On Computably Enumerable Sets over Function Fields

Alexandra Shlapentokh

East Carolina University

Joint Meetings 2017

Atlanta

January 2017
On Computably Enumerable Sets over Function Fields

Some History

Outline

1 Some History
   ■ A Question and the Answer

2 Function Fields

3 Constructing Single-fold Diophantine Definitions of \( \mathbb{Z} \) over Rings of Integral Functions

4 Finite-fold Diophantine Definition of C.E. Sets of Polynomial Rings over (Countable) Totally Real Fields of Constants
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?

Using modern terms one can ask if there exists a program taking coefficients of a polynomial equation as input and producing “yes” or “no” answer to the question “Are there integer solutions?”.

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 Matiyasevich. Actually a much stronger result was proved. It was shown that the recursively enumerable subsets of $\mathbb{Z}$ are the same as the Diophantine subsets of $\mathbb{Z}$.
Diophantine Sets: a Number-Theoretic Definition

Let $R$ be a ring and let $m \in \mathbb{Z}_{>0}$. A subset $A \subseteq R^m$ 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 element $(t_1, \ldots, t_m) \in R^m$ 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 $R$. 

Remark

Diophantine sets can also be described as the sets existentially definable in the language of rings or as projections of algebraic sets.

A consequence of the MDRP result

There are undecidable Diophantine subsets of $\mathbb{Z}$. 

**Diophantine Sets: a Number-Theoretic Definition**

Let $R$ be a ring and let $m \in \mathbb{Z}_{>0}$. 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 element $(t_1, \ldots, t_m) \in R^m$ we have that

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

$$\uparrow \downarrow$$

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

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

**Remark**

*Diophantine sets can also be described as the sets existentially definable in the language of rings or as projections of algebraic sets.*
Diophantine Sets: a Number-Theoretic Definition

Let $R$ be a ring and let $m \in \mathbb{Z}_{>0}$. 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 element $(t_1, \ldots, t_m) \in R^m$ 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 $R$.

Remark

Diophantine sets can also be described as the sets existentially definable in the language of rings or as projections of algebraic sets.

A consequence of the MDRP result

There are undecidable Diophantine subsets of $\mathbb{Z}$. 
Some observations

- For any ring $R$, $m \in \mathbb{Z}_{>0}$ and any Diophantine subset $A$ of $R^m$, a Diophantine definition of $A$ is not unique. For example, if $R$ is an integral domain and $f(\bar{t}, \bar{x})$ is a Diophantine definition of a set $A$, then so is $f(\bar{t}, \bar{x})^\ell$ for any $\ell \in \mathbb{Z}_{>0}$.
Some observations

- For any ring \( R, m \in \mathbb{Z}_{>0} \) and any Diophantine subset \( A \) of \( R^m \), a Diophantine definition of \( A \) is not unique. For example, if \( R \) is an integral domain and \( f(\bar{t}, \bar{x}) \) is a Diophantine definition of a set \( A \), then so is \( f(\bar{t}, \bar{x})^\ell \) for any \( \ell \in \mathbb{Z}_{>0} \).

- It is often the case that given \( R, A \) and \( f \) as above, for any \( \bar{t} \in A \) the polynomial equation

\[
f(\bar{t}, \bar{x}) = 0
\]

has many solutions \( \bar{x} \in R^k \), possibly infinitely many solutions.
Let $R$ be a ring and let $m \in \mathbb{Z}_{>0}$. A subset $A \subset R^m$ is called single-fold (finite-fold) 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 element $(t_1, \ldots, t_m) \in R^m$ we have that

$$\exists \ a \ unique \ (\text{resp. finitely \ many}) \ \tilde{x} \in R^k \text{ such that}$$

$$p(t_1, \ldots, t_m, x_1, \ldots, x_k) = 0$$

$$\uparrow$$

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

In this case we call $p(T_1, \ldots, T_m, X_1, \ldots, X_k)$ a single-fold (finite-fold) Diophantine definition of $A$ over $R$. 
A Question of Yu. Matiyasevich

Is every Diophantine subset of $\mathbb{Z}$ single-fold (or at least finite-fold) Diophantine?
A Question of Yu. Matiyasevich

Is every Diophantine subset of $\mathbb{Z}$ single-fold (or at least finite-fold) Diophantine?

