Pacific Journal of Mathematics

HILBERT'S TENTH PROBLEM FOR ALGEBRAIC FUNCTION FIELDS OF CHARACTERISTIC 2

Kirsten Eisenträger

Volume 210 No. 2 June 2003

PACIFIC JOURNAL OF MATHEMATICS
Vol. 210, No. 2, 2003

HILBERT'S TENTH PROBLEM FOR ALGEBRAIC FUNCTION FIELDS OF CHARACTERISTIC 2

Kirsten Eisenträger

Let K be an algebraic function field of characteristic 2 with constant field C_K. Let C be the algebraic closure of a finite field in K. Assume that C has an extension of degree 2. Assume that there are elements u, x of K with u transcendental over C_K and x algebraic over $C(u)$ and such that $K = C_K(u, x)$. Then Hilbert's Tenth Problem over K is undecidable. Together with Shlapentokh's result for odd characteristic this implies that Hilbert's Tenth Problem for any such field K of finite characteristic is undecidable. In particular, Hilbert's Tenth Problem for any algebraic function field with finite constant field is undecidable.

1. Introduction.

Hilbert's Tenth Problem in its original form can be stated in the following form: Is there a uniform algorithm that determines, given a polynomial equation with integer coefficients, whether the equation has an integer solution or not? In [**Mat70**] Matijasevich proved that the answer to this question is no, i.e., that Hilbert's Tenth Problem is undecidable. Since then various analogues of this problem have been studied by asking the same question as above for polynomial equations with coefficients and solutions over some other commutative ring R. Perhaps the most important unsolved question in this area is Hilbert's Tenth Problem over the field of rational numbers. There are also many results that prove undecidability: It was proved in [**Den80**] and [**DL78**] that Hilbert's Tenth Problem is undecidable for various rings of algebraic integers, and [**Den78**] proves the undecidability of the problem for rational functions over formally real fields. In [**KR92a**] Kim and Roush proved that Hilbert's Tenth Problem over $\mathbb{C}(t_1, t_2)$ is undecidable. Diophantine undecidability has also been proved for some rational function fields of characteristic p: Pheidas [**Phe91**] has shown that Hilbert's Tenth Problem is undecidable for rational function fields over finite fields of characteristic greater than 2 and Videla [**Vid94**] has proved the analogous result for characteristic 2. Kim and Roush [**KR92b**] proved undecidability for rational function fields of characteristic $p > 2$ whose constant fields do not contain the algebraic closure of a finite field. In [**Shl00**] Shlapentokh proved that the problem for algebraic function fields over possibly infinite constant fields of characteristic $p > 2$ is undecidable. This paper will solve the analogous problem over function fields of characteristic 2, so Hilbert's Tenth Problem for any such field of finite characteristic is undecidable. We will first describe the general approach that is used to prove the undecidability of Hilbert's Tenth Problem for any function field of positive characteristic. The approach is based on an idea that was first introduced by Denef in [**Den79**] and further developed by Pheidas in [**Phe91**] and Shlapentokh in [**Shl96**] and [**Shl00**].

Before we can describe the idea in detail we need to define what an algebraic function field is:

Definition 1.1. A field extension K/C_K is said to be an *algebraic function field* (*of one variable*) if these conditions hold:

1) The transcendence degree of K/C_K is 1;
2) K is finitely generated over C_K; and
3) C_K is algebraically closed in K.

In this case there exists $t \in K$, transcendental over C_K, such that the degree of the field extension $[K : C_K(t)]$ is finite. The field C_K is called the constant field of K.

We also need to define two notions that we will use below:

Definition 1.2.

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

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

When R is not a finitely generated algebra over $\mathbb{Z}$, we restrict our attention to diophantine equations whose coefficients are in a finitely generated algebra over $\mathbb{Z}$. In particular, if R is a ring of polynomials or a field of rational functions in an indeterminate t, we only consider diophantine equations whose coefficients lie in the natural image of $\mathbb{Z}[t]$ in R.

1.1. Idea of Proof. Let $\mathbb{N}$ be the set of natural numbers $\{0, 1, 2, \dots\}$. The general idea of the proof is to reduce a certain decision problem over the natural numbers which we know to be undecidable to Hilbert's Tenth Problem over K. The undecidable structure that we will use is the diophantine theory of the natural numbers with addition and a predicate $|_p$ defined by $n|_p m$ if and only if $\exists s \in \mathbb{N}(m = p^s n)$. In [**Phe87**] Pheidas showed that this structure has an undecidable diophantine theory, i.e., there is no uniform algorithm that, given a system of equations over the natural numbers with addition and $|_p$, determines whether this system has a solution or not. To reduce this problem to Hilbert's Tenth Problem over K we first let G be a subfield of K containing an element t transcendental over C_K. The field G will be defined in Lemma 2.2. Also fix a prime $\mathfrak{p}$ of K which lies above a non-trivial prime of G. We can choose t and $\mathfrak{p}$ such that $\mathrm{ord}_{\mathfrak{p}} t = 1$. Both t and $\mathfrak{p}$ will be defined at the end of Section 2. Let $\mathcal{O}_{K,\mathfrak{p}} := \{x \in K : \mathrm{ord}_{\mathfrak{p}} x \geq 0\}$, and let $\mathcal{O}_{G,\mathfrak{p}} := G \cap \mathcal{O}_{K,\mathfrak{p}}$. Now let $\mathrm{INT}(\mathfrak{p})$ be any subset of K such that $\mathcal{O}_{G,\mathfrak{p}} \subseteq \mathrm{INT}(\mathfrak{p}) \subseteq \mathcal{O}_{K,p}$. We define a map f from the integers to subsets of K by associating to an integer n the subset $f(n) := \{x \in \mathrm{INT}(\mathfrak{p}) : \mathrm{ord}_{\mathfrak{p}} x = n\}$. Then $n_3 = n_1 + n_2$ ($n_i \in \mathbb{N}$) is equivalent to the existence of $z_i \in f(n_i)$ such that $z_3 = z_1 \cdot z_2$. This follows from the fact that $\mathrm{ord}_{\mathfrak{p}} z_1 + \mathrm{ord}_{\mathfrak{p}} z_2 = \mathrm{ord}_{\mathfrak{p}}(z_1 \cdot z_2)$ and that $t^{n_i} \in f(n_i)$. We also have for natural numbers n, m

$$\begin{aligned} n|_p m \quad &\iff \quad \exists s \in \mathbb{N} \;\; m = p^s n \\ &\iff \quad \exists x \in f(n)\; \exists y \in f(m)\; \exists s \in \mathbb{N} \;\; (\mathrm{ord}_{\mathfrak{p}} y = p^s \mathrm{ord}_{\mathfrak{p}} x). \end{aligned}$$

This equivalence can be seen easily, because we can let $x := t^n$ and $y := t^m$. But the last formula is equivalent to

$$\exists x \in f(n)\; \exists y \in f(m)\; \exists w \in K\; \exists s \in \mathbb{N}\; w = x^{p^s} \text{ and } \{w/y, y/w\} \subset \mathrm{INT}(\mathfrak{p}).$$

Here $w/y \in \mathrm{INT}(\mathfrak{p})$ and $y/w \in \mathrm{INT}(\mathfrak{p})$ just means that y and w have the same order at $\mathfrak{p}$.

If we have diophantine definitions for $p(K) := \{(x, w) \in K^2 : \exists s \in \mathbb{N}, w = x^{p^s}\}$ and $\mathrm{INT}(\mathfrak{p})$, then the above argument shows that for every system of equations with addition and $|_p$ we can construct a system of polynomial equations over K which will have solutions in K if and only if the original system of equations over $\mathbb{N}$ has solutions in $\mathbb{N}$. But the diophantine theory of $\mathbb{N}$ with $+$ and $|_p$ is undecidable; hence Hilbert's Tenth Problem over K is undecidable.

So the strategy for the proof will be to prove that $p(K)$ is diophantine and that there exists some set $\mathrm{INT}(\mathfrak{p})$ as above which is diophantine for the class of fields K that we are considering. This can be summarized as:

Theorem 1.3. *Let K be an algebraic function field of characteristic 2 with constant field C_K. Let C be the algebraic closure of a finite field in K. Assume that C has an extension of degree 2. Assume that there are elements u, x of K with u transcendental over C_K and x algebraic over $C(u)$ and such that $K = C_K(u, x)$. Then $p(K)$ is diophantine. Also there exists a subfield G of K as above with $C(t) \subseteq G$ for an element t transcendental over C_K. There exists a prime $\mathfrak{p}$ of K satisfying the conditions above such that $\mathrm{INT}(\mathfrak{p})$ is diophantine for some set $\mathrm{INT}(\mathfrak{p})$ with $\mathcal{O}_{G,\mathfrak{p}} \subseteq \mathrm{INT}(\mathfrak{p}) \subseteq \mathcal{O}_{K,\mathfrak{p}}$. So Hilbert's Tenth Problem over K is undecidable.*

In [**Shl00**] Shlapentokh proves that for such K in any characteristic $p > 0$ there exists some set $\mathrm{INT}(\mathfrak{p})$ as above which is diophantine. She also proves that $p(K)$ is diophantine when the characteristic of K is greater than 2, but her main lemmas are not valid in characteristic 2. So in order to prove undecidability in characteristic 2, the last open case, we need to prove that $p(K)$ is diophantine when the characteristic of K is 2. The rest of the paper is devoted to proving this. The outline of the proof follows Shlapentokh's proof for odd characteristic. Before we can prove this we first need to prove some properties of K and then set up some notation. The next section will do that. In Section 3 we will prove that the set $p(K)$ is diophantine in characteristic 2.

