Diophantine Generation, Horizontal and Vertical Problems, and the Weak Vertical Method

Alexandra Shlapentokh

East Carolina University,
Greenville, North Carolina, USA

March, 2007

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

Table of Contents

1 **Diophantine Sets, Definitions and Generation**
- Diophantine Sets
- Diophantine Generation
- Properties of Diophantine Generation

2 **Diophantine Family of $\mathbb{Z}$**

3 **Diophantine Family of a Polynomial Ring**

4 **Going Down**
- Horizontal and Vertical Problems
- The Weak Vertical Method

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?

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

One vs. Finitely Many

Replacing Two by One

Let R be a ring whose fraction field is not algebraically closed. Then any finite system of equations over R can be effectively replaced by a single polynomial equation over R with the identical R-solution set.

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

One vs. Finitely Many

Replacing Two by One

Let R be a ring whose fraction field is not algebraically closed. Then 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

Indeed let $h(T) = a_0 + a_1 T \ldots + \ldots T^n$ be a polynomial without roots in the fraction field of R. Let $f(\bar{x}), g(\bar{x}) \in R[\bar{x}]$. Then

$$\sum_{i=0}^{n} a_i f(\bar{x})^i g(\bar{x})^{n-i} = 0 \Leftrightarrow f(\bar{x}) = 0 \wedge g(\bar{x}) = 0.$$

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

One vs. Finitely Many

Replacing Two by One

Let R be a ring whose fraction field is not algebraically closed. Then 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

Indeed let $h(T) = a_0 + a_1 T \ldots + \ldots T^n$ be a polynomial without roots in the fraction field of R. Let $f(\bar{x}), g(\bar{x}) \in R[\bar{x}]$. Then

$$\sum_{i=0}^{n} a_i f(\bar{x})^i g(\bar{x})^{n-i} = 0 \Leftrightarrow f(\bar{x}) = 0 \wedge g(\bar{x}) = 0.$$

One=Finitely Many

Thus any finite system of polynomial equations over R can be effectively replaced by single polynomial equation over R with the identical R-solution set.

Diophantine Sets

A Number-Theoretic Version

Let R be a ring. 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

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

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

A Number-Theoretic Version

Let R be a ring. A subset $A \subset R^m$ is called Diophantine over R if there exists a polynomial $p(T_1, \dots T_m, X_1, \dots, X_k)$ with coefficients in R such that for any element $(t_1, \dots, t_m) \in R^m$ we have that

$$(\exists x_1, \dots, x_k \in R : p(t_1, \dots, t_m, x_1, \dots, x_k) = 0) \iff t \in A.$$

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

One=Finitely Many

We can allow Diophantine definition to consist of several polynomials without changing the nature of relation.

Using Diophantine Definitions to Solve the Problem

Lemma

Let R be a recursive ring of characteristic 0 such that $\mathbb{Z}$ has a Diophantine definition $p(T, \bar{X})$ over R. Then HTP is not decidable over R.

Using Diophantine Definitions to Solve the Problem

Lemma

Let R be a recursive ring of characteristic 0 such that $\mathbb{Z}$ has a Diophantine definition $p(T, \bar{X})$ over R. Then HTP is not decidable over R.

Proof.

Let $h(T_1, \ldots, T_l)$ be a polynomial with rational integer coefficients and consider the following system of equations.

$$\begin{cases} h(T_1, \ldots, T_l) = 0 \\ p(T_1, \bar{X}_1) = 0 \\ \ldots \\ p(T_l, \bar{X}_l) = 0 \end{cases} \tag{1}$$

It is easy to see that $h(T_1, \ldots, T_l) = 0$ has solutions in $\mathbb{Z} \iff$ (1) has solutions in R. Thus if HTP is decidable over R, it is decidable over $\mathbb{Z}$. $\square$

Diophantine Generation

Initial Data

- R_1, R_2 are rings with quotient fields F_1 and F_2 respectively.

Diophantine Generation

Initial Data

- R_1, R_2 are rings with quotient fields F_1 and F_2 respectively.
- F is a field such that $F_1 \subseteq F$ and $F_2 \subseteq F$ and F/F_2 is a finite extension.

Diophantine Generation

Initial Data

- R_1, R_2 are rings with quotient fields F_1 and F_2 respectively.
- F is a field such that $F_1 \subseteq F$ and $F_2 \subseteq F$ and F/F_2 is a finite extension.
- $\Omega = \{\omega_1, \ldots, \omega_n\}$ is a basis F over F_2.

