Hilbert’s Tenth Problem over Holomorphy Rings of Function Fields of Characteristic 0

Alexandra Shlapentokh

East Carolina University

October 2009
# Table of Contents

1. The Original Problem
2. Function Fields and Holomorphy Rings
3. The Main Results
4. What do we know about HTP over Function Fields of Characteristic 0?
5. Proving Undecidability over Function Fields Using a Definition of Order
6. Proving Undecidability over Holomorphy Rings
Outline

1. The Original Problem
2. Function Fields and Holomorphy Rings
3. The Main Results
4. What do we know about HTP over Function Fields of Characteristic 0?
5. Proving Undecidability over Function Fields Using a Definition of Order
6. Proving Undecidability over Holomorphy Rings
Hilbert’s Tenth Problem over Holomorphy Rings of Function Fields of Characteristic 0

The Original Problem

Hilbert’s Question About Polynomial Equations

Is there an algorithm which can determine whether or not an arbitrary polynomial equation in several variables has solutions in integers?

This problem became known as Hilbert’s Tenth Problem
This question was answered negatively (with the final piece in place in 1970) in the work of Martin Davis, Hilary Putnam, Julia Robinson and Yuri Matijasevich.
A General Question

A Question About an Arbitrary Recursive Ring $R$

Is there an algorithm, which if given an arbitrary polynomial equation in several variables with coefficients in $R$, can determine whether this equation has solutions in $R$?
A General Question

A Question About an Arbitrary Recursive Ring $R$

Is there an algorithm, which if given an arbitrary polynomial equation in several variables with coefficients in $R$, can determine whether this equation has solutions in $R$?

In this talk we concentrate on the case when $R$ is a function field of characteristic 0 or a subring of such a field.
Lemma (Replacing Finitely Many by One)

Let $R$ be any ring such that its fraction field $K$ is not algebraically closed. In this case, any finite system of equations over $R$ can be effectively replaced by a single polynomial equation over $R$ with the identical $R$-solution set.
One vs. Finitely Many

Lemma (Replacing Finitely Many by One)

Let $R$ be any ring such that its fraction field $K$ is not algebraically closed. In this case, any finite system of equations over $R$ can be effectively replaced by a single polynomial equation over $R$ with the identical $R$-solution set.

Proof.

It is enough to consider the case of two equations: $f(x_1, \ldots, x_n) = 0$ and $g(x_1, \ldots, x_n) = 0$. If $h(x) = \sum_{i=0}^{k} a_i x^i$ is a polynomial over $R$ without any roots in $K$, then

$$t(x_1, \ldots, x_n) = \sum_{i=0}^{k} a_i f^i(x_1, \ldots, x_n) g^{k-i}(x_1, \ldots, x_n) = 0$$

(1)

has solutions in $K$ if and only if both $f(x_1, \ldots, x_n) = 0$ and $g(x_1, \ldots, x_n) = 0$ have solutions in $K$. \qed
Outline

1 The Original Problem

2 Function Fields and Holomorphy Rings

3 The Main Results

4 What do we know about HTP over Function Fields of Characteristic 0?

5 Proving Undecidability over Function Fields Using a Definition of Order

6 Proving Undecidability over Holomorphy Rings
Some definitions

**Definition (Function Fields)**

Let $C$ be a field and let $t_1, \ldots, t_k$ be algebraically independent over $C$. Let $K$ be a finite extension of $C(t_1, \ldots, t_k)$. Let $C_K$ be the algebraic closure of $C$ in $K$. Under these assumptions $K$ is called a function field in $k$ variables over a constant field $C_K$. 
Some definitions

**Definition (Function Fields)**

Let $C$ be a field and let $t_1, \ldots, t_k$ be algebraically independent over $C$. Let $K$ be a finite extension of $C(t_1, \ldots, t_k)$. Let $C_K$ be the algebraic closure of $C$ in $K$. Under these assumptions $K$ is called a function field in $k$ variables over a constant field $C_K$.