2. Setup and notation.

Let $\mathbb{N}$ be the set of natural numbers $\{0, 1, 2, \dots\}$. Let K, C_K, C, u and x be as in Theorem 1.3. We will use the following:

Notation 2.1. Let F be a field, and $k \in \mathbb{N}$. We denote by F^k the set $F^k := \{a^k : a \in F\}$.

We will now prove some properties of K that we will need later on. We may assume that u is not a square in K, because if $u = u_1^2$ with $u_1 \in K$ and $s \in \mathbb{N}$, we can replace u by u_1. Then $K = C_K(u, x) = C_K(u_1, x)$. Since the extension $K/C_K(u)$ can be generated by a single element, $u \in K^{2^s}$ only if $s \leq [K : C_K(u)]$, so replacing u by its square root terminates after a finite number of steps.

We have the following:

Lemma 2.2. *Let K, C_K, C, u, x be as above. Let G be the algebraic closure of $C(u)$ inside K. Then $G = C(u, x)$.*

Proof. First note that $C(u)$ is algebraically closed in $C_K(u)$, because C is algebraically closed in C_K ([**Deu73**], p. 117). Let $m := [K : C_K(u)]$. If $m = 1$, i.e., $x \in C_K(u)$, then the statement is true since $C(u)$ is algebraically closed in $C_K(u)$. So assume $x \notin C_K(u)$. Let $\alpha \in G$, $\alpha \notin C(u)$. Then by [**Lan93**] Lemma 4.10, p. 366,

$$[C(u, \alpha) : C(u)] = [C_K(u, \alpha) : C_K(u)] \leq [K : C_K(u)] = m. \tag{1}$$

In particular, $[C(u, x) : C(u)] = m$. Now assume by contradiction that there exists a $\beta \in G$, $\beta \notin C(u, x)$. Let $G_1 := C(u, x, \beta)$. Then $[G_1 : C(u)] > m$. Also G_1 is an algebraic function field with constant field C, and C is perfect. Then by [**Mas84**], p. 94 the extension $G_1/C(u)$ is finite and separable, since u is not a square in G_1. Hence there exists a primitive element $\gamma \in G_1$ with $C(u, \gamma) = G_1$. But then $[C(u, \gamma) : C(u)] = [G_1 : C(u)] > m$, contradicting (1). □

Definition 2.3. Let K be an algebraic function field with constant field C_K. A *constant field extension of K* is an algebraic function field L with constant field C_L such that $L \supseteq K$, $C_L \cap K = C_K$ and L is the composite extension of K and C_L, $L = C_L K$.

Proposition 2.4. *Let G be as in Lemma 2.2. Fix a positive integer k. For any sufficiently large positive integer h a finite constant extension of G contains a nonconstant element t and a set of constants V of cardinality $k + 2^h$ such that $0 \in V$, $1 \notin V$. Also we can choose t and V such that for all $c \in V$ the divisor of $t + c$ is of the form $\mathfrak{p}_c/\mathfrak{q}$, where the $\mathfrak{p}_c$'s and $\mathfrak{q}$ are prime divisors of degree 2^h.*

Proof. This is Theorem 6.11 of [**Shl00**] if C is infinite. The proof of the existence of t and V with the desired properties in Theorem 6.11 does not use that C is infinite; it only requires passing to a finite extension of C. □

Remark. In Proposition 2.4 we can choose V with the property that for all $s \in \mathbb{N}$ for all $c, c' \in V$ $c^{p^s} \neq c'$ if $c \neq c'$.

From now on we will assume that an element t and a set V of constants with the desired properties as in Proposition 2.4 already exist in G. (Otherwise rename the constant extension G again and work with it instead.) Enlarging the field of constants by a finite extension is okay as far as the undecidability of Hilbert's Tenth Problem is concerned. Also let $\mathfrak{p} := \mathfrak{p}_0$, so that the divisor of t is of the form $\mathfrak{p}/\mathfrak{q}$.

Proposition 2.5. *Let G, C, t be as above. Then $[G : C(t)]$ is separable, and $2^h = n = [G : C(t)]$.*

Proof. Since the divisor of t is of the form $\mathfrak{p}/\mathfrak{q}$, t is not a square in G. Also C is perfect. Hence $G/C(t)$ is separable by [**Mas84**], p. 22. Also by [**FJ86**], p. 13, $[G : C(t)] = \deg \mathfrak{p} = \deg \mathfrak{q} = 2^h$. □

Now we can prove that K is separably generated:

Corollary 2.6. *Let K be an algebraic function field with constant field C_K. Let C be the algebraic closure of a finite field in K. Assume that C has an extension of degree 2. Assume that there exist x, u as above. Let G, t be as above. Then $K/C_K(t)$ is separable.*

Proof. By Proposition 2.5 $G/C(t)$ is separable. The field K is the compositum of $C_K(t)$ and G over $C(t)$, hence $K/C_K(t)$ is also separable. □

Now we can use Lemma 6.13 of [**Shl00**] to see how the $\mathfrak{p}_c$'s and $\mathfrak{q}$ behave in the extension K.

Lemma 2.7 (Lemma 6.13 of [**Shl00**]). *Let H be an algebraic function field over a field of constants C_H. Let K be a constant field extension of H. Let C_K be the constant field of K, and assume H is algebraically closed in K. Let $t \in H - C_H$ be such that $H/C_H(t)$ is separable. Let $\mathfrak{a}$ be a prime of $C_H(t)$ remaining prime in the extension H and such that its residue field is separable over C_H. Then $\mathfrak{a}$ will have just one prime factor in K.*

This lemma easily implies the following corollary:

Corollary 2.8. *Let* $\{\mathfrak{p}_c : c \in V\}$ *and* $\mathfrak{q}$ *be as in Proposition* 2.4*. Then the* $\mathfrak{p}_c$*'s and* $\mathfrak{q}$ *remain prime in* K*.*

Proof. Lemma 2.7 applies, since K/C_K is a constant field extension of G/C: By construction C is algebraically closed in C_K, and also $C_K G = K$. The only thing we need to check is that $G \cap C_K = C$. Assume $\alpha \in G - C$. Then α is transcendental over C and also over C_K. Hence $\alpha \notin G \cap C_K$. Thus we can apply the lemma to the primes, $t, 1/t$ and $t + c$ of $C(t)$. Since C is perfect, the residue extensions of the primes will be separable. □

Since the $\mathfrak{p}_c$'s and $\mathfrak{q}$ remain prime in K we will just denote them by the same letters again when considering them as primes of K, and we will let $\mathfrak{p} := \mathfrak{p}_0$. Now we can fix some notation that we will use for the rest of the paper:

- K will denote an algebraic function field over a field of constants C_K of characteristic $p = 2$.
- C will denote the algebraic closure of a finite field inside C_K.
- t will denote a nonconstant element of $K - C_K$ such that the divisor of t is of the form $\mathfrak{p}/\mathfrak{q}$, where $\mathfrak{p}$, $\mathfrak{q}$ are primes of degree 2^h for some natural number h. Furthermore, $K/C_K(t)$ is separable, and $2^h = n = [K : C_K(t)]$.
- $\widetilde{C}_K$ will denote the algebraic closure of C_K, and $\widetilde{K} := \widetilde{C}_K K$.
- r will denote the number of primes of $\widetilde{K}$ ramifying in the extension $\widetilde{K}/\widetilde{C}_K(t)$.
- V will denote a subset of C, containing $n + 2r + 6$ elements, such that $0 \in V$, $1 \notin V$, and such for all $c \in V$ the divisor of $t + c$ is of the form $\mathfrak{p}_c/q$, where $\mathfrak{p}_c$ is a prime divisor of K. Also pick V such that for any $s \in \mathbb{N}$, $c, c' \in V$, we have $c^{p^s} \neq c'$, if $c \neq c'$.
- For all $c \in V$, $\mathfrak{P}_c$ will denote the prime of $C_K(t)$ lying below $\mathfrak{p}_c$, while $\mathfrak{Q}$ will denote the prime of $C_K(t)$ lying below $\mathfrak{q}$. Also let $\mathfrak{P} := \mathfrak{P}_0$. For all $c \in V$, $\mathfrak{P}_c$ and $\mathfrak{Q}$ do not split in the extension $K/C_K(t)$.
- For every $c \in V$, V_c will denote the set $V_c := \{c^{p^j} : j \in \mathbb{N}\}$. Since every $c \in V$ is algebraic over a finite field, V_c is a finite set for all $c \in V$.

To obtain t and V with the desired properties, we have to assume that C is sufficiently large, but this is not a restriction because we can enlarge the field of constants and by Proposition 2.4 a finite extension is enough. Let L be this finite extension. If Hilbert's Tenth Problem over L is undecidable, then Hilbert's Tenth Problem over K is also undecidable. So in the following we will assume that $L = K$ to simplify notation.

