Baire Category Theory and Hilbert's Tenth Problem inside $\mathbb{Q}$

Russell Miller[⋆]

Queens College – C.U.N.Y., 65-30 Kissena Blvd.
Queens NY 11367 USA
Graduate Center of C.U.N.Y., 365 Fifth Avenue
New York, NY 10016 USA
qcpages.qc.cuny.edu/~rmiller

Abstract. For a ring R, Hilbert's Tenth Problem $\text{HTP}(R)$ is the set of polynomial equations over R, in several variables, with solutions in R. We consider computability of this set for subrings R of the rationals. Applying Baire category theory to these subrings, which naturally form a topological space, relates their sets $\text{HTP}(R)$ to the set $\text{HTP}(\mathbb{Q})$, whose decidability remains an open question. The main result is that, for an arbitrary set C, $\text{HTP}(\mathbb{Q})$ computes C if and only if the subrings R for which $\text{HTP}(R)$ computes C form a nonmeager class. Similar results hold for 1-reducibility, for admitting a Diophantine model of $\mathbb{Z}$, and for existential definability of $\mathbb{Z}$.

1 Introduction

The original version of Hilbert's Tenth Problem demanded an algorithm deciding which polynomial equations from $\mathbb{Z}[X_1, X_2, \ldots]$ have solutions in the integers. In 1970, Matiyasevic [4] completed work by Davis, Putnam and Robinson [1], showing that no such algorithm exists. In particular, these authors showed that there exists a 1-reduction from the Halting Problem $\emptyset'$ to the set of such equations with solutions, by proving the existence of a single polynomial $h \in \mathbb{Z}[Y, \boldsymbol{X}]$ such that, for each n from the set ω of nonnegative integers, the polynomial $h(n, \boldsymbol{X}) = 0$ has a solution in $\mathbb{Z}$ if and only if n lies in $\emptyset'$. Since the membership in the Halting Problem was known to be undecidable, it followed that Hilbert's Tenth Problem was also undecidable.

One naturally generalizes this problem to all rings R, defining Hilbert's Tenth Problem for R to be the set

$$\text{HTP}(R) = \{f \in R[\boldsymbol{X}] : (\exists r_1, \ldots, r_n \in R^{<\omega})\ f(r_1, \ldots, r_n) = 0\}.$$

[⋆] The author was supported by Grant # DMS – 1362206 from the N.S.F., and by several grants from the PSC-CUNY Research Award Program. This work grew out of research initiated at a workshop at the American Institute of Mathematics and continued at a workshop at the Institute for Mathematical Sciences of the National University of Singapore. Conversations with Bjorn Poonen and Alexandra Shlapentokh have been very helpful in the creation of this article.

Here we will examine this problem for one particular class: the subrings R of the field $\mathbb{Q}$ of rational numbers. Notice that in this situation, deciding membership in $\text{HTP}(R)$ reduces to the question of deciding this membership just for polynomials from $\mathbb{Z}[\boldsymbol{X}]$, since one readily eliminates denominators from the coefficients of a polynomial. So, for us, $\text{HTP}(R)$ will always be a subset of $\mathbb{Z}[X_1, X_2, \ldots]$.

Subrings R of $\mathbb{Q}$ correspond bijectively to subsets W of the set $\mathbb{P}$ of all primes, via the map $W \mapsto \mathbb{Z}[\frac{1}{p} : p \in W]$. We write R_W for the subring $\mathbb{Z}[\frac{1}{p} : p \in W]$. In this article, we will move interchangeably between subsets of ω and subsets of $\mathbb{P}$, using the bijection mapping $n \in \omega$ to the n-th prime p_n, starting with $p_0 = 2$. For the most part, our sets will be subsets of $\mathbb{P}$, but Turing reductions and jump operators and the like will all be applied to them in the standard way. Likewise, sets of polynomials, such as $\text{HTP}(R)$, will be viewed as subsets of ω, using a fixed computable bijection from ω onto $\mathbb{Z}[\boldsymbol{X}] = \mathbb{Z}[X_0, X_1, \ldots]$.

We usually view subsets of $\mathbb{P}$ as paths through the tree $2^{<\mathbb{P}}$, a complete binary tree whose nodes are the functions from initial segments of the set $\mathbb{P}$ into the set $\{0, 1\}$. This allows us to introduce a topology on the space $2^{\mathbb{P}}$ of paths through $2^{<\mathbb{P}}$, and thus on the space of all subrings of $\mathbb{Q}$. Each basic open set $\mathcal{U}_\sigma$ in this topology is given by a node σ on the tree: $\mathcal{U}_\sigma = \{W \subseteq \mathbb{P} : \sigma \subset W\}$, where $\sigma \subset W$ denotes that when W is viewed as a function from $\mathbb{P}$ into the set $2 = \{0, 1\}$ (i.e., as an infinite binary sequence), σ is an initial segment of that sequence. Also, we put a natural measure μ on the class $\mathbf{Sub}(\mathbb{Q})$ of all subrings of $\mathbb{Q}$: just transfer to $\mathbf{Sub}(\mathbb{Q})$ the obvious Lebesgue measure on the power set $2^{\mathbb{P}}$ of $\mathbb{P}$. Thus, if we imagine choosing a subring R by flipping a fair coin (independently for each prime p) to decide whether $\frac{1}{p} \in R$, the *measure* of a subclass $\mathcal{S}$ of $\mathbf{Sub}(\mathbb{Q})$ is the probability that the resulting subring will lie in $\mathcal{S}$. Here we will focus on Baire category theory rather than on measure theory, however, as the former yields more useful results. For questions and results regarding measure theory, we refer the reader to Section 3 and to the forthcoming [5].