**Definition (Holomorphy Ring)**

Let $K$ be a one variable function field. Let $\mathcal{W}$ be a set of primes of $K$. Then let

$$O_{K, \mathcal{W}} = \{ x \in K : \text{ord}_p x \geq 0 \forall p \notin \mathcal{W} \}$$
Diophantine Sets and Definitions

Definition (Diophantine Sets)

If \( R \) is a ring, \( k \in \mathbb{Z}_{>0} \), and \( A \subset R^k \), then we say that \( A \) is Diophantine over \( R \) (or existentially definable over \( R \) in the language of rings) if there exists

\[
f(t_1, \ldots, t_k, x_1, \ldots, x_m) \in R[t_1, \ldots, t_k, x_1, \ldots, x_m]
\]

such that for any element \((t_1, \ldots, t_k) \in R^k\) we have that

\[
\exists x_1, \ldots, x_m \in R : f(t_1, \ldots, t_k, x_1, \ldots, x_m) = 0
\]

\(\Leftrightarrow\)

\((t_1, \ldots, t_k) \in A.\)

In this case we call \( f(t_1, \ldots, t_k, x_1, \ldots, x_m) \) a Diophantine definition of \( A \) over \( R \).
Some Properties of Diophantine Sets

Proposition

- We can allow Diophantine definitions to consist of several variables without changing the nature of the relation. (Follows from “One=Finitely Many”.)
Some Properties of Diophantine Sets

Proposition

- We can allow Diophantine definitions to consist of several variables without changing the nature of the relation. (Follows from “One=Finitely Many”.)

- Finite Intersections of Diophantine sets are Diophantine. (Follows from “One=Finitely Many”.)
Proposition

- We can allow Diophantine definitions to consist of several variables without changing the nature of the relation. (Follows from “One=Finitely Many”.)

- Finite Intersections of Diophantine sets are Diophantine. (Follows from “One=Finitely Many”.)

- Finite unions of Diophantine sets are Diophantine. (Product of Diophantine definitions is a Diophantine definition of the union.)
Proposition

If \( R \) is a holomorphy subring of any function field of characteristic 0, then the set of non-zero elements of \( R \) is Diophantine over \( R \).
Indeed, let $R$ be a holomorphy subring of a function field $K$ and suppose we know how to determine whether solutions exist over $R$. If $Q(x_1, \ldots, x_k)$ is a polynomial with coefficients in $R$, then

$$\exists x_1, \ldots, x_k \in K : Q(x_1, \ldots, x_k) = 0$$

$$\uparrow$$

$$\exists y_1, \ldots, y_k, z_1, \ldots, z_k \in R : Q\left(\frac{y_1}{z_1}, \ldots, \frac{y_k}{z_k}\right) = 0 \land z_1 \ldots z_k \neq 0.$$ 

So decidability of HTP over $R$ would imply the decidability of HTP over $K$. 
Outline

1 The Original Problem

2 Function Fields and Holomorphy Rings

3 The Main Results

4 What do we know about HTP over Function Fields of Characteristic 0?

5 Proving Undecidability over Function Fields Using a Definition of Order

6 Proving Undecidability over Holomorphy Rings
The Main Result

**Theorem (Countable Case)**

If $K$ is a countable recursive one variable function field of characteristic 0, then Hilbert’s Tenth Problem is not solvable over any holomorphy ring of $K$ not equal to the whole field.

(Moret-Bailly, S. 2009)
The Main Result

Theorem (Countable Case)

If $K$ is a countable recursive one variable function field of characteristic 0, then Hilbert’s Tenth Problem is not solvable over any holomorphy ring of $K$ not equal to the whole field. (Moret-Bailly, S. 2009)

Theorem (Uncountable Case)

If $K$ is a one variable function field of characteristic 0 over a field of constants $C$, then for any holomorphy ring of $K$ not equal to the whole field, there exist elements $x_1, \ldots, x_n \in K \setminus C$ such that there is no algorithm to tell whether a polynomial equation with coefficients in $\mathbb{Q}(x_1, \ldots, x_n)$ has solutions in the ring. (Moret-Bailly, S. 2009)
Outline

1. The Original Problem
2. Function Fields and Holomorphy Rings
3. The Main Results
4. What do we know about HTP over Function Fields of Characteristic 0?
5. Proving Undecidability over Function Fields Using a Definition of Order
6. Proving Undecidability over Holomorphy Rings
Field Results

Definition (Formally Real Field)

A field is called formally real if $-1$ is not a sum of squares.
What do we know about HTP over Function Fields of Characteristic 0?

