UNDECIDABILITY IN FUNCTION FIELDS OF POSITIVE CHARACTERISTIC

KIRSTEN EISENTRÄGER AND ALEXANDRA SHLAPENTOKH

ABSTRACT. We prove that the first-order theory of any function field K of characteristic $p > 2$ is undecidable in the language of rings without parameters. When K is a function field in one variable whose constant field is algebraic over a finite field, we can also prove undecidability in characteristic 2. The proof uses a result by Moret-Bailly about ranks of elliptic curves over function fields.

1. INTRODUCTION

The current investigation started as an attempt by the authors to resolve Hilbert's Tenth Problem for all function fields of positive characteristic. 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 $x_1, \ldots, x_n \in \mathbb{Z}$. Matiyasevich ([11]), building on earlier work by Davis, Putnam, and Robinson ([2]), 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 recursive commutative rings. Perhaps the most important unsolved question in this area is Hilbert's Tenth Problem over the field of rational numbers.

The function field analogue turned out to be much more tractable. We know that 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 ([13]), and then extended to all global function fields in [25, 18, 4]. We also have undecidability of Hilbert's Tenth Problem for certain function fields over possibly infinite constant fields of positive characteristic ([19, 17, 4, 9]). The results of [4] and [19] also generalize to higher transcendence degree (see [20]) 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 [6] the problem was shown to be undecidable for finite extensions of $k(t_1, \ldots, t_n)$ with $n \geq 2$ and k algebraically closed of odd characteristic.

So all known undecidability results for Hilbert's Tenth Problem in positive characteristic either require that the constant field not be algebraically closed or that we are dealing with a function field in at least 2 variables. The big open question that remains is whether Hilbert's Tenth Problem for a one-variable function field over an algebraically closed field of constants is undecidable.

The current methods for proving undecidability of Hilbert's Tenth Problem for function fields K of positive characteristic p usually require showing that the following sets are existentially definable in the language of rings : $\{(x, x^{p^s}) : x \in K, s \in \mathbb{Z}_{\geq 0}\}$ and $\{x \in K : \text{ord}_{\mathfrak{p}} x \geq 0\}$ for some nontrivial prime $\mathfrak{p}$ of K. In this paper we show that we can

Key words and phrases. Undecidability, elliptic curves, Hilbert's Tenth Problem.

K. Eisenträger was partially supported by NSF grant DMS-0801123 and a grant from the John Templeton Foundation. A. Shlapentokh was partially supported by NSF grants DMS-0354907 and DMS-0650927.

existentially define one of these sets for a large class of fields: we will prove that the set of p-th powers is existentially definable in *any* function field K of characteristic $p > 2$ whose constant field has transcendence degree at least one over $\mathbb{F}_p$.

By a *function field (in n variables)* over a field F we mean a field K containing F and n elements $x_1, \ldots, x_n$, algebraically independent over F, such that $K/F(x_1, \ldots, x_n)$ is a finite algebraic extension. The algebraic closure of F in K is called the constant field of K, and it is a finite extension of F.

Given the present difficulties of showing that Hilbert's Tenth Problem, or, equivalently, the existential theory of an arbitrary function field of positive characteristic is undecidable, one can also consider a weaker result, namely proving the undecidability of the first-order theory of these fields. Duret showed that the first-order theory of function fields (in n variables) over algebraically closed fields of positive characteristic is undecidable ([3]). In [1] Cherlin showed that the first-order theory of $F(t)$ is undecidable for infinite perfect fields F of positive characteristic. In [14] Pheidas extended this result to rational function fields $F(t)$ for any field F of characteristic $p \geq 5$, but he had to add a transcendental parameter t to the ring language to prove undecidability.

In this paper we generalize Duret's and Pheidas' results and prove that the first-order theory in the language of rings without parameters of *any* function field over a field of characteristic greater than 2 is undecidable. In the case the field of constants is algebraic over a finite field, we can also treat the case of characteristic 2.

The paper is organized as follows. We first show that the first-order theory for function fields K of positive characteristic is undecidable in the language of rings with finitely many parameters. This is done by defining a model of the nonnegative integers with addition and multiplication in K. Then, using a result of R. Robinson, we show that this also gives us the undecidability of the theory of K in the language of rings without parameters. The details of this argument are discussed in Section 5.

We have endeavored to make the presentation as uniform as possible across all the different types of fields. Thus, in the second section of the paper we first show that in order to establish the first-order undecidability of a function field of characteristic $p > 0$, it is enough to show that p-th powers of a specific field element are first-order definable. To define p-th powers of a specific element, the techniques we use depend on the constant field. When the constant field is algebraic over a finite field we generalize equations that have previously been used in [19, 4] to reduce the problem to the rational function field case. This is done in Section 3. When the constant field has transcendence degree ≥ 1 over $\mathbb{F}_p$, things are more complicated. In Section 4 we show that the p-th powers we want to define occur as x-coordinates of the K-rational points on a certain elliptic curve. We then use a theorem by Moret-Bailly about the rank of elliptic curves in extensions of function fields to reduce the general case to the rational function field case. The theorem by Moret-Bailly was also used in [5, 7, 12] to obtain undecidability results. Moret-Bailly's theorem only holds in odd characteristic, and so for higher transcendence degree we obtain undecidability for function fields of odd positive characteristic only.

2. USING p-TH POWERS TO CONSTRUCT A MODEL OF THE POSITIVE INTEGERS

2.1. **Statement of results.** The main result that we will prove in the first four sections is the following:

Theorem 2.1. *Let K be a function field of characteristic $p > 2$ or a function field in one variable of characteristic 2 whose constant field is algebraic over $\mathbb{F}_2$. There exists a finite set of parameters $\{z_1, \dots z_k\} \subseteq K$ (depending on K) such that first-order theory of K is undecidable in the language of rings augmented by $\{z_1, \dots, z_k\}$.*

From the result in Section 5 we obtain a strengthening of Theorem 2.1:

Theorem 2.2. *Let K be as in Theorem 2.1. Then the first-order theory of K is undecidable in the language of rings without parameters.*

2.2. **Idea of proof.** In this section we show that to prove Theorem 2.1, it is enough to define p-th powers of an element in the field with simple poles and zeros. To prove that this is enough we use a result of J. Robinson that shows how to define multiplication of positive integers in terms of addition and divisibility.

Remark 2.3. Since we are only interested in the function field K and not the underlying field F, we can always replace F with $F(x_2, \dots, x_n)$ and view a function field K/F in n variables as a function field $K/F(x_2, \dots, x_n)$ in one variable. So in the following all the function fields we consider will be function fields in one variable.

Notation 2.4. Let K be a function field (in one variable) of positive characteristic p over a field of constants F. Let F_0 be the algebraic closure of a finite field in F. Let $t \in K \setminus F$, and let $n = [K : F(t)]$. Let F' be the algebraic closure of F and let $F'K$ be the compositum of F' and K inside the algebraic closure of K.

The following result is due to J. Robinson (see [16]).

Lemma 2.5. *There exists a first-order formula $\mathscr{F}$ in the language $\langle \mathbb{Z}_{>0}, +, | \rangle$ such that for integers k, m, n, we have $k = mn \iff \mathscr{F}(k, m, n)$. Here $a \mid b$ means "a divides b" for positive integers a, b.*

An immediate corollary of this lemma is the fact that the first-order theory of $\langle \mathbb{Z}_{>0}, +, | \rangle$ is undecidable. So to prove the undecidability of the first-order theory of K it is enough to construct a model of the positive integers with addition and divisibility in K.

We say that we have a *model* of $\langle \mathbb{Z}_{>0}, +, | \rangle$ in K if there is a bijection $\phi : \mathbb{Z}_{>0} \to D$ between $\mathbb{Z}_{>0}$ and a definable subset D of K^d (for some $d \geq 1$), such that the graphs of $+$ and $|$ on D induced by ϕ correspond to definable subsets of D^3 and D^2, respectively.

As we will see in Theorem 2.9 below, we can construct a model of $\langle \mathbb{Z}_{>0}, +, | \rangle$ if we can define p-th powers of a specific element.

2.3. **From p-th powers of a special element to arbitrary p-th powers.** The known definitions of p-th powers in general are produced in the following manner: first define p-th powers of a specific element, then use p-th powers of this element to produce p-th powers of arbitrary elements.

Proposition 2.6. *Suppose the set $p(K, t) := \{x \in K : \exists s \in \mathbb{Z}_{\geq 0}, x = t^{p^s}\}$ is definable in K for some $t \in K \setminus F$ such that t has no zeros or poles at any $F'K$-prime ramifying in the extension $F'K/F'(t)$. Then the following subset of K^2 is also definable in K:*

$$\mathscr{X}(K) := \{(x, x^{p^s}) : s \in \mathbb{Z}_{\geq 0}, x \in K\}.$$

The proof of this proposition originally appeared in [19] for $p > 2$ and in [4] for $p = 2$. Most of the necessary ideas were already present in [13] and [18]. For the convenience of the reader we reproduce this proof in the appendix. (See Notation 7.1 and Lemmas and Propositions 7.20 – 7.24.)

Both [22] and [19] also prove the following corollary which will be needed below.

Corollary 2.7. *Let $t \in K \setminus F$ be as in Proposition 2.6, i.e. assume t has no zeros or poles at any $F'K$-prime ramifying in the extension $F'K/F'(t)$ and $p(K,t)$ is definable. Then the set*

$$\mathscr{B}(K,t) := \{(t^{p^s}, x^{p^s}, x) : s \in \mathbb{Z}_{>0}, x \in K\}$$

is definable in K.

Proof. Observe that by assumption all the zeros of t are simple in K. If $\mathfrak{p}$ is a K-zero of t, $x \in K$, and

$$v_i = x^i + \frac{1}{t}, \text{ where } i = 2, 3,$$

then $\mathrm{ord}_{\mathfrak{p}} v_i < 0$. Indeed if $\mathrm{ord}_{\mathfrak{p}} x \geq 0$ then $\mathrm{ord}_{\mathfrak{p}} v_i = -\mathrm{ord}_{\mathfrak{p}} t < 0$, and if $\mathrm{ord}_{\mathfrak{p}} x < 0$, then

$$\mathrm{ord}_{\mathfrak{p}} x^i < \mathrm{ord}_{\mathfrak{p}} t^{-1}$$

(since $\mathfrak{p}$ is a simple zero of t), and thus $\mathrm{ord}_{\mathfrak{p}} v_i = i\mathrm{ord}_{\mathfrak{p}} x$. Now set $w_i = \frac{1}{v_i} + 1$ and observe that $\mathrm{ord}_{\mathfrak{p}} w_i = 0$. Suppose now that the following system of equations has solutions in K:

$$\exists k_{1,i} \in \mathbb{Z}_{\geq 0} : z_{1,i} = (w_i t)^{p^{k_{1,i}}} \tag{2.1}$$

$$\exists k_{2,i} \in \mathbb{Z}_{\geq 0} : z_{2,i} = w_i^{p^{k_{2,i}}} \tag{2.2}$$

$$\exists k_3 \in \mathbb{Z}_{\geq 0} : z_3 = t^{p^{k_3}} \tag{2.3}$$

$$z_3 z_{2,i} = z_{1,i} \tag{2.4}$$

Since $\mathrm{ord}_{\mathfrak{p}} w_i = 0$, from (2.4) we conclude that $\mathrm{ord}_{\mathfrak{p}} z_3 = \mathrm{ord}_{\mathfrak{p}} z_{1,i}$ and therefore $k_{1,i} = k_3$ implying for both values of i that $k_{2,i} = k_{1,i} = k_3 = k$. Next set

$$u_i = \frac{1}{z_{1,i}/z_3 - 1} = v_i^{p^k}$$

and

$$y = \frac{u_3 - z_3^{-1}}{u_2 - z_3^{-1}} = \frac{x^{3p^k}}{x^{2p^k}} = x^{p^k}.$$

Finally we note that by Proposition 2.6 the set of pairs of solutions to (2.1) – (2.4) is definable. □

2.4. **Constructing a model with addition and divisibility.** The final result we will need to construct a model of $\langle \mathbb{Z}_{>0}, +, | \rangle$ is the the following proposition.

Proposition 2.8. *Let t be as above. If $\mathscr{X}(K) = \{(x, x^{p^s}), x \in K, s \in \mathbb{Z}_{>0}\}$ is definable in K, then the set*

$$\mathscr{C}(K,t) := \{(t^{p^b}, t^{p^c}, t^{p^{b+c}}) : b, c > 0\}$$

is definable in K.

Proof. Consider the following system of equations:

$$\exists x, z \in K : \begin{cases} x - 1 = t^{p^b} \\ \exists l \in \mathbb{Z}_{>0} : z = ((t+1)t^{p^c})^{p^l} \\ \exists j \in \mathbb{Z}_{>0} : z/x = t^{p^j} \end{cases} \tag{2.5}$$

By Proposition 2.6 the equations in (2.5) are first-order equations over K. We claim that for any $b, c > 0$, if this system has solutions $x, z \in K$ then $x/z = t^{p^{b+c}}$. Indeed, from the first equation we conclude that $x = (t+1)^{p^b}$. From the second equation we get that $z = (t+1)^{p^l} t^{p^{c+l}}$. Finally, from the third equation we have that $(t+1)^{p^l - p^b} t^{p^{c+l}} = t^{p^j}$. The only way this equality can hold is for $l = b$ and $j = b + c$. Conversely, we can always satisfy the system if $x = (t+1)^{p^b}$ and $z = (t+1)^{p^b} t^{p^{c+b}}$. □

We are now ready for the following theorem.

