Hilbert’s Tenth Problem for Subrings of the Rationals

Russell Miller
Queens College & CUNY Graduate Center

Workshop on Sets and Computations
Institute for Mathematical Sciences
National University of Singapore
22 April 2015

(Joint work with Kirsten Eisenträger, Jennifer Park, & Alexandra Shlapentokh.)
Hilbert’s Tenth Problem

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 $HTP(\mathbb{Z})$.

**Theorem (PMRD, 1970)**

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

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

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

$$p(X_1, \ldots, X_j) \in HTP(\mathbb{Q}) \implies (Y^d \cdot p\left(\frac{X_1}{Y}, \ldots, \frac{X_j}{Y}\right) \& Y > 0) \in HTP(\mathbb{Z})$$

$$\implies (Y^d \cdot p\left(\frac{X_1}{Y}, \ldots, \frac{X_j}{Y}\right) \& Y > 0) \in HTP(R_W)$$

$$\implies p(X_1, \ldots, X_j) \in HTP(\mathbb{Q}).$$

It is possible to have $W' \not\equiv_T HTP(R_W)$: let $W$ be c.e. and nonlow, so that $W' >_T \emptyset' \geq_T HTP(R_W)$. 
Explaining “$Y > 0$” as a polynomial

### Four Squares Theorem
An integer is nonnegative iff it is the sum of four squares of integers.

### Corollary
It follows that a rational $y$ is positive iff the following equation has a solution in integers:

$$y(1 + V_1^2 + V_2^2 + V_3^2 + V_4^2) = 1 + U_1^2 + U_2^2 + U_3^2 + U_4^2.$$ 

Moreover, any solution in $\mathbb{Q}$ shows that $y > 0$. So we have a polynomial in $y, \vec{U}, \vec{V}$ which has a solution (in an arbitrary $R_W$) iff $y > 0$. 

Russell Miller (CUNY)
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)**

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

**Theorem (Eisenträger-M-Park-Shlapentokh)**

There exist coinfinite sets $W$ with $HTP(R_W) \equiv_T HTP(\mathbb{Q})$. Indeed, such a $W$ can be computably enumerable, and so $R_W$ can be computably presentable.
Strategy below an $HTP(\mathbb{Q})$-oracle

Each set $W \subseteq \omega$ corresponds effectively to a set $P \subseteq \{\text{primes}\}$.

Enumerate all polynomials in $\mathbb{Z}[\vec{X}]$ effectively as $f_0, f_1, \ldots$. Let $P_0 = \emptyset$. At stage $s + 1$, let $p_0 < \cdots < p_s$ be the least primes of $P_s$. With the oracle, determine whether $f_s \in HTP(R(p_0, \ldots, p_s))$. If not, do nothing. If so, find a solution of $f_s$ here, and invert the primes needed (i.e. add new primes to $P_{s+1}$, and new elements to $W_{s+1}$) so as to put this solution in $R_W$.

So every $p_s$ (for every $s$) lies in $P$. Moreover, $f_s \in HTP(R_W)$ iff it went in by stage $s + 1$, which we can check using an $HTP(\mathbb{Q})$-oracle.
Enumerating $P$ with no oracle

We approximate $P = \{p_0 < p_1 < \cdots\}$ at each stage $s$.

Requirements for the finite-injury construction:

$P_k$: If $f_k \in HTP(\mathbb{Z}(p_0,\ldots,p_k))$, then $f_k \in HTP(R_W)$.

$N_e: p_e,s \notin P$.

At stage $s + 1 = \langle k, j \rangle$, we check whether any of the first $j$ tuples from $\mathbb{Z}(p_0,s,\ldots,p_k,s)$ is a solution to $f_k = 0$. If so, we invert primes in $R_W$ (i.e. add new elements to $W$) so as to put this solution in $R_W$, satisfying $P_k$.

$HTP(R_W) \leq_T HTP(\mathbb{Q})$:

Notice that $p_0 = 2$.

With an $HTP(\mathbb{Q})$-oracle, we can decide whether $f_0 \in HTP(\mathbb{Z}(p_0))$.

If so, find the stage $s_0$ at which a solution first entered $R_W$; else $s_0 = 0$.

