mathcal{E}_2 : (z_2^3 + az_2 + b)\, y^2 = x^3 + ax + b$ have rank one over L with generators $(z_1, 1)$ and $(z_2, 1)$, respectively (modulo 2-torsion).

Proof. This is proved in [Eis04]. In the proof we apply Theorem 5.2 with k chosen to be the algebraic closure of $\mathbb{C}(t_2)$ inside L. □

5.2. **Diophantine definition of the relation $|$.** To existentially define the relation $|$, we need an elliptic curve E as in Theorem 5.3 with the additional property that the point $(0, \sqrt{b})$ has infinite order. So from now on we fix E to be the smooth projective model of $y^2 = x^3 + x + 1$. This curve does not have complex multiplication, and the point $(0, 1)$ has infinite order (see the curve 496A1 in [Cre97]). We fix z_1, z_2 as in Theorem 5.3.

As before, let $F := \mathbb{C}(z_1, z_2)(h_1, h_2)$, where h_i is defined by $h_i^2 = z_i^3 + az_i + b$, for $i = 1, 2$. Let $M := L(h_1, h_2)$. Over M, the elliptic curves $\mathcal{E}_1$ and $\mathcal{E}_2$ are isomorphic to E. Let $P_1 := (z_1, h_1)$, $P_2 := (z_2, h_2)$ be the two points on E as before. From now on we will work with equations over M. To give a diophantine definition we would like to prove an analogue of Theorem 4.5. To make this theorem work we have to introduce extra equations.

Let $\alpha := [M : F]$. We have the following theorem:

Theorem 5.4. [Eis04] *There exists a finite set $U \subseteq \mathbb{Z}$ such that for all $m \in \mathbb{Z} - U$ we have: for all $n, r \in \mathbb{Z} - \{0\}$*

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

Outline of Proof. By the same argument as in the proof of Theorem 4.5, if $n = mr$, then the $\alpha + 1$ equations can all be satisfied.

For the other direction, the exceptional set U is necessary here because as in the proof for $\mathbb{C}(t_1, t_2)$, for each m, we construct a discrete valuation $w_m : M^* \twoheadrightarrow \mathbb{Z}$. This valuation w_m extends a certain other discrete valuation $v_m : F^* \twoheadrightarrow \mathbb{Z}$. We have to exclude all integers m, for which $w_m | v_m$ is ramified, and we define U to be this set of integers. Then U is finite by Theorem 6.1 from the appendix.

Assume that $n \neq mr$, and let $s := n - mr$. Assume by contradiction that we can satisfy all $\alpha + 1$ equations. We can show that for all $m \in \mathbb{Z} - U$ there exists a discrete valuation $w_m : M^* \twoheadrightarrow \mathbb{Z}$ such that $w_m(x(mP_1 + P_2)) = 1$ and such that $w_m(x(knP_1 + krP_2)) = 0$ for $k = 1, 2, 4, \ldots, 2^\alpha$. Let $P_2' = mP_1 + P_2$, and denote by $x_{s,r}$ the image of $x(sP_1 + rP_2') = x(nP_1 + rP_2)$ in the residue field ℓ of w_m. The proof of Theorem 5.4 proceeds by first showing that the elements $x_{s,r}\ ,\ \ldots,\ x_{2^\alpha s\,,\,2^\alpha r}$ are not squares in $\mathbb{C}(z_1, h_1)$, and then by proving

that the images of $x_{s,r}, \ldots, x_{2^{\alpha}s,2^{\alpha}r}$ in

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

But using Kummer theory one can show that since $[\ell : \mathbb{C}(z_1, h_1)] \leq \alpha$, the size of V is bounded by α as well. This gives us the desired contradiction. □

Once we have Theorem 5.4, it is easy to define the relation $|$ for all $m \in \mathbb{Z}$ as follows:

Let m_0 be a fixed element in $\mathbb{Z} - U$, 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

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

and we can just work with that formula instead. So

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

It is an easy exercise to show that $\mathcal{W}$ is existentially definable using Theorem 5.4. Since m_0 is a fixed integer, this together with Theorem 5.4 implies that the last expression is existentially definable in $(m, 1)$ and (n, r).

6. Appendix

In this section we state two theorems that we needed in Sections 4 and 5.

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. □

Theorem 6.2. *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]. □

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.

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson. The decision problem for exponential diophantine equations. *Ann. of Math. (2)*, 74:425–436, 1961.

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

[Eis04] Kirsten Eisenträger. Hilbert's Tenth Problem for function fields of varieties over $\mathbf{C}$. *Int. Math. Res. Not.*, 59:3191–3205, 2004.

[Eis06] Kirsten Eisenträger. Hilbert's Tenth Problem for function fields of varieties over number fields and p-adic fields. To appear in *J. Algebra*, 2006.

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

[KR95] K. H. Kim and F. W. Roush. Diophantine unsolvability over p-adic function fields. *J. Algebra*, 176(1):83–110, 1995.

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

[MB05] Laurent Moret-Bailly. Elliptic curves and Hilbert's Tenth Problem for algebraic function fields over real and p-adic fields. *J. Reine Angew. Math.*, 587:77–143, 2005.

[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.

[Phe91] Thanases Pheidas. Hilbert's tenth problem for fields of rational functions over finite fields. *Invent. Math.*, 103(1):1–8, 1991.

[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.

[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.