HILBERT'S TENTH PROBLEM FOR FUNCTION FIELDS OF VARIETIES OVER ALGEBRAICALLY CLOSED FIELDS OF POSITIVE CHARACTERISTIC

KIRSTEN EISENTRÄGER

ABSTRACT. Let K be the function field of a variety of dimension ≥ 2 over an algebraically closed field of odd characteristic. 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 $\overline{\mathbb{F}}_p(t_1, t_2)$ 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 other commutative rings R. We will refer to this as *Hilbert's Tenth Problem over R.*

While the problem over $\mathbb{Q}$ and over number fields in general is still open, the function field analogue turned out to be much more tractable. Hilbert's Tenth Problem for the function field k of a curve over a finite field is known to be undecidable. This was proved by Pheidas for $k = \mathbb{F}_q(t)$ with q odd [Phe91], and then extended to all global function fields in [Vid94, Shl96, Eis03a]. We also have undecidability of Hilbert's Tenth Problem for certain function fields over possibly infinite constant fields of positive characteristic ([Shl00, Shl03, Eis03a, KR92b]). The results of [Eis03a] and [Shl00] also generalize to higher transcendence degree (see [Shl02]) and give undecidability of Hilbert's Tenth Problem for finite extensions of $\mathbb{F}_q(t_1, \ldots, t_n)$ with $n \geq 2$.

In characteristic zero Hilbert's Tenth Problem is also known to be undecidable for several function fields: In 1978 Denef proved the undecidability of Hilbert's Tenth Problem for rational function fields $K(T)$ over formally real fields K [Den78], and in [MB05] this was extended to finite extensions of $K(T)$ for K formally real. Undecidability is also known for function fields over number fields and p-adic fields with $p > 2$ [KR95, MB05, Eis07]. Kim and Roush [KR92a] showed that the problem is undecidable for the purely transcendental function fields $\mathbb{C}(t_1, t_2)$ and $\overline{\mathbb{F}}_p(t_1, t_2)$ when $p > 2$. In [Eis04] this was generalized to finite extensions of $\mathbb{C}(t_1, , \ldots, t_n)$ for $n \geq 2$. In this paper we will generalize Kim and Roush's result [KR92a] and the result of [Eis04] to function fields of odd characteristic of transcendence degree at least 2.

Date: April 21, 2011.

The author was partially supported by National Science Foundation grant DMS-0801123 and a Sloan Research Fellowship.

In Hilbert's Tenth Problem over a commutative ring R, the coefficients of the equations have to be input into a Turing machine, so 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 prove the following theorem:

Theorem 1.1. *Let K be the function field of a variety of dimension ≥ 2 over an algebraically closed field k of characteristic $p > 2$. There exist elements $z_1, z_2 \in K$ which are algebraically independent over k such that Hilbert's Tenth Problem for K with coefficients in $\mathbb{F}_p[z_1, z_2]$ is undecidable.*

For simplicity of notation we will just refer to this as Hilbert's Tenth Problem for K.

Let $E/\mathbb{F}_p$ be an elliptic curve, and let $\mathfrak{R}$ be the ring of endomorphisms of E defined over $\overline{\mathbb{F}}_p$. Then $\mathfrak{R}$ is an order in a quadratic imaginary field or an order in a quaternion algebra. We will prove Theorem 1.1 by constructing a diophantine model of $\mathfrak{R} \times \mathfrak{R}$ over K with certain relations and then show that we can define the ring $\mathfrak{R}$ with addition and multiplication inside this model. Since we can show that the ring $\mathfrak{R}$ with addition and multiplication has an undecidable positive existential theory this implies that Hilbert's Tenth Problem for K is undecidable. The fact that we are working with function fields over an algebraically closed field is used in Section 6 where we apply the Tsen-Lang Theorem.

Our proof generalizes the techniques in [Eis04] which proved undecidability for finite extensions of $\mathbb{C}(t_1, \ldots, t_n)$ $(n \geq 2)$. The approach has to be changed in several places because we are working in positive characteristic. In [Eis04] an elliptic curve over $\mathbb{C}$ without CM was used to construct a model of $\mathbb{Z} \times \mathbb{Z}$. Elliptic curves over finite fields always have CM, so instead we construct a model of the endomorphism ring, which can be noncommutative. Furthermore, the arguments in [Eis04] used in many places that the point $(0, \beta)$ on the chosen elliptic curve over $\mathbb{C}$ had infinite order. This is not possible in our situation because any $\overline{\mathbb{F}}_p$-rational point on an elliptic curve over defined over $\mathbb{F}_p$ has finite order.

Remark 1. Suppose that the field K in Theorem 1.1 is given as $k(t_1, t_2, \ldots, t_n)(\alpha)$. (Since k is algebraically closed and hence perfect, K/k is separably generated and so it is always possible to describe K like this.) The same arguments as in [Eis07] show that the elements z_1, z_2 in Theorem 1.1 can be chosen in a subfield K_0 of K which is a finite extension of the field that is generated over $\mathbb{F}_p$ by $t_1, \ldots, t_n$ and the coefficients of the minimal polynomial of α. See Proposition 3.2, Proposition 3.4, Theorem 4.1 and the discussion at the beginning of Section 8.2 in [Eis07]. These results are stated for function fields of characteristic zero, but they also hold in positive characteristic.

2. A structure with an undecidable existential theory

To explain the main ideas of the proof we need to define the notion of a diophantine set and a diophantine model.

Definition 2.1. 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

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

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 S is *diophantine over R with coefficients in R'*.

Let k be an algebraically closed field of characteristic $p > 2$, and let K be a finite extension of $k(t_1, t_2, \ldots, t_n)$ $(n \geq 2)$. We will define a *diophantine model* of the structure

$$\mathcal{S} = \langle \mathfrak{R} \times \mathfrak{R}, +, |, \mathcal{Z}, \mathcal{W} \rangle$$

in K with coefficients in $\mathbb{F}_p[z_1, z_2]$. Here $\mathfrak{R}$ will be the endomorphism ring of a suitable elliptic curve E over $\mathbb{F}_p$, $+$ will denote the usual component-wise addition of pairs of elements of $\mathfrak{R}$, and $|$ represents a relation which satisfies

$$(m, 1) \mid (n, r) \Leftrightarrow n = r \cdot m.$$

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

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

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

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

Definition 2.2. A *diophantine model* of $\mathcal{S}$ over K is a diophantine subset $A \subseteq K^n$ equipped with a bijection $\phi : \mathfrak{R} \times \mathfrak{R} \to A$ such that under ϕ, the graphs of addition, $|$, $\mathcal{Z}$, and $\mathcal{W}$ in $\mathfrak{R} \times \mathfrak{R}$ correspond to diophantine subsets of A^3, A^2, A, and A^2, respectively.

