Measure theory and Hilbert's Tenth Problem inside $\mathbb{Q}$

Russell Miller [*]

October 5, 2016

Abstract

For a ring R, Hilbert's Tenth Problem HTP(R) is the set of polynomial equations over R, in several variables, with solutions in R. When $R = \mathbb{Z}$, it is known that the jump $\mathbb{Z}'$ is Turing-reducible to HTP($\mathbb{Z}$). We consider computability of HTP(R) for subrings R of the rationals. Applying measure theory to these subrings, which naturally form a measure space, relates their sets HTP(R) to the set HTP($\mathbb{Q}$), whose decidability remains an open question. We raise the question of the measure of the topological boundary of the solution set of a polynomial within this space, and show that if these boundaries all have measure 0, then for each individual oracle Turing machine Φ, the reduction $R' = \Phi^{\mathrm{HTP}(R)}$ fails on a set of subrings R of positive measure. That is, no Turing reduction of the jump R' of a subring R to HTP(R) holds uniformly on a set of measure 1.

1 Introduction

The original version of Hilbert's Tenth Problem demanded an algorithm deciding which polynomial equations from $\mathbb{Z}[X_0, X_1, \ldots]$ have solutions in integers. In 1970, Matiyasevic [5] completed work by Davis, Putnam and

[*] The author was partially supported by Grant # DMS − 1362206 from the National Science Foundation, and by several grants from the PSC-CUNY Research Award Program. This work grew out of research initiated at a workshop held at the American Institute of Mathematics and continued at a workshop held at the Institute for Mathematical Sciences of the National University of Singapore. The author wishes to acknowledge useful conversations with Bjorn Poonen and Alexandra Shlapentokh.

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 $h \in \mathbb{Z}[X, \vec{Y}]$ such that, for each n from the set ω of nonnegative integers, the polynomial $h(n, \vec{Y}) = 0$ 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

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

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 $\mathrm{HTP}(R)$ reduces to the question of deciding this membership just for polynomials from $\mathbb{Z}[\vec{X}]$, since one readily eliminates denominators from the coefficients of a polynomial in $R[\vec{X}]$. So, for us, $\mathrm{HTP}(R)$ 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 $\mathrm{HTP}(R)$, will be viewed as subsets of ω, using a fixed computable bijection from ω onto $\mathbb{Z}[\vec{X}] = \mathbb{Z}[X_0, X_1, \ldots]$.

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 class $\mathbf{Sub}(\mathbb{Q})$ 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 $\mathbf{Sub}(\mathbb{Q})$: 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 $\mathcal{S}$.

It is also natural, and in certain respects more productive, to consider Baire category theory on the space $\mathbf{Sub}(\mathbb{Q})$, as an alternative to measure theory. Here we will focus on measure theory. For questions and results regarding Baire category theory on subrings of $\mathbb{Q}$, we refer the reader to the forthcoming [6]. Due to the common subject matter of that article and this one, there is a substantial overlap between the introductions and background sections of the two papers, which we trust the reader to forgive. Naturally, we have also made every effort to maintain the same notation across both papers.

2 Background

2.1 Measure Theory and Cantor Space

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 $2^{<\omega}$. We assign to the basic open set

$$\mathcal{U}_{\sigma} = \{W \subseteq \mathbb{P} : (\forall n < |\sigma|)\ [n \in W \iff \sigma(n) = 1\}$$

the measure $2^{-|\sigma|}$, as in the standard Lebesgue measure on 2^{ω}, and extend this measure to all Lebesgue-measurable subsets of $2^{\mathbb{P}}$. Thus we have a natural measure on the space of all subrings R_W of $\mathbb{Q}$.

All sets $W \subseteq \omega$ satisfy $W \oplus \emptyset' \leq_T W'$, and for certain W, Turing-equivalence holds here. Those W for which $W \equiv_T W \oplus \emptyset'$ are said to be *generalized-low*, and it turns out that this is the standard situation, according to both measure and Baire category.

Lemma 2.1 (Folklore) *The class*

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

of generalized-low sets is comeager and has measure 1 *in* 2^{ω}. *However, there is no single Turing functional* Φ_e *for which the subclass*

$$\boldsymbol{GL}_{1,e} = \{W \in 2^{\omega} : W' = \Phi_e^{W \oplus \emptyset'}\}$$

has measure 1.

We express the content of the second statement by saying that although $W' \leq_T W \oplus \emptyset'$ on a set of measure 1, the reduction is *nonuniform.* This contrasts with the situation in Baire category, where a single Turing reduction does succeed on a comeager set.

We give the full proof of the measure-theoretic statements in Lemma 2.1 even though they are well known. They will be illustrative when we come to consider measures of boundary sets of polynomials.

Proof. First, for an arbitrary rational $\varepsilon > 0$, we describe a Turing reduction Φ_e for which $\mu(\mathbf{GL}_{1,e}) \geq 1 - \varepsilon$. This will prove that $\mathbf{GL}_1$ has measure 1.

With an oracle $W \oplus \emptyset'$, on input x, the functional Φ_e simultaneously performs two searches. At each stage s, it checks the first s strings $\sigma \in 2^{<\omega}$. Whenever it finds a σ for which $\Phi^{\sigma}_{x,s}(x)\!\downarrow$, it enumerates this σ into its set $S_{x,s}$. Simultaneously, for the s-th rational r, it asks its $\emptyset'$ oracle whether

$$(\exists t\ \exists\langle\sigma_0,\ldots,\sigma_n\rangle \in (2^{<\omega})^{<\omega})\ [\mu(\cup_i \mathcal{U}_{\sigma_i}) > r\ \&\ (\forall i \leq n)\Phi^{\sigma_i}_{x,t}(x)\!\downarrow].$$

If this statement is false, it enumerates that r into its set $R_{x,s}$. (We start with $r = 1$ in $R_{x,0}$, since the statement must be false for this r.)