For all $W \subseteq \mathbb{P}$, we have Turing reductions, which in fact are 1-reductions:

$$W \oplus \text{HTP}(\mathbb{Q}) \leq_1 \text{HTP}(R_W) \leq_1 W'.$$

For instance, the Turing reduction from $HTP(R_W)$ to W' can be described by a computable injection which maps each $f \in \mathbb{Z}[\boldsymbol{X}]$ to the code number $h(f)$ of an oracle Turing program which, on every input, searches for a solution $\boldsymbol{x}$ to $f = 0$ in $\mathbb{Q}$ for which the primes dividing the denominators of the coordinates in $\boldsymbol{x}$ all lie in the oracle set W. The reduction from $\text{HTP}(\mathbb{Q})$ to $\text{HTP}(R_W)$ uses the fact that every element of $\mathbb{Q}$ is a quotient of elements of R_W, so that $f(\boldsymbol{X})$ has a solution in $\mathbb{Q}$ if and only if $Y^d \cdot f(\frac{X_1}{Y}, \ldots, \frac{X_n}{Y})$ has a solution in R_W with $Y > 0$. The condition $Y > 0$ is readily expressed using the Four Squares Theorem. Finally, $W \leq_1 \text{HTP}(R_W)$ by mapping p to $(pX - 1)$.

The topological space $2^{\mathbb{P}}$ of all paths through $2^{<\mathbb{P}}$, which we treat as the space of all subrings of $\mathbb{Q}$, is obviously homeomorphic to *Cantor space*, the space 2^ω of all paths through the complete binary tree $2^{<\omega}$. Hence this space satisfies the property of Baire, that no nonempty open set is meager. We recall the relevant definitions. Here as before, $\overline{\mathcal{A}}$ represents the complement of a subset $\mathcal{A} \subseteq 2^{\mathbb{P}}$, and we will write $\text{cl}(\mathcal{A})$ for the topological closure of $\mathcal{A}$ and $\text{Int}(\mathcal{A})$ for its interior.

Definition 1. *A subset $\mathcal{B} \subseteq 2^{\mathbb{P}}$ is said to be* nowhere dense *if its closure $cl(\mathcal{B})$ contains no nonempty open subset of $2^{\mathbb{P}}$. In particular, every set $\mathcal{U}_\sigma$ with $\sigma \in 2^{<\mathbb{P}}$ must intersect $Int(\overline{\mathcal{B}})$, the interior of the complement of $\mathcal{B}$.*

The union of countably many nowhere dense subsets of 2^ω is called a meager set*, or a* set of first category*. Its complement is said to be* comeager*.*

All sets $W \subseteq \omega$ satisfy $W \oplus \emptyset' \leq_T W'$, and for certain W, Turing-equivalence holds here. Indeed, it is known that the class

$$\mathbf{GL}_1 = \{W \in 2^\omega : W' \equiv_T W \oplus \emptyset'\}$$

is comeager, although its complement is nonempty. In computability theory, elements of $\mathbf{GL}_1$ are called *generalized-low*$_1$ *sets*. The low sets – i.e., those W with $W' \leq_T \emptyset'$ – clearly lie in $\mathbf{GL}_1$.

Lemma 1 (Folklore). *There exists a Turing functional Ψ such that $\{W \subseteq \omega : \Psi^{W \oplus \emptyset'} = \chi_{W'}\}$ is comeager. It follows that $\boldsymbol{GL}_1$ is comeager.*

Proof. Consider the following oracle program Ψ for computing W' from $W \oplus \emptyset'$. With this oracle, on input e, the program searches for a string $\sigma \subseteq W$ such that either (1) $(\exists s)\ \Phi^\sigma_{e,s}(e)\downarrow$, or (2) $(\forall \tau \supseteq \sigma)(\forall s)\ \Phi^\tau_{e,s}(e)\uparrow$. The program uses its $\emptyset'$ oracle to check the truth of these two statements for each $\sigma \subseteq W$. If it ever finds that (1) holds, it concludes that $e \in W'$; while if it ever finds that (2) holds, it concludes that $e \notin W'$. Thus, $\Psi^{W \oplus \emptyset'}$ can only fail to compute W' if there exists some $e \notin W'$ such that, for every n, some $\tau \supset W \restriction n$ has $\Phi^\tau_e(e)\downarrow$. This can happen, but for each single e, the set of those W for which this happens constitutes the boundary of the open set $\{W : e \in W'\}$. This boundary is nowhere dense (cf. Lemma 3 below), so the union of these sets (over all e) is meager, and $\Psi^{W \oplus \emptyset'} = \chi_{W'}$ for every W outside this meager set. □

$\mathbf{GL}_1$ also has measure 1, but no single Turing functional computes W' from $W \oplus \emptyset'$ uniformly on a set of measure 1.

Lemma 2 (Folklore). *If $A \not\geq_T B$, then $\mathcal{C} = \{W : A \oplus W \geq_T B\}$ is meager.*

Proof. To show that $\mathcal{C}$ is meager, define $\mathcal{C}_e = \{W \subseteq \mathbb{P} : \Phi^{A \oplus W}_e = \chi_B\}$, so $\mathcal{C} = \cup_e \mathcal{C}_e$. We claim that, if $\sigma \in 2^{\mathbb{P}}$ and $\mathcal{U}_\sigma \subseteq \mathrm{cl}(\mathcal{C}_e)$, the following hold.

