TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 369, Number 11, November 2017, Pages 8291–8315
http://dx.doi.org/10.1090/tran/7075
Article electronically published on June 13, 2017

AS EASY AS $\mathbb{Q}$: HILBERT'S TENTH PROBLEM FOR SUBRINGS OF THE RATIONALS AND NUMBER FIELDS

KIRSTEN EISENTRÄGER, RUSSELL MILLER, JENNIFER PARK, AND ALEXANDRA SHLAPENTOKH

Abstract. Hilbert's Tenth Problem over the rationals is one of the biggest open problems in the area of undecidability in number theory. In this paper we construct new, computably presentable subrings $R \subseteq \mathbb{Q}$ having the property that Hilbert's Tenth Problem for R, denoted $\mathrm{HTP}(R)$, is Turing equivalent to $\mathrm{HTP}(\mathbb{Q})$.

We are able to put several additional constraints on the rings R that we construct. Given any computable nonnegative real number $r \leq 1$ we construct such rings $R = \mathbb{Z}[\mathcal{S}^{-1}]$ with $\mathcal{S}$ a set of primes of lower density r. We also construct examples of rings R for which deciding membership in R is Turing equivalent to deciding $\mathrm{HTP}(R)$ and also equivalent to deciding $\mathrm{HTP}(\mathbb{Q})$. Alternatively, we can make $\mathrm{HTP}(R)$ have arbitrary computably enumerable degree above $\mathrm{HTP}(\mathbb{Q})$. Finally, we show that the same can be done for subrings of number fields and their prime ideals.

1. Introduction

Hilbert's Tenth Problem asks to find an algorithm that takes as input any polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$ and decides whether $f = 0$ has a solution in $\mathbb{Z}^n$. In 1969, Matiyasevich [Mat70], using work by Davis, Putnam and Robinson [DPR61], proved that no such algorithm exists. One can also ask the same question for polynomial equations with coefficients and solutions in other *computably presentable* rings R (see Definition 2.2). We call this *Hilbert's Tenth Problem over R*. For any such ring R, fixing an effective enumeration $\{f_e\}_{e \in \mathbb{Z}_{>0}}$ of the polynomials with coefficients in R once and for all, Hilbert's Tenth Problem over R is equivalent to asking whether the set

$$\mathrm{HTP}(R) := \{e \in \mathbb{Z}_{>0} : f_e(\vec{x}) = 0 \text{ has a solution in } R\}$$

is decidable in $\mathbb{Z}_{>0}$, and hence in $\mathbb{Z}$, since $\mathbb{Z}_{>0}$ is decidable in $\mathbb{Z}$. Thus, for the rest of the paper, we use $\mathrm{HTP}(R)$ to denote both Hilbert's Tenth Problem over R and also a subset of $\mathbb{Z}_{>0}$. As yet, the answer for $\mathrm{HTP}(\mathbb{Q})$ is unknown.

Remark 1.1. By an effective enumeration of polynomials we mean an enumeration which allows us effectively to retrieve the degree and the coefficients of a polynomial

Received by the editors February 9, 2016 and, in revised form, August 28, 2016 and September 22, 2016.

2010 *Mathematics Subject Classification.* Primary 11U05; Secondary 12L05, 03D45.

The first author was partially supported by NSF grant DMS-1056703.

The second author was partially supported by NSF grants DMS-1001306 and DMS-1362206 and by several PSC-CUNY Research Awards.

The third author was partially supported by NSF grant DMS-1069236 and by an NSERC PDF grant.

The fourth author was partially supported by NSF grant DMS-1161456.

from its sequence number and conversely to get the sequence number effectively from the degree and coefficients. It is not hard to show that the decidability of $\mathrm{HTP}(R)$ does not depend on the choice of the effective enumeration.

Two key notions for relating $\mathrm{HTP}(R)$ for some ring R to $\mathrm{HTP}(\mathbb{Z})$ are the notions of a diophantine set and a diophantine model.

Definition 1.2. Let R be a commutative ring. Suppose $A \subseteq R^k$ for some $k \in \mathbb{N}$. Then A is *diophantine over* R if there exists a polynomial f in $k+n$ variables with coefficients in R such that

$$A = \{\mathbf{t} \in R^k : \exists\, x_1, \ldots, x_n \in R,\ f(\mathbf{t}, x_1, \ldots, x_n) = 0\}.$$

Definition 1.3. A *diophantine model of* $\mathbb{Z}$ *over a ring* R is a subset $A \subseteq R^k$ (for some $k > 0$) that is diophantine over R, together with a bijection $\varphi : \mathbb{Z} \to A$, under which the graphs of addition and multiplication (which are subsets of $\mathbb{Z}^3$) correspond to subsets of $A^3 \subseteq R^{3k}$ under φ that are diophantine over R.

If $\mathbb{Z}$ admits a diophantine definition over R or, more generally, if there is a diophantine model of the ring $\mathbb{Z}$ over R, then the undecidability of $\mathrm{HTP}(R)$ can be deduced from that of $\mathrm{HTP}(\mathbb{Z})$. However, Mazur [Maz92] conjectured that if X is a variety over $\mathbb{Q}$, then the topological closure of $X(\mathbb{Q})$ in $X(\mathbb{R})$ has finitely many components. This implies (see [CZ00]) that $\mathbb{Z}$ is not diophantine over $\mathbb{Q}$ and that there is no diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$. Nonetheless, Koenigsmann [Koe16] obtains a first-order definition of $\mathbb{Z}$ over $\mathbb{Q}$, using only universal quantifiers.

Pheidas, following ideas of Denef ([Den80]), introduced a new line of ideas for trying to determine the status of $\mathrm{HTP}(\mathbb{Q})$ via a relaxed notion of diophantine model called *diophantine interpretation*. He showed that $\mathrm{HTP}(\mathbb{F}_q(t))$ is undecidable for any odd prime power q (see [Phe87i] and [Phe87ii]). This result was further generalized to $\mathrm{HTP}(K)$, where K is any function field of positive characteristic not containing the algebraic closure of a finite field or a function field of a variety of transcendence degree at least 2. In fact in all cases it was shown that $\mathrm{HTP}(K)$ is equivalent to the Halting Problem discussed below in section 2. For further details the reader is referred to [Phe91], [Vid94], [Eis03], [ES16], and [Eis12].

Yet another idea led to an exploration of the rings between $\mathbb{Z}$ and $\mathbb{Q}$ to see if any of them admit a diophantine definition or a diophantine model of the integers. Subrings of $\mathbb{Q}$ are in bijection with subsets $\mathcal{S}$ of the set $\mathcal{P}$ of the prime numbers; one associates to $\mathcal{S}$ the ring $\mathbb{Z}[\mathcal{S}^{-1}]$. If $\mathcal{S}$ is finite, one can obtain a diophantine definition of $\mathbb{Z}$ over rings $\mathbb{Z}[\mathcal{S}^{-1}]$ from [Rob49], and hence $\mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}])$ is undecidable. From the same work of Robinson [Rob49], it also follows that if $\mathcal{P} - \mathcal{S}$ is finite, then $\mathbb{Z}[\mathcal{S}^{-1}]$ is diophantine over $\mathbb{Q}$. Therefore, for such $\mathcal{S}$, $\mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}])$ is decidable if and only if $\mathrm{HTP}(\mathbb{Q})$ is decidable. When $\mathcal{S}$ is both infinite and co-infinite (i.e. $\mathcal{P} - \mathcal{S}$ is infinite) we have the following result by Poonen.

Theorem ([Poo03])**.** *There exist computable sets* $\mathcal{S}$ *that are both infinite and co-infinite, of natural density zero and of natural density one, such that* $\mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}])$ *is undecidable.*

This remarkable paper was followed by generalizations in [ES09], [Per11], and [EES11]. However, no attempt has been made so far to compare $\mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}])$ to $\mathrm{HTP}(\mathbb{Q})$. As it is still unknown whether $\mathrm{HTP}(\mathbb{Q})$ is decidable or not, one could try to compare $\mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}])$ for different $\mathcal{S}$ using the notion of Turing reducibility.

Definition 1.4. Given a set $B \subseteq R$, an *oracle for* B takes as input an element of R and outputs YES or NO, depending on whether the element belongs to B. For $A, B \subseteq R$, A is *Turing reducible to* B (written $A \leq_T B$) if there is an algorithm that determines membership in A using an oracle for B. We say that A *is Turing equivalent to* B ($A \equiv_T B$) if $A \leq_T B$ and $B \leq_T A$. The set of equivalence classes under $\equiv_T$ are called *Turing degrees*. (The notion of an oracle is also discussed in section 2.)

The first result of this paper concerns the subrings R of $\mathbb{Q}$ for which $\mathrm{HTP}(R) \equiv_T \mathrm{HTP}(\mathbb{Q})$.

Theorem (Theorem 3.17)**.** *For every computable real number* $0 \leq r \leq 1$*, there exists a computably enumerable set* $\mathcal{S}$ *of primes such that* $\mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}]) \equiv_T \mathrm{HTP}(\mathbb{Q})$ *and* $\mathcal{S}$ *has lower density* r*.*

We have imposed the condition that $\mathcal{S}$ is *computably enumerable* because of the following reason: since Hilbert's Tenth Problem is primarily concerned with algorithms for rings, we want to consider rings in which addition and multiplication are computable, called computably presentable rings (see section 2 for a precise definition).

For $\mathcal{S} \subset \mathcal{P}$, if the ring $R = \mathbb{Z}[\mathcal{S}^{-1}]$ is computably presentable, then there is an algorithm such that, when left running forever, prints out exactly $\mathcal{S}$ by listing all the primes appearing in the denominator of the elements of R. In this case, $\mathcal{S}$ is said to be computably enumerable (see section 2 for a precise definition). Conversely, if $\mathcal{S}$ is computably enumerable, then R is computably presentable.

Matiyasevich, building on the work of Davis, Putnam, and Robinson [DPR61], showed that every computably enumerable subset of the integers is diophantine. This implies that $\mathrm{HTP}(\mathbb{Z})$ is Turing equivalent to the halting set. Since there are infinitely many different Turing degrees of undecidable computably enumerable sets (constructed by [Fri57] and [Muc56], who independently invented the priority method), this is much stronger than showing that Hilbert's Tenth Problem over $\mathbb{Z}$ is undecidable.

To our knowledge, all attempts so far to prove undecidability for $\mathrm{HTP}(\mathbb{Q})$ try to prove that $\mathrm{HTP}(\mathbb{Q}) \equiv_T \mathrm{HTP}(\mathbb{Z})$. However, it is possible that $\mathrm{HTP}(\mathbb{Q}) <_T \mathrm{HTP}(\mathbb{Z})$ while $\mathrm{HTP}(\mathbb{Q})$ is undecidable. One could argue that the results of this paper do not point in this direction.

In section 3.1, we construct an infinite and co-infinite set $\mathcal{S}$ with $\mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}]) \equiv_T \mathrm{HTP}(\mathbb{Q})$. Then in section 3.2, we modify these constructions to make $\mathcal{S}$ infinite, co-infinite, and computably enumerable, thus making $\mathbb{Z}[\mathcal{S}^{-1}]$ computably presentable; this process is more technical, using priority constructions from computability theory. We hope that the initial proofs will afford the reader some insight before encountering the details necessary to ensure computable enumerability of $\mathcal{S}$. We also get an infinite sequence of nested rings $R_i := \mathbb{Z}[\mathcal{S}_i^{-1}]$ satisfying $\mathrm{HTP}(R_i) \equiv_T \mathrm{HTP}(\mathbb{Q})$ and for which the relative upper density of $\mathcal{S}_{i-1} - \mathcal{S}_i$ is 1 for all $i > 0$ (see Corollary 3.16).

The next theorem produces examples of a different flavor. Let $\mathcal{S}$ be a computably enumerable set of primes and let $R = \mathbb{Z}[\mathcal{S}^{-1}]$. We trivially have $\mathrm{HTP}(R) \geq_T R$, but it is possible to get $\mathrm{HTP}(R) \equiv_T R$, while also choosing $\mathcal{S}$ such that $\mathrm{HTP}(R) \equiv_T \mathrm{HTP}(\mathbb{Q})$.

Theorem (Special case of Theorem 4.1)**.** *There exists a computably presentable ring $R = \mathbb{Z}[\mathcal{S}^{-1}]$, with $\mathcal{S}$ a computably enumerable subset of the prime numbers of lower density 0, such that $R \equiv_T \mathrm{HTP}(R) \equiv_T \mathrm{HTP}(\mathbb{Q})$.*

The general version of Theorem 4.1 shows that many of the preceding arguments can in fact produce computably presentable subrings $R \subseteq \mathbb{Q}$ for which $\mathrm{HTP}(R)$ is Turing-equivalent to an arbitrary c.e. set S, provided only that $S \geq_T \mathrm{HTP}(\mathbb{Q})$.

Finally we have the complementary ring versions as in [ES09] and [EES11].

Theorem (Theorem 3.18)**.** *For any positive integer m, the set of all rational primes $\mathcal{P}$ can be represented as a union of pairwise disjoint sets $\mathcal{S}_1 \ldots, \mathcal{S}_m$, each of upper density 1 and such that for all i we have that $\mathrm{HTP}(\mathbb{Z}[\mathcal{S}_i^{-1}]) \leq_T \mathrm{HTP}(\mathbb{Q})$ and $\mathcal{S}_i \leq_T \mathrm{HTP}(\mathbb{Q})$.*

Theorem (Corollary 3.19)**.** *There are infinitely many subsets $\mathcal{S}_0, \mathcal{S}_1, \ldots$ of the set $\mathcal{P}$ of primes, all of lower density 0, all computable uniformly from an $\mathrm{HTP}(\mathbb{Q})$-oracle (so that the rings $R_j = \mathbb{Z}[\mathcal{S}_j^{-1}]$ are also uniformly computable below $\mathrm{HTP}(\mathbb{Q})$), with $\bigcup_j \mathcal{S}_j = \mathcal{P}$ and $\mathcal{S}_i \cap \mathcal{S}_j = \emptyset$ for all $i < j$, and such that $\mathrm{HTP}(\mathbb{Z}_{\mathcal{S}_j}) \equiv_T \mathrm{HTP}(\mathbb{Q})$ for every j.*

All of the above results generalize to **all** number fields, which is very different from the theorems that deal with diophantine models of $\mathbb{Z}$. There, the unconditional results apply only to number fields with extra properties, such as the existence of an elliptic curve defined over $\mathbb{Q}$ and of rank one over $\mathbb{Q}$ and over the number field in question. We discuss the number field situation in detail in section 6.