These searches continue until we reach a stage s at which some r in $R_{x,s}$ has the property that $\mu(\cup_{\sigma \in S_{x,s}} \mathcal{U}_\sigma) + \frac{\varepsilon}{2^{x+1}} \geq r$. Since $\mu(\cup_{\sigma \in S_x} \mathcal{U}_\sigma)$ (where $S_x = \cup_s S_{x,s}$) must equal the infimum of the subset $\cup_s R_{x,s}$ of $\mathbb{Q}$, it is clear that this process eventually halts. When it does, we use the W-oracle to check whether any of the finitely many σ already in $S_{x,s}$ is an initial segment of W. If so, we conclude that $\Phi^W_x(x)\!\downarrow$; if not, we conclude that $\Phi^W_x(x)\!\uparrow$.

Of course, this conclusion will not always be correct. However, it fails only on the class of those W for which $\Phi^W_x(x)\!\downarrow$ but no initial segment of W lies in the finite set $S_{x,s}$ we had enumerated by the stage s at which the process halted. The class of all these W must have measure $\leq \frac{\varepsilon}{2^{x+1}}$, since $S_x = \{W : \Phi^W_x(x)\!\downarrow\}$, which has measure $\leq r$, and at least $r - \frac{\varepsilon}{2^{x+1}}$ of this set has initial segments in $S_{x,s}$. Since the process gives the wrong answer (on input x) only for a class of measure $\leq \frac{\varepsilon}{2^{x+1}}$, the class of all W such that, for that W and some x, it gives the wrong answer is a class of measure $\leq \varepsilon$, as required.

Now we prove the nonuniformity, by constructing (the index x of) a specific program. Fix an effective numbering $\sigma_0 = \langle\rangle$, $\sigma_1 = \langle 0\rangle$, $\sigma_2 = \langle 1\rangle, \ldots$ of all of $2^{<\omega}$. The function Φ_x, on arbitrary input, halts if and only if there exists an n such that its oracle has initial segment $\sigma_n\widehat{\ }1^{n+2}$ (that is, σ_n followed by $(n+2)$ consecutive 1's). Notice that the class $\mathcal{A}$ of all W such that

$\Phi_x^W(x)\downarrow$ has measure $\leq \sum_n 2^{-|\sigma_n|-n-2} \leq \sum_n 2^{-(n+2)} = \frac{1}{2}$. It follows that, if a functional Φ_e computes W' from $W \oplus \emptyset'$ uniformly on a class of measure 1, then there must be sets W for which $\Phi_e^W(x)\downarrow= 0$. However, the initial segment $\sigma \subseteq W$ used in this computation is equal to σ_n for some n, and then $\Phi_e^V(x)$ must give the same output 0, incorrectly, on each V in the basic open set $\mathcal{U}_{\sigma_n \frown 1^{n+2}}$. Since each basic open set has positive measure, we see that Φ_e fails, on a class of positive measure, to compute W' from $W \oplus \emptyset'$ correctly. ■

The proof of Lemma 2.1 showed that $\mathbf{GL}_1$ had measure 1 by showing that, for each $\varepsilon > 0$, a single Turing functional could compute W' from $W \oplus \emptyset'$ correctly on a set of measure $> 1 - \varepsilon$. This near-uniformity may sound like a useful fact, but in fact the next lemma can be adapted to show that it has to be the case in order for that lemma to be true at all.

Lemma 2.2 *(Folklore) Suppose $\mu\{W : A \oplus W \geq_T B\} > r$. Then there exists a single Turing functional Ψ such that $\mu\{W : \Psi^{A \oplus W} = B\} > r$.*

Proof. The idea is that we glue finitely many functionals together, using initial segments of the different W to choose which one to run. Formally, set $r + \varepsilon = \mu\{W : A \oplus W \geq_T B\}$. Since there are only countably many Turing functionals in all, there must exist finitely many functionals $\Psi_0, \ldots, \Psi_m$ such that

$$\mu\{W : (\exists e \leq m)\ \Psi_e^{A \oplus W} = B\} > r + \frac{\varepsilon}{2}.$$

But then, for each $e \leq m$, there must also exist finitely many initial segments $\sigma_{e0}, \ldots, \sigma_{ek_e}$ such that

$$\sum_{e \leq m} \mu\{W : (\exists j \leq k_e)\ [\sigma_{ej} \subseteq W \ \&\ \Psi_e^{A \oplus W} = B]\} > r + \frac{\varepsilon}{4},$$

and such that all these σ_{ej} are pairwise incomparable. So the desired functional Ψ, given any oracle $V \oplus W$, checks to see whether any of the finitely many σ_{ej} is an initial segment of W: if so, it runs Ψ_e on its oracle, while if not, it simply diverges. ■

Lemma 2.3 *(Folklore) Let $A \not\geq_T B$. Then the class $\mathcal{C} = \{W : A \oplus W \geq_T B\}$ has measure 0.*