Diophantine Generation

Initial Data

- R_1, R_2 are rings with quotient fields F_1 and F_2 respectively.
- F is a field such that $F_1 \subseteq F$ and $F_2 \subseteq F$ and F/F_2 is a finite extension.
- $\Omega = \{\omega_1, \ldots, \omega_n\}$ is a basis F over F_2.
- $P(X_1, \ldots, X_n, Y, Z_1, \ldots, Z_m)$ is a polynomial over R_2.

Diophantine Generation

Initial Data

- R_1, R_2 are rings with quotient fields F_1 and F_2 respectively.
- F is a field such that $F_1 \subseteq F$ and $F_2 \subseteq F$ and F/F_2 is a finite extension.
- $\Omega = \{\omega_1, \ldots, \omega_n\}$ is a basis F over F_2.
- $P(X_1, \ldots, X_n, Y, Z_1, \ldots, Z_m)$ is a polynomial over R_2.
- For any $x_1, \ldots, x_n, y \in R_2$, we have that

$$\exists z_1, \ldots, z_m \in R_2 : P(x_1, \ldots, x_n, y, z_1, \ldots, z_m) = 0$$
$$\Downarrow$$
$$y \neq 0$$

Diophantine Generation

Initial Data

- R_1, R_2 are rings with quotient fields F_1 and F_2 respectively.
- F is a field such that $F_1 \subseteq F$ and $F_2 \subseteq F$ and F/F_2 is a finite extension.
- $\Omega = \{\omega_1, \ldots, \omega_n\}$ is a basis F over F_2.
- $P(X_1, \ldots, X_n, Y, Z_1, \ldots, Z_m)$ is a polynomial over R_2.
- For any $x_1, \ldots, x_n, y \in R_2$, we have that

$$\begin{gathered}\exists z_1, \ldots, z_m \in R_2 : P(x_1, \ldots, x_n, y, z_1, \ldots, z_m) = 0 \\ \Downarrow \\ y \neq 0\end{gathered}$$

- $x \in R_1 \iff$

$$\begin{gathered}\exists a_1, \ldots, a_n, b, c_1, \ldots, c_m \in R_2 : x = \textstyle\sum_{i=1}^{n} \frac{a_i}{b}\omega_i \\ \text{AND} \\ P(a_1, \ldots, a_n, b, c_1, \ldots, c_m) = 0\end{gathered}$$

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

Diophantine Generation

Terminology and Notation

If all the conditions in the previous slide are satisfied

- we say that R_1 is Dioph-generated over R_2 and write $R_1 \leq_{Dioph} R_2$;

Diophantine Generation

Terminology and Notation

If all the conditions in the previous slide are satisfied

- we say that R_1 is Dioph-generated over R_2 and write $R_1 \leq_{Dioph} R_2$;
- we call the field F containing fraction fields of R_1 and R_2 a defining field;

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

Diophantine Generation

Terminology and Notation

If all the conditions in the previous slide are satisfied

- we say that R_1 is Dioph-generated over R_2 and write $R_1 \leq_{Dioph} R_2$;
- we call the field F containing the fraction fields of R_1 and R_2 a defining field;
- we call the basis Ω of F over F_2 a Diophantine basis of R_2 over R_1.

What's the point?

Why Diophantine Generation?

Diophantine definitions define a relation between a set and a subset, for example between a ring of characteristic 0 and $\mathbb{Z}$. When we construct a Diophantine definition we use elements of a bigger set to define (existentially) the elements of the smaller set. However we often deal with existentially definable relations going in the opposite direction: we use elements of a smaller set to define (existentially) elements of the bigger set. It is to produce a uniform description of both cases when we are dealing with the rings, that we introduce the notion of Diophantine generation.

Properties of Diophantine Generation

Assume that for some rings R_1 and R_2 we have that $R_1 \leq_{Dioph} R_2$.

- The defining field F can be any field containing F_1 and F_2. In particular, assuming we placed F_1 and F_2 within some algebraically closed field, we can let F be the compositum of F_1 and F_2.

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

Properties of Diophantine Generation

Assume that for some rings R_1 and R_2 we have that $R_1 \leq_{Dioph} R_2$.