Let R' be a subring of K. A *diophantine model* of $\mathcal{S}$ over K *with coefficients in* R' is a diophantine model of $\mathcal{S}$, where A and the graphs of addition, $|, \mathcal{Z}$ and $\mathcal{W}$ are diophantine over K with coefficients in R'.

2.1. **The structure $\mathcal{S}$ has an undecidable existential theory.** We will now show that constructing a model of $\mathcal{S}$ is sufficient to prove undecidability of Hilbert's Tenth Problem for K. This generalizes Proposition 2.3 in [Eis04].

Proposition 2.3. *Let $E/\mathbb{F}_p$ be an elliptic curve, and let $\mathfrak{R}$ be the ring of endomorphisms of E defined over $\overline{\mathbb{F}}_p$. The structure*

$$\mathcal{S} = \langle \mathfrak{R} \times \mathfrak{R}, +, |, \mathcal{Z}, \mathcal{W} \rangle$$

has an undecidable existential theory.

Proof. We will first show that we can existentially define $\mathfrak{R}$ with addition and multiplication inside $\mathcal{S}$. We interpret the elements $n \in \mathfrak{R}$ as the pair $(n, 0)$. The set $\{(n, 0) : n \in \mathfrak{R}\}$ is existentially definable in $\mathcal{S}$ through the relation $\mathcal{Z}$. Addition of elements n, m of $\mathfrak{R}$ corresponds to the addition of the pairs $(n, 0)$ and $(m, 0)$. To define multiplication of the elements $m, r \in \mathfrak{R}$, note that $n = r \cdot m$ if and only if $(m, 1) \mid (n, r)$, hence $n = r \cdot m$ if and only if

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

We can now finish the proof of the proposition by showing that the existential theory of $\langle \mathfrak{R}, 0, 1; +, \times \rangle$ is undecidable: Since $\mathfrak{R}$ is the endomorphism ring of an elliptic curve defined over $\overline{\mathbb{F}}_p$, $\mathfrak{R}$ is either an order in a quadratic imaginary field or an order in a quaternion algebra. If $\mathfrak{R}$ is an order in a quadratic imaginary field F, denote by $\mathcal{O}_F$ its maximal order. By [Den75], Hilbert's Tenth Problem for $\mathcal{O}_F$ is undecidable. The ring $\mathfrak{R}$ has finite index in $\mathcal{O}_F$, and $\mathcal{O}_F$ is the integral closure of $\mathfrak{R}$ in F. By [Eis03b, Lemma 7.5, p.68], Hilbert's Tenth Problem for $\mathfrak{R}$ is undecidable as well.

Suppose now that $\mathfrak{R}$ is an order in a quaternion algebra D. Let $\alpha \in \mathfrak{R}$ be an element with $\alpha^2 \in \mathbb{Q}$, and $\alpha^2 < 0$ (see [Sil94, III.9.3]). Then $F := \mathbb{Q}(\alpha)$ is a quadratic imaginary extension of $\mathbb{Q}$, and the following argument shows that the centralizer of α in D is F. If the

centralizer contained another element $\beta \notin F$, then $\mathbb{Q}(\alpha, \beta)$ would have to be a field, since β commutes with α and with the elements of $\mathbb{Q}$, and we would have $[\mathbb{Q}(\alpha, \beta) : \mathbb{Q})] > 2$. But the maximal subfields $G \subset D$ have degree 2 over $\mathbb{Q}$, contradiction.

It follows that the centralizer of α in $\mathfrak{R}$ is an order $\mathcal{O}$ in F. Since $\mathcal{O}$ is the set of all elements in $\mathfrak{R}$ that commute with α, it is existentially definable in $\mathfrak{R}$ as $\{x \in \mathfrak{R} : x\alpha - \alpha x = 0\}$. Since Hilbert's Tenth Problem for $\mathcal{O}$ is undecidable the result follows. □

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 with coefficients in $\mathbb{F}_p[z_1, z_2]$. In Sections 3 through 6 we will construct this model.

In [Eis04] we proved the following:

Proposition 2.4. *The relation $\mathcal{W}$ can be defined entirely in terms of the other relations.*

This implies that once we have a diophantine set which is in bijection with $\mathfrak{R} \times \mathfrak{R}$ it is enough to existentially define $\mathcal{Z}, +$, and $|$. To do this we will first prove that endomorphisms of an elliptic curve can be related to points on certain twists of E.

3. Relating endomorphisms to points on twists

Before we can construct the diophantine model of $\mathcal{S}$ we need some facts about points on twisted elliptic curves.

Setup and Notation: Throughout this section F will denote a field of characteristic $p > 2$ which contains the algebraic closure $\overline{\mathbb{F}}_p$ of $\mathbb{F}_p$. We will denote by E an elliptic curve over $\mathbb{F}_p$, given by an affine equation $E : y^2 = P(x)$, and $\mathfrak{R}$ will be its ring of endomorphisms defined over $\overline{\mathbb{F}}_p$, $\mathfrak{R} = \mathrm{End}_{\overline{\mathbb{F}}_p}(E)$. We denote by $\mathrm{Rat}_F(E, E)$ the F-rational maps from E to E.

Let $\mathcal{E}$ be an elliptic curve over $\overline{\mathbb{F}}_p(T)$ with affine equation

$$\mathcal{E} : P(T)\, y^2 = P(x).$$

Then $\mathcal{E}$ is a twist of E. We identify T with the rational function $(x, y) \mapsto x$ on E, and we denote the function $(x, y) \mapsto y$ by U. Then $\overline{\mathbb{F}}_p(T, U)$ is the function field of E over $\overline{\mathbb{F}}_p$, where $U^2 = P(T)$. We denote by $F(T, U)$ the function field of E over F.

