# CHAIN CONDITIONS IN COMPUTABLE RINGS

CHRIS J. CONIDIS

Abstract. Friedman, Simpson, and Smith [7, 8] showed that, over $\mathsf{RCA}_0$, the statements "Every ring has a maximal ideal" and "Every ring has a prime ideal" are equivalent to $\mathsf{ACA}_0$ and $\mathsf{WKL}_0$, respectively. More recently, Downey, Lempp, and Mileti [5] have shown that, over $\mathsf{RCA}_0$, the statement "Every ring that is not a field contains a nontrivial ideal" is equivalent to $\mathsf{WKL}_0$.

In this article we explore the reverse mathematical strength of the classic theorems from commutative algebra which say that every Artinian ring is Noetherian, and every Artinian ring is of finite length. In particular we show that, over $\mathsf{RCA}_0$, the former implies $\mathsf{WKL}_0$ and is implied by $\mathsf{ACA}_0$, while over $\mathsf{RCA}_0$+$\mathsf{B}\Sigma_2$, the latter is equivalent to $\mathsf{ACA}_0$.

## 1. Introduction

In the modern algebraic literature, effective field theory dates back to the work of van der Waerden [23], who examined the existence of splitting algorithms for polynomial rings over fields. A quarter of a century later, the subject was formally introduced by Frölich and Shepherdson [9], who gave the standard formal definitions, and further developed the basic ideas of van der Waerden. Soon after the development of computable field theory, mathematicians began to develop the theory of computable rings.

**Definition 1.1.** A *computable ring* (with identity) is a computable subset $R \subseteq \mathbb{N}$, together with computable binary operations $+$ and $\cdot$ on $R$, and elements $0, 1 \in R$, such that $(R, 0, 1, +, \cdot)$ is a ring (with identity $1 \in R$).

Two of the most natural and important questions that were asked by computable ring theorists are the following [22]. Let $R$ be a computable commutative ring with identity.

(1) Given $a_1, a_2, \ldots, a_n \in R$, is the finitely generated ideal $\langle a_1, a_2, \ldots, a_n\rangle$ of $R$ computable?
(2) Given any $a_1, a_2, \ldots, a_n \in R$, is the finitely generated ideal $\langle a_1, a_2, \ldots, a_n\rangle$ uniformly computable in its generators?

It is not difficult to show that (1) and (2) hold for any computable presentation of the ring of integers $\mathbb{Z}$. Furthermore, Kronecker [15] showed that every finitely generated ideal of $\mathbb{Z}[X_1, X_2, \ldots, X_n]$ is computable. Many algorithms for this sort of problem have been studied and implemented using Gröbner bases.

Let $F$ be a field, and let $F[X_1, X_2, \ldots, X_n]$ denote the ring of polynomials in $n$ variables, with coefficients in $F$. We have the following related results of Hilbert and Hermann.

**Theorem 1.2** (Hilbert Basis Theorem)**.** *Every ideal of $F[X_1, X_2, \ldots, X_n]$ is finitely generated.*

The author was partially supported by NSERC grant PGS D2-344244-2007. Furthermore, he would like to acknowledge the helpful input he received from his thesis advisors, R.I. Soare, D.R. Hirschfeldt, and A. Montalbán. He would also like to especially thank J.R. Mileti for suggesting this topic, and A. Montalbán for his help in editing the initial drafts.

**Corollary 1.3** (Hermann, 1926 [11, 22])**.** *If $k$ is a computable field, then the ideal membership problem for $F[X_1, \ldots, X_n]$ is decidable, uniformly in the generators.*

The Hilbert Basis Theorem is the main motivation for the study of Noetherian rings. We now define what it means for a ring to be Noetherian, and give an equivalent characterization. Then we state the Generalized Hilbert Basis Theorem for Noetherian rings. From now on $R$ will always denote a commutative ring with identity.

**Definition 1.4.** $R$ is *Noetherian* if every increasing chain of ideals $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots \subseteq I_N \subseteq \cdots$ in $R$ eventually stabilizes. In other words, there exists a number $N_0 \in \mathbb{N}$, such that for all $N \geq N_0$ we have that $I_{N_0} = I_N$. More generally, an $R$-module $M$ is Noetherian if every increasing sequence of $R$-submodules of $M$ eventually stabilizes.

