Baire Category for Hilbert's Tenth Problem Inside $\mathbb{Q}$

Russell Miller

Queens College & CUNY Graduate Center

Computability in Europe
Paris
27 June 2016

Slides available at
qcpages.qc.cuny.edu/~rmiller/slides.html

HTP: Hilbert's Tenth Problem

Definition

For a ring R, *Hilbert's Tenth Problem for R* is the set

$$HTP(R) = \{p \in R[X_0, X_1, \ldots] : (\exists \vec{a} \in R^{<\omega})\ p(a_0, \ldots, a_n) = 0\}$$

of all polynomials (in several variables) with solutions in R.

So $HTP(R)$ is c.e. relative to (the atomic diagram of) R.

Hilbert's original formulation in 1900 demanded a decision procedure for $HTP(\mathbb{Z})$.

Thm. (Matiyasevich 1970, using Davis-Putnam-Robinson, 1961)

$HTP(\mathbb{Z})$ is undecidable by Turing machines: indeed, $HTP(\mathbb{Z}) \equiv_1 \emptyset'$.

The most obvious open question is the Turing degree of $HTP(\mathbb{Q})$.

Subrings R_W of $\mathbb{Q}$

A subring R of $\mathbb{Q}$ is characterized by the set of primes p such that $\frac{1}{p} \in R$. For each $W \subseteq \omega$, set

$$R_W = \left\{ \frac{m}{n} \in \mathbb{Q} \ : \ \text{all prime factors } p_k \text{ of } n \text{ have } k \in W \right\}$$

be the subring generated by inverting the k-th prime p_k for all $k \in W$.

We often move effectively between W (a subset of ω) and $P = \{p_n : n \in W\}$, the set of primes which W describes.

Notice that R_W is computably presentable precisely when W is c.e., while R_W is a computable subring of $\mathbb{Q}$ iff W is computable.

We will treat $\{f \in \mathbb{Z}[\vec{X}] : (\exists \vec{x} \in R_W^{<\omega})\ f(\vec{x}) = 0\}$ as $HTP(R_W)$.

Basic facts about $HTP(R_W)$

- $HTP(R_W) \leq_1 W'$.
- $W \leq_1 HTP(R_W)$.
  (Reason: $k \in W \iff (p_k X - 1) \in HTP(R_W)$.)
- $HTP(\mathbb{Q}) \leq_1 HTP(R_W)$. Reason:

$$
\begin{aligned}
& p(X_1, \ldots, X_j) \in HTP(\mathbb{Q}) \\
& \quad \Longrightarrow \left(\left(Y^d \cdot p\left(\frac{X_1}{Y}, \ldots, \frac{X_j}{Y} \right) \right)^2 + (\ulcorner Y > 0 \urcorner)^2 \right) \in HTP(\mathbb{Z}) \\
& \quad \Longrightarrow \left(\left(Y^d \cdot p\left(\frac{X_1}{Y}, \ldots, \frac{X_j}{Y} \right) \right)^2 + (\ulcorner Y > 0 \urcorner)^2 \right) \in HTP(R_W) \\
& \quad \Longrightarrow p(X_1, \ldots, X_j) \in HTP(\mathbb{Q}).
\end{aligned}
$$

Subrings with $HTP(R_W) \equiv_T HTP(\mathbb{Q})$

A commutative ring is *local* if it has a unique maximal ideal, and *semilocal* if it has only finitely many maximal ideals. The semilocal subrings R_W are exactly those with W cofinite. If $\overline{W} = \{n_0, \ldots, n_j\}$, we write $\mathbb{Z}_{(p_{n_0},\ldots,p_{n_j})}$ for R_W.

Fact (Shlapentokh, following J. Robinson)

Every semilocal subring R_W has $HTP(R_W) \equiv_1 HTP(\mathbb{Q})$. Both reductions are uniform in (a strong index for) the finite set $\overline{W}$.

Theorem (Eisenträger-M.-Park-Shlapentokh)

There exist coinfinite c.e. W with $HTP(R_W) \equiv_T HTP(\mathbb{Q})$.

