# HTP-Complete Rings of Rational Numbers

Russell Miller [*]

November 11, 2021

**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 $R$. We view $HTP$ as an enumeration operator, mapping each set $W$ of prime numbers to $HTP(\mathbb{Z}[W^{-1}])$, which is naturally viewed as a set of polynomials in $\mathbb{Z}[X_1, X_2, \ldots]$. It is known that for almost all $W$, the jump $W'$ does not 1-reduce to $HTP(R_W)$. In contrast, we show that every Turing degree contains a set $W$ for which such a 1-reduction does hold: these $W$ are said to be *HTP-complete*. Continuing, we derive additional results regarding the impossibility that a decision procedure for $W'$ from $HTP(\mathbb{Z}[W^{-1}])$ can succeed uniformly on a set of measure 1, and regarding the consequences for the boundary sets of the $HTP$ operator in case $\mathbb{Z}$ has an existential definition in $\mathbb{Q}$.

**Key Words**: boundary sets, computability theory, Hilbert's Tenth Problem, HTP-completeness, subrings of the rational numbers.

## 1 Introduction

For a ring $R$, Hilbert's Tenth Problem $HTP(R)$ is the set of polynomial equations over $R$, in several variables, with solutions in $R$:

$$HTP(R) = \bigcup_{n \in \mathbb{N}} \{f \in R[X_1, \ldots, X_n] : (\exists x_1, \ldots, x_n \in R) \; f(x_1, \ldots, x_n) = 0\}.$$

For countable rings $R$, one can ask effectiveness questions about $HTP(R)$, which is always computably enumerable relative to a presentation of $R$ (that is, relative to the atomic diagram of a ring isomorphic to $R$ with $\omega$ as its underlying set; cf. [11]). That it may be *properly* computably enumerable was established for the fundamental example $R = \mathbb{Z}$ by Matiyasevich in [10], completing work by Davis, Putnam, and Robinson in [1]: they showed that the Halting Problem is 1-reducible to $HTP(\mathbb{Z})$. This was the resolution of Hilbert's original Tenth Problem, in which Hilbert had demanded an algorithm deciding membership in $HTP(\mathbb{Z})$. (Simpler constructions exist of computable rings $R$ for which $HTP(R)$ is undecidable; indeed one will be described at the end of Section 4.) In contrast, the decidability of $HTP(\mathbb{Q})$ remains an open question, and is the subject of intense study.

The subrings of $\mathbb{Q}$ are in bijection with the subsets $W$ of the set $\mathbb{P}$ of all prime numbers, via the map $W \mapsto \mathbb{Z}[W^{-1}]$. Thus these subrings form a topological space homeomorphic to Cantor space $2^{\mathbb{P}}$, on which one can therefore consider questions of Lebesgue measure and Baire category. We then view $HTP$ as an operator, mapping each $W \subseteq \mathbb{P}$ to the set $HTP(\mathbb{Z}[W^{-1}])$. Notice that, to decide $HTP(\mathbb{Z}[W^{-1}])$, one need only decide membership in it for polynomials from $\mathbb{Z}[X_1, X_2, \ldots]$, and so we normally view $HTP(\mathbb{Z}[W^{-1}])$ as its own intersection with $\mathbb{Z}[X_1, X_2, \ldots]$. This allows for a uniform Gödel coding of each $HTP(\mathbb{Z}[W^{-1}])$ as a subset of $\omega$. For simplicity we often write $R_W$ for the ring $\mathbb{Z}[W^{-1}]$, and $HTP(R_W)$ for its $HTP$.

This article continues a program by the author of approaching $HTP(\mathbb{Q})$ by viewing the collection of all subrings of $\mathbb{Q}$ as a topological space in this way and considering the "common" behavior of the sets $HTP(R)$. Certain properties hold of $HTP(R)$ for every $R$ in a "large" set of rings (corresponding to a subset of measure 1 within Cantor space, say, or to a comeager subset), while other properties occur less frequently. In turn, that program fits within the broader framework of examining $HTP(R)$ for subrings $R \subseteq \mathbb{Q}$ in general, an endeavor that includes the notable work of Poonen [14, 15] and many others. The results in Section 4 here may be seen as fitting into the larger program, whereas the results in Sections 5 and 6 are mainly of interest within the smaller program.

The jump $W'$ of a set $W \subseteq \mathbb{P}$ is readily seen to give an upper bound for the complexity of the set $HTP(R_W)$, which is always c.e. relative to $W$. It is known from work in [8] that for many subrings $R_W$ of $\mathbb{Q}$, the complexity of $HTP(R_W)$ is strictly below that of $W'$; this will be generalized here in Theorem 5.2. In contrast, in Section 4, we will show that sets $W$ with

2

$HTP(R_W) \equiv_1 W'$ are ubiquitous, in the sense that they exist within every Turing degree. Such sets will be said to be *HTP-complete*. In Section 5 we will consider the weaker relationship of Turing-reducibility between $HTP(R_W)$ and $W'$, whereas in Section 6 we will consider consequences that would follow in case $\mathbb{Z}$ has an existential definition in $\mathbb{Q}$ – which is an open question, and represents the strongest conjecture normally considered about the difficulty of deciding $HTP(\mathbb{Q})$. (If such an existential definition exists, then $HTP(\mathbb{Z})$ itself 1-reduces to $HTP(\mathbb{Q})$, and therefore so does the Halting Problem.) Before that, Sections 2 and 3 provide lemmas established earlier in [2] and [8], which will be of use in the subsequent sections. For basic information about computability theory, [20] remains an excellent source, but [17] will be more helpful for the concept of enumeration reducibility in Section 5.

## 2　Background

The following lemma appears in [2], but it has been known ever since the pioneering work of Julia Robinson in [16], in which Robinson gave the first definition of the set $\mathbb{Z}$ within the field $\mathbb{Q}$. It will be important for us at several junctures, as it enables us to "ignore" a given finite set of primes when dealing with the $HTP$ operator, and thus facilitates finite-injury constructions.

**Proposition 2.1 (Robinson [16])** *For every prime $p$, there is a polynomial $g_p(Z, X_1, X_2, X_3)$ such that for all rationals $q$, we have*

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

*Moreover, $g_p$ may be computed uniformly in $p$.*

**Corollary 2.2** *For each finite subset $A_0 \subseteq \mathbb{P}$, a polynomial $f(Z_0, \dots, Z_n)$ has a solution in $R_{(\mathbb{P}-A_0)}$ if and only if*

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

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

For a proof using the more recent results of [7], see Proposition 5.4 in [2].

　　Our principal tool for proving Theorem 4.1 and its corollaries will be the equations $X^2 + qY^2 = 1$. Here we review the relevant number-theoretic

3

results, previously applied to this purpose in [8] by Kramer and the author. The main point is that for each odd prime $q$, there is an infinite decidable set $V$ of primes such that $R_V$ contains no nontrivial solutions to $X^2 + qY^2 = 1$, yet for every $p \notin V$, the ring $\mathbb{Z}[\frac{1}{p}]$ does contain a nontrivial solution. (Here the trivial solutions are $(\pm 1, 0)$, which in Section 4 will be ruled out as solutions, at the cost of turning $(X^2 + qY^2 - 1)$ into a messier polynomial.)

**Definition 2.3** For a fixed odd prime $q$, a prime $p$ is *q-appropriate* if $p$ is odd and $p \neq q$ and $\left(\frac{-q}{p}\right) = 1$ (that is, $-q$ is a square modulo $p$).

The crux of Lemma 2.4 is that the $q$-appropriate primes are precisely the possible factors of the denominator in a nontrivial solution to $x^2 + qy^2 = 1$, thus justifying the term *q-appropriate*. This lemma comprises Lemmas 4.2 and 4.4 from [8], where the proofs may be found.

**Lemma 2.4** *Fix an odd prime $q$, and let $x$ and $y$ be positive rational numbers with $x^2 + qy^2 = 1$. Then every odd prime factor $p$ of the least common denominator $c$ of $x$ and $y$ must be q-appropriate.*

*Conversely, suppose that $p$ is q-appropriate. Then there is a primitive solution $(a, b, p^k)$ to $X^2 + qY^2 = Z^2$ with $k \geq 1$. Hence there is a nontrivial solution to $X^2 + qY^2 = 1$ in the ring $\mathbb{Z}[\frac{1}{p}]$.*

*Finally, for $q \equiv 3 \bmod 4$, a prime $p \neq q$ is q-appropriate if and only if $p$ is a square modulo $q$. When $q \equiv 1 \bmod 4$, a prime $p \neq q$ is q-appropriate if and only if 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 $q$.*

*It follows that q-appropriateness of $p$ is decidable uniformly in $q$.* ∎

Of course, a single prime $p$ can be $q$-appropriate for many different $q$. Therefore, adjoining $\frac{1}{p}$ to a ring may create solutions of the equations $X^2 + qY^2 = 1$ for many values of $q$. The purpose of the following corollary (in concert with Proposition 2.1 above) is to allow us to create a solution to the equation of our choice without disrupting the solvability of other such equations in the ring. Corollary 2.5 is a modest extension of Corollary 4.3 in [8], where $I$ was the set $\{0, 1, \ldots, e - 1\}$.