Field Results

**Definition (Formally Real Field)**

A field is called **formally real** if $-1$ is not a sum of squares.

**Theorem**

HTP is unsolvable over function fields of the following types:

- Over constant fields which are formally real or are subfields of a finite extension of $\mathbb{Q}_p$ for some rational prime $p$. (Denef 1978, Kim and Roush 1995, Moret-Bailly 2006, Eisenträger 2007)

Remark

If the field is uncountable we have to adjust the statement of the problem.
Field Results

Definition (Formally Real Field)

A field is called formally real if $-1$ is not a sum of squares.

Theorem

HTP is unsolvable over function fields of the following types:

- Over constant fields which are formally real or are subfields of a finite extension of $\mathbb{Q}_p$ for some rational prime $p$. (Denef 1978, Kim and Roush 1995, Moret-Bailly 2006, Eisenträger 2007)

- Over $\mathbb{C}$ and of transcendence degree at least 2. (Kim and Roush 1992, Eisenträger 2004)
Field Results

**Definition (Formally Real Field)**
A field is called formally real if \(-1\) is not a sum of squares.

**Theorem**
HTP is unsolvable over function fields of the following types:

- Over constant fields which are formally real or are subfields of a finite extension of \(\mathbb{Q}_p\) for some rational prime \(p\). (Denef 1978, Kim and Roush 1995, Moret-Bailly 2006, Eisenträger 2007)

- Over \(\mathbb{C}\) and of transcendence degree at least 2. (Kim and Roush 1992, Eisenträger 2004)

**Remark**
If the field is uncountable we have to adjust the statement of the problem.
Hilbert’s Tenth Problem over Holomorphy Rings of Function Fields of Characteristic 0
Proving Undecidability over Function Fields Using a Definition of Order

Outline

1. The Original Problem
2. Function Fields and Holomorphy Rings
3. The Main Results
4. What do we know about HTP over Function Fields of Characteristic 0?
5. Proving Undecidability over Function Fields Using a Definition of Order
6. Proving Undecidability over Holomorphy Rings
Let $R$ be any holomorphy subring of $K$, including the case of $R = K$. Assume there exists a subset $Z \subset R$ satisfying the following conditions:

- $\mathbb{Z} \in Z$
Proposition

Let $R$ be any holomorphy subring of $K$, including the case of $R = K$. Assume there exists a subset $Z \subset R$ satisfying the following conditions:

- $\mathbb{Z} \in Z$

- There exists a prime $\mathfrak{p}$ of $K$ such that for all $x \in Z$ there exists $m \in \mathbb{Z}$ such that $\text{ord}_\mathfrak{p}(x - m) > 0$. 
A Special Set

Proposition

Let $R$ be any holomorphy subring of $K$, including the case of $R = K$. Assume there exists a subset $Z \subseteq R$ satisfying the following conditions:

- $\mathbb{Z} \in Z$
- There exists a prime $\mathfrak{p}$ of $K$ such that for all $x \in Z$ there exists $m \in \mathbb{Z}$ such that $\text{ord}_\mathfrak{p}(x - m) > 0$.
- $Z$ is Diophantine over $K$.