2. Some facts from computability theory

In this section we collect the definitions and facts from computability theory used in this paper. We start with the most fundamental notions.

Definition 2.1. A subset T of $\mathbb{Z}$ is *computable* (or *recursive* or *decidable*) if there exists an algorithm (formally, a Turing machine; informally, a computer program) that takes as input any integer t and, within finitely many steps, outputs YES or NO according to whether $t \in T$. The set T is *computably enumerable* (or *c.e.*, also known as *recursively enumerable*) if it can be listed algorithmically: some program, running forever, outputs all the elements of T (and nothing else), although not necessarily in increasing order. It is well known that there exist c.e. sets that are not computable.

Next we define the rings that are the focus of this paper.

Definition 2.2. An infinite ring R is *computably presentable* if there is a bijection $R \to \mathbb{Z}_{>0}$ such that the addition and multiplication in R correspond to computable functions $\mathbb{Z}_{>0} \times \mathbb{Z}_{>0} \to \mathbb{Z}_{>0}$ under this bijection. The isomorphic copy of R with domain $\mathbb{Z}_{>0}$ is said to be a *computable presentation* of R. We extend this definition by allowing a finite subset of $\mathbb{Z}_{>0}$ in place of $\mathbb{Z}_{>0}$ itself, so that every finite ring is computably presentable.

Below we will often use the notion of an oracle. We give an informal description of this concept below. For a rigorous definition we refer the reader to [Rog67]. Given a set $B \subseteq \mathbb{Z}$, we sometimes treat B as an *oracle* for a computation of a

function f. This means that the computation follows a program, but the program is allowed to use a subroutine which takes an input n and returns the value of the characteristic function $\chi_B(n)$. The oracle set B itself may not be computable; this is simply a method of saying that if we could compute B, then we would be able to compute f. Such a function is said to be *B-computable*. A set C is B-computable (or *Turing-reducible to* B, written $C \leq_T B$) if χ_C is B-computable.

For $\mathcal{S} \subseteq \mathcal{P}$, $R = \mathbb{Z}[\mathcal{S}^{-1}]$ being computable presentable is equivalent to $\mathcal{S}$ being computably enumerable, and it is also equivalent to $\mathrm{HTP}(R)$ being computably enumerable. Here we consider $\mathrm{HTP}(R)$ as a subset of the positive integers as discussed above: i.e. we fix a computable enumeration of all polynomials (in any number of variables) with integer coefficients and let $\mathrm{HTP}(R)$ be the set of indices corresponding to the polynomials with a root in R^k for the appropriate k. Assuming our enumeration of polynomials is computable or effective, as described above, as a matter of convenience, we can view $\mathrm{HTP}(R)$ as a set of polynomials, writing "$f_e \in \mathrm{HTP}(R)$" in place of "$e \in \mathrm{HTP}(R)$". (An elementary but useful introduction to computable rings and fields appears in [Mil08].)

There are countably many programs (or algorithms) and they can be listed effectively, i.e., there is an algorithm which, given $n \in \mathbb{Z}_{>0}$, determines the corresponding program. Fix such an enumeration. The *Halting Problem* is the c.e. set of pairs (m, n) such that the mth program terminates on input n. Classical computability theory shows that every c.e. set is Turing reducible to the Halting Problem, and also that the Halting Problem is not computable. As we have mentioned already, there are infinitely many Turing degrees of computably enumerable sets that are undecidable, but not Turing equivalent to the Halting Problem. An oracle for the Halting Problem can decide membership in each of these sets but not vice versa.

3. Examples of rings R with $\mathrm{HTP}(R) \equiv_T \mathrm{HTP}(\mathbb{Q})$

3.1. **Constructing rings with an $\mathrm{HTP}(\mathbb{Q})$-oracle.** In this section we first present a simpler version of the construction given in section 3.2. While it illustrates the role of definability of integrality at a prime in the construction, the ring R produced by this simple version is not necessarily computably presentable. It is computable only relative to the oracle for $\mathrm{HTP}(\mathbb{Q})$, and here $\mathrm{HTP}(R)$ is as defined in section 1.

Proposition 3.1. *There is a subring $R = \mathbb{Z}[\mathcal{S}^{-1}] \subseteq \mathbb{Q}$ with $\mathrm{HTP}(R) \equiv_T \mathrm{HTP}(\mathbb{Q})$, where $\mathcal{S} \leq_T \mathrm{HTP}(\mathbb{Q})$, and $\mathcal{S}$ is co-infinite as a subset of the primes.*

For co-finite sets $\mathcal{S}$, $\mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}])$ is always Turing-equivalent to $\mathrm{HTP}(\mathbb{Q})$. This fact is integral to our arguments in Proposition 3.1, and we present it as Corollary 5.6 below, deferring its rather technical proof until then. (It is completely independent of Proposition 3.1 and the subsequent results in section 3 and section 4.)

Proof. Fix a computable enumeration $\langle f_e \rangle_{e \in \mathbb{N}}$ of $\mathbb{Z}[X_1, X_2, \ldots]$. Let $\mathcal{S}_0 = \emptyset$ and $\mathcal{U}_0 = \emptyset$. We proceed in stages; the nth stage determines the finite sets $\mathcal{S}_n$ and $\mathcal{U}_n$.

Assume we have just completed stage $n \geq 0$. Now consider the polynomial equation $f_n(\mathbf{X}) = 0$ and use the $\mathrm{HTP}(\mathbb{Q})$-oracle together with Corollary 5.6 to determine whether this polynomial equation has solutions in $\mathbb{Z}[\mathcal{P} - \mathcal{U}_n]$. This is possible by Proposition 5.4 below. If the answer is "no," then f_n is put on the list of polynomials without solutions in our ring. If the answer is "yes," then we add

f_n to the list of polynomials with solutions in our ring and search for a solution integral at primes in $\mathcal{U}_n$. Once we locate the solution, we add all the primes which appear in the denominators of this solution to $\mathcal{S}_n$ to form $\mathcal{S}_{n+1}$. Finally, we set $\mathcal{U}_{n+1} = \mathcal{U}_n \cup \{p\}$, where p is the least prime not in $\mathcal{U}_n \cup \mathcal{S}_{n+1}$. This completes stage $n+1$, with $\mathcal{U}_{n+1} \cap \mathcal{S}_{n+1} = \emptyset$. We let $\mathcal{S} = \bigcup_{n=0}^{\infty} \mathcal{S}_n$ and $\mathcal{U} = \bigcup_{n=0}^{\infty} \mathcal{U}_n$.

To determine whether the nth prime p_n is inverted in our ring, we just need to follow the construction until at most the $(n+1)$-st stage, since (by induction on n) p_n must lie in $\mathcal{S}_{n+1} \cup \mathcal{U}_{n+1}$. (Here we regard 2 as p_0.) At the same time, to determine whether a given polynomial has solutions in our ring, all we need to do is again wait for the stage of the construction where this polynomial was processed. Thus, we have $\mathcal{S} \leq_T \mathrm{HTP}(\mathbb{Q})$ and $\mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}]) \leq_T \mathrm{HTP}(\mathbb{Q})$. Finally, $\mathcal{U}$ must be infinite, since each $\mathcal{U}_n$ contains n primes, and $\mathcal{U} = \mathcal{P} - \mathcal{S}$, since the nth prime lies in the (disjoint) union $\mathcal{S}_{n+1} \cup \mathcal{U}_{n+1}$. Thus $\mathcal{S}$ is co-infinite. □

Remark 3.2. In the previous proof, it is possible to ensure that $\mathcal{S}$ is infinite as well as co-infinite by adding a prime to $\mathcal{S}_{n+1}$ each time a prime is added to $\mathcal{U}_{n+1}$. If the process in the proof happened to build a finite $\mathcal{S}$, then we have a stronger statement: in this case, $\mathrm{HTP}(\mathbb{Q})$ would have to compute $\mathrm{HTP}(\mathbb{Z})$, since $\mathrm{HTP}(\mathbb{Z}) \equiv_T \mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}])$ for all finite $\mathcal{S}$.

Even though $\mathrm{HTP}(\mathbb{Q})$ is c.e. and the set $\mathcal{S}$ in Proposition 3.1 is enumerated using only an $\mathrm{HTP}(\mathbb{Q})$-oracle, $\mathcal{S}$ itself need not be c.e. The process of enumerating $\mathcal{S}$ required asking membership questions about $\mathrm{HTP}(\mathbb{Q})$, and the computable enumeration of $\mathrm{HTP}(\mathbb{Q})$ is not sufficient to answer such questions. Therefore, the subring R built here need not be computably presentable. (Of course, if $\mathrm{HTP}(\mathbb{Q})$ should turn out to be decidable, then the procedure in the proposition would indeed enumerate $\mathcal{S}$ computably.)

3.2. **Constructing computably presentable rings with a priority argument.** From now on, we let $\mathcal{P}$ denote the set of all rational primes, let $\mathcal{W} = \{q_1, q_2, q_3, \ldots\} \subseteq \mathcal{P}$ be an infinite c.e. set of primes, written in order of enumeration (not necessarily in increasing order), and let $\mathcal{W}_s = \{q_1, \ldots, q_s\}$. Further, let $\mathcal{R} \subseteq \mathcal{P} - \mathcal{W}$ be any computable set. Let $\mathcal{M} = \mathcal{W} \cup \mathcal{R}$. Observe that $\mathcal{M}$ is still c.e. The reader is encouraged to assume that $\mathcal{R} = \emptyset$ (and therefore $\mathcal{M} = \mathcal{W}$) for the first reading. In Theorem 3.17 and Theorem 4.1 we will use a nonempty $\mathcal{R}$.

We construct a computably presentable ring R of the form $\mathbb{Z}[\mathcal{S}^{-1}]$ satisfying $\mathrm{HTP}(R) \equiv_T \mathrm{HTP}(\mathbb{Z}[\mathcal{M}^{-1}])$, with $\mathcal{W} \cup \mathcal{R} = \mathcal{M}$ and with $\mathcal{S}$ being a computably enumerable infinite and co-infinite set in $\mathcal{M}$. (In Theorem 3.17, we will have $\mathcal{R} \subset \mathcal{S}$, but in Theorem 4.1 only a proper subset of $\mathcal{R}$ will be in $\mathcal{S}$ to be inverted.) In particular, if $\mathcal{W} = \mathcal{P}$ and $\mathcal{R} = \emptyset$, then we get a computably presentable ring R such that $\mathrm{HTP}(R) \equiv_T \mathrm{HTP}(\mathbb{Q})$. We remind the reader that the preceding section did not accomplish this, since the ring R constructed there required the use of an $\mathrm{HTP}(\mathbb{Q})$-oracle in its construction. In contrast, the ring R that we build here is entirely defined by an effective algorithm, with no oracle required; this makes it a computably presentable ring as defined in the introduction.

The rings of the form $\mathbb{Z}[\mathcal{S}^{-1}]$ with $\mathcal{S} \subseteq \mathcal{P}$ computably enumerable (but not necessarily co-infinite) are precisely the computably presentable subrings of $\mathbb{Q}$ (which are not necessarily computable but necessarily c.e.). We let

$$\mathtt{E} := \{(f, \vec{x}, j) : \exists n \geq 0 \text{ such that } f \in \mathbb{Z}[X_1, \ldots, X_n], \vec{x} \in (\mathbb{Z}[\mathcal{M}^{-1}])^n, j \in \mathbb{Z}_{>0}\},$$

and we let $g\colon \mathbb{Z}_{>0} \to \mathtt{E}$ be a computable bijection. We do not actually make explicit use of the last coordinate j; its role is to ensure that the pair $(f, \vec{x})$ appears in the sequence infinitely often.

3.2.1. *The construction of the set $\mathcal{S}$.* Let $\{f_e\}_{e\in\mathbb{Z}_{>0}}$ be an enumeration of all polynomials $f \in \mathbb{Z}[X_1, \ldots]$. For each $e \geq 0$, we introduce a boolean variable $\mathtt{R}_e$, to be updated depending on whether $f_e \in \mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}])$ in the course of the construction. At the beginning of the construction, $\mathtt{R}_e$ is set to FALSE for all $e > 0$, and $\mathtt{R}_0$ is set to TRUE at the beginning of the construction. In our construction, at each step s, we will define sets $\mathcal{S}_s$ and $\mathcal{V}_s$; at the end of the construction, we will define $\mathcal{S} = \bigcup_s \mathcal{S}_s$. Let $h : \mathbb{Z}_{\geq 0} \to \mathbb{Z}_{\geq 0}$ be a computable function satisfying $h(0) = 0$ and several other conditions to be specified later.

- At stage $s = 0$: let $\mathcal{S}_0 = \emptyset, \mathcal{V}_0 = \emptyset$, $\mathtt{R}_0$ =TRUE.
- At stage $s > 0$: Let $e, \vec{x}, j$ be such that $g(s) = (f_e, \vec{x}, j)$. Here f_e is the eth polynomial in the enumeration $\{f_1, f_2, \ldots\}$ defined above. Let $\mathcal{V}_s$ be the set of the first $h(s)$ elements in the enumeration of $(\mathcal{W} - \mathcal{S}_{s-1})$, obtained from the given enumeration of $\mathcal{W}$ by removing elements of $\mathcal{S}_{s-1}$. Since $\mathcal{R} \cap \mathcal{W} = \emptyset$, we also have $\mathcal{R} \cap \mathcal{V}_s = \emptyset$.
  (1) If $\mathtt{R_e}$ = FALSE, $\vec{x} \in \mathbb{Z}[(\mathcal{M} - \mathcal{V}_s)^{-1}]^n$ and $f_e(\vec{x}) = 0$, then let $\mathcal{S}_s := \mathcal{S}_{s-1} \cup \mathcal{T}_s$, where $\mathcal{T}_s$ is the set of primes used in the denominators in $\vec{x}$. Notice that $\mathcal{S}_s \cap \mathcal{V}_s = \emptyset$, since none of these primes lies in $\mathcal{V}_s$. Here, we set $\mathtt{R_e}$ = TRUE. (Remark 3.3(2) explains why this step is effective.)
  (2) Otherwise, let $\mathcal{S}_s := \mathcal{S}_{s-1}$.
- In the end, let $\mathcal{S} := \bigcup_{s=1}^{\infty} \mathcal{S}_s$ and $R = \mathbb{Z}[\mathcal{S}^{-1}]$. Since this construction is entirely effective, $\mathcal{S}$ is computably enumerable, and so R is computably presentable.