3. *p*-th power equations.

Using the notation that we set up in the last section will now prove that the set $p(K) = \{(x,y) \in K^2 : \exists s \in \mathbb{N}, y = x^{2^s}\}$ is diophantine which is Theorem 3.12 below. The main ingredient for proving this is the next theorem. It gives an equivalent definition of what it means for (x,y) to be in $p(K)$. Eventually we want to find polynomial equations describing these relations, so the goal afterwards will be to rewrite the equations below as polynomial equations.

Theorem 3.1. *Given $x, y \in K$, let $u := \frac{x^2+t^2+t}{x^2+t}$ and $\widetilde{u} := \frac{x^2+t^{-2}+t^{-1}}{x^2+t^{-1}}$. Let $v := \frac{y^2+t^{2^{s+1}}+t^{2^s}}{y^2+t^{2^s}}$ and $\widetilde{v} := \frac{y^2+t^{-2^{s+1}}+t^{-2^s}}{y^2+t^{-2^s}}$ for some $s \in \mathbb{N}$.*

Then $y = x^{2^s}$ if and only if

$$\exists r \in \mathbb{N}\ v = u^{2^r} \tag{2}$$

$$\exists j \in \mathbb{N}\ \widetilde{v} = \widetilde{u}^{2^j}. \tag{3}$$

Proof. Suppose $y = x^{2^s}$. Let $r = j = s$. Then (2) and (3) are satisfied. This completes one direction of the proof.

On the other hand, suppose that r and j as in the statement of the theorem exist. Then

$$v = \left(\frac{x^2+t^2+t}{x^2+t}\right)^{2^r} = \frac{x^{2^{r+1}}+t^{2^{r+1}}+t^{2^r}}{x^{2^{r+1}}+t^{2^r}} = \frac{y^2+t^{2^{s+1}}+t^{2^s}}{y^2+t^{2^s}}.$$

So

$$(x^{2^{r+1}}+t^{2^{r+1}}+t^{2^r})(y^2+t^{2^s}) = (x^{2^{r+1}}+t^{2^r})(y^2+t^{2^{s+1}}+t^{2^s}),$$

i.e.,

$$t^{2^{r+1}}y^2 + t^{2^{r+1}+2^s} = x^{2^{r+1}}t^{2^{s+1}} + t^{2^r+2^{s+1}}.$$

Thus

$$y^2 = (x^{2^{r+1}}t^{2^{s+1}} + t^{2^r+2^{s+1}} + t^{2^{r+1}+2^s}) \cdot t^{-2^{r+1}}. \tag{4}$$

Hence if we can show that $r = s$, then $y^2 = x^{2^{s+1}}$, so $y = x^{2^s}$, since the characteristic of K is 2. So our goal is to show that $r = s$.

Similarly to the calculations above we get

$$\widetilde{v} = \left(\frac{x^2+t^{-2}+t^{-1}}{x^2+t^{-1}}\right)^{2^j} = \frac{x^{2^{j+1}}+t^{-2^{j+1}}+t^{-2^j}}{x^{2^{j+1}}+t^{-2^j}} = \frac{y^2+t^{-2^{s+1}}+t^{-2^s}}{y^2+t^{-2^s}},$$

and we get

$$y^2 = (x^{2^{j+1}}t^{-2^{s+1}} + t^{-2^j-2^{s+1}} + t^{-2^{j+1}-2^s}) \cdot t^{2^{j+1}}. \tag{5}$$

By (4)

$$y = (x^{2^r}t^{2^s} + t^{2^{r-1}+2^s} + t^{2^r+2^{s-1}}) \cdot t^{-2^r} \tag{6}$$

(unless r or s are < 1), and by (5)

$$y = (x^{2^j} t^{-2^s} + t^{-2^s - 2^{j-1}} + t^{-2^j - 2^{s-1}}) \cdot t^{2^j} \tag{7}$$

(unless j or $s < 1$). Eliminating y from (6) and (7), we get

$$(t^{2^s - 2^r} x^{2^r}) + (t^{2^j - 2^s} x^{2^j}) = t^{2^s - 2^{r-1}} + t^{2^{s-1}} + t^{2^{j-1} - 2^s} + t^{-2^{s-1}}. \tag{8}$$

Now assume that y is a square, say $y = z^2$ (and $s, j, r > 0$). Then

$$v = \frac{z^4 + t^{2^{s+1}} + t^{2^s}}{z^4 + t^{2^s}} = \left(\frac{z^2 + t^{2^s} + t^{2^{s-1}}}{z^2 + t^{2^{s-1}}} \right)^2 = (v')^2.$$

Hence

$$v = (v')^2 = u^{2^r}, \text{ so } u^{2^{r-1}} = \left(\frac{z^2 + t^{2^s} + t^{2^{s-1}}}{z^2 + t^{2^{s-1}}} \right) = v'.$$

Similarly $\widetilde{v} = (\widetilde{v}')^2$ and $\widetilde{u}^{2^{j-1}} = \widetilde{v}'$, so in the new formulae s, r and j are replaced by $s-1, r-1$ and $j-1$, respectively, and we're done if we can show that $z = x^{2^{s-1}}$. Hence we can reduce the problem to the case where either (a) $s = 0$ or $r = 0$ or $j = 0$, or (b) y is not a square.

Case (a). $s = 0$: If $s = 0$, then $v = \frac{y^2+t^2+t}{y^2+t}$, and v is not a square since $\frac{dv}{dt} = \frac{y^2+t^2+t+y^2+t}{(y^2+t)^2} = \frac{t^2}{(y^2+t)^2} \neq 0$. So if $s = 0$, then $v = \frac{y^2+t^2+t}{y^2+t} = u^{2^r}$. Since v is not a square, this implies $r = 0$. Hence $r = s = 0$ and we're done.

If $r = 0$, then $v = u$. By the same argument as above u is not a square. Now if $s > 0$, then v is a square and hence u is a square, contradiction. Hence $r = s = 0$, and we're done. The case $j = 0$ follows from symmetry.

Case (b). By Case (a) we may assume $r > 0, s > 0$ and $j > 0$ and by contradiction let's assume that $r \neq s$. If we look at Equations (6) and (7), we see that y is a square unless (i) $s = 1$ or (ii) both $r = j = 1$.

(i) Suppose $s = 1$. Since we're done if $r = s$ we may assume that $r \geq 2, j \geq 2$. From (8) we obtain

$$t^{2-2^r} x^{2^r} + t^{2^j - 2} x^{2^j} = t^{2-2^{r-1}} + t^{2^{j-1}-2} + t + \frac{1}{t}$$

or

$$(t^{1-2^{r-1}} x^{2^{r-1}} + t^{2^{j-1}-1} x^{2^{j-1}} + t^{1-2^{r-2}} + t^{2^{j-2}-1})^2 = t + \frac{1}{t}.$$

Since $j \geq 2$ and $r \geq 2$ the left side is a square. The right side is not, contradiction.

(ii) Suppose $r = j = 1$. Again since we're done if $r = s$ we may assume $s > 1$. By (8) we have

$$x^2(t^{2^s-2} + t^{2-2^s}) = t^{1-2^s} + t^{2^s-1} + \frac{1}{t^{2^{s-1}}} + t^{2^{s-1}}.$$

Let $\mathfrak{p}$ be the simple zero of t. Since $1-2^s < -2^{s-1}$ $(s \geq 2)$, the right side has a pole of odd order at $\mathfrak{p}$, while the left side is a square, so it only has poles of even order. This proves the theorem. □

So the goal for the rest of this section is to show that the relations we used in the statement of the theorem are diophantine. To do that it will clearly be enough to show that the following four sets are diophantine:

$$S := \{\, t^{2^s} : s \in \mathbb{N}\}, \quad S' := \{\, (t^{-1})^{2^s} : s \in \mathbb{N}\},$$

$$T := \left\{ (x,w) \in K^2 : \exists s \in \mathbb{N}, w = \left(\frac{x^2+t^2+t}{x^2+t}\right)^{2^s} \right\},$$

and

$$T' := \left\{ (x,w) \in K^2 : \exists s \in \mathbb{N}, w = \left(\frac{x^2+(t^{-1})^2+t^{-1}}{x^2+t^{-1}}\right)^{2^s} \right\}.$$

It is enough to prove that S and T are diophantine, because we can replace t by t^{-1} and replace V by $W := \left\{\frac{1}{c} : c \in (V - \{0\})\right\} \cup \{0\}$ in Section 2. Then we can also replace t by t^{-1} and V by W in the whole proof to obtain diophantine definitions for S' and T'.

Lemma 3.5 and Corollary 3.7 below will show that S is diophantine, and Corollary 3.11 will show that T is diophantine.

3.1. The set $S = \{\, t^{2^s} : s \in \mathbb{N}\}$ is diophantine. To prove that S is diophantine, we first need a definition and a lemma:

Definition 3.2. Let $w \in K$. The *height* of w is the degree of the zero divisor of w.

Remark. Equivalently, we could have defined the height of $w \in K$ to be the degree of the pole divisor of w.