Proof. If $\mu(\mathcal{C}) > 0$, then there is some σ for which $\frac{\mu(\mathcal{C}\cap\mathcal{U}_\sigma)}{\mu(\mathcal{U}_\sigma)} > \frac{1}{2}$. (See e.g. [4, Lemma 3.1a] for a proof of this result, which is standard. The broader principle is the *Zero-One Law*, which states that all measurable subsets of 2^ω invariant under Turing equivalence have measure either 0 or 1.) Let $\delta = \mu(\mathcal{U}_\sigma) = \frac{1}{2^{|\sigma|}}$, and pick $\varepsilon > 0$ so that $\mu(\mathcal{C}\cap\mathcal{U}_\sigma) = \frac{\delta}{2} + \varepsilon$. Now by Lemma 2.2, there is a single Turing functional Φ such that $\Phi^{A\oplus W} = B$ for all W in a subclass of $\mathcal{U}_\sigma$ of measure $\frac{\delta}{2} + \frac{\varepsilon}{2}$. But then we could compute B directly from A: $B(x) = n$ iff there exist finitely many pairwise-incomparable strings $\tau \supseteq \sigma$ of total measure $> \frac{\delta}{2}$ for which $\Phi^{A\oplus\tau}(x)\downarrow = n$. ■

In [11], Stillwell went much further, proving the decidability of the entire almost-everywhere theory of the Turing degrees under meet, join, and jump. (The class of pairs of sets A and B for which the meet $A \wedge B$ is defined has measure 1, so it is reasonable to discuss the almost-everywhere theory with $\wedge$ as a binary function.)

2.2 Subrings of the Rationals

Now we turn to background results specifically about subrings of $\mathbb{Q}$. For all $W \subseteq \mathbb{P}$, we have the Turing reductions

$$W \oplus \mathrm{HTP}(\mathbb{Q}) \leq_T \mathrm{HTP}(R_W) \leq_T W'.$$

Indeed, each of these two Turing reductions is a 1*-reduction*. For instance, the Turing reduction from $HTP(R_W)$ to W' can be described by a computable injection which maps each $f \in \mathbb{Z}[\vec{X}]$ to the code number $h(f)$ of an oracle Turing program which, on every input, searches for a solution $\vec{x}$ in $\mathbb{Q}$ to the equation $f = 0$ for which the primes dividing the denominators of the coordinates in $\vec{x}$ all lie in the oracle set W. The reduction $W \leq_T \mathrm{HTP}(R_W)$ is simple: $p \in W$ if and only if $(pX - 1) \in \mathrm{HTP}(R_W)$. The reduction from $\mathrm{HTP}(\mathbb{Q})$ to $\mathrm{HTP}(R_W)$ uses the fact that every element of $\mathbb{Q}$ is a quotient of elements of R_W, so that $f(\vec{X})$ 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 $Y > 0$. (Here d is the total degree of f, so that Y^d suffices to cancel all denominators.) Since the Four Squares Theorem ensures that every nonnegative integer is a sum of four squares of integers, we may express the condition $Y > 0$ by a polynomial: if a rational y is positive, then there is a solution in $\mathbb{Z}$ to:

$$h(y, U_1, \ldots, U_4, V_1, \ldots, V_4) = y(1 + V_1^2 + \cdots + V_4^2) - (1 + U_1^2 + \cdots + U_4^2).$$

Conversely, any solution in $\mathbb{Q}$ to $h(y,\vec{U},\vec{V})=0$ forces $y>0$. It follows that when $y>0$, this polynomial has a solution in every subring of $\mathbb{Q}$, while when $y \leq 0$, it has no solution in any subring. Therefore we may use it within any subring we like, to define the positive elements there. From all this we see (for arbitrary W) that $f \in \mathrm{HTP}(\mathbb{Q})$ if and only if the following polynomial lies in $\mathrm{HTP}(R_W)$:

$$\left(Y^d \cdot f\left(\frac{X_1}{Y},\ldots,\frac{X_n}{Y}\right)\right)^2 + (h(Y,\vec{U},\vec{V}))^2.$$

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. 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. This result, stated formally below, essentially follows from work of Julia Robinson in [9]. For a proof by Eisenträger, Park, Shlapentokh, and the author, see [2].

Proposition 2.4 (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 $f \in \mathbb{Z}[\vec{X}]$,*

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

That is, $HTP(R_{\mathbb{P}-A_0})$ is 1-reducible to $HTP(\mathbb{Q})$ 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

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

Therefore, an arbitrary $g(Z_0,\ldots,Z_n)$ has a solution in $R_{\mathbb{P}-A_0}$ if and only if

$$(g(\vec{Z}))^2 + \sum_{p\in A_0, j\leq n} (f_p(Z_j,X_{1j},X_{2j},X_{3j}))^2$$

has a solution in $\mathbb{Q}$.

3 The Boundary Set of a Polynomial

For a polynomial $f \in \mathbb{Z}[\vec{X}]$ and a subring $R_W \subseteq \mathbb{Q}$, there are three possibilities. First, f may lie in $\text{HTP}(R_W)$. 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. For this reason, the set $\mathcal{A}(f) = \{W : f \in \text{HTP}(R_W)\}$ is open: 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.

The second possibility is that there may be a finitary reason why $f \notin \text{HTP}(R_W)$: 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 $\text{HTP}(R_{\mathbb{P}-A_0})$ is 1-reducible to $\text{HTP}(\mathbb{Q})$, by Proposition 2.4; indeed the two sets are computably isomorphic, with a computable permutation of $\mathbb{Z}[\vec{X}]$ mapping one onto the other. We write

$$\mathcal{C}(f) = \{W \subseteq \mathbb{P} : (\exists \text{ finite } A_0 \subseteq \overline{W})\ f \notin \text{HTP}(R_{\mathbb{P}-A_0})\}$$

for the set of W where this second possibility holds. $\mathcal{C}(f)$ is another open set, for the same reasons that $\mathcal{A}(f)$ is open.

