ON THE COMPUTABILITY OF THE UNIFORM KRULL INTERSECTION THEOREM

CHRIS J. CONIDIS

Abstract. We examine the complexity of the dichotomous decision procedure that divides the standard proof of the Krull Intersection Theorem (KIT) into two cases by examining the computability complexity of a uniform version of KIT for infinite uniformly computable sequences of integral domains. In this context we show that, while the standard decision procedure found in many texts can only be obtained via the ability to (uniformly) answer two-quantifier questions via $\mathbf{0}''$, there is a modified procedure of lesser complexity that also yields KIT in this context.

1. Introduction

The Hilbert Basis Theorem [Hil90] for polynomial rings over commutative rings is considered one of the first nonconstructive mathematical arguments, and its effective context was examined first by Buchberger [Buc74], and then by others such as Simpson [Sim88] and [Hat94]. Generally speaking, the Hilbert Basis Theorem says that if R is a Noetherian[1] commutative ring (with identity), then the polynomial ring $R[X]$ is also Noetherian; by induction it follows that the multivariate polynomial ring $R[X_0, X_1, \ldots, X_n]$ is also Noetherian, and a more general form of the theorem pertains to finitely generated modules over Noetherian rings. The standard proof essentially takes an infinite sequence of polynomials in $R[X]$ such that no polynomial is generated via its sequential predecessors (over $R[X]$), and produces a corresponding infinite sequence of "minimal" leading $R-$coefficients (i.e. coefficients corresponding to polynomials of minimal degree, modulo sequential predecessor polynomials) such that no coefficient is in the $R-$span of its sequential predecessors. Finding these minimal coefficients in general requires the utilization of nonconstructive methods.

Two consequences of the Hilbert Basis Theorem, whose proofs always seem to require it, are the Artin-Rees Lemma and the Krull Intersection Theorem. More specifically, the Artin-Rees Lemma seems to require the Hilbert Basis Theorem, and is then used in the proof of the Krull Intersection Theorem. Moreover, the proof of the Krull Intersection Theorem is of a dichotomous nature in that it is essentially divided into two cases; one case utilizes Nakayama's Lemma, while the other case employs the Artin-Rees Lemma. Moreover, from a constructive persepective, the witnesses (chains) satisfying the conclusion of the theorem that are produced exist in "different parts" of the ring; i.e. the construction takes place in a different subset of the ring.

Sometimes a logical analysis of a theorem from classical mathematics can yield new insights and bring new aspects of the theorem to light that may have corresponded to previous intuitions not yet formalized. For example, in the algebraic context, a well-known result of Friedman, Simpson, and Smith [FSS83, FSS85] that examines the complexity of the theorem "every ring has a prime ideal" in the context of Reverse Mathematics and show it to be weaker

2010 *Mathematics Subject Classification.* Primary 03F35;
Secondary 03D80, 13E10.

Key words and phrases. Computability Theory, Reverse Mathematics, Proof Theory, Definability, Commutative Ring Theory, Neotherian Ring Theory, Krull Intersection Theorem, Artin-Rees Lemma.

[1] R is *Noetherian* if every ascending chain of ideals eventually stabilizes.

than saying "every ring has a maximal ideal." From a model-theoretic perspective, [FSS83] constructs a model of Second-Order Arithmetic in which every ring has a prime ideal, but not every ring has a maximal ideal. A similar result is achieved in [Con19] for the theorem that says "Every Artinian ring is Noetherian," where the author shows the significant role that annihilator ideals play in Artinian rings.

1.1. **This Article.** The purpose of this article is to examine the complexity of this dichotomy from an effective perspective. In particular, we will show that, while the decision procedure for the classical dichotomy has a Turing complexity corresponding to sets that are solutions for problems defined by two-quantifier formulas, there is a simpler alternative dichotomy of strictly weaker Turing complexity corresponding to the decision procedure that uniformly decides, for any given pair of computably enumerable sets W, V, such that $W \cup V$ is infinite, an infinite element of $\{W, V\}$.[2]

2. Background

Let $\omega = \{0, 1, 2, \ldots\}$ denote the standard natural numbers. For any sets A, B we use standard set-theoretic exponential notation $|A|$ to denote the cardinality of A, and A^B to denote the set of functions from B to A. Also, $A^{<\omega}$ denotes the set of finite sequences of $A-$elements, and for any $\alpha \in A^{<\omega}$, $|\alpha| \in \omega$ denotes the length of α while $\alpha(k) \in A$ denotes the $(k+1)^{th}$ bit of α, $0 \leq k < |\alpha|$, $k \in \omega$. For any $\alpha, \beta \in A^{<\omega}$ we write $\alpha \subseteq \beta$ to mean that α is a prefix of β; i.e. we have that $|\alpha| \leq |\beta|$ and $\alpha(k) = \beta(k)$ for all $k = 0, 1, \ldots, |\alpha| - 1$.