Remark 3.3.

(1) Every element of $\mathcal{R}$ must belong to $\mathcal{S}$, as $\mathcal{V}_s$ never stops elements of $\mathcal{R}$ from being added to $\mathcal{S}$. For each $p \in \mathcal{R}$, at the stage s with $g(s) = (px - 1, \frac{1}{p}, 1)$, we will be in case (1) of the above construction, and so p will be added to the set $\mathcal{S}$ of primes to be inverted if p was not already inverted.
(2) Check whether $\vec{x} \in \mathbb{Z}[(\mathcal{M} - \mathcal{V}_s)^{-1}]^n$ is an algorithmic operation since we are given that $\vec{x} \in \mathbb{Z}[\mathcal{M}^{-1}]^n$. Thus we just need to check that none of the finitely many primes of $\mathcal{V}_s$ occur in the denominator of $\vec{x}$.

Definition 3.4. Let $s_0 = 0$. For each $e \geq 1$, we define s_e to be the smallest positive integer strictly bigger than s_{e-1} such that all of the eventually true variables among $\mathtt{R}_1, \ldots, \mathtt{R}_{e-1}$ have been set to TRUE by stage s_e of the above construction and such that $g(s_e) = (f_e, \vec{x}, j)$.

The stage s_e must exist, since only finitely many $\mathtt{R}_i$ are considered to define it. Computing s_e requires an oracle, as we will see in Theorem 3.9. In the following sections, we will show that $\mathrm{HTP}(\mathbb{Z}[\mathcal{M}^{-1}]) \geq_T \mathrm{HTP}(R)$, given that the function h satisfies the following conditions:

(3.1) $h(s_e) \to \infty$ as $e \to \infty$.

(3.2) $h(s_e) \leq h(s')$ when $s' > s_e$ satisfies
$$g(s') = (f_{e'}, \vec{x}, j) \text{ for some } \vec{x},\ j, \text{ and } e' > e.$$

(3.3) $h(s) = h(s_e)$ whenever $g(s) = (f_e, \vec{x}, j)$ for some $e, \vec{x}, j$ with $s \geq s_e$.

Remark 3.5. Our definition of the stages s_e and condition (2) imply that $h(s_{e-1}) \leq h(s_e)$, since $s_{e-1} < s_e$ and $g(s_{e-1}) = (f_{e-1}, \vec{x}, j)$ and $g(s_e) = (f_e, \vec{x}', j')$ for an appropriate $\vec{x}, \vec{x}', j, j'$.

For example, the function h given by $h(s) = e$ (where $g(s) = (f_e, \vec{x}, j)$) clearly satisfies this set of conditions (since $h(s) = h(s_e) = e$ for any stage s at which $g(s) = (f_e, \vec{x}, j)$). It may make it easier to understand the paper to assume this for now, and also that $\mathcal{W} = \mathcal{P}$. In Corollary 3.10 we will use the function $h(s) = e$. However, later on in section 3.3, we will make other choices of h and $\mathcal{W}$ as well.

3.2.2. *Analyzing the complement of $\mathcal{S}$ in $\mathcal{W}$.* We now describe a procedure that determines the complement of $\mathcal{S}$ in order of enumeration in $\mathcal{W}$. In Theorem 3.9 we show that the complement can be computed with the aid of an oracle for $\mathrm{HTP}(\mathbb{Z}[\mathcal{M}^{-1}])$. As $\mathcal{S}$ satisfies $\mathcal{R} \subseteq \mathcal{S} \subseteq \mathcal{R} \cup \mathcal{W} = \mathcal{M}$, we focus on describing the set of primes in $\mathcal{W}$ that are not in $\mathcal{S}$, which we denote by $\mathcal{W} - \mathcal{S}$.

Proposition 3.6. *For $e > 0$, the first $h(s_e)$ primes in $\mathcal{W} - \mathcal{S}_{s_e}$ (under our enumeration of $\mathcal{W}$) are precisely the first $h(s_e)$ primes in $\mathcal{W} - \mathcal{S}$.*

Proof. It suffices to prove for any fixed $e > 0$ that, at every stage $t \geq s_e$, the first $h(s_e)$ primes in $\mathcal{W} - \mathcal{S}_{s_e}$, which we denote by $p_1, p_2, \ldots, p_{h(s_e)}$ in order of enumeration into $\mathcal{W}$, are the first $h(s_e)$ primes in $\mathcal{W} - \mathcal{S}_t$.

We use induction on t. For the base case $t = s_e$, the claim is true by definition of the set $\mathcal{W} - \mathcal{S}_{s_e}$. For the induction step, assume $\{p_1, \ldots, p_{h(s_e)}\}$ are the first $h(s_e)$ elements of $\mathcal{W} - \mathcal{S}_{t-1}$ (in the order of enumeration of $\mathcal{W}$). Now consider the stage t of construction 3.2.1 with $g(t) = (f_{e'}, \vec{x}, j)$. If we are in case (2) at this stage, then $\mathcal{S}_{t-1} = \mathcal{S}_t$ and $\{p_1, \ldots, p_{h(s_e)}\}$ are the first $h(s_e)$ elements of $\mathcal{W} - \mathcal{S}_t$.

If we are in case (1), then we must have $e' \geq e$, since otherwise $\mathtt{R}_{e'}$ would change from FALSE to TRUE at stage $t > s_e$, contradicting the definition of s_e. Also, by conditions (2) and (3) we have that $h(t) \geq h(s_e)$, with construction 3.2.1 implying that $\mathcal{V}_t$ (the set of primes that cannot be inverted at this stage) is the set of the first $h(t)$ elements of $\mathcal{W} \setminus \mathcal{S}_{t-1}$. Thus, $\{p_1, \ldots, p_{h(s_e)}\} \subset \mathcal{V}_t$ while $\mathcal{V}_t \cap \mathcal{T}_t = \emptyset$. We remind the reader that $\mathcal{T}_t$ is the set of primes in the denominator of a root of $f_{e'}$ being processed at this stage t. Also, by definition, $\mathcal{S}_t = \mathcal{S}_{t-1} \cup \mathcal{T}_t$. Thus, $\{p_1, \ldots, p_{h(s_e)}\} \subseteq \mathcal{W} - \mathcal{S}_t$. □

Remark 3.7. Since $h(s_e) \to \infty$ as $e \to \infty$, it follows that the set $\mathcal{W} - \mathcal{S}$ is infinite.

We now show that an $\mathrm{HTP}(\mathbb{Z}[\mathcal{M}^{-1}])$-oracle is enough to determine polynomials with solutions in the constructed ring $R = \mathbb{Z}[\mathcal{S}^{-1}]$. The proof is divided into two parts. First, we show that the membership of f_e in $\mathrm{HTP}(R)$ can be determined by the end of stage s_e (Proposition 3.8). Then we show that the s_e can be computed using an oracle for $\mathrm{HTP}(\mathbb{Z}[\mathcal{M}^{-1}])$.

Proposition 3.8. *For each $e > 0$, the following are equivalent:*

(i) $\mathtt{R}_e = \mathrm{TRUE}$ *at some stage s (thus, at all stages $\geq s$);*
(ii) $f_e \in \mathrm{HTP}(R)$*;*
(iii) $f_e \in \mathrm{HTP}(\mathbb{Z}[(\mathcal{M} - \{p_1, \ldots, p_{h(s_e)}\})^{-1}])$.

Proof. The implication (i)⇒(ii) is trivial, the implication (ii)⇒(iii) follows directly from Proposition 3.6, and so we need only to prove (iii)⇒(i). Suppose that $f_e \in \mathrm{HTP}(\mathbb{Z}[(\mathcal{M} - \{p_1, \ldots, p_{h(s_e)}\})^{-1}])$. This means that there exists a solution

$\vec{x} \in \mathbb{Z}[(\mathcal{M} - \{p_1, \ldots, p_{h(s_e)}\})^{-1}]$ such that $f_e(\vec{x}) = 0$. Consider a stage $s > s_e$ in construction 3.2.1 such that $g(s) = (f_e, \vec{x}, j)$ for some j.

If $\mathtt{R}_e$ is already set to TRUE by this stage, we are done. Otherwise, we must be in case (1) at this stage of the construction, since

$$\begin{aligned}\mathcal{V}_s &= \{\text{first } h(s) \text{ primes of } \mathcal{W} \text{ not in } \mathcal{S}_{s-1}\} \\ &= \{\text{first } h(s_e) \text{ primes of } \mathcal{W} \text{ not in } \mathcal{S}_{s-1}\} \quad \text{(condition (3.3))} \\ &= \{p_1, \ldots, p_{h(s_e)}\} \quad \text{(Proposition 3.6).}\end{aligned}$$

Then $\vec{x} \in \mathrm{HTP}(\mathbb{Z}[(\mathcal{M} - \{p_1, \ldots, p_{h(s_e)}\})^{-1}]) = \mathrm{HTP}(\mathbb{Z}[(\mathcal{M} - \mathcal{V}_s)^{-1}])$, so $\mathtt{R}_e$ is set to TRUE at this stage. □

This proposition serves as an important tool for computing s_e using the $\mathrm{HTP}(\mathbb{Z}[\mathcal{M}^{-1}])$-oracle via Corollary 5.6 and finitely many primes in place of the whole set $\mathcal{S}$.

Theorem 3.9. *The ring* $R = \mathbb{Z}[\mathcal{S}^{-1}]$ *satisfies* $\mathrm{HTP}(\mathbb{Z}[\mathcal{M}^{-1}]) \geq_T \mathrm{HTP}(R)$.

Proof. To show that $\mathrm{HTP}(\mathbb{Z}[\mathcal{M}^{-1}]) \geq_T \mathrm{HTP}(R)$ it is enough to show that given $e \in \mathbb{Z}_{>0}$, the oracle for $\mathrm{HTP}(\mathbb{Z}[\mathcal{M}^{-1}])$ can compute s_e. Indeed, we show that knowing s_e is enough to determine whether $f_e \in \mathrm{HTP}(R)$. By Proposition 3.8, we have that $f_e \in \mathrm{HTP}(R)$ if and only if $f_e \in \mathrm{HTP}(\mathbb{Z}[(\mathcal{M} - \{p_1, \ldots, p_{h(s_e)}\})^{-1}])$. If we can compute s_e, we can run construction 3.2.1 for s_e stages so that we can determine the primes $p_1, \ldots, p_{h(s_e)}$. Now these primes can be plugged into the procedure discussed in Corollary 5.6 to determine whether $f_e \in \mathrm{HTP}(\mathbb{Z}[(\mathcal{M} - \{p_1, \ldots, p_{h(s_e)}\})^{-1}])$ using the oracle for $\mathrm{HTP}(\mathbb{Z}[\mathcal{M}^{-1}])$.

We now show how, given an $e \in \mathbb{Z}_{>0}$, the oracle for $\mathrm{HTP}(\mathbb{Z}[\mathcal{M}^{-1}])$ computes s_e. We proceed by induction.

Base case. By definition, s_1 is the smallest $s > 0$ such that $g(s) = (f_1, \vec{x}, j)$ for some $\vec{x}$ and some j. This s is certainly computable by running construction 3.2.1 through a sufficient number of stages until the first component of $g(s)$ is equal to f_1. Also, such a stage exists because *every* triple of the form $(f_1, \vec{x}, j)$ is in the image of $g(s)$.

Induction step. Suppose that by using the oracle for $\mathrm{HTP}(\mathbb{Z}[\mathcal{M}^{-1}])$ we have computed s_e. In this case, without loss of generality, we can assume that we have also computed $p_1, \ldots, p_{h(s_e)}$, and therefore can determine whether $f_e \in \mathrm{HTP}(R)$, as described above. If $f_e \notin \mathrm{HTP}(R)$, then s_{e+1} is the smallest $s > s_e$ such that $g(s) = (f_{e+1}, \vec{x}, j)$ for some $\vec{x}$ and some j. Such an s can certainly be computed by running construction 3.2.1 through a sufficient number of stages. If $f_e \in \mathrm{HTP}(R)$, then we first run construction 3.2.1 through a sufficient number of stages to find the smallest possible stage $\bar{s} \geq s_e$ such that $g(\bar{s}) = (e, \vec{x}, j)$ for some $\vec{x}$ and some j with $f_e(\vec{x}) = 0$. The existence of $\bar{s}$ is guaranteed by the fact that $f_e \in \mathrm{HTP}(R)$ and each pair $(f_e, \vec{x})$ appears with infinitely many j. Now we look for the smallest $s > \bar{s}$ such that $g(s) = (f_{e+1}, \vec{x}, j)$ for some $\vec{x}$ and some j. We set $s_{e+1} = s$. □

Corollary 3.10. *There exists a subset* $\mathcal{S} \subseteq \mathcal{P}$ *that is infinite and co-infinite, such that the ring* $R[\mathcal{S}^{-1}]$ *satisfies* $\mathrm{HTP}(\mathbb{Q}) \equiv_T \mathrm{HTP}(R)$.

Proof. Choose $h(s) = e$, where $g(s) = (f_e, \vec{x}, j)$, $\mathcal{R} = \emptyset$, and $\mathcal{W} = \mathcal{P}$. □

3.3. **Imposing density conditions.** In this section, we show that a more complicated choice of h lets us impose a density condition on the set $\mathcal{S}$. We first need to define the relative upper and lower density of sets of primes. Given a subset $\mathcal{S} \subseteq \mathcal{W} = \{q_1, \ldots, q_n, \ldots\}$, we define

$$\limsup_{n\to\infty} \frac{|\mathcal{S} \cap \{q_1, \ldots, q_n\}|}{n}$$

to be the *upper density of a subset $\mathcal{S}$ relative to $\mathcal{W}$*. The *relative lower density* can be defined in a similar fashion. Both of these depend on the choice of the enumeration of $\mathcal{W}$, as well as on $\mathcal{W}$ itself: a set $\mathcal{S}$ could have upper density 0 in $\mathcal{W}$ under one enumeration of $\mathcal{W}$, yet have upper density 1 in the same set $\mathcal{W}$ under a different enumeration. However, if $\mathcal{W} = \mathcal{P}$ and we enumerate the primes into $\mathcal{P}$ in increasing order, then the upper (resp. lower) density of $\mathcal{S}$ relative to $\mathcal{W}$ matches the usual notion of upper (resp. lower) density. If the upper and lower density are equal, this quantity is the *natural density* of $\mathcal{S}$ in $\mathcal{W}$.