**Theorem 1.5.** *$R$ is Noetherian if and only if every ideal of $R$ is finitely generated.*

**Theorem 1.6** (Generalized Hilbert Basis Theorem)**.** *If $R$ is Noetherian, then $R[X_1, \ldots, X_n]$ is Noetherian.*

Baur [3] showed that every ideal in a Noetherian ring is computable, but not always uniformly computable with respect to generators. Furthermore, Hingston [12] proved an effective analog of the primary decomposition theorem for Noetherian rings. With the thought of solving the uniform version of the ideal membership problem in mind, we now turn our attention to the following definition from classical algebra.

**Definition 1.7.** $R$ is *Artinian* if every decreasing chain of ideals $I_0 \supseteq I_1 \supseteq I_2 \supseteq \cdots \supseteq I_N \supseteq \cdots$ in $R$ eventually stabilizes. In other words, there exists a number $N_0 \in \mathbb{N}$, such that for all $N \geq N_0$ we have that $I_{N_0} = I_N$. More generally, an $R$-module $M$ is Artinian if every decreasing sequence of $R$-submodules of $M$ eventually stabilizes.

In terms of the ideal membership problem discussed above, the following is known regarding Artinian rings.

**Theorem 1.8** (Baur [3], 1974)**.** *Every computable Artinian ring $R$ has an ideal membership algorithm that is uniform in the generators.*

The following classic theorem of algebra relates the fundamental algebraic notions of Artinian and Noetherian rings, and is the main focus of our study.

**Theorem 1.9** (Akizuki [1], Hopkins [13])**.** *If $R$ is Artinian, then $R$ is Noetherian.*

We hope that by this point we have convinced the reader of the natural and significant role that Noetherian and Artinian rings have played in the development of effective ring theory. The main goal of this article is to determine, from the point of view of computability theory, the strength of Theorem 1.9. To achieve this goal, we shall classify the computability strength required to go from an infinite strictly increasing chain of ideals in $R$, to an infinite strictly decreasing chain of ideals in $R$. More specifically, we shall prove our first main theorem, which we now state. A set is of PA degree if it can compute a complete and consistent extension of the theory of Peano Arithmetic (a more formal definition is given in the next section).

**Theorem** (Theorem 4.1)**.** *There exists a computable integral domain $R$, such that $R$ contains an infinite uniformly computable strictly increasing chain of ideals, and such that every infinite strictly decreasing chain of ideals in $R$ is of PA degree.*

The following theorem (1.11) is actually a corollary of the proof of Theorem 1.9. In Section 6, we prove that its computability strength is at least that of the halting set $\emptyset'$. First, however, we give a definition which we use to state the theorem. Classically, this definition is not standard because (by Theorem 1.11) it is equivalent to saying that $R$ is Artinian.

**Definition 1.10.** $R$ is *strongly Noetherian* if $R$ has finite length (as an $R$-module). In other words, $R$ is strongly Noetherian if and only if there is a number $N \in \mathbb{N}$, such that the length of any strictly increasing chain of ideals in $R$ is bounded by $N$.

**Theorem 1.11** (Akizuki [1], Hopkins [13])**.** *If $R$ is Artinian, then $R$ is strongly Noetherian.*

A key ingredient in the classification of the computability strength of Theorem 1.11 is the following, which we prove in Section 6.

**Theorem** (Theorem 6.1)**.** *There exists a computable ring $R$ such that for every $n \in \mathbb{N}$, $R$ contains a strictly increasing chain of ideals of length $n$, and such that every infinite strictly decreasing chain of ideals in $R$ computes the halting set $\emptyset'$.*

Determining the computability strength of a given theorem is frequently equivalent to determining that theorem's reverse mathematical strength. Therefore, once we have determined the effective content of Theorems 1.9 and 1.11, we will translate our results into the language of reverse mathematics. We now state these results. The necessary definitions are given in the next section.