Proposition 3.1. *Each endomorphism $\phi \in \mathfrak{R}$ is of the form $\phi = (f_1(T), U \cdot f_2(T))$ with $f_1(T), f_2(T) \in \overline{\mathbb{F}}_p(T)$ and $(f_1(T), f_2(T)) \in \mathcal{E}(\overline{\mathbb{F}}_p(T))$.*

Proof. This is proved in [KR92a, Proposition 7] for elliptic curves over $\mathbb{C}$, and the proof for $\overline{\mathbb{F}}_p$ ($p > 2$) is the same. □

The following Proposition and Corollaries give a correspondence between points on $\mathcal{E}$ and endomorphisms of E. Our statement is in terms of $2 \cdot \mathcal{E}(F(T))$ since $\mathcal{E}(F(T))$ contains points of order 2 which do not correspond to endomorphisms.

Proposition 3.2. *There is an injective homomorphism $\psi : \mathcal{E}(F(T)) \to \mathrm{Rat}_F(E, E)$. For $(X, Y) \in 2 \cdot \mathcal{E}(F(T))$ we have $(X, UY) \in 2 \cdot \mathrm{End}_F(E)$.*

Proof. This is similar to the proof of Lemma 3.1. in [Den78]. Let ψ_1 be the $F(T, U)$-rational map

$$\psi_1 : \mathcal{E} \to E : (X, Y) \mapsto (X, UY).$$

Let $\psi_2 : E(F(T, U)) \to \mathrm{Rat}_F(E, E)$ be the map given by

$$(V, W) \mapsto ((x, y) \mapsto (V(x, y), W(x, y))).$$

Let $\psi : \mathcal{E}(F(T)) \to \mathrm{Rat}_F(E,E)$ be given by $\psi := \psi_2 \circ \psi_1$.

The map ψ_1 is a group homomorphism since it is rational and $\psi_1(\mathbf{O}) = \mathbf{O}$. The map ψ_2 is clearly a homomorphism, so $\psi = \psi_2 \circ \psi_1$ is a homomorphism as well. Let $(X,Y) \in \mathcal{E}(F(T))$. Then $T \circ \psi(X,Y) = X$ and $U \circ \psi(X,Y) = UY$. Hence ψ is injective. We have

$$\mathrm{Rat}_F(E,E) = \mathrm{End}_F(E) \oplus E(F),$$

where we identify a point of $E(F)$ with the constant map from E onto this point.

If $(X,Y) \in \mathcal{E}(F(T))$ and $\psi(X,Y) \in E(F)$, then by looking at ψ_2 we see that Y must be 0, and so (X,Y) is a point of order 2. This proves the second part of the proposition. □

From Proposition 3.2 and its proof we immediately obtain:

Corollary 3.3. *Let $\psi : \mathcal{E}(F(T)) \to \mathrm{Rat}_F(E,E)$ be as in the previous proposition. Then $\psi((T,1))$ is the endomorphism of E given by $P \mapsto P$. In particular, $(T,1) \in \mathcal{E}(F(T))$ has infinite order.*

Corollary 3.4. *Let $E, \mathcal{E}, F$ be as above. Then $\mathcal{E}(F(T)) = \mathcal{E}(\overline{\mathbb{F}}_p(T))$, and the restriction of the homomorphism ψ to $2 \cdot \mathcal{E}(F(T))$,*

$$\psi : 2 \cdot \mathcal{E}(F(T)) \to 2 \cdot \mathfrak{R}$$

is a bijection onto $2 \cdot \mathfrak{R}$.

Proof. Propositions 3.1 and 3.2 imply that the restriction of $\psi : 2 \cdot \mathcal{E}(F(T)) \to 2 \cdot \mathrm{End}_F(E)$ is a bijection. Since $\mathrm{End}_F(E) = \mathfrak{R}$ by [Con04, Theorem 2.1], we have that

$$\psi : 2 \cdot \mathcal{E}(F(T)) \to 2 \cdot \mathfrak{R}$$

is a bijection as well. The first part now follows from the fact that ψ restricted to $2 \cdot \mathcal{E}(\overline{\mathbb{F}}_p(T))$ is also a bijection onto $2 \cdot \mathfrak{R}$, together with the proof of Proposition 3.2 since the full 2-torsion of $\mathcal{E}$ is already defined over $\overline{\mathbb{F}}_p(T)$. □

4. Choosing twists using Moret-Bailly's theorem

Let K be as in Theorem 1.1. To prove undecidability for K it clearly suffices to construct a diophantine model of $\langle 2 \cdot \mathfrak{R} \times 2 \cdot \mathfrak{R}, +, |, \mathcal{Z}, \mathcal{W} \rangle$ over K. To do this we will construct two twists $\mathcal{E}_1$ and $\mathcal{E}_2$ of E which are of the form

$$\mathcal{E}_i : P(z_i)\, y^2 = P(x),$$

with $z_i \in K$ (for $i = 1, 2$) and such that the natural injection $\iota : \mathcal{E}_i(\mathbb{F}_p(T)) \hookrightarrow \mathcal{E}_i(K)$ induced by $T \mapsto z_i$ is *almost* a bijection (defined below). We will then use the K-rational points on $\mathcal{E}_i$ to get a diophantine set over K that is in bijection with $2 \cdot \mathfrak{R}$.

To obtain the twists $\mathcal{E}_1$ and $\mathcal{E}_2$ that we need for our construction of the diophantine model, we need a theorem by Moret-Bailly [MB05]. Let k be a field of characteristic $p > 2$ which is transcendental over a finite field. Let C be a smooth projective geometrically connected curve over k with function field K. Let Q be a finite nonempty set of closed points of C so that the residue fields of $q \in Q$ are separable over k. Let $E : y^2 = P(x)$ be an elliptic curve over k with $P(0) \neq 0$. In [MB05] Moret-Bailly also introduces another curve Γ, but for our application of his theorem we only have to consider the special case where $\Gamma = E$.

Definition 4.1. Let k, C, K, E, Q be as above. Let $g : C \to \mathbf{P}^1_k$ be a non-constant k-morphism corresponding to an injection $k(T) \hookrightarrow K$ 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.

Note: Our notation follows Moret-Bailly's equivalent setup from an earlier version of [MB05] (because of the twisted elliptic curve we use here): We assume that the polynomial $R(t)$ defining Γ is without multiple roots and satisfies $R(0) \neq 0$. We are also in the situation $\Gamma = E$, but the double cover π is given by the x-coordinate. With this notation, we have $R(T) = P(T)$ and the twisted curve $y^2 = R(T)P(x)$ in [MB05, 1.4.6] is isomorphic to $R(T)y^2 = P(x)$ (which is the twist that we use) via $(X, Y) \mapsto (X, Y/R(T))$.