**Corollary 2.5** *Let $3 = q_0 < q_1 < \cdots$ be the odd prime numbers. Then, for every $e \in \omega$ and every finite set $I \subseteq \omega - \{e\}$, there are infinitely many primes $p$ that are $q_e$-appropriate but (for all $i \in I$) are not $q_i$-appropriate.*

*Proof.* Write $I = \{i_0 < \cdots < i_j\}$. Our goal is to show that there is a residue $n$ modulo $m = 4q_{i_0} \cdots q_{i_j} \cdot q_e$ which is prime to $m$ and satisfies all the criteria dictated by the final part of Lemma 2.4, so that each prime $p$ congruent to $n$ modulo $m$ will satisfy the corollary. For $m_0 = 4q_{i_0}$, we choose $n_0 \equiv 1 \bmod 4$ such that $n_0$ is not a square mod $q_{i_0}$, noting that for each residue $r$ mod $q_{i_0}$, one of $r, r + q_{i_0}, r + 2q_{i_0}, r + 3q_{i_0}$ must be $\equiv 1 \bmod 4$. Setting $m_{k+1} = m_k \cdot q_{i_{k+1}}$ inductively for $k < j$, we see that the residue $n_k$ mod $m_k$ yields distinct residues $n_k, n_k + m_k, \ldots, n_k + m_k(q_{i_{k+1}} - 1) \bmod m_{k+1}$, each congruent to a distinct residue mod $q_{i_{k+1}}$. So we may choose $n_{k+1}$ to be one of these residues which is not a square mod $q_{i_{k+1}}$. Once we have produced $n_j$ (a residue modulo $m_j$), we do the same process with $q_e$, except that now we choose the new residue $n$ mod $m$ so that $n$ is a nonzero square mod $q_e$. With $n \equiv 1 \bmod 4$, this means that each prime with residue $n$ mod $m$ will be $q_e$-appropriate (as $n$ is a square mod $q_e$), but will be $q_{i_k}$-inappropriate for all $k \leq j$ (as $n$ is not a square mod $q_{i_k}$). Finally, $n$ is nonzero modulo 4, modulo $q_e$, and modulo each $q_{i_k}$, hence is prime to $m$. Therefore, Dirichlet's theorem on arithmetic progressions (see [18, Chap. 6, §4]) shows that infinitely many primes are congruent to $n$ mod $m$, so the corollary holds. ∎

The equation $X^2 + qY^2 = 1$ may be seen as stating that an element $x + y\sqrt{-q}$ of the field $\mathbb{Q}(\sqrt{-q})$ has norm 1 there. It has been pointed out that many other sets of norm equations of totally complex extensions of degree 2 would admit similar results to Lemma 2.4 and Corollary 2.5, and therefore could presumably be used to give alternative constructions for Theorem 4.1.

# 3   HTP-Completeness

A computably enumerable set $C$ is said to be 1-*complete* if every c.e. set $D$ is 1-reducible to $C$, written $D \leq_1 C$. By definition this means that for each $D$, there is a computable total injective function $h : \omega \to \omega$ such that

$$(\forall x \in \omega) \ [x \in D \iff h(x) \in C].$$

The function $h$ is called a 1-*reduction*. Of course, the Halting Problem $\emptyset'$ is 1-complete, and so 1-completeness of an arbitrary c.e. set $C$ is equivalent to

the statement $\emptyset' \leq_1 C$. More generally, for any set $A \subseteq \omega$ at all, the jump $A'$ is 1-complete among sets computably enumerable in $A$, in exactly the same sense. Details appear in [20, §III.2].

For a subset $W \subseteq \mathbb{P}$ of the set $\mathbb{P}$ of all prime numbers, we define the subring $R_W = \mathbb{Z}[W^{-1}]$ in which the primes with multiplicative inverses are precisely those in $W$. The HTP operator maps $W$ to $HTP(R_W)$, as detailed in [8], and this set is clearly computably enumerable relative to $W$, since a $W$-oracle allows one to list out all rational numbers in $R_W$ and search for solutions to polynomial equations. Therefore we automatically have $HTP(R_W) \leq_1 W'$. In the case $W = \emptyset$, so that $R_W = \mathbb{Z}$, the Matiyasevich-Davis-Putnam-Robinson result shows that the reverse reduction also holds: $\emptyset' \leq_1 HTP(R_\emptyset)$. This means that $\emptyset$ is *HTP-complete*, according to our new definition: its HTP is as complicated as possible.

**Definition 3.1** A set $W \subseteq \mathbb{P}$ of prime numbers is said to be *HTP-complete* if every set $V$ that is $W$-computably enumerable satisfies $V \leq_1 HTP(R_W)$. Equivalently, $W$ is HTP-complete if and only if $W' \leq_1 HTP(R_W)$. This is also equivalent to requiring $W' \equiv_1 HTP(R_W)$, or, by Myhill's Theorem, to demanding that $W'$ and $HTP(R_W)$ be computably isomorphic.

It is also natural to say that $W$ is *diophantine-complete* if every $V$ c.e. in $W$ is diophantine in the ring $R_W = \mathbb{Z}[W^{-1}]$. However, the only sets $W$ currently known to have this property are the finite sets.

In contrast to $\emptyset$, it is unknown whether $\mathbb{P}$ is HTP-complete, since $R_\mathbb{P} = \mathbb{Q}$. However, there is a broad result from [8] (see [8, Cor. 3.3] and the preceding remarks there), building on theorems of Jockusch and Kurtz [4, 9]. It will appear again in this article, generalized as Theorem 5.2, with a proof.

**Theorem 3.2 (see [8])** *The set of all HTP-complete subsets of $\mathbb{P}$ is meager within the power set of $\mathbb{P}$ and has Lebesgue measure $0$ there.*

This implies that the MRDP result for $\mathbb{Z}$ (that is, for $W = \emptyset$) is an anomaly: most subrings of $\mathbb{Q}$ do not have such strong HTP's. Of course, $\emptyset$ is hardly a representative element of the power set of $\mathbb{P}$, so it is not surprising that it acts strangely. Likewise, it would not be surprising if $\mathbb{Q}$ (that is, $R_\mathbb{P}$) did the same. Nevertheless, it raises the question of just how many subsets of $\mathbb{P}$ are HTP-complete, and provides the initial answer: "very few," in terms of both Lebesgue measure and Baire category. In the next section,

we balance this by showing that HTP-complete sets, although meager, are ubiquitous: they appear in every Turing degree, and therefore there must be continuum-many of them.

# 4 Building HTP-complete Sets

**Theorem 4.1** *Every Turing degree contains an HTP-complete set $V$. Indeed, there is a uniform procedure which, given any set $C$, computes an HTP-complete set $V \equiv_T C$.*

To be clear: our procedure works uniformly on $C$, but given two distinct Turing-equivalent sets $C$, it will generally compute distinct sets $V$. Indeed, one can make the uniform procedure one-to-one, so that this is always the case. It follows that there are countably many HTP-complete sets Turing-equivalent to the given $C$. Thus every Turing degree contains infinitely many HTP-complete sets.

*Proof.* The following procedure, using the oracle $C$, computes the required set $V$, as we prove after giving the construction. The construction will begin with $V_0 = \mathbb{P}$ and will delete elements from $V$ at various stages, so that $V = \cap_s V_s$ is clearly $\Pi_1^C$. Afterwards we will argue that in fact $V \leq_T C$, and then that $C \leq_T V$.

The requirement $\mathcal{R}_e$ demands that

$$g_e \in HTP(R_V) \iff \Phi_e^C(e)\downarrow,$$

where $g_e$ is a polynomial we will define below. For now it is acceptable to let the following polynomial stand in for $g_e$, using the $e$-th odd prime $q_e$:

$$f_e(X, Y, \ldots) = (X^2 + q_e Y^2 - 1)^2 + \left( Y \left( 1 + \sum_{i=1}^{4} Z_i^2 \right) - \left( 1 + \sum_{i=1}^{4} W_i^2 \right) \right)^2$$

whose solutions correspond to those pairs of rational numbers $(x, y)$ with $x^2 + q_e y^2 = 1$ and $y > 0$. In fact, if $\Phi_e^C(e)\uparrow$, then this $f_e$ may have solutions in $\mathbb{Q}$, but will have no solutions in a particular semilocal subring of $\mathbb{Q}$ determined in advance by the construction; whereas if $\Phi_e^C(e)\downarrow$, then it will have solutions in every semilocal subring. This gives us a finite amount of wiggle room,

enough for the following finite-injury construction, and at the end we will replace $f_e$ by a $g_e$ appropriate to the semilocal subring.

At each stage $s > \langle e, 0 \rangle$, $\mathcal{R}_e$ may protect various $q_e$-appropriate primes $p_{e,t}$ from being removed from $V$. If it ever sees $\Phi_e^C(e)$ converge, it will begin protecting primes, and will protect them from then on, unless injured by a higher-priority requirement. As long as $\Phi_{e,s}^C(e)$ diverges, its strategy is to remove from $V$ all $q_e$-appropriate primes it can (but only finitely many at each stage).

We start by making a (uniformly computable) list of the primes which each $\mathcal{R}_e$ will be allowed to protect. Writing $p_{e,-1} = e$ for convenience, we define, for each $e \geq 0$ and $t \geq 0$:

$$p_{e,t} = \min\{\text{primes } p > p_{e,t-1} : (\forall i \leq e + t) \, [p \text{ is } q_i\text{-appropriate} \iff i = e]\}.$$

Corollary 2.5 shows that this set is nonempty, and Lemma 2.4 shows that it is decidable uniformly in $e$ and $t$. Thus $p_{e,0}$ is $q_i$-inappropriate for all $i < e$, so that $\mathcal{R}_e$ will avoid any conflict with higher-priority requirements $\mathcal{R}_i$ which might need to remove $q_i$-appropriate primes from $V$. The next prime $p_{e,1}$ has all these properties and is also $q_{e+1}$-inappropriate, so that if $\mathcal{R}_e$ comes to protect this prime, it will not injure $\mathcal{R}_{e+1}$ by doing so. As $\mathcal{R}_e$ protects increasingly larger primes, it respects more and more requirements of lower priority.

At the stage $s + 1$, we are given $V_s$, and we find the least prime of the form $p_{e,t}$ that has not been considered at any previous stage. At this stage, we consider this prime, fixing the $e$ and $t$ thus determined and writing $s'$ for the (earlier) stage at which $p_{e,t-1}$ was considered (or $s' = 0$ if $t = 0$). We compute $\Phi_{e,s}^C(e)$. If this computation converges, then $\mathcal{R}_e$ continues to protect all primes it protected at stage $s'$ (except any that may have been removed from $V$ by higher-priority requirements in the interim), and also protects $p_{e,t}$. If it diverges, then $\mathcal{R}_e$ does not protect any primes at this stage, and deletes from $V_{s+1}$ those (finitely many) primes $p \in V_s$ satisfying:

- $e < p < p_{e,t}$; and

- $p$ is $q_e$-appropriate; and

- $(\forall i < e) \, \mathcal{R}_i$ is not protecting $p$ at this stage.