The third possibility is that neither of the first two holds: W may not lie in $\mathcal{A}(f) \cup \mathcal{C}(f)$. Now 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 $\text{Int}(\overline{\mathcal{A}(f)})$ is similarly a union of basic open sets, and these can be enumerated by an $\text{HTP}(\mathbb{Q})$-oracle, since $\text{HTP}(\mathbb{Q})$ decides $\text{HTP}(R)$ 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 $\text{Int}(\overline{\mathcal{A}(f)})$. This set $\mathcal{B}(f)$ will be the focus of much of the rest of this article. Topologically, it is indeed the boundary of $\mathcal{A}(f)$, since it contains exactly those points which lie neither in the interior of $\mathcal{A}(f)$ (namely $\mathcal{A}(f)$ itself) nor in the interior of its complement. Therefore $\mathcal{B}(f)$ is always closed. In computability theory, $\mathcal{B}(f)$ is a Π^0_2 subset of $2^{\mathbb{P}}$, and indeed is $\Pi_1^{\text{HTP}(\mathbb{Q})}$, since with an $\text{HTP}(\mathbb{Q})$-oracle one can enumerate its complement $(\mathcal{A}(f) \cup \mathcal{C}(f))$.

To reduce the computability discussion to first-order, one can say of nodes σ that it is Σ^0_1 for $\mathcal{U}_\sigma$ to be contained within $\mathcal{A}(f)$, while it is $\text{HTP}(\mathbb{Q})$-decidable whether $\mathcal{U}_\sigma \subseteq \mathcal{C}(f)$. However, no $\mathcal{U}_\sigma$ can be contained within any $\mathcal{B}(f)$. Indeed, if $\mathcal{U}_\sigma \not\subseteq \mathcal{C}(f)$, then some $\tau \supseteq \sigma$ must have $\mathcal{U}_\tau \subseteq \mathcal{A}(f)$. It follows that, in Baire category theory, $\mathcal{B}(f)$ is nowhere dense, as shown in

[6], and therefore the union

$$\mathcal{B} = \bigcup_{f \in \mathbb{Z}[\vec{X}]} \mathcal{B}(f)$$

is meager. Since meager sets often (but not always) are of measure 0, and vice versa, we will ask below whether $\mathcal{B}$ has measure 0 (or equivalently, whether every $\mathcal{B}(f)$ has measure 0). Theorem 3.4 will suggest the importance of this question.

3.1 Examples of $\mathcal{B}(f)$

A boundary set $\mathcal{B}(f)$ can be empty, but need not be, and we now give a specific example where it is nonempty. The basic idea is to use the polynomial $X^2 + Y^2 - 1$. Of course, this polynomial has two trivial solutions $(0, 1)$ and $(1, 0)$ in $\mathbb{Z}$, so we modify it: our actual f has as its solutions those rationals (x, y) with $x^2 + y^2 = 1$ and $x > 0$ and $y > 0$. This is readily accomplished using the Four Squares Theorem. Technically, the polynomial f uses twelve other variables as well, but it has a solution in R_W iff R_W contains positive rationals (x, y) with $x^2 + y^2 = 1$.

Now if this f lies in $\mathrm{HTP}(R_W)$, we may write each solution in R_W as $(\frac{a}{c}, \frac{b}{c})$, where a, b, c are all nonzero integers with no common factors and $c > 1$. Every prime p dividing c must lie in W. For each such p, we have $a^2 + b^2 \equiv 0 \bmod p$. But p cannot divide both a and b (lest it be a common factor), and so easy arithmetic yields

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

This forces $p \not\equiv 3 \bmod 4$. It follows that f has no solutions in any subring R_V for which V contains only primes congruent to 3 modulo 4.

On the other hand, it is known that every prime $p \equiv 1 \bmod 4$ is a sum of two squares of integers. Poonen pointed out that, writing $p = m^2 + n^2$, this yields

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

With p prime, we know $mn \neq 0$ and $m \neq \pm n$, so this is a solution to f in the subring $R_{\{p\}}$. It follows that f has solutions in every subring R_W for which W contains any prime $\equiv 1 \bmod 4$, and only in such subrings. (The only remaining prime that could divide c is 2, in which case 4 divides c^2. But if $a^2 + b^2 = c^2 \equiv 0 \bmod 4$, then a and b must both be even, giving them a common factor with c.)

It now follows that $\mathcal{A}(f)$ has measure 1, since the probability is 1 that an arbitrary W contains at least one prime $\equiv 1 \bmod 4$. Hence $\mathcal{C}(f)$, being open of measure 0, must be empty. But we saw above that $\mathcal{A}(f) \neq 2^{\mathbb{P}}$, so $\mathcal{B}(f) \neq \emptyset$, although $\mu(\mathcal{B}(f)) = 0$. In particular, every subring W which contains no prime $\equiv 1 \bmod 4$ has the defining property for being in the boundary set of f: no initial segment $\sigma \subset W$ determines whether or not R_W contains a solution to f.

Next, imitating the foregoing proof, we show that for each odd prime q, there is an infinite decidable set V of primes such that R_V contains no nontrivial solutions to $X^2 + qY^2 = 1$. (Here the trivial solution is $(1, 0)$, which can be ruled out by a messier polynomial, just as above.)

Lemma 3.1 *Fix a prime $q \equiv 3 \bmod 4$, and let x and y be positive rational numbers with $x^2 + qy^2 = 1$. Then every prime factor of the least common denominator of x and y is a square modulo q.*

For a prime $q \equiv 1 \bmod 4$, the situation is a little more complicated. If $x^2 + qy^2 = 1$ and $y \neq 0$ and a prime p divides the least common denominator of x and y, then one of the following holds:

- *$p \equiv 1 \bmod 4$ and p is a square modulo q.*
- *$p \equiv 3 \bmod 4$ and p is not a square modulo q.*

Proof. We proceed similarly to the $q = 1$ case done above. Suppose that $q \equiv 3 \bmod 4$ and a, b, c are positive integers, with no common factor, satisfying $a^2 + qb^2 = c^2$. Thus $\left(\frac{a}{b}\right)^2 \equiv -q \bmod p$ for every prime p dividing c. If $p \equiv 1 \bmod 4$, then -1 is also a square mod p, so q is a square mod p, and by quadratic reciprocity p must be a square mod q. Likewise, if $p \equiv 3 \bmod 4$, then -1 is not a square mod p, so q is not either; but with both p and q congruent to $3 \bmod 4$, quadratic reciprocity now shows that p is again a square mod q. (The number-theoretic results here may be found in any standard text on the subject, e.g., [10].)