Now we know $p_1$, so decide whether $f_1 \in HTP(\mathbb{Z}(p_0,p_1))$, etc.
Corollaries

Corollary (Eisenträger-M-Park-Shlapentokh)
For every c.e. set $U \geq_T \text{HTP}(\mathbb{Q})$, there exists a computably presentable subring $R \subseteq \mathbb{Q}$ with $\text{HTP}(R) \equiv_T U$.

The construction mixes the requirements above with coding requirements, which invert a certain specific prime in $R$ whenever we see a new element enter $U$.

Open Question
For such a $U$, does there exist a computable subring $R \subseteq \mathbb{Q}$ with $\text{HTP}(R) \equiv_T U$?
Density of $W$

**Definition**

For each $W \subseteq \omega$, the *natural density of $W$* is the limit

$$\lim_{s \to \infty} \frac{|W \upharpoonright (s + 1)|}{s + 1}.$$

The *upper and lower densities* of $W$ are the limsup and liminf here.

**Corollary (Eisenträger-M-Park-Shlapentokh)**

For every $\Delta^0_2$ real number $r \in [0, 1]$, there exists a computably presentable subring $R_W \subseteq \mathbb{Q}$ with $HTP(\mathbb{Q}) \equiv_T HTP(R_W)$ for which $W$ has lower density $r$ and upper density 1.
Upper density of $\mathcal{W}$

Open Question (more number-theoretic)

Can we keep $HTP(R_\mathcal{W}) \equiv_T HTP(\mathbb{Q})$ and control the upper density of $\mathcal{W}$? Is there any infinite c.e. such $\mathcal{W}$ with upper density $< 1$?

The danger is that a polynomial $f$ may have solutions in $R_\mathcal{W}$ for every cofinite $\mathcal{W}$, but that each solution requires inverting at least $\epsilon$-many of the first $s$ primes (for various $s$, but with some fixed $\epsilon > 0$). So adding a solution of $f$ to $R_\mathcal{W}$ will require bumping the density $\frac{|W(s+1)|}{s+1}$ up to $\epsilon$, at least temporarily.

However, it seems hopeless to try to keep all solutions of $f$ out of $R_\mathcal{W}$. Recall that $HTP(\mathbb{Z}) \equiv_T \emptyset'$. As long as $HTP(\mathbb{Q})$ says that we have not yet ruled out all solutions of $f$, there could still be a solution in $\mathbb{Z}$.

The real question is: do “spiky” polynomials such as these actually exist?
Maximal sets

**Definition**

A ring $R_W \subseteq \mathbb{Q}$ is *polymaximal* if, for every polynomial $f \notin HTP(R_W)$, there exists a finite set $S_0 \subseteq \overline{W}$ such that $f \notin HTP(\mathbb{Z}(S_0))$.

So, for each $f$, there is a finitary reason why it is or is not in $HTP(R_W)$. Notice that, whenever a c.e. set $W$ is maximal, $R_W$ is polymaximal.

**Proposition**

For every polymaximal subring $R_W$, we have

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

To decide whether $f \in HTP(R_W)$, we search for either a solution to $f$ in $R_W$ (using the $W$-oracle) or a finite $S_0$ as above (using both oracles).
Polymaximality is not universal

Let $f(X, Y, \overline{U})$ be the polynomial:

$$f = (X^2 + Y^2 - 1)^2 + (X > 0)^2 + (Y > 0)^2.$$  

Solutions $(\frac{a}{c}, \frac{b}{c})$ correspond to Pythagorean triples $(a, b, c)$. Suppose a prime $p$ divides $c$. Then $a^2 + b^2 \equiv 0 \mod p$, and so

$$-1 \equiv \left(\frac{a}{b}\right)^2 \mod p.$$  

This forces either $p = 2$ or $p \equiv 1 \mod 4$. Therefore:

**Proposition**

Let $R$ contain inverses of exactly those primes $\equiv 3 \mod 4$. Then $f \notin \text{HTP}(R)$. 

Maximality is not universal

However, $f \in \text{HTP}(R_W)$ for all 1-generic $W$, since, for each product $n$ of finitely many primes,

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

So the subring $R$ (inverting all primes $\equiv 3 \mod 4$) is not polymaximal.