■ Who cares?
A Question of Yu. Matiyasevich

Is every Diophantine subset of $\mathbb{Z}$ single-fold (or at least finite-fold) Diophantine?

- Who cares?
- What makes you think that the answer might be positive?
Proposition (Yu. Matiyasevich 1977)

Let $A \subseteq \mathbb{Z}_m^m \geq 0$ be a c.e. set. In this case there exist $P(\bar{Z}, \bar{X}) \in \mathbb{Z}[\bar{Z}, \bar{X}]$ such that

$$(a_1, \ldots, a_m) \in A \iff \exists \text{ unique } (y, x_1, \ldots, x_k) \in \mathbb{Z}_k^{k+1} : P(\bar{a}, \bar{x}) = y + 4^y.$$
Proposition (Yu. Matiyasevich 1977)

Let \( A \subset \mathbb{Z}^m_{\geq 0} \) be a c.e. set. In this case there exist \( P(\vec{Z}, \vec{X}) \in \mathbb{Z}[\vec{Z}, \vec{X}] \) such that

\[
(a_1, \ldots, a_m) \in A \iff \exists \text{ unique } (y, x_1, \ldots, x_k) \in \mathbb{Z}^{k+1}_{\geq 0} : P(\vec{a}, \vec{x}) = y + 4^y.
\]

Corollary

Every c.e. set of non-negative integers is single-fold (finite-fold) Diophantine over \( \mathbb{Z}_{\geq 0} \) if and only if the set

\[
\{(y, 2^y) | y \in \mathbb{Z}_{\geq 0}\}
\]

is single-fold (finite-fold) Diophantine over \( \mathbb{Z} \).
A problem of effective solution sizes

Let $P(T, X_1, \ldots, X_m)$ be a polynomial with coefficients in $\mathbb{Z}$ and assume that for some suitably chosen functions

\[ \sigma : \mathbb{Z} \to \mathbb{Z}_{\geq 0}, \]

\[ \nu : \mathbb{Z} \to \mathbb{Z}_{\geq 0}, \]

we have that for every $a \in \mathbb{Z}$, the number of integer $m$-tuples with $P(a, \bar{x}) = 0$ is at most $\nu(a)$ and $\max |x_i| < \sigma(a)$. If we can compute $\sigma(x)$, then we can compute (some version of) $\nu(x)$. The question is whether, given $\nu(x)$, it is always possible to compute (some version of) $\sigma(x)$. If all Diophantine subsets of $\mathbb{Z}$ have a single-fold representation, then the answer is "no".
A consequence of existence of a single-fold definitions for all c.e. sets

**Proposition**

Let $A \subset \mathbb{Z}$ be c.e. but non-computable and assume that $P(Z, X_1, \ldots, X_m)$ is a single-fold definition of $A$ over $\mathbb{Z}$. Then for any total computable function $\sigma : \mathbb{Z} \rightarrow \mathbb{Z}$ there exists $a \in A$ such that $P(a, x_1, \ldots, x_k) = 0 \land \max(|x_1|, \ldots, |x_k|) > \sigma(a)$. 
A consequence of existence of a single-fold definitions for all c.e. sets