Lemma 3.3. *Let $w \in K$, let $a, b \in C$. Then all the zeros of $\frac{w+a}{w+b}$ are zeros of $w+a$ and all the poles of $\frac{w+a}{w+b}$ are zeros of $w+b$. Furthermore, the height of $\frac{w+a}{w+b}$ is equal to the height of w.*

Proof. This is Lemma 2.4 in [**Shl00**]. □

Lemma 3.4. *Let $u, v, z \in \widetilde{K} := \widetilde{C}_K K$, assume that $z \notin \widetilde{C}_K$, and let $y \in \widetilde{C}_K(z)$. Assume that y, z do not have zeros or poles at any valuation of $\widetilde{K}$ ramifying in the extension $\widetilde{K}/\widetilde{C}_K(z)$ and that $\widetilde{K}/\widetilde{C}_K(z)$ is separable. Moreover, assume*

$$y + z = u^4 + u \tag{9}$$

$$\frac{1}{y} + \frac{1}{z} = v^4 + v. \tag{10}$$

Then $y = z^{4^k}$ for some $k \geq 0$.

Proof. Recall that for a field F and a natural number k, F^k denotes the set $F^k = \{a^k : a \in F\}$. In $\widetilde{C}_K(z)$ the zeros and poles of z are simple. Assuming that z satisfies the conditions of Lemma 3.4 thus amounts to assuming that all zeros and poles of z are simple in $\widetilde{K}$.

Equation (9) and the fact that z has simple poles imply that $y \notin \widetilde{C}_K$, so $y \in (\widetilde{K})^{4^s}$ only if $s \leq [\widetilde{K} : \widetilde{C}_K(z)]$. If $y = w^4$ with $w \in \widetilde{C}_K(z)$, then $w + z = (u+w)^4 + (u+w)$ and $1/w + 1/z = (v + 1/w)^4 + (v + 1/w)$. So if we can prove that $w = z^{4^s}$ for some $s \in \mathbb{N}$, then $y = w^4 = z^{4^{s+1}}$. Hence we may assume without loss of generality that $y \notin (\widetilde{C}_K(z))^4$.

Let $\frac{\mathcal{A}}{\mathcal{B}}$ be the divisor of z in $\widetilde{K}$, where $\mathcal{A}$ and $\mathcal{B}$ are relatively prime effective divisors. By assumption, all the prime factors of $\mathcal{A}$ and $\mathcal{B}$ are distinct. Also all the poles of $u^4 + u$ and $v^4 + v$ have orders divisible by 4.

Claim. The divisor of y is of the form $\mathcal{E}^4\mathcal{D}$ where all the prime factors of $\mathcal{D}$ come from $\mathcal{A}$ or $\mathcal{B}$. Also the factors of $\mathcal{A}$ that appear in $\mathcal{D}$, will appear to the first power in $\mathcal{D}$ and the factors of $\mathcal{B}$ that appear in $\mathcal{D}$ occur to the power -1.

Proof of Claim. Let $\mathfrak{t}$ be a prime which is not a factor of $\mathcal{A}$ or $\mathcal{B}$. Without loss of generality assume $\mathfrak{t}$ is a pole of y. Then, since $\mathrm{ord}_{\mathfrak{t}} z = 0$, we have

$$0 > \mathrm{ord}_{\mathfrak{t}} y = \mathrm{ord}_{\mathfrak{t}}(z+y) = \mathrm{ord}_{\mathfrak{t}}(u^4+u) \equiv 0 \mod 4.$$

Now let $\mathfrak{t}$ be a factor of $\mathcal{A}$ or $\mathcal{B}$. Again without loss of generality assume $\mathfrak{t}$ is a pole of y. If $\mathfrak{t}$ is a factor of $\mathcal{A}$, then $\mathrm{ord}_{\mathfrak{t}} y = \mathrm{ord}_{\mathfrak{t}}(y+z) = \mathrm{ord}_{\mathfrak{t}}(u^4+u)$. Hence $\mathfrak{t}$ is a pole of u, so $\mathrm{ord}_{\mathfrak{t}} y \equiv 0 \mod 4$. If, however, $\mathfrak{t}$ is a factor of $\mathcal{B}$, there are two possibilities: Either $\mathrm{ord}_{\mathfrak{t}} y = \mathrm{ord}_{\mathfrak{t}} z = -1$ or again $\mathrm{ord}_{\mathfrak{t}} y = \mathrm{ord}_{\mathfrak{t}}(u^4+u) \equiv 0 \mod 4$. This proves the claim.

On the other hand, $\mathcal{A}$ and $\mathcal{B}$ considered as divisors over $\widetilde{C}_K(z)$ are prime divisors, and since $y \in \widetilde{C}_K(z)$, we can deduce that the divisor of y is of the form $\mathcal{E}^4\mathcal{A}^a\mathcal{B}^b$, with either, $a, b = 0$ or $a = 1, b = -1$, since the degree of the zero and the pole divisor must be the same.

Case I: $a = b = 0$.

Since no prime which is a zero of y ramifies in the extension $\widetilde{K}/\widetilde{C}_K(z)$, the divisor of y in $\widetilde{C}_K(z)$ is also a fourth power of another divisor. In the rational function field $\widetilde{C}_K(z)$ every degree 0 divisor is principal, so $y \in (\widetilde{C}_K(z))^4$.

Case II: $a = 1, b = -1$.

In this case, the divisor of $\frac{y}{z}$ is of the form $\mathcal{E}^4$ and hence $\frac{y}{z} = f^4$ for some $f \in \widetilde{C}_K(z)$ by the same argument as in Case I. Hence $y + z = u^4 + u$ can be rewritten as $z\left(\frac{y}{z}+1\right) = z(f+1)^4 = u^4 + u$. Since $f+1$ is a rational function in z, we can rewrite this as

$$z\left(\frac{f_1}{f_2}\right)^4 = u^4 + u \tag{11}$$

where f_1, f_2 are relatively prime polynomials in $\widetilde{C}_K[z]$, and f_2 is monic. Equation (11) shows: Any valuation which is a pole of u is either a pole of z or a zero of f_2. Let $\mathfrak{c}$ be a pole of u which is a zero of f_2. Then, since f_2 is a polynomial in z, $\mathfrak{c}$ is not a pole of z. So we must have $|\mathrm{ord}_{\mathfrak{c}} f_2| = |\mathrm{ord}_{\mathfrak{c}} u|$. Hence $s := f_2 \cdot u$ will have poles only at the valuations which are poles of z. Thus we can rewrite (11) in the form

$$zf_1^4 + s^4 = sf_2^3. \tag{12}$$

Furthermore, let $\mathfrak{c}$ be a zero of f_2. As pointed out above, $\mathfrak{c}$ is not a pole of z, so $\mathfrak{c}$ is not a pole of s. So we can deduce that for a zero $\mathfrak{c}$ of f_2 we have $\mathrm{ord}_{\mathfrak{c}}(s^4 + zf_1^4) = \mathrm{ord}_{\mathfrak{c}}(sf_2^3) \geq 3$. Thus $\mathrm{ord}_{\mathfrak{c}}(d(s^4 + zf_1^4)) \geq 2$, so $\mathrm{ord}_{\mathfrak{c}}(f_1^4\, dz) \geq 2$. Here dz denotes a Kähler differential. Since $\mathfrak{c}$ is unramified in the extension $\widetilde{K}/\widetilde{C}_K(z)$, $\mathrm{ord}_{\mathfrak{c}}(dz) = 0$. Hence $\mathrm{ord}_{\mathfrak{c}}(f_1^4) \geq 2$, i.e., f_1 has a zero at $\mathfrak{c}$. Since f_1 and f_2 are relatively prime polynomials, this implies that f_2 has no zeros, i.e., $f_2 = 1$. Hence y is a polynomial in z. Exactly the same argument applied to $\frac{1}{y}$ shows that $\frac{1}{y}$ is a polynomial in $\frac{1}{z}$. Thus $y = z^l$ for some $l \geq 0$ and $y + z = z^l + z = u^4 + u$. If $y = z$, we are done. Otherwise this implies that all the poles of $y + z$ have order l (the poles of z are simple), and also, that all the poles of $y + z$ are divisible by 4. Hence $4|l$.

So in both cases, Case I and Case II, we could deduce that either $y = z$ or that $y \in (\widetilde{C}_K(z))^4$. Since we assumed that $y \notin (\widetilde{C}_K(z))^4$ this concludes the proof of the Claim. □

Lemma 3.5. *For all $c, c' \in V$ let $t_{c,c'} := \frac{t+c}{t+c'}$. Let $w, v, u, u_{d,d'}, v_{d,d'}$ be elements of K such that $\forall c \in V\ \exists d \in V_c$ such that $\forall c' \in V\ \exists d' \in V_{c'}$ such that the following equations are satisfied:*

$$w + t = u^4 + u \tag{13}$$

$$\frac{1}{w} + \frac{1}{t} = v^4 + v \tag{14}$$

$$w_{d,d'} = \frac{w+d}{w+d'} \tag{15}$$

$$w_{d,d'} + t_{c,c'} = u_{d,d'}^4 + u_{d,d'} \tag{16}$$

$$\frac{1}{w_{d,d'}} + \frac{1}{t_{c,c'}} = v_{d,d'}^4 + v_{d,d'}. \tag{17}$$

Then $w = t^{4^s}$ for some natural number s.