1. $\forall x \forall \tau \supseteq \sigma\ [\Phi^{A \oplus \tau}_e(x)\uparrow$ or $\Phi^{A \oplus \tau}_e(x)\downarrow = \chi_B(x)]$.
2. $\forall x \exists \tau \supseteq \sigma\ [\Phi^{A \oplus \tau}_e(x)\downarrow]$.

To see that (1) holds, suppose $\Phi^{A \oplus \tau}_e(x)\downarrow$. With $\mathcal{U}_\tau \subseteq \mathcal{U}_\sigma \subseteq \mathrm{cl}(\mathcal{C}_e)$, some $W \in \mathcal{C}_e$ must have $\tau \subseteq W$. But then $\chi_B(x) = \Phi^{A \oplus W}_e(x)\downarrow = \Phi^{A \oplus \tau}_e(x)$.

To see (2), fix any $W \in \mathcal{C}_e$ with $\sigma \subseteq W$: such a W must exist, since $\mathcal{U}_\sigma \subseteq \mathrm{cl}(\mathcal{C}_e)$. Then we can take τ to be the restriction of this W to the use of the computation $\Phi^{A \oplus W}_e(x)$ (or $\tau = \sigma$ if the use is $< |\sigma|$).

But now every $\mathcal{C}_e$ must be nowhere dense, since any σ satisfying (1) and (2) would let us compute B from A: given x, just search for some $\tau \supseteq \sigma$ and some s for which $\Phi^{A \oplus \tau}_{e,s}(x)\downarrow$. By (2), our search would discover such a τ eventually, and by (1) we would know $\chi_B(x) = \Phi^{A \oplus \tau}_{e,s}(x)$. Since $A \not\geq_T B$, this is impossible. □

Finally, on a separate topic, it will be important for us to know that whenever R is a semilocal subring of $\mathbb{Q}$, we have $\mathrm{HTP}(R) \leq_1 \mathrm{HTP}(\mathbb{Q})$. Indeed, both the Turing reduction and the 1-reduction are uniform in the complement. (The result essentially follows from work of Julia Robinson in [8]. For a proof by Eisenträger, Park, Shlapentokh, and the author, see [2].) Recall that the *semilocal* subrings of $\mathbb{Q}$ are precisely those of the form R_W where the set W is cofinite in $\mathbb{P}$, containing all but finitely many primes.

Proposition 1 (see Proposition 5.4 in [2]). *There exists a computable function G such that for every n, every finite set $A_0 = \{p_1, \ldots, p_n\} \subset \mathbb{P}$ and every $f \in \mathbb{Z}[\boldsymbol{X}]$,*

$$f \in \mathit{HTP}(R_{\mathbb{P}-A_0}) \iff G(f, \langle p_1, \ldots, p_n \rangle) \in \mathit{HTP}(\mathbb{Q}).$$

That is, $\mathit{HTP}(R_{\mathbb{P}-A_0})$ is 1-reducible to $\mathit{HTP}(\mathbb{Q})$ for all semilocal $R_{\mathbb{P}-A_0}$, uniformly in A_0. □

The proof in [2], using work from [3], actually shows how to compute, for every prime p, a polynomial $f_p(Z, X_1, X_2, X_3)$ such that for all rationals q, we have

$$q \in R_{\mathbb{P}-\{p\}} \iff f_p(q, \boldsymbol{X}) \in \mathrm{HTP}(\mathbb{Q}).$$

2 Baire Category and HTP($\mathbb{Q}$)

For a polynomial $f \in \mathbb{Z}[\boldsymbol{X}]$ and a subring $R_W \subseteq \mathbb{Q}$, there are three possibilities. First, f may lie in $\mathrm{HTP}(R_W)$. If this holds for R_W, the reason is finitary: W contains a certain finite (possibly empty) subset of primes generating the denominators of a solution. Second, there may be a finitary reason why $f \notin \mathrm{HTP}(R_W)$: there may exist a finite subset A_0 of the complement $\overline{W}$ such that f has no solution in $R_{\mathbb{P}-A_0}$. For each finite $A_0 \subset \mathbb{P}$, the set $\mathrm{HTP}(R_{\mathbb{P}-A_0})$ is 1-reducible to $\mathrm{HTP}(\mathbb{Q})$, by Proposition 1; indeed the two sets are computably isomorphic, with a computable permutation of $\mathbb{Z}[\boldsymbol{X}]$ mapping one onto the other. Therefore, the existence of such a set A_0 (still for one fixed f) is a $\Sigma_1^{\mathrm{HTP}(\mathbb{Q})}$ problem.

The third possibility is that neither of the first two holds. An example is given in [5], where it is shown that a particular polynomial f fails to lie in $\mathrm{HTP}(R_{W_3})$, where W_3 is the set of all primes congruent to 3 modulo 4, yet that, for every finite set V_0 of primes, there exists some W disjoint from V_0 with $f \in \mathrm{HTP}(R_W)$. We consider sets such as this W_3 to be on the *boundary* of f, in consideration of the topology of the situation. The set $\mathcal{A}(f) = \{W : f \in \mathrm{HTP}(R_W)\}$ is open in the usual topology on $2^{\mathbb{P}}$, since, for any solution of f in R_W and any $\sigma \subseteq W$ long enough to include all primes dividing the denominators in that solution, every other $V \supseteq \sigma$ will also contain that solution. Moreover, one can computably enumerate the collection of those σ such that the basic open set $\mathcal{U}_\sigma = \{W : \sigma \subseteq W\}$ is contained within $\mathcal{A}(f)$. The set $\mathrm{Int}(\overline{\mathcal{A}(f)})$ is similarly a union of basic open sets, and these can be enumerated by an $\mathrm{HTP}(\mathbb{Q})$-oracle, since $\mathrm{HTP}(\mathbb{Q})$ decides $\mathrm{HTP}(R)$ uniformly for every semilocal ring R. The *boundary* $\mathcal{B}(f)$ of f remains: it contains those W which lie neither in $\mathcal{A}(f)$ nor in $\mathrm{Int}(\overline{\mathcal{A}(f)})$. The boundary can be empty, but need not be, as seen in the example mentioned above.