When $q \equiv 1 \bmod 4$, a similar analysis, with careful use of quadratic reciprocity, gives the result stated in the lemma. ■

One could use Lemma 3.1 to build infinitely many distinct polynomials (with different prime values of q) such that there is an infinite set V for which

R_V contains no solution of any of those polynomials, yet for which no finite subset of the complement of V suffices to establish that any individual one of those polynomials fails to have a solution in R_V. (Saying the same thing: every one of these polynomials has solutions in every HTP-generic subring of $\mathbb{Q}$.) In particular, for every prime q and every nonzero $j \in \mathbb{Z}$, we have

$$\left(\frac{j^2-q}{j^2+q}\right)^2 + q \cdot \left(\frac{2j}{j^2+q}\right)^2 = 1,$$

so that $X^2+qY^2 = 1$ has a nontrivial solution in each subring with the prime factors of (j^2+q) inverted. Given a finite set $\{r_1, \dots r_k\}$ of primes which we may not invert, just take $j = \Pi_{r_i \neq q}\, r_i$; then no r_i divides (j^2+q), and so the semilocal ring $R_{\mathbb{P}-\{r_1,\dots,r_k\}}$ contains the above solution to the polynomial.

3.2 HTP-genericity

Recall that $\mathcal{B}$ denotes the union of all boundary sets $\mathcal{B}(f)$, over all polynomials $f \in \mathbb{Z}[\vec{X}]$. For a set W to fail to lie in $\mathcal{B}$, it must be the case that for every polynomial f, either $f \in \text{HTP}(R_W)$ 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 $\text{HTP}(R_W) \leq W \oplus \text{HTP}(\mathbb{Q})$ for all $W \in \overline{\mathcal{B}}$, but indeed that the reduction is uniform on $\overline{\mathcal{B}}$.

Definition 3.2 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.

Proposition 3.3 *HTP(R_W) is Turing-reducible to $W \oplus$ HTP($\mathbb{Q}$) uniformly on the set $\overline{\mathcal{B}}$. That is, there exists a single Turing reduction Φ such that, for every HTP-generic set W, $\Phi^{W \oplus HTP(\mathbb{Q})} = HTP(R_W)$.*

Proof. Given $f \in \mathbb{Z}[\vec{X}]$ as input, the program for Φ simply searches for either a solution $\vec{x}$ 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 HTP($\mathbb{Q}$) oracle, using Proposition 2.4, confirms that $f \notin \text{HTP}(R_{\mathbb{P}-A_0})$. When it finds either of these, it outputs the corresponding answer about membership of f in 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 $\mathcal{B}$. ■

Theorem 3.4 *$\mu(\mathcal{B}) = 0$ if and only if there exists a Turing reduction of HTP(R_W) to $W \oplus$ HTP($\mathbb{Q}$) which succeeds uniformly on a class of measure 1. Moreover, if these equivalent conditions hold, then:*

1. *The measures $\mu(\mathcal{A}(f))$ and $\mu(\mathcal{C}(f))$ are HTP($\mathbb{Q}$)-computable uniformly in f. (This claim is precisely defined later in this subsection.)*

2. *There is* no *Turing reduction of W' to HTP(R_W) which succeeds uniformly on a class of measure 1.*

Proof. Proposition 3.3 proves the forwards direction of the equivalence immediately. For the backwards direction, suppose that $\text{HTP}(R_W) = \Phi^{W\oplus\text{HTP}(\mathbb{Q})}$ for every W in a class $\mathcal{D}$ of measure 1. Fix any polynomial f, and any set $W \in \mathcal{B}(f)$. Then $f \notin \text{HTP}(R_W)$, but we claim that $\Phi^{W\oplus\text{HTP}(\mathbb{Q})}(f)$ cannot halt and output 0. If it did, then fix n large enough that $\Phi^{(W\restriction n)\oplus\text{HTP}(\mathbb{Q})}(f)\downarrow= 0$. Then also $\Phi^{V\oplus\text{HTP}(\mathbb{Q})}(f)\downarrow= 0$ for every $V \supset W\restriction n$. However, since $W \in \mathcal{B}(f)$, there exists some $V \supset W\restriction n$ for which $f \in \text{HTP}(R_V)$. Fix $m \geq n$ large enough that $f \in \text{HTP}(R_{V\restriction m})$. Then, for every $U \supset V\restriction m$, we have both $f \in \text{HTP}(R_U)$ and $\Phi^{U\oplus\text{HTP}(\mathbb{Q})}(f)\downarrow= 0$, contradicting the assumption that Φ succeeds uniformly on a class of measure 1. Thus we must have either $\Phi^{W\oplus\text{HTP}(\mathbb{Q})}(f)\uparrow$ or $\Phi^{W\oplus\text{HTP}(\mathbb{Q})}(f)\downarrow\neq 0$ whenever $W \in \mathcal{B}(f)$. But since Φ succeeds uniformly on a class of measure 1, this means that every class $\mathcal{B}(f)$ has measure 0, and hence so does the countable union $\mathcal{B}$ of these classes.

