Hilbert's Tenth Problem for the Rational Numbers and their Subrings

Russell Miller

Queens College & CUNY Graduate Center

Journées sur les Arithmétiques Faibles

CUNY Graduate Center
29 May 2019

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 $HTP(\mathbb{Q})$.

News flash

News flash

Problem: find integers solving the following equations:

$X^3 + Y^3 + Z^3 = 29.$

$X = 1,\ Y = 1,\ Z = 3.$ Easy. (Also $X = 4,\ Y = -3,\ Z = -2.$)

$X^3 + Y^3 + Z^3 = 30.$

$X = -283{,}059{,}965,\ Y = -2{,}218{,}888{,}517,\ Z = 2{,}220{,}422{,}932.$

$X^3 + Y^3 + Z^3 = 31.$

No solutions.

$X^3 + Y^3 + Z^3 = 32.$

No solutions.

$X^3 + Y^3 + Z^3 = 33.$

Open problem!

News flash

Problem: find integers solving the following equations:

$X^3 + Y^3 + Z^3 = 29.$

$X = 1,\ Y = 1,\ Z = 3$. Easy. (Also $X = 4,\ Y = -3,\ Z = -2$.)

$X^3 + Y^3 + Z^3 = 30.$

$X = -283{,}059{,}965,\ Y = -2{,}218{,}888{,}517,\ Z = 2{,}220{,}422{,}932.$

$X^3 + Y^3 + Z^3 = 31.$

No solutions.

$X^3 + Y^3 + Z^3 = 32.$

No solutions.

$X^3 + Y^3 + Z^3 = 33.$

Open problem! NOW CLOSED PROBLEM (Booker, March 2019):
$(8{,}866{,}128{,}975{,}287{,}528)^3 + (-8{,}778{,}405{,}442{,}862{,}239)^3 + (-2{,}736{,}111{,}468{,}807{,}040)^3 = 33.$

Comparing $\mathbb{Z}$ to other subrings

Theorem (Matiyasevich-Davis-Putnam-Robinson, 1970)

Every computably enumerable set $S \subseteq \mathbb{N}$ is diophantine in the ring $\mathbb{Z}$, i.e., defined there by a polynomial $f \in \mathbb{Z}[X, Y_1, \ldots, Y_n]$ as

$$S = \{x \in \mathbb{N} : (\exists y_1, \ldots, y_n \in \mathbb{Z})\ f(x, y_1, \ldots, y_n) = 0\}.$$

But...

Comparing $\mathbb{Z}$ to other subrings

Theorem (Matiyasevich-Davis-Putnam-Robinson, 1970)

Every computably enumerable set $S \subseteq \mathbb{N}$ is diophantine in the ring $\mathbb{Z}$, i.e., defined there by a polynomial $f \in \mathbb{Z}[X, Y_1, \ldots, Y_n]$ as

$$S = \{x \in \mathbb{N} : (\exists y_1, \ldots, y_n \in \mathbb{Z})\ f(x, y_1, \ldots, y_n) = 0\}.$$

But...

Theorem

For almost every subring R of $\mathbb{Q}$, there exists a set C that is computably enumerable relative to R, but is *not* diophantine in R.

Comparing $\mathbb{Z}$ to other subrings

Theorem (Matiyasevich-Davis-Putnam-Robinson, 1970)

Every computably enumerable set $S \subseteq \mathbb{N}$ is diophantine in the ring $\mathbb{Z}$, i.e., defined there by a polynomial $f \in \mathbb{Z}[X, Y_1, \ldots, Y_n]$ as

$$S = \{x \in \mathbb{N} : (\exists y_1, \ldots, y_n \in \mathbb{Z})\ f(x, y_1, \ldots, y_n) = 0\}.$$

But...

Theorem

For almost every subring R of $\mathbb{Q}$, there exists a set C that is computably enumerable relative to R, but is *not* diophantine in R.

Questions:

- "Computably enumerable *relative to R*"??