It follows quickly from Baire category theory that the boundary set for a polynomial $f \in \mathbb{Z}[\boldsymbol{X}]$ must be nowhere dense. In general the boundary set $\partial\mathcal{A}$ of a set $\mathcal{A}$ within a space $\mathcal{S}$ is defined to equal $(\mathcal{S} - \mathrm{Int}(\mathcal{A}) - \mathrm{Int}(\overline{\mathcal{A}}))$, and thus is always closed.

Lemma 3. *For every open set $\mathcal{A}$ in a Baire space $\mathcal{S}$, the boundary set $\partial\mathcal{A}$ is nowhere dense. In particular, for each $f \in \mathbb{Z}[\boldsymbol{X}]$, the boundary set $\mathcal{B}(f) = \partial(\mathcal{A}(f))$ must be nowhere dense. Hence the* entire boundary set

$$\mathcal{B} = \{W \subseteq \mathbb{P} : (\exists f \in \mathbb{Z}[\boldsymbol{X}])\ W \in \mathcal{B}(f)\} = \cup_{f\in\mathbb{Z}[\boldsymbol{X}]}\mathcal{B}(f)$$

is meager.

Proof. Since $\mathcal{A}$ is open, every open subset $\mathcal{V}$ of the closure of $\partial\mathcal{A}$ (namely $\partial\mathcal{A}$ itself) lies within the complement $\overline{\mathcal{A}}$, hence within $\mathrm{Int}(\overline{\mathcal{A}})$, which is also disjoint from $\partial\mathcal{A}$. This proves that $\partial\mathcal{A}$ is nowhere dense. Hence $\mathcal{B}$, the countable union of such sets, is meager. □

For a set W to fail to lie in $\mathcal{B}$, it must be the case that for every polynomial f, either $f \in \mathrm{HTP}(R_W)$ or else some finite initial segment of W rules out all solutions to f. This is an example of the concept of *genericity*, common in both computability and set theory, so we adopt the term here. With this notion, we can show not only that $\mathrm{HTP}(R_W) \leq W \oplus \mathrm{HTP}(\mathbb{Q})$ for all W in the comeager set $\overline{\mathcal{B}}$, but indeed that the reduction is uniform on $\overline{\mathcal{B}}$.

Definition 2. *A set $W \subseteq \mathbb{P}$ is* HTP-generic *if $W \notin \mathcal{B}$. In this case we will also call the corresponding subring R_W HTP-generic. By Lemma 3, HTP-genericity is comeager.*

Proposition 2. *For every HTP-generic set W, $HTP(R_W) \equiv_T W \oplus HTP(\mathbb{Q})$, via uniform Turing reductions. Hence there is a single Turing reduction Φ such that the following set is comeager:*

$$\{W \subseteq \mathbb{P} : \Phi^{W\oplus HTP(\mathbb{Q})} = \chi_{HTP(R_W)}\}.$$

Proof. Given $f \in \mathbb{Z}[\boldsymbol{X}]$ as input, the program for Φ simply searches for either a solution $\boldsymbol{x}$ to $f = 0$ in $\mathbb{Q}$ for which all primes dividing the denominators lie in the oracle set W, or else a finite set $A_0 \subseteq \overline{W}$ such that the $\mathrm{HTP}(\mathbb{Q})$ oracle, using Proposition 1, confirms that $f \notin \mathrm{HTP}(R_{\mathbb{P}-A_0})$. When it finds either of these, it outputs the corresponding answer about membership of f in $\mathrm{HTP}(R_W)$. If it never finds either, then $W \in \mathcal{B}(f)$, and so this process succeeds for every W except those in the meager set $\mathcal{B}$. (The reduction $W \oplus \mathrm{HTP}(\mathbb{Q}) \leq_T \mathrm{HTP}(R_W)$ was described in Section 1.) □

Corollary 1. *For every set $C \subseteq \omega$, the following are equivalent*

1. *$C \leq_T HTP(\mathbb{Q})$.*

2. $\{W \subseteq \mathbb{P} : C \leq_T HTP(R_W)\} = 2^{\mathbb{P}}$.
3. $\{W \subseteq \mathbb{P} : C \leq_T HTP(R_W)\}$ *is not meager.*

This opens a new possible avenue to a proof of undecidability of HTP($\mathbb{Q}$): one need not address $\mathbb{Q}$ itself, but only show that for most subrings R_W, HTP(R_W) can decide the halting problem (or some other fixed undecidable set C). Constructions in the style of [6, Theorem 1.3] offer an approach to the problem along these lines: that theorem, proven by Poonen, shows that the set of subrings R with $\emptyset' \leq_T$ HTP(R) has size continuum and is large in certain other senses. Poonen constructs decidable subsets $T_0, T_1 \subseteq \mathbb{P}$, both of asymptotic density 0 within $\mathbb{P}$, such that for every $W \subseteq \mathbb{P}$ with $T_0 \subseteq W$ and $T_1 \cap W = \emptyset$, the subring R_W has $\emptyset' \leq_T$ HTP(R_W). This feels like a substantial collection of subrings, but the conditions $T_0 \subseteq W$ and $T_1 \cap W = \emptyset$ each imply that this set of subrings is nowhere dense, and therefore this set does not by itself enable us to apply Corollary 1. Moreover, it is not clear that any of Poonen's subrings need be HTP-generic.