2.1. **Computability Theory.** We assume some familiarity with basic Computability Theory, as found in [Soa16]. Recall that $\{\varphi_e\}_{e\in\omega}$ denotes an effective (i.e. computable) enumeration of the partial computable functions that such that φ_e, $e \in \omega$, may or may not halt on a particular input $x \in \omega$, and

$$\emptyset' = \{e \in \omega : \varphi_e(e) \text{ halts}\}$$

Turing's incomputable Halting Set. We say that $X \subseteq \omega$ is *computable* whenever we can decide, for each $x \in \omega$, whether or not $x \in X$ via some total φ_e, $e \in \omega$, such that $\varphi(x) = 1$ if $x \in X$ and $\varphi_e(x) = 0$ otherwise. Also, we say that a sequence $\{X_n\}_{n\in\omega}$ is *uniformly computable* whenever there is a single algorithm with index $e \in \omega$ that computes every X_n in the sense that $\varphi_e(n, x) = 1$ whenever $x \in X_n$ and $\varphi_e(n, x) = 0$ otherwise. We also have the notion of relative computability and oracle Turing machines, denoted $\{\Phi_e\}_{e\in\omega}$. We identify $A, B \subseteq \omega$ with their respective characteristic functions $\chi_A, \chi_B \in 2^\omega$, and we say that B *computes* A, or that A *is Turing reducible to* B, whenever we have that

$$A = \Phi_e^B$$

for some $e \in \omega$, and in this case we write $A \leq_T B$. This leads to an equivalence relation $\equiv_T$ on subsets of ω such that $A \equiv_T B$, $A, B \subseteq \omega$, whenever we have that $A \leq_T B$ and $B \leq_T A$, and we call the resulting equivalence classes *Turing degrees* and denote them via boldface letters such as $\mathbf{x}$; we denote the Turing degree of $\emptyset'$ by $\mathbf{0'}$. If $X \subseteq \omega$ belongs to the Turing degree $\mathbf{x}$, then from the point of view of Computability Theory, X is essentially indistinguishable from any other $Y \in \mathbf{x}$ because $A \leq_T X$ if and only if $A \leq_T Y$, for any $A \subseteq \omega$. We also have a notion of the Halting Set relative to $A \subseteq \omega$:

$$A' = \{e \in \omega : \Phi_e^A(e) \text{ halts}\},$$

[2]More details on Computability Theory are given in the The Turing complexity for uniformly deciding which of W, V is inifnite is called PA relative to Turing's Halting Set. The way we describe it in the following section involves computing infinite paths through infinite finitely branching trees computable from Turing's Halting Set. It is well-known that these definitions are equivalent.

that allows for iterations of Turing's Halting Set; one iteration of particular relevance for us is the "double-jump"

$$\emptyset'' = \{e \in \omega : \Phi_e^{\emptyset'}(e) \text{ halts}\} \in \mathbf{0}''.$$

We say that $A \subseteq \omega$ is *computably enumerable* if it is the domain of some φ_e, namely

$$W_e = \{x \in \omega : \varphi_e(x) \text{ halts}\}.$$

Moreover, it is well-known that

$$\text{Inf} = \{e \in \omega : |W_e| = \infty\} \equiv_T \emptyset''.$$

The notion of uniform computability can be relativized to oracles A in a very natural way. Recall that there is a computable function $\psi : \omega \times \omega \to \omega$, and this allows us to speak of the computability of sets $X \subseteq \omega \times \omega$; we say that $f : \omega \to \omega$, i.e. $f \in \omega^\omega$, is computable whenever its graph is computable.

Fix a computable enumeration of finite sequences of natural numbers, $\omega^{<\omega}$. It follows that the prefix relation on $\omega^{<\omega}$ is computabe, and we say that $T \subseteq \omega^{<\omega}$ is a *tree* whenever it is closed under the prefix relation. We say that T is *finitely branching* if there is a $T-$computable function (i.e. $f \leq_T T$), $f : T \to \omega$, such that for any $\alpha \in T$, the one-bit extension $\alpha x \notin T$, for any $x > f(\alpha)$. In other words, $f(\alpha) \in \omega$ bounds the single extension bits of $\alpha \in T$. A well-known combinatorial result known as König's Lemma based on iterating the Infinite Pigeonhole Principle[3] says that any infinite finitely branching tree $T \subseteq \omega$, $|T| = \infty$, has an infinite path $f \in \omega^\omega$ such that for each $k \in \omega$,

$$\alpha_k = \langle f(0), f(1), \ldots, f(k)\rangle \in T \subseteq \omega^{<\omega}.$$

The next definition is standard.

Definition 2.1. *Given $A \subseteq \omega$, we say that $\mathbf{x}$ is <u>PA relative to A</u> whenever every $A-$computable tree $T \subseteq \omega^{<\omega}$ has an infinite path $f \in \omega^\omega$ such that $f \leq_T \mathbf{x}$.*

The technique of diagonalization allows one to construct, for any Turing degree $\mathbf{x}$, an infinite $\mathbf{x}-$computable binary-branching tree with no $\mathbf{x}-$computable path. Therefore, if $\mathbf{x}$ is PA Turing degree relative to $A \subseteq \omega$, then $\mathbf{x}$ cannot be computable via the oracle A. However, a well-known consequence of the Jockusch-Soare Low Basis Theorem [JS74] says that, for any given set $A \subseteq \omega$, there is a Turing degree $\mathbf{x}$ that is PA relative to A and <u>low over A</u>, i.e. $\mathbf{x}$ computes A and $\mathbf{x}' \equiv A'$. Since $\mathbf{x} <_T \mathbf{x}'$ for any Turing degree $\mathbf{x}$, there is a Turing degree $\mathbf{x}$ that is PA over $\mathbf{0}'$ and

$$\mathbf{x} <_T \mathbf{x}' \equiv_T \mathbf{0}''.$$

In the context of this article, the standard dichotomous proof has Turing complexity $\mathbf{0}''$ (see Theorem 3.1 below), while our alternative dichotomous proof has the stictly weaker complexity $\mathbf{x}$ (Theorem 4.1). Thus, the alternative dichotomy is of a strictly weaker logical complexity than the standard one.