We will use the following notation for our density calculations in the following sections.

Notation 3.11. Suppose that $\mathcal{U} \subset \mathcal{W}$ is finite. Let $i_{\mathcal{W}}(\mathcal{U})$ be the largest index i such that $q_i \in \mathcal{U}$ (or 1 if $\mathcal{U}$ is empty). We define

$$\mu_{\mathcal{W}}(\mathcal{U}) := \frac{|\mathcal{U}|}{i_{\mathcal{W}}(\mathcal{U})}.$$

Remark 3.12 (Constructing sets with $\mu_{\mathcal{W}}$ arbitrarily close to 1, containing a given finite set $\mathcal{U}$ and avoiding a given finite set $\mathcal{S}$). Let $\mathcal{S} \subset \mathcal{W}$ be a finite set such that $\mathcal{S} \cap \mathcal{U} = \emptyset$. Let $i = i_{\mathcal{W}}(\mathcal{U} \cup \mathcal{S})$ and consider a set $\mathcal{U}_k = \mathcal{U} \cup \{q_{i+1}, q_{i+2}, \ldots, q_{i+k}\}$. Now $\mu_{\mathcal{W}}(\mathcal{U}_k) = \frac{|\mathcal{U}_k|}{i_{\mathcal{W}}(\mathcal{U}_k)} = \frac{|\mathcal{U}|+k}{i+k} \longrightarrow 1$ as $k \longrightarrow \infty$ and at the same time $\mathcal{U}_k \cap \mathcal{S} = \emptyset$.

Remark 3.13. Let $\mathcal{S} \subset \mathcal{W}$ and let $t \in \mathbb{Z}_{>0}$. Let $\mathcal{V}$ be the set of the first t elements of $\mathcal{W}$ not in $\mathcal{S}$, and let $\mathcal{V}'$ be a set of any t elements not in $\mathcal{S}$. We have that $i_{\mathcal{W}}(\mathcal{V}) \leq i_{\mathcal{W}}(\mathcal{V}')$ and therefore $\mu_{\mathcal{W}}(\mathcal{V}) \geq \mu_{\mathcal{W}}(\mathcal{V}')$.

Define a function $h(s)$ to be equal to the least positive integer greater than or equal to e that yields $\mu_{\mathcal{W}}(\mathcal{V}_s) > \frac{e}{e+1}$ (where e is such that $g(s) = (f_e, \vec{x}, j)$). With this choice $h(s)$ is computable and well-defined by Remark 3.12 because $\mathcal{S}_{s-1}$ is a finite set.

Proposition 3.14. *The function $h(s)$ satisfies conditions* (3.1)–(3.3).

Proof. First, condition (3.1) is trivially satisfied, since by definition of s_e we have that $g(s_e) = (f_e, \vec{x}, j)$ for some $\vec{x}$ and some j, and therefore $h(s_e) \geq e$ and $h(s_e) \to \infty$ as $e \to \infty$.

To show that condition (3.2) is satisfied, we first show that if $e \geq e'$ and $s \geq s'$ while $g(s) = (f_e, \vec{x}, j)$, $g(s') = (f_{e'}, \vec{x}', j')$, then $h(s) \geq h(s')$. First of all, $\mathcal{S}_{s'-1} \subseteq \mathcal{S}_{s-1}$ and $\frac{e}{e+1} \geq \frac{e'}{e'+1}$. Now assume $h(s) < h(s')$. Now we have, by the definition of $h(s)$,

$$e' \leq e \leq h(s) < h(s'). \tag{3.4}$$

By Remark 3.13, if $\mathcal{V}'_s$ were any set of the form $\{$*any* $h(s)$ primes not lying in $\mathcal{S}_{s-1}\}$, then $\mu_{\mathcal{W}}(\mathcal{V}_s) \geq \mu_{\mathcal{W}}(\mathcal{V}'_s)$. The primes not contained in $\mathcal{S}_{s-1}$ are also not contained

in $\mathcal{S}_{s'-1}$ (although the $h(s)$ primes above are not necessarily the first $h(s)$ ones in the enumeration of $\mathcal{W}$), and so

$$\begin{aligned}\mu_{\mathcal{W}}(\mathcal{V}_s) &:= \mu_{\mathcal{W}}(\text{first } h(s) \text{ primes not in } \mathcal{S}_{s-1})\\ &= \mu_{\mathcal{W}}(\text{the same } h(s) \text{ primes as above not in } \mathcal{S}_{s'-1})\\ &\leq \mu_{\mathcal{W}}(\text{first } h(s) \text{ primes not in } \mathcal{S}_{s'-1})(\text{by Remark 3.13})\\ &\leq \frac{e'}{e'+1} \text{ (by minimality of the choice of } h(s') \text{ and (3.4))}\\ &< \mu_{\mathcal{W}}(\text{the first } h(s') \text{ primes not in } \mathcal{S}_{s'-1}) =: \mu_{\mathcal{W}}(\mathcal{V}_{s'}).\end{aligned}$$

But then $\frac{e'}{e'+1} \geq \mu_{\mathcal{W}}(\mathcal{V}_s) > \frac{e}{e+1}$, which is a contradiction when $e \geq e'$. Thus condition (3.2) is satisfied.

To show that condition (3.3) holds we need to use an induction argument similar to the one used in Proposition 3.6. (We cannot use Proposition 3.6 itself as it was proved under the assumption that $h(s)$ satisfied the three conditions under consideration.) The argument is almost identical. We again need to consider what happens to the primes of $\mathcal{V}_{s_e}$, which are the first $h(s_e)$ noninverted primes of $\mathcal{W}$ at the end of the stage s_e, between the stage s_e and any other stage $\tilde{s}$ with $g(\tilde{s}) = (f_e, \vec{x}, j)$ for some $\vec{x}$ and some j. More specifically, we want to show that these primes do not get inverted. As in Proposition 3.6, we need to consider two cases: we are at the stage $s' > s_e$ with the corresponding $e' < e$ or at the stage $s' > s_e$ with the corresponding $e' \geq e$. In the first case, by definition of s_e, we must be in the second clause of construction 3.2.1 and no new primes are inverted. In the second case, $h(s') \geq h(s_e)$ by condition (3.2), and so the only primes which can be inverted at this stage are primes not in $\mathcal{V}_{s_e}$.

Thus, when the construction starts the stage $\tilde{s}$, the primes of $\mathcal{V}_{s_e}$ are not inverted and $\mathcal{V}_{s_e}$ must satisfy the requirements for $h(\tilde{s})$ that are the same as the requirements for $h(s_e)$. So by the minimality requirement on $h(s)$, we must have $h(s_e) = h(\tilde{s})$. □

Theorem 3.15. *For each infinite c.e. set $\mathcal{W}$ of primes and each computable enumeration of $\mathcal{W}$, there exists a set $\mathcal{S} \subseteq \mathcal{W}$ such that $\mathcal{W} - \mathcal{S}$ has relative upper density 1 in $\mathcal{W}$ and such that $\mathrm{HTP}(\mathbb{Z}[\mathcal{W}^{-1}]) \geq_T \mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}])$. In particular, $\mathcal{S}$ has relative lower density 0 in $\mathcal{W}$.*

Proof. Set $\mathcal{R} = \emptyset$ in the above construction, so that using notation of Theorem 3.9 we have $\mathcal{W} = \mathcal{M}$. That $\mathrm{HTP}(\mathbb{Z}[\mathcal{W}^{-1}]) \geq_T \mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}])$ now follows from Theorem 3.9. As for the density, we consider the stages s_e for $e \in \mathbb{Z}_{>0}$, at which we have

$$\mu_{\mathcal{W}}(\{p_{i_1}, \ldots, p_{i_{h(s_e)}}\}) > \frac{e}{e+1}.$$

Considering these stages s_e, we see that $\lim_{e\to\infty} \mu_{\mathcal{W}}(\mathcal{V}_{s_e}) = 1$, so that the relative upper density of $\mathcal{S}$ in $\mathcal{W}$ is 1. □

From the theorem above we can obtain the following corollary, which requires repeated applications of the theorem.

Corollary 3.16. *There exists a sequence $\mathcal{P} = \mathcal{W}_0 \supset \mathcal{W}_1 \supset \mathcal{W}_2 \ldots$ of uniformly c.e. sets of rational primes (with $\mathcal{P}$ denoting the set of all primes, enumerated in ascending order) such that*

(1) $\mathrm{HTP}(\mathbb{Z}[\mathcal{W}_i^{-1}]) \equiv_T \mathrm{HTP}(\mathbb{Q})$ *for $i \in \mathbb{Z}_{>0}$.*

(2) *$\mathcal{W}_{i-1} - \mathcal{W}_i$ has the relative upper density (with respect to the enumeration of $\mathcal{W}_{i-1}$) equal to 1 for all $i \in \mathbb{Z}_{>0}$.*
(3) *The relative lower density of $\mathcal{W}_i$ (with respect to the enumeration of $\mathcal{W}_{i-1}$) is 0, for $i \in \mathbb{Z}_{>0}$.*

Proof. By transitivity we can arrange that $\mathrm{HTP}(\mathbb{Q}) \geq_T \mathrm{HTP}(\mathbb{Z}[\mathcal{W}_i^{-1}])$ for all i. On the other hand, Corollary 5.2 implies that $\mathrm{HTP}(\mathbb{Q}) \leq_T \mathrm{HTP}(\mathbb{Z}[\mathcal{W}_i^{-1}])$. □

3.4. **Arbitrary lower density.** As remarked in the introduction, it is desirable to have the density for the set of inverted primes to be equal to 0. However, it seems that this is difficult to accomplish using this construction. We can, however, control the lower density:

Theorem 3.17. *For every computable real number r between 0 and 1 there exists a c.e. set $\mathcal{S}$ of primes such that the lower density of $\mathcal{S}$ is r and $\mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}]) \equiv_T \mathrm{HTP}(\mathbb{Q})$.*

To be clear: here, a *computable real number* r is a real number such that some computable sequence of rational numbers has limit r. The upper and lower cuts defined in $\mathbb{Q}$ by r will therefore be Turing-reducible to the Halting Problem $\emptyset'$, but need not be decidable. This definition, common in number theory, is less strict than the usual meaning of the same phrase in computability theory.

Proof. Let r be a computable real number. We set the parameters of the construction of section 3.2.1 as follows: $\mathcal{M} = \mathcal{P}$; $\mathcal{R} \subseteq \mathcal{P}$ is some computable set of density r (to understand why such a set of primes always exists, see [EES11]); $\mathcal{W} := \mathcal{P} - \mathcal{R}$, enumerated in ascending order (computably, since $\mathcal{R}$ is computable); and $h(s)$ the least integer $\geq e$ such that $\mu_{\mathcal{W}}(\mathcal{V}_s) > \frac{e}{e+1}$, where $g(s) = (f_e, \vec{x}, j)$, exactly as in the construction in 3.2.1. (This $h(s)$ also satisfies conditions (3.1)-(3.3) for the same reason as Proposition 3.14.)

Then as in Theorem 3.15, the set $\mathcal{S}_{\mathcal{W}} := \mathcal{S} \cap (\mathcal{P} - \mathcal{R}) = \mathcal{S} \cap \mathcal{W}$ has relative lower density 0 in $\mathcal{W}$.

Further, this choice of parameters ensures that all the primes of $\mathcal{R}$ are inverted by the end of the construction, as in Remark 3.3. It remains to show that the set $\mathcal{R} \cup \mathcal{S}_{\mathcal{W}} = \mathcal{S}$ is of (absolute) lower density r. For any integer m, we have the identity

$$\begin{aligned} \frac{\#\{q \in \mathcal{S}_{\mathcal{W}}, q \leq m\}}{\#\{q \in \mathcal{P}, q \leq m\}} &= \frac{\#\{q \in \mathcal{S}_{\mathcal{W}}, q \leq m\}}{\#\{q \in \mathcal{W}, q \leq m\}} \cdot \frac{\#\{q \in \mathcal{W}, q \leq m\}}{\#\{q \in \mathcal{P}, q \leq m\}} \\ &\leq \frac{\#\{q \in \mathcal{S}_{\mathcal{W}}, q \leq m\}}{\#\{q \in \mathcal{W}, q \leq m\}}. \end{aligned} \tag{3.5}$$

Thus $\mathcal{S}_{\mathcal{W}}$ has absolute lower density 0. At the same time,

$$\frac{\#\{q \in \mathcal{S}, q \leq m\}}{\#\{q \in \mathcal{P}, q \leq m\}} = \frac{\#\{q \in \mathcal{S}_{\mathcal{W}}, q \leq m\}}{\#\{q \in \mathcal{P}, q \leq m\}} + \frac{\#\{q \in \mathcal{R}, q \leq m\}}{\#\{q \in \mathcal{P}, q \leq m\}}. \tag{3.6}$$

Since $\mathcal{R}$ has absolute density r, the liminf of the right side as $m \to \infty$ is r. □

3.5. **Complementary rings.** We also show that by modifying the construction of section 3.1 to obtain several rings $R_i = \mathbb{Z}[\mathcal{S}_i^{-1}]$ at once, we may arrange that the sets $\mathcal{S}_i$ form a partition of the set of all primes. In this case, the sets $\mathcal{S}_i$ are not built to be computably enumerable, and so the rings R_i may not be computably presentable.

Theorem 3.18. *For any positive integer m, the set of all rational primes $\mathcal{P}$ can be represented as a union of pairwise disjoint sets $\mathcal{S}_1, \ldots, \mathcal{S}_m$, each of upper density 1 and such that for all i we have that* $\mathrm{HTP}(\mathbb{Z}[\mathcal{S}_i^{-1}]) \leq_T \mathrm{HTP}(\mathbb{Q})$ *and* $\mathcal{S}_i \leq_T \mathrm{HTP}(\mathbb{Q})$.