In this case HTP is undecidable over $R$. 
**Proof.**

Let

$$Q(x_1, \ldots, x_k) = 0$$  \hspace{0.5cm} (2)

be a polynomial equation over $\mathbb{Z}$ and consider the following system of equations:

$$\begin{cases} 
Q(x_1, \ldots, x_k) = 0, \\
x_1 \in \mathbb{Z}, \\
\ldots, \\
x_k \in \mathbb{Z}.
\end{cases} \hspace{0.5cm} (3)$$

We claim that (2) has solutions in $\mathbb{Z}$ if and only if (3) has solutions in $K$. Indeed, if (2) has solutions in $\mathbb{Z}$, then clearly (3) has solutions in $K$. At the same time if (3) has solutions $(a_1, \ldots, a_k)$ in $K$, then for some $(m_1, \ldots, m_k) \in \mathbb{Z}$ we have that $\text{ord}_p(Q(a_1, \ldots, a_k) - Q(m_1, \ldots, m_k)) > 0$ and therefore $\text{ord}_p(Q(m_1, \ldots, m_k)) > 0$ implying $Q(m_1, \ldots, m_k) = 0$ since $Q(m_1, \ldots, m_k) \in \mathbb{Q}$. 

\[\square\]
Constructing $\mathbb{Z}$.

The Main Tools

- An elliptic curve of rank 1
- Diophantine definability of the valuation ring of a prime of the field:

$$O_p = \{ y \in K : \text{ord}_p y \geq 0 \}$$
Let $K$ be a function field of characteristic 0 over a field of constants $C$. Let $\mathfrak{p}$ be a degree one prime of $K$. Let $\mathfrak{D}$ be a divisor of $K$ such that $\text{ord}_q \mathfrak{D} \in \{0, 1\}$ for any prime $q$ of $K$, $\text{ord}_\mathfrak{p} \mathfrak{D} = 0$, and the degree of $\mathfrak{D}$ is at least $2g_K + 2$, where $g_K$ is the genus of $K$. Let $F(T)$ be a nonsingular cubic polynomial over $\mathbb{Q}$ such that the elliptic curve $Y^2 = F(X)$ has no complex multiplication. Then there exists an $x \in K$ such that its pole divisor is $\mathfrak{D}$, $\text{ord}_\mathfrak{p} x > 0$, and the elliptic curve $E_x$ defined by the equation

$$F\left(\frac{1}{x}\right) Y^2 = F(X)$$

has the property that $E_x(C(x)) = E_x(K)$. Also $E_x(C(x))$ is of rank 1 generated by the point with affine coordinates $(\frac{1}{x}, 1) \in E(C(x)) \setminus E(C)$ modulo 2-torsion.
Properties of the Generator

**Notation**

Let $P$ be the point on the elliptic curve $E_x$ with the affine coordinates $(\frac{1}{x}, 1)$. For $n \in \mathbb{Z} \neq 0$ let $P_n$ be the $n$-th multiple of $P$ and let $(x_n, y_n)$ be the affine coordinates of $P_n$.

**Lemma**

For any $n \in \mathbb{Z} \neq 0$ we have that $\text{ord}_p(x_n y_n - n) > 0$.

**Lemma**

The set $E^{\text{even}} = \{(x_{2n}, y_{2n}), n \in \mathbb{Z} \neq 0\}$ is Diophantine over $K$. 
Constructing the Set $Z$ Using a Definition of Order

**Definition of $Z$**

A $K$-element $z$ belongs to $Z$ if and only if one of the following conditions is satisfied

$$z = 0$$

$$\exists (a, b) \in E \text{ even } \land \text{ord}_p (2z - x a b) > 0$$
Constructing the Set $\mathbb{Z}$ Using a Definition of Order

**Definition of $\mathbb{Z}$**

A $K$-element $z$ belongs to $\mathbb{Z}$ if and only if one of the following conditions is satisfied

- $z = 0$
Constructing the Set $Z$ Using a Definition of Order

**Definition of $Z$**

A $K$-element $z$ belongs to $Z$ if and only if one of the following conditions is satisfied

- $z = 0$
- $\exists (a, b) \in E^{even} \land \text{ord}_p(2z - x \frac{a}{b}) > 0$
Constructing the Set $Z$ Using a Definition of Order

**Definition of $Z$**

A $K$-element $z$ belongs to $Z$ if and only if one of the following conditions is satisfied