Our computable analysis of the alternative dichotomous proof of the Krull Intersection Theorem is facilitated by those Turing degrees $\mathbf{x}$ that are PA relative to Turing's Halting Set $\emptyset'$. Taking $\emptyset'$ as an oracle essentially allows the algorithms $\Phi_e^{\emptyset'}$ to have access to information that is the solution set to any question given by a single quantifier $(\forall, \exists)$ over a computable predicate; one example is the characterization of $\emptyset'$ itself given via the solution set

$$\emptyset' = \{e \in \omega : (\exists s \in \omega)[\Phi_e(e) \text{ halts after } s-\text{many steps}]\}.$$

Part of our construction in the alternative dichotomous proof of KIT, based on the Artin-Rees Lemma, will involve constructing an infinite finitely branching tree $T \in \mathbf{0}'$ all of whose infinite paths compute strictly ascending chains of ideals in a given ring. More details on

[3] Recall that the Infinite Pigeonhole Principle says that any finite partition of ω has an infinite member.

algebraic concepts, such as the notion of an ascending chain of ideals in a ring, can be found in the following subsection.

2.2. **Algebra.** We assume some familiarity with basic Algebra, as can be found in the early chapters of [DF99, Eis95, Mat04]. For us a ring A will always be countable, commutative, with an indentity element $1 = 1_A \in A$. Recall that an *ideal* is a subset $I \subseteq A$ closed under addition and $A-$scalar multiplication, and if $I, J \subseteq A$ are ideals we can define another ideal via

$$I \cdot_A J = I \cdot J = \left\{ \sum_{k=1}^{n} x_k \cdot_A y_k : n \in \omega,\ x_k \in I,\ y_k \in J \right\},$$

thus leading to the construction of

$$I^n = \underbrace{I \cdot_A I \cdot_A \cdots \cdot_A I}_{n}$$

for any $n \in \omega$. It follows that $I \cdot J \subseteq I, J$, and hence $I^{n+1} \subseteq I^n$, for all $n \in \omega$, from which we can obtain the ideal

$$I^\infty = \bigcap_{k \in \omega} I^k.$$

For any given $X \subseteq R$, let $\langle X \rangle_A = \langle X \rangle \subseteq A$ denote the $A-$span of X; it follows that $\langle X \rangle$ is an $A-$ideal and it is called the *ideal generated by* X. Moreover, an ideal $I \subseteq A$ is called *finitely generated* (or, more simply, *finite*) whenever there is a finite $X \subseteq A$ such that $\langle X \rangle_A = I$. The notation $a|b$, $a, b \in A$, means that *a divides* b; i.e. $b = c \cdot_A a$, for some $c \in A$. An ascending *chain* of $(A-)$ideals is an ordered sequence of ideals indexed by a downward closed $N \subseteq \omega$ such that

$$I_n \subseteq I_{n+1},\ n, n+1 \in N.$$

A chain of ideals is *strictly ascending* whenever

$$I_n \subsetneq I_{n+1},\ n, n+1 \in N.$$

Recall that A is Noetherian whenever it contains no infinite strictly ascending chains of ideals; i.e. every ascending chain of $A-$ideals eventually stabilizes. An element $x \in A$ is called a *zero divisor* whenever $x \cdot y =_A 0$, for some $y \in A$, and A is called an *integral domain* if (it is commutative and) has no zero divisors.

Theorem 2.2 (Krull Intersection Theorem, [Mat04, Theorem 8.10])**.** *Let A be a Noetherian integral domain containing a proper (finitely generated) ideal $I \subsetneq A$. Then $I^\infty = 0$.*

The previous theorem can be restated in the following more constructive form via contrapositive.

Theorem 2.3 (Krull Intersection Theorem (KIT))**.** *If A is an integral domain containing a proper ideal I such that $I^\infty \neq 0$, then A is not Noetherian.*

Definition 2.4. *Let A be a ring as in Theorem 2.3; we say that A is a <u>KIT$-$instance</u>, and we say that an infinite strictly ascending chain of $A-$ideals $\{J_n\}_{n\in\omega}$ is a corresponding <u>$(A-)$KIT$-$solution</u>.*

In a natural way, we may also speak of uniform KIT$-$solutions $\{J_{n,k}\}_{n,k\in\omega}$ to infinitely many KIT$-$instances $\{A_n\}_{n\in\omega}$ such that for each $n \in \omega$ we have that

$$J_{n,0} \subsetneq J_{n,1} \subsetneq \cdots \subsetneq J_{n,k} \subsetneq \cdots \subsetneq A_n.$$

For each $n \in \omega$, let $I_n \subsetneq A_n$, $I_n^\infty = \cap_{k\in\omega} I_n^k \neq 0$, be as in Theorem 2.3 above, and let $Z_n = \{z_{n,1}, z_{n,2}, \ldots, z_{n,N_n}\}$, $n, N_n \in \omega$ be a finite $I-$generating set.