Proof. Recall that the divisor of t in K is of the form $\mathfrak{p}/\mathfrak{q}$, and that $\mathfrak{P}$ and $\mathfrak{Q}$ are the primes of $C_K(t)$ lying below $\mathfrak{p}$ and $\mathfrak{q}$, respectively. Thus the degree of $\mathfrak{Q}$ is one. Similarly, for all $c \in V$ the degree of the primes $\mathfrak{P}_c$ in $C_K(t)$ is one. Hence $\mathfrak{Q}$ and all the $\mathfrak{P}_c$'s will remain prime in the constant field extension $\widetilde{C}_K(t)/C_K(t)$. By Lemma 6.16 in [**Shl00**] their factors will be unramified in the extension $\widetilde{K}/\widetilde{C}_K(t)$. Hence for all $c, c' \in V$, $t_{c,c'}$ has neither zeros nor poles at any prime ramifying in the extension $\widetilde{K}/\widetilde{C}_K(t)$.

In the second paragraph of the proof of Lemma 2.6 of [**Shl00**], pp. 471-472, translated to our notation, Shlapentokh proves that for some $c_0 \in V$ there exists a subset V' of V containing $n+1$ elements, not containing c_0, and such that for any $d_0 \in V_{c_0}$, for all $c' \in V'$, for any $d' \in V_{c'}$, $w_{d_0,d'}$ does not have zeros or poles at any prime ramifying in the extension $\widetilde{K}/\widetilde{C}_K(t)$. Her argument uses the fact that there are exactly r primes ramifying in the extension $\widetilde{K}/\widetilde{C}_K(t)$, and it does not use the characteristic of K, so the same proof works here. We have two cases to consider:

Case I: $w \in C_K(t)$.

If w is in $C_K(t)$, then pick a $d_0 \in V_{c_0}$ and for some $c' \in V'$ pick a $d' \in V_{c'}$ such that (16) and (17) are satisfied. Then $w_{d_0,d'} \in C_K(t)$, and we can apply Lemma 3.4 to $t_{c_0,c'}$ instead of t, and to $w_{d_0,d'}$ to conclude that $w_{d_0,d'} = t_{c_0,c'}^{4^s}$ for some $s \geq 0$. (Note that $C_K(t) = C_K(t_{c_0,c'})$.) So

$$\frac{w+d_0}{w+d'} = \left(t_{c_0,c'}\right)^{4^s}.$$

If $s = 0$, then we can check that $w = t$. (See the last part of Lemma 3.3.) Otherwise write $1 + \frac{d_0+d'}{w+d'} = \left(t_{c_0,c'}\right)^{4^s}$.

Hence $w + d' = \left(\frac{1}{t_{c_0,c'}+1}\right)^{4^s} \cdot (d_0 + d')$. Since $(d_0 + d')$ is an element of C and hence a fourth power this implies that $w + d' \in (C_K(t))^4$, and hence $w \in (C_K(t))^4$, say $w = \widetilde{w}^4$. We can rewrite Equations (13) and (14) as

$$\widetilde{w} + t = (u+\widetilde{w})^4 + (u+\widetilde{w}) \tag{18}$$

$$\frac{1}{\widetilde{w}} + \frac{1}{t} = \left(v + \frac{1}{\widetilde{w}}\right)^4 + \left(v + \frac{1}{\widetilde{w}}\right). \tag{19}$$

Also

$$w_{d,d'} = \frac{w+d}{w+d'} = \frac{w+\widetilde{d}^4}{w+\widetilde{d}'^4} = \left(\frac{\widetilde{w}+\widetilde{d}}{\widetilde{w}+\widetilde{d}'}\right)^4$$

for $d \in V_c, d' \in V_{c'}$ and some suitable $\widetilde{d} \in V_c$ and $\widetilde{d}' \in V_{c'}$. This lets us rewrite Equations (16) and (17) in a similar fashion. So we can rewrite Equations (13) through (17), and $\widetilde{w} \in C_K(t)$. Equation (13) and the fact that t has only simple zeros imply that $w \notin C_K$. Hence after finitely many iterations we must be in the position where $s = 0$.

Case II: $w \notin C_K(t)$.

In this case we will derive a contradiction. $w \notin C_K(t)$ would imply that $w_{d,d'} \notin C_K(t)$ for all d and d'.

By putting $\alpha := u^2 + u$ we can rewrite Equation (13) as

$$w + t = \alpha^2 + \alpha. \tag{20}$$

Similarly by putting $\beta := v^2 + v$, $\alpha_{d,d'} := u_{d,d'}^2 + u_{d,d'}$, $\beta_{d,d'} := v_{d,d'}^2 + v_{d,d'}$ we can rewrite (14),(16) and (17) as

$$\frac{1}{w} + \frac{1}{t} = \beta^2 + \beta \tag{21}$$

$$w_{d,d'} + t_{c,c'} = \alpha_{d,d'}^2 + \alpha_{d,d'} \tag{22}$$

$$\frac{1}{w_{d,d'}} + \frac{1}{t_{c,c'}} = \beta_{d,d'}^2 + \beta_{d,d'}. \tag{23}$$

Let $c_0 \in V$ be as above. By the same argument as in [**Shl00**], p. 472, with p replaced by 2, (20) through (23) imply that $\exists d_0 \in V_{c_0}$ such that $\forall c' \in V'\ \exists d' \in V_{c'}$ such that the divisor of $w_{d_0,d'}$ is of the form $\mathcal{A}^2 \mathfrak{p}_{d'}^a \mathfrak{p}_{d_0}^b$. Here $\mathfrak{p}_{d_0}$ and $\mathfrak{p}_{d'}$ are prime divisors, a is either -1 or 0, and b is either 1 or 0. Now the proof follows word for word that of Lemma 2.6 in [**Shl00**], p. 472 with p replaced by 2 to prove that in this case $w = \widetilde{w}^2$ with $\widetilde{w} \in K$. For this part of the proof we only used Equations (20) through (23). Now we can rewrite Equations (20) through (23) with w replaced by $\widetilde{w}$. Since $w \notin C_K(t)$, $\widetilde{w} \notin C_K(t)$. So we can keep replacing w by its square root over and over, contradicting that $w \in K^{2^s}$ only if $s \leq [K : C_K(t)]$. So $w = t^{4^s}$ for some $s \in \mathbb{N}$. □

Corollary 3.6. *The set* $S_1 := \{\, t^{4^s} : s \in \mathbb{N} \,\}$ *is diophantine over* K*.*

Proof. Lemma 3.5 shows that an element $w \in K$ satisfying Equations (13) through (17) must be of the form $w = t^{4^s}$ for some $s \in \mathbb{N}$. What we have left to show is that if $w = t^{4^s}$ for some $s \in \mathbb{N}$, then we can satisfy Equations (13) through (17). If $w = t$, let $u = 0$ and $v = 0$. For the general case we use the fact that for any $x \in K$ and any $s \in \mathbb{N}$ we have

$$x^{4^s} - x = (x^{4^{s-1}} + x^{4^{s-2}} + \cdots + x)^4 - (x^{4^{s-1}} + x^{4^{s-2}} + \cdots + x).$$

So if $w = t^{4^s}$ with $s \geq 1$, let $u = t^{4^{s-1}} + \cdots + t^4 + t$. For v take

$$\frac{1}{t^{4^{s-1}}} + \cdots + \frac{1}{t^4} + \frac{1}{t}.$$

Now fix $c \in V$. To satisfy the other equations we can use the same argument, if we can show that $\exists d \in V_c$ such that $\forall c' \in V \exists d' \in V_{c'}$ such that $w_{d,d'} = (t_{c,c'})^{4^s}$. This is done in Corollary 2.7 in [**Shl00**]. □

Corollary 3.7. *The set* $S = \{\, t^{2^s} : s \in \mathbb{N} \,\}$ *is diophantine over* K*.*

Proof. This follows from the fact that

$$w \in S \iff (w \in S_1 \text{ or } \exists z \in K\, (z^2 = w \text{ and } z \in S_1)).$$

3.2. The set $T = \left\{(x,w) \in K^2 : \exists s \in \mathbb{N}, w = \left(\frac{x^2+t^2+t}{x^2+t}\right)^{2^s}\right\}$ is diophantine over K.