Comparing $\mathbb{Z}$ to other subrings

Theorem (Matiyasevich-Davis-Putnam-Robinson, 1970)

Every computably enumerable set $S \subseteq \mathbb{N}$ is diophantine in the ring $\mathbb{Z}$, i.e., defined there by a polynomial $f \in \mathbb{Z}[X, Y_1, \ldots, Y_n]$ as

$$S = \{x \in \mathbb{N} : (\exists y_1, \ldots, y_n \in \mathbb{Z})\ f(x, y_1, \ldots, y_n) = 0\}.$$

But...

Theorem

For almost every subring R of $\mathbb{Q}$, there exists a set C that is computably enumerable relative to R, but is *not* diophantine in R.

Questions:

- "Computably enumerable *relative to R*"??
- How does one show diophantine undefinability of a set?

Comparing $\mathbb{Z}$ to other subrings

Theorem (Matiyasevich-Davis-Putnam-Robinson, 1970)

Every computably enumerable set $S \subseteq \mathbb{N}$ is diophantine in the ring $\mathbb{Z}$, i.e., defined there by a polynomial $f \in \mathbb{Z}[X, Y_1, \ldots, Y_n]$ as

$$S = \{x \in \mathbb{N} : (\exists y_1, \ldots, y_n \in \mathbb{Z})\ f(x, y_1, \ldots, y_n) = 0\}.$$

But...

Theorem

For almost every subring R of $\mathbb{Q}$, there exists a set C that is computably enumerable relative to R, but is *not* diophantine in R.

Questions:

- "Computably enumerable *relative to R*"??
- How does one show diophantine undefinability of a set?
- Whadaya mean, "almost every" subring of $\mathbb{Q}$?

Computably enumerable relative to R

For a subring $R \subseteq \mathbb{Q}$, let

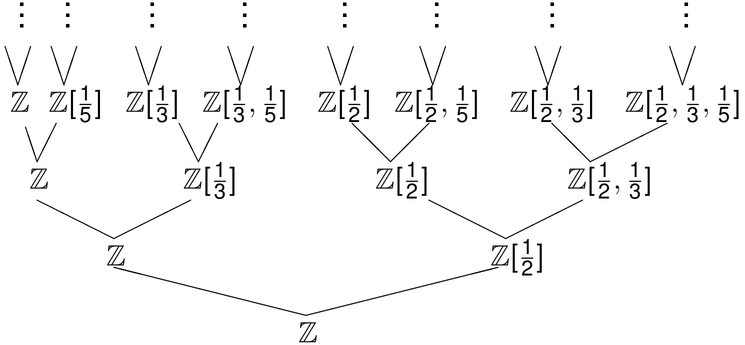
$$D = \{x \in R : (xY - 1) \in HTP(R)\} = \{x \in R : (\exists y \in R)\ xy = 1\}.$$

If $R = \mathbb{Z}[W^{-1}]$ for a reasonably complex set W of primes, then $D \cap \mathbb{N}$ is D-computable, but may not be computably enumerable. So D may fail to be computably enumerable too – yet is diophantine in R.

In general, sets D diophantine in R need not be c.e., but will always be *R-computably enumerable*: given an “oracle” for R (or equivalently W), we can list out all elements of R and search through them for a solution to any given polynomial, thus listing out all elements of D.

So the R-computably enumerable sets are the natural candidates to be diophantine in R. When $R = \mathbb{Z}$, they are all diophantine in $\mathbb{Z}$ – but the theorem says that this is a rare situation.

Picture of the subrings of $\mathbb{Q}$



Half of all subrings contain $\frac{1}{2}$; half do not. A quarter contain $\frac{1}{2}$ and $\frac{1}{3}$; another quarter contain $\frac{1}{2}$ but not $\frac{1}{3}$; and so on. This yields Lebesgue measure on the space of all subrings of $\mathbb{Q}$. Baire category also applies.