Theorem 2.9. *Assume that t has no zeros or poles at any $F'K$-prime ramifying in the extension $F'K/F'(t)$ (and thus all poles and zeros of t are simple). Suppose that the set $p(K,t)$ is definable in K. Then $\langle \mathbb{Z}_{>0}, +, | \rangle$ has a model over K.*

Proof. We map $s > 0$ to t^{p^s}. Then $s = s_1 + s_2 \Leftrightarrow (t^{p^{s_1}}, t^{p^{s_2}}, t^{p^s}) \in \mathscr{C}(K,t)$. Further $s_1 \Big| s_2$ if and only if $(p^{s_1} - 1) \Big| (p^{s_2} - 1)$ if and only if there exists $x \in K$ such that

$$x^{p^{s_1}-1} = t^{p^{s_2}-1}, \tag{2.6}$$

since at least one pole or zero of t is simple. Indeed suppose that the equality holds and let $\mathfrak{q}$ be a simple pole or zero of t. Then

$$p^{s_2} - 1 = \pm \mathrm{ord}_{\mathfrak{q}} t^{p^{s_2}-1} = \pm \mathrm{ord}_{\mathfrak{q}} x^{p^{s_1}-1} \equiv 0 \mod p^{s_1} - 1.$$

Conversely, if $p^{s_2} - 1 = l(p^{s_1} - 1)$ for some $l \in \mathbb{Z}_{>0}$, then we can set $x = t^l$ and (2.6) will hold.

Hence $s_1 \Big| s_2$ if and only if

$$\exists\, x, y \in K \left((t^{p^{s_1}}, y, x) \in \mathscr{B}(K,t) \ \wedge \ y/x = t^{p^{s_2}}/t \right).$$

The result now follows from the fact that the sets $p(K,t), \mathscr{B}(K,t)$ and $\mathscr{C}(K,t)$ are all definable in K. □

2.5. **Defining p-th powers of one special element.** We now address the issue of defining p-th powers of one specific element when the constant field is perfect. In the next proposition we observe that if we avoid ramified zeros and poles and consider rational functions only, we have the desired result.

Proposition 2.10 ([22], Lemma 8.3.3, Corollary 8.3.4, and Proposition 8.3.8)**.** *Assume t has no zeros or poles with factors ramifying in the extension $F'K/F'(t)$. (This assumption implies that all zeros and poles of t are simple in $F'K$ and K and thus t has no zeros or poles ramifying in the extension $K/F(t)$.) Let $a = 1$ if $p > 2$ and let $a = 2$ if $p = 2$. Suppose further that F is perfect and for some element $w \in F(t)$, having no poles or zeros at the*

primes ramifying in the extension $K/F(t)$, there exist $u, v \in K$ such that the following system is satisfied.

$$\begin{cases} \dfrac{1}{w} - \dfrac{1}{t} = u^{p^a} - u \\ w - t = v^{p^a} - v \end{cases} \tag{2.7}$$

Then for some $s \in \mathbb{Z}_{\geq 0}$ we have that $w = t^{p^{as}}$. Conversely, if $w = t^{p^{as}}, s \geq 0$, then there exist $u, v \in F(t)$ satisfying (2.7). (For the last assertion we do not need the requirement that F is perfect.)

Proof. This proposition is proved in the appendix (Proposition 7.12). □

Unfortunately, we cannot always assume that an arbitrary rational field element w has only unramified poles and zeros. However, this problem can be solved rather easily if we modify the equations. The next remark and the proposition below deal with an arbitrary element $w \in F(t)$.

Remark 2.11. We recall from Notation 2.4 that K/F was a function field of positive characteristic p and F_0 denoted the algebraic closure of a finite field in F. By Proposition 7.3 and Lemma 7.4 from the appendix we can enlarge the constant field and assume that F_0 contains elements $c_0 = 0, c_1, \ldots, c_{2n(\alpha)+2}$ such that when $i \neq j$ we have for all $k \in \mathbb{Z}_{\geq 0}$ that $c_i^{p^k} \neq c_j$. Here $n(\alpha)$ is the constant that is defined in Lemma 7.4 from the appendix.

We can now prove the following proposition.

Proposition 2.12. *Assume F is perfect, t is not a p-th power in K and has no poles or zeros at primes ramifying in the extension $F'K/F'(t)$. Let $c_0, \ldots, c_{2n(\alpha)+2}$ be as in Remark 2.11, and let $V_i = \{c_i^{p^k}, k \in \mathbb{Z}_{\geq 0}\}$.*

Let $a = 1$ if $p > 2$ and let $a = 2$ if $p = 2$. Let $w \in F(t)$, suppose that (2.7) *holds and for all $i \neq j \in \{1, \ldots, 2n(\alpha)+2\}$, for some $b \in V_i, c \in V_j$ there exist $u_{i,j,b,c}, v_{i,j,b,c} \in K$ such that*

$$\begin{cases} \dfrac{w-b}{w-c} - \dfrac{t-c_i}{t-c_j} = u_{i,j,b,c}^{p^a} - u_{i,j,b,c} \\ \dfrac{w-c}{w-b} - \dfrac{t-c_j}{t-c_i} = v_{i,j,b,c}^{p^a} - v_{i,j,b,c} \end{cases} \tag{2.8}$$

Then for some $s \in \mathbb{Z}_{\geq 0}$ we have that $w = t^{p^{as}}$. Conversely, if $w = t^{p^{as}}$ for some $s \in \mathbb{Z}_{\geq 0}$ then the equations can be satisfied as specified above (even if F is not perfect).

Proof. First of all, by Lemma 7.15 and Lemma 7.4, we conclude that for some c_i, c_j and $b \in V_i, c \in V_j$, we have that $t-c_i, t-c_j, w-b, w-c$ do not have zeros at any prime ramifying in the separable extension $K/F(t)$ and therefore $\dfrac{t-c_i}{t-c_j}, \dfrac{w-b}{w-c} \in F(t)$ do not have zeros or poles at any primes ramifying in the extension $K/F(t)$. Now applying Proposition 2.10 we conclude that either

$$\frac{w-b}{w-c} = \left(\frac{t-c_i}{t-c_j}\right)^{p^{as}} \tag{2.9}$$

for some $s > 0$ or

$$\frac{w-b}{w-c} = \frac{t-c_i}{t-c_j}. \tag{2.10}$$

In the first case from (2.9) we deduce

$$1+\frac{c-b}{w-c}=1+\frac{c_j^{p^{as}}-c_i^{p^{as}}}{t^{p^{as}}-c_j^{p^{as}}}$$

and therefore

$$w=At^{p^{as}}+B,$$

where $A,B\in F_0$, making w a p^a-th power of an element of $F(t)$. Let $\tilde{w},\tilde{b},\tilde{c}$ be such that $\tilde{w}^{p^a}=w,\tilde{b}^{p^a}=b,\tilde{c}^{p^a}=c$ and observe that if $b\in V_i$, then $\tilde{b}\in V_i$ and similarly, if $c\in V_j$, then $\tilde{c}\in V_j$. Note further, that as in the proof of Proposition 2.10, we can rewrite (2.8) in the following way: for all $i\neq j\in\{1,\dots,2n(\alpha)+2\}$, for some $\tilde{b}\in V_i,\tilde{c}\in V_j$ there exist $u_{i,j,\tilde{b},\tilde{c}},v_{i,j,\tilde{b},\tilde{c}}\in K$ such that

$$\text{(2.11)}\qquad\begin{cases}\dfrac{\tilde{w}-\tilde{b}}{\tilde{w}-\tilde{c}}-\dfrac{t-c_i}{t-c_j}=u_{i,j,\tilde{b},\tilde{c}}^{p^a}-u_{i,j,\tilde{b},\tilde{c}}\\ \dfrac{\tilde{w}-\tilde{c}}{\tilde{w}-\tilde{b}}-\dfrac{t-c_j}{t-c_i}=v_{i,j,\tilde{b},\tilde{c}}^{p^a}-v_{i,j,\tilde{b},\tilde{c}}\end{cases}$$

We can also rewrite (2.7) as in the proof of Proposition 2.10.

In the second case we obtain $w=At+B$ for some $A,B\in F_0$. However, if we plug in this expression for w into (2.7), we obtain a contradiction unless $A=1$ and $B=0$. Indeed, the only way $\frac{1}{At+B}-\frac{1}{t}=u^{p^a}-u$ can hold is for $B=0$, because unless $B=0$, the poles of $\frac{1}{At+B}$ and $\frac{1}{t}$ are different and all the poles of t are simple in K. Now consider $w-t=At-t=v^{p^a}-v$. Since t has simple poles in K, the only way this equation can hold is for $A=1$.

We now note that Case 1 can occur only finitely many times and after taking p^a-th root of w sufficiently many times we will be in the second case, concluding that $w=t^{p^{as}}$ for some non-negative integer s.

Finally we show that if $w=t^{p^{as}}$ for some $s\in\mathbb{Z}_{\geq 0}$ we can satisfy (2.7) and (2.8). To begin with, (2.7) can be satisfied by (7.26) (from the appendix). To see that we can satisfy (2.8), note that for every i and any $s\in\mathbb{Z}_{\geq 0}$ we have that $c_i^{p^{as}}\in V_i$. Therefore for all $i\neq j\in\{1,\dots,2n(\alpha)+2\}$, for some $b\in V_i,c\in V_j$ we have that

$$\left(\frac{t-c_i}{t-c_j}\right)^{p^{as}}=\frac{t^{p^{as}}-b}{t^{p^{as}}-c}$$

and therefore we can use (7.26) with $x=\dfrac{t-c_i}{t-c_j}$ to satisfy (2.8).

□

To define p-th powers of a special element t over fields of transcendence degree one and higher transcendence degree we will use some of the equations that were used in [19] and [4]. What we need to make the same arguments go through in our more general setup is a set of equations over K that forces its solutions to be in the rational function field $F(t)$ and which are satisfied by all elements t^{p^s}, $s\in\mathbb{Z}_{>0}$. I.e., we want a set $\mathscr{S}$ which is definable in K such that $p(K,t)\subseteq\mathscr{S}\subseteq F(t)$ and thus we can apply Proposition 2.12. This will be accomplished in the next two sections. For the transcendence degree one case, the equations defining $\mathscr{S}$ are given in Corollary 3.6. For higher transcendence degree, they are given in Proposition 4.7 below.

3. Defining p-th powers for function fields whose constant field is algebraic

We start with the following remark concerning known results.

Remark 3.1. Let K/F be a function field in one variable of positive characteristic p with F algebraic over a finite field. When F has an extension of degree p, the results in [19] and [4] show that the existential theory of K in the language of rings with finitely many parameters and hence also the first-order theory of K in the language of rings with finitely many parameters are undecidable. In the process of showing existential undecidability of these function fields it was also shown that for a field K as above the set $\mathscr{X}(K) = \{(x, x^{p^s}), x \in K, s \in \mathbb{Z}_{\geq 0}\}$ is *existentially* definable. Hence we can make additional assumptions about the field of constants for the algebraic case and assume that we are in a situation that is not covered by [19] or [4].

Notation 3.2.

- Let K/F be a function field in one variable of positive characteristic p.
- Assume that F is algebraic over a finite field and has no extension of degree p.
- Let t be a fixed element of $K \setminus F$ which is not a p-th power in K.
- We write g_K for the genus of K, and when $f \in F[X, Y]$ defines a plane curve $\mathscr{C}$ over F, we denote by g_f the genus of the function field of $\mathscr{C}$ and also refer to this as the genus of f.

In this section we will show how to define p-th powers of the element t under the above assumptions.

Lemma 3.3. *For a pair of positive integers $k = p^l, u$, let*

$$f_{k,u}(X, Y) = Y^{p^k} - Y + \frac{1}{\prod_{i=1}^{u}(X - d_i)},$$

where $d_1, \ldots, d_u$ are distinct elements of F. Then for any $a \in F$ there exists $b \in F$ such that $f_{k,u}(a, b) = 0$.

Proof. Fix an $a \in F$ and let α_1, α_2 be roots of $f_{k,u}(a, Y)$ in the algebraic closure of F. Then $(\alpha_1^{p^k} - \alpha_2^{p^k}) - (\alpha_1 - \alpha_2) = 0$. Thus, $\alpha_1 - \alpha_2 = c$ belongs to a field of degree $k = p^l$ over a field of p elements and therefore $c \in F$. Since F is algebraic over a finite field, the extension $F(\alpha_1)/F$ is cyclic. Assume that $[F(\alpha_1) : F] = m > 1$ and let $\sigma \in \mathrm{Gal}(F(\alpha_1)/F)$ be a generator. Then for some $c \in F$ we have that $\sigma(\alpha_1) = \alpha_1 + c$ and $\mathrm{id}(\alpha_1) = \sigma^m(\alpha_1) = \alpha_1 + mc = \alpha_1$. Thus $m \equiv 0 \mod p$, and $F(\alpha_1)/F$ has a subextension of degree p over F, contradicting our assumption on F. □

Lemma 3.4. *There exists a set $A \subset K^2$, diophantine over K such that $A \subset F^2$ and for all $a \in F$ there exists $c \in F$ such that $(a, c) \in A$. In particular, F is existentially definable in K.*

Proof. Before we proceed with the proof we should note that using the effective version Chebotarev Density Theorem (see [8], Proposition 6.4.8) one could show that any infinite field algebraic over a finite field is anti-Mordellic and therefore one could use a result of Poonen and Pop to see that F is first-order definable in K (see [15]). However in our case we can give a very simple existential definition of F along the lines of [3], [10] and [21].