Lemma 3.8. *Let $x \in K$. Let t be as above, i.e., $\widetilde{K}/\widetilde{C}_K(t)$ is separable and the divisor of t is of the form $\frac{\mathfrak{p}}{\mathfrak{q}}$. Let $u = \frac{x^2+t^2+t}{x^2+t}$, and let $a \in C$, $a \neq 1$. Then $u+a$ has only simple zeros and simple poles, except possibly for zeros at $\mathfrak{p}, \mathfrak{q}$ or primes ramifying in the extension $\widetilde{K}/\widetilde{C}_K(t)$.*

Proof. First we will show that the zeros of $u+a$ away from the ramified primes and $\mathfrak{p}$ and $\mathfrak{q}$ are simple: By Lemma 4.4 in [**Shl96**] it is enough to show that $u+a$ and $\frac{du}{dt}$ do not have common zeros. We have

$$\frac{d(u+a)}{dt} = \frac{(x^2+t^2+t)+(x^2+t)}{(x^2+t)^2} = \frac{t^2}{(x^2+t)^2} \quad \text{and}$$
$$u+a = \frac{x^2+t^2+t}{x^2+t} + a = 1 + a + \frac{t^2}{x^2+t}.$$

Suppose $\mathfrak{c}$ is a zero of $d(u+a)/dt$ satisfying the above conditions. Then $\mathfrak{c}$ is not a zero of t, so $\mathfrak{c}$ must be a pole of x^2+t, i.e., a pole of x. If $\mathfrak{c}$ is a pole of x, then it is a zero of $\frac{t^2}{x^2+t}$, and hence not a zero of $1+a+\frac{t^2}{x^2+t}$. Hence $d(u+a)/dt$ and $u+a$ have no zeros in common, except possibly the ones mentioned above.

We will now show that all poles at above described valuations are simple: Since u and $u+a$ have the same poles, it is enough to show that the poles of u are simple. u has simple poles if and only if the zeros of u^{-1} are simple. So we'll show that the zeros of $v = u^{-1}$ are simple by doing exactly the same thing as above. Let $v := u^{-1} = \frac{x^2+t}{x^2+t^2+t}$. Then

$$\frac{dv}{dt} = \frac{(x^2+t+x^2+t^2+t)}{(x^2+t^2+t)^2} = \frac{t^2}{(x^2+t^2+t)^2} \quad \text{and}$$
$$v = \frac{x^2+t}{x^2+t^2+t} = 1 - \frac{t^2}{(x^2+t^2+t)^2}.$$

Again let $\mathfrak{c}$ be a zero of dv/dt satisfying the above conditions. Again $\mathfrak{c}$ has to be a pole of x. So $\mathfrak{c}$ is a zero of v, but not a zero of $1 - \frac{t^2}{x^2+t^2+t}$, since $\mathfrak{c}$ is not a zero or pole of t. Hence all the zeros of u^{-1} are simple except possibly for the ones mentioned above. □

Lemma 3.9. *Let $x, v \in K^*$, let $u := \frac{x^2+t^2+t}{x^2+t}$. For all $c, c' \in V$, $g \in \{-1, 1\}$ let*

$$u_{c,c',g} := \frac{u^g + c}{u^g + c'}.$$

For $d \in V_c, d' \in V_{c'}, g \in \{-1,1\}$ *let*

$$v_{d,d',g} := \frac{v^g + d}{v^g + d'}.$$

In addition assume that $\forall c \in V\ \exists d \in V_c$ *such that* $\forall c' \in V\ \exists d' \in V_{c'}$ *such that the following equations hold for for* $e, g \in \{-1,1\}$*, and some* $s \in \mathbb{N}$*:*

$$v_{d,d',g}^e + u_{c,c',g}^e = \sigma_{d,d',e,g}^4 + \sigma_{d,d',e,g} \tag{24}$$

$$v_{d,d',g}^{2e} t^{4^s} + u_{c,c',g}^{2e} t = \lambda_{d,d',e,g}^4 + \lambda_{d,d',e,g} \tag{25}$$

$$(u^g + c)^e + (v^g + d)^e = \mu_{d,e,g}^4 + \mu_{d,e,g}. \tag{26}$$

Then for some natural number m*,* $v = u^{4^m}$*.*

Proof. It is sufficient to prove that the result is valid in $\widetilde{K} := \widetilde{C}_K K$, so we work in $\widetilde{K}$. We will first prove the following:

Claim. For all $c, c \in V, g \in \{-1,1\}$, $u_{c,c',g}$ has no multiple zeros or poles except possibly at the primes ramifying in $\widetilde{K}/\widetilde{C}_K(t)$ or $\mathfrak{p}$ or $\mathfrak{q}$.

Proof of Claim. By Lemma 3.3 we have that for all c, c', g as above all the poles of $u_{c,c',g}$ are zeros of $u^g + c'$ and all the zeros of $u_{c,c',g}$ are zeros of $u^g + c$. By Lemma 3.8 and by assumption on c and c', all the zeros of $u^g + c'$ and $u^g + c$ are simple, except possibly for zeros at $\mathfrak{p}$, $\mathfrak{q}$ or primes ramifying in the extension $\widetilde{K}/\widetilde{C}_K(t)$. This proves the claim.

Also since $\frac{du}{dt} \neq 0$, u is not a second power in $\widetilde{K}$. We will show the following: (a) If $s = 0$, then $u = v$, and (b) if $s > 0$, then v is a fourth power of some element in $\widetilde{K}$.

Case (a): Suppose that $s = 0$, and set $g = 1$.

Again, using Shlapentokh's argument in Lemma 2.6 of [**Shl00**] there exists $c_0 \in V$ and $V' \subseteq (V - \{c_0\})$ containing $n+1$ elements, such that for all $d_0 \in V_{c_0}$, for all $c' \in V'$, and for all $d' \in V_{c'}$, $u_{c_0,c',1}$ and $v_{d_0,d',1}$ have no zeros or poles at the primes of $\widetilde{K}$ ramifying in the extension $\widetilde{K}/\widetilde{C}(t)$ or at $\mathfrak{p}$ or $\mathfrak{q}$. For indices selected in this way, all the poles and zeros of $u_{c_0,c',1}$ are simple. Pick $d_0 \in V_{c_0}$ and for all $c' \in V'$ pick $d' \in V_{c'}$ such that Equations (24) and (25) are satisfied. Equations (25) and (24) imply:

$$v_{d_0,d',1}^2 t^{4^s} + u_{c_0,c',1}^2 t = \lambda_{d_0,d',1,1}^4 + \lambda_{d_0,d',1,1} \tag{27}$$

$$v_{d_0,d',1}^2 + u_{c_0,c',1}^2 = \sigma_{d_0,d',1,1}^8 + \sigma_{d_0,d',1,1}^2. \tag{28}$$

From (27) and (28) we obtain (since $s = 0$)

$$\lambda_{d_0,d',1,1}^4 + \lambda_{d_0,d',1,1} = t(\sigma_{d_0,d',1,1}^8 + \sigma_{d_0,d',1,1}^2).$$

All the poles of $\lambda_{d_0,d',1,1}$ and $\sigma_{d_0,d',1,1}$ are poles of $u_{c_0,c',1}$, $v_{d_0,d',1}$ or t, and thus are not at any valuation ramifying in the extension $\widetilde{K}/\widetilde{C}_K(t)$. By

Lemma 4.4 applied to $\sigma = \sigma^2_{d_0,d',1,1}$ and (28)

$$v^2_{d_0,d',1} + u^2_{c_0,c',1} = 0.$$

Thus $v_{d_0,d',1} = u_{c_0,c',1}$. From here on the proof is word for word like the proof of Lemma 2.10 in [**Shl00**], top of p. 477, showing that if $s = 0$, then $u = v$.

Case (b): Suppose now that $s > 0$. Again set $g = 1$. Let c_0 and V' be selected as above.

Again we can pick $d_0 \in V_{c_0}$ and for all $c' \in V'$ we can pick $d' \in V_{c'}$ such that Equations (24) through (26) are satisfied and such that the corresponding $u_{c_0,c',1}$ and $v_{d_0,d',1}$ do not have zeros or poles at the primes of $\widetilde{K}$ ramifying in the extension $\widetilde{K}/\widetilde{C}(t)$ or at $\mathfrak{p}$ or $\mathfrak{q}$. We can use the same argument as in Lemma 3.4 to show that either:

- (i) For all d' chosen as above the divisor of $v_{d_0,d',1}$ in $\widetilde{K}$ is a fourth power of another divisor, or
- (ii) for some $c' \in V'$ and some $d' \in V_{c'}$ and some prime $\mathfrak{t}$ not ramifying in $\widetilde{K}/\widetilde{C}(t)$ and not equal to $\mathfrak{p}$ or $\mathfrak{q}$, $\mathrm{ord}_{\mathfrak{t}} v_{d_0,d'} \in \{1, -1\}$.

In Case (i), because of our choice of the $v_{d_0,d'}$'s and Proposition 4.3, a short calculation shows that $v \in \widetilde{K}^4$:

$$\begin{aligned} v^{-1}_{d_0,d',1} &= \frac{v + d_0}{v + d'} = 1 + \frac{(d' + d_0)}{v + d_0} \\ &= (d' + d_0)\left(\frac{1}{d' + d_0} + \frac{1}{v + d_0}\right), \end{aligned}$$

where $d_0 \in V_{c_0}$ is fixed, and we have $d' \in V_{c'}$, and all d' are distinct. Also V' contains $n + 1$ elements, so by Proposition 4.3 applied to $\frac{1}{v+d'}$ we have that $\frac{1}{v+d'} \in \widetilde{K}^4$. This implies that $v \in \widetilde{K}^4$. This finishes Case (i).

So assume now that we are in Case (ii): Without loss of generality, assume that $\mathfrak{t}$ is a pole of $v_{d_0,d',1}$ (and hence neither a zero nor a pole of t).