In the computability context, none of $A_n, I_n \subset A_n, I^\infty$ *are necessarily computable, while* $\{Z_n\}_{n\in\omega}$ *is not necessarily uniformly computable in the index* $n \in \omega$. *For us, a* *uniform* KIT$-$*instance* *is an infinite uniformly computable sequence*

$$\mathfrak{A} = \{A_n, I_n, I_n^\infty, Z_n\}_{n\in\omega}$$

of computable KIT$-$*instances* A_n, $I_n \subsetneq A_n$, $I_n^\infty = \cap_{k\in\omega} I_n^k \neq 0$, $\langle Z_n\rangle_{A_n} = I_n$, *as in Theorem 2.3.*

The standard proof of KIT can be found in [Mat04]. It has a dichotomous nature, being divided into two cases depending upon whether or not $I \cdot I^\infty = I^\infty$. Moreover, each half of the dichotomy is handled via a different algebraic technique that we will review more explicitly later on in this subsection. More specifically, our examination of this dichotomy from a computability perspective is achieved via a computability-theoretic analysis of the uniform KIT$-$solutions $\{J_{n,k}\}_{n,k\in\omega}$ to computable KIT$-$instances $\{A_n\}_{n\in\omega}$; the idea being that for each $n \in \omega$ the KIT$-$solution $\{J_{n,k}\}_{k\in\omega}$ is achieved via one half of the dichotomy and the computational complexity of deciding which half of the dichotomy to use for A_n is encoded in the uniform KIT$-$solution set.

From a purely algebraic (set-theoretic) perspective, while the standard dichotomous proof of KIT (Theorem 2.3) always produces an infinite strictly ascending chain $\{J_n\}_{n\in\omega}$ such that either

- $J_0 \subsetneq J_1 \subsetneq \cdots \subsetneq J_k \subsetneq \cdots \subseteq I^\infty$, for all $k \in \omega$; or else
- $J_0 \nsubseteq I^\infty$;

depending on which half of the dichotomy is achieved by A, our alternative dichotomous proof of KIT relaxes the second condition-item above to the following weaker condition:

- $J_k \nsubseteq I^\infty$, for some $k \in \omega$,

and in doing so achieves a strictly weaker computational strength. This is the main difference between the standard and alternative dichotomies, and our main results highlight the computational significance of this difference.

The following two subsections review the main algebraic techniques employed by each half of the standard dichotomy in the proof of Theorem 2.3.

2.2.1. *Nakayama's Lemma.* Nakayama's Lemma [Mat04, Theorem 2.2] forms the core of one half of the KIT$-$proof dichotomy; namely the half of the proof in which we have that $I \cdot I^\infty = I^\infty$.

Theorem 2.5 (Nakayama's Lemma)**.** *Let* A *be a ring, and* M *be a finite(ly generated)* $A-$*module. Suppose that* $I \subseteq A$ *is an ideal such that* $I \cdot M = M$, *then there exists* $a \in A$ *such that*

$$a \cdot M = 0 \quad \text{and} \quad A \equiv 1 \mod I.$$

In the context of integral domains no such $a \in A$ can exist, and so Nakayama's Lemma becomes the following.

Theorem 2.6. *Let* A *be an integral domain, and* M *be a finite(ly generated)* $A-$*module. Then, if* $I \subseteq A$ *is an ideal, we must have that*

$$I \cdot M \subsetneq M.$$

In other words, if $\eta_1, \eta_2, \ldots, \eta_n$ *generate* M, *then* $\eta_k \notin I \cdot M$ *for some* $1 \leq k \leq n$, $k \in \omega$.

The proof of Nakayma's Lemma involves the theory of determinants of finitely generated modules, and so it comes as no surprise that it can be carried out effectively, and moreover uniformly effectively if the generators are given in such a fashion. More information can be found in [Mat04, Theorems 2.1, 2.2; pages 7-8].

2.2.2. *The Artin-Rees Argument.* We now outline what we consider to be the core of the proof of the Artin-Rees Lemma (especially from an effective point of view); see the proof of [Mat04, Theorem 8.5], especially the part of the proof that begins with the phrase "set $c = \max\{d_1, d_2, \ldots, d_t\}\ldots$" to the end, for more details. The following lemma summarizes the content of that part of the proof in the context of the proof of the Krull Intersection Theorem. In this context the module M is replaced by the finitely generated $A-$ideal I, and the submodule $N \subseteq M$ becomes a subideal $J \subseteq I$. For a proof see the text.

Lemma 2.7. *Let R be a ring, I a finitely generated ideal containing an ideal $J \subseteq I$. Then, if $\alpha_1, \alpha_2, \ldots, \alpha_n$, $n \in \omega$, generate I and $\{p_k\}_{k\in\omega}$ is an infinite sequence of homogeneous polynomials of strictly increasing degree in the indeterminates $X_1, X_2, \ldots, X_n$ with $A-$coefficients such that for each $k \in \omega$,*

$$p_k(\alpha_1, \alpha_2, \ldots, \alpha_n) \in I \setminus I \cdot J,$$

then for each $k \in \omega$ we have that

$$p_{k+1} \notin \langle p_0, p_1, \ldots, p_k\rangle_{A[X_0,X_1,\ldots,X_n]},$$

because A is not Noetherian.