Similar tricks with polynomials $X^2 + qY^2 - 1$, for other primes $q$, allow similar results with other subrings (inverting all primes $\equiv k \mod q$).
## Definition

Fix any $f \in \mathbb{Z}[\tilde{X}]$. The **solvability set** of $f$ is the set

$$\text{Sol}(f) = \{ W \subseteq \omega : f \in \text{HTP}(R_W) \}.$$

This is an effectively open subset of Cantor space. The **measure** $\mu(f)$ of this polynomial is the measure of Sol($f$).

As yet we only know that all 2-adic rationals can be $\mu(f)$. We conjecture that $\mu(X^2 + qY^2 - 1 \& X > 0 \& Y > 0) = 1$ as well.

To get any other value as $\mu(f)$ would require $f$ to be spiky, in somewhat the same sense as described earlier.
Guessing at the measure of $f$

Locally open question

For our $f$ above, saying $X^2 + Y^2 = 1$ & $X > 0$ & $Y > 0$, what is $\mu(f)$? (Also for $X^2 + qY^2 = 1$.)

As noted, whenever $\frac{1}{n^2+1} \in R_W$ (for any $n$), we have $f \in HTP(R_W)$. 

Bunyakovsky Conjecture (1857), roughly stated

For every irreducible $g \in \mathbb{Z}[X]$, if there exist $m, n \in \omega$ with $g(m)$ prime to $g(n)$, then the image of $\mathbb{Z}$ under $g$ contains infinitely many primes.

This is known to hold for all $g$ of degree 1 (Dirichlet's Theorem). However, it apparently remains open for each individual nonlinear $g$!
Guessing at the measure of $f$

Locally open question

For our $f$ above, saying $X^2 + Y^2 = 1 \& X > 0 \& Y > 0$, what is $\mu(f)$? (Also for $X^2 + qY^2 = 1$.)

As noted, whenever $\frac{1}{n^2+1} \in R_W$ (for any $n$), we have $f \in HTP(R_W)$.

Bunyakovsky Conjecture (1857), roughly stated

For every irreducible $g \in \mathbb{Z}[X]$, if there exist $m, n \in \omega$ with $g(m)$ prime to $g(n)$, then the image of $\mathbb{Z}$ under $g$ contains infinitely many primes.

This is known to hold for all $g$ of degree 1 (Dirichlet’s Theorem). However, it apparently remains open for each individual nonlinear $g$!

Notice that, for our $f$ to have $\mu(f) = 1$, it would suffice to have arbitrarily large pairs $(p, q)$ of primes with some power $p^j q^k$ of the form $n^2 + 1$. Likewise for triples, etc.
Theorem
TFAE:

- $HTP(R_W) \leq_T W \oplus HTP(\mathbb{Q})$ uniformly on a measure-1 set of $W$.
- For all $f \in \mathbb{Z}[\vec{X}]$, the complement $\overline{\text{Sol}(f)}$ is an almost-open set.

If these hold, then some functional $\Phi$ has $\Phi^{HTP(\mathbb{Q})}(f) = \mu(f)$ for all $f$. 

Fact (see Nies, *Computability and Randomness*, e.g.)
The class of all generalized low $1$ sets, i.e. those $W$ satisfying $W' \leq_T W \oplus \emptyset'$, has measure $1$. However, there is no single Turing reduction which works uniformly on a set of measure $1$. So, under the equivalent conditions above, no single Turing reduction $W' = \Phi^{HTP(R_W)}$ could hold uniformly on a set of measure $1$. 

Russell Miller (CUNY)
Theorem

TFAE:

- $\text{HTP}(R_W) \leq_T W \oplus \text{HTP}(\mathbb{Q})$ uniformly on a measure-1 set of $W$.
- For all $f \in \mathbb{Z}[\vec{X}]$, the complement $\overline{\text{Sol}(f)}$ is an almost-open set.

If these hold, then some functional $\Phi$ has $\Phi^{\text{HTP}(\mathbb{Q})}(f) = \mu(f)$ for all $f$.

Fact (see Nies, *Computability and Randomness*, e.g.)

The class of all generalized low$_1$ sets, i.e. those $W$ satisfying

$$W' \leq_T W \oplus \emptyset',$$

has measure 1. However, there is no single Turing reduction which works uniformly on a set of measure 1.

So, under the equivalent conditions above, no single Turing reduction $W' = \Phi_e^{\text{HTP}(R_W)}$ could hold uniformly on a set of measure 1.