Again look at Equations (27) and (28). Since t does not have a pole or a zero at $\mathfrak{t}$ and since the right hand sides of Equations (27) and (28) only have poles of order ≥ 4,

$$\mathrm{ord}_{\mathfrak{t}}(v^2_{d_0,d',1} t^{4^s} + u^2_{c_0,c',1} t) = \mathrm{ord}_{\mathfrak{t}}(\lambda^4_{d_0,d',1,1} + \lambda_{d_0,d',1,1}) \geq 0 \text{ and} \tag{29}$$

$$\mathrm{ord}_{\mathfrak{t}}(v^2_{d_0,d',1} + u^2_{c_0,c',1}) = \mathrm{ord}_{\mathfrak{t}}(\sigma^8_{d_0,d',1,1} + \sigma^2_{d_0,d',1,1}) \geq 0. \tag{30}$$

Thus

$$\mathrm{ord}_{\mathfrak{t}} v^2_{d_0,d',1}(t^{4^s} + t) \geq 0.$$

Hence it follows that $\mathrm{ord}_{\mathfrak{t}}(t^{4^s} + t) \geq 2|\mathrm{ord}_{\mathfrak{t}} v_{d_0,d',1}|$. But in $\widetilde{C}_K(t)$ all the zeros of $t^{4^s} + t$ are simple. So this function can have multiple zeros only at primes ramifying in the extension $\widetilde{K}/\widetilde{C}_K(t)$. But by assumption $\mathfrak{t}$ is not one of these primes, and so we have a contradiction unless $v \in \widetilde{K}^4$. This shows that if $s > 0$, then Equations (24) through (26) can be rewritten in the same fashion as in Lemma 3.5 with v replaced by its fourth roots, and in (25) s is replaced by $s-1$. Therefore, after finitely many iterations of this rewriting procedure we will be in the case of $s = 0$, which was treated in Case (a). Hence, for some natural number m, $v = u^{4^m}$. □

Corollary 3.10. *The set* $T_1 := \left\{(x,w) \in K^2 : \exists s \in \mathbb{N}, w = \left(\frac{x^2+t^2+t}{x^2+t}\right)^{4^s}\right\}$ *is diophantine over* K.

Proof. Let $x \in K$, and let $u = \frac{x^2+t^2+t}{x^2+t}$. Lemma 3.9 shows that an element $v \in K$ satisfying Equations (24) through (26) must be of the form $v = u^{4^k}$ for some $k \in \mathbb{N}$. So we have to show now that if $v = u^{4^k}$ for some $k \in \mathbb{N}$, then Equations (24) through (26) can be satisfied. The proof of this is almost identical to Corollary 3.6. □

Corollary 3.11. *The set* $T := \left\{(x,w) \in K^2 : \exists s \in \mathbb{N}, w = \left(\frac{x^2+t^2+t}{x^2+t}\right)^{2^s}\right\}$ *is diophantine over* K.

Proof. This follows from the fact that

$$(x,w) \in T \iff (x,w) \in T_1 \text{ or } \exists z \in K\,(z^2 = w \text{ and } (x,z) \in T_1).$$

□

Theorem 3.12. *The set* $\{(x,y) \in K^2 : \exists s \in \mathbb{N}, y = x^{2^s}\}$ *is diophantine over* K.

Proof. By Corollary 3.7, Corollary 3.11 and the remark after Theorem 3.1, the sets S, S', T, and T' are diophantine. Together with Theorem 3.1 this finishes the proof. □

4. Appendix.

In the appendix we give proofs for Proposition 4.3 and Lemma 4.4. Both were used in Lemma 3.9.

Lemma 4.1. *Let F/G be a finite extension of fields of positive characteristic p. Let $\alpha \in F$ be such that all the coefficients of its monic irreducible polynomial over G are in G^{p^2}. Then $\alpha \in F^{p^2}$.*

Proof. This is Lemma 2.1 in [**Shl00**] with p replaced by p^2, and the same proof works here. □

Corollary 4.2. *Let F/G be a finite separable extension of fields of positive characteristic p. Let $[F : G] = n$. Let $x \in F$ be such that $F = G(x)$, and such that for distinct $a_0, \dots, a_n \in G$, $\mathrm{N}_{F/G}(a_i^{p^2} - x) = y_i^{p^2}$ with $y_i \in G$. Then $x \in F^{p^2}$.*

Proof. This is very similar to Lemma 2.2 in [**Shl00**]. Let $H(T) = A_0+A_1T+\cdots+T^n$ be the irreducible polynomial of x over G. Then $H(a_i^{p^2}) = y_i^{p^2}$ for $i \in \{0,\dots,n\}$. This gives us the following linear system of equations:

$$\begin{pmatrix} 1 & a_0^{p^2} & \dots & a_0^{p^2(n-1)} & a_0^{p^2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & a_n^{p^2} & \dots & a_n^{p^2(n-1)} & a_n^{p^2n} \end{pmatrix} \begin{pmatrix} A_0 \\ \vdots \\ 1 \end{pmatrix} = \begin{pmatrix} y_0^{p^2} \\ \vdots \\ y_n^{p^2} \end{pmatrix}.$$

We can use Cramer's rule to solve the system and to conclude that $A_i \in G^{p^2}$ for all i. Then by the previous lemma, $x \in F^{p^2}$. □

Now we can apply the corollary to our situation:

Proposition 4.3. *Let $v \in \widetilde{K}$, and assume that for some distinct $a_0,\dots,a_n \in C$, the divisor of $v+a_i$ is of the form $\mathcal{D}_i^{p^2}$ for divisors $\mathcal{D}_i$ of $\widetilde{K}$, $i = 0,\dots,n$. Moreover, assume that for all i, $v + a_i$ does not have zeros or poles at any prime ramifying in the extension $\widetilde{K}/\widetilde{C}_K(t)$. Then $v \in \widetilde{K}^{p^2}$.*

Proof. This is almost the same as Lemma 2.9 in [**Shl00**]: First assume that $v \in \widetilde{C}_K(t)$. Since $v+a_i$ does not have any zeros or poles at primes ramifying in the extension $\widetilde{K}/\widetilde{C}_K(t)$, the divisor of $v + a_i$ in $\widetilde{C}_K(t)$ is of the form $\mathcal{E}_i^{p^2}$. In $\widetilde{C}_K(t)$ every divisor of degree zero is principal, so $v + a_i \in (\widetilde{C}_K(t))^{p^2}$ and hence $v \in (\widetilde{C}_K(t))^{p^2}$. Therefore $v \in \widetilde{K}^{p^2}$.

So now assume that $v \notin \widetilde{C}_K(t)$. From our assumption on $v + a_i$ it follows that in $\widetilde{C}_K(t, v)$ the divisor of $v + a_i$ is a p^2 power of another divisor. Since the divisor of $\mathrm{N}_{\widetilde{C}_K(t,v)/\widetilde{C}_K(t)}(v + a_i)$ is equal to the corresponding norm of the divisor of $(v+a_i)$, it follows that the divisor of the $\widetilde{C}_K(t, v)/\widetilde{C}_K(t)$ norm of $(v + a_i)$ is of the form $\mathcal{N}_i^{p^2}$, and hence $\mathrm{N}_{\widetilde{C}_K(t,v)/\widetilde{C}_K(t)}(v + a_i) \in (\widetilde{C}_K(t))^{p^2}$. Now apply Corollary 4.2 with $G = \widetilde{C}_K(t)$ and $F = \widetilde{C}_K(t, v)$. □

Lemma 4.4. *Let $\sigma, \mu \in K$. Assume that all the primes that are poles of σ or μ do not ramify in the extension $\widetilde{K}/\widetilde{C}_K(t)$. Moreover assume that*

$$t(\sigma^4 + \sigma) = \mu^4 + \mu. \tag{31}$$

Then $\sigma^4 + \sigma = \mu^4 + \mu = 0$.

Proof. Let $\mathcal{A}$, $\mathcal{B}$ be effective divisors of K, relatively prime to each other and to $\mathfrak{p}$ and $\mathfrak{q}$, such that the divisor of σ is of the form $\frac{\mathcal{A}}{\mathcal{B}}\mathfrak{p}^i\mathfrak{q}^k$, where i and k are integers.

Claim 1. For some effective divisor $\mathcal{C}$ relatively prime to $\mathcal{B}$, $\mathfrak{p}$ and $\mathfrak{q}$, some integers j, m, the divisor of μ is of the form $\frac{\mathcal{C}}{\mathcal{B}}\mathfrak{p}^j\mathfrak{q}^m$.