Thus $\mathcal{R}_e$ takes another step towards removing all $q_e$-appropriate primes from $V$, since it still appears that $\Phi_e^C(e)$ diverges. This completes the stage, and we set $V = \cap_s V_s$.

We remark that in this construction, if a prime $p$ is ever protected by a requirement $\mathcal{R}_e$, then $p = p_{e,t}$ for some $t$ and no requirement will ever remove $p$ from $V$. $\mathcal{R}_e$ will not: its computation must have converged in order for it to have protected $p$ in the first place, and so it will continue to protect $p$. Moreover, its protection stops any lower-priority $\mathcal{R}_j$ from removing $p$ from $V$. Finally, higher-priority $\mathcal{R}_i$'s will not remove $p$ from $V$ because to have been chosen as $p_{e,t}$, $p$ must have been $q_i$-inappropriate for each such $i$.

We now claim that $V$ is $C$-computable. For a given prime $p$, only requirements $\mathcal{R}_e$ with $e \leq p$ are ever allowed to remove $p$ from $V$. For each $e \leq p$, we can compute the least number $t_e$ for which $p < p_{e,t_e}$. If this $\mathcal{R}_e$ ever removes $p$ from $V$, it must do so by the stage $s_e$ at which $p_{e,t_e}$ is considered; the only reasons why it would not have removed $p$ from $V$ by this stage are either that $p$ is $q_e$-inappropriate or that $\Phi_e^C(e)$ converged before stage $s_e$, or that a higher-priority $\mathcal{R}_i$ is protecting $p$ at that stage. In each of these cases, $\mathcal{R}_e$ will never remove $p$ from $V$. So, by computing the maximum such stage $s = \max_{e \leq p} s_e$ and running the construction up to that stage $s$ (using a $C$-oracle), we can check whether $p \in V$ or not. Thus $V \leq_T C$.

Next we claim that every $\mathcal{R}_e$ is satisfied. Here it is necessary to define the specific polynomial $g_e$ to be used. Let $f_e$ be as above, and let $g_e$ be derived from $f_e$ using Proposition 2.1, so that, for every tuple $(x, y, \vec{z}, \vec{w}) \in \mathbb{Q}^{10}$,

$$g_e(x, y, \vec{z}, \vec{w}) = 0 \iff f_e(x, y, \vec{z}, \vec{w}) = 0 \ \& \ (x, y, \vec{z}, \vec{w}) \in Q_e^{10},$$

where $Q_e$ is the semilocal subring of $\mathbb{Q}$ in which all primes are inverted except those of the form $p_{j,t}$ with $j + t \leq e$. We claim that the map $e \mapsto g_e$ will be a 1-reduction from $C'$ to $HTP(R_V)$. Clearly this map is injective, since each $f_e$ used a different coefficient $q_e$. Moreover, it is computable, because the $C$-oracle is not invoked in the definition of the primes $p_{e,t}$, nor for defining $g_e$. So it remains to see that $e \in C'$ just if $g_e \in HTP(R_V)$.

Suppose first that $e \in C'$, and fix the least stage $s+1$ at which we consider a prime of the form $p_{e,t}$ and for which $\Phi_{e,s}^C(e) \downarrow$. From this stage on, each prime $p_{e,t'}$ with $t' \geq t$ will be protected by $\mathcal{R}_e$, starting at the stage at which it is considered. Since it was chosen to be $q_i$-inappropriate for all $i < e$, and since no lower-priority $\mathcal{R}_j$ can remove from $V$ a prime protected by $\mathcal{R}_e$, each such $p_{e,t'}$ lies in $V$ and gives a solution to $f_e$ in $R_V$. As these primes $p_{e,t'}$ are arbitrarily large, $g_e$ must lie in $HTP(R_V)$.

On the other hand, if $e \notin C'$, then $\mathcal{R}_e$ acts to remove primes from $V$ at each stage $s + 1$ at which any prime $p_{e,t}$ is considered. Therefore, it

ultimately removes from $V$ every $q_e$-appropriate prime $p > e$ except those which are protected by higher-priority requirements $\mathcal{R}_j$. However, each prime $p_{j,t}$ protected by $\mathcal{R}_j$ was chosen to be $q_i$-inappropriate for all $i \leq j + t$ except for $i = j$. In particular, $p_{j,t}$ is $q_e$-inappropriate whenever $e \leq j + t$; and if $e > j + t$, then $\frac{1}{p_{j,t}} \notin Q_e$. Therefore, no $q_e$-appropriate prime is inverted in the subring $(R_V \cap Q_e)$, and so $g_e \notin HTP(R_V)$.

This shows that $C' \leq_1 HTP(R_V)$, via the map $e \mapsto g_e$. It follows that $C' \leq_1 V'$ and therefore $C \leq_T V$ by the Jump Theorem [20, Thm. III.2.3]. On the other hand, with $V \leq_T C$, we have $V' \leq_1 C'$, and of course $HTP(R_V) \leq_1 V'$, so $V$ is HTP-complete. ∎

**Corollary 4.2** *For every Turing degree $\boldsymbol{d} \geq_T \boldsymbol{0}'$, there is a subring of $\mathbb{Q}$ for which Hilbert's Tenth Problem has Turing degree $\boldsymbol{d}$.*

*Proof.* This follows from Theorem 4.1 along with the surjectivity of the jump operator above $\boldsymbol{0}'$, which was first established by Friedberg in [3]. ∎

Many readers will recall [14, Theorem 1.3] of Poonen, described in detail in [19, Ch. 12]. It gives disjoint infinite decidable sets $T_1$ and $T_2$ of primes, both of asymptotic density 0, such that for every $W \supseteq T_1$ disjoint from $T_2$, $R_W$ admits a diophantine model of arithmetic on the positive integers, making $\emptyset' \leq_1 HTP(R_W)$. Unfortunately, the sets $W \subseteq \mathbb{P}$ containing all of $T_1$ (let alone disjoint from $T_2$) form a class that, while of cardinality $2^\omega$, is meager and has measure 0 in $2^{\mathbb{P}}$. Thus this theorem cannot be combined with the results in [12] or [13]. Its conclusion about uncountability resembles Theorem 4.1, which showed that $\{W : W' \leq_1 HTP(R_W)\}$ has size continuum, despite being meager of measure 0 . If the goal is to consider $HTP(\mathbb{Q})$, then $\emptyset' \leq_1 HTP(R_W)$ seems just as relevant as $W' \leq_1 HTP(R_W)$, and Poonen's stronger result about diophantine interpretation, proven by an entirely different and deeper method than here, could be the key to a final answer. (Cf. Theorems 41 and 53 of [12].)

We also remark briefly that using the foregoing method with $C = \emptyset$, one can also prove that there is a decidable subring $R_W \subseteq \mathbb{Q}$ for which $HTP(R_W) \equiv_1 \emptyset'$. Of course, the Matiyasevich-Davis-Putnam-Robinson theorem already proved this result for the far more challenging specific case $R = \mathbb{Z}$. Still, the results here again suggest how a computability-theoretic approach, using techniques such as finite-injury constructions along with basic number theory, can sometimes yield new and different proofs. One continues to hope that those techniques, combined with a deeper use of number

10

theory than in this article, might accomplish more than either discipline can achieve on its own.

Our method here does not appear to provide answers to any of the questions raised in [2, Remarks 3.20 & 4.8] by Eisenträger, Miller, Park, and Shlapentokh. Those questions generally want the degree of $HTP(R_W)$ to be held down, so that $W' \not\leq_T HTP(R_W)$, whereas the method of this section is appropriate for coding information into $HTP(R_W)$ and thus making its Turing degree large.

# 5   Enumeration Operators

Theorem 3.2 was proven with no use of the HTP-operator specifically. It used only the fact that $HTP$ is an *enumeration operator*. Recall that an *enumeration* of a subset $A$ of $\omega$ is a subset $B$ of $\omega$ that, when viewed as a subset of $\omega^2$, projects onto $A$ via the projection $\pi_1$:

$$A = \pi_1(B) = \{x \in \omega : (\exists y) \ \langle x, y \rangle \in B\}.$$

This is equivalent to various other definitions (often using functions).

**Definition 5.1** Let $G : 2^\omega \to 2^\omega$ be a function. $G$ is said to be an *enumeration operator* if there exists a Turing functional $\Gamma$ such that, for every $A \in 2^\omega$ and every enumeration $C$ of $A$, $\Gamma^C$ is a total function from $\omega$ into $\{0, 1\}$ and is the characteristic function of an enumeration of $G(A)$. (It is also natural to refer to $\Gamma$ itself as the enumeration operator, but it confuses matters. We will say here that $\Gamma$ *represents* $G$.)

We write $B \leq_e A$, and say that $B$ is *enumeration-reducible to $A$*, or *e-reducible to $A$*, if there is an enumeration operator $G$ with $G(A) = B$. This is equivalent to the usual definition, e.g. in [17, §9.7].

It is immediate from the definition that if $\Gamma$ represents an enumeration operator and $\pi_1(C_0) = \pi_1(C_1)$, then $\pi_1(\Gamma^{C_0}) = \pi_1(\Gamma^{C_1})$. We note that other definitions of $e$-reducibility are standard in the literature, and are readily shown to be equivalent to this one. The essence is that there exists a uniform procedure that accepts any enumeration of $A$ and uses it to compute an enumeration of $G(A)$.