- $z = 0$
- $\exists (a, b) \in E^{even} \land \text{ord}_p(2z - xa/b) > 0$

**Proposition**

*If the set $0_p = \{ x \in K : \text{ord}_p x \geq 0 \}$ is Diophantine over $K$, then $Z$ is Diophantine over $K.*
Outline

1. The Original Problem
2. Function Fields and Holomorphy Rings
3. The Main Results
4. What do we know about HTP over Function Fields of Characteristic 0?
5. Proving Undecidability over Function Fields Using a Definition of Order
6. Proving Undecidability over Holomorphy Rings
Divisibility by $x$ and Definition of Order over a Ring

**Proposition**

Let $R = O_{K,W}$, where $p \not\in W$ and $x \in O_{K,W}$. By assumption $\text{ord}_p x > 0$ and for any $w \in R \cap C(x)$ we have that

$$\text{ord}_p w > 0 \iff \frac{w}{x} \in R.$$ 

Thus we have a Diophantine definition of a set $\hat{O}_p \supseteq O_p \cap C(x)$ over $R$. 

Divisibility by $x$ and Definition of Order over a Ring

Proposition

Let $R = O_{K,W}$, where $\mathfrak{p} \notin W$ and $x \in O_{K,W}$. By assumption $\text{ord}_x x > 0$ and for any $w \in R \cap C(x)$ we have that

$$\text{ord}_x w > 0 \iff \frac{w}{x} \in R.$$

Thus we have a Diophantine definition of a set $\hat{O}_p \supseteq O_p \cap C(x)$ over $R$.

Proof.

The right to left direction is obvious. Further, if $\mathfrak{p}$ is the prime below $\mathfrak{p}$ in $C(x)$, then for any $w \in C(x)$ we have that $\text{ord}_x w = e(\mathfrak{p}/\mathfrak{p}') \text{ord}_{\mathfrak{p}'} w$. Thus, $\text{ord}_x w > 0$ if and only if $\text{ord}_{\mathfrak{p}'} w > 0$. Further $\text{ord}_{\mathfrak{p}'} x = 1$ implying that $\frac{w}{x} \in R \cap C(x)$.
Remark

If $K = C(x)$ then $\hat{O}_p = O_p$ or in other words we can define the order at $p$. 
Relative Primality over $R$

**Definition**

Let $a, b \in R$ and assume that for any $q \not\in \mathcal{W}$ we have that $\text{ord}_q a > 0 \Rightarrow \text{ord}_q b = 0$. In this case we say that $a$ is relatively prime to $b$ in $R$ and write $(a, b)_R = 1$. 


Relative Primality over $R$

**Definition**

Let $a, b \in R$ and assume that for any $q \notin \mathcal{W}$ we have that $\text{ord}_q a > 0 \Rightarrow \text{ord}_q b = 0$. In this case we say that $a$ is relatively prime to $b$ in $R$ and write $(a, b)_R = 1$.

**Lemma**

For $a, b \in R \setminus \{0\}$ we have that $(a, b)_R = 1$ is equivalent to the existence of $A, B \in R$ such that $Aa + Bb = 1$. (In other words the set of all relatively prime pairs of $R$ is Diophantine over $R$.)
Observe that the set

\[ E^{\text{even}} = \{(a_1, a_2, b_1, b_2) \in R^4 : x_{2n} = \frac{a_1}{a_2}, y_{2n} = \frac{b_1}{b_2}\}, \]

where \( x_{2n}, y_{2n} \in K \), \([2n]P = (x_{2n}, y_{2n}) \), \( n \in \mathbb{Z} \neq 0 \) is Diophantine over \( R \), and we can represent non-zero even multiples of \( P \) by equivalence classes of quadruples of elements of \( R \).
Representing Elliptic Curve Points over a Ring

### Elliptic Points as Equivalence Classes of Quadruples

Observe that the set

$$E^{even} = \{(a_1, a_2, b_1, b_2) \in R^4 : x_{2n} = \frac{a_1}{a_2}, y_{2n} = \frac{b_1}{b_2}\},$$

where $x_{2n}, y_{2n} \in K$, $[2n]P = (x_{2n}, y_{2n})$, $n \in \mathbb{Z} \neq 0$ is Diophantine over $R$, and we can represent non-zero even multiples of $P$ by equivalence classes of quadruples of elements of $R$.

