Hilbert's Tenth Problem

Peter Mayr

Computability Theory, March 3, 2021

Diophantine sets

The following is based on

- M. Davis. Hilbert's Tenth Problem is unsolvable. The American Mathematical Monthly, Vol. 80, No. 3 (Mar., 1973), pp. 233-269.

Departing from our usual convention let $\mathbb{N} = \{1, 2, \dots\}$ here.

Definition

$A \subseteq \mathbb{N}^k$ is **Diophantine** if there exists a polynomial $f(\underbrace{x_1, \dots, x_k}_{\bar{x}}, \underbrace{y_1, \dots, y_\ell}_{\bar{y}}) \in \mathbb{Z}[\bar{x}, \bar{y}]$ such that

$$\bar{x} \in A \text{ iff } \exists \bar{y} \in \mathbb{N}^\ell \; f(\bar{x}, \bar{y}) = 0.$$

Examples of Diophantine sets

- composite numbers: $\{x \in \mathbb{N} \;:\; \exists y_1, y_2 \; x = (y_1 + 1)(y_2 + 1)\}$
- order relation: $x_1 \leq x_2$ iff $\exists y \; x_1 + y - 1 = x_2$

Diophantine functions

Definition

A partial function $f : \mathbb{N}^k \to_p \mathbb{N}$ is **Diophantine** if its graph

$$\{(\bar{x}, f(\bar{x})) \ : \ \bar{x} \in \mathrm{domain}\, f\}$$

is Diophantine.

Example

Polynomial functions $\{(\bar{x}, y) \ : \ y = p(\bar{x})\}$ are Diophantine.

Encoding tuples

Other Diophantine functions are harder to construct.
E.g. there is an encoding of k-tuples into natural numbers with Diophantine inverse:

Lemma (Sequence Number Theorem)

There is a Diophantine function $S(i, u)$ such that

- $S(i, u) \leq u$ and
- $\forall k \in \mathbb{N} \, \forall (a_1, \ldots, a_k) \in \mathbb{N}^k \, \exists u \in \mathbb{N} \, \forall i \leq k : \; S(i, u) = a_i$

Proof.

Omitted. □

The crucial lemma

Lemma

The exponential function $h(n, k) := n^k$ is Diophantine.

Proof.

Analysis of Diophantine equations starting from the Pell equation

$$x^2 - dy^2 = 1$$
$$d = a^2 - 1 \ (a > 1)$$

Details omitted. □

Corollary

The following are Diophantine:

$$\binom{n}{k}, \quad n!, \quad \prod_{i=1}^{z}(x + yi)$$

Closure of Diophantine predicates

Lemma

The class of Diophantine predicates is closed under $\wedge, \vee$, existential quantifiers and bounded universal quantifiers.

Proof.

- **Conjunction:** $\exists \bar{y}\ f(\bar{x}, \bar{y}) = 0 \wedge \exists \bar{z}\ g(\bar{x}, \bar{z}) = 0$
  $$\equiv \exists \bar{y}, \bar{z}\ f(\bar{x}, \bar{y})^2 + g(\bar{x}, \bar{z})^2 = 0$$
- **Disjunction:** $\exists \bar{y}\ f(\bar{x}, \bar{y}) = 0 \vee \exists \bar{z}\ g(\bar{x}, \bar{z}) = 0$
  $$\equiv \exists \bar{y}, \bar{z}\ f(\bar{x}, \bar{y}) \cdot g(\bar{x}, \bar{z}) = 0$$
- **Existential quantifier:** immediate
- **Bounded universal quantifiers:** $\forall z < k\, \exists \bar{y}\ f(\bar{x}, z, \bar{y}) = 0$
  Substantially harder, uses that $\prod_{i=1}^{k}(x + yi)$ is Diophantine.

□

Example

Primes are Diophantine:
x is prime iff $x > 1 \wedge \forall y, z < x\ [yz < x \vee yz > x \vee y = 1 \vee z = 1]$

Diophantine = recursive

Theorem
A partial function is Diophantine iff it is recursive.

Proof.
$\Rightarrow$: The graph of a Diophantine function f is of the form

$$\{(\bar{x}, y) \ : \ \exists \bar{z} \ p(\bar{x}, y, \bar{z}) = 0\}$$

for a polynomial p with integer coefficients, hence c.e.
Thus f is computable (=recursive).

$\Leftarrow$: Show recursive functions are Diophantine by induction.

Base case: Clearly successor and projections are Diophantine.