- The defining field F can be any field containing F_1 and F_2. In particular, assuming we placed F_1 and F_2 within some algebraically closed field, we can let F be the compositum of F_1 and F_2.
- Any basis of any defining field F over F_2 is a Diophantine basis.

Diophantine Sets, Definitions and Generation

Diophantine Sets

Diophantine Generation

Properties of Diophantine Generation

Diophantine Family of $\mathbb{Z}$

Diophantine Family of a Polynomial Ring

Going Down

Horizontal and Vertical Problems

The Weak Vertical Method

Properties of Diophantine Generation

Assume that for some rings R_1 and R_2 we have that $R_1 \leq_{Dioph} R_2$.

- The defining field F can be any field containing F_1 and F_2. In particular, assuming we placed F_1 and F_2 within some algebraically closed field, we can let F be the compositum of F_1 and F_2.
- Any basis of any defining field F over F_2 is a Diophantine basis.
- If $R_1 \subset R_2$, then $R_1 \leq_{Dioph} R_2 \iff R_1$ has a Diophantine definition over R_2.

Properties of Diophantine Generation

Assume that for some rings R_1 and R_2 we have that $R_1 \leq_{Dioph} R_2$.

- The defining field F can be any field containing F_1 and F_2. In particular, assuming we placed F_1 and F_2 within some algebraically closed field, we can let F be the compositum of F_1 and F_2.
- Any basis of any defining field F over F_2 is a Diophantine basis.
- If $R_1 \subset R_2$, then $R_1 \leq_{Dioph} R_2 \iff R_1$ has a Diophantine definition over R_2.
- If $R_1 \leq_{Dioph} R_2$ and $R_2 \leq_{Dioph} R_3$ then $R_1 \leq_{Dioph} R_3$. Thus it makes sense to say that $R_1 \equiv_{Dioph} R_2$ if $R_1 \leq_{Dioph} R_2$ and $R_2 \leq_{Dioph} R_1$.

Properties of Diophantine Generation

Assume that for some rings R_1 and R_2 we have that $R_1 \leq_{Dioph} R_2$.

- The defining field F can be any field containing F_1 and F_2. In particular, assuming we placed F_1 and F_2 within some algebraically closed field, we can let F be the compositum of F_1 and F_2.
- Any basis of any defining field F over F_2 is a Diophantine basis.
- If $R_1 \subset R_2$, then $R_1 \leq_{Dioph} R_2 \iff R_1$ has a Diophantine definition over R_2.
- If $R_1 \leq_{Dioph} R_2$ and $R_2 \leq_{Dioph} R_3$ then $R_1 \leq_{Dioph} R_3$. Thus it makes sense to say that $R_1 \equiv_{Dioph} R_2$ if $R_1 \leq_{Dioph} R_2$ and $R_2 \leq_{Dioph} R_1$.
- If $R_1 \leq_{Dioph} R_2$ and HTP is undecidable over R_1, then HTP is undecidable over R_2.

Properties of Diophantine Generation

Going Up and then Down Property

Let $R_1 \subset R_2$ be rings and assume $R_2 \leq_{Dioph} R_1$. Then for any set $A \subset R_2$ such that A is Diophantine over R_2 we have that $A \cap R_1$ is Diophantine over R_1.

Properties of Diophantine Generation

Going Up and then Down Property

Let $R_1 \subset R_2$ be rings and assume $R_2 \leq_{Dioph} R_1$. Then for any set $A \subset R_2$ such that A is Diophantine over R_2 we have that $A \cap R_1$ is Diophantine over R_1.

Finite Intersection Property

Suppose R_1, R_2, R_3 are rings with $R_1 \subset R_3, R_2 \subset R_3, R_1 \leq_{Dioph} R_3$ and $R_2 \leq_{Dioph} R_3$. Then $R_1 \cap R_2 \leq_{Dioph} R_3$.

Properties of Diophantine Generation

Diophantine Generation of the Fraction Field

Let R be a ring and let F be its fraction field. Then $F \leq_{Dioph} R \iff$ the set of non-zero elements of R is Diophantine over R.

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

Properties of Diophantine Generation

Diophantine Generation of the Fraction Field

Let R be a ring and let F be its fraction field. Then $F \leq_{Dioph} R \iff$ the set of non-zero elements of R is Diophantine over R.