### Representing $x^{\frac{x_n}{y_n}}$ over $R$

Note that $\text{ord}_p x^{\frac{x_n}{y_n}} = 0$ and therefore, for any $n \in \mathbb{Z} \neq 0$ we have that $x^{\frac{x_n}{y_n}} = \frac{a}{b}$, where $a, b \in R$ and $\text{ord}_p b = 0$. In fact, since $x, x_n, y_n \in C(x)$, we can require $(a, b)_R = 1$. The relative primeness condition will insure that $\text{ord}_p b = 0$ since $\text{ord}_p (x^{\frac{x_n}{y_n}}) = \text{ord}_p \frac{a}{b} = 0$.

Further the set $F$ defined by:

$$\{(a, b) \in R^2 | (a, b)_R = 1 \land \exists (a_1, a_2, b_1, b_2) \in E^{even} : x \frac{a_1 b_2}{a_2 b_1} = \frac{a}{b}\}$$

is also Diophantine over $R$. 
Defining a set $Z$ over $R$

**Definition of $Z$**

An $R$-element $z$ belongs to $Z$ if and only if one of the following conditions is satisfied
Defining a set \( Z \) over \( R \)

**Definition of \( Z \)**

An \( R \)-element \( z \) belongs to \( Z \) if and only if one of the following conditions is satisfied

- \( z = 0 \)
Defining a set $Z$ over $R$

**Definition of $Z$**

An $R$-element $z$ belongs to $Z$ if and only if one of the following conditions is satisfied

- $z = 0$
- $\exists (a, b) \in F, w \in R : (2zb - a) = xw$
Proving Undecidability over Holomorphy Rings

**Defining a set \( Z \) over \( R \)**

**Proof.**

Suppose we have \( (2zb - a) = xw \). Since, \( \text{ord}_p x > 0 \) we must have \( \text{ord}_p (2zb - a) > 0 \). Further

\[
\text{ord}_p b = 0 \Rightarrow \text{ord}_p \left( 2z - \frac{a}{b} \right) = \text{ord}_p \left( 2z - x \frac{x_{2n}}{y_{2n}} \right) > 0
\]

for some \( n \in \mathbb{Z}_{\neq 0} \), implying \( \text{ord}_p (z - n) > 0 \).

Next suppose \( z = n \in \mathbb{Z}_{\neq 0} \) and conclude that \( \text{ord}_p (2z - x \frac{x_{2n}}{y_{2n}}) > 0 \).

Further, there exists \( (a, b) \in F \cap C(x) \) such that \( \frac{a}{b} = x \frac{x_{2n}}{y_{2n}} \), implying \( \text{ord}_p (2z - \frac{a}{b}) > 0 \). Since \( 2z - \frac{a}{b} \in C(x) \), we actually have \( \text{ord}_p (2z - \frac{a}{b}) > 0 \) and therefore \( \text{ord}_p (2zb - a) > 0 \) leading to \( x \mid_R (2zb - a) \).
A Few Remaining Matters

Moret-Bailly uses an element $x$ such that

- it has a zero at a degree 1 prime,
- all the poles are simple,
- the degree of its pole divisor is large enough relative to the genus of the field.

We need $x \in R = O_{K,W}$ with at least one zero not in $W$. Thus we need a degree one prime $p \notin W$, and $W$ must be large enough relative to the genus of $K$. If the complement of $W$ does not have any degree one primes, we always can extend the constant field so that some prime not in $W$ has a factor of degree one, and work in the integral closure of our original ring in the extension.

If $W$ is infinite, then we can always find enough primes to serve as poles of $x$, and the case of a finite $W$ was handled in a 1992 paper using Pell equations.