Theorem, re-stated

For measure-1-many and comeager-many subrings R of $\mathbb{Q}$, there exists a set C that is c.e. relative to R, but is *not* diophantine in R.

Background from computability theory

Recall: the *Halting Problem* $\emptyset'$ is the universal computably enumerable set. Every other c.e. set can be computed from $\emptyset'$. Knowing that $\emptyset'$ is diophantine in $\mathbb{Z}$, we know that every c.e. set is diophantine there.

For an arbitrary subring $R = \mathbb{Z}[W^{-1}]$ of $\mathbb{Q}$, we have something similar. First make a computable list of the W-computable functions:

$$\Phi_0^W,\ \Phi_1^W,\ \Phi_2^W, \ldots$$

The *jump* W' is the universal W-computably enumerable set:

$$W' = \{\langle e, x\rangle \in \mathbb{N}^2 : \Phi_e^W \text{ halts on input } x\}.$$

Every other W-c.e. set can be computed from W'. If W' is diophantine in $\mathbb{Z}[W^{-1}]$, then every c.e. set is diophantine there. So the theorem is equivalent to:
For almost all sets W of primes, W' is not diophantine in $\mathbb{Z}[W^{-1}]$.

Reducibilities: (1) $\Longrightarrow$ (2) $\Longrightarrow$ (3)

1. W' is diophantine in $\mathbb{Z}[W^{-1}]$ iff, for some $f \in \mathbb{Z}[X, Y_1, Y_2, \ldots]$,

$$(\forall x \in \mathbb{N}) \left[\begin{array}{rcl} x \in W' & \iff & \exists \vec{y} \in \mathbb{Z}[W^{-1}] \ \ f(x, \vec{y}) = 0 \\ & \iff & f(x, \vec{Y}) \in HTP(\mathbb{Z}[W^{-1}]) \end{array} \right].$$

Reducibilities: (1) $\implies$ (2) $\implies$ (3)

1. W' is diophantine in $\mathbb{Z}[W^{-1}]$ iff, for some $f \in \mathbb{Z}[X, Y_1, Y_2, \ldots]$,

$$(\forall x \in \mathbb{N}) \left[\begin{array}{rcl} x \in W' & \iff & \exists \vec{y} \in \mathbb{Z}[W^{-1}] \;\; f(x, \vec{y}) = 0 \\ & \iff & f(x, \vec{Y}) \in HTP(\mathbb{Z}[W^{-1}]) \end{array} \right].$$

2. $W' \leq_1 HTP(\mathbb{Z}[W^{-1}])$: W' is 1*-reducible* to $HTP(\mathbb{Z}[W^{-1}])$ if, for some 1-1 computable function H,

$$(\forall x \in \mathbb{N}) \; [\; x \in W' \iff H(x) \in HTP(\mathbb{Z}[W^{-1}]) \;].$$

Reducibilities: (1) $\implies$ (2) $\implies$ (3)

1. W' is diophantine in $\mathbb{Z}[W^{-1}]$ iff, for some $f \in \mathbb{Z}[X, Y_1, Y_2, \ldots]$,

$$(\forall x \in \mathbb{N}) \left[\begin{array}{rcl} x \in W' & \iff & \exists \vec{y} \in \mathbb{Z}[W^{-1}] \ \ f(x, \vec{y}) = 0 \\ & \iff & f(x, \vec{Y}) \in HTP(\mathbb{Z}[W^{-1}]) \end{array} \right].$$

2. $W' \leq_1 HTP(\mathbb{Z}[W^{-1}])$: W' is 1*-reducible* to $HTP(\mathbb{Z}[W^{-1}])$ if, for some 1-1 computable function H,

$$(\forall x \in \mathbb{N}) \ [\ x \in W' \iff H(x) \in HTP(\mathbb{Z}[W^{-1}])\ ].$$

3. $W' \leq_T HTP(\mathbb{Z}[W^{-1}])$: W' is *Turing-reducible* to $HTP(\mathbb{Z}[W^{-1}])$ if, for some Turing program Φ,

   Φ with oracle $HTP(\mathbb{Z}[W^{-1}])$ computes the char. function $\chi_{W'}$.