In [MB05] Moret-Bailly proves:

Lemma 4.2. *Given C, E, Q as above, we can always find an admissible morphism g. If g is admissible for E, then for all but finitely many $\lambda \in k^*$, λg is still admissible.*

We will also use the following terminology that was used by Moret-Bailly.

Definition 4.3. Let $\gamma : A \to B$ be a morphism of abelian groups. We say that γ is *almost bijective* if γ is injective and Coker γ is a finite p-group. (Here p is the characteristic of the function field K.)

Now we can state Moret-Bailly's theorem.

Theorem 4.4. [MB05, Theorem 1.8] *Let k, C, K, E, Q be as above. Let $f \in K$ be admissible for E, Q. Let $\mathcal{E}_{\lambda f}$ be the elliptic curve whose affine equation is given by*

$$\mathcal{E}_{\lambda f} : P(\lambda f)\, y^2 = P(x).$$

Let $u \in k$ be transcendental over $\mathbb{F}_p$. Then the natural homomorphism $\mathcal{E}(k(T)) \hookrightarrow \mathcal{E}_{\lambda f}(K)$ induced by the inclusion $k(T) \hookrightarrow K$ that sends T to λf is almost bijective for infinitely many $\lambda \in \mathbb{F}_p[u]$.

We can now use Theorem 4.4 to prove the following theorem.

Theorem 4.5. *Let k, K be as in Theorem 1.1. Let F be the algebraic closure of $k(t_3, \ldots, t_n)$ in K. Let $E : y^2 = P(x)$ be an elliptic curve defined over $\mathbb{F}_p$ with $P(0) \neq 0$. As before, let*

$$\mathcal{E} : P(T)\, y^2 = P(x).$$

We can choose $z_1, z_2 \in K$ such that $F(z_1, z_2)$ has transcendence degree 2 over F and such that for the elliptic curves $\mathcal{E}_i : P(z_i)\, y^2 = P(x)$ $(i = 1, 2)$, the natural homomorphism $\mathcal{E}(\overline{\mathbb{F}}_p(T)) \hookrightarrow \mathcal{E}_i(K)$ induced by the inclusion $\overline{\mathbb{F}}_p(T) \hookrightarrow K$ that sends T to z_i is almost bijective.

Proof. Let k' be the algebraic closure of $F(t_2)$ 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 so that the residue fields of $q \in Q$ are separable over k'. Choose an element $f \in K$ that is admissible for E and Q. Since f is non-constant, f is transcendental over $F(t_2)$. Now we can apply Theorem 4.4 with $k = k'$, and K, C, E, Q, f as defined above, and with $u = t_2$. By Theorem 4.4 there exists a nonzero $\lambda \in \mathbb{F}_p[t_2]$ such that the natural homomorphism $\mathcal{E}(k'(T)) \hookrightarrow \mathcal{E}_{\lambda f}(K)$ induced by the inclusion $k'(T) \hookrightarrow K$ that sends T to λf is almost bijective. By Corollary 3.4, the inclusion $\mathcal{E}(\overline{\mathbb{F}}_p(T)) \hookrightarrow \mathcal{E}_{\lambda f}(K)$ is almost bijective as well. By Lemma 4.2 there exists a non-constant $\nu \in \mathbb{F}_p[t_2]$ such that the zeros of ν are not zeros of λ and such that $\nu \cdot f$ is still admissible for E. Pick such a $\nu \in \mathbb{F}_p[t_2]$ and let

$g := \nu \cdot f$. By Theorem 4.4 applied to g and Corollary 3.4, there exists a nonzero $\mu \in \mathbb{F}_p[t_2]$ such that $\mathcal{E}(\overline{\mathbb{F}}_p(T)) \hookrightarrow \mathcal{E}_{\mu g}(K)$ is almost bijective. Let $z_1 := \lambda f$, and let $z_2 := \mu g = \mu\nu f$. To complete the proof it remains to show that $F(z_1, z_2)$ has transcendence degree 2 over F. By our choice of ν the element $z_1/z_2 = \lambda/(\mu \cdot \nu) \in F(t_2)$ is transcendental over F. We are done if we can show that z_1 is transcendental over $F(t_2)$ since $F(z_1/z_2) \subseteq F(t_2)$. As pointed out above, the element f is transcendental over $F(t_2)$, and since $\lambda \in \mathbb{F}_p[t_2]$ the same is true for $\lambda f = z_1$. This shows that the transcendence degree of $F(z_1/z_2, z_1) = F(z_1, z_2)$ over F is at least 2, and since $F(z_1, z_2) \subseteq K$, which is algebraic over $F(t_1, t_2)$, the transcendence degree must equal 2. □

We will now use Theorem 4.5 and Corollary 3.4 to construct a diophantine set A which is in bijection with $2^{\mathfrak{N}} \times 2^{\mathfrak{N}}$.

5. Diophantine definition of A and existential definitions of $+$ and $\mathcal{Z}$

As before, let K be the function field of a variety of dimension ≥ 2 over an algebraically closed field k of characteristic $p > 2$. Let E, z_1, z_2 be as in Theorem 4.5, and let $\mathcal{E}_1$ and $\mathcal{E}_2$ be the corresponding twists with equation

$$\mathcal{E}_i : P(z_i)\, y^2 = P(x) \quad (i = 1, 2).$$

To be able to define a suitable set A which is in bijection with $2^{\mathfrak{N}} \times 2^{\mathfrak{N}}$ we will work in an algebraic extension L of K. Let $L := K(h_1, h_2)$, where h_i is defined by $h_i^2 = P(z_i)$, 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. Similarly there is an isomorphism between $\mathcal{E}_2$ and E that sends a point (x, y) on $\mathcal{E}_2$ to the point $(x, h_2 y)$ 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.

Now we can define the set A. Let A_1 be the subset of $E(L)$ defined by

$$A_1 := \{2 \cdot (x, h_1 y) : (x, y) \in \mathcal{E}_1(F(z_1, z_2))\}.$$

Similarly, let $A_2 \subseteq E(L)$ be given by $A_2 := \{2 \cdot (x, h_2 y) : (x, y) \in \mathcal{E}_2(F(z_1, z_2))\}$. Now we define A to be $A := A_1 \times A_2$. Then $A \subseteq E(L) \times E(L)$ and by Corollary 3.4, the set A is in bijection with $2^{\mathfrak{N}} \times 2^{\mathfrak{N}}$. The next proposition shows that A is existentially definable.