**Theorem 1.12** ($\mathsf{RCA}_0$)**.** *Theorem 1.9 implies $\mathsf{WKL}_0$, and is implied by $\mathsf{ACA}_0$.*

**Theorem 1.13** ($\mathsf{RCA}_0$+$\mathsf{B}\Sigma_2$)**.** *Theorem 1.11 is equivalent to $\mathsf{ACA}_0$.*

## 2. Background

In this section we give the reader general background information about computability theory and reverse mathematics. Throughout the rest of this article the term *ring* shall mean *commutative ring with identity.* We assume that the reader is familiar with the basic definitions and theorems of ring theory. For a reference on commutative algebra and ring theory, please consult any of the following standard texts [2, 6, 16, 17].

### 2.1. Computability Theory.

For a general reference on computability theory, we refer the reader to Soare [21]. We call a function $f : \mathbb{N}^n \to \mathbb{N}$ or a set $A \subseteq \mathbb{N}$ *computable* if there is a computer program that outputs the value $f(x) \in \mathbb{N}$ on input $x \in \mathbb{N}^n$. A set $A \subseteq \mathbb{N}$ is *computably enumerable* (c.e.) if it is the range of a computable function $f : \mathbb{N} \to \mathbb{N}$.

Given a set $A \subseteq \mathbb{N}$, let $A(x)$ denote its characteristic function. For any sets $A, B \subseteq \mathbb{N}$, we say that $A$ is *computable relative to* $B$, and write $A \leq_T B$, if there is a computer program that, when given access to the (possibly noncomputable) function $B(x)$, outputs $A(x)$ on input $x \in \mathbb{N}$. The resulting equivalence classes (under relative computation) are called *Turing degrees.* Given a set $A \subseteq \mathbb{N}$, we let $A'$ denote the halting set relative to $A$.

The sort of question that we most often consider in this article asks for the sets of natural numbers that can compute an infinite strictly decreasing chain of ideals in rings with an infinite uniform computable strictly increasing chain of ideals. Related questions have been studied in the past. For example, if one asks for the sets that can compute a maximal ideal in a computable ring, or a finitely generated nontrivial ideal in a computable ring that is not a field, then the answer is (the sets that compute) $\emptyset'$.

**Theorem 2.1** (Friedman, Simpson, Smith [7, 8]**).** (1) *Suppose that $R$ is a computable ring. Then there exists a maximal ideal $M$ of $R$ such that $M \leq_T \emptyset'$.*
(2) *There exists a computable local ring $R$ such that the unique maximal ideal $M$ of $R$ satisfies $M \equiv_T \emptyset'$.*

**Theorem 2.2** (Downey, Lempp, Mileti [5]**).** (1) *Suppose that $R$ is a computable ring that is not a field. Then there is a nontrivial finitely generated ideal $I$ of $R$ such that $I \leq_T \emptyset'$.*
(2) *There exists a computable ring $R$ that is not a field such that every nontrivial finitely generated ideal $I$ of $R$ satisfies $\emptyset' \leq_T I$.*

2.2. **Weak König's Lemma.** One combinatorial principle which we use in this article is known as *Weak König's Lemma.* We now state several definitions and theorems that are related to Weak König's Lemma.

**Definition 2.3.** By $2^{<\mathbb{N}}$, we mean the set of finite sequences of 0's and 1's, partially ordered by the substring relation $\subseteq$.

**Definition 2.4.** (1) A *tree* is a subset $T$ of $2^{<\mathbb{N}}$, such that for all $\sigma \in T$, if $\tau \in 2^{<\mathbb{N}}$ and $\tau \subseteq \sigma$, then $\tau \in T$. In other words, a tree is a subset of $2^{<\mathbb{N}}$ that is closed downwards under $\subseteq$.
(2) An *infinite path* or *branch* of a tree $T$ is a function $f : \mathbb{N} \to \{0, 1\}$ such that for every $n \in \mathbb{N}$ we have that
$$\langle f(0), f(1), \cdots, f(n)\rangle \in T.$$

We now state Weak König's Lemma.

**Proposition 2.5** (Weak König's Lemma)**.** *Every infinite tree has an infinite path.*

Weak König's Lemma is not computably true, in the following sense.