The jump operator $J$, mapping each $A$ to $A'$, is the prototype of the functions called *pseudojump operators* by Jocksuch and Shore in [5, 6], whose

11

output can be enumerated uniformly when we are given $A$ itself (not just an enumeration) as the oracle. However, the jump operator is not an enumeration operator. To see this, notice that if it were, then $\emptyset'' = J(\emptyset')$ would also be computably enumerable, since we could run the representation $\Gamma$ on a computable enumeration of $\emptyset'$ to get a computable enumeration of $J(\emptyset')$. For a better understanding of the failure of the jump to be an enumeration operator, consider a functional $\Phi_e$ for which, for all $x$,

$$\Phi_e^A(x) = \begin{cases} 0, & \text{if } 17 \notin A; \\ \uparrow, & \text{if } 17 \in A. \end{cases}$$

Now if some functional $\Gamma$ represented the jump (as an enumeration operator), then with $A = \emptyset$ we would have $\Gamma^\emptyset(e) = 1$, as $\emptyset$ itself is an enumeration of $\emptyset$. But if $u$ is the use of this computation, then one readily can create an enumeration $C$ of an arbitrary $B \subseteq \omega$ with $C{\restriction}u = 0^u$, and $\Gamma^C(e)$ would have to equal $1$ for each such $C$, by the Use Principle. Hence $\Gamma$ either fails to be an enumeration operator, or else fails to compute the jump, because many sets $A$ (indeed a class of measure $\frac{1}{2}$) have $e \notin A'$.

The next result generalizes Theorem 3.2, and we now give a proof, by exactly the same means as in [8, Cor. 3.3].

**Theorem 5.2** *For every enumeration operator $E$, the collection $\{A \in 2^\omega : A' \leq_1 E(A)\}$ is meager and has measure $0$.*

*Proof.* With $E$ fixed, we show that $A' \not\leq_1 E(A)$ for every set $A$ such that, for some set $B <_T A$, $A$ is $B$-computably enumerable. Indeed, $E(A)$ must then also be $B$-c.e., so $E(A) \leq_1 B'$. However, with $A \not\leq_T B$, we have $A' \not\leq_1 B'$, by the Jump Theorem (see e.g. [20, Thm. III.2.3]). It would now contradict the transitivity of 1-reducibility to have $A' \leq_1 E(A)$.

By results of Jockusch and his student (at the time) Kurtz in [4, 9], the class of *relatively c.e. sets*, i.e., those $A$ for which a $B$ exists as described above, is a comeager class of measure $1$. The theorem follows. ∎

On the other hand, it is quite possible for $\{A \in 2^\omega : A' \leq_T E(A)\}$ to be comeager and to have measure $1$. Indeed, the enumeration operator mapping $A$ to $(\emptyset' \oplus A)$ has this property: it is well-known that the class $GL_1$ of *generalized-low* sets, i.e., those satisfying $A' \leq_T \emptyset' \oplus A$, is comeager and has full measure. Here we focus on the possibility of computing $A'$ uniformly (via a single Turing functional) from $E(A)$.

**Theorem 5.3** *For every Turing functional $\Psi$ and every enumeration operator $E$, $\mu(\{A \in 2^\omega : \chi_{A'} = \Psi^{E(A)}\}) < 1$.*

**Corollary 5.4** *For every Turing operator $\Phi$, there exists a set $\mathcal{S}$ of positive measure such that, for all $W \in \mathcal{S}$,*

$$\Phi^{HTP(R_W)} \neq \chi_{W'}.$$

*Proof of Theorem 5.3.* We fix an index $e$ for a Turing functional defined as follows:

$$\Phi_e^A(x) = \begin{cases} 0, & \text{if } (\exists m > 1) \ \{m+1, m+2, \ldots, 2m\} \cap A = \emptyset; \\ \uparrow, & \text{otherwise.} \end{cases}$$

Thus the measure of the set of those $A$ with $e \in A'$ is at most $\frac{1}{2}$ (in fact, somewhat less than $\frac{1}{2}$ because of overlaps) and certainly positive. Suppose that, on a set of measure 1, $\Psi^{E(A)} = A'$ (that is, $\Psi^{E(A)}$ computes the characteristic function of $A'$). Then $\mu(\{A : \Psi^{E(A)}(e)\!\downarrow= 0\}) > 0$. By the countable additivity of Lebesgue measure, there must exist a specific $\sigma \in 2^{<\omega}$ such that $\Psi^\sigma(e)\!\downarrow= 0$ and such that $\mu(\{A : \sigma \sqsubseteq E(A)\}) > 0$. Indeed, since the relation $\sigma^{-1}(1) \subseteq E(A)$ is always created by a finite subset of $A$, there must then exist a finite set $S_0$ such that $\sigma \sqsubseteq E(S_0)$ and $\mu(\{A : S_0 \subseteq A \ \& \ \sigma \sqsubseteq E(A)\}) > 0$, since there are only countably many finite subsets $S$ of $\omega$. (To avoid confusion, in this proof we write $\sigma \sqsubseteq E(A)$ to mean that $\sigma$ is an initial segment of $E(A) \in 2^\omega$, and $S \subseteq A$ to mean simply that $S$ is a subset of $A$, not necessarily an initial segment.)

We fix such a $\sigma$ and such an $S_0$, and choose an integer $m > \max(S_0)$ (with $m > 1$ as well). Let $\mathcal{W} = \{A : S_0 \subseteq A \ \& \ \sigma \sqsubseteq E(A)\}$, which is thus guaranteed to have positive measure. Now consider the class

$$\mathcal{V} = \{B \in 2^\omega : (\exists A \in \mathcal{W}) \ B = A - \{m+1, m+2, \ldots, 2m\}\}.$$

For every such $B$, $m$ witnesses that $e \in B'$, according to our definition of $\Phi_e$. (In contrast, only measure-0-many $A \in \mathcal{W}$ lie in $\mathcal{V}$, since $e \notin A'$.) Moreover, since $m > \max(S_0)$, all $B \in \mathcal{V}$ have $S_0 \subseteq B$ and thus have $E(S_0) \subseteq E(B)$, since enumeration operators are clearly monotone under $\subseteq$. On the other hand, each $B \in \mathcal{V}$ has a corresponding $A \in \mathcal{W}$ for which $B \subseteq A$, so that $E(B) \subseteq E(A)$. Together these yield $\sigma \sqsubseteq E(B)$, since $E(S_0)$ and $E(A)$ agree up to $|\sigma|$. But now, for every $B \in \mathcal{V}$, we have $\Psi^{E(B)}(e)\!\downarrow= \Psi^\sigma(e) = 0$, even though $e \in B'$.

13

It remains to show that $\mathcal{V}$ has positive measure. Suppose $\{\mathcal{U}_{\tau_i} : i \in \omega\}$ is a cover of $\mathcal{V}$ by basic open subsets $\mathcal{U}_{\tau_i} = \{C : \tau_i \sqsubseteq C\}$ of Cantor space, and suppose that this cover has total Lebesgue measure $r$. By the definition of $\mathcal{V}$, we may assume that $\tau_i(n) = 0$ for all $n \in \{m+1, \ldots, 2m\}$ and all $i$ with $n < |\tau_i|$. Now, for each of the $(2^m - 1)$-many binary strings $\rho$ of length $m$ (excluding the zero string $0^m$), let $\mathcal{T}_{i,\rho} = \mathcal{U}_{\tau_{i,\rho}}$, where

$$\tau_{i,\rho}(n) = \begin{cases} \rho(n - (m+1)), & \text{if } m+1 \leq n \leq 2m \ \& \ n < |\tau_i|; \\ \tau_i(n), & \text{otherwise.} \end{cases}$$

That is, $\tau_{i,\rho}$ is the same as $\tau_i$, except that the portion from $(m+1)$ up to $2m$, which was all zeroes in $\tau_i$, is replaced by the (nonzero) string $\rho$. Thus $\mu(\mathcal{U}_{\tau_i}) = \mu(\mathcal{T}_{i,\rho})$ for all $i$ and $\rho$. Since the sets $\mathcal{U}_{\tau_i}$ form a cover of $\mathcal{V}$, the definition of $\mathcal{V}$ shows that the sets $\mathcal{T}_{i,\rho}$ form an cover of $\mathcal{W}$ by basic open sets in Cantor space, so that their total measure is $\geq \mu(\mathcal{W}) > 0$. Also, for any two distinct $\rho$ (and the same $i$), the strings $\tau_{i,\rho}$ are distinct; whereas for distinct $i$ and the same $\rho$, the overlap between strings $\tau_{i,\rho}$ is equal in measure to the overlap between the corresponding $\tau_i$. It follows that

$$\mu(\mathcal{W}) \leq \mu\left(\bigcup_{i \in \omega} \bigcup_{\text{nonzero } \rho \in 2^m} \mathcal{T}_{i,\rho}\right) = (2^m - 1) \cdot \mu\left(\bigcup_i \mathcal{U}_{\tau_i}\right).$$

Therefore, this open cover $\{\mathcal{U}_{\tau_i}\}$ of $\mathcal{V}$ has Lebesgue measure at least $\frac{\mu(\mathcal{W})}{2^m - 1}$, and this positive lower bound is independent of the choice of cover of $\mathcal{V}$. So $\mu(\mathcal{V})$ is positive as well, and we saw above that $\Psi^{E(B)}(e) \downarrow \neq B'(e)$ for all $B \in \mathcal{V}$. ∎

It remains possible, therefore, that $W' \leq_T HTP(R_W)$ might hold for measure-1-many sets $W$, but if so, it requires infinitely many Turing functionals to establish this fact. Similarly, the reduction $A' \leq_T \emptyset' \oplus A$ can be established on a set of measure $(1-\epsilon)$ by a single functional $\Phi$ (for arbitrarily small $\varepsilon > 0$), but countably many functionals are required to show that it holds on a set of measure 1. (In that case, the countably many functionals can be produced uniformly in the rational number $\varepsilon > 0$.)

# 6 Existential Definability of $\mathbb{Z}$

Existential definability of a subset $S$ of $\mathbb{Q}$ (in the usual model-theoretic notion, i.e., defining a unary relation on the field $\mathbb{Q}$ whose elements are

14

precisely the elements of $S$) is equivalent to $S$ being *diophantine* in the ring $\mathbb{Q}$. This means that, for some $n$, $S$ is defined by a single polynomial $f \in \mathbb{Q}[X, Y_1, \ldots, Y_n]$ as follows:

$$(\forall r \in \mathbb{Q}) \ [r \in S \iff (\exists \vec{y} \in \mathbb{Q}^n) \ f(r, \vec{y}) = 0].$$

All more complicated existential definitions can be boiled down to definitions of this form.

