Definability, Diophantine equations, Hilbert's 10th

We consider two (related?) problems.

Problem 1 We showed, for $A \subseteq \mathbb{N}^k$
A definable in $\mathcal{N}$ iff
A arithmetical (i.e. $A \in \bigcup \Sigma^0_n$)

But what is precise relation between definable and arithmetical hierarchies?

quantifier free
Definable: $QF, \exists_1, \forall_1, \exists_2, \forall_2 \ldots$
Arithmetical: $\Delta^0_1, \Sigma^0_1, \Pi^0_1, \Delta^0_2, \Sigma^0_2, \Pi^0_2, \ldots$

We observed: A defined by q.f. φ
$\Rightarrow A$ recursive so
$QF \subseteq \Delta^0_1$

In this case: containment is strict
(why: if φ q.f. $\exists$ poly time algorithm to determine $\varphi(\vec{a})$ or $\neg\varphi(\vec{a})$ — just need to check, if something is or is not root of a poly essentially some finite # of times)

Follows $\exists_1 \subseteq \Sigma^0_1$ $\forall_1 \subseteq \Pi^0_1$ etc...

Q: Are these containments ever strict? In particular: is $\Sigma_1^0 = \exists_1$ T or F?

Problem 2: **Def'n** a **Diophantine equation** is an equation of the form $F(x_1, \ldots, x_k) = 0$ where $F \in \mathbb{Z}[x_1, \ldots, x_k]$ is a multivariate polynomial w/ coeffs in $\mathbb{Z}$

(Note: can always rewrite such an eq'n as $G(\vec{x}) = H(\vec{x})$ where G, H have coeffs in $\mathbb{N}$)

Often interested in finding integer solutions to such equations

Ex's: $x^2 + y^2 - z^2 = 0$ has inf many integer solutions

$x^3 + y^3 - z^3 = 0$ has no nonzero integer sol'ns

(Pell's eq'n) $x^2 - ky^2 - 1 = 0$ has as many sol'ns, iff k not a perfect square

Q: (Hilbert's 10th): is there an algorithm that can decide whether a given Diophantine eq'n has integer sol'ns?

i.e. recursive

First notice: there is such an algorithm if there is an algorithm deciding if a given equation has non-negative integer sol'ns.

Why: - Sps we have alg. deciding if there are sol'ns in $\mathbb{Z}$ and $F(x_1, \ldots, x_k) = 0$ is Diophantine

- Consider $F'(p_1, q_1, r_1, s_1, \ldots, p_k, q_k, r_k, s_k)$
$= F(p_1^2+q_1^2+r_1^2+s_1^2, \ldots, p_k^2+q_k^2+r_k^2+s_k^2)$
- By Lagrange every non-negative integer is a sum of four squares
- Follows: F has sol'ns in $\mathbb{N}$ if F' has sol'ns in $\mathbb{Z}$.

Conversely: sps we have alg. to determine if there are sol'ns in $\mathbb{N}$ on $F(x_1, \ldots, x_k) = 0$ is Dio.

- Let $F' = \prod_{\substack{\text{all } +/- \\ \text{combos}}} F(+/- x_1, \ldots, +/- x_k)$

- F has integer sol'ns if F' has sol'ns in $\mathbb{N}$. ✓

Both probs solved quickly by the following famous result:

Theorem (Matiyasevich, 1970) Sps $R(n_1, \dots, n_k)$ is r.e. Then there are poly's $G(x_1, \dots, x_k, y_1, \dots, y_m)$, $H(x_1, \dots, x_k, y_1, \dots, y_m)$ w/ coeffs in $\mathbb{N}$ s.t.

$$R(\vec{n}) \text{ iff } \exists \vec{y} \left[G(\vec{n}, \vec{y}) = H(\vec{n}, \vec{y}) \right]$$

Note: ① any R defined by such expression is r.e., so is iff

② "very nice" way to define r.e. sets: "$\exists \vec{y}$ (term = term)"

③ Using $F = G - H$ can rewrite $\exists \vec{y} \, (F(\vec{n}, \vec{y}) = 0)$ ← diophantine

w/ F coeffs in $\mathbb{Z}$

Solution to prob 1: $\exists_1 = \Sigma_1^0$ and ①+② shows even better: every r.e. R defined by $\exists \vec{y} \, (G = H)$, q.f. part just atomic fmla — we need for $\wedge, \vee, \neg$.

$\forall_1 = \Pi_1^0$ too? (think about it...)

Solution to prob 2 : - No such algorithm exists.

- if it did, then $\forall x$ $A \in \Sigma^*$ / Δ^*,
- by theorem there is $F \in \mathbb{Z}[\dots]$ s.t. $A(\vec{n})$ iff $\exists \vec{y}\,(F(\vec{n},\vec{y}) = 0)$
- but algorithm can determine, $\forall \vec{n}$, if $\exists \vec{y}$ $F(\vec{n},\vec{y}) = 0$, i.e. iff $\vec{n} \in A$
  $\Rightarrow$ A recursive, contradiction. ✓

Another nifty consequence:

Corollary if $A \subseteq \mathbb{N}$ is r.e. then there is a poly $F(\vec{x}) \in \mathbb{Z}[\vec{x}]$ s.t.

$$A = \{F(\vec{x}) \mid x_i \in \mathbb{N}\} \cap \mathbb{N}$$

(i.e. $n \in A$ iff $\exists \vec{x} \in \mathbb{N}^k$ $F(\vec{x}) = n$)

Pf: By Matiyasevich, there is poly G s.t. $R(a)$ iff $\exists x_1, \dots, x_k$ $G(a, \vec{x})$

Let $F(x_1, \dots, x_k, \vec{x}) := (x+1)(1 - G^2(\vec{x}, x)) - 1$

Observe: $F(\vec{x}, x) \geq 0 \Rightarrow$ [redacted] $G(x, \vec{x}) = 0$ and in this case $F(\vec{x}, x) = x$
↑ so $x \in A$

and conversely if $G(x, \vec{x}) = 0$ ($\iff x \in A$) then $F(\vec{x}, x) = x$.