Proof

First suppose that $F \leq_{Dioph} R$. Then $F = \{\frac{a}{b} | a, b \in R \wedge \exists x_1, \ldots, x_m \in R : P(a, b, x_1, \ldots, x_m)\} = 0$, where $P(a, b, x_1, \ldots, x_m) = 0 \Rightarrow b \neq 0$. Then $P(1, Y, X_1, \ldots, X_m)$ is a Diophantine definition of the set of non-zero elements of R. Next assume the set of non-zero elements of R has a Diophantine definition $P(T, X_1, \ldots, X_m)$ over R. Then $F = \{\frac{a}{b} | a, b \in R \wedge \exists x_1, \ldots, x_m \in R : P(b, x_1, \ldots, x_m) = 0\}$.

Diophantine Sets, Definitions and Generation

Diophantine Sets

Diophantine Generation

Properties of Diophantine Generation

Diophantine Family of $\mathbb{Z}$

Diophantine Family of a Polynomial Ring

Going Down

Horizontal and Vertical Problems

The Weak Vertical Method

Properties of Diophantine Generation

Diophantine Generation of the Fraction Field

Let R be a ring and let F be its fraction field. Then $F \leq_{Dioph} R \iff$ the set of non-zero elements of R is Diophantine over R.

Proof

First suppose that $F \leq_{Dioph} R$. Then $F = \{\frac{a}{b} | a, b \in R \wedge \exists x_1, \ldots, x_m \in R : P(a, b, x_1, \ldots, x_m)\} = 0$, where $P(a, b, x_1, \ldots, x_m) = 0 \Rightarrow b \neq 0$. Then $P(1, Y, X_1, \ldots, X_m)$ is a Diophantine definition of the set of non-zero elements of R. Next assume the set of non-zero elements of R has a Diophantine definition $P(T, X_1, \ldots, X_m)$ over R. Then $F = \{\frac{a}{b} | a, b \in R \wedge \exists x_1, \ldots, x_m \in R : P(b, x_1, \ldots, x_m) = 0\}$.

Proposition

If R is any integrally closed subring of a global field and F is its fraction field, then $F \leq_{Dioph} R$. (Denef 1980, S. 1994)

Properties of Diophantine Generation

Diophantine Generation of Integral Closure

Let R_1 be a ring with a fraction field F_1. Assume $F_1 \leq_{Dioph} R_1$. Let F_2 be a finite extension of F_1 and let R_2 be the integral closure of R_1 in F_2. Then $R_2 \leq_{Dioph} R_1$.

Properties of Diophantine Generation

Diophantine Generation of Integral Closure

Let R_1 be a ring with a fraction field F_1. Assume $F_1 \leq_{Dioph} R_1$. Let F_2 be a finite extension of F_1 and let R_2 be the integral closure of R_1 in F_2. Then $R_2 \leq_{Dioph} R_1$.

Proof

Let $\{\omega_1, \ldots, \omega_n\}$ be a basis of F_2 over F_1. Now consider the set $\{y = \sum_{i=1}^{n} \frac{a_i}{b}\omega_i : b \neq 0 \wedge \exists b_{n-1}, \ldots, b_0 \in R_1 : y^n + b_{n-1}y^{n-1} + \ldots + b_0 = 0\}$.

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

A Project

Diophantine Family of $\mathbb{Z}$

Integrally closed subrings of finite extensions of $\mathbb{Q}$

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

A Project

Diophantine Family of $\mathbb{Z}$

Integrally closed subrings of finite extensions of $\mathbb{Q}$

A Problem

Describe the structure of the Diophantine classes of the Diophantine family of $\mathbb{Z}$.

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

A Project

Diophantine Family of $\mathbb{Z}$

Integrally closed subrings of finite extensions of $\mathbb{Q}$

A Problem

Describe the structure of the Diophantine classes of the Diophantine family of $\mathbb{Z}$.

First Questions

- Do we know whether the rings of the Diophantine family of $\mathbb{Z}$ are in more than one class?
- Do we have examples of classes with more than one element?