Proposition 5.1. *The set A is existentially definable in $\langle\, L, +, \cdot\, ; 0, 1, z_1, z_2, h_1, h_2, S \,\rangle$.*

Proof. Let $H := \mathcal{E}_1(F(z_1, z_2))$ and $G := \mathcal{E}_1(K)$. By Theorem 4.5, H is a subgroup of finite index in G and G/H is a finite p-group. Hence for some integer k, $p^k G \subseteq H$ and $p^k G$ has finite index in G. Since G is diophantine over K, and since multiplication by p^k is given by explicit equations, the set $p^k G$ is diophantine over K. Then H is diophantine over K as well:

Let $Q_1, \ldots, Q_\ell$ be coset representatives for $p^k G$ in H. Then for $P \in E(L)$

$$P \in H \Leftrightarrow (\exists\, S \in p^k G)(P = S + Q_1) \vee \cdots \vee (P = S + Q_\ell).$$

Since we have a predicate for elements of K the set G is existentially definable in L, and hence the set A_1 is existentially definable in L in our language as well. By repeating the same argument with $\mathcal{E}_1$ replaced by $\mathcal{E}_2$, we see that the set A_2 is also existentially definable in L. Hence A is existentially definable in L. □

5.1. **Existential definitions of $+$ and $\mathcal{Z}$.** The unary relation $\mathcal{Z}$ is existentially definable, since this is the same as showing that the set $H = \mathcal{E}_1(F(z_1, z_2))$ is diophantine, which was done in Proposition 5.1. 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 $|$. This is done in the next section.

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

As before, let K be the function field of a variety of dimension ≥ 2 over an algebraically closed field k of characteristic $p > 2$. Now we will show how to existentially define the relation $|$ in $L = K(h_1, h_2)$. As before, we denote by F the algebraic closure of $k(t_3, \ldots, t_n)$ in K so that L and K are both finite extensions of $F(z_1, z_2)$. Let $\alpha := [L : F(z_1, z_2, h_1, h_2)]$.

6.1. **Finding a point of large order.** In our construction, $E : y^2 = P(x)$ is an elliptic curve over $\mathbb{F}_p$. For any finite field $\mathbb{F}_q$ of positive characteristic p, $E(\mathbb{F}_q)$ is isomorphic to a product of two cyclic groups [Sil94, Exercise 5.6]. By the Hasse-Weil bound, $|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$, so we can find an extension $\mathbb{F}_q$ of $\mathbb{F}_p$ such that $E(\mathbb{F}_q)$ contains a point (X_0, Y_0) of order $> 2^\alpha + 1$. Then $Y_0 \neq 0$, since (X_0, Y_0) does not have order 2.

Let E_0 be the elliptic curve defined over $\mathbb{F}_q$ with equation

$$E_0 : y^2 = P(x + X_0) = P_0(x).$$

Then E_0 is isomorphic to E over $\mathbb{F}_q$, since a point (x, y) on E corresponds to $(x - X_0, y)$ on E_0. The point $(0, 0)$ is not on E_0, since $(X_0, 0)$ is not on E. Also, since $(0, Y_0)$ is a point on E_0, the constant term of $P_0(x)$ in the Weierstrass equation for E_0 is Y_0^2. Moreover, the points $(0, Y_0)$ and $(0, -Y_0) = -(0, Y_0)$ on E_0 have order $> 2^\alpha + 1$.

The field L contains the algebraic closure of a finite field, so over L, $\mathcal{E}_1$ and $\mathcal{E}_2$ are isomorphic to E_0, and the isomorphism sends a point (x, y) on $\mathcal{E}_1$ to $(x - X_0, h_1 y)$ and similarly for $\mathcal{E}_2$. Let $P_1 := (z_1 - X_0, h_1) = (s_1, h_1)$ and $P_2 := (z_2 - X_0, h_2) = (s_2, h_2)$, with z_1, z_2, h_1, h_2 as in Section 5. Then as in Proposition 5.1, the set $A := A_1 \times A_2$ with $A_i = \{2 \cdot (x - X_0, h_i y) : (x, y) \in \mathcal{E}_i(z_1, z_2)\}$ $(i = 1, 2)$ is existentially definable in the language $\langle L, +, \cdot : z_1, z_2, h_1, h_2, S\rangle$. Let $\mathrm{End}(E_0)$ denote the endomorphism ring of E_0 over $\overline{\mathbb{F}}_p$. The endomorphism rings of E_0 and E are isomorphic, and so $A_1 \times A_2$ is isomorphic to $2 \cdot \mathrm{End}(E_0) \times 2 \cdot \mathrm{End}(E_0)$. From now on we will identify the set $A_1 \times A_2$ with $2 \cdot \mathrm{End}(E_0) \times 2 \cdot \mathrm{End}(E_0)$.

Remark 2. By the results in Section 3, the set $A_1 \times A_2$ constructed above consists exactly of pairs (mP_1, nP_2) with $m, n \in 2\,\mathrm{End}(E_0)$. Here mP_i denotes the image of P_i under the endomorphism m $(i = 1, 2)$.

6.2. **Existential definition of divisibility.** In the following $x(P)$ will denote the x-coordinate of a point P on E_0, and $y(P)$ will denote the y-coordinate of P. As above, $E : y^2 = P(x)$ is an elliptic curve defined over $\mathbb{F}_p$ with $P(0) \neq 0$, and E_0 is the elliptic curve with equation

$E_0 : y^2 = P(x + X_0) = P_0(x)$ with $X_0 \in \mathbb{F}_q$, and where X_0 is chosen such that $(0, \pm Y_0) \in E_0(\overline{\mathbb{F}}_p)$ have order $> 2^\alpha + 1$. The points $P_1, P_2 \in E_0(L)$ are defined as in Section 6.1.

To give an existential definition of the divisibility relation we will use the fact that

$$(m, 1) \mid (n, r) \Leftrightarrow (m, 1) \mid (kn, kr)$$

for a nonzero element $k \in \mathrm{End}(E_0)$.