3. The Complexity of the Standard Dichotomy

The standard proof of KIT is divided into cases based on whether or not $I \cdot I^\infty = I^\infty$. The purpose of this section is to show that in general the complexity of the standard KIT$-$proof dichotomy is at least the double-jump $\mathbf{0}''$. More specifically, in the next theorem we construct an infinite uniformly computable KIT$-$sequence

$$\{\mathfrak{A}_n\}_{n\in\omega} = \{A_n, I_n, I_n^\infty\}_{n\in\omega}$$

such that for each $n \in \omega$

- A_n is an integral domain containing the ideal I_n, such that
- $0 \neq I_n^\infty = \cap_{k\in\omega} I_n^k$.

Furthermore we will ensure that

$$\{n \in \omega : I \cdot_{A_n} I^\infty = I^\infty\} = \{n \in \omega : W_n \text{ is infinite}\} = \mathrm{Inf},$$

i.e. deciding the standard dichotomy for $\{A_n\}_{n\in\omega}$ requires $\mathbf{0}''$.

Theorem 3.1. *The infinite uniformly computable sequence $\{\mathfrak{A}_n\}_{n\in\omega}$ described in the previous paragraph exists.*

Proof. We describe a uniformly computable procedure for constructing each

$$\mathfrak{A}_n = (A_n, I_n, I_n^\infty, x_n),\ n \in \omega,$$

with the properties described above. More specifically, however, when $n \in \mathrm{Inf}$ via the infinite computable strictly increasing enumeration

$$W_n = \{s_1 < s_2 < s_3 < \cdots < s_k < \cdots : k \in \omega\} \subseteq \omega,$$

we ensure that

$$I_n \cdot I_n^\infty = I_n^\infty \cdot I_n^\infty = I_n^\infty$$

via elements $\{X_{s_k} : k \in \omega\} \subseteq I_n^\infty$ such that

$$I_n^\infty = \langle X_{\ell_k} : k \in \omega\rangle_{A_n}$$

and

$$X_{\ell_{k+1}}^2 = X_{\ell_k},\ k \in \omega.$$

Let

$$\vec{X} = \{X_k : k \in \omega\},\ \mathbb{Q}_\infty = \mathbb{Q}[\vec{X}] = \mathbb{Q}[x_k : k \in \omega];$$

for each $n \in \omega$ we will have that

- $A_n = A$ is a quotient of $\mathbb{Q}_\infty$ via uniformly computable multiplication relations described below;
- $I_n = I = \langle X_k : k \in \omega \rangle_A$;
- $x_n = x = X_0 \in I_n^\infty = I^\infty = \cap_{k \in \omega} I^k \subseteq I \subseteq A$;

Our construction of A proceeds in stages as follows:

Stage $s = 0$: set $\ell_0 = 0$, implying that $X_0 = X_{\ell_0} \in I^\infty$ as specified in the third item above.

Stage $s + 1 > 0$: let $\alpha \in \omega$ be least such that X_α has not been mentioned yet in the construction. There are two cases to consider; the first case says that $s + 1 \in W = W_n$. In this case let $k \in \omega$ be largest such that $\ell_k \in \omega$ is defined; we set $\ell_{k+1} = \alpha$ and introduce the (uniformly computable) multiplication relation

$$X_{\ell_{k+1}}^2 = X_{\ell_k}.$$

Otherwise we have that $s + 1 \notin W$. In this case let $k, \alpha \in \omega$ be as in the previous paragraph, and introduce the (uniformly computable) multiplication relation

$$X_{\ell_k} = \prod_{j=\alpha}^{\alpha+d-1} X_j$$

, where $d \in \omega$ is chosen so that $p = d + 1$ is a prime number greater than any prime that we have considered so far in the construction. Note that d is also the degree of the product term in the displayed relation.

This concludes our construction.

It follows from our (simple) construction above that the sequence

$$\mathfrak{A}_n = (A_n, I_n, I_n^\infty, x_n),\ n \in \omega,$$

is uniformly computable in n. To verify that

$$I_n \cdot I_n^\infty = I_n^\infty \text{ if and only if } n \in \mathrm{Inf}$$

note that if

$n \in \mathrm{Inf}$: There are infinitely many $s \in \omega$, $s > 0$ for which our construction realizes the case one procedure, thus producing the infinite sequence of indices $\{\ell_k : k \in \omega\}$ mentioned above such that $X_{\ell_{k+1}}^2 = X_{\ell_k}$, $k \in \omega$.

$n \notin \mathrm{Inf}$: There are only finitely many stages in which are construction realizes case one, and therefore there exists $s_0 \in \omega$ such that for all stages $s \geq s_0$ our construction realizes the case two procedure. Now, by our construction it follows that if k_0 is the value of k at stage s_0 then k_0 is the value of k at all future stages as well and

$$I_n^\infty = \langle X_{\ell_k} : 0 \leq k \leq k_0 \rangle$$

and moreover (since our construction never realizes case one at any stage $s \geq s_0$)

$$X_{\ell_k} \notin I_n \cdot I_n^\infty.$$

- Finally, note that in either of the two items above we have that $I^\infty = \cap_{k \in \omega} I^k$. In the case $n \in \mathrm{Inf}$ we actually have that $I^\infty \cdot I^\infty = I^\infty$, since the sequence $\{\ell_k\}_{k \in \omega}$ is defined for all k. On the other hand, if $n \notin \mathrm{Inf}$ then our construction at stages $s \geq s_0$ ensures that $X_{\ell_{k_0}} \in I^\infty$ and consequently $X_{\ell_k} \in I^\infty$, $1 \leq k \leq k_0$, since (by construction) each X_{ℓ_k} is a power of $X_{\ell_{k_0}}$.