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

Members of the Family of $\mathbb{Z}$

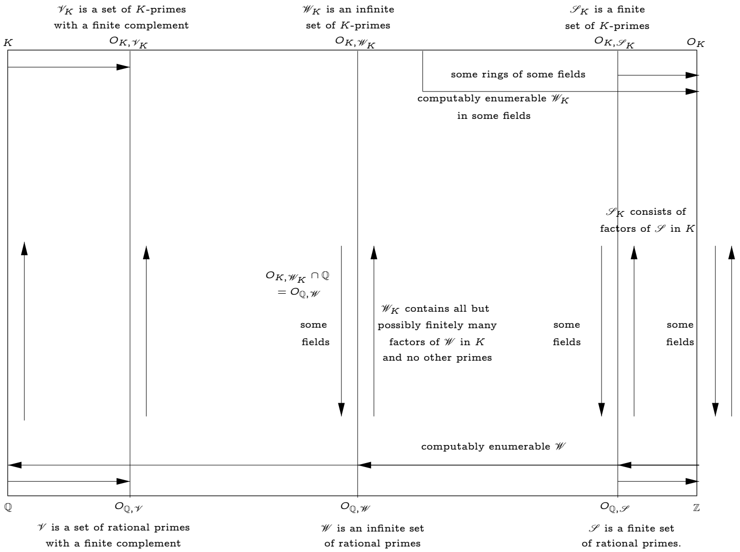
Definition

Let K be a number field and let $\mathcal{S}$ be a set of (non-archimedean) primes of K. Let $O_{K,\mathcal{S}}$ be the following subring of K.

$$\{x \in K : \operatorname{ord}_{\mathfrak{p}} x \geq 0 \ \forall \mathfrak{p} \notin \mathcal{S}\}$$

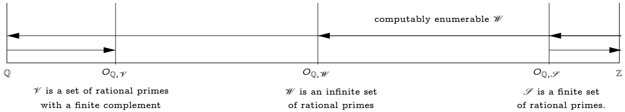
If $\mathcal{S} = \emptyset$, then $O_{K,\mathcal{S}} = O_K$. If $\mathcal{S}$ contains all the primes of K, then $O_{K,\mathcal{S}} = K$. If $\mathcal{S}$ is finite, we call the ring small. If $\mathcal{S}$ is infinite, we call the ring large.

What We Know about the Diophantine Family of $\mathbb{Z}$.



Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

Things Below



What is Dioph-generated over $\mathbb{Z}$?

Let $\mathcal{W}$ be any set of primes of $\mathbb{Q}$. Then from the MRDP Theorem we know that $O_{\mathbb{Q},\mathcal{W}} \leq_{Dioph} \mathbb{Z} \iff \mathcal{W}$ is r.e. Indeed, let $\mathcal{W}$ be any r. e. set of rational primes. Then the set D of all integers which are products of primes in $\mathcal{W}$ is also r.e. Further, since every r.e. subset of $\mathbb{Z}$ is Diophantine, for some polynomial $P(T, \bar{X})$ over $\mathbb{Z}$, for all $t, \bar{x}$ in $\mathbb{Z}$ we have that $P(t, \bar{x}) = 0 \iff t \in D$. Thus, $O_{\mathbb{Q},\mathcal{W}} = \{\frac{m}{d} : m \in \mathbb{Z} \wedge \exists \bar{x} P(d, \bar{x}) = 0\}$. Conversely, if $O_{\mathbb{Q},\mathcal{W}} \leq_{Dioph} \mathbb{Z}$. Then $O_{\mathbb{Q},\mathcal{W}} = \{\frac{m}{d} : \exists \bar{y} Q(m, d, \bar{y}) = 0\}$, where $Q(m, d, \bar{y})$ is a polynomial over $\mathbb{Z}$ and $\bar{y}$ takes values in $\mathbb{Z}$. Consider all the possible values of d such that there exists $\bar{y}$ with $Q(1, d, \bar{y}) = 0$. The set of all such d's is r.e. and therefore the set of all the prime factors of d's is also r.e.

How Many Diophantine Classes?

More Than One Class

Since not all sets of primes are r.e., it follows that there exists more than one Diophantine class.

How Many Diophantine Classes?

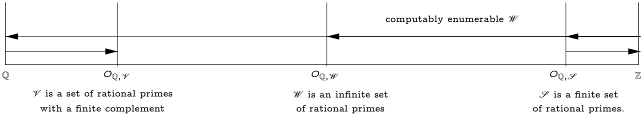
More Than One Class

Since not all sets of primes are r.e., it follows that there exists more than one Diophantine class.

Infinitely Many Diophantine Classes

Using the fact that Diophantine Generation implies relative enumerability and there are infinitely many enumerability classes (or partial degrees), we can show that there are infinitely many Diophantine classes.