**Proposition**

Let $A \subset \mathbb{Z}$ be c.e. but non-computable and assume that $P(Z, X_1, \ldots, X_m)$ is a single-fold definition of $A$ over $\mathbb{Z}$. Then for any total computable function $\sigma : \mathbb{Z} \rightarrow \mathbb{Z}$ there exists $a \in A$ such that

$$P(a, x_1, \ldots, x_k) = 0 \land \max(|x_1|, \ldots, |x_k|) > \sigma(a).$$

**Proof.**

Suppose there exists a total computable $\sigma : \mathbb{Z} \rightarrow \mathbb{Z}$ such that for all $a \in A$ we have that

$$P(a, x_1, \ldots, x_k) = 0 \land \max(|x_1|, \ldots, |x_k|) < \sigma(a).$$

Then given any $b \in \mathbb{Z}$ we can compute $\sigma(b)$ and check whether there exist $x_1, \ldots, x_k$ with $|x_i| < \sigma(b)$ and $P(b, x_1, \ldots, x_k) = 0$. If the answer is “yes”, then $b \in A$. Otherwise, $b \not\in A$. Hence we would have an algorithm to check membership in $A$ in contradiction of our assumption on $A$. □
Outline

1. Some History
   - A Question and the Answer

2. Function Fields

3. Constructing Single-fold Diophantine Definitions of \( \mathbb{Z} \) over Rings of Integral Functions

4. Finite-fold Diophantine Definition of C.E. Sets of Polynomial Rings over (Countable) Totally Real Fields of Constants
Rings of Integral Functions

Definition (Integral Closure)
Let $R_1 \subseteq R_2$ be integral domains and let $\text{Int}(R_1) \subseteq R_2$ be the set of all elements of $R_2$ satisfying monic irreducible polynomials with coefficients in $R_1$. Then $\text{Int}(R_1)$ is called the integral closure of $R_1$ in $R_2$. (It can be shown that $\text{Int}(R_1)$ is also a ring.)
Rings of Integral Functions

**Definition (Integral Closure)**
Let $R_1 \subset R_2$ be integral domains and let $\text{Int}(R_1) \subseteq R_2$ be the set of all elements of $R_2$ satisfying monic irreducible polynomials with coefficients in $R_1$. Then $\text{Int}(R_1)$ is called the integral closure of $R_1$ in $R_2$. (It can be shown that $\text{Int}(R_1)$ is also a ring.)

**Definition (Integral Functions)**
Let $k$ be a field, let $t$ be transcendental over $k$, and let $K$ be a finite extension of $k(t)$. Then a ring of integral functions of $K$ is the integral closure of $k[t]$ in $K$. 
The Main Results

Theorem (Joint work with R. Miller)

1. Rational integers have a single-fold Diophantine definition over any ring of integral functions of any function field of characteristic 0.

2. Every c.e. set of integers has a single-fold Diophantine definition over any ring of integral functions of any function field of characteristic 0.

3. All c.e. subsets of polynomial rings over rings of integers of totally real number fields have finite-fold Diophantine definitions.
Outline

1. Some History
   - A Question and the Answer

2. Function Fields

3. Constructing Single-fold Diophantine Definitions of $\mathbb{Z}$ over Rings of Integral Functions

4. Finite-fold Diophantine Definition of C.E. Sets of Polynomial Rings over (Countable) Totally Real Fields of Constants
One vs. Finitely Many

Lemma (Replacing Finitely Many by One)

Let $R$ be any integral domain 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 integral domain 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 $h(x) = \sum_{i=0}^{k} a_i x^i$, $a_k \neq 0$ 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 $K$.\[\square\]
Corollary

Let $R$ be an integral domain and let $A$ and $B$ be subsets of $R$ single-fold (finite-fold) over $R$. Then $A \cap B$ is single-fold (finite-fold) over $R$. 
Lemma (Denef 1978)

Let $R$ be an integral domain of characteristic 0 and $x$ transcendental over $R$. Let $s \in R[x] \setminus R$. Let $(f_n(s), g_n(s)) \in R[x]$ be such that

$$f_n(s) - (s^2 - 1)^{1/2} g_n(s) = (s - (s^2 - 1)^{1/2})^n.$$ 

In this case

1. $\deg f_n = n \deg s$, $\deg g_n = (n - 1) \deg s$.
2. $\ell$ dividing $n$ is equivalent to $g_\ell$ dividing $g_n$.
3. The pairs $(f_n, g_n)$ are all the solutions to $f^2 - (s^2 - 1)g^2 = 1$ in $R[x]$. 