Proof. We imitate the construction given in section 3.1, defining all $\mathcal{S}_{1,s}, \ldots, \mathcal{S}_{m,s}$ so that their pairwise intersections are always empty, but their union is an initial segment of $\mathbb{Z}$, growing ever larger as n increases. (As before we will have $\mathcal{S}_i = \bigcup_{s=1}^{\infty} \mathcal{S}_{i,s}$.) Start with $\mathcal{S}_{i,0} = \emptyset$ for all $i = 1, \ldots, m$ and fix the same computable list $\langle f_e \rangle_{e \in \mathbb{Z}_{>0}}$ as before. Also, set all $\mathtt{R}_{e,i}, i = 1, \ldots, m$, to FALSE. We proceed in stages with $i = 0, \ldots, m-1$. For stage $s = me + i > 0$, let $\mathcal{W}_s = \bigcup_{j \neq i} \mathcal{S}_{j,s-1}$, and use the oracle for $\mathrm{HTP}(\mathbb{Q})$ to determine whether f_e has a root $\vec{x}$ in $\mathbb{Z}[\overline{\mathcal{W}}_s^{-1}]$. We go through a different sequence of actions depending on the answer.

"Yes": Let $\mathcal{T}_{i,s}$ be the smallest set of primes such that $\vec{x} \in \mathbb{Z}[\mathcal{T}_{i,s}^{-1}]$. Next set $\mathtt{R}_{i,e} =$ TRUE, and let i_s be the index (in the listing of all primes) of the largest prime used in the construction so far. Now set

$$\mathcal{S}_{i,s} = \mathcal{S}_{i,s-1} \cup \mathcal{T}_{i,s} \cup \{\text{every prime with index in the interval } [1, 2^{i_s}] \text{ not in } \mathcal{W}_s\},$$

and set $\mathcal{S}_{j,s} = \mathcal{S}_{j,s-1}$ for $j \neq i$. (The reason for including the last set of primes is to ensure upper density 1 for $\mathcal{S}_i$. Indeed, in the computation of the upper density, at this point we get from $\mathcal{S}_{i,s}$ a term that will be greater than or equal to $\frac{2^{i_s}}{i_s + 2^{i_s}}$, so it converges to 1 as $s \to \infty$.)

"No": As above, let i_s be the index (in the listing of all primes) of the largest prime used in the construction so far. Now set

$$\mathcal{S}_{i,s} = \mathcal{S}_{i,s-1} \cup \{\text{every prime with index in the interval } [1, 2^{i_s}] \text{ not in } \mathcal{W}_s\},$$

and set $\mathcal{S}_{j,s} = \mathcal{S}_{j,s-1}$ for $j \neq i$.

To determine whether f_e has a solution in $\mathbb{Z}[\mathcal{S}_i^{-1}]$, all we need to do is run the construction until the step $me + i$. If $\mathtt{R}_{e,i}$ is not set to TRUE at this point, it never will be. Similarly, to determine if a prime p_j is in $\mathcal{S}_i$ we just need for the construction to process this prime to see where it was put. Thus, both assertions concerning Turing reducibility are true. □

One can also build countably many rings with the same property instead of building m rings as in Theorem 3.18.

Corollary 3.19. *There exist infinitely many subsets $\mathcal{S}_1, \mathcal{S}_2, \ldots$ of the set $\mathcal{P}$ of primes, all of lower density 0, all computable uniformly from an* $\mathrm{HTP}(\mathbb{Q})$*-oracle (so that the rings $R_j = \mathbb{Z}[\mathcal{S}_j^{-1}]$ are also uniformly computable below* $\mathrm{HTP}(\mathbb{Q})$*), with the property that $\bigcup_j \mathcal{S}_j = \mathcal{P}$ and $\mathcal{S}_i \cap \mathcal{S}_j = \emptyset$ for all $i < j$, and such that* $\mathrm{HTP}(\mathbb{Z}[\mathcal{S}_j^{-1}]) \equiv_T \mathrm{HTP}(\mathbb{Q})$ *for every j.*

Proof. Use the construction from Theorem 3.18, but loop through a computable listing of all pairs $(i, e) \in \mathbb{N}^2$ with the first index referring to the set of primes and the second to a polynomial. □

Remark 3.20. Notice that if the sets $\mathcal{S}_i$ in Theorem 3.18 were all c.e. (or if those in Corollary 3.19 were uniformly c.e.), then they would all be computable. It is not clear that the theorems of this section fail to hold when one demands that the set(s) of inverted primes be computable, but the constructions given here do not suffice. (In Remark 4.8, we will mention how close we can come.) It is an open

question, worthy of attention, whether there exists a computable co-infinite set $\mathcal{S}$ of primes with $\mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}]) \equiv_T \mathrm{HTP}(\mathbb{Q})$.

4. Rings R such that $R \equiv_T \mathrm{HTP}(R) \equiv_T \mathrm{HTP}(\mathbb{Q})$

In this section we construct examples where HTP of a ring is no more complicated than the ring itself. One such example is already known: if $\mathcal{S}$ is a computably enumerable subset of $\mathcal{P}$ with Turing degree $\mathbf{0}'$, such as the Halting Problem itself, then $\mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}])$ is also computably enumerable, hence $\leq_T \mathcal{S}$. However, we wish to build sets $\mathcal{S}$ of Turing degree $< \mathbf{0}'$: we will show that every computably enumerable Turing degree $\geq_T \mathrm{HTP}(\mathbb{Q})$ contains a c.e. set $\mathcal{S}$ with $\mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}]) \equiv_T \mathcal{S}$. (Of course, if $\mathrm{HTP}(\mathbb{Q})$ is decidable, then $\mathbb{Q}$ would be another example of this phenomenon.)

Theorem 4.1. *For every computably enumerable set $B \subset \mathbb{Z}_{>0}$ with $\mathrm{HTP}(\mathbb{Q}) \leq_T B$, there exists a computably presentable ring $\mathbb{Z}[\mathcal{S}^{-1}]$, with $\mathcal{S}$ a computably enumerable subset of the prime numbers of lower density 0, such that $\mathcal{S} \equiv_T \mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}]) \equiv_T B$. (By setting $B \equiv_T \mathrm{HTP}(\mathbb{Q})$, we obtain a ring R with $\mathrm{HTP}(R) \equiv_T \mathrm{HTP}(\mathbb{Q})$.)*

We prove the theorem in the remainder of this section. The required construction, while similar to construction 3.2.1, is more complicated. The proof proceeds as follows: first we construct a computably enumerable set $\mathcal{S}$. Then we prove that $\mathcal{S}$ possesses certain properties that are used to show that $B \geq_T \mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}])$ (Theorem 4.5) and $\mathcal{S} \geq_T B$ (Proposition 4.6). This of course will imply that $\mathcal{S} \equiv_T \mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}])$, since $\mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}]) \geq_T \mathcal{S}$ for obvious reasons.

Before we get started we review and introduce some notation.

- $H : \mathbb{Z}_{>0} \longrightarrow B$ will denote a computable function enumerating B.
- $\mathcal{R}$ is a computable infinite sequence of primes of density 0. As before, let $\mathcal{W} = \mathcal{P} - \mathcal{R}$ and observe that $\mathcal{W}$ is computable.
- For each $s > 1$, let $y_s \in \mathcal{R}$ be the xth least element of $\mathcal{R} - \mathcal{S}_s$ where $x = H(s)$.

To ensure that B can be computed from $\mathcal{S}$ we will arrange that the following is true:

$(*)$ $\forall x, s, t \in \mathbb{Z}_{>0}$, if $H(s) = x$ and the sets $\mathcal{R} - \mathcal{S}$ and $\mathcal{R} - \mathcal{S}_t$ agree on their least x elements, then $t > s$.

Given a positive integer x, let

$$t_x = \min\{t \in \mathbb{Z}_{>0} | \mathcal{R} - \mathcal{S} \text{ and } \mathcal{R} - \mathcal{S}_t \text{ agree on their least } x \text{ elements}\}.$$

It is not hard to see that t_x is computable from the $\mathcal{S}$-oracle (as a function of x). Indeed, all we have to do is to run the construction and compare the first x elements of $\mathcal{R} - \mathcal{S}$ and $\mathcal{R} - \mathcal{S}_i$, where i is the current stage. Eventually the first x elements of the two sets under consideration will be the same. The earliest stage at which this happens is t_x. Now if $(*)$ holds we know that t_x is greater than s, the stage (if one exists) such that $H(s) = x$.

Therefore, assuming $(*)$ holds, to determine if $x \in B$, we just have to check values of H from $H(1)$ up to $H(t_x)$ to see if any of them is equal to x.

To make sure that $t_x > s$, the xth least element of $\mathcal{R} - \mathcal{S}_s$ (denoted above by y_s) will be added to $\mathcal{S}_{s+1}$ so that $\mathcal{R} - \mathcal{S}_s$ and $\mathcal{R} - \mathcal{S}$ cannot agree on their least x elements.

To see why the set differences cannot agree on the least x elements any earlier, note the following more general phenomenon: if an integer $z \in (\mathcal{R} - \mathcal{S}_t) \cap (\mathcal{R} - \mathcal{S})$, then $z \in \mathcal{R} - \mathcal{S}_u$ for all $u \geq t$, since we only add things to sets $\mathcal{S}_u$, never remove them. Therefore, if for some $u < s$ we had that $\mathcal{R} - \mathcal{S}_u$ and $\mathcal{R} - \mathcal{S}$ agree on their least x elements, say $a_1, \ldots, a_x$, then $a_1, \ldots, a_x \in \mathcal{R} - \mathcal{S}_s \subseteq \mathcal{R} - \mathcal{S}_u$ and $a_1, \ldots, a_x$ are still the least x elements of the sets $\mathcal{R} - \mathcal{S}_s$ and $\mathcal{R} - \mathcal{S}$, contradicting that $a_x = y_s \in \mathcal{S}_{s+1} \subseteq \mathcal{S}$ in our construction.

4.1. **The construction of the set $\mathcal{S}$.** As we mentioned above, this construction is similar to construction 3.2.1, but modified to accommodate the equivalence $(*)$. As before, for each $e \geq 1$, we introduce a boolean variable $\mathtt{R}_e$ and we also have $\mathtt{R}_0$=TRUE at the beginning of the construction. At the beginning of the construction, $\mathtt{R}_e$ is set to FALSE for all $e > 0$. At each step s of the construction, we define the sets $\mathcal{S}_s$ and $\mathcal{V}_s$; at the end of the construction, we will define $\mathcal{S} = \bigcup_s \mathcal{S}_s$. Below the "complement" notation will denote the complement in the set of all primes again.

- At stage $s = 0$: let $\mathcal{S}_0 = \emptyset, \mathcal{V}_0 = \emptyset$.
- At stage $s > 0$: suppose $g(s) = (f_e, \vec{x}, j) \in \mathtt{E}$, where f_e is the eth polynomial in the enumeration $\{f_1, f_2, \ldots\}$ as defined above. At this stage, we will consider this polynomial f_e.

  We now reconsider the function $h(s)$ and the set $\mathcal{V}_s$. The function $h(s)$ is defined the same way as above in Proposition 3.14, i.e., $h(s)$ is the smallest integer greater than or equal to e such that

$$\mu_{\mathcal{W}}(\text{the set of the first } h(s) \text{ primes of } \mathcal{W} \text{ not in } \mathcal{S}_{s-1}) > \frac{e}{e+1}.$$

  Let

$$\mathcal{V}_s = \{p_{i_1}, \ldots, p_{i_{h(s)}}\} \cup \{ \text{ the least } e \text{ elements of } (\mathcal{R} - (\mathcal{S}_{s-1} \cup \{y_s\}))\}.$$

Now there are two cases:

(1) If $\mathtt{R}_e$ = FALSE, $\vec{x} \in \mathbb{Z}[(\mathcal{P} - \mathcal{V}_s)^{-1}]$ and $f_e(\vec{x}) = 0$, then let $\mathcal{S}_s = \mathcal{S}_{s-1} \cup \mathcal{T}_s \cup \{y_s\}$, where $\mathcal{T}_s$ is the least set of primes such that $\vec{x} \in (\mathbb{Z}[\mathcal{T}_s^{-1}])^n$. (The set $\mathcal{T}_s$ is allowed to have elements from $\mathcal{R} - \mathcal{V}_s$.) Here, we set $\mathtt{R}_e$ = TRUE.
(2) Otherwise, $\mathcal{S}_s = \mathcal{S}_{s-1} \cup \{y_s\}$.

In the end, let $\mathcal{S} = \bigcup_{s=1}^{\infty} \mathcal{S}_s$ and $R = \mathbb{Z}[\mathcal{S}^{-1}]$. Since this construction is entirely effective, $\mathcal{S}$ is computably enumerable, and so R is computably presentable.

4.2. **Analyzing the complement of $\mathcal{S}$.** We now describe the procedure determining the complement of $\mathcal{S}$ in order. The following notation will be useful: Let $\mathcal{V} := (\mathcal{P} - \mathcal{S}) \cap (\mathcal{P} - \mathcal{R}) = \{p_{i_1}, p_{i_2}, \ldots\}$ in order of a fixed enumeration, and let $\mathcal{H} := (\mathcal{P} - \mathcal{S}) \cap \mathcal{R} = \{w_1, w_2, \ldots\}$ in order of a fixed enumeration. We will use the familiar variable s_e, but it will be defined inductively in a slightly different manner, together with another variable v_e. We define

- $s_0 = 0$.
- For $e \geq 1$ we let v_e be the smallest positive integer greater than s_{e-1} such that for each positive integer $i \in [1, e]$, either $i \notin B$ or for some $s < v_e$ we have that $H(s) = i$.
- For $e \geq 1$ we let s_e be the smallest possible positive integer greater than v_e such that $g(s_e) = (f_e, \vec{x}, j)$ for some $\vec{x}$ and some j, and $\mathtt{R_{e-1}}$ has either been set to TRUE or never will be.

We start with the following proposition.

Proposition 4.2. *At every stage $u \geq s_e$, we have that $\{p_{i_1}, \ldots, p_{i_{h(s_e)}}\} \subset \mathcal{V}_u$.*

Proof. This proof is analogous to the proofs of Proposition 3.14 and Proposition 3.6, since the function $h(s)$ and the sequence $\{s_e\}$ satisfy the assumptions of these propositions. □

To determine $\mathcal{H} = \{w_1 < w_2 < \ldots\}$ in order we use the following proposition.