It is unknown whether the set $\mathbb{Z}$ is existentially definable in the field $\mathbb{Q}$. Julia Robinson gave the first definition of $\mathbb{Z}$ in $\mathbb{Q}$, in [16]. That definition was $\Pi_4$. Significant subsequent work has reduced the complexity of such definitions: Poonen [15] gave a $\Pi_2$ definition, and then Koenigsmann [7] gave a $\Pi_1$ (that is, purely universal) definition. Thus we seem to be getting closer to an existential definition. However, there are number-theoretic conjectures, notably by Mazur, that would imply the existential undefinability of $\mathbb{Z}$ in $\mathbb{Q}$.

An existential definition of $\mathbb{Z}$ in $\mathbb{Q}$ would imply $HTP(\mathbb{Z}) \leq_1 HTP(\mathbb{Q})$, and hence $\emptyset' \leq_1 HTP(\mathbb{Q})$, so it is highly relevant to this article. However, our purpose in this section is to investigate other possible consequences of $\exists$-definability of $\mathbb{Z}$ in $\mathbb{Q}$. The main point is that, if any of these consequences should be shown not to hold, it would follow that $\mathbb{Z}$ is not diophantine in $\mathbb{Q}$.

From an existential definition of $\mathbb{Z}$ within the field $\mathbb{Q}$, we would immediately get a stronger result.

**Lemma 6.1** *If $\mathbb{Z}$ has an existential definition in $\mathbb{Q}$, then indeed there is a polynomial $h \in \mathbb{Z}[X, Y_1, \ldots, Y_k]$ such that, for all $x \in \mathbb{Q}$,*

$$x \in \mathbb{Z} \iff (\exists \vec{y} \in \mathbb{Q}^k) \ h(x, \vec{y}) = 0 \iff (\exists \vec{y} \in \mathbb{Z}^k) \ h(x, \vec{y}) = 0.$$

*Thus the formula $(\exists Y_1 \cdots \exists Y_k) h(X, \vec{Y}) = 0$ would define $\mathbb{Z}$ not only in $\mathbb{Q}$, but also in every subring of $\mathbb{Q}$. Likewise, every c.e. set would have an existential definition that holds in every subring of $\mathbb{Q}$.*

*Proof.* Assume that the formula $(\exists Z_1, \ldots, Z_j) \ g(X, \vec{Z}) = 0$ defines $\mathbb{Z}$ in $\mathbb{Q}$, with $g$ of total degree $d$. Define $h(X, \vec{Y}, \vec{T})$ to be the polynomial

$$g\left(X, \frac{Y_1}{1 + T_1^2 + \cdots + T_4^2}, \ldots, \frac{Y_j}{1 + T_1^2 + \cdots + T_4^2}\right) \cdot (1 + T_1^2 + \cdots + T_4^2)^d$$

Now if $x \in \mathbb{Z}$, then there is $\vec{z} \in \mathbb{Q}^j$ with $g(x, \vec{z}) = 0$. Taking a positive common denominator $v \in \mathbb{Z}_{>0}$ of the rationals $z_i$, use the Four Squares

15

Theorem to write $v - 1 = t_1^2 + t_2^2 + t_3^2 + t_4^2$ with all $t_i \in \mathbb{Z}$ and let $y_i = vz_i$. Then $(\vec{y}, \vec{t})$ is a solution to $h(x, \vec{Y}, \vec{T}) = 0$ in $\mathbb{Z}$, hence in every subring of $\mathbb{Q}$.

Conversely, for any $(x, \vec{y}, \vec{t})$ in a subring of $\mathbb{Q}$ with $h(x, \vec{y}, \vec{t}) = 0$, setting $z_i = \frac{y_i}{1 + t_1^2 + t_2^2 + t_3^2 + t_4^2}$ gives $g(x, \vec{z}) = 0$ with all $z_i \in \mathbb{Q}$, so $x \in \mathbb{Z}$. ∎

## 6.1 Preservation of $m$-reductions

It was seen in [8] that the HTP operator can fail to preserve Turing reductions, and indeed that it can sometimes reverse them: it is possible to have $V <_T W$, yet $HTP(R_W) <_T HTP(R_V)$, with strictness in both relations. (This result is [8, Corollary 5.3].) Whether the same operator must respect the stronger notion of $m$-reducibility remains an open question. Here we connect that question to the existential definability of $\mathbb{Z}$ in $\mathbb{Q}$, first giving the relevant definitions.

**Definition 6.2** For subsets $A, B \subseteq \omega$, a computable total function $F : \omega \to \omega$ is an *m-reduction* from $A$ to $B$ if it satisfies

$$(\forall x \in \omega) \ [x \in A \iff F(x) \in B].$$

A 1-*reduction* is just an $m$-reduction which is also one-to-one (as opposed to *many-to-one*, whence the terminology). We write $A \leq_1 B$ and $A \leq_m B$ to denote the existence of 1-reductions and $m$-reductions, respectively. Clearly these are both partial preorders on the power set of $\omega$.

The reader may wonder why the distinction is made between $m$- and 1-reducibility. There do exist sets $A$ and $B$ with $A \leq_m B$ but $A \nleq_1 B$, and they can be chosen to be infinite and coinfinite (thus avoiding the simple situation where $1 \leq |B| < |A| < \infty$). Nevertheless, in computability theory, 1-reducibility is regarded as nearly equivalent to $m$-reducibility. Our first lemma suggests that this seems to hold here as well.

**Lemma 6.3** *For sets $A \subseteq \omega$ and $W \subseteq \mathbb{P}$, we have $A \leq_m HTP(R_W)$ if and only if $A \leq_1 HTP(R_W)$.*

*Proof.* For the nontrivial direction, let $G$ be an $m$-reduction. Then each value $G(n)$ is a polynomial in $\mathbb{Z}[X_1, X_2, \ldots]$, say, and we simply define:

$$F(n) = (G(n))^2 + (X_0)^{2n}.$$

The polynomial $F(n)$ (from $\mathbb{Z}[X_0, X_1, \ldots]$) has a solution in $R_W$ just if $G(n)$ does, and the exponent $2n$ makes $F$ injective. ∎

**Corollary 6.4** *If the HTP operator respects m-reductions, then it respects 1-reductions.* ∎

Nevertheless, there is an important reason to distinguish between 1- and *m*-reducibility, as seen in the following theorem.

**Theorem 6.5** *Each of the following implies the next.*

1. *$Z$ is existentially definable in the field $\mathbb{Q}$.*

2. *The HTP operator respects m-reducibility (i.e., if $V \leq_m W$, then $HTP(R_V) \leq_m HTP(R_W)$).*

3. *$\emptyset' \leq_1 HTP(\mathbb{Q})$.*

In contrast, we do not know whether (3) follows from the assumption that HTP preserves 1-reductions.

*Proof.* We first show that (2) implies (3). Consider $V = \{3\}$ and $W = \mathbb{P} - \{3\}$. Clearly $V \leq_m W$: just let $F(3) = 5$ and $F(p) = 3$ for all $p \neq 3$. (This would work for any nonempty finite $V$ and any proper cofinite $W$, of course.) By (2), we get $HTP(\mathbb{Z}[\frac{1}{3}]) \leq_m HTP(R_{\mathbb{P}-\{3\}})$. But Julia Robinson showed that $\emptyset' \leq_1 HTP(\mathbb{Z}[\frac{1}{3}])$ (and likewise for all finitely generated subrings of $\mathbb{Q}$), whereas $HTP(R_{\mathbb{P}-\{3\}}) \leq_1 HTP(\mathbb{Q})$ by Corollary 2.2, proving (3).

Next we assume (1) and prove (2). With an *m*-reduction from $V$ to $W$, we can readily compute an *m*-reduction from $R_V$ to $R_W$: that is, a computable, total, function $G$ with

$$(\forall q \in \mathbb{Q}) \; [q \in R_V \iff G(q) \in R_W].$$

$\exists$-definability of $\mathbb{Z}$ implies that every c.e. set, and in particular the graph of $G$, is diophantine in $\mathbb{Q}$, so by Lemma 6.1 we have a polynomial $g$ such that, for all $q, r \in \mathbb{Q}$:

$$G(q) = r \iff g(q, r, Z_1, \ldots, Z_m) \in HTP(\mathbb{Z})$$
$$\iff g(q, r, Z_1, \ldots, Z_m) \in HTP(\mathbb{Q}).$$

Thus the following holds of every $f \in \mathbb{Z}[X_0, \ldots, X_{k-1}]$:

$$
\begin{aligned}
f \in HTP(R_V) \iff & (\exists \vec{q} \in (R_V)^k) \; f(\vec{q}) = 0 \\
\iff & (\exists \vec{q} \in \mathbb{Q}^k)(\exists \vec{r} \in (R_W)^k) \; [f(\vec{q}) = 0 \; \& \; (\forall i < k) \; G(q_i) = r_i] \\
\iff & (\exists \vec{q} \in \mathbb{Q}^k)(\exists \vec{r} \in (R_W)^k) \\
& [f(\vec{q}) = 0 \; \& \; (\forall i < k) \; g(q_i, r_i, Z_{i1}, \ldots, Z_{im}) \in HTP(R_W)] \\
\iff & (\exists \vec{s}, d, \vec{r}, z_{01}, \ldots, z_{km} \in R_W) \; \left[ f\left(\frac{s_1}{d}, \ldots, \frac{s_k}{d}\right) = 0 \; \& \right. \\
& \left. \& \; (\forall i < k) \; g\left(\frac{s_i}{d}, r_i, z_{i1}, \ldots, z_{im}\right) = 0 \; \& \; d \neq 0 \right]
\end{aligned}
$$

Since the equations (and the inequation) in the second-to-last line can all be collected into a single polynomial equation with the $d$'s cleared from the denominators, we have computed (from $f$) a single polynomial which lies in $HTP(R_W)$ just if $f$ itself lies in $HTP(R_V)$. ■

## 6.2   Boundary Sets of Polynomials

The key to our use of the polynomials $f_e$ built using $(X^2 + q_e Y^2 - 1)$ in Theorem 4.1, and also in the results in [8], was that, once we built $f_e$ and thus ruled out the trivial solutions, they have nonempty *boundary sets*, according to the following definition.