Proof of Claim 1. Let $\mathfrak{t}$ be a pole of μ such that $\mathfrak{t} \neq \mathfrak{p}$ and $\mathfrak{t} \neq \mathfrak{q}$. Then

$$0 > 4\,\mathrm{ord}_{\mathfrak{t}}\mu = \mathrm{ord}_{\mathfrak{t}}(\mu^4 + \mu) = \mathrm{ord}_{\mathfrak{t}}(t(\sigma^4 + \sigma)) = \mathrm{ord}_{\mathfrak{t}}(\sigma^4 + \sigma) = 4\,\mathrm{ord}_{\mathfrak{t}}\sigma.$$

Conversely, let $\mathfrak{t}$ be a pole of σ such that $\mathfrak{t} \neq \mathfrak{p}$ and $\mathfrak{t} \neq \mathfrak{q}$. Then

$$0 > 4\,\mathrm{ord}_{\mathfrak{t}}\sigma = \mathrm{ord}_{\mathfrak{t}}(\sigma^4 + \sigma) = \mathrm{ord}_{\mathfrak{t}}(t(\sigma^4 + \sigma)) = \mathrm{ord}_{\mathfrak{t}}(\mu^4 + \mu) = 4\,\mathrm{ord}_{\mathfrak{t}}\mu.$$

This proves the claim.

By the Strong Approximation Theorem there exists $b \in K^*$ such that the divisor of b is of the form $\frac{\mathcal{B}\mathcal{D}}{\mathfrak{q}^l}$, where $\mathcal{D}$ is an effective divisor relatively prime to $\mathcal{A}$, $\mathcal{C}$, $\mathfrak{p}$ and $\mathfrak{q}$ and l is a natural number.

Claim 2.

$$b\sigma = s_1 t^i \text{ and } b\mu = s_2 t^j,$$

where s_1, s_2 are integral over $C_K[t]$ and have zero divisors relatively prime to $\mathfrak{p}$ and $\mathcal{B}$.

Proof of Claim 2. The divisor of $b\sigma$ is

$$\frac{\mathcal{B}\mathcal{D}}{\mathfrak{q}^l}\frac{\mathcal{A}}{\mathcal{B}}\mathfrak{p}^i\mathfrak{q}^k = \mathcal{D}\mathcal{A}\mathfrak{p}^i\mathfrak{q}^{k-l} = (\mathcal{D}\mathcal{A}\mathfrak{q}^{k-l+i})\left(\frac{\mathfrak{p}^i}{\mathfrak{q}^i}\right).$$

Thus the divisor of $s_1 := b\sigma/t^i$ is of the form $\mathcal{D}\mathcal{A}\mathfrak{q}^{k-l+i}$. Therefore $\mathfrak{q}$ is the only pole of s_1, so s_1 is integral over $C_K[t]$. By construction $\mathcal{A}$ and $\mathcal{D}$ are relatively prime to $\mathfrak{p}$ and $\mathcal{B}$. A similar argument applies to $s_2 := b\mu/t^j$. This proves the claim.

Multiplying (31) by b^4 we obtain the following equation (using the claim):

$$t(s_1^4 t^{4i} + b^3 s_1 t^i) = s_2^4 t^{4j} + b^3 s_2 t^j. \tag{32}$$

Suppose $i < 0$. Then the left side of (32) has a pole of order $|4i+1|$ at $\mathfrak{p}$. This would imply that $j < 0$, and the right side has a pole of order $|4j|$ at $\mathfrak{p}$, contradiction. Thus we can assume that i, j are both nonnegative. We can rewrite (32) as

$$(s_1^4 t^{4i+1} + s_2^4 t^{4j}) = b^3(s_1 t^{i+1} + s_2 t^j).$$

Let $\mathfrak{t}$ be any prime factor of $\mathcal{B}$ in $\widetilde{K}$. Then $\mathfrak{t}$ does not ramify in the extension $\widetilde{K}/C_{\widetilde{K}}(t)$ by our assumption on σ. Also $\mathfrak{t}$ is not a pole of s_1, s_2 or t.

Thus

$$\mathrm{ord}_{\mathfrak{t}}(s_1^4 t^{4i+1} + s_2^4 t^{4j}) = \mathrm{ord}_{\mathfrak{t}}(b^3(s_1 t^{i+1} + s_2 t^j)) \geq 3.$$

We have

$$0 < \mathrm{ord}_{\mathfrak{t}}(d(s_1^4 t^{4i+1} + s_2^4 t^{4j})) = \mathrm{ord}_{\mathfrak{t}}(s_1^4\, d(t^{4i+1})) = \mathrm{ord}_{\mathfrak{t}}(s_1^4) + \mathrm{ord}_{\mathfrak{t}}(d(t^{4i+1})).$$

Since $\mathfrak{t}$ is unramified in the extension $\widetilde{K}/\widetilde{C}_K(t)$ and since $\mathfrak{t}$ is not a zero or a pole of t, $\mathrm{ord}_{\mathfrak{t}}(d(t^{4i+1})) = 0$. So s_1 has a zero at $\mathfrak{t}$. This, however, is impossible, because $\mathfrak{t}$ is a prime factor of $\mathcal{B}$, but the zero divisor of s_1 is relatively prime to $\mathcal{B}$. So $\mathcal{B}$ must be the trivial divisor. This implies that in (31) all the functions are integral over $C_K[t]$, i.e., they can have poles at $\mathfrak{q}$ only. So if μ is not constant, it must have a pole at $\mathfrak{q}$. But then the left side of (31) has a pole at $\mathfrak{q}$ of odd order, while the right side of (31) has a pole at $\mathfrak{q}$ of even order, which is a contradiction.

Thus μ must be a constant. But if a function $h \in K$ is integral over $C_K[t]$, and $t \cdot h$ is constant, then $h = 0$. Thus $\sigma^4 + \sigma = 0$. Then $\mu^4 + \mu = 0$ also. □

Remark. A. Shlapentokh informed the author by email on March 31, 2003, that she has an argument in her paper [Compositio Math., 132 (2002), pp. 99-120] that reduces the case of finite transcendence degree to transcendence degree 1. Together with the result in this paper this implies that Hilbert's Tenth Problem is undecidable for function fields F of characteristic 2, finitely generated over a field C that is algebraic over a finite field, and such that C has an extension of degree 2.

References

[Den78] J. Denef, *The Diophantine problem for polynomial rings and fields of rational functions*, Trans. Amer. Math. Soc., **242**(1978), 391-399, MR 58 #10809, Zbl 0399.10048.

[Den79] ______, *The Diophantine problem for polynomial rings of positive characteristic* in 'Logic Colloquium '78 (Mons, 1978)', 131-145, North-Holland, Amsterdam, 1979, MR 81h:03090, Zbl 0457.12011.

[Den80] ______, *Diophantine sets over algebraic integer rings*, II, Trans. Amer. Math. Soc., **257**(**1**) (1980), 227-236, MR 81b:12031, Zbl 0426.12009.

[DL78] J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, J. London Math. Soc. (2), **18**(**3**) (1978), 385-391, MR 80a:12030, Zbl 0399.10049.

[Deu73] M. Deuring, *Lectures on the Theory of Algebraic Functions of One Variable*, Lecture Notes in Mathematics, **314**, Springer-Verlag, Berlin, 1973, MR 49 #8970, Zbl 0249.14008.

[FJ86] M.D. Fried and M. Jarden, *Field Arithmetic*, Springer-Verlag, Berlin, 1986, MR 89b:12010, Zbl 0625.12001.

[KR92a] K.H. Kim and F.W. Roush, *Diophantine undecidability of* $C(t_1, t_2)$, J. Algebra, **150**(**1**) (1992), 35-44, MR 93h:03062, Zbl 0754.11039.

[KR92b] ______, *Diophantine unsolvability for function fields over certain infinite fields of characteristic p*, J. Algebra, **152**(**1**) (1992), 230-239, MR 93k:11114, Zbl 0768.12008.

[Lan93] S. Lang, *Algebra*, Springer-Verlag, New York, third edition, 1993, CMP 1 878 556, Zbl 0848.13001.

[Mas84] R.C. Mason, *Diophantine Equations over Function Fields*, Cambridge University Press, Cambridge, 1984, MR 86b:11026, Zbl 0533.10012.

[Mat70] Ju.V. Matijasevič, *The Diophantineness of enumerable sets*, Dokl. Akad. Nauk SSSR, **191** (1970), 279-282, MR 41 #3390.

[Phe87] T. Pheidas, *An undecidability result for power series rings of positive characteristic*, II, Proc. Amer. Math. Soc., **100**(**3**) (1987), 526-530, MR 89c:03075, Zbl 0664.03008.

[Phe91] ______, *Hilbert's tenth problem for fields of rational functions over finite fields*, Invent. Math., **103**(**1**) (1991), 1-8, MR 92e:11145, Zbl 0696.12022.

[Shl96] A. Shlapentokh, *Diophantine undecidability over algebraic function fields over finite fields of constants*, J. Number Theory, **58**(**2**) (1996), 317-342, MR 97d:12010, Zbl 0856.11058.

[Shl00] ______, *Hilbert's tenth problem for algebraic function fields over infinite fields of constants of positive characteristic*, Pacific J. Math., **193**(**2**) (2000), 463-500, MR 2001e:12008.

[Vid94] C.R. Videla, *Hilbert's tenth problem for rational function fields in characteristic* 2, Proc. Amer. Math. Soc., **120**(**1**) (1994), 249-253, MR 94b:11122, Zbl 0795.03015.

Received July 1, 2002 and revised September 11, 2002.

Department of Mathematics
University of California
Berkeley, CA 94720
E-mail address: eisentra@math.berkeley.edu