### Lemma (S. 1992)

Let $R$ be an integral domain of characteristic 0 and let $x$ be transcendental over $R$. Let $k$ be the fraction field of $R$ and let $K$ be a finite extension of $k(x)$. Let $I$ be the integral closure of $R[x]$ in $K$. Then there exists $s \in I$, such that $s$ is not algebraic over $R$ and the set of pairs $(f_n(s), g_n(s)) \in R[s]$ satisfying

$$f_n(s) - (s^2 - 1)^{1/2} g_n(s) = (s - (s^2 - 1)^{1/2})^n.$$ 

also has the following properties.

1. $\deg f_n(s) = n$, $\deg g_n = (n - 1)$ as polynomials in $s$,
2. $\ell$ dividing $n$ is equivalent to $g_\ell$ dividing $g_n$,
3. The pairs $(f_n, g_n)$ are all the solutions to $f^2 - (s^2 - 1)g^2 = 1$ in $I$. 
Generating Positive Integers

Some basic algebra

\[
\frac{\varepsilon^n - 1}{\varepsilon - 1} = \varepsilon^{n-1} + \varepsilon^{n-2} + \ldots + 1 \equiv n \pmod{(\varepsilon - 1)}
\]

in \(\mathbb{Z}[^{\varepsilon}]\). Now set \(\varepsilon = s - \sqrt{s^2 - 1}, \varepsilon^n = f_n - g_n\sqrt{s^2 - 1}, f_n, g_n \in \mathbb{Z}[s]\)

and rewrite the equivalence above as

\[
f_n - 1 - g_n\sqrt{s^2 - 1} \equiv n(s - \sqrt{s^2 - 1}) \pmod{(s - 1 - \sqrt{s^2 - 1})^2},
\]

\[
f_n - 1 - g_n\sqrt{s^2 - 1} - n(s - \sqrt{s^2 - 1}) =
\]

\[
(s - 1 - \sqrt{s^2 - 1})^2(a + b\sqrt{s^2 - 1}), a, b \in \mathbb{Z}[s],
\]

\[
f_n - 1 - g_n\sqrt{s^2 - 1} - n(s - \sqrt{s^2 - 1}) =
\]

\[
(2s^2 - 2s - 2(s - 1)\sqrt{s^2 - 1})(a + b\sqrt{s^2 - 1}), a, b \in \mathbb{Z}[s],
\]

\[
g_n + n = 2a(s - 1) + b(2s^2 - 2s) = 2(s - 1)(a + bs).
\]
Generating Negative Integers

More basic algebra

Now set $\varepsilon^{-1} = s + \sqrt{s^2 - 1}$, $\varepsilon^{-n} = f_n + g_n\sqrt{s^2 - 1}$, $f_n, g_n \in \mathbb{Z}[s]$ and rewrite the equivalence above as

$$f_n - 1 + g_n\sqrt{s^2 - 1} \equiv n(s + \sqrt{s^2 - 1}) \mod (s - 1 + \sqrt{s^2 - 1})^2,$$

$$f_n - 1 + g_n\sqrt{s^2 - 1} - n(s + \sqrt{s^2 - 1}) =$$

$$(s - 1 + \sqrt{s^2 - 1})^2(a + b\sqrt{s^2 - 1}), a, b \in \mathbb{Z}[s],$$

$$f_n - 1 + g_n\sqrt{s^2 - 1} - n(s + \sqrt{s^2 - 1}) =$$

$$(2s^2 - 2s - 2(s - 1)\sqrt{s^2 - 1})(a + b\sqrt{s^2 - 1}), a, b \in \mathbb{Z}[s],$$

$$g_n - n = 2a(s - 1) + b(2s^2 - 2s) = 2(s - 1)(a + bs).$$
The Main Part of the Definition of $\mathbb{Z}$