The theorem says that almost all W have $W' \not\leq_1 HTP(\mathbb{Z}[W^{-1}])$.

Proof of the theorem

A set W is *relatively c.e.* if there is some other set V that can enumerate W (so $W \leq_1 V'$) but cannot compute W (so $W \not\leq_T V$).

With $W \not\leq_T V$, the *Jump Theorem* shows that $W' \not\leq_1 V'$.

But since V can enumerate W, it can also enumerate $HTP(\mathbb{Z}[W^{-1}])$, so $HTP(\mathbb{Z}[W^{-1}]) \leq_1 V'$.

Together these show that $W' \not\leq_1 HTP(\mathbb{Z}[W^{-1}])$. Finally we apply:

Theorem (Jockusch 1981; Kurtz 1981)

The relatively c.e. sets are co-meager and have measure 1 in Cantor space.

We call W *HTP-complete* if $W' \leq_1 HTP(\mathbb{Z}[W^{-1}])$. So our theorem says that HTP-completeness is rare.

Intuition for the proof: enumeration operators

Enumerating W' requires you to be able to compute W. Enumerating $HTP(\mathbb{Z}[W^{-1}])$ only requires you to be able to enumerate W. In almost all cases there is a set V that can do the latter but not the former, and in all those cases, W' is more complex, in terms of $\leq_1$, than $HTP(\mathbb{Z}[W^{-1}])$.

Intuition for the proof: enumeration operators

Enumerating W' requires you to be able to compute W. Enumerating $HTP(\mathbb{Z}[W^{-1}])$ only requires you to be able to enumerate W. In almost all cases there is a set V that can do the latter but not the former, and in all those cases, W' is more complex, in terms of $\leq_1$, than $HTP(\mathbb{Z}[W^{-1}])$.

In order to enumerate W', V must be able to *compute* W (that is, $W \leq_T V$). For instance, consider the oracle program Φ_e which halts iff its oracle set W does *not* contain the number 19. Thus

$$e \in W' \iff 19 \notin W.$$

A set V that can only enumerate W can never be sure whether this program Φ_e^W, with W as its oracle, will halt. So V can never enumerate e into W' with certainty, even if in fact $e \in W'$.

Summary: *HTP* is an *enumeration operator*; the jump is not.

What about Turing reducibility?

We know that $W' \not\leq_1 HTP(\mathbb{Z}[W^{-1}])$ almost everywhere.
If $W' \not\leq_T HTP(\mathbb{Z}[W^{-1}])$ on a comeager set, then we would apply

Theorem (M, 2016)

For any set $C \subseteq \mathbb{N}$ (such as $\emptyset'$), the following are equivalent:

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

to show that $HTP(\mathbb{Q}) \not\geq_T \emptyset'$. This would be remarkable.

Conversely, if $W' \leq_T HTP(\mathbb{Z}[W^{-1}])$ on a comeager set, then
HTP($\mathbb{Q}$) $\geq_T \emptyset'$. This too would be remarkable.
(It is open whether a similar equivalence holds for Lebesgue measure.)

What about Turing reducibility?

We know that $W' \not\leq_1 HTP(\mathbb{Z}[W^{-1}])$ almost everywhere.
If $W' \not\leq_T HTP(\mathbb{Z}[W^{-1}])$ on a comeager set, then we would apply

Theorem (M, 2016)

For any set $C \subseteq \mathbb{N}$ (such as $\emptyset'$), the following are equivalent:

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

to show that $HTP(\mathbb{Q}) \not\geq_T \emptyset'$. This would be remarkable.

Conversely, if $W' \leq_T HTP(\mathbb{Z}[W^{-1}])$ on a comeager set, then HTP($\mathbb{Q}$) $\geq_T \emptyset'$. This too would be remarkable.
(It is open whether a similar equivalence holds for Lebesgue measure.)