The proof is a priority construction: we add to R_W a solution to the polynomial f_n if we can do so without putting any of the first n elements of $\overline{W}$ into W. The above Fact then yields $HTP(R_W) \leq_T HTP(\mathbb{Q})$.

HTP-generic subrings

The subrings built for the EMPS theorem have the following property:

Definition

A subring $R_W \subseteq \mathbb{Q}$ is *HTP-generic* if, for every $f \in \mathbb{Z}[\vec{X}]$, either $f \in HTP(R_W)$ or there exists some finite $F_0 \subseteq \overline{W}$ for which $f \notin HTP(R_{\overline{F_0}})$.

This says that the decision about whether $f \in HTP(R_W)$ always stems from a finitary fact about W. Either W contains finitely many primes which yield a solution to f; or else W omits a finite set F_0 of primes and thereby rules out all solutions to f.

HTP-generic subrings

The subrings built for the EMPS theorem have the following property:

Definition

A subring $R_W \subseteq \mathbb{Q}$ is *HTP-generic* if, for every $f \in \mathbb{Z}[\vec{X}]$, either $f \in HTP(R_W)$ or there exists some finite $F_0 \subseteq \overline{W}$ for which $f \notin HTP(R_{\overline{F_0}})$.

This says that the decision about whether $f \in HTP(R_W)$ always stems from a finitary fact about W. Either W contains finitely many primes which yield a solution to f; or else W omits a finite set F_0 of primes and thereby rules out all solutions to f.

Proposition

If R_W is HTP-generic, then $HTP(R_W) \equiv_T W \oplus HTP(\mathbb{Q})$.

Topology of the Cantor space of all subrings of $\mathbb{Q}$

Recall: subrings R_W correspond to elements W of Cantor space 2^ω. For every f, the set

$$\mathcal{A}(f) = \{W \subseteq \omega : f \in HTP(R_W)\}$$

is open in 2^ω. So likewise is the set

$$\mathcal{C}(f) = \{W \subseteq \omega : (\exists \text{ finite } F_0 \subseteq \overline{W})\ f \notin HTP(R_{\overline{F_0}})\}.$$

Definition

The *boundary set* $\mathcal{B}(f)$ *of* f is the complement of $\mathcal{A}(f) \cup \mathcal{C}(f)$ in 2^ω.

Indeed $\mathcal{B}(f) = 2^\omega - (\text{Int}(\mathcal{A}(f)) \cup \text{Int}(\ \overline{\mathcal{A}(f)}\ ))$, so this is the topological boundary of $\mathcal{A}(f)$.

If W is HTP-generic, then for all f, we have $W \notin \mathcal{B}(f)$.

A polynomial with $\mathcal{B}(f)$ nonempty

Define $f(X, Y, \ldots) = (X^2 + Y^2 - 1)^2 + (\ulcorner X > 0 \urcorner)^2 + (\ulcorner Y > 0 \urcorner)^2$, and set $W_3 = \{$indices k of primes $p_k \equiv 3 \bmod 4\}$.

Solutions to $f = 0$ correspond to nonzero pairs $(\frac{a}{c}, \frac{b}{c})$ with $a^2 + b^2 = c^2$.

If an odd prime p divides c, then $a^2 \equiv -b^2 \bmod p$, and so -1 is a square modulo p. Hence $p \equiv 1 \bmod 4$. This proves $f \notin HTP(R_{W_3})$.

But if $p \equiv 1 \bmod 4$, then $p = m^2 + n^2$ for some $m, n \in \mathbb{Z}$, and then

$$\left(\frac{m^2 - n^2}{p}\right)^2 + \left(\frac{2mn}{p}\right)^2 = \frac{(m^4 - 2m^2n^2 + n^4) + 4m^2n^2}{p^2}$$
$$= \frac{(m^2 + n^2)^2}{p^2} = 1.$$

So $f \in HTP(R_{\{p\}})$ for all $p \equiv 1 \bmod 4$, and thus $W_3 \in \mathcal{B}(f)$.

Baire category theory

Fact

The boundary of an open set in a Baire space is always nowhere dense. Since all $\mathcal{A}(f)$ are open, $\mathcal{B} = \cup_{f \in \mathbb{Z}[\vec{X}]} \mathcal{B}(f)$ is a meager set.