**Proposition**

The system below is satisfied over $\mathbb{Q}[s]$ if and only if $x$ is a non-zero integer.

\[
\begin{align*}
    f^2 - (s^2 - 1)g^2 &= 1, \\
    x &\text{ is a non-zero constant}, \\
    g &\equiv x \mod (s - 1).
\end{align*}
\]

**Proof.**

- If the system is satisfied then $g = \pm g_n \equiv \pm n \mod (s - 1)$ for some $n \in \mathbb{Z}_{>0}$. Therefore $x \equiv \pm n \mod (s - 1)$ or $s - 1$ divides $x \pm n$. Since $x \pm n$ is a constant, it can be divisible by a polynomial of positive degree only if it is 0, i.e. $x = \pm n$.
- If $x = \pm n, n \in \mathbb{Z}_{>0}$, then for some $g = \pm g_n$, we have that $x \equiv \pm g \mod (s - 1)$.

Note that given a choice of the sign for $x$, the choice of the sign for $g$ is fixed.
Defining constants

- We don’t have a uniform definition of constants.
- Rings of integral functions contain the constant field. We can use the fact that all non-zero constants have inverses in the ring to separate constants from non-constant elements.
- In the case of a polynomial ring over a field it would be sufficient to require for an element to be invertible, since no non-constant polynomial has an inverse.
- In the case of a ring of integral functions, one might have to require for $x, x + 1, \ldots, x + k$ to be invertible. The number $k$ will depend on the ring.
- If the ring of constants does not have “enough” invertible elements, we can use divisibility to define constants.
The Main Results

Theorem (Joint work with R. Miller)

1. Rational integers have a single-fold Diophantine definition over any ring of integral functions of any function field of characteristic 0.

2. Every c.e. set of integers has a single-fold Diophantine definition over any ring of integral functions of any function field of characteristic 0.

3. All c.e. subsets of polynomial rings over rings of integers of totally real number fields have finite-fold Diophantine definitions.
Units and Constants in $\mathbb{Q}[s, \sqrt{s^2 - 1}]$

- $\varepsilon = s - \sqrt{s^2 - 1}$ is a unit in $\mathbb{Q}[s, \sqrt{s^2 - 1}]$ since $\varepsilon^{-1} = s + \sqrt{s^2 - 1}$.
- $\varepsilon - b, b \neq 0$ is not a unit in this ring and in particular if $c \neq 0$ is a constant, then $\varepsilon - b$ does not divide $c$ in $\mathbb{Q}[s, \sqrt{s^2 - 1}]$.

Proof.

- The map $\sigma : \mathbb{Q}[s, \sqrt{s^2 - 1}] \rightarrow \mathbb{Q}[s, \sqrt{s^2 - 1}]$ sending $\sqrt{s^2 - 1}$ to $-\sqrt{s^2 - 1}$ and not moving $\mathbb{Q}[s]$ is an isomorphism.
- If $s - \sqrt{s^2 - 1} - b$ is a unit, then $s + \sqrt{s^2 - 1} - b$ is also a unit.
- The map $N : \mathbb{Q}[s, \sqrt{s^2 - 1}] \rightarrow \mathbb{Q}[s]$ sending $a + b\sqrt{s^2 - 1}, a, b \in \mathbb{Q}[s]$ to $(a + b\sqrt{s^2 - 1})(a - b\sqrt{s^2 - 1})$ is a homomorphism sending units to units.
- $(s - \sqrt{s^2 - 1} - b)(s + \sqrt{s^2 - 1} - b) = (s - b)^2 - (s^2 - 1) = -2bs + b^2 + 1$ is a linear polynomial and so not a unit in $\mathbb{Q}[s]$. 

