HTP in Positive Characteristic

Alexandra Shlapentokh

East Carolina University

October 2007
Table of Contents

1 A Brief History of Diophantine Undecidability over Number Fields
   ■ The Original Problem
   ■ Extensions to Number Fields

2 How Things are Done
   ■ Diophantine Sets, Definitions and Models
   ■ HTP over a Field vs. HTP over a Subring

3 A Brief History of HTP over Function Fields of Characteristic 0
   ■ Some Definitions
   ■ Field Results
   ■ Ring Results

4 HTP over Function Fields of Positive Characteristic
   ■ A Longer History of Diophantine Undecidability for Function Fields of Positive Characteristic
   ■ Multiplication through Addition and Divisibility
   ■ $p$-th Powers over a Function Field
   ■ Defining Order at a Prime

5 Back to the First-Order Theory
   ■ A Short History of First-Order Decidability over Function Fields of Positive Characteristic
   ■ $P$-th Powers are Enough
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 $R$?

Arguably, the most important open problems in the area concern the Diophantine status of the ring of integers of an arbitrary number field and the Diophantine status of $\mathbb{Q}$. 
Review: Number Fields and Their Ring of Integers

**Definition (Number Fields)**

Let $K \subset \mathbb{C}$ be a finite extension of $\mathbb{Q}$. Then we will call $K$ a number field.

**Definition (Totally Real Fields)**

A number field is called totally real if for any embedding $\sigma : K \rightarrow \mathbb{C}$ we have that $\sigma(K) \subset \mathbb{R}$.

**Definition (The Ring of Integers of a Number Field)**

Let $K$ be a number field and let $O_K$ be the integral closure of $\mathbb{Z}$ inside $K$. Then $O_K$ is called the ring of integers of $K$. Alternatively, the integers of $K$ are elements of $K$ satisfying monic irreducible polynomials over $\mathbb{Z}$.
The Rings of Integers of Number Fields.

Theorem

HTP is unsolvable over the rings of integers of the following fields:

- Extensions of degree 4, totally real number fields and their extensions of degree 2. (Denef, 1980 & Denef, Lipshitz, 1978)
  Note that these fields include all Abelian extensions.
- Number fields with exactly one pair of non-real embeddings (Pheidas, S. 1988)
- Any number field $K$ such that there exists an elliptic curve $E$ of positive rank defined over $\mathbb{Q}$ with $[E(K) : E(\mathbb{Q})] < \infty$. (Poonen, S. 2003)
- Any number field $K$ such that there exists an elliptic curve of rank 1 over $K$ and an Abelian variety over $\mathbb{Q}$ keeping its rank over $K$. (Cornelissen, Pheidas, Zahidi, 2005)
The Rings between $\mathbb{Z}$ and $\mathbb{Q}$

A Ring in between

Let $S$ be a set of (non-archimedean) primes of $\mathbb{Q}$. Let $O_{\mathbb{Q},S}$ be the following subring of $\mathbb{Q}$.

$$\left\{ \frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0, n \text{ is divisible by primes of } S \text{ only} \right\}$$

If $S = \emptyset$, then $O_{\mathbb{Q},S} = \mathbb{Z}$. If $S$ contains all the primes of $\mathbb{Q}$, then $O_{\mathbb{Q},S} = \mathbb{Q}$. If $S$ is finite, we call the ring **small**. If $S$ is infinite, we call the ring **large**.
Examples of Big and Small Rings

**Example of a Small Ring**

\[
\left\{ \frac{m}{3^a5^b} : m \in \mathbb{Z}, a, b \in \mathbb{Z}_{>0} \right\}
\]

**Example of a Big Ring**

\[
\left\{ \prod p_i^{a_i} : m \in \mathbb{Z}, a_i \in \mathbb{Z}_{>0}, p_i \equiv 1 \mod 3 \right\}
\]
Review: Primes and Order at a Prime

**Definition (Primes of Number Fields)**
A prime of a number field is a prime ideal of the ring of integers of the field or, alternatively, a non-archimedean valuation of a field.

**Definition (Order at a Prime)**
Let \( x \in O_K, x \neq 0 \) and let \( p \) be a prime of \( K \) (a prime ideal of \( O_K \)). Then there exists a number \( n \in \mathbb{Z}_{\geq 0} \) such that \( x \in p^n \) but \( x \notin p^{n+1} \). Then \( n \) is called the order of \( x \) at \( p \) and we write \( \text{ord}_p x = n \).