So, what about it? When does $W' \leq_T HTP(\mathbb{Z}[W^{-1}])$?

Example of Turing reducibility

For many subrings $\mathbb{Z}[W^{-1}]$, we have $HTP(\mathbb{Z}[W^{-1}]) \leq_T HTP(\mathbb{Q}) \oplus W$.

To decide whether f lies in $HTP(\mathbb{Z}[W^{-1}])$:

- Use the W-oracle to list out the elements of the ring and search through them for a solution to $f = 0$.
- For each finite set S_0 disjoint from W, use the $HTP(\mathbb{Q})$-oracle to decide whether $f = 0$ has a solution in the subring $\mathbb{Z}[\overline{S_0}^{-1}]$. If not, conclude that it has no solution in $\mathbb{Z}[W^{-1}]$ either.

For many subrings of $\mathbb{Q}$, this process will always terminate (for every f). Such subrings $\mathbb{Z}[W^{-1}]$ are called *HTP-generic*, and for them, $HTP(\mathbb{Z}[W^{-1}])$ is Turing-equivalent to $HTP(\mathbb{Q}) \oplus W$.

Soon we will also see subrings where this process fails to terminate.

When does $W' \leq_T HTP(\mathbb{Z}[W^{-1}])$?

There are sets W for which $W' \not\leq_T HTP(\mathbb{Z}[W^{-1}])$. For instance, this holds whenever W itself is the jump of another set. However, the sets for which we know $W' \not\leq_T HTP(\mathbb{Z}[W^{-1}])$ form a class of measure 0. So $W' \leq_T HTP(\mathbb{Z}[W^{-1}])$ might yet hold on a class of measure 1.

When does $W' \leq_T HTP(\mathbb{Z}[W^{-1}])$?

There are sets W for which $W' \not\leq_T HTP(\mathbb{Z}[W^{-1}])$. For instance, this holds whenever W itself is the jump of another set. However, the sets for which we know $W' \not\leq_T HTP(\mathbb{Z}[W^{-1}])$ form a class of measure 0. So $W' \leq_T HTP(\mathbb{Z}[W^{-1}])$ might yet hold on a class of measure 1. However, it cannot be uniform:

Theorem

For each Turing functional Ψ, the set

$$\{W \subseteq \mathbb{P} : W' \neq \Psi^{HTP(\mathbb{Z}[W^{-1}])}\}$$

has positive measure. Thus it is impossible for any single program to compute W' from $HTP(\mathbb{Z}[W^{-1}])$ uniformly on a set of measure 1.

More generally, this theorem holds of all *enumeration operators*, such as $W \mapsto HTP(\mathbb{Z}[W^{-1}])$. It (obviously) does not hold of the jump operator $W \mapsto W'$ itself, which is not an enumeration operator.

A different enumeration operator

From an enumeration of W, we can easily enumerate $E(W) = \emptyset' \oplus W$. Consider the analogy between *HTP* and this enumeration operator E.

Baire category:

- $W' \equiv_T \emptyset' \oplus W$ for comeager-many W.
- $HTP(\mathbb{Z}[W^{-1}]) \equiv_T HTP(\mathbb{Q}) \oplus W$ for comeager-many W.

Essentially the same procedure works in both cases.

A different enumeration operator

From an enumeration of W, we can easily enumerate $E(W) = \emptyset' \oplus W$. Consider the analogy between *HTP* and this enumeration operator E.

Baire category:

- $W' \equiv_T \emptyset' \oplus W$ for comeager-many W.
- $HTP(\mathbb{Z}[W^{-1}]) \equiv_T HTP(\mathbb{Q}) \oplus W$ for comeager-many W.

Essentially the same procedure works in both cases.