Proof. Trivially ($1 \implies 2 \implies 3$), since all W satisfy HTP($\mathbb{Q}$) $\leq_T$ HTP(R_W). So assume (3). Then by Proposition 2, $C \leq_T W \oplus$ HTP($\mathbb{Q}$) holds on a non-meager set, as the intersection of a non-meager set with a comeager set cannot be meager. So by Lemma 2, $C \leq_T$ HTP($\mathbb{Q}$). □

Having examined classes of subsets of $\mathbb{P}$ defined by Turing reductions involving HTP(R_W), we now replace Turing reducibility by 1-reducibility and ask similar questions about classes so defined. It is not known whether there exists a subring $R \subseteq \mathbb{Q}$ for which $\emptyset' \leq_T$ HTP(R_W) but $\emptyset' \not\leq_1$ HTP(R_W), and we have no good candidates for such a subring. Ever since the original proof of undecidability of Hilbert's Tenth Problem in [1, 4], every Turing reduction ever given from the Halting Problem to any HTP(R) with $R \subseteq \mathbb{Q}$ has in fact been a 1-reduction. Of course, if $\emptyset' \leq_1$ HTP($\mathbb{Q}$), then $\emptyset' \leq_1$ HTP(R) for all subrings R, so in some sense $\mathbb{Q}$ itself is the "only" candidate.

We have a result for 1-reducibility analogous to Corollary 1, but the proof is somewhat different.

Theorem 1. *For every set $C \subseteq \omega$ with $C \not\leq_1$ HTP($\mathbb{Q}$), the following class is meager:*

$$\mathcal{O} = \{W \subseteq \mathbb{P} : C \leq_1 HTP(R_W)\}.$$

Proof. One naturally views $\mathcal{O}$ as the union of countably many subclasses $\mathcal{O}_e = \{W \subseteq \mathbb{P} : C \leq_1 \text{HTP}(R_W) \text{ via } \varphi_e\}$. Of course, for those e for which the e-th Turing function φ_e is not total, this class is empty. We claim that if any one of these $\mathcal{O}_e$ fails to be nowhere dense, then $C \leq_1$ HTP($\mathbb{Q}$), contrary to the assumption of the theorem.

Suppose that indeed $\mathcal{O}_e$ fails to be nowhere dense, and fix a σ for which $\mathcal{U}_\sigma \subseteq \text{cl}(\mathcal{O}_e)$. Let $A_0 = \sigma^{-1}(0)$ contain those primes excluded from all $W \in \mathcal{U}_\sigma$, and set $R = R_{(\mathbb{P}-A_0)}$. Now whenever $n \in C$ and $W \in \mathcal{O}_e$, the polynomial $\varphi_e(n)$ must lie in HTP(R_W). Since some $W \in \mathcal{O}_e$ lies in U_σ, we must have

$\varphi_e(n) \in \mathrm{HTP}(R)$, because $R_W \subseteq R$ whenever $W \in \mathcal{U}_\sigma$. On the other hand, suppose $n \notin C$. If R contained a solution to the polynomial $\varphi_e(n)$, then some $\tau \supseteq \sigma$ would by itself invert the finitely many primes required to generate this solution, and thus we would have $\mathcal{U}_\tau \cap \mathcal{O}_e = \emptyset$. With $\mathcal{U}_\sigma \subseteq \mathrm{cl}(\mathcal{O}_e)$, this is impossible, and so, whenever $n \notin C$, we have $\varphi_e(n) \notin \mathrm{HTP}(R)$.

Thus R itself lies in $\mathcal{O}_e$, as φ_e is a 1-reduction from C to $\mathrm{HTP}(R)$. But R is semilocal, inverting all primes p except those with $\sigma(p) = 0$. By Proposition 1, we have $\mathrm{HTP}(R) \leq_1 \mathrm{HTP}(\mathbb{Q})$, and so $C \leq_1 \mathrm{HTP}(\mathbb{Q})$. □

Now we prove two similar results, one about subrings of $\mathbb{Q}$ which admit diophantine models and one about subrings which admit existential definitions of the integers within the subring. In both cases, the result is a sort of zero-one law: that the given phenomenon must either hold almost everywhere (i.e., on a comeager set of subrings) or almost nowhere (i.e., on a meager set). We begin with the diophantine models.

Definition 3. *In a ring R, a* diophantine model of $\mathbb{Z}$ *consists of three polynomials h, h_+, and $h_\times$, with $h \in R[X_1, \ldots, X_n, \boldsymbol{Y}]$ and $h_+, h_\times \in R[X_1, \ldots, X_{3n}, \boldsymbol{Y}]$ (for some n), such that the set*

$$\{\boldsymbol{x} \in R^n : (\exists \boldsymbol{y} \in R^{<\omega})\ h(\boldsymbol{x}, \boldsymbol{y}) = 0\}$$

(equivalently, $\{\boldsymbol{x} \in R^n : h(\boldsymbol{x}, \boldsymbol{Y}) \in HTP(R)\}$) is isomorphic to the structure $(\mathbb{Z}, +, \cdot)$ under the binary operations whose graphs are defined by

$$\{(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3) \in R^{3n} : h_+(\boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{x}_3, \boldsymbol{Y}) \in HTP(R)\}$$

for addition and the corresponding set with $h_\times$ for multiplication.