In particular, for e.g. the set of primes P there is a poly $F(\vec{x})$ whose positive outputs are exactly the primes.

Proving Matyasevich

Def'n $R \subseteq \mathbb{N}^k$ is diophantine if there is $F \in \mathbb{Z}[\vec{y}]$ s.t. $R(\vec{a})$ iff $\exists \vec{y}\,(F(\vec{a}, \vec{y}) = 0)$

theorem is: R is r.e. iff diophantine
$\Rightarrow$ is hard direction

Def'n. $f : \mathbb{N}^k \to \mathbb{N}$ is diophantine if its graph is, i.e. "$f(\vec{x}) = y$" is diophantine.

to prove Maty: enough to prove every (partial) recursive f is dio.
why: if R r.e. then $R = \mathrm{dom}(f)$ for some rec. f.

$\vec{a} \in R$ iff $\exists y\, f(\vec{a}) = y$
iff for some $F \in \mathbb{Z}[\,]$ by M
$\exists y \exists \vec{x} F(\vec{a}, y, \vec{x}) = 0$

$\Rightarrow R$ also defined by dio eq'n

Proof of Matiy.

We induct on construction of recursive f's to reduce problem to showing closure of diophantine-ness under certain quantifiers, connectives etc.

1) Basic functions are diophantine:
C_n, Π^n_i, S defined by
$y = 0$
$y - x_i = 0$
$y - (x+1) = 0$ resp.

(can make them "look more dio" by adding dummy variables ex. $\exists z\,(y-(x+1)=0)$)

2) Composition of dio functions are dio:
if $f(\vec{x}) = h(g_1(\vec{x}), \ldots, g_m(\vec{x}))$
for h, g_i dio we have

$$f(\vec{x}) = y \text{ iff } \exists y_1 \ldots \exists y_m \big(g_1(\vec{x}) = y_1 \wedge g_2(\vec{x}) = y_2 \wedge \ldots \wedge g_m(\vec{x}) = y_m \wedge h(y_1, \ldots, y_m) = y \big)$$

need to show: dio relations closed under $\exists$ and $\wedge$

3) minimalization: if $f(\vec{x}) = \mu y [g(\vec{x},y)=0]$ and g is dio then

$$f(\vec{x}) = y \text{ iff } g(\vec{x},y)=0 \wedge \forall z<y \exists w [w>0 \wedge g(\vec{x},z)=w]$$

So need to know: $w>0$ is diophantine and diophantine-nes closed under bdd quantification $\forall z<y$

4) primitive recursion: if f defined by:

$$f(0,\vec{x}) = g(\vec{x})$$
$$f(n+1,\vec{x}) = h(f(n,\vec{x}), n, \vec{x})$$

g, h diophantine

then: $f(n,\vec{x}) = y$ iff $(i=0 \wedge g(\vec{x})=y)$
$\vee [i>0 \wedge \exists a \exists b (g(\vec{x}) = \beta(a,b,0)$
$\wedge \forall j<i (\beta(a,b,j+1) =$
$h(\beta(a,b,j), j, \vec{x})$
$\wedge \beta(a,b,i) = y]$

So need to know: β is diophantine, dio relations closed under $\vee$ and substitution by dio functions.

Thus we'll be done if we can prove:

Crucial Lemma. The collection of diophantine sets contains the relations $x<y$, $\beta(a,b,i)=z$, is closed under substitution by diophantine functions, $\exists$ quantification, bounded $\forall x<y$ quantification, and the connectives $\wedge$ and $\vee$.

- Most of these straightforward
- hardest by far is bounded $\forall x<y$ quantification
- relies on some real number theory boil down partly to showing exponentiation $x^y=z$ is dio.

Let's power thru some of the non $\forall x<y$ parts...

- We'll also need $x \equiv y \pmod{z}$ is dio.

- $\exists$: obvious

- $\wedge$ and $\vee$: if $R(\vec{x})$, $S(\vec{x})$ defined by pdy's $F(\vec{x},\vec{z})$ and $G(\vec{x},\vec{z})$ then:

$$\exists \vec{y}\, \exists \vec{z}\, (F^2(\vec{x},\vec{y}) + G^2(\vec{x},\vec{z}) = 0)$$

defines $R(\vec{x}) \wedge S(\vec{x})$

and:

$$\exists \vec{y}\, \exists \vec{z}\, (F(\vec{x},\vec{y})\, G(\vec{x},\vec{y}) = 0)$$

defines $R(\vec{x}) \vee S(\vec{x})$

- substitution: if $R(\vec{x},y)$ and $f(\vec{z})$ are def then $(\vec{x},\vec{z}) \in R(\vec{x}, f(\vec{z}))$ iff

$$\exists y\, (R(\vec{x},y) \wedge f(\vec{z}) = y)$$

↑ quantifying over $\mathbb{N}$ remember

- $x < y$ iff $\exists z\, \exists w\, (y - (x+z) = 0 \wedge w+1 = z)$

- $x \equiv y \pmod z$ iff

$$\exists m\, ((x-y) - mz = 0 \vee (y-x) - mz = 0)$$

- $\beta(a,b,i) = k$ iff

$$a \equiv k \bmod b(i+1)+1 \quad \wedge$$
$$k < b(i+1)+1$$

So remains to show $\forall x < y \ldots$