**Definition 6.6** For a polynomial $f \in \mathbb{Z}[X_1, X_2, \ldots]$, write:

- $\mathcal{A}(F) = \{W \in 2^{\mathbb{P}} : f \in HTP(R_W)\}$;

- $\mathcal{C}(F) = \{W \in 2^{\mathbb{P}} : (\exists \text{ finite } S_0 \subseteq \overline{W}) \; f \notin HTP(R_{\mathbb{P}-S_0})\}$;

- $\mathcal{B}(F) = 2^{\mathbb{P}} - \mathcal{A}(f) - \mathcal{C}(f)$; the *boundary set* of $f$.

With $\mu$ as the Lebesgue measure on $2^{\mathbb{P}}$, we also write $\alpha(f) = \mu(\mathcal{A}(f))$, $\beta(f) = \mu(\mathcal{B}(f))$, and $\gamma(f) = \mu(\mathcal{C}(f))$.

The Cantor space $2^{\mathbb{P}}$ is equipped with the usual topology. Here $\mathcal{A}(f)$ is always an open set, since each solution to $f$ requires only that a certain finite set of primes be inverted in $R_W$. $\mathcal{C}(f)$ is the interior of the complement of $\mathcal{A}(f)$, the set of subrings where the non-invertibility of some finite set of primes rules out the possibility of a solution to $f$. Therefore, $\mathcal{B}(f)$ is indeed the topological boundary of $\mathcal{A}(f)$, and contains those $W$ such that $f$ has no

solution in $R_W$, but such that, for every $n$, it is possible to extend $W{\restriction}n$ to some set $V$ with $f \in HTP(R_V)$. (In the phrase of Alexandra Shlapentokh, $f$ "never loses hope" of having a solution in $R_W$.) Often $\mathcal{B}(f)$ is empty, but the polynomials $f_e$ have nonempty boundary sets: indeed $\mathcal{B}(f_e)$ contains every subset of the set of $q_e$-inappropriate primes, which Lemma 2.4 showed to be an infinite set. This is what allowed our coding to work, in Theorem 4.1: no matter how many primes we removed from $V$, there was always some prime not yet removed which, if it stayed in $V$, would cause $f_e$ to lie in $HTP(R_W)$. So, no matter how long $\Phi_e^C(e)$ might take to converge, we could always code its convergence into $HTP(R_W)$ when and if we saw the computation halt.

On the other hand, the definitions of $\alpha$, $\beta$, and $\gamma$ suggested that we care about the measures of these sets, and here the $f_e$ polynomials are not so impressive. Indeed, $\alpha(f_e)$ is always 1, for every $e$, because the set of $q_e$-appropriate primes is infinite and the inversion of any single element of that set will yield a solution to $f_e$. It remains an open question whether any polynomial $f$ at all can have $\beta(f) > 0$. In this section we discuss the possible consequences of an answer to this question.

The overall boundary set $\mathcal{B}$ is defined by:

$$\mathcal{B} = \bigcup_{f \in \mathbb{Z}[X_1, X_2, \ldots]} \mathcal{B}(f).$$

Each $\mathcal{B}(f)$ is nowhere dense in $2^{\mathbb{P}}$, in the sense of Baire category, and therefore $\mathcal{B}$ itself is meager. This shows that there must exist subrings of $\mathbb{Q}$ which lie in no boundary set $\mathcal{B}(f)$. These are called *HTP-generic* subrings, and are studied in [12, 13]. As noted above, although the complement $\overline{\mathcal{B}}$ is comeager and thus large in the sense of Baire category, it is unknown whether its measure is 0 or 1, and even values between 0 and 1 have not been ruled out. We remark that, for an individual polynomial $f$, we always have $\beta(f) < 1$, because the only way to have $\alpha(f) = 0$ is for the open set $\mathcal{A}(f)$ to be empty, in which case $\mathcal{C}(f) = 2^{\mathbb{P}}$ and $\mathcal{B}(f) = \emptyset$.

## 6.3 Noncomputable $\beta(f)$

The next theorem will be superseded by Theorem 6.9, but its proof is useful as an introduction to the proof of the latter theorem, and so we present it in full here.

**Theorem 6.7** *If the boundary set $\mathcal{B}$ has measure $< 1$, then there is no existential definition of $\mathbb{Z}$ within the field $\mathbb{Q}$.*

*Proof.* We prove the contrapositive, by assuming that $\mathbb{Z}$ does have an $\exists$-definition in $\mathbb{Q}$ and showing, for an arbitrary positive real number $r < 1$ which is approximable from below, that there exists a polynomial $f \in \mathbb{Z}[\vec{X}]$ with $\alpha(f) = r$ and $\gamma(f) = 0$. ("Approximable from below" means that the left Dedekind cut of $r$ is c.e.) This will establish that the measure $\beta(f) = 1 - r$, proving the theorem, since $\mathcal{B}(f) \subseteq \mathcal{B}$.

So fix such a number $r$, and let $q_0, q_1, \ldots$ be a computable, strictly increasing sequence of positive rational numbers with $\lim_s q_s = r$. Let $n_0$ be the least integer with $2^{-n_0} \le q_0$, which is to say, $1 - 2^{-n_0} \ge 1 - q_0$. Now define by recursion

$$n_{k+1} = \min\{n \in \mathbb{N} : (1 - 2^{-n}) \cdot (1 - 2^{-n_k}) \cdots (1 - 2^{-n_0}) \ge 1 - q_{k+1}\}.$$

With $q_{k+1} > q_k$, such an $n_{k+1}$ always exists (and must be positive, since $q_{k+1} < 1$), and the sequence $\langle n_i \rangle_{i \in \mathbb{N}}$ is computable. Moreover, by the minimality of each $n_k$, $\prod_{k \ge 0}(1 - 2^{-n_k}) = 1 - \lim_k q_k = 1 - r$.

Next, let $x_0 = p_0 \cdot p_1 \cdots, p_{n_0 - 1}$ be the product of the first $n_0$ prime numbers. Then set $x_{k+1} = p_{n_0 + \cdots + n_k} \cdots p_{n_0 + \cdots + n_{k+1} - 1}$ to be the product of the next $n_{k+1}$ primes, for each $k$ in turn. The set $D = \{x_k : k \in \mathbb{N}\}$ is computably enumerable (indeed computable), hence diophantine. Since we are assuming that $\mathbb{Z}$ is $\exists$-definable in $\mathbb{Q}$, there exists a polynomial $g \in \mathbb{Z}[X, Y_1, \ldots, Y_m]$ such that

$$D = \{x \in \mathbb{Z} : g(x, Y_1, \ldots, Y_m) \in HTP(\mathbb{Z})\}$$
$$= \{x \in \mathbb{Q} : g(x, Y_1, \ldots, Y_m) \in HTP(\mathbb{Q})\}.$$

(This simply requires that we start with a polynomial which defines the set $D = \{x_k : k \in \mathbb{N}\}$ within $\mathbb{Z}$, and then apply Lemma 6.1 to transfer the definition of $\{x_k : k \in \mathbb{N}\}$ to $\mathbb{Q}$.) The $f(X, \vec{Y}, T)$ we desire is simply the sum

$$(g(X, Y_1, \ldots, Y_m))^2 + (XT - 1)^2.$$

We claim that this $f$ satisfies $\alpha(f) = r$ and $\gamma(f) = 0$.

Notice first that every solution $(x, \vec{y}, t)$ to $f$ in $\mathbb{Q}$ must have $g = 0$, hence has $x \in \mathbb{Z}$ and all $y_i \in \mathbb{Z}$. But then $x = x_k$ for some $k$, by our choice of $g$, and $t = \frac{1}{x_k}$. In order for this solution to lie in a subring $R$ of $\mathbb{Q}$, therefore,

that subring $R$ must contain multiplicative inverses of all the prime factors $p_{n_0+\cdots+n_{k-1}}, \ldots, p_{n_0+\cdots+n_k-1}$ of this $x_k$. (Notice that this list contains exactly $n_k$ primes.)

Conversely, suppose that a subring $R$ does contain all these primes (for some $k$). Then it contains $t = \frac{1}{x_k}$, and since $x_k \in \mathbb{N}$, there exist integers $y_1, \ldots, y_m$ which, along with $x_k$ and $t$, form a solution to $f$ in $R$.

Therefore, the subrings in which $f$ has a solution are exactly those in which, for some $k$, all of the $n_k$ prime factors of $x_k$ have inverses. For a single $k$, the measure of the set of such subrings is $2^{-n_k}$. Since all distinct $x_k$ have completely distinct prime factors, the set of subrings containing no solution to $f$ therefore has measure

$$\prod_k (1 - 2^{-n_k}) = 1 - r,$$

and so the set $\mathcal{A}(f)$ of subrings with solutions to $f$ has measure precisely equal to $r$. That is, $\alpha(f) = r$.

Finally, it is clear that every semilocal subring $R$ of $\mathbb{Q}$ contains a solution of $f$. Indeed, for some $k$, $R$ must contain inverses of all primes $\geq p_{n_0+\cdots+n_k}$, so our analysis above yields a solution in $R$. It follows that $\mathcal{C}(f) = \emptyset$, so $\beta(f) = 1 - \alpha(f) - \gamma(f) = 1 - r$. ∎

The proof of Theorem 6.7 actually showed more. Assuming an $\exists$-definition of $\mathbb{Z}$ in $\mathbb{Q}$, we constructed a polynomial $f$ with $\alpha(f) = r$ and $\beta(f) = 1 - r$, under the condition that $r \in (0, 1)$ be approximable from below. In particular, this shows that both $\alpha(f)$ and $\beta(f)$ can be noncomputable, since a real number $r$ can be approximable from below without being approximable from above.