More Things Below



Lemma

Let K be a number field and let $\mathcal{S}_K$ be a finite set of primes of K. Let $\mathcal{W}_K$ be any set of primes of K. Then $O_{K,\mathcal{W}_K} \leq_{Dioph} O_{K,\mathcal{W}_K \cup \mathcal{S}_K}$ (Julia Robinson and others).

More Than One Element in a Class

If we combine this lemma with what we know about Diophantine Generation over $\mathbb{Z}$, we will conclude that for any finite set of $\mathbb{Q}$-primes $\mathcal{S}$ we have that $O_{K,\mathcal{S}} \equiv_{Dioph} \mathbb{Z}$. Taking into account that the set of non-zero elements is Diophantine over any ring $O_{\mathbb{Q},\mathcal{V}}$, we also conclude that if $\mathcal{V}$ contains all but finitely many primes of $\mathbb{Q}$, we have that $\mathbb{Q} \equiv_{Dioph} O_{\mathbb{Q},\mathcal{V}}$.

Small Members of the Number Field Family.

Theorem

$\mathbb{Z} \equiv_{Dioph} O_K$ *for the following number fields* K*:*

- *Extensions of degree 4, totally real number fields (i.e. finite extensions of* $\mathbb{Q}$ *all of whose embeddings into* $\mathbb{C}$ *are real) 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 2002, Poonen, S. 2003)*
- *Any number field* K *such that there exists an elliptic curve of rank 1 over* K *and an Abelian variety of positive rank over* $\mathbb{Q}$ *keeping its rank over* K*. (Cornelissen, Pheidas, Zahidi, 2005)*

Big Members of the Number Field Family

Theorem

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

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

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

- *The natural density of $\mathcal{S}$ is greater $1 - \dfrac{1}{[K : \mathbb{Q}]} - \varepsilon$.*
- $\mathbb{Z} \equiv_{Dioph} O_K \equiv_{Dioph} O_{K,\mathcal{S}}$.

(S. 2002, 2003, 2006)

Note that this result says nothing about subrings of $\mathbb{Q}$.

Just One of the Unanswered Questions

Is $\mathbb{Z} \equiv_{Dioph} \mathbb{Q}$?

Since we know that $\mathbb{Q} \leq_{Dioph} \mathbb{Z}$, we "just" need to determine whether $\mathbb{Z} \leq_{Dioph} \mathbb{Q}$ or, in other words, whether $\mathbb{Z}$ has a Diophantine definition over $\mathbb{Q}$.

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

Another Project

Diophantine Family of a Polynomial Ring over a Finite Constant Field

All the integrally closed subrings of finite extensions and subextensions of $\mathbb{F}_p(t)$ – a function field over a finite field of characteristic $p > 0$.

A Problem

Describe the structure of the Diophantine classes of the Diophantine family of $\mathbb{F}_p[t]$.

Members of the Family of $\mathbb{F}_p[t]$

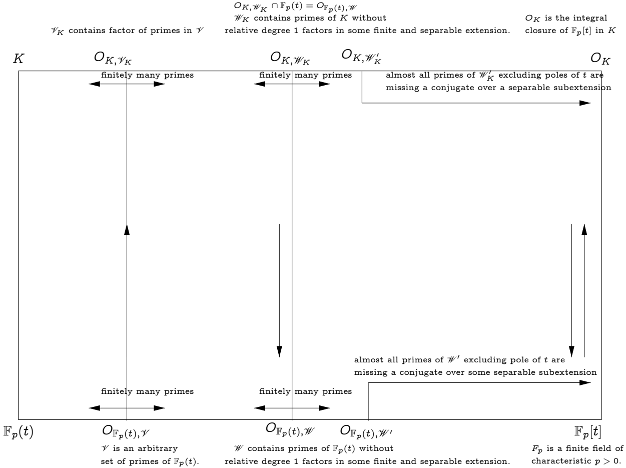
Definition

Let K be a function field over a finite field of constants and let $\mathcal{S}$ be a set of its primes. Let $O_{K,\mathcal{S}}$ be the following subring of K.

$$\{x \in K : \operatorname{ord}_{\mathfrak{p}} x \geq 0 \ \forall \mathfrak{p} \notin \mathcal{S}\}$$

Here $\mathcal{S} \neq \emptyset$ or the ring will contain only constants. If $\mathcal{S}$ contains all the primes of K, then $O_{K,\mathcal{S}} = K$. If $\mathcal{S}$ is finite, we call the ring small. If $\mathcal{S}$ is infinite, we call the ring large.