Theorem 6.1. *There exists a finite set $U \subseteq 2\,\mathrm{End}(E_0)$ such that for all $m \in 2\,\mathrm{End}(E_0) - U$ we have: for all $n, r \in 2\,\mathrm{End}(E_0)$*

$$\begin{aligned}
&(m, 1) \mid (n, r) \Leftrightarrow \\
&\quad (\ \exists\, \xi_0, \rho_0 \in L\ \ x(nP_1 + rP_2)\, \xi_0^2 + x(mP_1 + P_2)\, \rho_0^2 = 1 \\
&\quad \wedge\ \exists\, \xi_1, \rho_1 \in L\ \ x(2nP_1 + 2rP_2)\, \xi_1^2 + x(mP_1 + P_2)\, \rho_1^2 = 1 \\
&\qquad\qquad \cdots \\
&\quad \wedge\ \exists\, \xi_\alpha, \rho_\alpha \in L\ \ x(2^\alpha nP_1 + 2^\alpha rP_2)\, \xi_\alpha^2 + x(mP_1 + P_2)\, \rho_\alpha^2 = 1\ )\ .
\end{aligned}$$

Here, for $n \in 2\,\mathrm{End}(E_0)$, nP_i denotes the image of P_i under n $(i = 1, 2)$.

Proof. For the first implication, assume that $(m, 1) \mid (n, r)$, *i.e.* $n = r \cdot m$. Let $P \in E(L)$. By Proposition 3.1, any endomorphism $\varphi : E \to E$ is of the form $(f_1(T), U f_2(T))$ with $f_1(T), f_2(T) \in \overline{\mathbb{F}}_p(T)$, and hence it follows that $x(\varphi(P))$ and $y(\varphi(P))$ are in $\overline{\mathbb{F}}_p(x(P), y(P))$. Hence also for $r : E_0 \to E_0$, both $x(mP_1 + P_2)$ and $x(r(mP_1 + P_2)) = x(nP_1 + rP_2)$ are elements of $\overline{\mathbb{F}}_p(x(mP_1 + P_2), y(mP_1 + P_2))$, which has transcendence degree one over $\overline{\mathbb{F}}_p$. This means that we can apply the Tsen-Lang Theorem (Theorem 7.3 in the appendix) to the quadratic form

$$x(nP_1 + rP_2)\xi^2 + x(mP_1 + P_2)\rho^2 - \omega^2$$

to conclude that there exists a nontrivial zero (ξ, ρ, ω) over $\overline{\mathbb{F}}_p(x(mP_1 + P_2), y(mP_1 + P_2)) \subseteq F(x(mP_1 + P_2), y(mP_1 + P_2))$. By Proposition 7.2 from the appendix this implies that there exists a nontrivial zero (ξ, ρ, ω) with $\omega \neq 0$. The same can be done for the other equations.

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

Step 1. There exists a finite set $U \subseteq 2\,\mathrm{End}(E_0)$ such that for all $m \in 2\,\mathrm{End}(E_0) - U$ there exists a discrete valuation $w_m : L^* \twoheadrightarrow \mathbb{Z}$ such that $w_m(x(mP_1 + P_2)) > 0$ and odd, and such that $w_m(x(knP_1 + krP_2)) = 0$ for $k = 1, 2, 4, \ldots, 2^\alpha$.

Proof: Recall that $P_1 = (s_1, h_1) = (z_1 - X_0, h_1) \in E_0(L)$ is the point on E_0 corresponding to $(z_1, 1)$ on $\mathcal{E}_1$. Similarly $P_2 = (s_2, h_2) \in E_0(L)$ is the point on E_0 corresponding to $(z_2, 1)$ on $\mathcal{E}_2$. Since $(z_i, 1) \in \mathcal{E}_i(L)$ has infinite order (Corollary 3.3) and since $E_0, \mathcal{E}_1$, and $\mathcal{E}_2$ are isomorphic over L, P_1 and P_2 are points of infinite order on E_0.

Fix $m \in 2\,\mathrm{End}(E_0)$. Let $P_2' = mP_1 + P_2 = (s_2', h_2')$. Let $\tilde{F} := F(s_1, s_2, h_1, h_2) = F(z_1, z_2, h_1, h_2)$. Then

$$\tilde{F} = F(s_1, s_2, h_1, h_2) = F(s_1, h_1, s_2', h_2') = F(x(P_1), y(P_1), x(P_2'), y(P_2')),$$

because the same argument as above (in the proof of the other direction) implies that $F(s_1, h_1, s_2', h_2') \subseteq F(s_1, h_1, s_2, h_2)$. Since $s_2 = x(P_2' - mP_1)$ and $h_2 = y(P_2' - mP_1)$, we also have $F(s_1, h_1, s_2, h_2) \subseteq F(s_1, h_1, s_2', h_2')$.

Now let $\tilde{v}_m : \tilde{F}^* \twoheadrightarrow \mathbb{Z}$ be a discrete valuation which extends the discrete valuation $\tilde{v}$ of $F(s_1, h_1)(s_2')$ associated to s_2'.

Let L_0 be an intermediate field between $\tilde{F} = F(s_1, s_2, h_1, h_2)$ and L such that $L_0/\tilde{F}$ is separable and such that L/L_0 is purely inseparable. Let

$$U := \{m \in 2\operatorname{End}(E_0) : \tilde{v}_m \text{ ramifies in } L_0\}.$$

Then U is finite by [Deu73, p. 111]. Suppose that $m \notin U$, *i.e.* that $\tilde{v}_m$ does not ramify in L_0. Let v_m be an extension of $\tilde{v}_m$ to L_0. Then $x(P_2')$ is still a uniformizer for v_m.

Now choose an extension w_m of v_m to L and normalize it such that $w_m : L^* \twoheadrightarrow \mathbb{Z}$. The extension L/L_0 is purely inseparable, so $w_m(x(P_2')) = p^h$ for some $h \geq 0$ by [Deu73, p. 111]. In particular, since L is a field of characteristic $p > 2$, $w_m(x(P_2'))$ is odd and positive. The valuation w_m is trivial on $F(s_1, h_1)$, and the residue field ℓ_m of w_m is a finite extension of $F(s_1, h_1)$. Let $s := n - rm$. By assumption, $s \neq 0$. We have $x(nP_1 + rP_2) = x(sP_1 + rP_2')$, and the image of this element in the residue field ℓ_m is $x(s(s_1, h_1) + r(0, Y_0))$. Since (s_1, h_1) has infinite order on E_0, its image under an endomorphism is also a point of infinite order. The points on E_0 whose x-coordinate is zero, $(0, Y_0)$ and $(0, -Y_0)$, are defined over $\overline{\mathbb{F}}_p$ and hence have finite order. Hence the image of $x(sP_1 + rP_2')$ in ℓ_m must be nonzero, and so $w_m(x(sP_1 + rP_2')) = w_m(x(nP_1 + rP_2)) = 0$. A similar argument shows that $w_m(x(knP_1 + krP_2)) = 0$.