**Proposition 2.6.** *There is a computable tree $T$ with no computable infinite path.*

The following definition is intended to characterize the degrees that compute solutions to Weak König's Lemma.

**Definition 2.7.** [[19]] Given $A, B \subseteq \mathbb{N}$, we say that $A$ is *PA over $B$* if every $B$-computable infinite tree has an $A$-computable infinite path. We say that a set $A$ is of PA degree if $A$ is PA over $\emptyset$.

A degree is PA over $\emptyset$ if and only if it can compute a complete and consistent extension of the theory of Peano Arithmetic [19].

A classic theorem of Jockusch and Soare says that there exist solutions to Weak König's Lemma that are not very far away from being computable, in the following sense.

**Theorem 2.8** (Low Basis Theorem – Jockush, Soare [14]**).** *For any set $B$, there is a set $A$ that is PA over $B$, and such that $A' \equiv_T B'$.*

The following theorems relate PA degrees to the complexity of ideals in compuable rings.

**Theorem 2.9** (Friedman, Simpson, Smith [7, 8]**).** (1) *Let $R$ be a computable ring, and $A \subset \mathbb{N}$ be of PA degree. Then there is a prime ideal $P \subset R$ that is computable relative to $A$.*
(2) *There exists a computable ring $R$ such that every prime ideal $P$ of $R$ is of PA degree.*

**Theorem 2.10** (Downey, Lempp, Mileti [5]**).** *There exists a computable ring $R$ that is not a field and such that every nontrivial ideal $I$ of $R$ is of PA degree.*

We now give an equivalent definition of PA degrees, which is more convenient for our purposes.

**Proposition 2.11** ([19]). *The following are equivalent.*

1. $D \subset \mathbb{N}$ *is of PA degree.*
2. *For any two disjoint c.e. sets* $A, B \subseteq \mathbb{N}$*, there is a set* $C$*, computable relative to* $D$*, such that* $A \subseteq C$ *and* $C \cap B = \emptyset$*. We call* $C$ *a separator for* $A$ *and* $B$*.*

*Furthermore, there are disjoint c.e. sets* $A, B$ *such that if a set* $D$ *can compute a separator for* $A$ *and* $B$*, then* $C$ *computes a separator for any given pair of disjoint c.e. sets.*

Hence, whenever we wish to construct a set $D \subseteq \mathbb{N}$ of PA degree, we will fix disjoint c.e. sets $A, B$ as in the previous proposition, and construct $D$ so that it computes a separator for $A$ and $B$.

2.3. **Reverse Mathematics.** The standard reference in reverse mathematics is Simpson [20]. In the context of reverse mathematics we shall work over the weak base system $\mathsf{RCA}_0$ (Recursive Comprehension Axiom), which consists of the discretely ordered semiring axioms for $\mathbb{N}$, as well as comprehension for $\Delta^0_1$ formulas, and induction for $\Sigma^0_1$ formulas ($\mathsf{I}\Sigma_1$). More generally and more formally, for any fixed $k \in \mathbb{N}$, $\mathsf{I}\Sigma_k$ is the scheme which says that for any $\Sigma^0_k$ formula $\varphi$ the following holds:

$$(\mathsf{I\Sigma_k}) \qquad (\varphi(0) \wedge (\forall n)[\varphi(n) \rightarrow \varphi(n+1)]) \rightarrow (\forall n)\varphi(n)$$

In addition to $\mathsf{I}\Sigma_k$, we also use a bounding principle called $\mathsf{B}\Sigma_k$. For every number $k \in \mathbb{N}$, $\mathsf{B}\Sigma_k$ says that for any given $\Sigma^0_k$ formula $\varphi(x)$, and any $n \in \mathbb{N}$, we have the following:

$$(\mathsf{B\Sigma_k}) \qquad (\forall i < n)(\exists x)\varphi(x) \rightarrow (\exists u)(\forall i < n)(\exists x < u)\varphi(x)$$

It is a well-known fact that $\mathsf{B}\Sigma_2$ is equivalent to the infinite pigeonhole principle (see [10], Theorem I.2.23). The infinite pigeonhole principle says that if there exists a number $n \in \mathbb{N}$, and a function $f : \mathbb{N} \rightarrow \{0, 1, 2, \dots, n-1\} = n$, then there exists a number $u < n$ and infinitely (i.e. unboundedly) many $x \in \mathbb{N}$ such that $f(x) = u$. It is also well-known that for every $k \in \mathbb{N}$, $\mathsf{B}\Sigma_k$ lies strictly between $\mathsf{I}\Sigma_k$ and $\mathsf{I}\Sigma_{k-1}$ [10, 18].

