1 H10 and Diophantine Set

Let $A \subset \mathbb{Z}$, consider the membership problem: given $n \in \mathbb{Z}$, is n in A?

Definition 1. A is computable $\iff$ there is an algorithm to determine membership in A.

Definition 2. A is listable $\iff$ there is a program that prints out exactly the elements of A.

Remark 1. computable $\implies$ listable.

Example 1. The set of primes is computable.

$\{x^3 + y^3 + z^3 : x, y, z \in \mathbb{Z}\}$ is listable. But it is unknown if it is computable.

Theorem 1 (1936)**.** *There exists a listable $A \subseteq \mathbb{N}$ which is not computable.*

Proof. Consider $\{2^p 3^x : \text{program } p \text{ halts on input } x\}$

This is listable: run all p on all x, in parallel. Print $2^p 3^x$ whenever it halts.

This is however not computable, since testing membership in A is equivalent to asking the halting problem. □

Definition 3 (Hilbert 10th Problem)**.** Input $f \in \mathbb{Z}[X_1, ..., X_n]$. Does there exist $\underline{x} \in \mathbb{Z}^n$ such that $f(\underline{x}) = 0$?

The end goal is to prove that there does not exists an algorithm to answer H10. But in this note, we make a simplification: it is enough to show that there is no algorithm, that when we input $f \in \mathbb{Z}[X_1, \ldots, X_n]$, outputs whether this function has a positive solution.

This is enough, because suppose there is an algorithm to test for integer solutions. Then we can simply take any $f(X_1, \ldots, X_n)$ and replace all occurrences of X_i with $1 + {A_i}^2 + B_i^2 + C_i^2 + D_i^2$, and look for solutions in A_i, B_i, C_i, D_i. There is a algorithm implies there is an algorithm to detect positive integers.

Therefore, in what follows, unless otherwise stated, we are working with positive integers.

Now we make an important definition. Suppose instead of asking for roots (like in H10), we instead suppose there is a root and ask what coefficients the polynomial can have.

Definition 4. A set $A \subseteq \mathbb{N}^m$ is Diophantine if there is a polynomial $p \in \mathbb{Z}[A_1, \ldots A_n, X_1, ..., X_m]$, such that $A = \{\underline{x} \in \mathbb{N} : \exists \underline{y}\, p(\underline{x}, \underline{y}) = 0\}$

Definition 5. A function $f : \mathbb{N}^m \to \mathbb{N}^n$ is Diophantine if its graph is a Diophantine set, i.e. if

$$\{x_1, \ldots, x_m, y_1, \ldots, y_n \mid \underline{y} = f(x_1, \ldots, x_m)\}$$

is a Diophantine set. Similarly define a Diophantine relation on the natural numbers.

Remark 2. These definitions are originally made in the general form, as subsets of the integers.

Theorem 2 (Davis, Putnam, Robinson, Matiyasevich 1970 [Mat93])**.** *$A \subseteq \mathbb{N}^m$ is Diophantine $\iff$ A is listable.*

Theorem 2 has the following consequence:

Corollary 1. *H10 is undecidable.*

In this note we give the idea of the proof of Theorem 2, following [Dav73].

2 Examples of Diophantine Sets

1. $\{x, y \in \mathbb{N} : x \mid y\}$ is Diophantine: $x \mid y \iff \exists d\ x = yd$. Alternatively write $x \mid y$ is Diophantine.
2. The composite numbers: x composite $\iff \exists y, z :\ x = (y + 1)(z + 1)$.
3. The intersection of two Diophantine sets is Diophantine: suppose
$$S_1 = \{\underline{x} \in \mathbb{N}^m \mid \exists \underline{y}\ f_1(\underline{x}, \underline{y}) = 0\}$$
$$S_2 = \{\underline{x} \in \mathbb{N}^m \mid \exists \underline{z}\ f_2(\underline{x}, \underline{z}) = 0\}$$
Then
$$S_1 \cap S_2 = \{\underline{x} \in \mathbb{N}^m \mid \exists \underline{y}, \underline{z}, f_1(\underline{x}, \underline{y})^2 + f_2(\underline{x}, \underline{z})^2 = 0\}$$
4. The union of two Diophantine sets is Diophantine. Let S_1, S_2 be defined as above. Then
$$S_1 \cup S_2 = \{\underline{x} \in \mathbb{N}^m \mid \exists \underline{y}, \underline{z}, f_1(\underline{x}, \underline{y}) \cot f_2(\underline{x}, \underline{z}) = 0\}$$
5. $x < y$ is a Diophantine equation: $x < y \iff \exists z \in \mathbb{N}, y = x + z$.
6. $y = \lfloor x \rfloor$, $x \pmod y$ are Diophantine relations.