Let \( y \in K, y \neq 0 \) and write \( y = \frac{x_1}{x_2} \) for some \( x_1, x_2 \in O_K \). Then we define \( \text{ord}_p y = \text{ord}_p x_1 - \text{ord}_p x_2 \). We also set \( \text{ord}_p 0 = \infty \).

**Example**
If \( K = \mathbb{Q} \), \( p = 3 \) and \( y = \frac{25}{9} \), then \( \text{ord}_p y = -2 \).
The Rings in between the Ring of Integers and a Number Field

A Ring in the Middle of a Number Field $K$

Let $\mathcal{V}$ be a set of primes of a number field $K$. Then define

$$O_{K,\mathcal{V}} = \{x \in K : \text{ord}_p x \geq 0 \ \forall p \not\in \mathcal{V}\}.$$  

If $\mathcal{V} = \emptyset$, then $O_{K,\mathcal{V}} = O_K$ – the ring of integers of $K$. If $\mathcal{V}$ contains all the primes of $K$, then $O_{K,\mathcal{V}} = K$. If $\mathcal{V}$ is finite, we call the ring small. If $\mathcal{V}$ is infinite, we call the ring big or large.
Theorem

*HTP is unsolvable over small subrings of \( \mathbb{Q} \).*

Theorem

*For any number field \( K \), if HTP is unsolvable over \( O_K \), then HTP is unsolvable over any small subring of \( K \).*

(Julia Robinson and others)
**Theorem**

Let $K$ be a number field satisfying one of the following conditions:

- $K$ is a totally real field.
- $K$ is an extension of degree 2 of a totally real field.
- There exists or an elliptic curve $E$ defined over $\mathbb{Q}$ such that $[E(K) : E(\mathbb{Q})] < \infty$.

Let $\varepsilon > 0$ be given. Then there exists a set $S$ of non-archimedean primes of $K$ such that

- The natural density of $S$ is greater than $1 - \frac{1}{[K : \mathbb{Q}]} - \varepsilon$.
- HTP is unsolvable over $O_{K,S}$.

Theorem

Let $K$ be a number field with a rank one elliptic curve. Then there exist recursive sets of $K$-primes $T_1$ and $T_2$, both of natural density zero and with an empty intersection, such that for any set $S$ of primes of $K$ containing $T_1$ and avoiding $T_2$, Hilbert’s Tenth Problem is unsolvable over $O_{K,S}$. (Poonen 2003: the case of $K = \mathbb{Q}$; Poonen, S. 2005: the general case)
Let $R$ be an integral domain. Then a subset $A \subset R^m$ is called Diophantine over $R$ if there exists a polynomial $p(T_1, \ldots, T_m, X_1, \ldots, X_k)$ with coefficients in $R$ such that for any $m$-tuple $(t_1, \ldots, t_m) \in R^m$ we have that

$$\exists x_1, \ldots, x_k \in R : p(t_1, \ldots, t_m, x_1, \ldots, x_k) = 0$$

$$\updownarrow$$

$$(t_1, \ldots, t_m) \in A.$$

In this case we call $p(T_1, \ldots, T_m, X_1, \ldots, X_k)$ a Diophantine definition of $A$ over $R$. 

Diophantine Sets

Other Descriptions

Diophantine sets can also described as projections of algebraic sets or sets existentially definable in the language of rings.
Diophantine Subsets of $\mathbb{Z}$

**MDRP Theorem**

The recursively enumerable subsets of $\mathbb{Z}$ are the same as the Diophantine subsets of $\mathbb{Z}$.

**Corollary**

There are undecidable Diophantine subsets of $\mathbb{Z}$.
Suppose $A \subset \mathbb{Z}$ is an undecidable Diophantine set with a Diophantine definition $P(T, X_1, \ldots, X_k)$. Assume also that we have an algorithm to determine existence of integer solutions for polynomials. Now, let $a \in \mathbb{Z}_{>0}$ and observe that $a \in A$ iff $P(a, X_1, \ldots, X_k) = 0$ has solutions in $\mathbb{Z}^k$. So if can answer Hilbert’s question effectively, we can determine the membership in $A$ effectively.
Diophantine Models

**Definition**

Let $R_1, R_2$ be two recursive rings and let $\phi : R_1 \longrightarrow R_2^m, m \in \mathbb{Z}_{>0}$ be an injective recursive map sending Diophantine sets of $R_1^k, k \in \mathbb{Z}_{>0}$ to Diophantine sets of $R_2^{k+m}$. Then $\phi$ is called a Diophantine model of $R_1$ over $R_2$.