Baire category theory

Fact

The boundary of an open set in a Baire space is always nowhere dense. Since all $\mathcal{A}(f)$ are open, $\mathcal{B} = \cup_{f \in \mathbb{Z}[\vec{X}]} \mathcal{B}(f)$ is a meager set.

Corollary (M, 2016)

On a comeager set of subrings R_W of $\mathbb{Q}$, the equivalence holds:

$$HTP(R_W) \equiv_T W \oplus HTP(\mathbb{Q}).$$

In particular, this holds on the set $\overline{\mathcal{B}}$ of all HTP-generic subrings.

Results for $HTP(\mathbb{Q})$

Theorem (M, 2016)

For any set $C \subseteq \omega$ (such as $\emptyset'$), the following are equivalent:

1. $HTP(\mathbb{Q}) \geq_T C$.
2. $HTP(R_W) \geq_T C$ for all subrings R_W of $\mathbb{Q}$.
3. $HTP(R_W) \geq_T C$ for a non-meager set of subrings R_W.

If (3) holds, then it holds on a non-meager set of HTP-generic subrings. Therefore, $W \oplus HTP(\mathbb{Q}) \geq_T C$ for non-meager-many W. We then infer (1) by applying:

Lemma (folklore)

If $A \not\geq_T C$, then $\{W \subseteq \omega : W \oplus A \geq_T C\}$ is meager.

Other reductions

Theorem (M, 2016)

- $HTP(\mathbb{Q}) \geq_1 C \iff \{W : HTP(R_W) \geq_1 C\}$ is non-meager.
- $(\mathbb{Z}, +, \cdot)$ has a Diophantine definition in $\mathbb{Q} \iff$ it has a Diophantine definition in non-meager-many subrings R_W.
- $\mathbb{Z}$ is existentially definable in $\mathbb{Q} \iff$ $\mathbb{Z}$ is existentially definable in non-meager-many subrings R_W.

So one can hope to address these questions about $HTP(\mathbb{Q})$ without dealing specifically with $\mathbb{Q}$ itself: just show that the property holds on a sufficiently large set of subrings of $\mathbb{Q}$. Poonen and others have already produced continuum-many subrings $R \subseteq \mathbb{Q}$ with HTP$(R) \geq_T \emptyset'$.

On the other hand, we conjecture that those subrings of $\mathbb{Q}$ are not HTP-generic, and therefore do not move us towards undecidability results for HTP$(\mathbb{Q})$. The arguments above show the necessity of studying HTP-generic subrings to make any progress.

What about Lebesgue measure?

There is a close analogy between measure theory and Baire category: meager sets are often (but not always!) of measure 0, and vice versa.

Open Question

Does there exist some $f \in \mathbb{Z}[\vec{X}]$ with $\mu(\mathcal{B}(f)) > 0$?

If not – or even if $\mu(\mathcal{B}(f))$ is computable uniformly in f – then we can derive results for measure theory and $HTP(\mathbb{Q})$ similar to the results for Baire category.

Recently we established:

Theorem (M., 2016)

If $\mathbb{Z}$ has an existential definition in the field $\mathbb{Q}$, then $\mu(\mathcal{B}) = 1$, and indeed the measures of $\mathcal{A}(f)$ and $\mathcal{B}(f)$ can be arbitrary left-c.e. and left-$\emptyset'$-c.e. reals > 0 satisfying $\mu(\mathcal{A}(f)) + \mu(\mathcal{B}(f)) \leq 1$.

Conclusions?

In our example with $X^2 + Y^2 = 1$, $\mathcal{B}(f)$ turns out to contain all subsets of $W_3 \cup \{2\}$ – and nothing else, since every $p \equiv 1 \bmod 4$ yields a solution to f.
(Thanks to Poonen for proving this for all such p.)

However, this $\mathcal{B}(f)$ has measure 0: the odds of omitting every prime $\equiv 1 \bmod 4$ are zero. So we still have the original question:

Open Question

Does there exist some $f \in \mathbb{Z}[\vec{X}]$ with $\mu(\mathcal{B}(f)) > 0$?