2.1 Exponential Function

Is the function $h(n,k) = n^k$ Diophantine?

Historically this is a very important question. It is positive answer of this problem by Matiyasevich that led to the negative answer of H10. We will give the idea of the proof next week.

As an important consequence, we now have that binomial coefficient $\binom{n}{k}$ and the factorial are both Diophantine.

2.2 Bounded Operators

In this section, we will use what we have proved to show the following lemma about bounded operators:

Lemma 1. *If P is a polynomial, then both of the following sets are Diophantine:*

$$R = \left\{ \langle y, \underline{x} \rangle \} \mid (\exists k)_{k \leq y} (\exists y_1, \ldots, y_m) \left[P(y, k, \underline{x}, \underline{y}) = 0 \right] \right\}$$

$$S = \left\{ \langle y, \underline{x} \rangle \} \mid (\forall k)_{k \leq y} (\exists y_1, \ldots, y_m) \left[P(y, k, \underline{x}, \underline{y}) = 0 \right] \right\}$$

That R is Diophantine is trivial. Here, we prove that a simplified form of S is Diophantine:

Claim 1. *The following set is Diophantine:*

$$S = \{ \langle y, \underline{x} \rangle \mid (\forall k)_{k \leq y} \, P(y, k, \underline{x}) = 0 \}$$

First of all, we define a notion of a polynomial Q being much bigger than P:

Definition 6. We say polynomial Q dominates polynomial P if

1. $Q(y, x_1, \ldots, x_n) > y$
2. For all $k \leq y$, $|P(y, k, x_1, \ldots, x_n)| \leq Q(y, x_1, \ldots, x_n)$

The idea is the following:

Claim 2. *Fix y, take a polynomial Q that completely dominates P. Then:*

$$(\forall k)_{k \leq y} \, P(y, k, \underline{x}) = 0 \iff$$
$$(\exists c, t) \left[1 + ct = \prod_{k=1}^{y} (1 + kt) \right] \wedge t = Q(y, \underline{x})! \wedge P(y, c, \underline{x}) \equiv 0 \pmod{1 + ct}$$

The idea behind the claim is that take any prime $p_k \mid (1 + kt)$, then $1 + kt \equiv 1 + ct \equiv 0 \pmod{p_k}$ and so $k \equiv c \pmod{p_k}$. It follows that $P(y, c, \underline{x}) \equiv P(y, k, \underline{x}) \equiv 0 \pmod{p_k}$

But since $p_k \nmid kt$ and t is huge, p_k must also be huge. So the previous equivalence gives $P(y, k, \underline{x}) = 0$.

Proof of Claim 1. First suppose $p_k \mid (1 + kt)$. Then $1 + ck \equiv 1 + kt \pmod{p_k}$, so $k \equiv c \pmod{p_k}$, and $P(y, k, \underline{x}) \equiv P(y, c, \underline{x}) \pmod{p_k}$.

However, $t = Q(y, \underline{x})!$, so every divisor of $1 + kt$ is bigger than $Q(y, u, \underline{x})$. In particular, this means $p_k > Q(y, \underline{x}) > P(y, k, \underline{x})$.

Therefore we have $P(y, k, \underline{x}) = 0$ for all $k \leq y$.

($\implies$) That there exists a polynomial Q that dominates P is easy to see. Suppose that $\forall k \leq y, P(y, k, \underline{x}) = 0$. Let $t = Q(y, \underline{x})!$. Since $\prod_{k=1}^{y} (1 + kt) \equiv 1 \pmod{t}$, there exists some $c \in \mathbb{N}$ such that $1 + ct = \prod_{k=1}^{y} (1 + kt)$.