What We Know about the Diophantine Family of $\mathbb{F}_p[t]$.



Diophantine Generation, Horizontal and Vertical Problems, and the Weak Vertical Method

Alexandra Shlapentokh

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

Invariance of a Diophantine Class and Finite Sets of Primes

Theorem

Let K be a global function field and let $\mathfrak{p}$ be a prime of K. Then the set of elements of K integral at $\mathfrak{p}$ is Diophantine over K. (Rumely, 1980, S. 1994, 2000)

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

Invariance of a Diophantine Class and Finite Sets of Primes

Theorem

Let K be a global function field and let $\mathfrak{p}$ be a prime of K. Then the set of elements of K integral at $\mathfrak{p}$ is Diophantine over K. (Rumely, 1980, S. 1994, 2000)

Theorem

Let K be a global function field of characteristic $p > 0$. Then the set $\{(x, x^{p^s}), s \in \mathbb{Z}_{\geq 0}, x \in K\}$ is Diophantine over K. (Pheidas for rational fields and $p > 2$, 1991; Videla for rational field and $p = 2$, 1994; S. function fields, $p > 2$, 1996; Eisenträger, function fields, $p = 2$, 2001.)

Invariance of a Diophantine Class and Finite Sets of Primes

Theorem

Let K be a global function field and let $\mathfrak{p}$ be a prime of K. Then the set of elements of K integral at $\mathfrak{p}$ is Diophantine over K. (Rumely, 1980, S. 1994, 2000)

Theorem

Let K be a global function field of characteristic $p > 0$. Then the set $\{(x, x^{p^s}), s \in \mathbb{Z}_{\geq 0}, x \in K\}$ is Diophantine over K. (Pheidas for rational fields and $p > 2$, 1991; Videla for rational fields and $p = 2$, 1994; S. function fields, $p > 2$, 1996; Eisenträger, function fields, $p = 2$, 2001.)

Corollary

Let K be a global function field of characteristic $p > 0$. Let $\mathcal{S}_1, \mathcal{S}_2$ be two sets of primes of K such that $(\mathcal{S}_1 \setminus \mathcal{S}_2) \cup (\mathcal{S}_2 \setminus \mathcal{S}_1)$ is a finite set. Then $O_{K,\mathcal{S}_1} \equiv_{Dioph} O_{K,\mathcal{S}_2}$. (S. 1996)

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

Diophantine Equivalence of the Small Members of the Function Field Family

Theorem

Let K_2/K_1 be a finite extension of function fields of characteristic $p > 0$ over finite fields of constants. Let $\mathcal{S}_2, \mathcal{S}_1$ be finite non-empty sets of primes of K_2 and K_1 respectively. Then $O_{K_2,\mathcal{S}_2} \equiv_{Dioph} O_{K_1,\mathcal{S}_1}$. (S. 1993)

Diophantine Generation over Big Members of the Function Field Family

Theorem

Let K be a function field over a finite field of constants. Let $\mathcal{S}$ be a finite set of primes of K. Let $\varepsilon > 0$ be given. Then there exists a set $\mathcal{W}$ of primes of K such that the Dirichlet density of $\mathcal{S}$ is greater ε and $O_{K,\mathcal{S}} \leq_{Dioph} O_{K,\mathcal{W}}$.(S. 1998, 2002)

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

Diophantine Generation over Big Members of the Function Field Family

Theorem

Let K be a function field over a finite field of constants. Let $\mathcal{S}$ be a finite set of primes of K. Let $\varepsilon > 0$ be given. Then there exists a set $\mathcal{W}$ of primes of K such that the Dirichlet density of $\mathcal{S}$ is greater ε and $O_{K,\mathcal{S}} \leq_{Dioph} O_{K,\mathcal{W}}$.(S. 1998, 2002)

Corollary

Let $\mathbb{F}_p$ be a finite field of characteristic $p > 0$. Let t be transcendental over $\mathbb{F}_p$. Then for any $\varepsilon > 0$ there exists a set $\mathcal{W}$ of primes of $\mathbb{F}_p(t)$ (irreducible polynomials) of Dirichlet density greater than $1 - \varepsilon$ such that $F_p[t] \leq_{Dioph} O_{\mathbb{F}_p(t),\mathcal{W}}$.