The idea is to construct an equation f whose genus is greater than the genus of K and then use the Riemann-Hurwitz formula to show that all the K-rational solutions must be F-rational. We also have to ensure that f has enough solutions over F. Consider an

equation $f_{k,u}(X,Y) = Y^{p^k} - Y + \prod_{i=1}^{u} \frac{1}{(X-d_i)}$, where k and u are as above and $d_1, \ldots, d_u$ are all distinct and in F. For suitable large k and u the genus of this equation is higher than the genus of K. To see that this is so consider the field extension $F_{k,u}(X,Y)$ of $F(X)$ where $f_{k,u}(X,Y) = 0$. It is clear that in this extension the primes corresponding to $(X-d_1), \ldots, (X-d_u)$ are completely ramified. It is also clear from considering the difference between any two roots of this equation as in the lemma above, that no other prime of $F(X)$ is ramified in the extension $F_{k,u}(X,Y)/F(X)$. Furthermore, the $F_{k,u}(X,Y)$-factor of $(X-d_i)$ is of relative degree 1 and also of degree 1 in $F(X,Y)$. Let $g_X = 0$ be the genus of $F(X)$, and let $g_{f_{k,u}}$ be the genus of $F_{k,u}(X,Y)$. Then by the Riemann-Hurwitz formula and Remark 3.5.7 of [8], we have that

$$2g_{f_{k,u}} - 2 \geq p^k(g_X - 2) + \deg \sum_{i=1}^{u} (p^k - 1)\mathfrak{P}_i,$$

where for $i = 1, \ldots, u$, we let $\mathfrak{P}_i$ denote the prime above $X - d_i$. Thus,

$$g_{f_{k,u}} \geq \frac{1}{2}(u(p^k-1) - 2p^k + 2) = \frac{1}{2}(p^k u - u - 2p^k + 2) = \frac{(u-2)(p^k-1)}{2}.$$

Now choose k_0, u_0 large enough so that $g_{f_{k_0,u_0}}$ is greater than g_K, the genus of K. Let $f := f_{k_0,u_0}$, let $F(X,Y)$ be the corresponding field extension of $F(X)$, and g_f its genus.

Now assume that there exists a solution $x, y \in K \setminus F$ to $f(X,Y) = 0$. Then $F(X,Y) \simeq F(x,y)$, so $F(X,Y)$ can be viewed as a subfield of K. If x is not a p-th power in K, then the extension $K/F(x)$ is separable (see Lemma B1.32 of [22]) and as a consequence of the Riemann-Hurwitz formula, $g_K \geq g_f$, contradicting the hypothesis.

If x is a p-th power in K, then $\prod_{i=1}^{u}(x-d_i)$ is also a p-th power in K since F is algebraic over a finite field, and therefore all the coefficients d_i of f are also p-th powers. Consequently y is also a p-th power in K. Thus, by replacing all the terms of f by their p-th roots we can obtain a new equation $f^{(1)}(X,Y) = 0$ which is a "p-th root" of f. The equation $f^{(1)}$ has the same genus as f because its genus only depends on the values k_0, u_0 that were chosen above. Since x and y were both p-th powers in K, the equation $f^{(1)}(X,Y) = 0$ also has a non-constant solution in K. Thus, at some point we will have an equality $f^{(\ell)}(\tilde{x}, \tilde{y}) = 0$, with the genus of $f^{(\ell)}$ higher than the genus of K and $\tilde{x}$ not a p-th power in K. Consequently, $f(X,Y) = 0$ can only have constant solutions in K. At the same time, by Lemma 3.3, for all $x \in F$ we have $y \in F$ so that $f(x,y) = 0$. □

Proposition 3.5 (Slightly modified Theorem 10.1.1 of [22]). *Suppose for some $w \in K$, for infinitely many primes $\mathfrak{A}$ of $F(t)$ we have that*

$$w \equiv b(\mathfrak{A}) \mod \mathfrak{A}, \tag{3.1}$$

where $b(\mathfrak{A}) \in F$ and we interpret the equivalence as saying that for any factor $\mathfrak{c}$ of $\mathfrak{A}$ in K we have that $\mathrm{ord}_{\mathfrak{c}}(w - b(\mathfrak{A})) \geq e(\mathfrak{c}/\mathfrak{A})$, the ramification degree of $\mathfrak{c}$ over $\mathfrak{A}$. Then $w \in F(t)$.

Proof. Let $\{\omega_1 = 1, \ldots, \omega_k\}$ be a basis of K over $F(t)$. Further, let $\mathscr{V}$ be the set of all primes of $F(t)$ satisfying the following conditions.

(1) Each prime of $\mathscr{V}$ is unramified in the extension $K/F(t)$.
(2) w is integral at all primes of $\mathscr{V}$.
(3) For each $\mathfrak{A} \in \mathscr{V}$ we have that (3.1) holds.

(4) $\{\omega_1, \ldots, \omega_n\}$ is a local integral basis with respect to every prime of $\mathscr{V}$ or in other words every $\mathfrak{A} \in \mathscr{V}$ is relatively prime to the the discriminant of the basis.

First of all we note that from (4) we conclude that any element $z \in K$ integral with respect to $\mathfrak{A} \in \mathscr{V}$, i.e. integral with respect to every factor of $\mathfrak{A}$ in K, can be written as $z = \sum_{i=1}^{n} f_i\omega_i$, where for all $i = 1, \ldots, n$, we have that $f_i \in F(t)$ and f_i is integral at $\mathfrak{A}$. Next observe that only finitely many primes of $F(t)$ can fail to satisfy (1), (2) and (4), and therefore $\mathscr{V}$ is an infinite set. Now write $w = \sum_{i=1}^{n} A_i\omega_i$, where $A_i \in F(t)$. Observe that for all $\mathfrak{A} \in \mathscr{V}$, we have that $w - b(\mathfrak{A})$ is equivalent to zero modulo every prime $\mathfrak{A}$ of $\mathscr{V}$. At the same time

$$w - b(\mathfrak{A}) = A_1 - b(\mathfrak{A}) + A_2\omega_2 + \cdots + A_n\omega_n.$$

For each prime $\mathfrak{A}$ of $\mathscr{V}$, let $B(\mathfrak{A}) \in F(t)$ be such that $\mathrm{ord}_{\mathfrak{A}}B(\mathfrak{A}) = 1$. Then $z = \dfrac{w - b(\mathfrak{A})}{B(\mathfrak{A})}$ is integral at $\mathfrak{A}$ and thus $z = \sum_{i=1}^{n} f_i(\mathfrak{A})\omega_i$, where $f_i(\mathfrak{A})$ are elements of $F(t)$ integral at $\mathfrak{A}$. We observe further

$$A_1 - b(\mathfrak{A}) + A_2\omega_2 + \cdots + A_n\omega_n = w - b(\mathfrak{A}) = B(\mathfrak{A})z = \sum_{i=1}^{n} B(\mathfrak{A})f_i(\mathfrak{A})\omega_i.$$

Thus, for $i = 2, \ldots, n$ for all $\mathfrak{A}$ in $\mathscr{V}$ we have that $A_i = B(\mathfrak{A})f_i(\mathfrak{A})$, implying that for $i = 2, \ldots, n$, for all $\mathfrak{A}$ in $\mathscr{V}$ we have that $\mathrm{ord}_{\mathfrak{A}}A_i > 0$. This is impossible unless for $i = 2, \ldots, n$ we have that $A_i = 0$ and thus $w \in F(t)$. □

Corollary 3.6. *Suppose that for some $w \in K$ and infinitely many $(b, c) \in F^2$ we have that the following system has a solution u_b in K:*

$$\frac{1}{w - c} - \frac{1}{t - b} = u_b^p - u_b \tag{3.2}$$

Then $w \in F(t)$. Conversely, if for some positive integer s we have that $w = t^{p^s}$, then for any $b \in F$, there exist $c \in F, u_b \in F(t)$ such that equation (3.2) is satisfied.

Proof. First of all observe that the extension $K/F(t)$ is separable since t is not a p-th power in K. (See Lemma B1.32 of [22].) Thus only finitely many primes ramify in the extension $K/F(t)$. Let $\mathfrak{P}_b$ be the prime of $F(t)$ corresponding to $t - b$, and let $\mathfrak{p}_b$ be any factor of $\mathfrak{P}_b$ in K. Since only finitely many primes ramify in $K/F(t)$ it follows that in K $\mathrm{ord}_{\mathfrak{p}_b}(t-b) = 1$ for all but finitely many $b \in F$. On the other hand, for any pole $\mathfrak{q}_b$ of u_b in K we have that $\mathrm{ord}_{\mathfrak{q}_b}(u_b^p - u_b) \equiv 0 \mod p$. Thus, for all but finitely many $b \in F$, for all factors $\mathfrak{p}_b$ of the rational prime $\mathfrak{P}_b$ in K we have that $\mathrm{ord}_{\mathfrak{p}_b}(w - c) > 0$. In other words, for infinitely many $(b, c) \in F^2$ we have that $w \equiv c \mod \mathfrak{P}_b$, where $\mathfrak{P}_b$ is, as above, the zero divisor in K and $F(t)$ of $t - b$. Now the first assertion of the corollary follows from Proposition 3.5. The second assertion of the corollary follows from equation (7.26) (from the appendix). □

Finally we note that putting together Remark 3.1, Proposition 2.12, Lemma 3.4 and Corollary 3.6 we obtain the main result of this section.

Theorem 3.7. *Let K be a function field (in one variable) whose constant field F is algebraic over a finite field of characteristic $p > 0$. Let t be an element of $K \setminus F$ such that no zero or pole of t ramifies in the extension $F'K/F'(t)$. Then the set $p(K, t) = \{x \in K : \exists s \in \mathbb{Z}_{>0}\ x = t^{p^s}\}$ is first-order definable in K.*

Remark 3.8. We would like to note here that given our assumptions on F and Lemma 7.4, any $t \in K \setminus F$ such that it is not a p-th power in K and therefore generates a separable rational subextension, can always be replaced by $\dfrac{t-a}{t-b}$, with a, b algebraic over a finite field, so that the resulting element has no zeros or poles ramifying in the extension $F'K/F'(t) = F'K/F'\left(\dfrac{t-a}{t-b}\right)$.

4. Defining p-th powers over fields of higher transcendence degree

Let K be a function field of characteristic $p > 2$ with constant field F, and assume that F has transcendence degree at least one over a finite field. To define p-th powers of a suitable element t we will use a theorem by Moret-Bailly ([12]). Here, we quickly review Moret-Bailly's notation and state the theorem in the form we need.

Definition 4.1. Let $u : A \to B$ be a morphism of abelian groups. We say that u is *p-almost bijective* if u is injective and Coker u is a finite p-group.

By [12, Theorem 1.8], the following theorem holds:

Theorem 4.2. *Let F be a field of characteristic $p > 2$, and assume that F contains an element which is transcendental over $\mathbb{F}_p$. Let K be a function field in one variable with constant field F, and let*

$$E : y^2 = P(x)$$

be an elliptic curve which is defined over a finite field contained in F. There exists a non-constant element $t \in K$ such that t is not a p-th power in K and the elliptic curve $\mathscr{E}$ given by

$$\mathscr{E} : P(t)\, y^2 = P(x)$$

has the property that the natural homomorphism $\mathscr{E}(F(t)) \hookrightarrow \mathscr{E}(K)$ induced by the inclusion $F(t) \hookrightarrow K$ is p-almost bijective.

Notation 4.3. From now on, let $P(x), E$ and t be as in Theorem 4.2. Let s be an element in a quadratic extension of K satisfying $s^2 = P(t)$. Let $q = p^r$ be the size of a finite field containing all the coefficients of the equation defining E.

Let F' be as above an algebraic closure of F, and as before let $K' = F'K$.

By [12, Theorem 1.8], it follows that the natural homomorphism $\mathscr{E}(F(t)) \hookrightarrow \mathscr{E}(K')$ is still p-almost bijective.

Proposition 4.4. *The set $\mathscr{E}(F(T))$ is diophantine over K and over K'.*

Proof. Let $A := \mathscr{E}(F(T))$ and $B := \mathscr{E}(K)$. The set B is clearly diophantine over K, and B is finitely generated by [23, Theorem 6.1, p. 230]. By Theorem 4.2, A is a subgroup of finite index in B and B/A is a finite p-group.

Hence for some integer k we have that $p^k B \subseteq A$ and $p^k B$ has finite index in B. Since B is diophantine over K, and since multiplication by p^k is given by explicit equations, the set $p^k B$ is diophantine over K. It is easy to see that this implies that A is diophantine over K:

Let $Q_1, \ldots, Q_\ell$ be coset representatives for $p^k B$ in A. Then for $P \in \mathscr{E}(K)$

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

The same argument with K replaced by K' shows that A is also diophantine over K'. $\square$

From the proposition above we also obtain the following easy corollary.