**Corollary 6.8** *If $\mathbb{Z}$ has an existential definition in $\mathbb{Q}$, then for every real number $r \in (0, 1)$ which is approximable from below, then there is a polynomial $f \in \mathbb{Z}[\vec{X}]$ with $\alpha(f) = r$ and $\beta(f) = 1 - r$.* ∎

Finally, we remark that in the proof of Theorem 6.7, it is possible to put an upper bound on the degrees of the polynomials $f$ produced. First of all, the polynomials $h$ and $j$ (and $(XT - 1)$) are all fixed independently of $r$, and hence so is the total degree $d$ of $h$. Only $g$ depends on $r$: $g$ was chosen to define (in $\mathbb{Z}$) the set $D$ of products $x_k$ of primes, and the number of prime factors of each $x_k$ depends on $r$. However, by fixing a single polynomial

21

$G \in \mathbb{Z}[E, X, Y_1, \ldots, Y_k]$ which defines the Halting Problem in $\mathbb{Z}$, we may then take our $g$ (for a given $r$) to be of the form $G(e, X, \vec{Y})$ for some natural number $e$. (In fact, the choice of $e$ can be made effectively, once we know an index for the computable sequence $\langle q_k \rangle_{k \in \mathbb{N}}$ of rationals approaching $r$ from below.) Therefore, regardless of the value of $r$, the total degree of $g$ need never be more than that of the fixed polynomial $G$, and this in turn puts a bound on the total degree of the $f$ we eventually produced.

## 6.4 Reals of Greater Complexity

Having seen in Subsection 6.3 how to use arbitrary c.e. sets, along with the assumption of $\exists$-definability of $\mathbb{Z}$ in $\mathbb{Q}$, to build polynomials $f$ with $\beta(f)$ non-computable, we now enhance our construction of the c.e. set, so as to make $\beta(f)$ have even higher complexity. From its definition, $\beta(f) = 1 - \alpha(f) - \gamma(f)$, and $\alpha(f)$ must always be approximable from below, while $\beta(f)$ must be $HTP(\mathbb{Q})$-approximable from below, hence $\emptyset'$-approximable from below. We will emulate Theorem 6.7, assuming $\exists$-definability of $\mathbb{Z}$ in $\mathbb{Q}$ and building a c.e. set of products of primes so as to show that these are the best possible bounds on the complexity of these real numbers.

**Theorem 6.9** *Assume that $\mathbb{Z}$ has an $\exists$-definition in $\mathbb{Q}$. Then, given any two positive real numbers $u$ and $v$ with $u + v < 1$, such that $u$ is computably approximable from below and $v$ is $\emptyset'$-computably approximable from below, there exists a polynomial $f$ with $\alpha(f) = u$ and $\gamma(f) = v$, hence with $\beta(f) = 1 - u - v$.*

*Proof.* We repeat the technique of Theorem 6.7, by enumerating the product $\Pi_{p \in I} \, p$ of a finite set $I$ of primes into a c.e. set $D$ when we want the subring $\mathbb{Z}[I]$ to contain a solution to our polynomial $f$. This $f$ will be defined as $g^2 + (XT - 1)^2$ exactly as in that theorem, using a polynomial $g(X, \vec{Y})$ that defines $D$ in $\mathbb{Q}$ (which exists by the hypothesis of $\exists$-definability of $\mathbb{Z}$ in $\mathbb{Q}$). However, the enumeration of $D$ is now more intricate: distinct elements of $D$ need no longer be relatively prime.

The enumeration of $D$ yields an enumeration of a c.e. set of nodes $\sigma \in 2^{<\mathbb{P}}$: those $\sigma$ such that the products of the primes in $\sigma^{-1}(1)$ lies in $D$. (Notice that a single element of $D$ may produce several such $\sigma$. For example, if $35 \in D$, then the strings 0011, 1011, 0111, and 1111 all are enumerated.) By the construction, then, these $\sigma$ will be precisely the nodes naming the open set

$\mathcal{A}(f)$, which will contain all subrings of $\mathbb{Q}$ extending any such $\sigma$. At a stage $s$ in our construction, those $\sigma$ such that this product is divisible by some $x \in D_s$ (that is, by some $x$ already enumerated into $D$) will be said to be colored green at this stage. (We think of them as having a "green light": a solution to $f$ in the relevant subring is already known.) At stage $s$, the nodes colored red will be those nodes $\tau$ such that no $\sigma \supseteq \tau$ is green. Thus a node may cease to be red at a particular stage, when it or a successor turns green; if this happens, it will never again be red, although this node itself might also never turn green.

By assumption there exsts a computable, strictly increasing sequence $\langle u_s \rangle_{s \in \omega}$ of positive rational numbers with $u = \lim_s u_s$. Additionally, there exists a computable total "chip" function $c : \omega \to (0,1) \cap \mathbb{Q}$ such that

$$\{q \in \mathbb{Q} : 0 < q < v\} = \{q \in \mathbb{Q} \cap (0,1) : c^{-1}((0,q]) \text{ is finite}\},$$

so that the strict left Dedekind cut defined by $v$ is precisely the set of rational numbers receiving only finitely many "chips" from $c$. ([20, Thm. IV.3.2] gives the essence of the construction of $c$.) Notice also that with $v < 1 - u$, there will be infinitely many $s$ with $c(s) < 1 - u < 1 - u_s$. Indeed, by fixing a rational number $q_0 \in (v, 1 - u)$ and ignoring all stages $s$ with $c(s) > q_0$, we may assume that $c(s) < 1 - u_s$ for every stage $s$.

At stage 0, $D_0$ is empty. At stage $s + 1$, only finitely many nodes can be minimal (under $\subseteq$) with the property of having been green at stage $s$, since (by induction) $D_s$ was finite. We fix the least level $l_s$ such that every minimal green node at stage $s$ lies at a level $\leq l_s$; thus, at each level $\geq l_s$, every node must be either red or green at stage $s$. (Below that level, a node may be neither color at stage $s$.) We can list out the (finitely many) nodes that are minimal with the property of having been red at stage $s$: let these be $\rho_{0,s}, \ldots, \rho_{j_s,s}$, ordered by length so that $|\rho_{i,s}| \leq |\rho_{i+1,s}|$ and so that, if these lengths are equal, then $\rho_{i,s} \prec \rho_{i+1,s}$ in the lexicographic order $\prec$ on nodes. We regard $\rho_{0,s}, \ldots, \rho_{j_s,s}$ as a priority ordering of the minimal red nodes.

Recall that some rational $c(s + 1) \in (0,1)$ received a chip at this stage. Find the greatest $k_s \leq j_s$ such that

$$\sum_{i=0}^{k_s} 2^{-|\rho_{i,s}|} < c(s+1),$$

and for each of $\rho_{0,s}, \ldots, \rho_{k_s,s}$, declare all of its successors at level $l_s$ to be prioritized. (This means that they will all still be red at the end of this

23

stage, and therefore so will $\rho_{0,s}, \ldots, \rho_{k_s,s}$.) Let $\sigma_{0,s}, \ldots, \sigma_{m_s,s}$ be the finitely many nodes of length $l$ that were red at stage $s$ but are not prioritized.

Our intention is to introduce a green node above each of these non-prioritized nodes $\sigma_{i,s}$, so that they will no longer be red. Therefore, for each $\sigma_{i,s}$ in turn, we enumerate into $D_{s+1}$ the product $x_{i,s}$ of a set of prime numbers such that:

- whenever $\sigma_{i,s}(p) = 1$, then $p$ divides $x_{i,s}$; and

- whenever $\sigma_{i,s}(p) = 0$, then $p$ does not divide $x_{i,s}$; and

- $x_{i,s}$ has certain other prime factors $\notin \mathrm{dom}(\sigma)$, as defined below (after Lemma 6.10).

The point of the first two rules is that now $\sigma_{i,s}$ extends to some node that is colored green at stage $s+1$ (since $x_{i,s} \in D_{s+1}$). However, we must ensure that no prioritized node $\rho_{k,s}$ extends to a node that becomes green when $x_{i,s}$ enters $D$. To understand why this is not immediate, recall that if the number 35 enters $D$, so as to make the node 0011 turn green, then the nodes 1011, 0111, and 1111 will all also turn green, since they correspond to rings containing $\frac{1}{35}$. However, Lemma 6.10 shows that these now-accidentally-green nodes cannot have been prioritized.

**Lemma 6.10** *For each $i \leq m_s$ and each $k \leq k_s$, some prime $q$ has $\rho_{k,s}(q) = 0$ but $\sigma_{i,s}(q) = 1$, so that $\frac{1}{x_{i,s}} \notin \mathbb{Z}[\mathbb{P} - \rho_{k,s}^{-1}(0)]$.*

*Proof.* Let $\rho \subseteq \sigma_{i,s}$ be minimal such that $\rho$ is red at stage $s$ (so, by our definition of $\sigma_{i,s}$ above, $\rho = \rho_{j,s}$ for some $j > k_s$). We must have either $|\rho_{k,s}| < |\rho|$, or $\rho_{k,s} \prec \rho$. Now if $\rho_{k,s} \prec \rho$, then the least prime $q$ at which they differ has $\rho_{k,s}(q) = 0$ and $\rho(q) = 1$, forcing $\sigma_{i,s}(q) = 1$ since $\sigma_{i,s}$ restricts to $\rho$. But if $|\rho_{k,s}| < |\rho|$, then $\rho{\upharpoonright}|\rho_{k,s}|$ cannot be red as well, by the minimality of $\rho$, and so some $q \in \rho_{k,s}^{-1}(0)$ must have $\rho(q) = 1$, for otherwise $\rho{\upharpoonright}|\rho_{k,s}|$ would have been red (as any green successor of $\rho{\upharpoonright}|\rho_{k,s}|$ would have given rise to a green successor of $\rho_{k,s}$). ∎