Proposition 4.3. *If $\{w_1, \ldots, w_e\} =$ the least e elements of $\mathcal{R} \cap \mathcal{V}_{s_e}$, then for every $t \geq 0$, we have that $\{w_1, \ldots, w_e\} \subset \mathcal{V}_{t+s_e}$.*

Proof. We use strong induction on e again. The base case of $t = 0$ is clear. So assume that $t > 0$ and $\{w_1, \ldots, w_e\} =$ the least e elements of $\mathcal{R} \cap \mathcal{V}_{s_e-1+t}$. Let $g(t + s_e) = (f_{e'}, \vec{x}, j) \in \mathtt{E}$ (as defined on page 8296). If $e' \leq e$, then $\mathcal{T}_{t+s_e} = \emptyset$ (since $\mathtt{R}_{e'}$ has either been satisfied already or will never be). Thus, only y_{t+s_e} is added to $\mathcal{S}_{t-1+s_e}$ to form $\mathcal{S}_{t+s_e}$. By assumption on $v_e < s_e$, we have that $H(t + s_e) > e$, and therefore the first e elements of $\mathcal{R} - \mathcal{S}_{t-1+s_e}$ and $\mathcal{R} - \mathcal{S}_{t+s_e}$ are the same.

Suppose now that $e' > e$. In this case $\mathcal{V}_{t+s_e}$ will contain $w_1, \ldots, w_e$ and $\mathcal{T}_{t+s_e}$ cannot contain any of $w_1, \ldots, w_e$. Further, y_{t+s_e} cannot be among $w_1, \ldots, w_e$ for the same reason as above. □

Proposition 4.4. *For each $e \geq 0$, the following are equivalent:*

(i) $\mathtt{R}_e =$ TRUE*;*
(ii) $f_e \in \mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}])$*;*
(iii) $f_e \in \mathrm{HTP}(\mathbb{Z}[(\mathcal{P} - \mathcal{V}_{s_e})^{-1}])$.

Proof. The proof is analogous to the proof of Proposition 3.8. □

Theorem 4.5. $B \geq_T \mathrm{HTP}(\mathbb{Z}[\mathcal{S}^{-1}])$.

Proof. We follow construction 4.1, using a B-oracle to compute stages s_e (and hence the primes of $\mathcal{V}_{s_e}$) recursively, starting with $s_0 = 0$. Assume inductively that we have computed s_{e-1}. First, using the B-oracle, we check whether $e \in B$. If $e \notin B$, then we know $v_e = s_{e-1} + 1$, while if $e \in B$, then either $v_e = 1 + s_{e-1}$ (if some $s \leq s_{e-1}$ has $H(s) = e$) or else v_e is the unique integer v with $H(v) = e$ (if this v is $> s_{e-1}$). Since H is computable, we have thus determined v_e.

Knowing v_e, we then find the least integer $s > v_e$ such that $g(s) = (f_{e-1}, \vec{x}, j) \in \mathtt{E}$. Compute $\mathcal{V}_s$ for this stage and use the B-oracle to determine whether $f_{e-1} \in \mathrm{HTP}(\mathbb{Z}[(\mathcal{P} - \mathcal{V}_s)^{-1}])$. (This is possible by Proposition 5.4, because $\mathrm{HTP}(\mathbb{Q}) \leq_T B$.) If the answer is "no," then set $s_e = s$. If the answer is "yes," find the least stage $\hat{s} \geq s$ such that $g(\hat{s}) = (f_{e-1}, \vec{x}, j')$, $\vec{x} \in \mathbb{Z}[(\mathcal{P} - \mathcal{V}_{\hat{s}})^{-1}] = \mathbb{Z}[(\mathcal{P} - \mathcal{V}_s)^{-1}]$, and $f_{e-1}(\vec{x}) = 0$. Then s_e will be the least integer $\geq \hat{s}$ with $g(s_e) = (f_e, \vec{x}, j)$ for some $\vec{x}$ and some j. □

The last proposition we need to complete the proof of Theorem 4.1 states the following.

Proposition 4.6. $\mathcal{S} \geq_T B$.

Proof. We use an $\mathcal{S}$-oracle to determine membership in B. Given a positive integer x, run the construction until it reaches a stage s at which $\mathcal{P} - \mathcal{S}$ and $\mathcal{P} - \mathcal{S}_s$ agree on at least their smallest x elements. If $x \notin \{H(1), H(2), \ldots, H(s)\}$, then

$x \notin B$ by property $(*)$, which was introduced right before section 4.1. Otherwise $x \in \text{range}(H) = B$. □

Remark 4.7 (Density). Our final observation concerns the assertion on density in Theorem 4.1. The construction above did not consider density, but the assertion can be fulfilled by applying the same methods as in Theorem 3.15.

Remark 4.8. Mathematicians familiar with priority arguments will not be surprised to learn that standard lowness requirements (e.g. from [Soa87, VII.1]) can be mixed in with certain of the constructions in the preceding two sections. In Theorem 3.17, for example, we can build a c.e. set $\mathcal{S} \subseteq \mathcal{P}$ which is low (i.e., $\mathcal{S}' \leq_T \emptyset'$), has arbitrary computable lower density r, and satisfies $\text{HTP}(\mathbb{Q}) \equiv_T \text{HTP}(\mathbb{Z}[\mathcal{S}^{-1}])$. It follows that the entire subring $\mathbb{Z}[\mathcal{S}^{-1}]$ has low Turing degree as a subset of $\mathbb{Q}$. This is the closest we currently come to answering the question in Remark 3.20. The construction is a technical extension of that for Theorem 3.17, and we do not include it here.

It is open whether a low set $\mathcal{S}$ could satisfy Theorem 4.1, where a c.e. set $B \geq_T \text{HTP}(\mathbb{Q})$ is given arbitrarily. The requirement that $\mathcal{S} \equiv_T B$ would have to be dropped, of course, but it seems possible that a low c.e. set $\mathcal{S}$, of lower density 0, might satisfy $\text{HTP}(\mathbb{Z}[\mathcal{S}^{-1}]) \equiv_T B$. However, the techniques we have used do not suffice to prove this.

5. Computing $\text{HTP}(R)$ from $\text{HTP}(\mathbb{Q})$ for a semilocal ring $R \subseteq \mathbb{Q}$

We begin with results necessary to show that $\text{HTP}(R) \geq_T \text{HTP}(\mathbb{Q})$ for all rings $R \subseteq \mathbb{Q}$.

Proposition 5.1 ([Shl94], Theorem 4.2)**.** *Let R be any subring of $\mathbb{Q}$. Then the set of nonzero elements of R is existentially definable over R.*

This proposition implies:

Corollary 5.2. *For every ring $R \subset \mathbb{Q}$, we have that* $\text{HTP}(\mathbb{Q}) \leq_T \text{HTP}(R)$.

Proof. Every element of $\mathbb{Q}$ can be written as a ratio x/y with $x, y \in R, y \neq 0$. Thus we can replace all the variables ranging over $\mathbb{Q}$ by quotients of variables ranging over R and add equations stipulating that the denominators are not zero using Proposition 5.1. □

In a similar fashion one can show that the following corollary is true as well.

Corollary 5.3. *For every ring $R \subset \mathbb{Q}$, every $m > 0$, and every set $A \subset \mathbb{Q}^m$ diophantine over $\mathbb{Q}$, the set $A \cap R^m$ is diophantine over R.*

This corollary will be used below to prove that an oracle for $\text{HTP}(\mathbb{Z}[\mathcal{M}^{-1}])$ also gives an oracle for $\text{HTP}(\mathbb{Z}[(\mathcal{M} - \mathcal{P}_0)^{-1}])$, for any finite set of primes $\mathcal{P}_0 \subseteq \mathcal{M}$ (Corollary 5.6).

Now, we give an effective version of Julia Robinson's result concerning the diophantine definition of elements in $\mathbb{Q}$ that are integral at a finite set of primes. This lets us decide from an $\text{HTP}(\mathbb{Q})$-oracle whether polynomials have solutions in certain semilocal rings $\mathbb{Z}[(\mathcal{P} - \{p_1, \ldots, p_n\})^{-1}]$. We show that the following result is true.

Proposition 5.4. *Let $\mathcal{P}_0 = \{p_1, \ldots, p_n\}$ be any finite set of primes. Then the set* $\text{HTP}(\mathbb{Z}[(\mathcal{P} - \mathcal{P}_0)^{-1}])$ *is computable uniformly in* $\text{HTP}(\mathbb{Q})$ *in the following sense: there exists an algorithm, using* $\text{HTP}(\mathbb{Q})$ *as an oracle, that can decide, given any*

such $\mathcal{P}_0$, whether any given polynomial with coefficients in $\mathbb{Q}$ has a solution in $\mathbb{Z}[(\mathcal{P}-\mathcal{P}_0)^{-1}]$.

Lemma 5.5. *Let $f_{a,b}$ be the polynomial*

$$f_{a,b}(x_{11},x_{12},x_{13},x_{14}) = x_{11}^2 - ax_{12}^2 - bx_{13}^2 + abx_{14}^2 - 1.$$

Then for $i \in \{1,2\}$ and $j \in \{1,2,3,4\}$:

(1) *For $p = 2$,*

$$\mathbb{Z}_{(2)} = \{2(x_{11}+x_{12}+y_{11}+y_{12}) \mid \exists x_{ij}, y_{ij} \in \mathbb{Q} : f_{3,3}(x_{1j})^2 + f_{3,3}(x_{2j})^2 + f_{2,5}(y_{1j})^2 + f_{2,5}(y_{2j})^2 = 0\}.$$

(2) *If $p \equiv 3 \bmod 8$, then*

$$\mathbb{Z}_{(p)} = \{2(x_{11}+x_{12}+y_{11}+y_{12}) \mid \exists x_{ij}, y_{ij} \in \mathbb{Q} : f_{-1,p}(x_{1j})^2 + f_{-1,p}(x_{2j})^2 + f_{2,p}(y_{1j})^2 + f_{2,p}(y_{2j})^2 = 0\}.$$

(3) *If $p \equiv 5 \bmod 8$, then*

$$\mathbb{Z}_{(p)} = \{2(x_{11}+x_{12}+y_{11}+y_{12}) \mid \exists x_{ij}, y_{ij} \in \mathbb{Q} : f_{-2p,-p}(x_{1j})^2 + f_{-2p,-p}(x_{2j})^2 + f_{2p,-p}(y_{1j})^2 + f_{2p,-p}(y_{2j})^2 = 0\}.$$

(4) *If $p \equiv 7 \bmod 8$, then*

$$\mathbb{Z}_{(p)} = \{2(x_{11}+x_{12}+y_{11}+y_{12}) \mid \exists x_{ij}, y_{ij} \in \mathbb{Q} : f_{-1,-p}(x_{1j})^2 + f_{-1,-p}(x_{2j})^2 + f_{2p,p}(y_{1j})^2 + f_{2p,p}(y_{2j})^2 = 0\}.$$

(5) *If $p \equiv 1 \bmod 8$, and if $q \equiv 3 \bmod 8$ is a prime such that $\left(\frac{p}{q}\right) = -1$, then*

$$\mathbb{Z}_{(p)} = \{2(x_{11}+x_{12}+y_{11}+y_{12}) \mid \exists x_{ij}, y_{ij} \in \mathbb{Q} : f_{-2p,q}(x_{1j})^2 + f_{-2p,q}(x_{2j})^2 + f_{2p,q}(y_{1j})^2 + f_{2p,q}(y_{2j})^2 = 0\}.$$

Proof. We first prove part (1) in detail. The set

$$S_{a,b} := \{2x_1 \in \mathbb{Q} | \exists x_2, x_3, x_4 \in \mathbb{Q} : f_{a,b}(x_1,x_2,x_3,x_4) = 0\}$$

is equal to the set of norm-1 elements of the twisted quaternion algebra $\mathbb{Q}\cdot 1 \oplus \mathbb{Q}\cdot\alpha \oplus \mathbb{Q}\cdot\beta \oplus \mathbb{Q}\cdot\alpha\beta$ with $\alpha^2 = a$, $\beta^2 = b$, and $\alpha\beta = -\beta\alpha$. By [Koe16, Proposition 10(a)], we know that

$$\mathbb{Z}_{(2)} = (S_{3,3} + S_{3,3}) + (S_{2,5} + S_{2,5}),$$

from which the conclusion follows.

The rest of the lemma follows by similar methods of proof: parts (2) to (4) are [Koe16, Proposition 10(b)], and part (5) is [Koe16, Proposition 10(c)]. □

For simplicity in notation, let $q \in \{1,2,3,5,7\}$ satisfy $q \equiv p \bmod 8$, and let f_q be the polynomial that defines $\mathbb{Z}_{(p)}$ as in the previous lemma. Now we can prove Proposition 5.4.

Proof of Proposition 5.4. Let $\mathcal{P}_0 = \{p_1,\dots,p_n\}$ and $Q(Z_1,\dots,Z_k) \in \mathbb{Z}[Z_1,\dots,Z_k]$. We need to ascertain whether $Q(Z_1,\dots,Z_K) = 0$ has any solutions in $\mathbb{Z}[\overline{\mathcal{P}_0}^{-1}]$. We proceed in the following fashion:

(1) If p_i is congruent to 1 modulo 8, choose a prime q_i such that $q_i \equiv 3 \bmod 8$ and $\left(\frac{p_i}{q_i}\right) = -1$.

(2) Consider the following system, which can be regarded as a single polynomial using sums of squares:

$$\begin{cases} Q(Z_1,\dots,Z_k)=0, \\ f_{(p_i \bmod 8)}(Z_i,x_{i2},x_{i3},x_{i4})=0, 1\le i\le n. \end{cases} \tag{5.1}$$

The above system has rational solutions $\{Z_i, x_{ij}\}$ if and only if $Q(Z_1,\dots,Z_k)=0$ has rational solutions integral at $p_1,\dots,p_n$, by the construction of the polynomials f_ℓ, $\ell\in\{1,2,3,5,7\}$. □

We also need Proposition 5.4 in a more general setting, since the general case of our construction in section 3.2 gives rings R such that $\mathrm{HTP}(R)\equiv_T \mathrm{HTP}(\mathbb{Z}[\mathcal{M}^{-1}])$.