Corollary 4.5. *There exists a polynomial equation $R(u, v, x_1, \ldots, x_l) \in K[u, v, x_1, \ldots, x_l]$ such that $R(u, v, x_1, \ldots, x_l) = 0$ for some $u, v, x_1, \ldots, x_l \in K'$ implies (u, v) are affine coordinates of a point in $\mathscr{E}(F(t))$. Conversely, if (u, v) are affine coordinates of a point in $\mathscr{E}(F(t))$ the equation $R(u, v, x_1, \ldots, x_l) = 0$ can be satisfied with $x_1, \ldots, x_l \in K$.*

Next we observe that p-th powers occur as affine coordinates of points of $\mathscr{E}$.

Lemma 4.6. *Let $\mathscr{E}, s, t, q$ be as in Notation 4.3. The point $(t^{q^m}, s^{q^m-1}) \in \mathscr{E}(F(t))$.*

Proof. Observe that $(P(t))^{q^m} = P(t^{q^m})$. Thus, $P(t)(s^{q^m-1})^2 = (P(t))^{q^m} = P(t^{q^m})$. Also $q^m - 1$ is even, so the point (t^{q^m}, s^{q^m-1}) has coordinates in the ground field. □

We conclude with the propositions defining p-th powers of t for the case of K of transcendence degree greater than one. We need to consider two cases: an element t selected so that Theorem 4.2 holds has zeros or poles which are not simple in $F'K$ or t does not have such zeros or poles.

Proposition 4.7. *Assume that t has no zeros or poles at any valuation ramifying in the extension $F'K/F'(t)$ and for some $z, w, u, v \in K$ the following system is satisfied over K' in the remaining variables.*

$$
\left\{
\begin{array}{c}
R(w, z, x_1, \ldots, x_l) = 0 \\
\forall i, j \in \{1, \ldots, 2n(\alpha) + 2\} \exists b \in V_i, c \in V_j : \\
\quad \dfrac{t - c_i}{t - c_j} - \dfrac{w - b}{w - c} = u^p_{i,j,b,c} - u_{i,j,b,c} \\
\quad \dfrac{t - c_j}{t - c_i} - \dfrac{w - c}{w - b} = v^p_{i,j,b,c} - v_{i,j,b,c} \\
\quad w - t = v^p - v \\
\quad \dfrac{1}{w} - \dfrac{1}{t} = u^p - u
\end{array}
\right. \tag{4.1}
$$

Then for some $s \in \mathbb{Z}_{\geq 0}$ we have that $w = t^{p^s}$. Conversely, if $w = t^{p^s}$, then the system has solutions in K.

In the second case we need to replace t by some t' without "bad" poles and zeros. Without loss of generality assume $t' = \dfrac{t - c_1}{t - c_2}$ is such that all of its poles and zeros in $F'K$ are simple. (We have enough constants algebraic over F_0 to construct t' by Remark 2.11.) Observe that $F(t) = F(t')$. We now modify slightly Proposition 4.7.

Proposition 4.8. *Assume that for some $z, w, w', u, v \in K$ the following system is satisfied over K' in all the remaining variables.*

$$
\left\{
\begin{array}{c}
R(w, z, x_1, \ldots, x_l) = 0 \\
\exists b \in V_1, c \in V_2 : w' = \frac{w-b}{w-c} \\
\forall i, j \in \{1, \ldots, 2n(\alpha) + 2\} \exists b \in V_i, c \in V_j : \\
\quad \dfrac{t' - c_i}{t' - c_j} - \dfrac{w' - b}{w' - c} = u^p_{i,j,b,c} - u_{i,j,b,c} \\
\quad \dfrac{t' - c_j}{t' - c_i} - \dfrac{w' - c}{w' - b} = v^p_{i,j,b,c} - v_{i,j,b,c}
\end{array}
\right. \tag{4.2}
$$

Then for some $s \in \mathbb{Z}_{\geq 0}$ we have that $w' = (t')^{p^s}$. Conversely, if $w' = (t')^{p^s}$, then the system has solutions in K.

Remark 4.9. The proof of Proposition 2.6 that p-th powers of the special element t allow us to define p-th powers of arbitrary elements x in K only used equations involving existential quantifiers. The proofs of Propositions 4.7 and 4.8 which defined p-th powers of t also only used existential quantifiers. So when the constant field of K contains transcendental elements over $\mathbb{F}_p$, the set $\left\{(x, x^{p^s}) : x \in K, s \in \mathbb{Z}_{\geq 0}\right\}$ is actually *existentially* definable in K.

5. Ring language

In this section we address the issue of the language needed to produce an undecidable set of sentences. We have already shown that we can construct a model of the positive integers $\mathbb{Z}_{>0}$ (and hence also of $\mathbb{Z}_{\geq 0}$) in the function field K. We used this model to prove Theorem 2.1.

In this section we will show that this easily implies Theorem 2.2 by using a result of R. Robinson, so we obtain undecidability of the first-order theory of K in the language of rings *without* parameters.

Corollary 5.1 (Theorem 2.2)**.** *Let K be a function field of characteristic $p > 2$. Then the first-order theory is undecidable in the language of rings without parameters. When K is a function field in one variable whose constant field is algebraic over a finite field, then we also obtain undecidability in characteristic 2.*

Proof. From the previous sections it follows that the equations we used to construct a model of $\mathbb{Z}_{\geq 0}$ are in the language $L_{\bar{d}} = \langle +, \cdot;\ 0, 1, \{d_1, \ldots, d_r\}\rangle$, for fixed elements $d_1, \ldots, d_r$ of K. In other words, we are working in the language of rings with finitely many parameters. To show that we can achieve undecidability in the ring language *without parameters*, we use a result of R. Robinson who gave an example of a finitely axiomatizable and essentially undecidable theory Q ([24, p. 32]). A theory is *essentially undecidable* if any consistent extension of it is also undecidable. Since Q is a subtheory of $\mathbb{Z}_{\geq 0}$ ([24, p. 51]), the axioms of Q hold in $\mathbb{Z}_{\geq 0}$. Let $Ax(\mathbb{Z}_{\geq 0})$ be the conjunction of all the axioms of Q. For a sentence ψ in the language $L = \langle +, \cdot, 0, 1\rangle$ let $\phi_K(\psi, \bar{d})$ be its translation in our model, and consider the set of all L-sentences ψ for which

$$\forall \bar{w}(\phi_K(Ax(\mathbb{Z}_{\geq 0}), \bar{w}) \to \phi_K(\psi, \bar{w})) \tag{5.1}$$

is true in K. This set contains the axioms of Q and therefore the theory generated by these sentences is an extension of Q. The extension is consistent. Suppose not. Then for some ψ as above we have that $Ax(\mathbb{Z}_{\geq 0}) \to \neg\psi$ holds in $\mathbb{Z}_{\geq 0}$, and hence $\phi_K(Ax(\mathbb{Z}_{\geq 0}), \bar{d}) \to \neg\phi_K(\psi, \bar{d})$ holds in K. But this contradicts (5.1). Since the collection of all L-formulas ψ satisfying (5.1) in K is undecidable, the set of all formulas of the form (5.1) true in K is also undecidable. Finally we note that the formulas in this set are in L. □

6. Open questions

Even though we proved that the first-order theory of function fields of characteristic $p > 2$ is undecidable, we needed transcendental elements in the construction of the model of the nonnegative integers. So the following questions arise naturally:

Question 6.1. Let K be a function field as in Theorem 2.1. Does K admit a model of $\langle \mathbb{Z}_{\geq 0}, +, \cdot\rangle$ in which the equations defining the model have integer coefficients?

Question 6.2. Is the degree of unsolvability of the first-order theory of K at least that of the first-order theory of $\mathbb{Z}$?

7. Appendix

Throughout the appendix we use the following notation.

Notation 7.1.

- Let F, K, F', K', t, n be as follows:
  - K is a function field of positive characteristic p over a field of constants F.
  - F' is the algebraic closure of F.
  - $K' = F'K$ is the compositum of K and F in the algebraic closure of K.
  - $t \in K \setminus F$ and t is not a p-th power in K. (Note that the last assumption implies that $K/F(t)$ is separable.)
  - $[K : F(t)] = n$.
- Let $a = 1$ if $p > 2$, and let $a = 2$ if $p = 2$.
- Let $c_0 = 0, \ldots, c_l \in F \setminus \{\pm 1\}$ and
  - let c_i be algebraic over a finite field;
  - let $r_i \in \mathbb{Z}_{>0}$ be the smallest positive integer such that $c_i^{p^{r_i}} = c_i$;
  - assume for any $0 < j \leq r_i, m \neq i$, we have that $c_i^{p^j} \neq c_m$;
  - Let $d_{i,j} = c_i^{p^j}, j \in \mathbb{Z}_{\geq 0}$.
- Let $C(K) = \{c_0, \ldots, c_l\}$.
- Let $\mathfrak{P}$ be the zero divisor of t in $F'K$ and let $\mathfrak{Q}$ be the pole divisor of t in $F'K$. Assume further that neither $\mathfrak{P}$ nor $\mathfrak{Q}$ contain any primes ramifying in the extension $F'K/F'(t)$. By abuse of notation we will also use $\mathfrak{P}$ and $\mathfrak{Q}$ to denote the zero and pole divisor of t in K and observe that they will also contain no primes ramifying in the extension $K/F(t)$.
- Let $\mathscr{E}(K, t)$ be the set of all primes of K with factors ramifying in the extension $F'K/F'(t)$ together with all the primes which are poles and zeros of t.
- $e(K, t) = |\mathscr{E}(K, t)|$ will denote the number of primes ramifying in the extension $F'K/F'(t)$ plus the number of poles and zeros of t in K'. By Lemma 7.4 we know that $e(K, t) < \infty$ since $e(K, t) \leq n(\alpha)$ plus the number of poles and zeros of t in K'. (The constant $n(\alpha)$ is defined in Lemma 7.4.)
- Let $l > (n + 2e(K, t)) + 2$ be a positive integer.
- For any $w \in K$, let

$$C_w = \{c \in C(K) : (\forall j \in \mathbb{Z}_{\geq 0})(\forall \mathfrak{p} \in \mathscr{E}(K, t))(\mathrm{ord}_{\mathfrak{p}}(w - c^{p^j}) \leq 0)\}.$$

- For $s \in \mathbb{Z}_{\geq 0}, i, k \in \{1, \ldots, l\}, j_i \in \{1, \ldots, r_i\}, j_k \in \{1, \ldots, r_k\}$, $e = -1, 1$, $m = 0, 1$, $u, v, \mu_{i,j_i,k,j_k,e,m}$, $\lambda_1, \lambda_{-1}, \sigma_{i,j_i,k,j_k} \in K$, let

$$D(s, i, j_i, k, e, m, j_k, u, v, \mu_{i,j_i,k,j_k,e,m}, \sigma_{i,j_i,k,j_k}, \lambda_1, \lambda_{-1})$$

be the following system of equations.

$$u_{i,k} = \frac{u + c_i}{u + c_k}, \tag{7.1}$$

$$v_{i,j_i,k,j_k} = \frac{v + d_{i,j_i}}{v + d_{k,j_k}}, \tag{7.2}$$

$$v_{i,j_i,k,j_k}^{2e} t^{mp^{as}} - u_{i,k}^{2e} t^m = \mu_{i,j_i,k,j_k,e,m}^{p^{as}} - \mu_{i,j_i,k,j_k,e,m}, \tag{7.3}$$

$$v_{i,j_i,k,j_k} - u_{i,k} = \sigma_{i,j_i,k,j_k}^{p^a} - \sigma_{i,j_i,k,j_k}, \tag{7.4}$$

$$v - u = \lambda_1^{p^a} - \lambda_1 \tag{7.5}$$

$$v^{-1} - u^{-1} = \lambda_{-1}^{p^a} - \lambda_{-1} \tag{7.6}$$

- Let $j, r, s \in \mathbb{Z}_{\geq 0}$, $u, \tilde{u}, v, \tilde{v}, x, y \in K$. Let $E(u, \tilde{u}, v, \tilde{v}, x, y, j, r, s)$ denote the following system of equations

$$v = u^{p^r} \tag{7.7}$$

$$\tilde{v} = \tilde{u}^{p^j} \tag{7.8}$$

$$u = \frac{x^p + t}{x^p - t} \tag{7.9}$$

$$\tilde{u} = \frac{x^p + t^{-1}}{x^p - t^{-1}} \tag{7.10}$$

$$v = \frac{y^p + t^{p^s}}{y^p - t^{p^s}} \tag{7.11}$$

$$\tilde{v} = \frac{y^p + t^{-p^s}}{y^p - t^{-p^s}} \tag{7.12}$$

- Let $j, r, s \in \mathbb{Z}_{\geq 0}$, $u, \tilde{u}, v, \tilde{v}, x, y \in K$, and let $E2(u, \tilde{u}, v, \tilde{v}, x, y, j, r, s)$ denote the following system of equations

$$v = u^{2^r} \tag{7.13}$$

$$\tilde{v} = \tilde{u}^{2^j} \tag{7.14}$$

$$u = \frac{x^2 + t^2 + t}{x^2 + t} \tag{7.15}$$

$$\tilde{u} = \frac{x^2 + t^{-2} + t^{-1}}{x^2 + t^{-1}} \tag{7.16}$$

$$v = \frac{y^2 + t^{2^{s+1}} + t^{2^s}}{y^2 + t^{2^s}} \tag{7.17}$$

$$\tilde{v} = \frac{y^2 + t^{-2^{s+1}} + t^{-2^s}}{y^2 + t^{-2^s}} \tag{7.18}$$

Remark 7.2. The assumption that we have l constants algebraic over a finite field and satisfying assumptions above might require extending our field of constants. This is where we might need Proposition 7.3 assuring us that replacing the original field by a finite extension does not alter the situation.