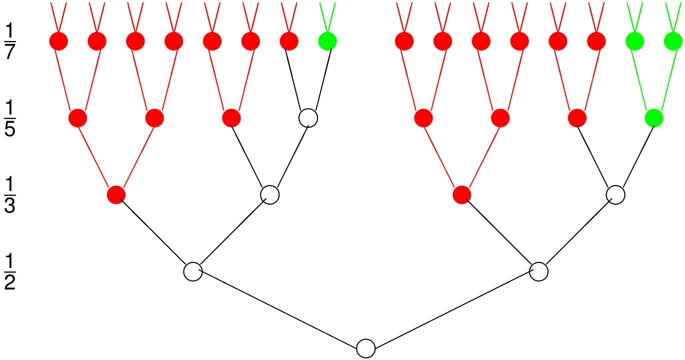
Lebesgue measure:

- $W' \equiv \emptyset' \oplus W$ for measure-1-many W, but no single procedure succeeds for measure-1-many.
- $HTP(\mathbb{Z}[W^{-1}]) \equiv_T HTP(\mathbb{Q}) \oplus W$ for all W except the set $\mathcal{B}$ of *boundary rings* $\mathbb{Z}[W^{-1}]$, i.e., those that are not HTP-generic.

We do not know the measure of $\mathcal{B}$. If $\mu(\mathcal{B}) = 0$, then a single procedure succeeds on a set of measure 1. If not, all is open.

Boundary rings

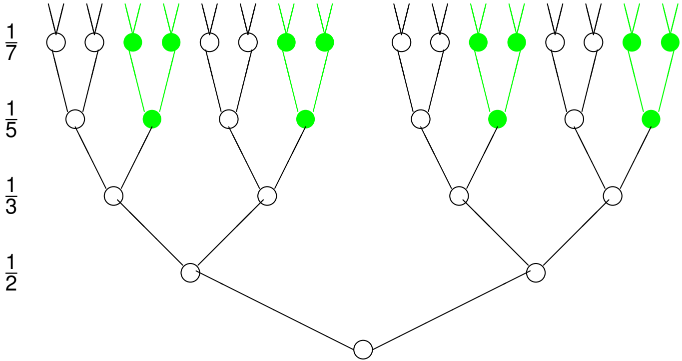
A simple polynomial: $f(X, Y) = (15X - 1)^2 + ((2Y - 1)(7Y - 1))^2$.
We use green and red to indicate subrings that do and do not have solutions to f.



By the level of $\frac{1}{7}$, all nodes are either red or green. There are no boundary rings for this polynomial.

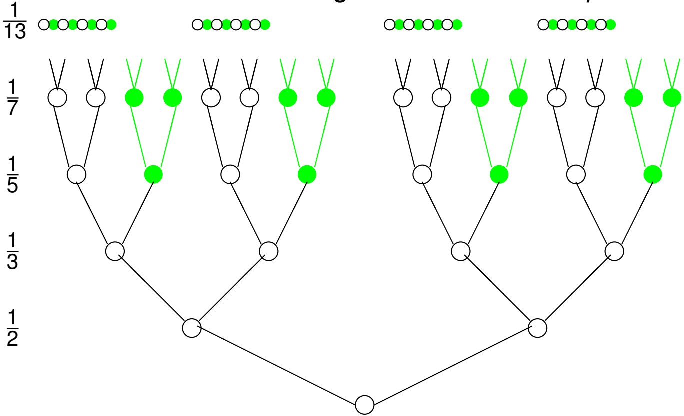
$$g(X, Y, \ldots) = (X^2 + Y^2 - 1)^2 + (X > 0)^2 + (Y > 0)^2$$

This g has solutions in those rings that invert some $p \equiv 1 \bmod 4$.