Defining exponentiation

**Theorem**

The following set has a single-fold definitions over $\mathbb{Q}[s]$:

$$EXP = \{(b, c, d) | b, c, d \in \mathbb{Z} \land |b| = |c|^{d}\}.$$
Proof.

Let \( \varepsilon = s - \sqrt{s^2 - 1} \). Consider the following equations and conditions: \( b, c, d \in \mathbb{Z}, b \neq 0 \) and \( \exists n \in \mathbb{Z}_{\geq 0}, x, y, \in \mathbb{Q}[\varepsilon, s] : \)

\[
\varepsilon^n \pm c = (\varepsilon - b)x \land d \pm \frac{\varepsilon^n - 1}{\varepsilon - 1} = y(\varepsilon - 1). \tag{2}
\]

From (2) we conclude that \((\varepsilon - b)\) divides \(\pm b^n - c\) in \(\mathbb{Q}[\varepsilon, s] = \mathbb{Q}[s, \sqrt{s^2 - 1}]\). Since \(b \neq 0\), we conclude that \(\pm b^n = c\), and \(n \geq 0\). At the same time, also from (2) we have that \(d = \pm n\). Conversely, assuming \(b, c, d \in \mathbb{Z}_{\geq 0}, b \neq 0\), it is easy to see that (2) can be satisfied with only one choice for the sign.
Complications: from $\mathbb{Z}$ to $\mathbb{Z}_{\geq 0}$.

Lagrange Four-Square Theorem does not produce single-fold definitions, only finite-fold. For any $y \in \mathbb{Z}$ we have

$$y \in \mathbb{Z}_{\geq 0} \iff y = x_1^2 + x_2^2 + x_3^2 + x_4^2, x_i \in \mathbb{Z}.$$ 

This definition of non-negative integers is finite-fold because each $x_i$ can take at most $2|y_i| + 1$ values.
Let \((b, d^4 + 1, 2d) \in \text{EXP}\), where \(2d \equiv \frac{b-1}{d^4} \mod d^4\). In this case we know that
\[
\frac{b-1}{d^4} = \frac{(d^4+1)^{2|d|-1} - 1}{d^4} =
\]
\[
2|d|d^4 + |d|(2|d| - 1)d^8 + \ldots + (\text{multiples of higher powers of } d) \frac{d^8}{d^4}
\]
\[
\equiv 2|d| \mod d^4
\]
and \(2d \equiv 2|d| \mod d^4\). Assuming \(|d| \neq 1\) and \(d < 0\), we have that \(d^3|4\) leading to a contradiction.
The Main Results

Theorem (Joint work with R. Miller)

1. Rational integers have a single-fold Diophantine definition over any ring of integral functions of any function field of characteristic 0.

2. Every c.e. set of integers has a single-fold Diophantine definition over any ring of integral functions of any function field of characteristic 0.

3. All c.e. subsets of polynomial rings over rings of integers of totally real number fields have finite-fold Diophantine definitions.
Outline

1 Some History
   ■ A Question and the Answer

2 Function Fields

3 Constructing Single-fold Diophantine Definitions of $\mathbb{Z}$ over Rings of Integral Functions

4 Finite-fold Diophantine Definition of C.E. Sets of Polynomial Rings over (Countable) Totally Real Fields of Constants
The Predecessors

The Predecessors


Definition

A finite extension of \( \mathbb{Q} \) is called **totally real** if all of its embedding into the algebraic closure of \( \mathbb{Q} \) are real.
Effective indexing or enumeration of polynomials

By an effective enumeration of polynomials over a chosen countable formally real field we mean a bijection from a ring into positive integers such that given a “usual” presentation of a polynomial (or an integral function in general) we can effectively compute the image of this polynomial (or this integral function), and conversely, given a positive integer, we can determine what polynomial (or integral function) was mapped to it.
Notation

