Hilbert's Tenth Problem as a Pseudojump Operator

Russell Miller

Queens College & CUNY Graduate Center

Logic Colloquium
Udine, Italy
26 July 2018

(Partially joint work with Ken Kramer.)

HTP: Hilbert's Tenth Problem

Definition

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

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

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

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

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

Theorem (DPRM, 1970)

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

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

HTP as a Pseudojump Operator

We will consider $HTP(R)$ for subrings $R \subseteq \mathbb{Q}$. Such subrings correspond bijectively to subsets W of $\mathbb{P} = \{$ all primes $\}$:

$$W \quad \longleftrightarrow \quad R_W := \mathbb{Z}\left[\frac{1}{p} \; : \; p \in W\right].$$

So the **HTP operator** maps $2^{\mathbb{P}}$ into $2^{\omega} \cong 2^{\mathbb{Z}[X_1, X_2, \ldots]}$ via

$$W \mapsto HTP(R_W).$$

Notice that $HTP(R_W)$ is always c.e. in W. (Indeed, there is a uniform enumeration reduction $HTP(R_W) \leq_e W$.) Also, $W \leq_T HTP(R_W)$, since $p \in W \iff (pX - 1) \in \text{HTP}(R_W)$. Therefore, *HTP* is a *pseudojump operator*, as defined by Jockusch and Shore.

HTP(R_W) vs. W'

It is immediate that HTP(R_W) $\leq_1$ W'. The MRDP result shows that 1-equivalence can hold: when $W = \emptyset$, we have HTP($R_\emptyset$) $\equiv_1$ $\emptyset'$.

It is possible to have $W' \not\equiv_T$ HTP(R_W): let W be c.e. and nonlow. Then we can still search effectively for solutions to $f = 0$ in R_W, so HTP(R_W) is c.e. Hence HTP(R_W) $\leq_1 \emptyset' <_T W'$ for such sets W.

In fact, HTP(R_W) $\equiv_1$ W is also possible, e.g. for a c.e. set $W \equiv_1 \emptyset'$. The sets $\emptyset$ and $\emptyset'$ already establish:

Fact

It is possible to have $HTP(R_V) \equiv_T HTP(R_W)$ even when $V \not\equiv_T W$.

First question today: when $V \equiv_T W$, must $HTP(R_V) \equiv_T HTP(R_W)$?

One useful polynomial

Define $f(X, Y, \ldots) = (X^2 + Y^2 - 1)^2 + (\text{“}X > 0\text{”})^2 + (\text{“}Y > 0\text{”})^2$.
Solutions to $f = 0$ correspond to nonzero pairs $(\frac{a}{c}, \frac{b}{c})$ with $a^2 + b^2 = c^2$. What are the prime factors of c here?

If 2 divides c, then $a^2 + b^2 \equiv 0 \bmod 4$, so $a^2 \equiv b^2 \equiv 0 \bmod 4$, so a, b, and c had a common factor of 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 $p \equiv 1 \bmod 4$.

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 $f \in HTP(R_W)$ iff W contains some $p \equiv 1 \bmod 4$.

Usefulness of $f(X, Y)$

Fix one index e. To make $\text{HTP}(R_V)$ encode the answer to the question "Is $e \in \textbf{Fin}$?" we start enumerating the c.e. set W_e.

- Each time W_e acquires a new element, delete the next prime $\equiv 1 \mod 4$ from V.

Thus we co-enumerate a set V of primes such that

$$e \in \textbf{Fin} \iff V \text{ contains a prime} \equiv 1 \mod 4 \iff f \in \text{HTP}(R_V).$$

Usefulness of $f(X, Y)$

Fix one index e. To make $\text{HTP}(R_V)$ encode the answer to the question "Is $e \in \mathbf{Fin}$?" we start enumerating the c.e. set W_e.

- Each time W_e acquires a new element, delete the next prime $\equiv 1 \bmod 4$ from V.

Thus we co-enumerate a set V of primes such that

$$e \in \mathbf{Fin} \iff V \text{ contains a prime} \equiv 1 \bmod 4 \iff f \in \text{HTP}(R_V).$$

Problem: this only encodes one bit of **Fin** into $\text{HTP}(R_V)$.

Many useful polynomials (joint with Ken Kramer)

Theorem (Kramer & M.)

The HTP operator ($W \mapsto HTP(R_W)$) does not respect Turing equivalence.

For this we need an entire sequence of polynomials. Here it is:

Lemma

For an odd prime q, let $f_q(X, Y) = X^2 + qY^2 - 1$ (modified to make $Y > 0$). Then in every solution $(\frac{a}{c}, \frac{b}{c}) \in \mathbb{Q}^2$ to $f_q = 0$, all prime factors p of c satisfy $(\frac{-q}{p}) = 1$, i.e., $-q$ is a square mod p.