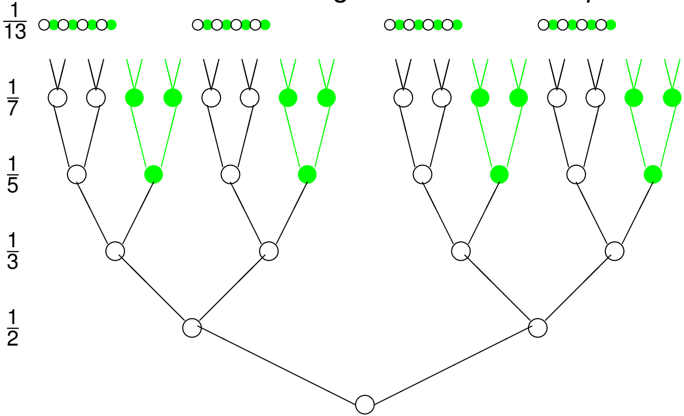
$g(X, Y, \ldots) = (X^2 + Y^2 - 1)^2 + (X > 0)^2 + (Y > 0)^2$

This g has solutions in those rings that invert some $p \equiv 1 \bmod 4$.



$g(X, Y, \ldots) = (X^2 + Y^2 - 1)^2 + (X > 0)^2 + (Y > 0)^2$

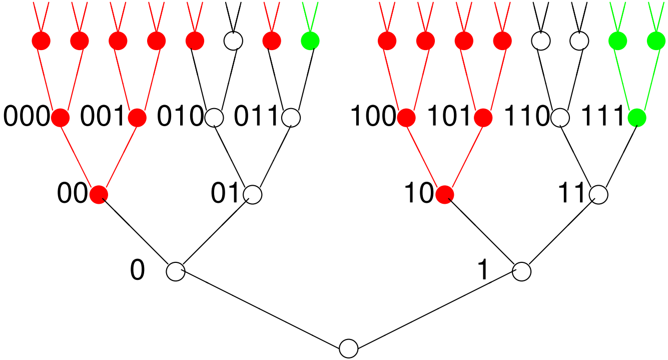
This g has solutions in those rings that invert some $p \equiv 1 \bmod 4$.



Now there are no red lights at all! However, no level is all-green either. So there exist rings whose paths are forever-blank. These are the *boundary rings* for this g: they form the topological boundary of the (open) set of rings with solutions to $g = 0$.

Same thing for E

For any fixed n, we can do the same analysis of E (or of the jump operator). For a string σ, a green light means that $n \in E(W)$ whenever $\sigma \sqsubseteq W$, and a red light means that $n \notin E(W)$ whenever $\sigma \sqsubseteq W$.



Again, there can exist forever-blank paths, and they are the boundary points for the open set of eventually-green paths.

The comparison

- For all enumeration operators (including *HTP* and *E*), the set of green lights is computably enumerable.

- For *E*, the set of red lights is $\leq_1 \overline{\emptyset'}$. The set of red lights for ALL *n* is $\equiv_1 \overline{\emptyset'}$.
- For *HTP*, the set of red lights is $\leq_1 \overline{HTP(\mathbb{Q})}$. The set of red lights for ALL polynomials is $\equiv_1 \overline{HTP(\mathbb{Q})}$.

- For *E*, the set of *W* that (for at least one *n*) lie in the boundary set is a meager set, but has measure 1.
- For *HTP*, the set of *W* that (for at least one polynomial) lie in the boundary set is a meager set. Its measure is unknown, and could equal 0.

Open questions

- Is there a polynomial for which the tree has infinitely many minimal red lights?
  (For *E* and the jump, the corresponding answer is positive.)

Open questions

- Is there a polynomial for which the tree has infinitely many minimal red lights?
  (For E and the jump, the corresponding answer is positive.)

- Is there a polynomial for which the boundary set has positive measure?

Open questions

- Is there a polynomial for which the tree has infinitely many minimal red lights?
  (For E and the jump, the corresponding answer is positive.)

- Is there a polynomial for which the boundary set has positive measure?
  (Theorem (M.): If not, then there is no existential definition of $\mathbb{Z}$ inside $\mathbb{Q}$.)

Open questions

- Is there a polynomial for which the tree has infinitely many minimal red lights?
  (For E and the jump, the corresponding answer is positive.)