If a computable ring R admits a diophantine model of $\mathbb{Z}$, then $\mathrm{HTP}(\mathbb{Z})$ can be coded into $\mathrm{HTP}(R)$, and so $\emptyset' \equiv_1 \mathrm{HTP}(\mathbb{Z}) \leq_1 \mathrm{HTP}(R)$. For subrings R_W of $\mathbb{Q}$ for which $\emptyset' \not\leq_T W$, this is the only known method of showing that $\emptyset' \leq_T \mathrm{HTP}(R_W)$ (apart from the original proof by Matiyasevich, Davis, Putnam, and Robinson for the case $W = \emptyset$, of course, which is what allows this method to succeed).

Definition 4. $\mathcal{D} = \{W \subseteq \mathbb{P} : R_W$ *admits a diophantine model of* $\mathbb{Z}\}$.

In this section we address the question of the size of the class $\mathcal{D}$. The main result fails to resolve this question, but shows it to have an "all-or-nothing" character.

Theorem 2. *The class $\mathcal{D}$ is non-meager if and only if there exists a particular triple $(h, h_+, h_\times)$ of polynomials over $\mathbb{Z}$ and a finite binary string $\sigma \in 2^{<\mathbb{P}}$ such that, for every HTP-generic $V \in \mathcal{U}_\sigma$, R_V admits a diophantine model of $\mathbb{Z}$ via these three polynomials.*

Moreover, if $\mathcal{D}$ is non-meager, then $\mathbb{P} \in \mathcal{D}$ (i.e., $\mathbb{Q}$ admits a diophantine model of $\mathbb{Z}$).

Proof. For each triple $\boldsymbol{h} = (h, h_+, h_\times)$ of polynomials of appropriate lengths over $\mathbb{Z}$, we set $\mathcal{D}_{\boldsymbol{h}}$ to contain those W for which $\boldsymbol{h}$ defines a diophantine model of $\mathbb{Z}$ within R_W. If each $\mathcal{D}_{\boldsymbol{h}}$ is nowhere dense, their countable union $\mathcal{D}$ is meager.

Now suppose that $\mathcal{D}$ is non-meager, so some class $\mathcal{D}_{\boldsymbol{h}}$ fails to be nowhere dense. Then there must be a string σ such that $\mathcal{U}_\sigma \subseteq \mathrm{cl}(\mathcal{D}_{\boldsymbol{h}})$. Using this σ and this $\boldsymbol{h}$, we now prove the main claim: all $W \in \mathcal{U}_\sigma$ with HTP-generic R_W lie in $\mathcal{D}_{\boldsymbol{h}}$. Let $R_0 = R_{\sigma^{-1}(1)}$ and $R_1 = R_{\mathbb{P}-\sigma^{-1}(0)}$ be the smallest and largest subrings (under $\subseteq$) in $\mathcal{U}_\sigma$, so R_0 is finitely generated and R_1 is semilocal.

Fix a single $W \supset \sigma$ with $W \in \mathcal{D}_{\boldsymbol{h}}$, and fix the tuples $\boldsymbol{x}_0$ and $\boldsymbol{x}_1$ from R_W which represent the elements 0 and 1 in the diophantine model defined in R_W by $\boldsymbol{h}$. It follows that $h_\times(\boldsymbol{x}_0, \boldsymbol{x}_0, \boldsymbol{x}_0, \boldsymbol{Y}) \in \mathrm{HTP}(R_W)$ and $h_\times(\boldsymbol{x}_1, \boldsymbol{x}_1, \boldsymbol{x}_1, \boldsymbol{Y}) \in \mathrm{HTP}(R_W)$. Now if any other tuple $\boldsymbol{x}$ from R_1 had $h(\boldsymbol{x}, \boldsymbol{Y}) \in \mathrm{HTP}(R_1)$ and $h_\times(\boldsymbol{x}, \boldsymbol{x}, \boldsymbol{x}, \boldsymbol{Y}) \in \mathrm{HTP}(R_1)$, then we could set $\tau = \sigma\hat{\ }111\cdots 1$ to contain enough primes that $R_{\tau^{-1}(1)}$ would contain $\boldsymbol{x}$, $\boldsymbol{x}_0$, and $\boldsymbol{x}_1$. This would mean that $\boldsymbol{h}$ could not define a diophantine model of $\mathbb{Z}$ in any R_V with $V \in \mathcal{U}_\tau$, contrary to hypothesis. Therefore, no other $\boldsymbol{x}$ from R_1 can do this. Now suppose that $\boldsymbol{x}_0$ does *not* lie within R_0. In this case, some extension $\rho = \sigma\hat{\ }000\cdots 0$ would exclude enough primes to ensure that $\boldsymbol{x}_0$ does not lie in $R_{\mathbb{P}-\rho^{-1}(0)}$, and then no $\tau \supseteq \rho$ would admit a diophantine model via $\boldsymbol{h}$, since no other tuple with the right properties lies in R_1. Again, this contradicts our hypothesis that $\mathcal{U}_\sigma \subseteq \mathrm{cl}(\mathcal{D}_{\boldsymbol{h}})$, since $\mathcal{D}_{\boldsymbol{h}} \cap \mathcal{U}_\rho$ would be empty, and so $\boldsymbol{x}_0$ lies in R_0. Similarly so does $\boldsymbol{x}_1$.