We also have that A is an integral domain since there is an injective homomorphism

$$\varphi : A \to \mathbb{A},$$

where $\mathbb{A}$ is the field of algebraic numbers, such that:

- $\varphi(X_{\ell_0}) = 1 \in \mathbb{A}$;
- $\varphi(X_{\ell_k})$, $k > 0$, $k \in \omega$, is a primitive 2^k-th root of unity; and
- $\varphi(X_j)$, $j = \alpha, \alpha+1, \ldots, \alpha+d-1$ are distinct primitive $(2^k p)^{th}$ roots of unity, where $\alpha, k, d \in \omega$, $p = d+1$, are as in case two (i.e. $s+1 \notin W$) of our construction above.

□

4. A Different Dichotomous Argument of Lesser Complexity

The previous section explains why the standard decision procedure employed by the proof of KIT has Turing complexity at least $\mathbf{0}''$ (at the uniform level). In this section we present a different dichotomy that simplifies the standard one. Although much of the algebra will not change, there will be some logical (i.e. set-theoretic) differences between our argument here and the standard one presented in many standard texts on Commutative Algebra; we discuss these differences afterwards.

Theorem 4.1. *Suppose that*

$$\mathfrak{A}_n = (A_n, I_n, I_n^\infty, Z_n),\ n \in \omega,$$

is a uniform $\mathsf{KIT}-$*sequence, and let* $\mathbf{x}$ *be a Turing degree that is PA relative to* $\mathbf{0}'$. *Then* $\mathbf{x}$ *computes a uniform sequence of chains of* A_n-*ideals,*

$$\mathfrak{J}_n = \{J_{n,k} : k \in \omega\},$$

uniformly in $n \in \omega$, *such that*

$$J_{n,0} \subsetneq J_{n,1} \subsetneq \cdots \subsetneq J_{n,k} \subsetneq \cdots \subsetneq A_n,\ k \in \omega.$$

Proof. Recall that, by our hypothesis on $\mathbf{x}$, $\mathbf{x}$ can answer single quantifier questions about each integral domain $\mathfrak{A}_n$, uniformly in $n \in \omega$. Consequently, for each $n \in \omega$ and finite set of A_n elements, $\mathbf{x}$ can construct the ideal they generate, uniformly in both n and the given finite set. For each $n \in \omega$ we will use our hypotheses on A_n and $\mathbf{x}$ to uniformly $\mathbf{x}-$compute an infinite sequence of A_n-elements $\{x_{n,k}\}_{k\in\omega}$ such that

$$x_{n,k+1} \notin \langle x_{n,0}, x_{n,1}, \ldots, x_{n,k}\rangle_{A_n},\ k \in \omega.$$

Therefore if we set

$$J_{n,k} = \langle x_{n,\ell} : \ell \leq k\rangle_{A_n},\ n, k \in \omega,$$

we will have proven the theorem.

Fix $n \in \omega$, and let $A = A_n$, $I = I_n$, $I_n^\infty = I^\infty$, and $Z = Z_n$. There are two phases to the construction of the infinite strictly ascending chain of $A_n = A-$ideals $\{J_{n,k} = J_k\}_{k\in\omega}$, $J_k \subsetneq J_{k+1} \subsetneq A$. As we mentioned in the previous paragraph, we construct the sequence one generator at a time, and there are essentially two types of generators:

(i) generators in I^∞; and
(ii) generators in $I \setminus I^\infty$.

The construction begins by considering generators of type (i) exclusively, and proceeds so that at some point it may switch to exclusively considering generators of type (ii) from that point on.

The first part of our construction begins with any $0 \neq x_0 \in I^\infty$. At stage $s+1 > 0$, $s \in \omega$ if we are still in phase one we assume that we are given a finite sequence of generators $x_0, x_1, x_2, \ldots, x_s \in I^\infty$ such that, for each $0 \leq k < s$,

$$\langle x_{k+1} \notin \langle x_\ell : 0 \leq \ell \leq k\rangle_A \subset I^\infty.$$

Furthermore, by construction and induction it will follow that $x_k \in I \cdot I^\infty$ for all $k < s$, but we might have that $x_s \notin I \cdot I^\infty$, which $\mathbf{0}'$ can decide (uniformly in n, and $x_0, x_1, \ldots, x_s$). If this is the case we proceed to the second phase of the construction (described in the following paragraph) at the current stage s. Otherwise we have that $x_k \in I \cdot I^\infty$ for all $0 \le k \le s$, and in this case Nakayama's Lemma [Mat04, Theorem 2.2] says that if $n_s \in \omega$ and $\{y_{s,j}\}_{j=0}^{n_s} \subseteq I^\infty$ is such that

$$x_0, x_1, \ldots, x_s \in I \cdot \langle y_{s,j} : 0 \le j \le n_s \rangle_A \subseteq I^\infty,$$

then either:

- $y_{s,j_0} \notin I \cdot \langle y_{s,j} : 0 \le j \le n_s \rangle_A$, for some $0 \le j_0 \le n_s$ which $\mathbf{x} \ge_T \mathbf{0}'$ can effectively decide (uniformly in n); or else
- there exists $a \in A$, $a \equiv 1 \mod A$, such that

$$a \cdot y_{s,j} =_A 0, \;\; j = 0, 1, \ldots, n_s.$$

However, this cannot be the case because A is assumed to be an integral domain.