Corollary 5.6. *Let $\mathcal{M}$ be any set of primes and let $\mathcal{P}_0=\{p_1,\dots,p_n\}\subseteq\mathcal{M}$ be any finite set of primes from $\mathcal{M}$. Then $\mathrm{HTP}(\mathbb{Z}[(\mathcal{M}-\mathcal{P}_0)^{-1}])$ is computable uniformly in $\mathrm{HTP}(\mathbb{Z}[\mathcal{M}^{-1}])$ in the following sense: there exists an algorithm, using $\mathrm{HTP}(\mathbb{Z}[\mathcal{M}^{-1}])$ as an oracle, that can decide, given any $\mathcal{P}_0$, whether any given polynomial with coefficients in $\mathbb{Z}[(\mathcal{M}-\mathcal{P}_0)^{-1}]$ has a solution in $\mathbb{Z}[(\mathcal{M}-\mathcal{P}_0)^{-1}]$.*

Proof. This is an immediate consequence of Corollary 5.3. □

6. Number fields

In this section, we discuss the extensions of our results to number fields. Throughout this section, K will denote a number field and $\mathcal{O}_K$ its ring of integers. Let $\mathcal{P}_K$ denote the set of finite primes of K, and if $\mathcal{S}$ is a set of prime ideals, let $\mathcal{O}_{K,\mathcal{S}}$ denote the ring of $\mathcal{S}$-integers, which is defined by

$$\mathcal{O}_{K,\mathcal{S}}=\{x\in K : \mathrm{ord}_{\mathfrak{p}}x\ge 0 \text{ for all } \mathfrak{p}\notin\mathcal{S}\}.$$

We first give a brief survey of what is known about Hilbert's Tenth Problem over finite extensions of $\mathbb{Q}$.

6.1. **Hilbert's Tenth Problem for subrings of number fields.** Hilbert's Tenth Problem for the ring of integers of a number field has been resolved in many cases, but undecidability for the ring of integers of *any* number field is only known under the assumption that the Shafarevich-Tate conjecture holds [MR10]. The theorem below summarizes what is known.

Theorem 6.1. *The ring $\mathbb{Z}$ has a diophantine definition and Hilbert's Tenth Problem is undecidable over the rings of integers of the following fields:*

- *Extensions of degree 4 that are not totally real and containing a subfield K such that $[K:\mathbb{Q}]=2$ or totally real number fields and their extensions of degree 2. (See* [DL78] *and* [Den80]*.) These fields include all Abelian extensions.*
- *Number fields with exactly one pair of nonreal embeddings. (See* [Phe88] *and* [Shl89]*.)*
- *Any number field K such that there exists an elliptic curve E of positive rank defined over $\mathbb{Q}$ with $[E(K):E(\mathbb{Q})]<\infty$. (See* [Poo02] *and* [Shl08]*.)*
- *Any number field K such that there exists an elliptic curve of rank 1 over K and an Abelian variety of positive rank over $\mathbb{Q}$ keeping its rank over K. (See* [CPZ05]*.)*

To measure the "size" of a set of primes of a number field one can also use the natural density defined below for a number field.

Definition 6.2. Let $\mathcal{S} \subseteq \mathcal{P}_K$. The *natural density* of $\mathcal{S}$ is defined to be the limit

$$\lim_{X\to\infty} \frac{\#\{\mathfrak{p} \in S : N\mathfrak{p} \leq X\}}{\#\{\mathfrak{p} \in \mathcal{P}_K : N\mathfrak{p} \leq X\}}$$

if it exists. (Here $N\mathfrak{p}$ denotes the size of the residue field of the prime or its norm.) If the limit above does not exist, one can talk about *upper* density by substituting lim sup for lim or *lower* density by substituting lim inf for lim.

The proposition below summarizes what we know about $\mathcal{S}$-integers of number fields.

Theorem 6.3.

- *If K is a totally real number field, an extension of degree 2 of a totally real number field or such that there exists an elliptic curve defined over $\mathbb{Q}$ and of the same positive rank over K and $\mathbb{Q}$, then for any $\varepsilon > 0$, there exists a set $\mathcal{W}$ of primes of K whose natural density is bigger than $1-[K:\mathbb{Q}]^{-1}-\varepsilon$ and such that $\mathbb{Z}$ has a diophantine definition over $O_{K,\mathcal{W}}$, thus implying that Hilbert's Tenth Problem is undecidable over $O_{K,\mathcal{W}}$. (See* [Shl97], [Shl02], [Shl00] *and* [Shl08]*.)*
- *Assume there is an elliptic curve defined over K with K-rank equal to 1. For every $t > 1$ and every collection $\delta_1, \ldots, \delta_t$ of nonnegative computable real numbers adding up to 1, the set of primes of K may be partitioned into t mutually disjoint computable subsets $\mathcal{S}_1, \ldots, \mathcal{S}_t$ of natural densities $\delta_1, \ldots, \delta_t$, respectively, with the property that $\mathbb{Z}$ admits a diophantine model in each ring $O_{K,\mathcal{S}_i}$. In particular, Hilbert's Tenth Problem is undecidable for each ring $O_{K,\mathcal{S}_i}$. (See* [PS05], [EE09], [Per11], [EES11]*.)*

In [MR10], Mazur and Rubin showed that if the Shafarevich-Tate conjecture holds, then for every cyclic extension of number fields M/K of prime degree there always exists an elliptic curve defined over K with K-rank and M-rank equal to one. So if the Shafarevich-Tate conjecture holds for all number fields, one can show the undecidability of Hilbert's Tenth Problem for the ring of integers and big rings for all number fields.

6.2. **Presenting primes of a number field in a computable manner.** Before proceeding with generalizations of our results, we need to discuss how we are going to present primes of number fields, which, unlike primes of $\mathbb{Q}$, do not necessarily correspond to a single number but are ideals, i.e. infinite subsets of the field. This data can be kept track of, since rings of integers are Dedekind domains, which have finite presentations.

Given a prime $\mathfrak{p}$ of K, let $a(\mathfrak{p}) \in K$ be such that $\mathrm{ord}_{\mathfrak{p}} a(\mathfrak{p}) = -1$, $a(\mathfrak{p})$ has nonnegative order at all other primes of K, and for every K-prime $\mathfrak{q} \neq \mathfrak{p}$, conjugate to $\mathfrak{p}$ over $\mathbb{Q}$, we have that $\mathrm{ord}_{\mathfrak{q}} a(\mathfrak{p}) = 0$. The proof of the following proposition can be found in [BS96].

Proposition 6.4. *Given a number field K, the following statements are true:*

(1) *There exists a computable procedure which outputs the following information for each rational prime p: $(a(\mathfrak{p}_1), e_1, f_1, \ldots, a(\mathfrak{p}_m), e_m, f_m)$, where $p = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_m^{e_m}$ is the factorization of p (the prime ideal corresponding to p, really) in K, and f_i is the relative degree of $\mathfrak{p}_i$ over p.*

(2) *There exists a computable procedure that for each $x \in K$ outputs the following information: $(q_1, a(\mathfrak{q}_1), ord_{\mathfrak{q}_1} x, \ldots, q_m, a(\mathfrak{q}_m), ord_{\mathfrak{q}_m} x)$, where q_i is a rational prime number, $\mathfrak{q}_i$ is a prime of K, and $q_i = \mathfrak{q}_i \cap \mathbb{Z}$. Moreover, for each K-prime $\mathfrak{q}$ such that $a(\mathfrak{q})$ is not on the list, we have that $ord_{\mathfrak{q}} x = 0$.*
(3) *There exists a computable procedure that for each $x \in K$ determines whether all of the real conjugates of x are positive.*

Using the proposition above we identify a prime $\mathfrak{p}$ of a number field K with a pair $(p, a(\mathfrak{p}))$, where $p = \mathfrak{p} \cap \mathbb{Z}$. We will fix a basis for K over $\mathbb{Q}$ and represent each $a(\mathfrak{p})$ by its rational coordinates with respect to the chosen basis. So finally a prime of K will correspond to an $(n+1)$-tuple of rational numbers, where $[K : \mathbb{Q}] = n$. Given a set of K-primes, we will now say that it is computable or c.e. if the corresponding set of $n+1$-tuples of rational numbers is computable or c.e.

6.3. **Effective diophantine definition of integrality at a finite set of primes.** Let K be a number field, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be a finite set of primes of K. In this section, we would like to prove the analogue of Proposition 5.4; that is,

Proposition 6.5. *Let $\mathcal{P}_0 = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ be any finite set of primes. Let $R = \bigcap_{1 \le i \le n} \mathcal{O}_{\mathfrak{p}_i} \cap K$. Then $\mathrm{HTP}(R)$ is computable uniformly in $\mathrm{HTP}(K)$, in the sense of Proposition 5.4.*

Let $a, b \in K^\times$ be chosen as in [Par13, Lemma 3.19]. Then we have the Artin homomorphism that is defined on the prime ideals as

$$\Psi : I^S \to \mathrm{Gal}(K(\sqrt{a}, \sqrt{b})/K) \cong \{\pm 1\}^2$$
$$\mathfrak{p} \mapsto \left(\left(\frac{a}{\mathfrak{p}}\right), \left(\frac{b}{\mathfrak{p}}\right) \right)$$

and extended linearly to all ideals in I^S, where S consists of all the infinite places and the places lying over $2ab$.

Lemma 6.6. *There exists a polynomial $f_{(1,1)} \in K[t, y_1, y_2, x_1, \ldots, x_m]$ for some $m \ge 1$ such that for all prime ideals $\mathfrak{p} \in I^S$ satisfying $\Psi(\mathfrak{p}) = (1,1)$, there exist elements $y_{\mathfrak{p},1}, y_{\mathfrak{p},2} \in K$ such that*

$$\mathcal{O}_{\mathfrak{p}} \cap K = \{t \in K : (\exists x_1, \ldots, x_m)\ f_{(1,1)}(t, y_{\mathfrak{p},1}, y_{\mathfrak{p},2}, x_1, \ldots, x_m) = 0\}.$$

Proof. This is [Par13, Lemma 3.25(c)]. □

Lemma 6.7. *Let $\sigma \in \{\pm 1\}^2$ with $\sigma \ne (1,1)$. Then there exists a polynomial $f_\sigma \in K[t, y, x_1, \ldots, x_{m_\sigma}]$ for some $m_\sigma \ge 1$ such that for all prime ideals $\mathfrak{p} \in I^S$ satisfying $\Psi(\mathfrak{p}) = \sigma$, there exists an element $y_{\mathfrak{p}} \in K$ such that*

$$\mathcal{O}_{\mathfrak{p}} \cap K = \{t \in K : (\exists x_1, \ldots, x_m)\ f_{(1,1)}(t, y_{\mathfrak{p}}, x_1, \ldots, x_m) = 0\}.$$

Proof. With [Par13, Proposition 2.3 and Definition 3.10], all that remains to do is to describe an algorithm that finds the element $y_{\mathfrak{p}}$ such that the Hilbert symbols satisfy $(y_{\mathfrak{p}}, a)_{\mathfrak{p}} = (y_{\mathfrak{p}}, b)_{\mathfrak{p}} = -1$, but such that at least one of $(y_{\mathfrak{p}}, a)_{\mathfrak{q}}$ or $(y_{\mathfrak{p}}, b)_{\mathfrak{q}}$ is equal to 1 for all places $\mathfrak{q} \ne \mathfrak{p}$. Such choice of y exists due to [Par13, Theorem 3.7]. Since there are explicit methods for computing Hilbert symbols, one enumerates all elements of K and computes the Hilbert symbols $(y, a)_{\mathfrak{q}}$ and $(y, b)_{\mathfrak{q}}$ at the places $\mathfrak{q}$ that satisfy $v_{\mathfrak{q}}(y) \equiv 1 \bmod 2$, until we find such a y (we only need to check finitely many places $\mathfrak{q}$ because of [Par13, Lemma 3.8]). Enumerating through the y's must

terminate, because of the existence of such a y. The f_σ can be described explicitly in terms of $y_{\mathfrak{p}}$, as in the previous subsection. □

Lemma 6.8. *For any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, the localization ring $(\mathcal{O}_K)_{\mathfrak{p}}$ is diophantine.*

Proof. This is [PS05, Proposition 2.2]. □

Now the proof of Proposition 6.5 proceeds exactly like that of Proposition 5.4: Given a polynomial $Q \in K[Z_1, \ldots, Z_k]$, we impose integrality conditions on the Z_ℓ at each of the primes $\mathfrak{p}_i \in \mathcal{P}_0$ using Lemma 6.6 and Lemma 6.7, as in Proposition 5.4.

6.4. **Turing reducibility between Hilbert's Tenth Problem for subrings of a number field K.** In this section we use Proposition 6.5 to prove results concerning big subrings of number fields along the lines of similar results for $\mathbb{Q}$. We apply this proposition in the same manner as over $\mathbb{Q}$ to construct rings R with $\mathrm{HTP}(R) \equiv_T \mathrm{HTP}(K)$.

There are several well known and easy to prove Turing relations between several types of rings and fields:

Proposition 6.9.

(1) $\mathrm{HTP}(K) \leq_T \mathrm{HTP}(\mathbb{Q})$.
(2) *If $\mathcal{S}$ is a cofinite set of K-primes, then* $\mathrm{HTP}(\mathcal{O}_{K,\mathcal{S}}) \equiv_T \mathrm{HTP}(K)$.
(3) *For any set of K-primes $\mathcal{S}$, including an empty set, we have* $\mathrm{HTP}(K) \leq_T \mathrm{HTP}(\mathcal{O}_{K,\mathcal{S}})$.
(4) *For any set $\mathcal{S}$ of K-primes with a diophantine definition or model of $\mathbb{Z}$, we have* $\mathrm{HTP}(\mathcal{O}_{K,\mathcal{S}}) \equiv_T \mathrm{HTP}(\mathbb{Z})$.
(5) *For any c.e. set of K-primes $\mathcal{S}$, possibly empty, we have* $\mathrm{HTP}(\mathcal{O}_{K,\mathcal{S}}) \leq_T \mathrm{HTP}(\mathbb{Z})$.

We now state our new results, for which we omit the proofs, since they are identical to the proofs of the results for $\mathbb{Q}$. The upper and lower relative natural density can be defined in an analogous manner for sets of primes of number fields, as it was for sets of rational primes. It will, in general, also depend on the underlying set as well as its ordering, as is the case for $\mathbb{Q}$.