Now suppose that the two equivalent conditions hold. (1) will follow from the more general Theorem 3.6 below. For (2), we simply note that by Lemma 2.1, no single Turing functional can compute W' from $W \oplus \emptyset'$ uniformly on a class of measure 1. Since we are assuming that HTP(R_W) can be computed from $W \oplus$ HTP($\mathbb{Q}$) (hence from $W \oplus \emptyset'$) uniformly on a class of measure 1, there cannot possibly exist a further reduction of W' to HTP(R_W) which also succeeds uniformly on a class of measure 1. (The intersection of two classes of measure 1 also has measure 1, of course.) ∎

For the next theorems, we simplify our notation by writing

$$\alpha(f) = \mu(\mathcal{A}(f)) \qquad \beta(f) = \mu(\mathcal{B}(f)) \qquad \gamma(f) = \mu(\mathcal{C}(f))$$

for each $f \in \mathbb{Z}[\vec{X}]$. Of course $\alpha(f) + \beta(f) + \gamma(f) = 1$. Notice, however, that we have very little *a priori* information about the values in the images of these functions. Complexity bounds exist, since $\alpha(f)$ is always a left-c.e. real number, and $\gamma(f)$ is always left-c.e. relative to HTP($\mathbb{Q}$), but it is not clear whether these real numbers need to be algebraic over $\mathbb{Q}$. The author is not aware of any polynomials f for which $\alpha(f)$ fails to be a dyadic rational, nor of any for which $\beta(f) > 0$. Likewise, it is open whether the set $\mathcal{C}(f)$ must always be a finite union of basic open sets $\mathcal{U}_\sigma$. (Our examples in Subsection 3.1 do show that $\mathcal{A}(f)$ can fail to be a finite union of basic open sets.)

In order to deal with these functions from ω (or from $\mathbb{Z}[\vec{X}]$) into $\mathbb{R}$, we will say that we can *compute* a real number r (such as $\alpha(f)$) if we can enumerate both the strict lower cut and the strict upper cut in $\mathbb{Q}$ defined by r. (Notice that if r itself is rational, this means that r will never appear in either cut.) Of course, an enumeration $E = \cup_s E_s$ of the non-strict lower cut of r quickly yields an enumeration of its strict lower cut: we may assume $|E_s| \leq s$ and take $E'_s = E_s - \{\max(E_s)\}$.

A *uniform enumeration* of the strict lower cuts of a sequence of real numbers $\langle r_i \rangle_{i\in\omega}$ (such as $\langle \alpha(f) \rangle_{f\in\mathbb{Z}[\vec{X}]}$) is a single procedure that, on input i, enumerates the strict lower cut of r_i; similarly for strict upper cuts. To *compute the sequence* $\langle r_i \rangle_{i\in\omega}$ *uniformly* means to enumerate both strict upper and lower cuts for the sequence uniformly. Finally, a function θ from ω into $\mathbb{R}$ (such as α, β, or γ) is *computable* if the sequence $\langle \theta(i) \rangle_{i\in\omega}$ is uniformly computable.

The next theorems show the potential power of being able to compute α, β, and γ. Of course, if it turns out that $\mu(\mathcal{B}) = 0$, then β would be very readily computable, and α and γ would both be HTP($\mathbb{Q}$)-computable.

Theorem 3.5 *The following are equivalent.*

1. *The strict upper cuts of the measures $\alpha(f)$ of polynomials f are computable uniformly in f.*
2. *$\alpha(f)$ is computable uniformly in f.*
3. *There is a single Turing functional Ψ such that, for all rational $\varepsilon > 0$,*

$$\mu(\{W \subseteq \mathbb{P} : (\forall f)\ HTP(R_W)(f) = \Psi^W(\varepsilon, f)\}) \geq 1 - \varepsilon.$$

Proof. The equivalence of (1) and (2) is immediate, since we can enumerate the lower cuts of $\alpha(f)$ uniformly in f simply by searching for solutions to f in $\mathbb{Q}$. The argument for (2) $\implies$ (3) is similar to the proof of Lemma 2.1. Given ε and the n-th polynomial f in $\mathbb{Z}[\vec{X}]$, we first approximate $\alpha(f)$

by finding an $r \in \mathbb{Q}$ with $r < \alpha(f) \leq r + \frac{\varepsilon}{2^{n+1}}$. (Since $\alpha(f)$ could be 0, we allow $r < 0$ here, in which case the next step is trivial.) Next, find finitely many solutions to f in $\mathbb{Q}$ such that the class of subrings containing these solutions has measure $\geq r$. If W contains any of these solutions, then output "yes" (that is, $f \in \text{HTP}(R_W)$); otherwise output "no." This output will be correct except on a class of measure $\leq \frac{\varepsilon}{2^{n+1}}$, and so our functional computes $\text{HTP}(R_W)$ correctly except on a class of measure $\leq \sum_n \frac{\varepsilon}{2^{n+1}} = \varepsilon$.