**Remark**

If $R_1 \subset R_2$ and $\phi$ is the inclusion map, then $R_1$ has a Diophantine definition over $R_2$. Conversely, if $R_1$ has a Diophantine definition over $R_2$, then $R_2$ has a Diophantine model of $R_1$ with $\phi$ being the inclusion map.
**Proposition**

Suppose $R_1$ has undecidable Diophantine sets and $R_2$ has a Diophantine model of $R_1$. Then $R_2$ also has undecidable Diophantine sets.

**Corollary**

If $R$ is a countable ring with a Diophantine model of $\mathbb{Z}$, then $R$ has undecidable Diophantine sets and therefore HTP is unsolvable over $R$.

**Remark**

Most of the known Diophantine undecidability results over algebraic extensions of $\mathbb{Q}$ are obtained by constructing a Diophantine definition of $\mathbb{Z}$. However, there are notable exceptions to this pattern, e.g. Poonen’s Theorem, where a Diophantine model which is not a Diophantine definition is constructed.
Remark

Let $R$ be a recursive ring. Let $\phi : \mathbb{Z} \rightarrow R$ be a recursive injection such that the inverse image of every Diophantine set in $R$ is a Diophantine set in $\mathbb{Z}$. Then $R$ has undecidable Diophantine sets and therefore HTP is unsolvable over $R$. 
Indeed, suppose we knew how to determine whether solutions exist over \(\mathbb{Z}\). Let \(Q(x_1, \ldots, x_k)\) be a polynomial with rational coefficients. Then

\[
\exists x_1, \ldots, x_k \in \mathbb{Q} : Q(x_1, \ldots, x_k) = 0
\]

\[
\Updownarrow
\]

\[
\exists y_1, \ldots, y_k, z_1, \ldots, z_k \in \mathbb{Z} : Q\left(\frac{y_1}{z_1}, \ldots, \frac{y_k}{z_k}\right) = 0 \land z_1 \ldots z_k \neq 0.
\]

So decidability of HTP over \(\mathbb{Z}\) would imply the decidability of HTP over \(\mathbb{Q}\).
Diophantine Undecidability of the Field is a Stronger Statement

Proposition

Let $K$ be any field. Let $R$ be a subring of $K$ such that

- $K$ is the fraction field of $R$,
- the set of non-zero elements of $R$ is existentially definable over $R$.

Then Diophantine undecidability of $K$ implies Diophantine undecidability of $R$. 

Review: What is a Function Field?

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 $K$. Then $K$ is called a function field in $k$ variables over a constant field $C_K$.

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

**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
Function Field Primes

Definition (Function Field Primes for the Rational Case)

Let $C$ be a field and let $x$ be transcendental over $C$. Then the primes of the rational function field $C(x)$ are

1. the prime ideals of $C[x]$ corresponding to irreducible polynomials in $x$.
2. the prime ideal corresponding to $\frac{1}{x}$ in the ring $C[\frac{1}{x}]$.

Definition (Function Field Primes for the Algebraic Case)

Let $K$ be a finite extension of $C(x)$. Let $R_x$ be the integral closure of $C[x]$ in $K$ and let $R_{1/x}$ be the integral closure of $C[\frac{1}{x}]$ in $K$. The primes of $K$ are

1. prime ideals of $R_x$,
2. prime ideals of $R_{1/x}$ containing $1/x$. 
Proving Undecidability of HTP over Function Fields of Characteristic 0

The Main Tools

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

\[ O_p = \{ x \in K : \text{ord}_p x \geq 0 \} \]

Theorem (Moret-Bailly, 2006)

- Let \( K \) be any function field of characteristic 0. Then there exists an elliptic curve of rank 1 defined over \( K \).
- Let \( K \) be a function field such that for some prime \( p \) of \( K \) we have that \( O_p \) is existentially definable over \( K \). Then HTP is unsolvable over \( K \).
**Definition (Holomorphy Ring)**

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

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

**Theorem (Moret-Bailly, S. work in progress)**

Let $K$ be any function field of characteristic 0 and let $\mathcal{W}$ be any set of primes of $K$ not containing all the primes of $K$. Then HTP is not solvable over $O_{K,\mathcal{W}}$. 
Theorem

HTP is unsolvable over the following fields:

- rational function fields over finite fields of characteristic greater than 2 (Pheidas, 1991);
- rational function fields over a constant field $C$, where $C$ is a proper subfield of the algebraic closure of a finite field (Kim and Roush, 1992).
- rational function fields over finite fields of characteristic 2 (Videla, 1994).
Theorem