Theorem 6.10. *If $\mathcal{W}$ is a c.e. set of primes of a number field K, then it contains a c.e. subset $\mathcal{S}$ such that the relative upper density of $\mathcal{V} = \mathcal{W} - \mathcal{S}$ is 1 and* $\mathrm{HTP}(\mathcal{O}_{K,\mathcal{W}}) \geq_T \mathrm{HTP}(\mathcal{O}_{K,\mathcal{S}})$.

Corollary 6.11. *There exists a sequence $\mathcal{P} = \mathcal{W}_0 \supset \mathcal{W}_1 \supset \mathcal{W}_2 \ldots$ of c.e. sets of primes of a number field K (with $\mathcal{P}$ denoting the set of all primes of K) such that*

(1) $\mathrm{HTP}(\mathcal{O}_{K,\mathcal{W}_i}) \equiv_T \mathrm{HTP}(K) \leq_T \mathrm{HTP}(\mathbb{Q})$ *for $i \in \mathbb{Z}_{>0}$.*
(2) *$\mathcal{W}_{i-1} - \mathcal{W}_i$ has the relative upper density (with respect to $\mathcal{W}_{i-1}$) equal to 1 for all $i \in \mathbb{Z}_{>0}$.*
(3) *The lower density of $\mathcal{W}_i$ is 0, for all $i \in \mathbb{Z}_{>0}$.*

Corollary 6.12. *There exists a computably enumerable subset $\mathcal{W}$ of K-primes, of lower natural density 0, such that* $\mathrm{HTP}(\mathbb{Q}) \geq_T \mathrm{HTP}(K) \equiv_T \mathrm{HTP}(\mathcal{O}_{K,\mathcal{W}})$.

Theorem 6.13. *For each computable real number r between 0 and 1 there is a c.e. set $\mathcal{S}$ of primes of K such that the lower density of $\mathcal{S}$ is r and* $\mathrm{HTP}(\mathcal{O}_{K,\mathcal{S}}) \equiv_T \mathrm{HTP}(K) \leq_T \mathrm{HTP}(\mathbb{Q})$.

Theorem 6.14. *For every computably enumerable set $B \subset \mathbb{Z}_{>0}$ with $\mathrm{HTP}(\mathbb{Q}) \leq_T B$, there exists a computably presentable ring $R = \mathcal{O}_{K,\mathcal{S}}$, with $\mathcal{S}$ a computably enumerable subset of primes of K of lower density 0, such that $\mathcal{S} \equiv_T R \equiv_T \mathrm{HTP}(R) \equiv_T B$. (By setting $B \equiv_T \mathrm{HTP}(\mathbb{Q})$, we can thus make $\mathrm{HTP}(R) \equiv_T \mathrm{HTP}(\mathbb{Q})$, of course.)*

Theorem 6.15. *For every positive integer m, the set of all K-primes $\mathcal{P}$ can be represented as a union of pairwise disjoint sets $\mathcal{S}_1, \ldots, \mathcal{S}_m$, each of upper density 1 and such that for all i we have that $\mathrm{HTP}(\mathcal{O}_{K,\mathcal{S}_i}) \equiv_T \mathrm{HTP}(K) \leq_T \mathrm{HTP}(\mathbb{Q})$ and $\mathcal{S}_i \leq_T \mathrm{HTP}(K)$.*

Theorem 6.16. *There exist infinitely many subsets $\mathcal{S}_1, \mathcal{S}_2, \ldots$ of the set $\mathcal{P}$ of K-primes, all of lower density 0, all computable uniformly from an $\mathrm{HTP}(K)$-oracle (so that the rings $R_j = \mathcal{O}_{K,\mathcal{S}_j}$ are also uniformly computable below $\mathrm{HTP}(K)$), which have $\bigcup_j \mathcal{S}_j = \mathcal{P}$ and $\mathcal{S}_i \cap \mathcal{S}_j = \emptyset$ for all $i < j$, and such that $\mathrm{HTP}(R_j) \equiv_T \mathrm{HTP}(K)$ for every j.*

Acknowledgments

This project was initiated at a workshop held at the American Institute of Mathematics after an extended conversation with Tom Scanlon. The authors are also grateful for suggestions and corrections from the anonymous referee.

References

[BS96] Eric Bach and Jeffrey Shallit, *Algorithmic number theory. Vol. 1*: *Efficient algorithms*, Foundations of Computing Series, MIT Press, Cambridge, MA, 1996. MR1406794

[CPZ05] Gunther Cornelissen, Thanases Pheidas, and Karim Zahidi, *Division-ample sets and the Diophantine problem for rings of integers* (English, with English and French summaries), J. Théor. Nombres Bordeaux **17** (2005), no. 3, 727–735. MR2212121

[CZ00] Gunther Cornelissen and Karim Zahidi, *Topology of Diophantine sets: remarks on Mazur's conjectures*, Hilbert's tenth problem: relations with arithmetic and algebraic geometry (Ghent, 1999), Contemp. Math., vol. 270, Amer. Math. Soc., Providence, RI, 2000, pp. 253–260, DOI 10.1090/conm/270/04377. MR1802017

[Den79] J. Denef, *The Diophantine problem for polynomial rings of positive characteristic*, Logic Colloquium '78 (Mons, 1978), Stud. Logic Foundations Math., vol. 97, North-Holland, Amsterdam-New York, 1979, pp. 131–145. MR567668

[Den80] J. Denef, *Diophantine sets over algebraic integer rings. II*, Trans. Amer. Math. Soc. **257** (1980), no. 1, 227–236, DOI 10.2307/1998133. MR549163

[DL78] J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers*, J. London Math. Soc. (2) **18** (1978), no. 3, 385–391, DOI 10.1112/jlms/s2-18.3.385. MR518221

[DPR61] Martin Davis, Hilary Putnam, and Julia Robinson, *The decision problem for exponential diophantine equations*, Ann. of Math. (2) **74** (1961), 425–436, DOI 10.2307/1970289. MR0133227

[Eis03] Kirsten Eisenträger, *Hilbert's tenth problem for algebraic function fields of characteristic 2*, Pacific J. Math. **210** (2003), no. 2, 261–281, DOI 10.2140/pjm.2003.210.261. MR1988534

[Eis12] Kirsten Eisenträger, *Hilbert's Tenth Problem for function fields of varieties over algebraically closed fields of positive characteristic*, Monatsh. Math. **168** (2012), no. 1, 1–16, DOI 10.1007/s00605-011-0364-7. MR2971736

[EE09] Kirsten Eisenträger and Graham Everest, *Descent on elliptic curves and Hilbert's tenth problem*, Proc. Amer. Math. Soc. **137** (2009), no. 6, 1951–1959, DOI 10.1090/S0002-9939-08-09740-2. MR2480276

[EES11] Kirsten Eisenträger, Graham Everest, and Alexandra Shlapentokh, *Hilbert's tenth problem and Mazur's conjectures in complementary subrings of number fields*, Math. Res. Lett. **18** (2011), no. 6, 1141–1162, DOI 10.4310/MRL.2011.v18.n6.a7. MR2915472

[ES09] Kirsten Eisenträger and Alexandra Shlapentokh, *Undecidability in function fields of positive characteristic*, Int. Math. Res. Not. IMRN **21** (2009), 4051–4086, DOI 10.1093/imrn/rnp079. MR2549950

[ES16] Kirsten Eisenträger and Alexandra Shlapentokh, *Hilbert's Tenth Problem over function fields of positive characteristic not containing the algebraic closure of a finite field*, to appear in J. European Math. Soc.

[Fri57] Richard M. Friedberg, *Two recursively enumerable sets of incomparable degrees of unsolvability (solution of Post's problem, 1944)*, Proc. Nat. Acad. Sci. U.S.A. **43** (1957), 236–238. MR0084474

[Koe16] Jochen Koenigsmann, *Defining $\mathbb{Z}$ in $\mathbb{Q}$*, Ann. of Math. (2) **183** (2016), no. 1, 73–93, DOI 10.4007/annals.2016.183.1.2. MR3432581

[Lan70] Serge Lang, *Algebraic number theory*, Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Don Mills, Ont., 1970. MR0282947

[Mat70] Ju. V. Matijasevič, *The Diophantineness of enumerable sets* (Russian), Dokl. Akad. Nauk SSSR **191** (1970), 279–282. MR0258744

[Maz92] Barry Mazur, *The topology of rational points*, Experiment. Math. **1** (1992), no. 1, 35–45. MR1181085

[MR10] B. Mazur and K. Rubin, *Ranks of twists of elliptic curves and Hilbert's tenth problem*, Invent. Math. **181** (2010), no. 3, 541–575, DOI 10.1007/s00222-010-0252-0. MR2660452

[Mil08] Russell Miller, *Computable fields and Galois theory*, Notices Amer. Math. Soc. **55** (2008), no. 7, 798–807. MR2436510

[Muc56] A. A. Mučnik, *On the unsolvability of the problem of reducibility in the theory of algorithms* (Russian), Dokl. Akad. Nauk SSSR (N.S.) **108** (1956), 194–197. MR0081859

[Par13] Jennifer Park, *A universal first-order formula defining the ring of integers in a number field*, Math. Res. Lett. **20** (2013), no. 5, 961–980, DOI 10.4310/MRL.2013.v20.n5.a12. MR3207365

[Per11] Stefan Perlega, *Additional results to a theorem of Eisenträger and Everest*, Arch. Math. (Basel) **97** (2011), no. 2, 141–149, DOI 10.1007/s00013-011-0277-7. MR2820576

[Phe88] Thanases Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers*, Proc. Amer. Math. Soc. **104** (1988), no. 2, 611–620, DOI 10.2307/2047021. MR962837

[Phe87i] Thanases Pheidas, *An undecidability result for power series rings of positive characteristic*, Proc. Amer. Math. Soc. **99** (1987), no. 2, 364–366, DOI 10.2307/2046642. MR870802

[Phe87ii] Thanases Pheidas, *An undecidability result for power series rings of positive characteristic. II*, Proc. Amer. Math. Soc. **100** (1987), no. 3, 526–530, DOI 10.2307/2046442. MR891158

[Phe91] Thanases Pheidas, *Hilbert's tenth problem for fields of rational functions over finite fields*, Invent. Math. **103** (1991), no. 1, 1–8, DOI 10.1007/BF01239506. MR1079837

[Poo02] Bjorn Poonen, *Using elliptic curves of rank one towards the undecidability of Hilbert's tenth problem over rings of algebraic integers*, Algorithmic number theory (Sydney, 2002), Lecture Notes in Comput. Sci., vol. 2369, Springer, Berlin, 2002, pp. 33–42, DOI 10.1007/3-540-45455-1_4. MR2041072

[Poo03] Bjorn Poonen, *Hilbert's tenth problem and Mazur's conjecture for large subrings of $\mathbb{Q}$*, J. Amer. Math. Soc. **16** (2003), no. 4, 981–990, DOI 10.1090/S0894-0347-03-00433-8. MR1992832

[PS05] Bjorn Poonen and Alexandra Shlapentokh, *Diophantine definability of infinite discrete nonarchimedean sets and Diophantine models over large subrings of number fields*, J. Reine Angew. Math. **588** (2005), 27–47, DOI 10.1515/crll.2005.2005.588.27. MR2196727

[Rob49] Julia Robinson, *Definability and decision problems in arithmetic*, J. Symbolic Logic **14** (1949), 98–114, DOI 10.2307/2266510. MR0031446

[Rog67] Hartley Rogers Jr., *Theory of recursive functions and effective computability*, McGraw-Hill Book Co., New York-Toronto, Ont.-London, 1967. MR0224462

[Shl89] Alexandra Shlapentokh, *Extension of Hilbert's tenth problem to some algebraic number fields*, Comm. Pure Appl. Math. **42** (1989), no. 7, 939–962, DOI 10.1002/cpa.3160420703. MR1008797

[Shl94] Alexandra Shlapentokh, *Diophantine classes of holomorphy rings of global fields*, J. Algebra **169** (1994), no. 1, 139–175, DOI 10.1006/jabr.1994.1276. MR1296586

[Shl97] Alexandra Shlapentokh, *Diophantine definability over some rings of algebraic numbers with infinite number of primes allowed in the denominator*, Invent. Math. **129** (1997), no. 3, 489–507, DOI 10.1007/s002220050170. MR1465332

[Shl00] Alexandra Shlapentokh, *Defining integrality at prime sets of high density in number fields*, Duke Math. J. **101** (2000), no. 1, 117–134, DOI 10.1215/S0012-7094-00-10115-9. MR1733734

[Shl02] Alexandra Shlapentokh, *Diophantine definability and decidability in large subrings of totally real number fields and their totally complex extensions of degree 2*, J. Number Theory **95** (2002), no. 2, 227–252. MR1924099

[Shl08] Alexandra Shlapentokh, *Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers*, Trans. Amer. Math. Soc. **360** (2008), no. 7, 3541–3555, DOI 10.1090/S0002-9947-08-04302-X. MR2386235

[Soa87] Robert I. Soare, *Recursively enumerable sets and degrees*: *A study of computable functions and computably generated sets*, Perspectives in Mathematical Logic, Springer-Verlag, Berlin, 1987. MR882921

[Vid94] Carlos R. Videla, *Hilbert's tenth problem for rational function fields in characteristic* 2, Proc. Amer. Math. Soc. **120** (1994), no. 1, 249–253, DOI 10.2307/2160192. MR1159179

Department of Mathematics, The Pennsylvania State University, University Park, Pennsylvania 16802

E-mail address: eisentra@math.psu.edu

URL: http://www.personal.psu.edu/kxe8/

Department of Mathematics, Queens College, 65-30 Kissena Boulevard, Queens, New York 11367 – and – Ph.D. Programs in Mathematics and Computer Science, CUNY Graduate Center, 365 Fifth Avenue, New York, New York 10016

E-mail address: Russell.Miller@qc.cuny.edu

URL: http://qcpages.qc.cuny.edu/~rmiller

Department of Mathematics, University of Michigan, Ann Arbor, Michigan 48109

E-mail address: jmypark@umich.edu

URL: www-personal.umich.edu/~jmypark/

Department of Mathematics, East Carolina University, Greenville, North Carolina 27858

E-mail address: shlapentokha@ecu.edu