For this value of c, $1 + ct \equiv 1 + kt \equiv 0 \pmod{1 + kt}$, so $k \equiv c \pmod{1 + kt}$, hence $P(y, c, \underline{x}) = P(y, k, \underline{x}) = 0 \pmod{1 + kt}$.

Now we attempt to use the Chinese Remainder Theorem to finish the proof:

Claim 3. *For all $l \neq k \leq y$, $1 + ly$ and $1 + ky$ are coprime.*

Proof. Suppose $p \mid 1 + lt$ and $p \mid 1 + kt$. Then because of the choice of t, $p > Q(y, \underline{x})$. However, $p \mid (1 + lt) - (1 + kt) = t(l - p)$, so $p \mid (l - k)$. But $|l - k| < y < Q(y, \underline{x})$, contradiction. □

So now, by CRT, we have that $P(y, c, \underline{x}) = P(y, k, \underline{x}) = 0 \pmod{1 + ct}$. □

2.3 Sequential Number Theorem

As a final proof that Diophantine functions can be very powerful, we present without proof the Sequence Number Theorem:

Theorem 3 (Sequence Number Theorem)**.** *There is a Diophantine function $S(i,u)$ such that*

1. *$S(i,u) \leq u$*
2. *For any sequence of natural numbers $a_1, \ldots, a_n$, there is $u \in \mathbb{N}$ such that $S(i,u) = a_i$ for all i.*

So the function S has the power to encode any sequence of numbers. This is a very useful theorem, in this abbreviated note we will use it once.

3 Recursive Function

We now define an alternative concept to computability:

Definition 7 (Recursive Function)**.** Recursive functions are all those functions obtainable from the initial functions:

$$c(x) = 0; \quad s(x) = x + 1; \quad U_i^n(x_1, \ldots, x_n) = x_i$$

Then iteratively applying the following functions:

1. **Composition:** $h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_n(x_1, \ldots, x_n))$
2. **Primitive Recursion:** yields function $h(x_1, ..., x_n, z)$ such that

$$h(x_1, x_2, \ldots, 1) = f(x_1, \ldots, x_n)$$
$$h(x_1, x_2, \ldots, t+1) = g(t, h(x_1, x_2, \ldots, t), x_1, ..., x_n)$$

3. **Minimilization**[1]: Given function y, yields function

$$h(x_1, \ldots, x_n) = \min_y (f(x_1, \ldots, x_n, y) = 0)$$

(assuming that for all tuples $\underline{x}$ we must have a y that satisfy $f(\underline{x}, y)$. If not, then the function is left undefined.)

Example 2.

1. For $x, y \in \mathbb{N}$, $x + y$, is partially recursive:

$$x + 1 = s(x)$$
$$x + (t+1) = s(x+t) = g(t, x+t, x)$$

where $g(u, v, w) = s(v)$. Finish using primitive recursion.

2. For $x, y \in \mathbb{N}$, $x \cdot y$ is recursive because

$$x \cdot 1 = U_1^1(x)$$
$$x(t+1) = xt + x = g(t, xt, x)$$

where $g(u, v, w) = v + w$, which we have already shown to be recursive.

3. All the constant functions $c(x) = k$, for $k \geq 0$.
4. All polynomials $P(x_1, \ldots, x_n)$ with positive integer coefficients.

Fact (Church-Turing): Partially recursive functions are identical to the set of functions that are Turing computable.

Theorem 4. *A function is Diophantine if and only if it is recursive.*

[1] Also known as unbounded operator, or μ-operator.

Proof. We will here show the converse in detail.

To obtain the converse: it is enough to show that e Diophantine functions are closed under composition, primitive recursion and minimalization.

Composition: suppose $h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_m(x_1, \ldots, x_n))$. Then

$$y = h(x_1 \ldots, x_n) \iff \exists (t_1, \ldots, t_n) \left(t_i = g_i(\underline{x}) \wedge y = f(\underline{(t)})\right)$$

Minimalization: suppose $h(x_1, \ldots, x_n) = \min_y(f(x_1, \ldots, x_n, y) = 0)$ for some Diophantine function f. Then

$$y = h(\underline{x}) \iff (\forall t)_{t \leq y}(t = y) \vee f(\underline{x}, t) \neq 0$$

This uses bounded quantifiers, but we have already proven that equations with this form is Diophantine. So we are done.