It remains to show that (3) $\implies$ (1). Here we use the uniformity of the procedure Ψ with respect to ε. Given an f, we wish to enumerate the upper cut of $\alpha(f)$. For each $s > 0$ in turn, set $\varepsilon = \frac{1}{s}$, and search for strings σ and naturals t such that $\Psi_t^{\sigma}(\frac{\varepsilon}{3}, f)\downarrow$. By assumption, we will eventually find a t and a finite set of strings $\sigma_0, \ldots, \sigma_k$ such that all $\Psi_t^{\sigma_i}(\frac{\varepsilon}{3}, f)\downarrow$ and $\mu(\cup_{i\leq k} \mathcal{U}_{\sigma_i}) \geq 1 - \frac{2\varepsilon}{3}$. Let $r = \mu(\cup_{\sigma(i)=1} \mathcal{U}_{\sigma_i})$, and enumerate all rationals $> r + \varepsilon$ into the upper cut of $\alpha(f)$. Now according to the computation by Ψ, at least $(1 - r - \frac{2\varepsilon}{3})$-much of $2^{\mathbb{P}}$ lies outside of $\mathcal{A}(f)$. Ψ may have been wrong about as much as $\frac{\varepsilon}{3}$ of these, but must have been correct on the remaining ones, whose measure is at least $(1 - r - \varepsilon)$. So our enumeration did nothing incorrect. Moreover, if $q \in \mathbb{Q}$ satisfies $q > \alpha(f)$, then once we reach an s with $\varepsilon = \frac{1}{s} < \frac{q-\alpha(f)}{2}$, we will have $r \leq \alpha(f) + \frac{\varepsilon}{3}$, and hence $r + \varepsilon \leq \alpha(f) + \frac{4\varepsilon}{3} < q$. Thus every $q > \alpha(f)$ will eventually be enumerated into the upper cut given by our procedure. This completes the proof. ∎

For the next theorem, we consider more than just the characteristic function of $\text{HTP}(R_W)$. For each polynomial f and each $W \subseteq \mathbb{P}$, define

$$\chi(f, W) = \begin{cases} 2, & \text{if } W \in \mathcal{A}(f); \\ 1, & \text{if } W \in \mathcal{B}(f); \\ 0, & \text{if } W \in \mathcal{C}(f). \end{cases}$$

Theorem 3.6 *The following are equivalent.*

1. *The strict lower cuts of the measures $\beta(f)$ of the boundary sets $\mathcal{B}(f)$ of polynomials f are enumerable uniformly in f using an HTP$(\mathbb{Q})$-oracle.*

2. *$\alpha(f)$, $\beta(f)$, and $\gamma(f)$ are all HTP$(\mathbb{Q})$-computable uniformly in f.*

3. *There is a single Turing functional Θ such that, for all rational $\varepsilon > 0$,*

$$\mu(\{W \subseteq \mathbb{P} : (\forall f)\ \chi(f, W) = \Theta^{W \oplus HTP(\mathbb{Q})}(\varepsilon, f)\}) \geq 1 - \varepsilon.$$

Proof. We can enumerate the strict lower cut of $\alpha(f)$, of course, just by searching for solutions of f in $\mathbb{Q}$, and with an HTP($\mathbb{Q}$)-oracle we can similarly enumerate the strict lower cut of $\gamma(f)$. Assuming (1), this allows us to use an HTP($\mathbb{Q}$)-oracle to enumerate the strict lower cuts of $\alpha(f)+\beta(f)$ and of $\gamma(f)+\beta(f)$. But $\gamma(f)=1-\alpha(f)-\beta(f)$, so we can then enumerate the strict upper cut of $\gamma(f)$, and similarly for the strict upper cut of $\alpha(f)$. Finally, the strict upper cut of $\beta(f)$ is just that of $(1-\alpha(f)-\gamma(f))$. Thus (1) $\implies$ (2).

Assuming (2), the program for Θ is along similar lines to that of Ψ in Theorem 3.5. Given ε, the n-th polynomial f, and an oracle for $W\oplus\mathrm{HTP}(\mathbb{Q})$, it uses the oracle to compute an r with $r<\alpha(f)<r+\frac{\varepsilon}{2^{n+2}}$, then finds a finite union of basic open sets, of measure $\geq r$, all contained within $\mathcal{A}(f)$. If W lies within one of these basic open sets, then it outputs 2 (that is, it concludes, correctly, that $f\in\mathrm{HTP}(R_W)$), and otherwise it continues with the procedure below. Thus, for this f, the class of W with $f\in\mathrm{HTP}(R_W)$ and $\Theta^{W\oplus\mathrm{HTP}(\mathbb{Q})}(f)\neq 2$ has measure at most $\frac{\varepsilon}{2^{n+2}}$.

If the program concludes (possibly incorrectly) that $f\notin\mathrm{HTP}(R_W)$, then it goes back to its $HTPQ$-oracle to approximate $\gamma(f)$, and finds an r' with $r'<\gamma(f)<r'+\frac{\varepsilon}{2^{n+2}}$. Using the entire oracle $W\oplus\mathrm{HTP}(\mathbb{Q})$, it then enumerates strings σ such that $f\notin\mathrm{HTP}(R_{\mathbb{P}-\sigma^{-1}(0)})$ until it has found a finite union of basic open sets, of measure $\geq r'$, contained within $\mathcal{C}(f)$. If W lies within any of these basic open sets, then the program outputs 0 (correctly, since $W\in\mathcal{C}(f)$); while otherwise it outputs 1. Thus, for this f, the class of W with $f\in\mathcal{C}(f)$ and $\Theta^{W\oplus\mathrm{HTP}(\mathbb{Q})}(f)\neq 0$ has measure at most $\frac{\varepsilon}{2^{n+2}}$, and so the class of those W such that the program output is incorrect has measure $\leq\frac{\varepsilon}{2^{n+1}}$. (The outputs 2 and 0 are always justified, so the only possible errors are output 1 with either $W\in\mathcal{A}(f)$ or $W\in\mathcal{C}(f)$. These are the two classes described above, each of measure $\leq\frac{\varepsilon}{2^{n+2}}$.) It follows that, apart from a class of measure $\leq\sum\frac{\varepsilon}{2^{n+1}}=\varepsilon$, the $\Theta^{W\oplus\mathrm{HTP}(\mathbb{Q})}$ outputs the correct answer for every f. This proves (3).