Proofs that can be carried out effectively (i.e. computably) can often be done in $\mathsf{RCA}_0$; indeed, the computable sets form a model of $\mathsf{RCA}_0$. The standard proofs the following propositions can be carried out effectively, except for that of Proposition 2.14, in which case a slightly modified version of the standard proof (which we give below) is valid in $\mathsf{RCA}_0$. It follows that each of the following propositions from elementary algebra (which we use throughout this article) hold in $\mathsf{RCA}_0$. Let $R$ be a ring, and $V$ be a vector space over the field $F$.

**Proposition 2.12** ($\mathsf{RCA}_0$). *Let* $I$ *be an ideal of the ring* $R$*. Then, if* $\varphi : R \rightarrow R/I$ *is the canonical quotient homomorphism, and* $\hat{J}$ *is an ideal of* $R/I$*, then* $\varphi^{-1}(\hat{J}) \subseteq R$ *exists, and is an ideal of* $R$ *containing* $I$*.*

**Proposition 2.13** ($\mathsf{RCA}_0$). *An ideal* $P \subset R$ *is prime if and only if* $R/P$ *is an integral domain.*

**Proposition 2.14** ($\mathsf{RCA}_0$). *Every maximal ideal of* $R$ *is prime.*

*Proof.* Suppose that $M \subset R$ is a maximal ideal, and consider the quotient $R/M = R_0$. Suppose, for a contradiction, that $M$ is not prime, and hence $R_0$ is not an integral domain. Then there exist nonzero elements $a, b \in R_0$ such that $ab = 0$. From this it follows that the (computably definable) annihilator of $a$, $A$, is a nontrivial ideal $0 \subset A \subset R_0$, from which it follows that there is an ideal $M \subset M' \subset R$, which contradicts the fact that $M$ is maximal. □

**Proposition 2.15** ($\mathsf{RCA}_0$). *If $P$ is a prime ideal of $R$, and $A, B$ are ideals of $R$ such that $AB \subseteq P$, then either $A \subseteq P$, or $B \subseteq P$.*

**Proposition 2.16** ($\mathsf{RCA}_0$). *If $I, J$ are ideals of $R$ such that $I + J = R$, then $IJ = I \cap J$.*

**Proposition 2.17** ($\mathsf{RCA}_0$). *If $M$ is a Noetherian $R$-module, then any submodule of $M$ is Noetherian (as an $R$-module), as is any quotient of $M$.*

**Proposition 2.18** ($\mathsf{RCA}_0$). *If $M$ is an Artinian $R$-module, then any submodule of $M$ is Artinian (as an $R$-module), as is any quotient of $M$.*

**Proposition 2.19** ($\mathsf{RCA}_0$). *A sequence of vectors $v_0, v_1, \ldots, v_n \in V$ is linearly independent (with respect to $F$) if and only if $v_0 \neq 0$, and for every $0 \leq k < n$, $v_{k+1}$ is not in the $F$-span of $v_0, v_1, \ldots, v_k$.*

**Proposition 2.20** ($\mathsf{RCA}_0$). *If $V$ has an $F$-basis consisting of $n$ elements, then all $F$-bases of $V$ contain exactly $n$ elements.*

If we add to $\mathsf{RCA}_0$ the formal statement that says for every set $X$ the set $X'$ exists, we obtain the system $\mathsf{ACA}_0$ (Arithmetical Comprehension Axiom). The arithmetic subsets of the natural numbers form a model of $\mathsf{ACA}_0$. Note that $\mathsf{ACA}_0$ is strictly stronger than $\mathsf{RCA}_0$, since $\mathsf{ACA}_0$ implies the existence of $\emptyset'$, a noncomputable set. Proofs that only require arithmetical constructions and verifications are usually valid in $\mathsf{ACA}_0$. For every $n \in \mathbb{N}$, $\mathsf{ACA}_0$ implies $\Sigma^0_n$-induction. Also, for every $n \in \mathbb{N}$, $\Sigma^0_n$-induction implies bounded $\Sigma^0_n$-comprehension (bounded $\Sigma^0_n$-comprehension says that every nonempty $\Sigma^0_n$ subset of $\mathbb{N}$ has a least element).