- Let $k$ be a totally real number field.
- Let $O_k$ be the ring of integers of $k$—the integral closure of $\mathbb{Z}$ in $k$.
- Let $\alpha_1, \ldots, \alpha_r$ be an integral basis of $O_k$ over $\mathbb{Z}$.
- Let $\theta : \mathbb{Z}_{>0} \rightarrow O_k[T]$ be the effective bijection discussed above.
- Denote $\theta(n) = P_n(T)$.
- Let $(X_n(T), Y_n(T)) \in O_k[T]$ be such that

$$X_n(T) - (T^2 - 1)^{1/2} Y_n(T) = (T - (T^2 - 1)^{1/2})^n.$$
$\theta$-c.e. subsets of $O_k[T]^m$

**Definition**

For any positive integer $m$ and any set $A \subseteq O_k[T]^m$, let

$$\theta^{-1}(A) = \{(r_1, \ldots, r_m) \in \mathbb{Z}_0^m \mid (P_{r_1}, \ldots, P_{r_m}) \in A\}.$$  

We say that a subset $A$ of $O_k[T]^m$ is c.e. if $\theta^{-1}(A)$ is a c.e. subset of $\mathbb{Z}^m$. 

---

On Computably Enumerable Sets over Function Fields
Finite-fold Diophantine Definition of C.E. Sets of Polynomial Rings over (Countable) Totally Real Fields of Constants
**Definition**

For any positive integer $m$ and any set $A \subseteq O_k[T]^m$, let
\[
\theta^{-1}(A) = \{(r_1, \ldots, r_m) \in \mathbb{Z}^m_{>0} | (P_{r_1}, \ldots, P_{r_m}) \in A\}.
\]
We say that a subset $A$ of $O_k[T]^m$ is c.e. if $\theta^{-1}(A)$ is a c.e. subset of $\mathbb{Z}^m$.

**Theorem**

Let $R$ be the ring of integers in a totally real number field $k$. Let $\theta$ be an effective indexing of $R[T]$; then every $\theta$-computably enumerable relation over $R[T]$ is a finite-fold Diophantine relation over $R[T]$.
What is needed for the proof?

It is enough to show that

- all c.e. subsets of $\mathbb{Z}$ are finite-fold Diophantine over the polynomial ring in question, ✓

and

- the indexing is finite-fold Diophantine or, in other words, the set

$$I = \{(n, P_n) | n \in \mathbb{Z}_{>0}\}$$

is finite-fold Diophantine over $O_k[T]$. 
How would it work?

If $A \subset O_k^m$ is a c.e. set, then $\theta^{-1}(A) \subset \mathbb{Z}^m$ is a c.e. subset over $\mathbb{Z}$ and hence finite-fold Diophantine over $O_k[T]$. Thus a Diophantine definition of $A$ will look like the following system of equations:

$$(Q_1, \ldots, Q_m) \in A \text{ if and only if }$$

$$\begin{cases} 
(r_1, \ldots, r_m) \in \theta^{-1}(A) \\
(r_j, Q_j) \in I, j = 1, \ldots, m
\end{cases}$$
Totally Positive Polynomials

Definition

If $F$ is a polynomial in $O_k[T]$, then $F$ is positive-definite on $k$ (denoted by $\text{Pos}(F)$) if and only if $|\sigma(F(t))| \geq 0$ for all $t \in k$ and for all real embeddings $\sigma$ of $k$ into its algebraic closure.