Induction step: Show that the class of Diophantine functions is closed under composition, primitive recursion, and search μ.

Composition: If $g, h_1, \ldots, h_k$ are Diophantine, then so is

$$f(\bar{x}) := g(h_1(\bar{x}), \ldots, h_k(\bar{x}))$$

since

$$y = f(\bar{x}) \text{ iff } \exists y_1, \ldots, y_k \, [y_1 = h_1(\bar{x}) \wedge \cdots \wedge y_k = h_k(\bar{x}) \wedge y = g(y_1, \ldots, y_k)]$$

Search μ: If $g(\bar{x}, y)$ is Diophantine, then so is

$$f(\bar{x}) := \min\{y \ : \ g(\bar{x}, y) = 0 \text{ and } (\bar{x}, t) \in \mathrm{domain}\, g \ \forall t \leq y\}$$

since

$$y = f(\bar{x}) \text{ iff } g(\bar{x}, y) = 0 \ \wedge \ \forall t \leq y \, \exists u \; g(\bar{x}, t) = u \neq 0.$$

Primitive recursion: For g, h Diophantine, define f by

$$f(\bar{x}, 1) := g(\bar{x})$$
$$f(\bar{x}, y+1) := h(\bar{x}, y, f(\bar{x}, y))$$

Idea: Encode $f(\bar{x}, 1), \ldots, f(\bar{x}, y)$ as some $u \in \mathbb{N}$ by the Sequence Number Theorem.

Then f is Diophantine since $z = f(\bar{x}, y)$ iff

$$\begin{aligned} \exists u \;\; [&S(1, u) = g(\bar{x}) \wedge \\ &\forall t < y \; S(t+1, u) = h(\bar{x}, y, S(t, u)) \wedge \\ &z = S(y, u)]. \end{aligned}$$

□

Hilbert's Tenth Problem is not solvable

MRDP-Theorem (Matiyasevich, Robinson, Davis, Putnam)

$A \subseteq \mathbb{N}$ is diophantine iff it is c.e.

Proof

$\Rightarrow$: immediate from definition

$\Leftarrow$: Assume A is c.e.

- Then we have a computable function f such that

$$A = \{x \in \mathbb{N} \ : \ \exists y \ f(x,y) = 0\}.$$

- Since f is Diophantine, the binary predicate $f(x,y) = 0$ is Diophantine.
- Thus A is Diophantine. $\square$

Corollary

There exists a polynomial $f(x, \bar{y}) \in \mathbb{Z}[x, \bar{y}]$ for which

$$\{x \in \mathbb{N} \ : \ \exists \bar{y} \in \mathbb{N}^{\ell} \ f(x, \bar{y}) = 0\}$$

is not computable.

Note

- Hence given a polynomial p over $\mathbb{Z}$, it is not decidable whether p has roots in $\mathbb{N}$.
- By a Theorem of Lagrange, every $n \in \mathbb{N}$ is the sum of 4 squares.
- Hence $p(y_1, \dots, y_\ell) = 0$ has solutions in $\mathbb{N}$ iff

  $$p(1 + a_1^2 + b_1^2 + c_1^2 + d_1^2, \dots, 1 + a_\ell^2 + b_\ell^2 + c_\ell^2 + d_\ell^2) = 0$$

  has solutions in $\mathbb{Z}$.
- Thus it is not decidable whether polynomials over $\mathbb{Z}$ have integer roots either.

Concluding remarks

1. Given a DTM that accepts $A \subseteq \mathbb{N}$, one can construct a polynomial f over $\mathbb{Z}$ such that

$$x \in A \text{ iff } \exists \bar{y} \in \mathbb{N}^{\ell}\ f(x, \bar{y}) = 0,$$

   and conversely.
2. Each Diophantine set can be defined with a polynomial of total degree ≤ 4 (arbitrary number of variables).
3. Each Diophantine set in $\mathbb{N}$ can be defined with a polynomial of ≤ 15 variables.
4. **Gödel's First Incompleteness Theorem:** For each consistent axiomatization Σ of arithmetic on $\mathbb{N}$, there exists a polynomial $f(\bar{x}) \in \mathbb{Z}[\bar{x}]$ without roots over $\mathbb{N}$ but such that

$$\forall \bar{x} : f(x) \neq 0$$

   is not provable from Σ.
   [Suppose otherwise. Since a DTM can enumerate all consequences of Σ, then also all polynomials without roots. Contradiction.]