Therefore, j_0 of the first item above exists; we set $x_{s+1} = y_{s,j_0}$ which ensures that

$$\langle x_k : 0 \le k \le s \rangle_A \subseteq I \cdot y_{s,j} : 0 \le j \le n_s \rangle_A \subsetneq \langle x_k : 0 \le k \le s+1 \rangle_A,$$

as we require of x_{s+1}. This completes phase one of our construction; it is possible that for some $n \in \omega$, $A = A_n$, we have that $I_n \cdot I_n^\infty = I_n^\infty$ and in this case our construction of

$$J_{n,0} \subsetneq J_{n,1} \subsetneq \cdots \subsetneq J_{n,k} \subsetneq \cdots \subsetneq A_n, \quad J_{n,k} = \langle x_{n,j} : 0 \le j \le k \rangle_{A_n},$$

will never leave phase one.

If we ever find ourselves in the second phase of the construction it is because at some stage $s_0 + 1 > 0$, $s_0 \in \omega$, we have discovered some $x_{s_0} \in I^\infty \setminus I \cdot I^\infty$ after having already constructed $x_0, x_1, \ldots, x_{s_0} \in I^\infty$ such that for each $0 \le k < s_0$, we have that

$$x_{k+1} \notin \langle x_j : 0 \le j \le k \rangle_A \subseteq I^\infty.$$

Now, from the point of view of phase two, stage s_0 is essentially stage 0, and so we assume without any loss of generality that $s_0 = 0$.[4] Now, since $x_{s_0} = x_0 \in I^\infty$, and

$$Z = Z_n = \{z_0, z_1, \ldots, z_{N_n}\}$$

generates I (over A), for each $j \in \omega$ there is a homogeneous polynomial

$$p_j \in A[X_0, X_1, \ldots, X_{N_n}]$$

of degree $d_j \ge j$ such that $x_0 = p_j(z_0, z_1, \ldots, z_{N_n}) \in I^\infty \setminus I \cdot I^\infty$. Furthermore, by passing to an infinite computable subsequence of j's we can essentially assume without any loss of generality that $\deg(p_j) = j$ for all j.[5]

Now the last part of of the proof of [Mat04, Theorem 8.5] beginning with "Set $c = \max\{d_1, \ldots, d_t\} \ldots$" until the end of the proof explains why for all $j \in \omega$ we have that

$$p_{j+1} \notin \langle p_0, p_1, \ldots, p_j \rangle_{A[X_0, X_1, \ldots, X_{N_n}]},$$

[4]The reader should keep in mind, however, the subtle fact that $\mathbf{x}$ *cannot decide* whether our construction will ever enter phase two, uniformly in $n \in \omega$, since this is essentially the same (i.e. Turing equivalent to) deciding whether or not $I_n \cdot I_n^\infty = I_n^\infty$, uniformly in n. In other words, in order for $\mathbf{x}$ to be able to handle both phases of our construction, uniformly in n, requires that we "pad phase two out" by some instances of phase one as we have already described how to do.

[5]We can also obtain the same result (algebraically) by absorbing appropriately many occurrences of I_n-generators z_i, $0 \le i \le N_n$, into the coefficients of p_j.

and via $\mathbf{0}' \leq_T \mathbf{x}$ we can recursively compute, uniformly in $n, j \in \omega$ a leading $p_j - A_n-$coefficient $x_j \in A$, along with a corresponding monomial summand m_j such that for each $\ell = 0, 1, \ldots, j-1$ we have that

$$x_j \notin \langle x_\ell : 0 \leq \ell < j,\ m_\ell | m_j \rangle_A.$$

Also, by the Hilbert Basis Theorem, for any given $j_0 \in \omega$, there exists $j_1 \in \omega$, $j_1 > j_0$, such that if we let

$$M_{j_0, j_1} = \{m_{j_0}, m_{j_0+1}, \ldots, m_{j_1} - 1\}$$

for all $j \geq j_1$ the monomial m_j is divisible by at least one of the monomials $\{m_\ell\}_{\ell=j_0}^{j_1}$, and by our construction of x_j, m_j it follows that

$$x_j \notin \langle x_\ell : j_0 \leq \ell < j_1,\ m_\ell | m_j \rangle_A.$$

Moreover, j_1 can be uniformly effectively obtained from j_0 via $\mathbf{0}'$. Setting $j_0 = 0$ and repeating this argument yields an infinite uniformly $\mathbf{0}'-$computable sequence

$$j_0 < j_1 < j_2 < \cdots < j_k < \cdots,\ k \in \omega,$$

such that for each $k \in \omega$ and $j \geq j_{k+1}$, $j \in \omega$, we have that

(i) the monomial m_j is divisible by at least one of the monomials $\{m_\ell\}_{j_k}^{j_{k+1}-1}$; and
(ii) $x_j \notin \langle x_\ell : j_k \leq \ell < j_{k+1} \rangle_A$.