Lemma

The relation $\text{Pos}$ is Diophantine over $O_k[t]$.
The relation \( \text{Pos} \) is Diophantine

We claim that the following equivalence holds: \( \text{Pos}(F) \) if and only if there exist \( F_1, \ldots, F_5 \in O_k[t], g \in \mathbb{Z} \setminus \{0\} \)

\[
g^2 F = F_1^2 + \ldots + F_5^2. \tag{3}
\]

If (3) holds, then clearly \( \text{Pos}(F) \) holds.
Conversely suppose that \( F \) is positive definite on \( k \). In this case it follows from a theorem of Pourchet that \( F \) can be written as a sum of five squares in \( k[t] \). Now multiplying by a suitable positive integer constant \( g^2 \) these polynomials can be taken to be in \( O_k[t] \), and hence (3) has solutions.
The relation Pos is Finite-fold Diophantine

We now show that for a given $g$ and $F$ there can be only finitely many solutions to (3). First of all, the degrees of $F_1, \ldots, F_5$ are bounded by the degree of $F$. Secondly, observe that for any $a \in O_k$ we have that $|\sigma(F_i(a))| \leq |\sigma(F(a))|$ for all $i$ and all embeddings $\sigma$. Since $F_i(a)$ is an algebraic integer of $k$ of bounded height, there are only finitely many $b \in k$ such that $F_i(a)$ can be equal to $b$. Thus, there are only finitely many possible values for the coefficients of any $F_i$. 
A c.e. relation on \( \mathbb{Z} \)

**Definition**

Define the relation \( \text{Par}(n, b, c, d, v_1, \ldots, v_r) \) on the rational integers as follows: \( \text{Par}(n, b, c, d, g, v_1, \ldots, v_r) \) if and only if the following conditions hold:

1. \( n \) is the enumeration index of a polynomial \( P_n \in O_k[T] \);
2. \( b, c, d, g \in \mathbb{Z}_{\geq 0}, v_1, \ldots, v_r \in \mathbb{Z} \);
3. \( d = \deg P_n \);
4. \( c \) is the smallest possible positive integer so that \( \text{Pos}(Y^{2}_{d+2} + c - P^2_n - 1) \);
5. \( g \) is the smallest possible positive integer so that there exist \( F_1, \ldots, F_5 \in O_k[T] \) satisfying \( g^2(Y^{2}_{d+2} + c - P^2_n - 1) = F_1^2 + \ldots F_5^2 \).
6. \( \forall x \in \mathbb{Z} : \) if \( 0 \leq x \leq d \) then \( Y_{d+2}(x) \leq b \);
7. \( P_n(2b + 2c + d) = v_1\alpha_1 + \ldots + v_r\alpha_r \).
The last bit

**Lemma (Zahidi)**

\[ F \in O_k[T] \land F = P_n \text{ is equivalent to } \exists b, c, d, v_1, \ldots, v_r \in O_k[T]: \]

1. \( \text{Par}(n, b, c, d, g, v_1, \ldots, v_r); \)
2. \( Y_{d+2}^2 + c - F^2 - 1 \in Pos; \)
3. \( F(2b + 2c + d) = v_1 \alpha_1 + \ldots v_r \alpha_r. \)
The Main Results

Theorem (Joint work with R. Miller)

1. Rational integers have a single-fold Diophantine definition over any ring of integral functions of any function field of characteristic 0.

2. Every c.e. set of integers has a single-fold Diophantine definition over any ring of integral functions of any function field of characteristic 0.

3. All c.e. subsets of polynomial rings over rings of integers of totally real number fields have finite-fold Diophantine definitions.
Theorem (Joint work with R. Miller)

Let $R$ be a ring of integral functions over the field of constants that is a finite extension of $\mathbb{Q}$. Then all c.e. subsets of $R$ are Diophantine over $R$. 

Corollary

Any polynomial ring contained in $R$ is Diophantine over $R$. 

Without the Finite-fold Requirement
Without the Finite-fold Requirement

**Theorem (Joint work with R. Miller)**

Let $R$ be a ring of integral functions over the field of constants that is a finite extension of $\mathbb{Q}$. Then all c.e. subsets of $R$ are Diophantine over $R$.

**Corollary**

Any polynomial ring contained in $R$ is Diophantine over $R$. 