**HTP is unsolvable over the following fields:**

- **algebraic function fields over finite fields of characteristic greater than 2** (S. 1996);
- **a field** $K = C(u, v) \otimes_{\mathbb{Z}/p} F$, **where** $p > 2$, $C$ **is algebraic** over $\mathbb{Z}/p$ **and has an extension of degree** $p$, $u$ **is transcendental** over $C$, $v$ **is algebraic** over $C(u)$, and $C(u,v)$ and $F$ **linearly disjoint** over $\mathbb{Z}/p$ (S. 2000);
- **$K$ as above** for $p = 2$ (Eisenträger 2003)
- **any field** $K$ **finitely generated** over $\mathbb{Z}/p$ (S. 2002)
- **a field** $K = E \otimes_{\mathbb{Z}/p} F$, **where** $E$ **is finitely generated** over a field $C$ **algebraic** over $\mathbb{Z}/p$ **and with an extension of degree** $p$, **and** $E$ and $F$ **linearly disjoint** over $\mathbb{Z}/p$ (S. 2003)
The Main Unsolved Question

A Problem
Let $C_p$ be the algebraic closure of $\mathbb{Z}/p$ for some rational prime $p$. Show that the existential theory of a function field (or even a rational function field) over $C_p$ is undecidable.
$p$-divisibility

**Definition**

Let $x, y \in \mathbb{Z}_{\neq 0}$ and let $p$ be a rational prime. Then we will say that $x|_p y$ if $y = xp^s$, where $s \in \mathbb{Z}_{\geq 0}$.

**Proposition (Pheidas 1987)**

*Let $p$ be a rational prime. Then multiplication is existentially definable in the system $(\mathbb{Z}_{\geq 0}, +, |_p)$.***
Proposition

Let $K$ be a countable function field over a field of constants $C$ of positive characteristic $p$. Let $q$ be a prime of $K$. Suppose the following subsets of $K$ are Diophantine over $K$:

$$INT = \{x \in K : \text{ord}_q x \geq 0\};$$

$$p(K) = \{(x, y) \in K^2 : y = x^{p^s}, s \in \mathbb{Z}_{\geq 0}\}.$$

Then HTP is unsolvable over $K$. 
Proof.

Send \( n \mapsto A_n = \{ x \in K : \text{ord}_q x = n \} \). Observe the following:

- For any \( x \in K \) we have that \( \exists n : x \in A_n \iff \text{ord}_q x \geq 0 \)
- \( x, y \in A_n \iff \text{ord}_q \frac{x}{y} = 0 \)
- \( x \in A_n, y \in A_m, z \in A_{n+m} \iff \text{ord}_q \frac{xy}{z} = 0 \)
- \( x \in A_n, y \in A_m, n \mid_p m \iff \exists s \in \mathbb{Z}_{\geq 0}, \exists z \in A_n : y = z^{p^s} \)
The General Plan

Notation
- Let $C$ be a field of characteristic $p > 0$,
- let $t$ be transcendental over $C$,
- let $K$ be a finite separable extension of $C(t)$.

The Three Step Program
1. Define $p$-th powers of $t$.
2. Define $p$-th powers of a set of functions with simple zeros and poles.
3. Define $p$-th powers of arbitrary functions.
Lemma (Pheidas)

Let $C$ be a finite field of characteristic $p > 2$. Let $t$ be transcendental over $C$. Then the equations below are satisfied with $u, v, w \in C(t)$ if and only if for some $s \in \mathbb{Z}_{\geq 0}$ we have that $w = t^{p^s}$.

\[
\begin{aligned}
    w - t &= v^p - v \\
    \frac{1}{w} - \frac{1}{t} &= u^p - u
\end{aligned}
\]

Satisfiability is easy

For any $x \in K$ and any $s \in \mathbb{Z}_{\geq 0}$

\[
x^{p^s} - x = (x^{p^{(s-1)}} + x^{p^{(s-2)}} + \ldots + x)^p - (x^{p^{(s-1)}} + x^{p^{(s-2)}} + \ldots + x)
\]
Constructing $p$-th powers of $t$

We proceed in two steps. First we show that if $w$ satisfies equation below, then it is a $p$-th power.

\[
\begin{align*}
\begin{cases}
w - t &= v^p - v \\
\frac{1}{w} - \frac{1}{t} &= u^p - u
\end{cases} \tag{3}
\end{align*}
\]