Most of the propositions in this Appendix can be found in [18], [4], [19], and [22]. We include them here for the convenience of the reader.

Proposition 7.3. *Let Q_i be either "$\forall$" or "$\exists$". Let M/K be a finite extension of fields with M not algebraically closed. Let $P(t_1,\dots,t_r,x_1,\dots,x_k) \in M[t_1,\dots,t_r,x_1,\dots,x_k]$. Let*

$$A_M = \{(t_1,\dots,t_r) \in M^r : Q_1x_1 \in M \dots Q_kx_k \in M : P(t_1,\dots,t_r,x_1,\dots,x_k) = 0\} \tag{7.19}$$

be a first-order definable set. Then there exists a polynomial

$$T(u_1,\dots,u_m,y_1,\dots,y_l) \in K[u_1,\dots,u_m,y_1,\dots,y_l],$$

and a first-order definable set

$$A_K = \{(u_1,\dots,u_m) \in K^m : Q_{k+1}y_1 \in K \dots Q_{k+l}y_l \in K : T(u_1,\dots,u_m,y_1,\dots,y_l)\} = 0 \tag{7.20}$$

such that for any $(t_1,\dots,t_r) \in M^r$ we have that $(t_1,\dots,t_r) \in A_M$ if and only if for some m-tuple $(u_1,\dots,u_m) \in K^m$ we have that $(u_1,\dots,u_m) \in A_K$. Thus, if M has a first-order model of $\mathbb{Z}$ in the language of rings augmented by finitely many parameters from M, then K has a first-order model of $\mathbb{Z}$ in the language of rings with finitely many parameters from K.

The proof of the proposition requires standard "rewriting" techniques utilizing a basis of M over K and the fact that over a field which is not algebraically closed we can replace a finite set of equations by a single equivalent equation.

Proposition 7.3 will play a role in case we need to extend the field of constants to ensure that we have "enough" conjugacy classes of constants algebraic over a finite field relative to the number of primes ramifying in $K/F(t)$ or $K'/F'(t)$, where F', as above, is the algebraic closure of F and $K' = F'K$ is the compositum of F' and K. In this connection we have the following lemma.

Lemma 7.4. *Let α be any generator of K over $F(t)$ with $K/F(t)$ separable. Let $h(T) = a_0 + a_1T + \cdots + T^n$ be the monic irreducible polynomial of α over $F(t)$. Let $D(\alpha) = \mathbf{N}_{K/F(t)}(h'(\alpha))$ where $h'(T)$ is the derivative of $h(T)$ with respect to T. Let $P(\alpha)$ be the pole divisor of $\prod_{i=0}^{n-1} a_i$. Since $F(t)$ is a rational function field, $D(\alpha)$ and $P(\alpha)$ are both polynomials in t. Let $n(\alpha)$ be the degree of the polynomial $D(\alpha)P(\alpha)$. Let $\hat{F}$ be any algebraic extension of F. Then the number of $\hat{F}(t)$ primes ramifying in the extension $\hat{F}K/\hat{F}(t)$ is less or equal to $n(\alpha)$.*

Proof. Since there is no constant field extension in the extension $K/F(t)$, we have that K and $\hat{F}(t)$ are linearly disjoint over $F(t)$. Thus, $\hat{F}K = \hat{F}(t)(\alpha)$ and $[\hat{F}K : \hat{F}(t)] = [K : F(t)] = n$. Therefore if $\mathfrak{q}$ is a prime of $\hat{F}(t)$ ramified in the extension $\hat{F}K/\hat{F}(t)$ we have two options: either $\mathfrak{q}$ divides the discriminant $D(\alpha)$ of the power basis of α, or α is not integral at $\mathfrak{q}$ and $\mathfrak{q}$ divides $P(\alpha)$. In either case $\mathfrak{q}$ divides $D(\alpha)P(\alpha)$. Since $P(\alpha)D(\alpha)$ is a polynomial, its degree is invariant under any constant field extension and therefore the number of primes dividing $P(\alpha)D(\alpha)$ in $\hat{F}(t)$ is bounded by the degree of this polynomial. □

The next lemma is a technical proposition necessary to define a derivation on a function field.

Proposition 7.5. *Let H be a function field over a perfect field of constants C of positive characteristic p. Let $y \in H$ be such that y is not a p-th power. Then in $H(y^{1/p})$ every element of H becomes a p-th power.*

Proof. Let $\beta \in H$, let $P(T) = A_0(y) + A_1(y)T + \cdots + A_{m-1}(y)T^{m-1} + T^m$ be the monic irreducible polynomial of β over $C(y)$, and observe that in $H(y^{1/p})$ all the coefficients of

$P(T)$ are p-th powers. Thus $\beta^{1/p}$ satisfies a polynomial of degree at most m over $C(y^{1/p})$. Now we have the following sequence of inequalities and equalities.

$$mp \geq [C(\beta^{1/p}, y^{1/p}) : C(y^{1/p})][C(y^{1/p}) : C(y)] = [C(\beta^{1/p}, y^{1/p}) : C(y)] = \tag{7.21}$$

$$[C(\beta^{1/p}, y^{1/p}) : C(\beta, y^{1/p})][C(\beta, y^{1/p}) : C(\beta, y)][C(\beta, y) : C(y)] \geq pm. \tag{7.22}$$

Since $[C(\beta, y^{1/p}) : C(\beta, y)][C(\beta, y) : C(y)] = pm$, we conclude that

$$[C(\beta^{1/p}, y^{1/p}) : C(\beta, y^{1/p})] = 1,$$

i.e. β becomes a p-th power in $H(y^{1/p})$. Since β was an arbitrary element of H, we now conclude that every element of H is a p-th power in $H(y^{1/p})$. □

As a corollary we have the following proposition.

Corollary 7.6. *Let H be a function field over a perfect field of constants C of positive characteristic p. If we let*

$$H_0 = \{w^p, w \in H\}$$

and let $t \in H$ be such that $H/C(t)$ is a separable extension, then $H = H_0(t)$ and $[H : H_0] = p$.

Proof. It is enough to see that t^p is not a p-th power in H_0. If it is, then $t \in H_0$, and $[H : C(t)]$ is not separable. □

The following sequence of propositions and definitions is taken from Section B.9 of [22].

Definition 7.7. Let t, H, H_0 be as in Corollary 7.6. Let $x \in H, x = \sum_{i=0}^{p-1} u_i t^i, u_i \in H_0$. Then define $dx/dt = \sum_{i=0}^{p-2} i u_i t^{i-1}$.

Proposition 7.6 assures us that we have defined dx/dt for all x.

We leave the proof of the next proposition to the reader.

Proposition 7.8. *The global derivation in Definition 7.7 satisfies the usual differentiation rules concerning the derivative of the sum and the product of functions as well as the Chain Rule.*

Below we show how to use the derivation to gain information about multiplicities of zeros and poles.

Proposition 7.9. *Let H be a function field of positive characteristic over a perfect field of constants C. Let $\mathfrak{p}$ be a prime of H and let $t \in H$ be such that $H/C(t)$ is separable and $\text{ord}_{\mathfrak{p}} t = 1$. Then for any $x \in H$, if $\text{ord}_{\mathfrak{p}} x \geq 0$, then $\text{ord}_{\mathfrak{p}} \frac{dx}{dt} \geq \text{ord}_{\mathfrak{p}} x - 1$.*

Proof. First of all we observe that by Proposition 7.6, the derivation with respect to t is well defined. Next write $x = \sum_{i=0}^{p-1} u_i t^i$, where $u_i \in H_0$ as in Definition 7.7. Observe that $\text{ord}_{\mathfrak{p}} u_i t^i \equiv i \mod p$ and therefore for $i \neq j$ we have that $\text{ord}_{\mathfrak{p}} u_i t^i \neq \text{ord}_{\mathfrak{p}} u_j t^j$. Thus,

$$0 \leq \text{ord}_{\mathfrak{p}} x = \min_{i=0,\ldots,p-1} \text{ord}_{\mathfrak{p}} u_i t^i$$

and $\text{ord}_{\mathfrak{p}} u_i \geq 0$. Now using the definition of derivation we consider two cases. In the first case $\text{ord}_{\mathfrak{p}} x \equiv 0 \mod p$ and therefore

$$\text{ord}_{\mathfrak{p}} x = \text{ord}_{\mathfrak{p}} u_0 \leq \min_{1 \leq j \leq p-1} \{\text{ord}_{\mathfrak{p}} t^j u_j\} - 1.$$

Thus

$$\begin{aligned}\mathrm{ord}_{\mathfrak{p}}\frac{dx}{dt} &= \min\{\mathrm{ord}_{\mathfrak{p}}u_1, \mathrm{ord}_{\mathfrak{p}}2u_2t, \ldots, \mathrm{ord}_{\mathfrak{p}}(p-1)u_{p-1}t^{p-2}\} \\ &= \min_{1\le j\le p-1}\{\mathrm{ord}_{\mathfrak{p}}t^ju_j\} - 1 \ge \mathrm{ord}_{\mathfrak{p}}x.\end{aligned}$$

In the second case we have that $\mathrm{ord}_{\mathfrak{p}}x \not\equiv 0 \mod p$. Then

$$\min_{i=0,\ldots,p-1}\mathrm{ord}_{\mathfrak{p}}(u_it^i) = \mathrm{ord}_{\mathfrak{p}}(u_jt^j),$$

where $1 \le j \le p-1$. But in this case,

$$\mathrm{ord}_{\mathfrak{p}}ju_jt^{j-1} = \min\{\mathrm{ord}_{\mathfrak{p}}u_1, \mathrm{ord}_{\mathfrak{p}}2u_2t, \ldots, \mathrm{ord}_{\mathfrak{p}}(p-1)u_{p-1}t^{p-2}\},$$

so that $\mathrm{ord}_{\mathfrak{p}}\frac{dx}{dt} = \mathrm{ord}_{\mathfrak{p}}x - 1$. □

We can strengthen the result of the lemma in the following fashion.

Corollary 7.10. *Let $\mathfrak{q}$ be a prime of a function field H over a perfect constant field of characteristic $p > 0$, let $w \in H$ be such that $ord_{\mathfrak{q}}w = 1$. Let $t \in H$ be as before such that $H/C(t)$ is separable. Assume further $ord_{\mathfrak{q}}\frac{dw}{dt} \ge 0$. Then for any $x \in H$ integral at $\mathfrak{q}$, we have that $ord_{\mathfrak{q}}\frac{dx}{dt} \ge ord_{\mathfrak{q}}x - 1$.*

Proof. Since w has order 1 at a prime, it is not a p-th power and therefore derivation with respect to w is defined. Now we use the Chain Rule:

$$\mathrm{ord}_{\mathfrak{q}}\frac{dx}{dt} = \mathrm{ord}_{\mathfrak{q}}\frac{dx}{dw} + \mathrm{ord}_{\mathfrak{q}}\frac{dw}{dt} \ge \mathrm{ord}_{\mathfrak{q}}\frac{dx}{dw} \ge \mathrm{ord}_{\mathfrak{q}}x - 1,$$

where the last inequality holds by Proposition 7.9. □

Corollary 7.11. *Let H be a function field over a perfect field of constants C of positive characteristic p. Let $t \in H$ be such that t is not a p-th power in H. Let $\mathfrak{p}$ be a prime of H such that it is not ramified in the extension $H/C(t)$ and is not a pole of t. Then for any $x \in H$, if $ord_{\mathfrak{p}}x > 1$, then $ord_{\mathfrak{p}}\frac{dx}{dt} > 0$.*

Proof. Let $P(t)$ be a monic irreducible polynomial corresponding to the prime of $C(t)$ lying below $\mathfrak{p}$. (We know such a polynomial exists because $\mathfrak{p}$ is not a pole of t.) Now, since $\mathfrak{p}$ is not ramified over $C(t)$ we must have $\mathrm{ord}_{\mathfrak{p}}P(t) = 1$. Further, $\frac{dP(t)}{dt}$ is a polynomial and therefore $\mathrm{ord}_{\mathfrak{p}}\frac{dP(t)}{dt} \ge 0$. Thus, by Corollary 7.10, for any $x \in H$ integral at $\mathfrak{p}$ we have that $\mathrm{ord}_{\mathfrak{p}}\frac{dx}{dt} \ge \mathrm{ord}_{\mathfrak{p}}x - 1$. Hence the conclusion of the corollary follows. □

Proposition 7.12 ([22], Lemma 8.3.3, Corollary 8.3.4, and Proposition 8.3.8)**.** *Let K, F, p, t be as in Notation 7.1. Assume also that F is perfect and for some element $w \in F(t)$, having no poles or zeros at the primes ramifying in the extension $K/F(t)$, there exist $u, v \in K$ such that the following system is satisfied.*

$$\text{(7.23)} \qquad \begin{cases} \frac{1}{w} - \frac{1}{t} - = u^{p^a} - u \\ w - t = v^{p^a} - v \end{cases}$$

Then for some $s \in \mathbb{Z}_{\ge 0}$ we have that $w = t^{p^{as}}$. Conversely, if $w = t^{p^{as}}, s \ge 0$, then there exist $u, v \in F(t)$ satisfying (7.23). (For the last assertion we do not need the requirement that F is perfect.)