By induction, we know that the measure $a_s$ of the set of all paths in $2^{\mathbb{P}}$ that include a green node at stage $s$ lies in $(u_s - \frac{1}{2^s}, u_s)$, and we wish to make $a_{s+1} \in (u_{s+1} - \frac{1}{2^{s+1}}, u_{s+1})$ as well. (Recall that $u_s < u_{s+1}$.) Now $a_s$ is precisely the measure of the set of nodes at level $l_s$ that are green at stage $s$. Meanwhile, the prioritized nodes at level $l_s$ have total measure $< c(s+1)$,

by our choice of $k_s$ above, and these should stay red at stage $s + 1$. We arranged beforehand that $u_{s+1} < 1 - c(s + 1)$, so that these requirements do not conflict. The remaining nodes at level $l_s$ are precisely $\sigma_{0,s}, \ldots, \sigma_{m_s,s}$. Above we stated that each of these will contribute some $x_{i,s}$ to $D_{s+1}$. By taking $x_{i,s}$ to have many prime factors $\notin \mathrm{dom}(\sigma_{i,s})$, we can make each $x_{i,s}$ contribute arbitrarily little measure to $a_{s+1}$, so it is not difficult to ensure that $a_{s+1} < u_{s+1}$. To make $a_{s+1} > u_{s+1} - \frac{1}{2^{s+1}}$, we add a larger amount of measure as needed, possibly enumerating several different numbers (but only finitely many) into $D_{s+1}$ instead of just a single $x_{i,s}$. For example, if $\sigma_{i,s} = 0011$ (with $l_s = 4$), then 5 and 7 must divide each $x_{i,s}$ and 2 and 3 must not; by enumerating both $5 \cdot 7 \cdot 11 \cdot 13$ and $5 \cdot 7 \cdot 11 \cdot 17 \cdot 19$ into $D_{s+1}$, we can make the two extensions 0011^11 and 0011^1011 turn green. (This would also make six other nodes, such as 1011^11, turn green, if they were not green already.) These first two nodes together have measure $\frac{5}{16} \cdot \frac{1}{2^{l_s}}$, which is five-sixteenths of the total measure available above 0011. How much else is added depends on whether 1011, 0111, and 1111 were already green or not, but it is clear that we can compute this, and that we could make any dyadic fraction of the total measure above the nodes $\sigma_{i,s}$ turn green. So it is easy to make $a_{s+1}$ sit in the desired interval $(u_{s+1} - \frac{1}{2^{s+1}}, u_{s+1})$, effectively, and this completes the construction.

With $a_s \in (u_s - \frac{1}{2^s}, u_s)$ for every $s$, it is clear that the resulting polynomial $f$ has $\mu(\mathcal{A}(f)) = \lim_s u_s = u$ as desired. We also claim that $\mu(\mathcal{C}(f)) = v$, which will complete the proof. In particular, whenever $q < v$, we can produce a subset of $\mathcal{C}(f)$ of measure $\geq q$; whereas when $v < q$, we will show that $\mu(\mathcal{C}(f)) < q$ as well.

First suppose $q < v$, and fix any rational $q' \in (q, v)$. Then there is some stage $s_0$ such that, for all $s \geq s_0$, we have $c(s) > q'$. Then at stage $s_0$, among the minimal red nodes $\rho_{0,s_0}, \ldots, \rho_{k_{s_0},s_0}$, the first $k$ (in this order) will in fact be this highest-priority minimal red nodes remaining at the end of the construction, where $k$ is maximal so that

$$\sum_{i=0}^{k} 2^{-|\rho_{i,s_0}|} < q'.$$

Now $\rho_{k+1,s_0}$ may or may not remain red forever after. If it does, then we have a set of red nodes of total measure $\geq q' > q$, as required; so assume that eventually a stage $s_1 > s_0$ is reached at which some node above this $\rho_{k+1,s_0}$ is colored green. Then at stage $s_1 + 1$, $\rho_{0,s_1+1}, \ldots, \rho_{k,s_1+1}$ will be the

25

same as at stage $s_0$, but $\rho_{k+1,s_1+1}$ will be different: either it will have greater length than $\rho_{k+1,s_0}$, or it will be $\succ \rho_{k+1,s_0}$. If it has the same length, then the same argument applies to this new $\rho_{k+1,s_1+1}$. Since there are only finitely many nodes at each level, we either reach a node at this level that stays red forever after, in which case again we have a set of red nodes of sufficiently large measure; or else $\rho_{k+1,s}$ will eventually have greater length than $\rho_{k+1,s_0}$. This argument then continues until we reach a stage $s$ at which

$$2^{-|\rho_{k+1,s}|} < q' - \sum_{i=0}^{k} 2^{-|\rho_{i,s_0}|},$$

at which point this new $\rho_{k+1,s}$ will remain red forever. The measure of the red set will become arbitrarily close to $q'$ via this process, and hence must eventually be $> q$. (With $q' < v$, it will eventually become $> q'$ as well, but this is irrelevant.) To see why it must become arbitrarily close to $q'$, notice that with $1 - u_s > c(s) > q'$ at all subsequent stages, there will always be a supply of red nodes of measure $> q'$, and the remainder of this measure will be partitioned into smaller and smaller chunks as the length of the next minimal red node keeps increasing, so that the measure of the permanently-minimal-red nodes cannot stay below $q'$ by any positive margin forever.

It remains to show that when $v < q$, we have $\mu(\mathcal{C}(f)) < q$ as well. Again it is useful to fix some $q'$ between $q$ and $v$, now with $v < q' < q$. Now there are infinitely many stages $s$ with $c(s) < q'$. If the measure of $\mathcal{C}(f)$ were $> q'$, then evetually there would be a finite set of minimal red nodes, of total measure $> q'$, all of which stayed red (and hence minimal) forever after. But at some subsequent stage $s$ we would have $c(s) < q'$, and at that stage the lowest-priority node in this finite set would acquire a green node above it, so would not in fact have been permanently red. With this contradiction, the proof is complete. ∎

The remarks at the conclusion of Theorem 6.7 can be applied and expanded here. The first claim in this corollary follows from Theorem 6.7; the second from Theorem 6.9.

**Corollary 6.11** *If the solution class $\mathcal{A}(f)$ of every polynomial $f \in \mathbb{Z}[\vec{X}]$ has computable measure, then there is no existential definition of $\mathbb{Z}$ in $\mathbb{Q}$. Likewise, if the boundary class $\mathcal{B}(f)$ of every polynomial $f \in \mathbb{Z}[\vec{X}]$ has $\emptyset'$-computable measure, then there is no existential definition of $\mathbb{Z}$ in $\mathbb{Q}$.* ∎

The following, while only a partial converse, serves to emphasize the importance of the measures of boundary sets.

**Corollary 6.12** *If there exists a polynomial $f$ for which the measure $\beta(f)$ of $\mathcal{B}(f)$ is not $\emptyset'$-computable – or simply fails to be approximable from above – then $HTP(\mathbb{Q})$ is undecidable.*

*Proof.* If $HTP(\mathbb{Q})$ is decidable, then the measures of both $\mathcal{A}(f)$ and $\mathcal{C}(f)$ are approximable from below, and therefore $\beta(f) = 1 - \alpha(f) - \gamma(f)$ is approximable from above. ∎

**Corollary 6.13** *Suppose that, for every polynomial $f \in \mathbb{Z}[X_0, X_1, \ldots]$, the set $\mathcal{C}(f)$ is an effective union of basic open sets in $2^{\mathbb{P}}$. (That is, suppose the red nodes in $2^{\mathbb{P}}$ for $f$ always form a computably enumerable set.) Then there is no existential definition of $\mathbb{Z}$ in $\mathbb{Q}$.*

In particular, this corollary applies if, for each single $f$, the set of minimal red nodes for $f$ is a finite set. The corollary would not require any method of determining the finite set uniformly from the polynomial. As of this writing, it is unknown whether there exists an $f$ for which the set of minimal red nodes is infinite (let alone not computably enumerable).

*Proof.* An effective union of basic open sets has as its measure a real number approximable from below, and here this measure is $\gamma(f)$. Since $\alpha(f)$ is always approximable from below, $\beta(f) = 1 - \alpha(f) - \gamma(f)$ would always be approximable from above, hence $\emptyset'$-computable, and we would then apply Theorem 6.9. ∎

# 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. *Transactions of the American Mathematical Society*, 369(11): 8291–8315, 2017.

[3] Richard M. Friedberg. A criterion for completeness of degrees of unsolvability. *Journal of Symbolic Logic*, 22: 159–160, 1957.

[4] Carl G. Jockusch, Jr. Degrees of generic sets. *Recursion theory: its generalisation and applications (Proc. Logic Colloq., Univ. Leeds, Leeds, 1979)*, London Mathematical Society Lecture Note Series 45: 110–139, 1981.

[5] Carl G. Jockusch, Jr. and Richard A. Shore. Pseudo jump operators I: the r.e. case. *Transactions of the AMS*, 275(2): 599–609, 1983.

[6] Carl G. Jockusch, Jr. and Richard A. Shore. Pseudo-jump operators II: transfinite iterations, hierarchies, and minimal covers. *Journal of Symbolic Logic*, 49: 1205–1236, 1984.

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

[8] Kenneth Kramer and Russell Miller. The Hilbert's-Tenth-Problem Operator. *Israel Journal of Mathematics*, 230(2): 693–713, 2019.

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

[10] Yuri V. Matiyasevich. The Diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR*, 191: 279–282, 1970.

[11] Russell Miller. Computable fields and Galois theory. Notices of the American Mathematical Society, 55(7): 798–807, 2008.

[12] 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, Springer LNCS 9709: 343–352, 2016.

[13] Russell Miller. Measure theory and Hilbert's Tenth Problem inside $\mathbb{Q}$, in *Sets and Computations*, eds. S.D. Friedman, D. Raghavan, & Y. Yang, Institute for Mathematical Sciences, National University of Singapore, Lecture Note Series 33: 253–269, 2017.

[14] 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.

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

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

[17] Hartley Rogers. *Theory of Recursive Functions and Effective Computability*. McGraw-Hill, New York, 1967.

[18] Jean-Pierre Serre. *A Course in Arithmetic*. Graduate Texts in Mathematics, vol. 7 (Berlin: Springer, 1973).

[19] Alexandra Shlapentokh. *Hilbert's Tenth Problem: Diophantine Classes and Extensions to Global Fields*. Cambridge U.P., Cambridge, UK, 2007.

[20] Robert I. Soare. *Recursively Enumerable Sets and Degrees*. Perspectives in Mathematical Logic. Springer-Verlag, Berlin, 1987.

Department of Mathematics
Queens College – C.U.N.Y.
65-30 Kissena Blvd.
Queens, New York 11367 U.S.A.

PhD 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