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

Step 2. The elements $x_{s,r}, x_{2s,2r}, \ldots, x_{2^\alpha s,2^\alpha r}$ are squares in ℓ_m, but they are not squares in the subfield $F(s_1, h_1)$.

Proof: Lemma 7.1 from the appendix implies that the elements $x_{s,r}$, $x_{2s,2r}$, ..., $x_{2^\alpha s,2^\alpha r}$ are squares in ℓ_m.

We have $x_{s,r} = x(s(s_1, h_1) + r(0, Y_0))$. To prove that the functions $x_{s,r}, x_{2s,2r}, \ldots, x_{2^\alpha s,2^\alpha r}$ are not squares in the subfield $F(s_1, h_1)$ of ℓ_m it suffices to show that each of these functions has a zero of odd order: By definition of h_1, s_1 and since $P(x + X_0) = P_0(x)$, we have $h_1^2 = P(z_1) = P_0(z_1 - X_0) = P_0(s_1)$, and so $F(s_1, h_1)$ is the function field of E_0 over F.

Hence we can consider $x_{s,r}$, $x_{2s,2r}$, $\cdots$, $x_{2^\alpha s,2^\alpha r}$ as functions $E_0 \to \mathbf{P}^1_F$. Then $x_{s,r}$ corresponds to the function on E_0 which can be obtained as the composition $P \mapsto sP + r(0, Y_0) \mapsto x(sP + r(0, Y_0))$. The x-coordinate map is of degree 2 and has two distinct zeros, namely $(0, Y_0)$ and $(0, -Y_0)$. The translation-by-$r(0, Y_0)$ map is an isomorphism of E_0 (but not an isogeny) and has degree 1. By [Sil94, II.2.12], the endomorphism $s : E_0 \to E_0$ factors as

$$E_0 \xrightarrow{\phi} E_0^{(\tilde{q})} \xrightarrow{\lambda} E_0$$

with ϕ the $\tilde{q}$-th power Frobenius map for some $\tilde{q} = p^r$ and $\lambda : E_0^{(\tilde{q})} \to E_0$ separable. (Here $E_0^{(\tilde{q})}$ is the curve that is given by $y^2 = \tilde{P}_0(x)$, and $\tilde{P}_0(x)$ is obtained from $P_0(x)$ by raising each coefficient to the $\tilde{q}$-th power.) Since λ is separable it is unramified, and so $\#\lambda^{-1}(P) = \deg \lambda$ for all P ([Sil94, II.2.7 and III.4.10]). The $\tilde{q}$-th power Frobenius map ϕ is purely inseparable, and satisfies $\#\phi^{-1}(P) = 1$ and $e_\phi(P) = \tilde{q}$ for all P ([Sil94, II.2.12 and II.2.6]). Here e_ϕ denotes the ramification degree. Hence the composition of these maps, $x_{s,r}$, has $2 \cdot \deg \lambda$ zeros. By the above argument and [Sil94, II.2.6(c)], each zero P of $x_{s,r}$ has ramification degree $e_{x_{s,r}}(P) = \tilde{q}$. By the definition of ramification degree this implies that $\operatorname{ord}_P(x_{s,r}) = \tilde{q}$, *i.e.* $x_{s,r}$ has $2 \cdot \deg \lambda$ zeros of order $\tilde{q}$. The same argument works for the other functions $x_{ks,kr}$. So each of the functions $x_{ks,kr}$, for $k = 1, 2, 4, \ldots, 2^\alpha$ has only zeros of odd order

(since $p > 2$). In particular, none of these functions is a square in $F(s_1, h_1)$.

Step 3. The images of $x_{s,r}, \ldots, x_{2^\alpha s,2^\alpha r}$ in

$$V := [(\ell_m^*)^2 \cap F(s_1, h_1)^*]/(F(s_1, h_1)^*)^2 \text{ are distinct.}$$

Proof: By Step 2 all elements $x_{2^k s,2^k r}$ are in $(\ell_m^*)^2 \cap F(s_1, h_1)^*$.

Suppose P is a zero of the rational function $x_{s,r}$, so $sP + r(0, Y_0) = (0, \pm Y_0)$. The following argument shows that P is not a zero or a pole of $x_{2^k s,2^k r}$ for $1 \leq k \leq \alpha$. If P were a zero or a pole of $x_{2^k s,2^k r}$, then we would have

$$2^k sP + 2^k r(0, Y_0) \in \{(0, Y_0), (0, -Y_0), \mathbf{O}\}.$$

If we combine this with the fact that $sP + r(0, Y_0) = (0, \pm Y_0)$, we get that in order for P to be a zero or a pole of $x_{2^k s,2^k r}$, $1 \leq k \leq \alpha$, we would have to have

$$\begin{aligned} (2^k - 1)(0, Y_0) &= \mathbf{O}, \\ 2^k(0, Y_0) &= \mathbf{O}, \text{ or} \\ (2^k + 1)(0, Y_0) &= \mathbf{O}. \end{aligned}$$

Since the elliptic curve E_0 was chosen so that the point $(0, Y_0)$ has order strictly greater than $2^\alpha + 1$, none of these cases can occur.

We can use the same argument to deduce that a zero of $x_{2^i s,2^i r}$ $(1 \leq i \leq \alpha)$ is neither a zero nor a pole of $x_{2^j s,2^j r}$ for $\alpha \geq j > i$. 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 $f \in F(s_1, h_1)$, because if, say, $j > i$ and P is a zero of the left-hand-side, then the left-hand-side has a zero of odd order at P by what we proved in Step 2, while the right-hand-side has a zero of even order at P. Hence all the elements are different in $V = ({\ell_m^*}^2 \cap F(s_1, h_1)^*)/(F(s_1, h_1)^*)^2$. This proves the claim.