Second, we show that if $w = w_1^p$ we can rewrite the equations above:

\[
\begin{align*}
\begin{cases}
w_1 - t &= (v^p - w_1^p) + (w_1 - v) = v_1^p - v_1 \\
\frac{1}{w_1} - \frac{1}{t} &= u^p - \frac{1}{w_1^p} + \frac{1}{w_1} - u = u_1^p - u_1
\end{cases} \tag{4}
\end{align*}
\]
A Property of Order at a Prime

Let $K$ be a function field and let $x, y \in K$. Let $p$ be a prime of $K$. Assume that $\mathrm{ord}_p x < \mathrm{ord}_p y$. Then $\mathrm{ord}_p(x + y) = \mathrm{ord}_p x$. Now let $a \in K$ be such that $\mathrm{ord}_p a = -1$ and consider

$$\mathrm{ord}_p(a^n + ax^n) = \begin{cases} 
\mathrm{ord}_p ax^n \equiv -1 \not\equiv 0 \mod n & \text{if } \mathrm{ord}_p x < 0, \\
\mathrm{ord}_p a^n \equiv 0 \mod n & \text{if } \mathrm{ord}_p x \geq 0.
\end{cases}$$
Inert Primes and Norms

**Definition (Inert Primes)**

Let $C$ be a finite field of characteristic $p > 0$. Let $t$ be trascendental over $C$ and let $K/C(t)$ be a cyclic extension of prime degree $q$. Let $p$ be a prime of $C(t)$ (i.e. either a prime ideal of $C[t]$ or $C[\frac{1}{t}]$.) Let $O_K$ be the integral closure of $C[t]$ (or $C[\frac{1}{t}]$) in $K$ and consider the ideal $pO_K$. If this ideal is a prime ideal of $O_K$ we say that $p$ is inert in the extension $K/C(t)$.

**Lemma**

Let $\sigma_1 = id, \ldots, \sigma_q$ be all the embeddings of $K$ into its algebraic closure leaving $C(t)$ fixed. Let $\alpha$ be a generator of $K$ over $C(t)$. Let $b_0, \ldots, b_{q-1}, y \in C(t)$ and consider the following equation:

$$\prod_{i=1}^{q} \left( b_0 + \sigma_i(\alpha)b_1 + \ldots + \sigma_i(\alpha^{q-1})b_{q-1} \right) = y$$

(If we were to multiply all the terms out, the resulting polynomial equation will have all of its coefficients in $C(t)$.) Then this equation has solutions $b_0, \ldots, b_{q-1}$ only if $\text{ord}_p y \equiv 0 \mod q$. 
Inert Primes and Norms

Proof.

Let \( x \in K \setminus C(t) \) and \( x = \sum_{j=0}^{q-1} b_j \alpha^j \), then \( y = N_{K/C(t)}(x) \) and \( \text{ord}_p y \equiv 0 \mod q \). If \( x \in C(t) \) and \( x = \sum_{j=0}^{q-1} b_j \alpha^j \), then \( b_1 = \ldots = b_{q-1} = 0 \) and \( y = x^q \). In this case \( \text{ord}_p y \equiv 0 \mod q \) also.

To insure that we always have solutions we need to add some factors to the right side and use several equations plus Hasse Norm Principle.

If the field of constants is algebraically closed, there are no inert primes in any extension, and therefore this method for defining integrality does not work.
What Do We Know about the First-Order Theory

Theorem

The first-order theory is undecidable for the following fields:

- rational function fields over perfect field of constants (Cherlin, 1984),
- function fields over algebraically closed fields of positive characteristic (Duret, 1986),
- rational function fields over any field of constants of characteristic greater than 5 (Pheidas, 2004),
- any function field of characteristic greater than 2 (Eisenträger, S. 2007),
- any function field over a field of constants algebraic over a finite field (Eisenträger, S. 2007).
**Proposition (Julia Robinson)**

Multiplication is definable in $\langle \mathbb{Z}_{\geq 0}, +, \mid \rangle$.

**Proposition**

Let $K / C(t)$ be a finite extension with $C$ of characteristic $p > 0$. Assume $p(K, t) = \{x \in K : \exists s \geq 0, x = t^{p^s}\}$ is first order definable. Then the following sets are first-order definable:

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

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

**Theorem**

Assume that $t$ has a simple pole or a simple zero. Suppose that the set $p(K, t)$ is first-order definable in $K$. Then $\langle \mathbb{Z}_{>0}, +, \mid \rangle$ has a model over $K$. 
Proof.

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

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

since at least one pole or zero of $t$ is simple.

Hence $s_1 \mid s_2$ if and only if

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

The result now follows from the fact that the sets $p(K, t), B(K, t)$ and $C(K, t)$ are all first-order definable in $K$. \qed