The proof that (3) $\implies$ (1) is entirely analogous to that in Theorem 3.5. To enumerate the strict lower cut of $\beta(f)$, using an HTP($\mathbb{Q}$)-oracle, we search for strings σ and naturals s,t for which $\Theta_s^{\sigma\oplus\mathrm{HTP}(\mathbb{Q})}(\frac{1}{t},f)\downarrow=1$. When (and if) we find such strings $\sigma_0,\ldots,\sigma_n$ (for any single t), we conclude that $\mu(\beta)\geq\mu(\cup_{i\leq n}\mathcal{U}_{\sigma_i})-\frac{1}{t}$, and we enumerate all rationals less than this value. As in Theorem 3.5, this process enumerates precisely the strict lower cut of $\beta(f)$. ■

4 Questions

The obvious question arising from this article is number-theoretic: does there exist a polynomial $f \in \mathbb{Z}[\vec{X}]$ with $\beta(f) > 0$? Equivalently, is $\mu(\mathcal{B}) > 0$? (Recall that $\beta(f)$ denotes the measure of the boundary set $\mathcal{B}(f)$ of the polynomial f, with $\mathcal{B} = \cup_f \mathcal{B}(f)$.) The useful analogy here is to the class $\mathcal{A} = \{W : x \in W'\}$ defined (for a specific index x) in Lemma 2.1. That class $\mathcal{A}$ had measure $\leq \frac{1}{2}$, and could readily have been built to have arbitrarily small positive measure. However, the interior of its complement was empty, and so the boundary of $\mathcal{A}$ had measure $\geq \frac{1}{2}$, and could have been made to have boundary of measure arbitrarily close to 1. The question is whether one can build a polynomial f for which the set $\mathcal{A}(f)$ acts the same way as the $\mathcal{A}$ from the lemma, with small measure itself but with $\mathcal{C}(f)$ empty, so that $\mathcal{B}(f)$ must have positive measure. (Of course, the question of possible values of $\beta(f)$ does not require $\mathcal{C}(f) = \emptyset$; this simply seems like the easiest way to address it.)

A stronger version of this question appears in [2]. There Eisenträger, Park, Shlapentokh, and the author ask (in essence) whether a polynomial f could have the properties that $\mathcal{C}(f) = \emptyset$, yet that there also exists $\varepsilon > 0$ such that for every $W \in \mathcal{A}(f)$, there is an n for which $\frac{|W \cap \{0,\ldots,n\}|}{n+1} > \varepsilon$. (One might as well assume here that W contains only the elements necessary to cause a single solution of f to appear in R_W.) The reasons for posing this question are explained there. For any f with these properties, the set $\mathcal{A}(f)$ would imitate the set $\mathcal{A}$ in our Lemma 2.1: not necessarily ending with a long string of 1's, but at least avoiding any string with too many 0's.

Several other questions are listed in Subsection 3.2. These include whether $\alpha(f)$ is always dyadic, or always rational, or always algebraic, or always computable; and also whether the set $\mathcal{C}(f)$ is always a finite union of basic open sets. The computability of the function α remains open: this is one of the equivalent conditions in Theorem 3.5. Notice that the ability to compute $\alpha(f)$ uniformly in f does not automatically confer the ability to decide HTP($\mathbb{Z}$): $\alpha(f)$ can equal 1 even when $f \notin$ HTP($\mathbb{Z}$), as in the first example in Subsection 3.1, for instance. Likewise, Theorem 3.6 proves three conditions to be equivalent, but leaves open the question of whether or not those conditions actually hold.

References

[1] Martin Davis, Hilary Putnam, and Julia Robinson. The decision problem for exponential diophantine equations. *Annals of Mathematics*, 74(3): 425–436, 1961.

[2] Kirsten Eisenträger, Russell Miller, Jennifer Park, and Alexandra Shlapentokh. As easy as $\mathbb{Q}$: Hilbert's Tenth Problem for subrings of the rationals, to appear.

[3] Jochen Koenigsmann. Defining $\mathbb{Z}$ in $\mathbb{Q}$. *Annals of Mathematics*, 183(1): 73–93, 2016.

[4] Stuart Kurtz. Randomness and Genericity in the Degrees of Unsolvability. Ph.D. thesis, University of Illinois at Urbana-Champaign, 1981.

[5] Yu. V. Matijasevič. The Diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*, 191: 279–282, 1970.

[6] Russell Miller. Baire category theory and Hilbert's Tenth Problem inside $\mathbb{Q}$, in *Pursuit of the Universal: 12th Conference on Computability in Europe, CiE 2016*, eds. A. Beckmann, L. Bienvenu & N. Jonoska *Lecture Notes in Computer Science* **9709** (Berlin: Springer-Verlag, 2016), 343–352.

[7] Bjorn Poonen. Hilbert's Tenth Problem and Mazur's conjecture for large subrings of $\mathbb{Q}$. *Journal of the AMS*, 16(4): 981–990, 2003.

[8] Bjorn Poonen. Characterizing integers among rational numbers with a universal-existential formula. *American Journal of Mathematics*, 131(3): 675–682, 2009.

[9] Julia Robinson. Definability and decision problems in arithmetic. *Journal of Symbolic Logic*, 14: 98–114, 1949.

[10] Jean-Pierre Serre. *A Course in Arithmetic.* Graduate Texts in Mathematics, Springer, Berlin, 1996.

[11] John Stillwell. Decidability of the "almost all" theory of degrees. *Journal of Symbolic Logic*, 37(3): 501–506, 1972.

Department of Mathematics
Queens College – C.U.N.Y.
65-30 Kissena Blvd.
Queens, New York 11367 U.S.A.
Ph.D. Programs in Mathematics & Computer Science
C.U.N.Y. Graduate Center
365 Fifth Avenue
New York, New York 10016 U.S.A.
E-mail: `Russell.Miller@qc.cuny.edu`