Proof. First of all note that all the poles of $v^{p^a} - v$ and $u^{p^a} - u$ in K are of orders divisible by p^a. Since zeros and poles of t are of orders equal to ± 1 (see Notation 7.1), we must conclude from (7.23) that the divisor of w in K is of the form $\mathfrak{U}^{p^a}\mathfrak{P}^{b_1}\mathfrak{Q}^{b_2}$. Indeed, let $\mathfrak{t}$ be a prime which is not a factor of $\mathfrak{P}$ or $\mathfrak{Q}$. Without loss of generality assume $\mathfrak{t}$ is a pole of w. Then, since $\mathrm{ord}_{\mathfrak{t}} t = 0$,

$$0 > \mathrm{ord}_{\mathfrak{t}} w = \mathrm{ord}_{\mathfrak{t}}(w - t) = \mathrm{ord}_{\mathfrak{t}}(v^{p^a} - v) \equiv 0 \text{ modulo } p^a.$$

Now let $\mathfrak{q}$ be a factor of $\mathfrak{Q}$ and consider the order at $\mathfrak{q}$. We have

$$\mathrm{ord}_{\mathfrak{q}}(w - t) = \mathrm{ord}_{\mathfrak{q}}(v^{p^a} - v).$$

Therefore, either $\mathrm{ord}_{\mathfrak{q}} w < -1$ and $\mathrm{ord}_{\mathfrak{q}} w \equiv 0 \mod p^a$, or $\mathrm{ord}_{\mathfrak{q}} w = \mathrm{ord}_{\mathfrak{q}} t = -1$. Since $w \in F(t)$ and no factor of $\mathfrak{Q}$ is ramified in the extension $K/F(t)$, the order of w at all the factors of $\mathfrak{Q}$ is the same. Thus, either $b_2 = -1$ or $b_2 \equiv 0 \mod p^a$. Similarly, for any prime factor $\mathfrak{p}$ of $\mathfrak{P}$ either $\mathrm{ord}_{\mathfrak{p}} w > 1$ and $\mathrm{ord}_{\mathfrak{p}} w \equiv 0 \mod p^a$, or $\mathrm{ord}_{\mathfrak{p}} w = \mathrm{ord}_{\mathfrak{p}} t = 1$. Thus, $b_1 = 1$ or $b_1 \equiv 0 \mod p^a$. Given these data, let examine the divisor of w in $F(t)$, where the divisor of t is of the form $\mathfrak{p}_0/\mathfrak{q}_0$, with $\mathfrak{p}_0, \mathfrak{q}_0$ being primes of $F(t)$. Since, by assumption w does not have any poles or zeros at primes ramifying in the extension $K/F(t)$, for any $F(t)$-prime $\mathfrak{t} \notin \{\mathfrak{p}_0, \mathfrak{q}_0\}$ we must have $\mathrm{ord}_{\mathfrak{t}} w \equiv 0 \mod p^a$. Thus in $F(t)$ the divisor of w is of the form $\mathfrak{D}^{p^a}\mathfrak{p}_0^{b_1}\mathfrak{q}_0^{b_2}$. Since the degree of this divisor must be 0, we deduce that either $|b_1| = |b_2| = 1$ or $b_1 \equiv b_2 \equiv 0 \mod p^a$. We will consider the two cases separately.

If we first assume that $|b_1| = |b_2| = 1$, then we can deduce that wt^{-1} is a p^a-th power in $F(t)$. This follows from the fact that in $F(t)$ every zero degree divisor is principal and the constant field is perfect. Thus, the second equation of (7.23) can be rewritten as

$$t(f-1)^{p^a} = v^{p^a} - v, \tag{7.24}$$

where $f \in F(t)$. Since $f - 1$ is a rational function in t, we can further rewrite (7.24) as

$$t(f_1^{p^a}/f_2^{p^a}) = v^{p^a} - v, \tag{7.25}$$

where f_1, f_2 are relatively prime polynomials in t over F and f_2 is monic. From this equation it is clear that any valuation that is a pole of v, is either a pole of t or a zero of f_2. Further, the absolute value of the order of any pole of v at any valuation which is a zero of f_2, must be the same as the order of f_2 at this valuation. Therefore, $s = f_2 v$ will have poles only at the valuations which are poles of t. We can rewrite (7.25) in the form

$$-tf_1^{p^a} + s^{p^a} = sf_2^{p^a - 1}.$$

Let $\mathfrak{c}$ be a zero of f_2. Then, since f_2 is a polynomial in t, we have that $\mathfrak{c}$ is not a pole of t. Since $p^a - 1 \geq 2$ and s is integral over $F[t]$, we have that $\mathrm{ord}_{\mathfrak{c}}(s^{p^a} - tf_1^{p^a}) \geq 2$.

Now observe that by Proposition 7.8

$$d(-tf_1^{p^a} + s^{p^a})/dt = -f_1^{p^a},$$

and since, by assumption, f_2 does not have any zeros at valuations ramifying in the extension $K/F(t)$, by Corollary 7.11,

$$\mathrm{ord}_{\mathfrak{c}}(-f_1^{p^a}) = \mathrm{ord}_{\mathfrak{c}}(d(-tf_1^{p^a} + s^{p^a})/dt) > 0.$$

Thus, f_1 has a zero at $\mathfrak{c}$. But f_1 and f_2 are supposed to be relatively prime polynomials. Hence, f_2 does not have any zeros, and thus is equal to 1. Therefore, w is a polynomial in t. Similarly, we can show that $1/w$ is a polynomial in $1/t$. Hence, w is a power of t, and

more specifically, unless $w = t$, we have that w must be a power of t divisible by p^a. So either we are done (if $w = t$) or $w = \tilde{w}^{p^a}$ for some $\tilde{w} \in F(t)$.

Next consider the case of $b_1 \equiv b_2 \equiv 0 \mod p^a$. In this case, since w does not have zeroes or poles ramifying in the extension $K/F(t)$, the divisor of w in $F(t)$ is a p^a-th power of another divisor, and as above this implies that $w = \tilde{w}^{p^a}$ for some $\tilde{w} \in F(t)$. So in any case, if $w \neq t$, we have that $w = \tilde{w}^{p^a}$ for some $\tilde{w} \in F(t)$. Assuming $w \neq t$ we do the following. Set $\tilde{v} = v - \tilde{w}, \tilde{u} = u - \tilde{w}^{-1}$ and observe that the following equations hold.

$$\tilde{w} - t = (v - \tilde{w})^{p^a} - (v - \tilde{w}) = \tilde{v}^{p^a} - \tilde{v}$$

$$\tilde{w}^{-1} - t^{-1} = (u - \tilde{w}^{-1})^{p^a} - (u - \tilde{w}^{-1}) = \tilde{u}^{p^a} - \tilde{u}$$

Since we can repeat this process only finitely many times, we conclude that $w = t^{p^{as}}$ for some $s \in \mathbb{Z}_{\geq 0}$.

It remains to show that if $w = t^{p^{as}}$ for some $s \in \mathbb{Z}_{\geq 0}$, we can satisfy (7.23). This can be deduced from the following equality:

$$x^{p^{as}} - x = (x^{p^{a(s-1)}} + x^{p^{a(s-2)}} + \cdots + x)^{p^a} - (x^{p^{a(s-1)}} + x^{p^{a(s-2)}} + \cdots + x) \tag{7.26}$$

□

Lemma 7.13 ([18], Lemma 4.5 or [22], Lemma 8.4.2)**.** *Let $p > 2$. Let $x \in F'K$. Let $u = \dfrac{x^p + t}{x^p - t}$. Let $b \in F', b \neq \pm 1$. Then all zeros and poles of $u^{\pm 1} + b$ are simple except possibly for zeros or poles of t or at primes ramifying in the extension $F'K/F'(t)$. (Here p, t, F', K are as in Notation 7.1.)*

Proof. It is enough to show that the proposition holds for u. The argument for u^{-1} follows by symmetry. First of all we note that the global derivation with respect to t is defined over $F'K$, and the derivative follows the usual rules by Definition 7.7 and Proposition 7.9. So consider

$$\frac{d(u+b)}{dt} = \frac{2x^p}{(x^p - t)^2}.$$

If $\mathfrak{t}$ is a prime of $F'K$ such that $\mathfrak{t}$ does not ramify in the extension $F'K/F'(t)$ and is not a pole or zero of t, then by Corollary 7.11 we have that

$$\mathrm{ord}_{\mathfrak{t}}(u+b) = \mathrm{ord}_{\mathfrak{t}} \frac{(1+b)x^p + (1-b)t}{x^p - t} > 1$$

if and only if $\mathfrak{t}$ is a common zero of $u + b$ and $\dfrac{d(u+b)}{dt}$. If $\mathrm{ord}_{\mathfrak{t}} \dfrac{2x^p}{(x^p - t)^2} > 0$, then $\mathfrak{t}$ is either a zero of x or a pole of $x^p - t$. Any zero of x, which is not a zero of t, is not a zero of $u + b$ for $b \neq 1$. Further, any pole of x is also not a zero of $u + b$. Thus all zeros of $u + b$ at primes not ramifying in the extension $F'K/F'(t)$ and different from poles and zeros of t are simple. Next we note that poles of $u + b$ are zeros of u^{-1}. Further

$$\frac{du^{-1}}{dt} = \frac{-2x^p}{(x^p + t)^2},$$

and by a similar argument u^{-1} and $\frac{du^{-1}}{dt}$ do not have any common zeros at any primes not ramifying in the extension $F'K/F'(t)$ and not being poles or zeros of t. □

The following lemma deals with the case of $p = 2$.

Lemma 7.14 ([4], Lemma 3.8)**.** *Let $p = 2$ and let F, F', K, t be as above. Let $x \in F'K$. Let $u = \dfrac{x^2 + t^2 + t}{x^2 + t}$. Let $b \in F'K, b \neq 1$. Then all zeros and poles of $u + b$ are simple except possibly for zeros or poles of t or at primes ramifying in the extension $K'/F'(t)$.*

Lemma 7.15 ([22], Lemma 8.2.10)**.** *For any $u, w \in K$, we have that $|C_w|$ and $|C_w \cap C_u|$ contain more than $n + 2$ elements. (Here n, K, C_w, C_u are as in Notation 7.1.)*

Proof. Consider the following table.

$$\begin{bmatrix} w - c_1 & w - c_1^p & \dots & w - c_1^{p^j} & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ w - c_l & w - c_l^p & \dots & w - c_l^{p^j} & \dots \end{bmatrix}$$

Observe that by assumption on the elements of $C(K)$ no two rows share an element, and the difference between any two elements of the table is constant. Thus, elements of at least $l - e(K, t)$ rows have no zero at any element of $\mathscr{E}(K, t)$ and consequently,

$$|C_w| \geq l - e(K, t) > n + 2 + e(K, t).$$

Next consider a table

$$\begin{bmatrix} u - b_1 & u - b_1^p & \dots & u - b_1^{p^j} & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ u - b_{|C_w|} & u - b_{|C_w|}^p & \dots & u - b_{|C_w|}^{p^j} & \dots \end{bmatrix}$$

where $b_i \in C_w$. By an analogous argument, at least $|C_w| - e(K, t)$ rows of this table contain no element with a zero at any valuation of $\mathscr{E}(K, t)$. Thus, at least $l - 2e(K, t) > n + 2$ elements are contained in $C_w \cap C_u$.

□

Lemma 7.16 ([22], Lemma 8.2.4)**.** *Let M/G be a finite separable extension of fields of positive characteristic p. Let $\alpha \in M$ be such that for some positive integer a, all the coefficients of its monic irreducible polynomial over G are p^a-th powers in G. Then α is a p^a-th power in M.*

Proof. Let $a_0^{p^a} + \cdots + a_{m-1}^{p^a} T^{m-1} + T^m$ be the monic irreducible polynomial of α over G. Let β be the element of the algebraic closure of M such that $\beta^{p^a} = \alpha$. Then β is of degree at most m over G. On the other hand, $G(\alpha) \subseteq G(\beta)$. Therefore, $G(\alpha) = G(\beta)$. □

Lemma 7.17 ([22], Lemma 8.2.5)**.** *Let M/G be a finite separable extension of fields of positive characteristic p. Let $[M : G] = n$. Let r be a positive integer. Let $x \in M$ be such that $M = G(x)$ and for distinct $b_0, \dots, b_n \in G$ we have that $\mathbf{N}_{M/G}(b_i^{p^r} - x) = y_i^{p^r}$. Then x is a p^r-th power in M.*

Proof. Let $U(T) = A_0 + A_1 T + \cdots + A_{n-1} T^{n-1} + T^n$ be the monic irreducible polynomial of x over G. Then for $i = 0, \dots, n$ we have that $U(b_i^{p^r}) = y_i^{p^r}$. Further, we have the following linear system of equations:

$$\begin{pmatrix} 1 & b_0^{p^r} & \dots & b_0^{p^r(n-1)} & b_0^{p^r n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & b_n^{p^r} & \dots & b_n^{p^r(n-1)} & b_n^{p^r n} \end{pmatrix} \begin{pmatrix} A_0 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} y_0^{p^r} \\ \vdots \\ y_n^{p^r} \end{pmatrix}$$

Using Cramer's rule to solve the system, it is not hard to conclude that for $i = 0, \ldots, n$ it is the case that A_i is a p^r-th power in G. Then, by Lemma 7.16, x is a p^r-th power in M. $\square$

Lemma 7.18 ([22], Lemma 8.4.1)**.** *Let M be a function field over a perfect field of constants L and let $t \in M$ be such that $M/L(t)$ is a finite and separable extension. Let m be a positive integer. Let $v \in M$ and assume that for some distinct $b_0 = 0, b_1, \ldots, b_n \in L$, the divisor of $v+b_0, \ldots, v+b_n$ is a p^m-th power of some other divisor of M. Then, assuming for all i we have that $v + b_i$ does not have any zeros or poles at any prime ramifying in the extension $M/L(t)$, it is the case that v is a p^m-th power in M.*

Proof. First assume $v \in L(t)$. Since $v + b_i$ does not have any zeros or poles at primes ramifying in the extension $M/L(t)$, the divisor of $v + b_i$ in $L(t)$ is a p^m-th power of another $L(t)$ divisor. Since in $L(t)$ every zero degree divisor is principal and the constant field is perfect, v is a p-th power in $L(t)$ and therefore in M. Next assume $v \notin L(t)$. Note that no zero or pole of $v + b_i$ is at any valuation ramifying in the extension $M/L(t, v)$. Hence, in $L(t, v)$ the divisor of $v + b_i$ is also a p^m-th power of another divisor. Finally note that $\mathbf{N}_{L(t,v)/L(t)}(v + b_i)$ will be a p^m-th power in $L(t)$ and apply Lemma 7.17.