Primitive Recursion: Suppose

$$\begin{aligned} h(x_1, \ldots, x_n, 1) &= f(x_1, \ldots, x_n) \\ h(x_1, \ldots, x_n, t+1) &= g(t, h(x_1, \ldots, x_n, t), f(x_1, \ldots, x_n)) \end{aligned}$$

The problem here is that even if we know that for each natural number $1 \leq i \leq t+1$, $h(\underline{x}, i)$ is a Diophantine equation, what we need to show is that $(\underline{x}, i) \mapsto h(\underline{x}, i)$ is also Diophantine. The fact that i is not fixes poses a problem. But this can be easily solved by encoding the sequence $h(\underline{x}, 1), h(\underline{x}, 2), \ldots, h(\underline{x}, t+1)$ as $S(i, u)$ for some u, using the Sequence Number Theorem. □

$$\begin{aligned} y = h(x_1, \ldots, x_n, z) \iff & \exists u \; S(1, u) = f(\underline{x}) \wedge \\ & \forall t < z, S(t+1, u) = g(t, S(t, u), \underline{x}) \\ & y = S(z, u) \end{aligned}$$

We are almost done, but not yet finished, since we have only proven that all images of Diophantine functions are listable, not all sets in general.

4 Beyond Integers

In this section assume $K/\mathbb{Q}$ is finite. the rings of integers $\mathcal{O}_K$ [2] is defined to be

$$\mathcal{O}_K = \{\alpha \in K : \alpha \text{ is a root of a monic polynomial over } \mathbb{Z}\}$$

A natural question arise: is H10 decidable over the rings of $\mathcal{O}_K$?

Denef–Lipshitz Conjecture: $\mathbb{Z}$ is $\mathcal{O}_K$-Diophantine.

Corollary 2 (Corollary of DL)**.** *H10 over $\mathcal{O}_K$ is undecidable.*

Proof of Corollary. Take $f \in \mathbb{Z}[X_1, \ldots, X_n]$ which, we want an algorithm to detect whether it has integer solutions or not.

Suppose that $\mathbb{Z}$ is Diophantine over $\mathcal{O}_K$, that means there is some polynomial ϕ such that $z \in \mathbb{Z} \iff \exists \underline{y}, \phi(z, \underline{y}) = 0$ holds.

So $f(X_1 \ldots X_n)$ has a solution in $\mathbb{Z}$ iff the following system of equations has a solution in $\mathcal{O}_K$:

$$\begin{aligned} & f(t_1, \ldots, t_n) = 0 \\ & \phi(t_1, \underline{y_1}) = 0 \\ & \phi(t_2, \underline{y_2}) = 0 \\ & \ldots \\ & \phi(t_n, \underline{y_n}) = 0 \end{aligned}$$

It is equally easy to ask for positive integer solutions for f, simply add to the equation, the sentences $t_i > 0$. □

[2] Not to be confused with $\mathcal{O}_K$ from valuation theory

DL is finally proved in 2024.

H10 over $\mathbb{Q}$ is still unknown, despite decades of effort. However, along the way we have achieved many partial results:

Theorem 5 (Poonen, 2009)**.** *$\mathbb{Z}$ is first-order definable in $\mathbb{Q}$ by an $\forall\forall\exists\exists\exists\exists\exists\exists\exists$ formula.*

Theorem 6 (Koenigsmann 2016)**.** *$\mathbb{Z}$ is first-order definable in $\mathbb{Q}$ by an $\forall\exists\ldots\exists$ formula.*

If only we can get rid of the $\forall$ symbol!

References

[Dav73] Martin Davis. Hilbert's tenth problem is unsolvable. *The American Mathematical Monthly*, 80(3):233–269, 1973.

[Mat93] Yuri V. Matiyasevich. *Hilbert's tenth problem.* MIT Press, Cambridge, MA, USA, 1993.