- Is there a polynomial for which the boundary set has positive measure?
  (Theorem (M.): If not, then there is no existential definition of $\mathbb{Z}$ inside $\mathbb{Q}$.)

- If boundary sets for polynomials can have measure $m > 0$, what is the possible complexity of (the left Dedekind cut of) m?
  The maximum possible complexity is Π^0_2, but can this be achieved?

It would be natural to ask such questions first about elliptic curves.

Boundary sets

To see that the boundary set for E has measure $> 1 - \frac{1}{2^k}$ (for any k), we can find an n for which the set of green lights has total measure $\frac{1}{2^k}$, but every node has a green light somewhere above it. Thus this tree has no red lights, and the open set of eventually-green nodes has measure only $\frac{1}{2^k}$.

For *HTP*, we know countably many polynomials that have nonempty boundary sets (like the g above). However, as with g, each of those boundary sets has measure 0. In work with Ken Kramer, we have used these polynomials to derive some positive results about the difficulty of deciding $HTP(R)$ for subrings R of $\mathbb{Q}$.

Theorem (from a lemma of Kramer)

For every set $C \subseteq \mathbb{N}$, there exists an HTP-complete set W of primes with $W \equiv_T C$. (Recall: this means $HTP(\mathbb{Z}[W^{-1}]) \equiv_1 W' \equiv_1 C'$.)

Example of the theorem

Setting $C = \emptyset$ gives a straightforward proof that a decidable subring $R \subseteq \mathbb{Q}$ can have $HTP(R) \equiv_! \emptyset'$.
We need an entire sequence of polynomials with properties like the $g(X, Y)$ above. Here it is:

Lemma (Kramer)

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.

Example of the theorem

Setting $C = \emptyset$ gives a straightforward proof that a decidable subring $R \subseteq \mathbb{Q}$ can have $HTP(R) \equiv_! \emptyset'$.
We need an entire sequence of polynomials with properties like the $g(X, Y)$ above. Here it is:

Lemma (Kramer)

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 $(\frac{-q}{p}) = 1$.

Coding the Halting Problem into $HTP(\mathbb{Z}[V^{-1}])$

We have a computable list of the elements: $\emptyset' = \{e_0, e_1, e_2, \ldots\} \subseteq \mathbb{N}$.

We build $V \subseteq \mathbb{P}$ in stages. At stage s, to code that $e_s \in \emptyset'$, we wish to make the polynomial $f_{q_{e_s}}$ lie in $HTP(\mathbb{Z}[V^{-1}])$, which requires putting a q_{e_s}-appropriate prime p into V:

- p should not be any of the first s prime numbers; and
- for every $j \leq s$ with $j \neq e_s$, p should NOT be q_j-appropriate.

The first condition makes V decidable. To decide (e.g.) whether $13 \in V$, just run the first 5 stages of this construction. $13 = q_5$ is the fifth odd prime, so if it has not entered V by then, it never will.

The second condition tries to ensure, for those $j \notin \emptyset'$, that no q_j-appropriate prime ever enters V. From stage j onwards, it succeeds. But what if some q_j-appropriate prime had already entered V before that?

Why does this work?

Here are the necessary lemmas for the construction to succeed.

Lemma (J. Robinson, 1949)

For each finite set $S_0 \subseteq \mathbb{P}$, the semilocal subring $\mathbb{Z}[\overline{S_0}^{-1}]$ is diophantine in $\mathbb{Q}$, and its definition is uniform in S_0.

This allows us to ask $HTP(\mathbb{Z}[V^{-1}])$ whether $\mathbb{Z}[V^{-1}]$ contains a solution to f_{q_j} that does NOT require inverting any of the primes that had already entered V by stage j.

Lemma

For every finite set $S_0 \subseteq \mathbb{P}$ and every prime $q \notin S_0$, there exist infinitely many primes that are q-appropriate but (for all $q' \in S_0$) not q'-appropriate.

Thus we can always find a prime satisfying the two conditions.
Recall: p is q-appropriate iff $-q$ is a square modulo p.