Many useful polynomials (joint with Ken Kramer)

Theorem (Kramer & M.)

The HTP operator ($W \mapsto HTP(R_W)$) does not respect Turing equivalence.

For this we need an entire sequence of polynomials. Here it is:

Lemma

For an odd prime q, let $f_q(X, Y) = X^2 + qY^2 - 1$ (modified to make $Y > 0$). Then in every solution $(\frac{a}{c}, \frac{b}{c}) \in \mathbb{Q}^2$ to $f_q = 0$, all prime factors p of c satisfy $(\frac{-q}{p}) = 1$, i.e., $-q$ is a square mod p.
Conversely, for any such p, $\mathbb{Z}[\frac{1}{p}]$ contains a nontrivial solution to $f_q = 0$.

So the *q-appropriate primes p* are those for which $(\frac{-q}{p}) = 1$.

Making $HTP(R_W)$ compute $\emptyset''$

Recall: **Fin** $= \{e : W_e \text{ is finite}\}$ is Σ^0_2-complete, hence $\equiv_T \emptyset''$.
We build a co-c.e. set V of primes, with the goal that $(\forall e)$

$$f_{q_e} \in HTP(R_V) \iff e \in \textbf{Fin}.$$

Each time W_e acquires a new element, we wish to remove the next q_e-appropriate prime from V. With a priority strategy, this succeeds all but finitely often. It is then possible to compute **Fin** from $HTP(R_V)$, using a theorem of Eisenträger-M.-Park-Shlapentokh on semilocal subrings of $\mathbb{Q}$.

However, $\overline{V}$ is c.e., so HTP$(R_{\overline{V}})$ is also c.e., hence $\leq_T \emptyset' < HTP(R_V)$. Thus $V \equiv_T \overline{V}$, yet HTP$(R_{\overline{V}})$ and HTP(R_V) differ by a full jump, which is the maximum possible difference.

HTP and Turing reducibility

We can use *high permitting* to prove

Theorem (Kramer & M.)

Below every high c.e. set C, there exists a Π^0_1 set $W \leq_T C$ with

$$HTP(R_W) \equiv_T \emptyset''.$$

High permitting (below a c.e. set $C <_T S$) builds U as before, so that HTP$(R_U) \equiv_T \emptyset''$.

Corollary (Kramer & M.)

There exist subrings R, S of $\mathbb{Q}$ with $R <_T S$ (as subsets of $\mathbb{Q}$), yet with

$$HTP(S) <_T HTP(R).$$

High permitting

Ordinary c.e. permitting below C would only ensure that infinitely many q_e-appropriate primes are permitted to be removed from U. High permitting (with C high) ensures that *all but finitely many* such primes leave U. Therefore, we can ask an $HTP(R_U)$ oracle whether f_{q_e} has roots in $R_{U-\{p_0,p_1,\ldots,p_n\}}$, for $n = 0, 1, 2, \ldots$.

Now $e \in$ **Inf** iff some n gives the answer "no," so $HTP(R_U)$ can enumerate **Inf**, and therefore can compute **Inf**. (Notice that $\overline{\emptyset'} \leq_1$ **Inf**, so enumerating **Inf** allows computation of $\emptyset'$, hence allows enumeration of **Fin** as well.)

A more specific question

Theorem

For every Σ^0_2 degree $\boldsymbol{d} \geq \mathbf{0}'$, there is a Π^0_1 set W with $HTP(R_W) \in \boldsymbol{d}$.

We have a Σ_1 set C with $C' \in \boldsymbol{d}$. The construction is similar to the preceding one, except that now we wish to code into HTP(R_W) whether

$$(\forall s)(\exists t > s)\ \left[\Phi^{C_s}_{e,s}(e)\downarrow \implies C_t\restriction \text{use} \neq C_s\restriction \text{use}\right].$$

Coding this makes $C' \leq_T HTP(R_W)$. The opposite reduction holds because $W \leq_T C$. For requirement e, we only enumerate elements $x > e$ into W. Given x, we wait until either x leaves W or every $\Phi^{C_s}_{e,s}(e)$ with $e \leq x$ has converged with correct $C_s\restriction$use. This is C-decidable.

1-reductions

The construction above can be refined to yield 1-reductions:

Tweak

For every Π^0_1 set C, there is another Π^0_1 set $W \equiv_T C$ such that $C' \equiv_1 W' \equiv_1 HTP(R_W)$.

This construction does *not* mix with the high permitting.

Using results of Jockusch and Kurtz, we infer:

Theorem

Measure-1-many and comeager-many sets $U \subseteq \mathbb{P}$ satisfy both of:

- $U' \not\leq_1 HTP(R_U)$ (this is a previous theorem)
- but there is a set $W \equiv_T U$ with $U' \equiv_1 W' \equiv_1 HTP(R_W)$;

These follow because almost all U are c.e. relative to some set $<_T U$.