Now one proceeds by induction on the subsequent elements of the diophantine model in R_1. Some tuple $\boldsymbol{x}_2$ from R_W must satisfy $h(\boldsymbol{x}_2, \boldsymbol{Y}) \in \mathrm{HTP}(R_W)$ and $h_+(\boldsymbol{x}_1, \boldsymbol{x}_1, \boldsymbol{x}_2, \boldsymbol{Y}) \in \mathrm{HTP}(R_W)$, and by the same arguments as above, we see that $\boldsymbol{x}_2$ is the only tuple in R_1 with this property, and then that $\boldsymbol{x}_2$ actually lies in R_0. Likewise, $\boldsymbol{x}_{-1}$ must satisfy $h(\boldsymbol{x}_{-1}, \boldsymbol{Y}) \in \mathrm{HTP}(R_W)$ and $h_+(\boldsymbol{x}_1, \boldsymbol{x}_{-1}, \boldsymbol{x}_0, \boldsymbol{Y}) \in \mathrm{HTP}(R_W)$, and again this forces $\boldsymbol{x}_{-1}$ to lie in R_0 and to be the unique tuple with these properties in R_1.

Continuing this induction, we see that every tuple in the domain of the diophantine model of $\mathbb{Z}$ in R_W actually lies in R_0, and hence in every R_W with $W \in \mathcal{U}_\sigma$; and moreover that these are the only tuples $\boldsymbol{x}$ in R_1 for which $h(\boldsymbol{x}, \boldsymbol{Y}) \in \mathrm{HTP}(R_1)$. Likewise, if some $\boldsymbol{x}_m$, $\boldsymbol{x}_n$ and $\boldsymbol{x}_p$ (representing m, n, and p in the diophantine model) satisfy $h_+(\boldsymbol{x}_m, \boldsymbol{x}_n, \boldsymbol{x}_p, \boldsymbol{Y}) \in \mathrm{HTP}(R_1)$, then for some k, $\tau = \sigma\hat{\ }1^k$ is long enough to ensure that every W extending τ must have $h_+(\boldsymbol{x}_m, \boldsymbol{x}_n, \boldsymbol{x}_p, \boldsymbol{Y}) \in \mathrm{HTP}(R_W)$. But some such W lies in $\mathcal{D}_{\boldsymbol{h}}$, so we must have $m + n = p$. The same works for $h_\times$, so $\boldsymbol{h}$ defines a diophantine model of $\mathbb{Z}$ in R_1.

It is not clear whether $\boldsymbol{h}$ defines a diophantine model in the subring R_0 (which, being finitely generated, lies in $\mathcal{B}$). The domain elements of the model in R_1 all lie in R_0, but the witnesses might not. However, suppose that $V \in \mathcal{U}_\sigma$ is HTP-generic, and fix any domain element $\boldsymbol{x}$. Let $\tau = V \restriction m$, for any $m \geq |\sigma|$. Then some $U \supseteq \tau$ lies in $\mathcal{D}_{\boldsymbol{h}}$, and so some extension of τ yields a solution to $h(\boldsymbol{x}, \boldsymbol{Y})$. Since V is HTP-generic (that is, $V \notin \mathcal{B}$), this forces $h(\boldsymbol{x}, \boldsymbol{Y}) \in \mathrm{HTP}(R_V)$. Likewise, for each fact coded by h_+ or $h_\times$ about domain elements of the model, some extension of $V \restriction m$ must yield a witness to that fact, and therefore

R_V itself contains such a witness. So $\boldsymbol{h}$ defines this same diophantine model in *every* HTP-generic subring R_V with $V \in \mathcal{U}_\sigma$, as required by the theorem.

Cases (1) and (2) of the theorem cannot both hold, because under (2), $\mathcal{U}_\sigma \cap \overline{\mathcal{B}}$ would be a nonmeager subset of $\mathcal{D}$. Moreover, the 1-reduction HTP$(R_1) \leq_1$ HTP$(\mathbb{Q})$ given in [2, Proposition 5.4] has sufficient uniformity that the images of h, h_+, and $h_\times$ under this reduction define a diophantine model of $\mathbb{Z}$ inside $\mathbb{Q}$. (Specifically, $h(\boldsymbol{X}, \boldsymbol{Y})$ maps to the sum of h^2 with several other squares of polynomials in such a way as to guarantee that all solutions use values from R_1 for the variables $\boldsymbol{X}$ and $\boldsymbol{Y}$; likewise with h_+ and $h_\times$.) This proves the final statement of the theorem. □

Now we continue with the question of existential definability of the integers.

Definition 5. *In a ring R, a polynomial $g \in \mathbb{Z}[X, \boldsymbol{Y}]$* existentially defines $\mathbb{Z}$ *if, for every $q \in R$,*

$$q \in \mathbb{Z} \iff g(q, \boldsymbol{Y}) \in \mathit{HTP}(R).$$

$\mathbb{Z}$ *is* existentially definable in R *if such a polynomial g exists.*

A ring in which $\mathbb{Z}$ is existentially definable must admit a very simple diophantine model of $\mathbb{Z}$, given by the polynomial g along with $h_+ = X_1 + X_2 - X_3$ and $h_\times = X_1 X_2 - X_3$. The question of definability of $\mathbb{Z}$ in the field $\mathbb{Q}$ was originally answered by Julia Robinson (see [8]), who gave a Π_4 definition. Subsequent work by Poonen [7] and then Koenigsmann [3] has resulted in a Π_1 definition of $\mathbb{Z}$ in $\mathbb{Q}$, but it remains unknown whether any existential formula defines $\mathbb{Z}$ there.