$\square$

Lemma 7.19 (This lemma is slightly modified from [22], Lemma 8.2.11)**.** *Let $\sigma, \mu \in F'K = K'$. Assume that all the primes that are poles of σ or μ do not ramify in the extension $F'K/F'(t)$. Further, assume the following equality is true.*

$$t(\sigma^{p^a} - \sigma) = \mu^{p^a} - \mu \tag{7.27}$$

Then $\sigma^{p^a} - \sigma = \mu^{p^a} - \mu = 0$. (Here a, F', K, t are as in Notation 7.1, and we remind the reader that by assumption the primes occurring in the divisor of t do not ramify in $F'K/F'(t)$.)

Proof. Let $\mathfrak{A}, \mathfrak{B}$ be integral divisors of K', relatively prime to each other and to $\mathfrak{P} = \prod_i \mathfrak{p}_i$ and $\mathfrak{Q} = \prod_i \mathfrak{q}_i$ (in other words, no prime occurring in $\mathfrak{A}$ or $\mathfrak{B}$ occurs in the divisor of t), and such that the divisor of σ is of the form $\dfrac{\mathfrak{A}}{\mathfrak{B}} \prod_i \mathfrak{p}_i^{n_i} \prod_i \mathfrak{q}_i^{k_i}$, where n_i, k_i are non-zero integers for all i. It is not hard to see that for some integral divisor $\mathfrak{C}$, relatively prime to $\mathfrak{B}, \mathfrak{P}$, and $\mathfrak{Q}$, some non-zero integers a_i, b_i, the divisor of μ is of the form $\dfrac{\mathfrak{C}}{\mathfrak{B}} \prod_i \mathfrak{p}_i^{a_i} \prod_i \mathfrak{q}_i^{b_i}$.

Indeed, if $\mathfrak{t}$ is a pole of μ such that $\mathfrak{t}$ does not divide $\mathfrak{P}$ or $\mathfrak{Q}$, then

$$0 > p^a \mathrm{ord}_{\mathfrak{t}}\mu = \mathrm{ord}_{\mathfrak{t}}(\mu^{p^a} - \mu) = \mathrm{ord}_{\mathfrak{t}}(t(\sigma^{p^a} - \sigma)) = \mathrm{ord}_{\mathfrak{t}}(\sigma^{p^a} - \sigma) = p^a \mathrm{ord}_{\mathfrak{t}}\sigma.$$

Conversely, if $\mathfrak{t}$ is a pole of σ such that $\mathfrak{t}$ does not divide $\mathfrak{P}$ or $\mathfrak{Q}$, then

$$0 > p^a \mathrm{ord}_{\mathfrak{t}}\sigma = \mathrm{ord}_{\mathfrak{t}}(\sigma^{p^a} - \sigma) = \mathrm{ord}_{\mathfrak{t}}(t(\sigma^{p^a} - \sigma)) = \mathrm{ord}_{\mathfrak{t}}(\mu^{p^a} - \mu) = p^a \mathrm{ord}_{\mathfrak{t}}\mu.$$

Further we can also deduce that for each $\mathfrak{p}_i$ we have that $\mathrm{ord}_{\mathfrak{p}_i}\sigma \geq 0$ and $\mathrm{ord}_{\mathfrak{p}_i}\mu \geq 0$. To see that this is the case suppose $\mathrm{ord}_{\mathfrak{p}_i}\sigma < 0$ and conclude that

$$\mathrm{ord}_{\mathfrak{p}_i} t(\sigma^{p^a} - \sigma) < 0, \text{ and} \tag{7.28}$$

$$\mathrm{ord}_{\mathfrak{p}_i} t(\sigma^{p^a} - \sigma) \not\equiv 0 \mod p. \tag{7.29}$$

At the same time (7.28) implies that

$$\mathrm{ord}_{\mathfrak{p}_i}(\mu^{p^a} - \mu) < 0, \text{ and} \tag{7.30}$$

$$\mathrm{ord}_{\mathfrak{p}_i}(\mu^{p^a} - \mu) \equiv 0 \mod p. \tag{7.31}$$

Therefore assuming $\mathrm{ord}_{\mathfrak{p}_i}\sigma < 0$ leads to a contradiction. Similarly, if $\mathrm{ord}_{\mathfrak{p}_i}\mu < 0$ then (7.30) and (7.28) hold and we again obtain a contradiction. Assuming that $\mathrm{ord}_{\mathfrak{q}_i}\sigma < 0$, $\mathrm{ord}_{\mathfrak{q}_i}\mu < 0$ results in a contradiction of a similar type. Thus, we can assume that $a_i, b_i, n_i, k_i \geq 0$ for all i.

By the Strong Approximation Theorem there exists $b \in K^\times$ such that the divisor of b is of the form $\mathfrak{B}\mathfrak{D}/\mathfrak{q}_1^c$, where $\mathfrak{D}$ is an integral divisor relatively prime to $\mathfrak{A}, \mathfrak{C}, \mathfrak{P}, \mathfrak{Q}$, and c is a positive integer. Then $b\sigma = s_1, b\mu = s_2$, where s_1, s_2 are integral over $F'[t]$ and have zero divisors relatively prime to $\mathfrak{B}$. Indeed, consider the divisors of $s_1 = b\sigma$:

$$\frac{\mathfrak{B}\mathfrak{D}}{\mathfrak{q}_1^c}\frac{\mathfrak{A}}{\mathfrak{B}}\prod_i \mathfrak{p}_i^{n_i}\prod_j \mathfrak{q}_j^{k_j} = \mathfrak{D}\mathfrak{A}\prod_i \mathfrak{p}_i^{n_i}\mathfrak{q}_1^{k_1-c}\prod_{j>1}\mathfrak{q}_j^{k_j}$$

The pole of s_1 is a factor of $\mathfrak{Q}$ and therefore s_1 is integral over $F'[t]$. Further, by construction $\mathfrak{A}$ and $\mathfrak{D}$ are integral divisors relatively prime to $\mathfrak{P}$ and $\mathfrak{B}$. A similar argument applies to s_2.

Multiplying through by b^{p^a} we will obtain the following equation.

$$t(s_1^{p^a} - b^{p^a-1}s_1) = s_2^{p^a} - b^{p^a-1}s_2. \tag{7.32}$$

We can now rewrite (7.32) in the form

$$(s_1^{p^a}t - s_2^{p^a}) = b^{p^a-1}(s_1t - s_2). \tag{7.33}$$

Let $\mathfrak{t}$ be any prime factor of $\mathfrak{B}$ in $F'K$. Then $\mathfrak{t}$ does not ramify in the extension $F'K/F'(t)$ and since $p^a > 2$, we know that $\mathrm{ord}_{\mathfrak{t}}(s_1^{p^a}t - s_2^{p^a}) \geq 2$. Further, since t is not a p-th power in $F'K$, the global derivation with respect to t is defined by Proposition 7.8, and by Corollary 7.11 we also have

$$\mathrm{ord}_{\mathfrak{t}}\frac{d(s_1^{p^a}t - s_2^{p^a})}{dt} > 0.$$

Finally,

$$\mathrm{ord}_{\mathfrak{t}}\frac{d(s_1^{p^a}t - s_2^{p^a})}{dt} = \mathrm{ord}_{\mathfrak{t}}(s_1^{p^a}).$$

Therefore, s_1 has a zero at $\mathfrak{t}$. This, however, is impossible by construction of s_1 as described above. Consequently, $\mathfrak{B}$ is a trivial divisor and μ and σ are constants since their pole divisor is trivial. Now (7.27) is implying that t times a constant is equal to a constant. This can happen only if both constants are zero. □

Lemma 7.20 ([22], Lemma 8.4.4)**.** *Let $s \in \mathbb{Z}_{>0}$. Let $x, v \in K \setminus \{0\}$ and assume that for some $\tilde{v} \in K$ we have that $\tilde{v}^{p^a} = v$. Let $u = \dfrac{x^p + t}{x^p - t}$ if $p > 2$ and let $u = \dfrac{x^2 + t^2 + t}{x^2 + t}$, if $p = 2$. Further, assume that*

$$\begin{gathered}\exists \mu_{i,j_i,k,j_k,e,m}, \sigma_{i,j_i,k,j_k}, \lambda_1, \lambda_{-1} \in K \\ \forall i \exists j_i \forall (k \neq i) \exists j_k \forall m \forall e : \\ D(s, i, j_i, k, j_k, m, e, u, v, \mu_{i,j_i,k,j_k,e,m}, \sigma_{i,j_i,k,j_k}, \lambda_1, \lambda_{-1})\end{gathered} \tag{7.34}$$

holds. Then

$$\begin{gathered}\exists \tilde{\mu}_{i,j_i,k,j_k,e,m}, \tilde{\sigma}_{i,j_i,k,j_k}, \tilde{\lambda}_1, \tilde{\lambda}_{-1} \in K \\ \forall i \exists j_i \forall (k \neq i) \exists j_k \forall m \forall e : \\ D(s-1, i, j_i, k, j_k, m, e, u, \tilde{v}, \tilde{\mu}_{i,j_i,k,j_k,e,m}, \tilde{\sigma}_{i,j_i,k,j_k}, \tilde{\nu}_{i,j_i,e}, \tilde{\lambda}_1, \tilde{\lambda}_{-1})\end{gathered} \tag{7.35}$$

holds.

Lemma 7.21 ([22], Lemma 8.4.5 and Corollary 8.4.6)**.** *Let $s \in \mathbb{Z}_{\geq 0}, x, v \in K \setminus \{0\}$. Let $u = \dfrac{x^p + t}{x^p - t}$, if $p > 2$, and let $u = \dfrac{x^2 + t^2 + t}{x^2 + t}$, if $p = 2$. Further, assume that (7.34) holds. Then $v = u^{p^{as}}$. Conversely, if $v = u^{p^{as}}$, then (7.34) holds.*

Proof. First of all, we claim that for all i, k, it is the case that $u_{i,k}$ has no multiple zeros or poles except possibly at the primes with factors ramifying in $F'K/F'(t)$, or poles or zeros of t. Indeed, all the poles of $u_{i,k}$ are zeros of $u + c_k$ and all the zeros of $u_{i,k}$ are zeros $u + c_i$. However, by Lemma 7.13 and by assumption on c_i and c_k, all the zeros of $u + c_k$ and $u + c_i$ are simple, except possibly for zeros at the primes which are zeros or poles of t or have factors ramifying in the extension $F'K/F'(t)$.

We will show that if $s > 0$ then v is a p^a-th power in K, and if $s = 0$ then $u = v$. This assertion together with Lemma 7.20 will produce the desired conclusion.

Note that by Corollary 7.15, we can choose distinct natural numbers $i, k_1, \ldots, k_{n+1} \in \{0, \ldots, l\}$ such that $\{c_i, c_{k_1}, \ldots, c_{k_{n+1}}\} \subset C_v \cap C_u$ and for all $1 \leq j_i \leq r_i, 1 \leq j_{k_f} \leq r_{k_f}$, with $f = 1, \ldots, n+1$, we have that u_{i,k_f} and $v_{i,j_i,k_f,j_{k_f}}$ have no zeros or poles at the primes of K with factors ramifying in the extension $F'K/F'(t)$, or primes occurring in the K-divisor of t. Note also that for thus selected indices, all the poles and zeros of u_{i,k_f} are simple. We now proceed to pick natural numbers $i, k_1, \ldots, k_{n+1}, j_i, j_{k_1}, \ldots, j_{k_{n+1}}$ such that the equations in (7.1) - (7.4) are satisfied for these values of indices, and u_{i,k_1}, $v_{i,j_i,k_1,j_{k_1}}, \ldots$, $u_{i,k_{n+1}}$, $v_{i,j_i,k_{n+1},j_{k_{n+1}}}$ have no poles or zeros at primes with factors ramifying in the extension $F'K/F'(t)$, or at primes occurring in the K-divisor of t.