Diophantine Sets, Definitions and Generation

Diophantine Sets

Diophantine Generation

Properties of Diophantine Generation

Diophantine Family of $\mathbb{Z}$

Diophantine Family of a Polynomial Ring

Going Down

Horizontal and Vertical Problems

The Weak Vertical Method

Horizontal and Vertical Problems

Horizontal Problems

Given two rings R_1 and R_2 from the Diophantine family of $\mathbb{Z}$, we will call the problem of determining the relation between their Diophantine classes horizontal if $R_1 \subset R_2$ and they have the same fraction field.

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

Horizontal and Vertical Problems

Horizontal Problems

Given two rings R_1 and R_2 from the Diophantine family of $\mathbb{Z}$, we will call the problem of determining the relation between their Diophantine classes horizontal if $R_1 \subset R_2$ and they have the same fraction field.

Vertical Problem

Suppose F_2, the fraction field of R_2, is a non-trivial finite extension of F_1, the fraction field of R_1. Then we will call the corresponding problem concerning Diophantine classes of R_1 and R_2 vertical.

The Weak Vertical Method

The Main Idea

If an *element above* is equivalent to an *element below* modulo sufficiently *large element below*, then the *element above* is really *below*.

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

The Weak Vertical Method

The Main Idea

If an *element above* is equivalent to an *element below* modulo sufficiently *large element below*, then the *element above* is really *below*.

Ingredients of the Weak Vertical Method

- An equation whose solutions above are really below and also such that we can manufacture integers out of its solutions. (Norm equations and elliptic curves have been used to construct such equations.)
- Bound equations. (Quadratic forms and divisibility have been used to construct the bounds.)

Diophantine Sets, Definitions and Generation
Diophantine Sets
Diophantine Generation
Properties of Diophantine Generation
Diophantine Family of $\mathbb{Z}$
Diophantine Family of a Polynomial Ring
Going Down
Horizontal and Vertical Problems
The Weak Vertical Method

An Example

Proposition

Let K/F be a number field extension with a basis $\Lambda = \{1, \alpha, \ldots, \alpha^{m-1}\} \subset O_K$. Let $x \in O_K, w, y \in O_F$. Assume that y is not zero and is not an integral unit. Let $c \in \mathbb{Z}_{>0}$ be fixed, let $n = [K : \mathbb{Q}]$. Suppose that the following equalities and inequalities hold.

$$x = \sum_{i=0}^{m-1} a_i \alpha^i, a_i \in F, \tag{2}$$

$$|\mathbf{N}_{K/\mathbb{Q}}(Da_i)| \leq |\mathbf{N}_{K/\mathbb{Q}}(y)^c|, \tag{3}$$

where D is the discriminant of Λ, and

$$x \equiv w \mod y^{2c}. \tag{4}$$

Then $x \in O_F$.

An Example

Proof.

From (2) and (4), we conclude that

$$x - w = (a_0 - w) + a_1\alpha + \ldots + a_{n-1}\alpha^{m-1} \equiv 0 \mod y^{2c}.$$

Thus,

$$\frac{x-w}{y^{2c}} = \frac{a_0 - w}{y^{2c}} + \frac{a_1}{y^{2c}}\alpha + \ldots + \frac{a_{m-1}}{y^{2c}}\alpha^{m-1} \in O_K.$$

We have that $\frac{Da_i}{y^{2c}} \in O_F$, and therefore $|\mathbf{N}_{K/\mathbb{Q}}(Da_i)| \geq \mathbf{N}_{K/\mathbb{Q}}(y^{2c})$ or $|\mathbf{N}_{K/\mathbb{Q}}(a_i)| = 0$. At the same time from (3) we conclude that

$$|\mathbf{N}_{K/\mathbb{Q}}(Da_i)| \leq |\mathbf{N}_{K/\mathbb{Q}}(y)|^c < \mathbf{N}_{K/\mathbb{Q}}(y)^{2c},$$

since y is not an integral unit. Hence, for $i = 1, \ldots, m$, we have that $|\mathbf{N}_{K/\mathbb{Q}}(a_i)| = 0$, and therefore $a_i = 0$, for $i = 1, \ldots, m-1$. Consequently, $x \in O_F$. □

Diophantine Sets, Definitions and Generation

Diophantine Sets

Diophantine Generation

Properties of Diophantine Generation

Diophantine Family of $\mathbb{Z}$

Diophantine Family of a Polynomial Ring

Going Down

Horizontal and Vertical Problems

The Weak Vertical Method