Definition 4.2. *Given any $\ell_1, \ell_2 \in \omega$, $\ell_1 < \ell_2$, let $k_1 \in \omega$ be greatest and $k_2 \in \omega$ be least such that*

$$j_{k_1} \leq \ell_1 < j_{k_1+1} < j_{k_1+2} < \cdots < j_{k_2-1} \leq \ell_2 \leq j_{k_2}.$$

For any monomials $m \in M_{j_{k_1}, j_{k_1+1}}$ and $m' \in M_{j_{k_2-1}, j_{k_2}}$, we say that m H−divides[6] m' whenever there is a sequence of monomials

$$m_1, m_2, \ldots, m_{k_2-k_1},\ m_i \in M_{j_{i+k_1-1}, j_{i+k_1}}, i \in \omega, 1 \leq i \leq k_2 - k_1,$$

such that for each $0 \leq i \leq k_2 - k_1 - 1$, $i \in \omega$, we have that $m_{k_1+i} | m_{k_1+i+1}$.

Remark 4.3. *It follows that the $H-$division relation is transitive, and so gives rise to a finitely branching tree structure on the monomials m_i, $i \in \omega$.*

Via induction, the Infinite Pigeonhole Principle, and item (i) above, one can show that for each $k \in \omega$ there is a monomial $m \in M_{j_k, j_{k+1}}$ such that for each $\ell > k$ m divides at least one monomial in $M_{j_\ell, j_{\ell+1}}$. This implies that our $H-$division tree, call it T, is infinite. It is obvious that the $H-$division relation is computable, however our construction of $\{j_k\}_{k\in\omega}$ could only be carried out uniformly via $\mathbf{0}'$, and so we cannot necessarily conclude that T is computable; rather, we only know that T is computable relative to $\mathbf{0}'$. However, by our hypothesis on $\mathbf{x}$ it follows that $\mathbf{x}$ computes an infinite path $f = \langle f(k) : k \in \omega \rangle \in \omega^\omega$ through T corresponding to an infinite sequence of monomials $\mathcal{M} = \langle m_{f(k)} : k \in \omega \rangle$ such that $m_{f(k)} | m_{f(k+1)}$ for all $k \in \omega$ and hence such that the corresponding $A-$coefficients $\{x_{f(k)}\}_{k\in\omega}$ satisfy

$$x_{f(k+1)} \notin \langle x_{f(\ell)} : \ell \leq k \rangle_A,\ k \in \omega.$$

Finally, upon setting $x_{s_0+k} = x_{f(k)}$ and recalling that $x_0, x_1, \ldots, x_{s_0-1} \in I^\infty$ are obtained via the first phase of the construction, we have that

$$J_0 \subsetneq J_1 \subsetneq \cdots \subsetneq J_{s_0-1} \subseteq I^\infty \subsetneq J_{s_0} \subsetneq J_{s_0+1} \subsetneq \cdots \subsetneq J_{s_0+k} \subsetneq \cdots \subsetneq A,\ k \in \omega,$$

is an infinite strictly ascending chain of $A = A_n-$ideals, computable in $\mathbf{x}$, uniformly in $n \in \omega$. □

[6]The H here stands for Hilbert; we are essentially reconstructing the argument of the Hilbert Basis Theorem in a more constructive fashion.

References

[Buc74] B. Buchberger. A theoretical basis for the reduction of polynomials to canonical forms. *ACM SIGSAM Bulletin*, 10(3):19–29, 1974.

[Con19] C.J. Conidis. The computability, definability, and proof theory of artinian rings. *Advances in Mathematics*, 341(1):1–39, 2019.

[DF99] D.S. Dummit and R.M. Foote. *Abstract Algebra.* John Wiley & Sons, 1999.

[Eis95] D. Eisenbud. *Commutative algebra with a view toward algebraic geometry.* Springer-Verlag, 1995.

[FSS83] H.M. Friedman, S.G. Simpson, and R.L. Smith. Countable algebra and set existence axioms. *Annals of Pure and Applied Logic*, 25:141–181, 1983.

[FSS85] H.M. Friedman, S.G. Simpson, and R.L. Smith. Addendum to: "countable algebra and set existence axioms". *Annals of Pure and Applied Logic*, 28:319–320, 1985.

[Hat94] K. Hatzikiriakou. A note on ordinal numbers and rings of formal power series. *Archive for Mathematical Logic*, 33(4):261–263, 1994.

[Hil90] D. Hilbert. Über die theorie der algebraischen formen. *Mathematische Annalen*, 36(4):473–534, 1890.

[JS74] C. G. Jockusch and R. I. Soare. Π^0_1-classes and degrees of theories. *Transactions of the AMS*, 173(1):33–56, 1974.

[Mat04] H. Matsumura. *Commutative Ring Theory.* Cambridge University Press, 2004.

[Sim88] S. G. Simpson. Ordinal numbers and the hilbert basis theorem. *J. Symbolic Logic*, 53:961–974, 1988.

[Soa16] R.I. Soare. *Turing Computability.* Springer-Verlag, 2016.

Department of Mathematics, College of Staten Island, City University of New York, Staten Island, NY 10314

Email address: chris.conidis@csi.cuny.edu