Definition 6. *$\mathcal{E}$ is the class of subrings of $\mathbb{Q}$ where $\mathbb{Z}$ is existentially definable:*

$$\mathcal{E} = \{W \subseteq \mathbb{P} : \mathbb{Z} \textit{ is existentially definable in } R_W\}.$$

We now address the question of the size of the class $\mathcal{E}$. As with $\mathcal{D}$, we show $\mathcal{E}$ to be either very large or very small, in the sense of Baire category.

Theorem 3. *The following are equivalent.*

1. *The class $\mathcal{E}$ is not meager.*
2. *There is a $\sigma \in 2^{<\mathbb{P}}$, and a single polynomial g which existentially defines $\mathbb{Z}$ in all HTP-generic subrings R_V with $V \in \mathcal{U}_\sigma$.*
3. *$\mathbb{P} \in \mathcal{E}$; that is, $\mathbb{Z}$ is existentially definable in $\mathbb{Q}$.*
4. *There is a single existential formula which defines $\mathbb{Z}$ in every subring of $\mathbb{Q}$.*

Proof. The proof that (1) $\implies$ (2) $\implies$ (3) proceeds along the same lines as that of Theorem 2, with $\mathcal{E}_g$ as the class of those W for which the polynomial g existentially defines $\mathbb{Z}$ within R_W. If every one of these classes is nowhere dense, then their countable union $\mathcal{E}$ is meager. Otherwise one proves (2), and from that (3), by a simplification of the same method as before, with no induction required. To see that (3) implies (4), notice that if $\mathbb{Z}$ is defined in $\mathbb{Q}$ by the formula $\exists \boldsymbol{Y}\ f(X, \boldsymbol{Y}) = 0$, and d is the total degree of f, then the formula

$$\exists \boldsymbol{Y} \exists Z\ [Z^d \cdot f\left(X, \frac{Y_1}{Z}, \ldots, \frac{Y_n}{Z}\right) = 0\ \&\ Z > 0]$$

defines $\mathbb{Z}$ in R_W. □

It is possible to turn Theorem 2 into an equivalence analogous to that in Theorem 3, with the third condition stating that $\mathbb{P} \in \mathcal{D}$. As far as we know, however, it is necessary to consider diophantine *interpretations* in subrings R_W, rather than diophantine models, in order to accomplish this.

3 Measure Theory

Normally there is a strong connection between measure theory and Baire category theory. Each defines a certain Σ-ideal of sets to be "small": the sets of measure 0, and the meager sets. In Cantor space, neither of these properties implies the other, but empirically they appear closely connected, especially when the sets are given by natural definitions: sets of measure 0 are often meager, and vice versa. (Exceptions to this principle do exist, however, and another difference was mentioned in the context of Lemma 1.)

Our results here rely heavily on the simple Lemma 3, stating that the boundary set $\mathcal{B}(f)$ of a polynomial f is nowhere dense. Most of our subsequent results have measure-theoretic analogues which would go through fairly easily, provided that these sets $\mathcal{B}(f)$ also have measure 0. However, determining the measure of the boundary set of a polynomial appears to be a nontrivial problem. It is unknown whether there exists any polynomial f for which $\mu(\mathcal{B}(f)) > 0$. Indeed, in work to appear elsewhere, the author has shown that if $\mu(\mathcal{B}(f)) = 0$ for all $f \in \mathbb{Z}[\boldsymbol{X}]$, then there is no existential definition of the set $\mathbb{Z}$ within the field $\mathbb{Q}$.

Moreover, if an f exists with $\mu(\mathcal{B}(f)) > 0$, it is unclear what other constraints on the real number $\mu(\mathcal{B}(f))$ exist, apart from the computability-theoretic upper bound given by its definition as $\mu(\mathcal{B}(f))$. Could such a number be transcendental? Or noncomputable? If not, is there an algorithm computing $\mu(\mathcal{B}(f))$ uniformly in f? These appear to be challenging questions, often with a more number-theoretic flavor than most of this article. Resolving them might make it possible to determine whether Hilbert's Tenth Problem on subrings of $\mathbb{Q}$ has measure-theoretic zero-one laws similar to those proven here for Baire category.

References

1. M. Davis, H. Putnam, and J. Robinson. The decision problem for exponential diophantine equations. *Annals of Mathematics (2)*, 74:425–436, 1961.
2. K. Eisenträger, R. Miller, J. Park, and A. Shlapentokh. As easy as $\mathbb{Q}$: Hilbert's Tenth Problem for subrings of the rationals, submitted for publication.
3. J. Koenigsmann. Defining $\mathbb{Z}$ in $\mathbb{Q}$. *Annals of Math.*, 183(1):73–93, 2016.
4. Yu. Matijasevič. The Diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*, 191:279–282, 1970.
5. R. Miller. Measure theory and Hilbert's Tenth Problem inside $\mathbb{Q}$, submitted.
6. B. Poonen. Hilbert's Tenth Problem and Mazur's conjecture for large subrings of $\mathbb{Q}$. *Journal of the AMS*, 16(4):981–990, 2003.
7. B. Poonen. Characterizing integers among rational numbers with a universal-existential formula. *American Journal of Mathematics*, 131(3):675–682, 2009.
8. J. Robinson. Definability and decision problems in arithmetic. *Journal of Symbolic Logic*, 14:98–114, 1949.