Now assume $s > 0$, and let f range over the set $\{1, \ldots, n+1\}$. First let $e = \pm 1$, while $m = 0$, and consider the two versions of the equation in (7.3) with these values of e and m.

$$v^2_{i,j_i,k_f,j_{k_f}} - u^2_{i,k_f} = \mu^{p^a}_{i,j_i,k_f,j_{k_f},1,0} - \mu_{i,j_i,k_f,j_{k_f},1,0}, \tag{7.36}$$

$$v^{-2}_{i,j_i,k_f,j_{k_f}} - u^{-2}_{i,k_f} = \mu^{p^a}_{i,j_i,k_f,j_{k_f},-1,0} - \mu_{i,j_i,k_f,j_{k_f},-1,0}, \tag{7.37}$$

Here either for all $f = 1, \ldots, n+1$, the divisor of $v_{i,j_i,k_f,j_{k_f}}$ in K is a p^a-th power of another divisor, or for some f and some prime $\mathfrak{t}$ without factors ramifying in the extension $F'K/F'(t)$ and not occurring in the K-divisor of t we have that $\mathrm{ord}_{\mathfrak{t}} v_{i,j_i,k_f,j_{k_f}} = \pm 1$.

In the first case, given the assumption that $v_{i,j_i,k_f,j_{k_f}}$'s do not have poles or zeros at ramifying primes and Lemma 7.18, we have that v is a p^a-th power in K.

So suppose the second alternative holds. In this case, without loss of generality, assume $\mathfrak{t}$ is a pole of $v_{i,j_i,k_f,j_{k_f}}$ for some f. Next consider the following equations

$$v^2_{i,j_i,k_f,j_{k_f}} t^{p^{as}} - u^2_{i,k_f} t = \mu^{p^a}_{i,j_i,k_f,j_{k_f},1,1} - \mu_{i,j_i,k_f,j_{k_f},1,1}, \tag{7.38}$$

$$v^2_{i,j_i,k_f,j_{k_f}} - u^2_{i,k_f} = \mu^{p^a}_{i,j_i,k_f,j_{k_f},0,1} - \mu_{i,j_i,k_f,j_{k_f},0,1}, \tag{7.39}$$

obtained from (7.3) by first making $e = 1, m = 1$ and then $e = 1, m = 0$. (If $\mathfrak{t}$ were a zero of $v_{i,j_i,k_f,j_{k_f}}$, then we would set e equal to -1 in both equations.) Since t does not have a pole or zero at $\mathfrak{t}$ and $p^a > 2$, we must conclude that

$$\mathrm{ord}_{\mathfrak{t}}(v^2_{i,j_i,k_f,j_{k_f}} t^{p^{as}} - u^2_{i,k_f} t) = \mathrm{ord}_{\mathfrak{t}}(\mu^{p^a}_{i,j_i,k_f,j_{k_f},1,1} - \mu_{i,j_i,k_f,j_{k_f},1,1}) \geq 0$$

and

$$\text{ord }_{\mathfrak{t}}(v^2_{i,j_i,k_f,j_{k_f}} - u^2_{i,k_f}) = \text{ord}_{\mathfrak{t}}(\mu^{p^a}_{i,j_i,k_f,j_{k_f},0,1} - \mu_{i,j_i,k_f,j_{k_f},0,1}) \geq 0$$

Thus,

$$\text{ord}_{\mathfrak{t}} v^2_{i,j_i,k_f,j_{k_f}}(t^{p^{as}} - t)$$

$$= \text{ord}_{\mathfrak{t}}(\mu^{p^a}_{i,j_i,k_f,j_{k_f},1,1} - \mu_{i,j_i,k_f,j_{k_f},1,1} - t\mu^{p^a}_{i,j_i,k_f,j_{k_f},0,1} + t\mu_{i,j_i,k_f,j_{k_f},0,1}) \geq 0.$$

Finally, we must deduce that $\text{ord}_{\mathfrak{t}}(t^{p^{as}} - t) \geq 2|\text{ord}_{\mathfrak{t}} v|$. But in $F(t)$ all the zeros of $(t^{p^{as}} - t)$ are simple. Thus, this function can have multiple zeros only at primes ramifying in the extension $K/F(t)$. By assumption $\mathfrak{t}$ is not one of these primes and thus we have a contradiction, unless v is a p^a-th power.

Suppose now that $s = 0$. Set $e = 1$ again and let $i, k_1, \ldots, k_{n+1}$ be selected as above. Then from (7.38) and (7.39) we obtain for $k_f \in \{k_1, \ldots, k_{n+1}\}$,

$$\mu^{p^a}_{i,j_i,k_f,j_{k_f},1,1} - \mu_{i,j_i,k_f,j_{k_f},1,1} = t(\mu^{p^a}_{i,j_i,k_f,j_{k_f},0,1} - \mu_{i,j_i,k_f,j_{k_f},0,1}).$$

Note here that all the poles of $\mu_{i,j_i,k_f,j_{k_f},1,1}$ and $\mu_{i,j_i,k_f,j_{k_f},0,1}$ are poles of u_{i,k_f}, $v_{i,j_i,k_f,j_{k_f}}$ or t, and thus are not at any valuation ramifying in the extension $K/F(t)$. From Lemma 7.19 and equation (7.39) we can then conclude that for all $k_f \in \{k_1, \ldots, k_{n+1}\}$

$$v^2_{i,j_i,k_f,j_{k_f}} - u^2_{i,k_f} = 0.$$

Thus, $v_{i,j_i,k_f,j_{k_f}} = \pm u_{i,k_f}$. Since all the poles of u_{i,k_f} are simple, (7.4) rules out "-". Therefore,

$$v_{i,j_i,k_f,j_{k_f}} = u_{i,k_f}. \tag{7.40}$$

Rewriting (7.40) we obtain

$$\frac{d_{i,j_i} - d_{k_f,j_{k_f}}}{v + d_{k_f,j_{k_f}}} = \frac{c_i - c_{k_f}}{u + c_{k_f}},$$

or

$$v = au + b, \tag{7.41}$$

where a, b are constants. However, unless $b = 0$, we have a contradiction with (7.6) because, unless $b = 0$, we have that v^{-1} and u^{-1} have different, and in the case of u, always simple poles. Finally, if $a \neq 1$, then we have a contradiction with (7.5) because the difference, unless it is 0 (and therefore $a = 1$), will have simple poles.

We now show that assuming $v = u^{p^{as}}$, all the equations can be satisfied. Observe that for any $x \in K$ and any $s \in \mathbb{Z}_{\geq 0}$

$$x^{p^{as}} - x = (x^{p^{a(s-1)}} + x^{p^{a(s-2)}} + \cdots + x)^{p^a} - (x^{p^{a(s-1)}} + x^{p^{a(s-2)}} + \cdots + x) \tag{7.42}$$

In view of equality (7.42), it is enough to show that for some $1 \leq j_i \leq r_i, 1 \leq j_k \leq r_k$, $v_{i,j_i,k,j_k} = (u_{i,k})^{p^{as}}$. Choose $j_i \equiv as$ modulo r_i. (Such a j_i exists since the set of all possible values of j_i contains a representative of every class modulo r_i.) Then for some integer ℓ we have that $c_i^{p^{as}} = (c_i^{p^{j_i}})^{p^{\ell r_i}} = c_i^{p^{j_i}}$. Similarly, choose $j_k \equiv as$ modulo r_k so that $c_k^{p^{as}} = c_k^{p^{j_k}}$. We can also use (7.42) to satisfy (7.5) and (7.6). □

We are now ready for the last sequence of propositions concluding the proof. We will have to separate the case of $p = 2$ again. We start with the case of $p > 2$.

Proposition 7.22 ([22], Proposition 8.4.8)**.** *Let $p > 2$. Let $x, y \in K$. Then there exist $v, \tilde{v}, u, \tilde{u}, v_1, \tilde{v}_1, u_1, \tilde{u}_1 \in K$, $s, i, j, r_1, j_1 \in \mathbb{Z}_{\geq 0}$ such that*

$$\begin{cases} E(u, \tilde{u}, v, \tilde{v}, x, y, j, i, s) \\ E(u_1, \tilde{u}_1, v_1, \tilde{v}_1, x+1, y+1, j_1, r_1, s) \end{cases} \tag{7.43}$$

hold if and only if $y = x^{p^s}$.

The following propositions treat the characteristic 2 case.

Lemma 7.23 ([22], Proposition 8.4.9)**.** *Let $p = 2$. Then for $x, y = \tilde{y}^2 \in K, j, r, s \in \mathbb{Z}_{\geq 0} \setminus \{0\}, u, \tilde{u} \in K$ there exist $v, \tilde{v} \in K$ such that*

$$E2(u, \tilde{u}, v, \tilde{v}, x, y, j, r, s) \tag{7.44}$$

holds if and only if there exist $v_1, \tilde{v}_1 \in K$ such that

$$E2(u_1, \tilde{u}_1, v_1, \tilde{v}_1, x, \tilde{y}, j-1, r-1, s-1) \tag{7.45}$$

holds.

Proposition 7.24 ([22], Proposition 8.4.10)**.** *Let $p = 2$. Then for $x, y \in K, s \in \mathbb{Z}_{\geq 0}$ there exist $j, r \in \mathbb{Z}_{\geq 0}$, $u, \tilde{u}, v, \tilde{v} \in K$ such that (7.44) holds if and only if $y = x^{2^s}$.*

ACKNOWLEDGMENTS

The authors would like to thank Arno Fehm and Stephen Simpson for helpful discussions leading to Corollary 5.1. The authors would also like to thank the Referee for numerous corrections and helpful comments.

REFERENCES

[1] Gregory L. Cherlin. Undecidability of rational function fields in nonzero characteristic. In *Logic colloquium '82 (Florence, 1982)*, volume 112 of *Stud. Logic Found. Math.*, pages 85–95. North-Holland, Amsterdam, 1984.

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

[3] Jean-Louis Duret. Sur la théorie élémentaire des corps de fonctions. *J. Symbolic Logic*, 51(4):948–956, 1986.

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

[5] Kirsten Eisenträger. Hilbert's tenth problem for function fields of varieties over $\mathbb{C}$. *Int. Math. Res. Not.*, (59):3191–3205, 2004.

[6] Kirsten Eisenträger. Hilbert's Tenth Problem for function fields of varieties over algebraically closed fields of positive characteristic, 2008. Preprint.

[7] Kirsten Eisenträger. Hilbert's Tenth Problem for function fields of varieties over number fields and p-adic fields. *Journal of Algebra*, 310:775–792, 2007.

[8] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge.* Springer-Verlag, Berlin, second edition, 2005.

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

[10] Jochen Koenigsmann. Defining transcendentals in function fields. *J. Symbolic Logic*, 67(3):947–956, 2002.

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

[12] Laurent Moret-Bailly. Elliptic curves and Hilbert's Tenth Problem for algebraic function fields over real and p-adic fields. *Journal für die Reine und Angewandte Mathematik*, 587:77–143, 2006.

[13] Thanases Pheidas. Hilbert's tenth problem for fields of rational functions over finite fields. *Inventiones Mathematicae*, 103:1–8, 1991.
[14] Thanases Pheidas. Endomorphisms of elliptic curves and undecidability in function fields of positive characteristic. *J. Algebra*, 273(1):395–411, 2004.
[15] Bjorn Poonen and Florian Pop. First-order characterization of function field invariants over large fields. *Model theory with applications to algebra and analysis*, Vol. 2, 255–271, London Math. Soc. Lecture Note Ser., 350, Cambridge Univ. Press, Cambridge, 2008.
[16] Julia Robinson. Definability and decision problems in arithmetic. *Journal of Symbolic Logic*, 14:98–114, 1949.
[17] Alexandra Shlapentokh. Diophantine undecidability for some function fields of infinite transcendence degree and positive characteristic. *Zapiski Seminarov POMI*, 304:141–167.
[18] Alexandra Shlapentokh. Diophantine undecidability of algebraic function fields over finite fields of constants. *Journal of Number Theory*, 58(2):317–342, June 1996.
[19] Alexandra Shlapentokh. Hilbert's tenth problem for algebraic function fields over infinite fields of constants of positive characteristic. *Pacific Journal of Mathematics*, 193(2):463–500, 2000.
[20] Alexandra Shlapentokh. Diophantine undecidability of function fields of characteristic greater than 2 finitely generated over a field algebraic over a finite field. *Compositio Mathematica*, 132(1):99–120, May 2002.
[21] Alexandra Shlapentokh. First-order definitions of rational functions and $\mathscr{S}$-integers over holomorphy rings of algebraic functions of characteristic 0. *Ann. Pure Appl. Logic*, 136(3):267–283, 2005.
[22] Alexandra Shlapentokh. *Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields*. Cambridge University Press, 2006.
[23] Joseph Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer-Verlag, New York, 1994.
[24] Alfred Tarski. Undecidable theories. Studies in Logic and the Foundations of Mathematics. North-Holland Publishing Company, Amsterdam, 1953. In collaboration with Andrzej Mostowski and Raphael M. Robinson.
[25] Carlos Videla. Hilbert's tenth problem for rational function fields in characteristic 2. *Proceedings of the American Mathematical Society*, 120(1):249–253, January 1994.

DEPARTMENT OF MATHEMATICS, THE PENNSYLVANIA STATE UNIVERSITY, UNIVERSITY PARK, PA 16802, USA.

DEPARTMENT OF MATHEMATICS, EAST CAROLINA UNIVERSITY, GREENVILLE, NC 27858, USA.