But now we have obtained a contradiction: since $[\ell_m : F(s_1, h_1)] \leq \alpha$, the size of V is bounded by α by Theorem 7.4 from the appendix, so it cannot contain $\alpha + 1$ distinct elements. This means that for all $m \in 2\operatorname{End}(E_0) - U$ the solvability of the $\alpha + 1$ equations implies that $n = rm$.

□

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 the divisibility relation $|$ has an existential definition.

Proposition 6.2. *The relation $\mathcal{W}$ is existentially definable.*

Proof. Let m_0 be a nonzero integer such that $m_0 \in 2\operatorname{End}(E_0) - U$. 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 $2\operatorname{End}(E_0) - U$, and since the set $\{(mP_1, nP_2) : m, n \in 2\operatorname{End}(E_0)\}$ is diophantine (see Remark 2), 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 6.1. □

The following corollary is the last piece that we need to construct the diophantine model of $\mathcal{S}$ and to complete the proof of Theorem 1.1.

Corollary 6.3. *The relation* $(m,1) \mid (n,r)$ *on* $2\operatorname{End}(E_0)\times 2\operatorname{End}(E_0)$ *is existentially definable in* $(m,1)$ *and* (n,r).

Proof. Let m_0 be as in the above proposition. By Theorem 6.1 the set U of "bad" points $m \in 2\operatorname{End}(E_0)$ finite. The endomorphism ring $\operatorname{End}(E_0)$ is a $\mathbb{Z}$-lattice. When we consider a $\mathbb{Z}$-basis for $2\operatorname{End}(E_0)$, we see that there exists a positive integer d such that $\{m_0 + dm : m \in 2\operatorname{End}(E_0)\} \cap U = \emptyset$. Since $n = rm \Leftrightarrow dn + rm_0 = d(rm) + rm_0 = r(dm + m_0)$ (since d is an integer), we have

$$(m,1) \mid (n,r) \Leftrightarrow (dm + m_0, 1) \mid (dn + rm_0, r),$$

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) by Theorem 6.1, since $(dm + m_0) \notin U$ for any $m \in 2\operatorname{End}(E_0)$. □

Remark 3. The equations in Theorem 6.1 are defined over $\mathbb{F}_{p^r}(z_1, h_1)$ for some $r > 0$. We still obtain that Hilbert's Tenth Problem for K with coefficients in $\mathbb{F}_p[z_1, z_2]$ is undecidable because the undecidability of Hilbert's Tenth Problem for K with coefficients in $\mathbb{F}_{p^r}[z_1, z_2]$ implies the undecidability of Hilbert's Tenth Problem with coefficients in $\mathbb{F}_p[z_1, z_2]$: Since $\mathbb{F}_{p^r} = \mathbb{F}_p[\alpha]$ for some $\alpha \in \mathbb{F}_{p^r}$, we can introduce an additional indeterminate x, add an extra equation saying that x satisfies the minimal polynomial of α, and write elements of $\mathbb{F}_{p^r}$ as polynomials of degree $< r$ in x with coefficients in $\mathbb{F}_p$.

7. Appendix

In this section we will state two results which were used to prove that the divisibility relation $\mid$ is diophantine.

We first need the following easy lemma.

Lemma 7.1. *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 over* k. *Then* a *is a square in the residue field of* k.

Proof. After multiplying b by a square we may assume that $v(b) = 1$. 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 $v(b) = 1$, it follows that $v(by^2)$ is odd. Hence $v(ax^2) = 0$ and $v(by^2) > 0$. Since $v(a) = 0$ and $v(b) = 1$, this implies that $v(x) = 0$ and $v(y) \geq 0$. 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. □

Proposition 7.2. *Let* k *be a field and let* $a, b, c \in k^*$. *If the quadratic form*

$$Q(x,y,z) = ax^2 + by^2 + cz^2$$

is isotropic, then there exists a zero (x_1, y_1, z_1) *of* Q *with* $z_1 \neq 0$.

Proof. Let (x,y,z) be a nontrivial zero of Q. If $z \neq 0$ we are done. If $z = 0$, then the quadratic form $ax^2 + by^2$ is isotropic and hence universal. In particular, $ax^2 + by^2$ represents $-c$, say $ax_1^2 + by_1^2 = -c$. Let $z_1 = 1$. Then (x_1, y_1, z_1) is a zero of Q with $z_1 \neq 0$. □

Theorem 7.3. *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 7.4. *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 $\mathrm{card}(V) = 2^{\dim V} \leq r$. □

References

[Con04] Brian Conrad. Gross-Zagier revisited. In *Heegner points and Rankin L-series*, volume 49 of *Math. Sci. Res. Inst. Publ.*, pages 67–163. Cambridge Univ. Press, Cambridge, 2004. With an appendix by W. R. Mann.

[Den75] Jan Denef. Hilbert's tenth problem for quadratic rings. *Proc. Amer. Math. Soc.*, 48:214–220, 1975.

[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.

[Eis03a] Kirsten Eisenträger. Hilbert's Tenth Problem for algebraic function fields of characteristic 2. *Pacific J. Math.*, 210(2):261–281, 2003.

[Eis03b] Kirsten Eisenträger. Ph.D. thesis, University of California, Berkeley. May 2003.

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

[Eis07] Kirsten Eisenträger. Hilbert's tenth problem for function fields of varieties over number fields and p-adic fields. *J. Algebra*, 310(2):775–792, 2007.

[KR92a] K. H. Kim and F. W. Roush. Diophantine undecidability of $\mathbf{C}(t_1, t_2)$. *J. Algebra*, 150(1):35–44, 1992.

[KR92b] K. H. Kim and F. W. Roush. Diophantine unsolvability for function fields over certain infinite fields of characteristic p. *J. Algebra*, 152(1):230–239, 1992.

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

[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.

[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.

[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.

[Shl02] Alexandra Shlapentokh. Diophantine undecidability of function fields of characteristic greater than 2, finitely generated over fields algebraic over a finite field. *Compositio Math.*, 132(1):99–120, 2002.

[Shl03] Alexandra Shlapentokh. Diophantine undecidability for some function fields of infinite transcendence degree and positive characteristic. *Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI)*, 304(Teor. Slozhn. Vychisl. 8):141–167, 171, 2003.

[Sil94] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994. Corrected reprint of the 1986 original.

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