By Proposition 2.6 above, it follows that Weak König's Lemma is not provable in $\mathsf{RCA}_0$. If we add the formal statement of Weak König's Lemma to the system $\mathsf{RCA}_0$, we obtain the system $\mathsf{WKL}_0$, which is strictly stronger than $\mathsf{RCA}_0$, and strictly weaker than $\mathsf{ACA}_0$. Through a careful analysis of the theorems above, we have the following.

**Theorem 2.21** (Friedman, Simpson, Smith [7, 8]).
1. *Over $\mathsf{RCA}_0$, $\mathsf{ACA}_0$ is equivalent to the statement "Every ring contains a maximal ideal."*
2. *Over $\mathsf{RCA}_0$, $\mathsf{WKL}_0$ is equivalent to the statement "Every ring contains a prime ideal."*

**Theorem 2.22** (Downey, Lempp, Mileti [5]). *Over $\mathsf{RCA}_0$, $\mathsf{WKL}_0$ is equivalent to the statement "Every ring that is not a field contains a nontrivial ideal."*

As an aside we now state a recent result on the reverse mathematics of vector spaces. In our analysis of the reverse mathematics of rings, we shall also prove some facts about the reverse mathematics of vector spaces.

**Theorem 2.23** (Downey, Hirschfeldt, Kach, Lempp, Montalbán, Mileti [4]). *Over $\mathsf{RCA}_0$, $\mathsf{WKL}_0$ is equivalent to the statement "Every vector space of dimension greater than 1 contains a nontrivial proper subspace."*

2.4. **The Plan of the Paper.** In Section 3 we prove that, over $\mathsf{RCA}_0+\mathsf{I}\Sigma_2$, several properties about Artinian rings follow from $\mathsf{WKL}_0$. In Section 4, we construct a computable ring $R$ containing a uniformly computable infinite strictly increasing chain of ideals, and such that every infinite strictly decreasing chain of ideals in $R$ contains a member of PA degree. We then use the existence of $R$ to show that, over

$\mathsf{RCA}_0$, the properties of Section 3 all imply (and hence are equivalent to) $\mathsf{WKL}_0$, as does Theorem 1.9.

In Section 5 we show that, over $\mathsf{RCA}_0$, Theorem 1.11 is implied by $\mathsf{ACA}_0$. From this it also follows that $\mathsf{ACA}_0$ proves Theorem 1.9. Hence, by the end of Section 5, we will have shown that Theorem 1.9 implies $\mathsf{WKL}_0$ and is implied by $\mathsf{ACA}_0$. In Section 6 we construct a computable ring $R$, with arbitrarily large finite strictly increasing chains of computable ideals, and such that every infinite strictly decreasing chain of ideals in $R$ computes the halting set $\emptyset'$. We then use the existence of $R$ to show that the statement "Every Artinian ring is strongly Noetherian" implies $\mathsf{ACA}_0$ over $\mathsf{RCA}_0+\mathsf{B}\Sigma_2$. Thus, by the end of this article we will have shown that, over $\mathsf{RCA}_0+\mathsf{B}\Sigma_2$, Theorem 1.11 is equivalent to $\mathsf{ACA}_0$.

## 3. $\mathrm{WKL}_0$ Upper Bound

The following definitions are standard.

**Definition 3.1.** The *nilradical of* $R$, $N \subset R$, is the set of all nilpotent elements of $R$. It is not difficult to show that $N$ is an ideal of $R$.

**Definition 3.2.** The *Jacobson radical of* $R$, $J \subset R$, is the intersection of all maximal ideals $M \subset R$. Notice that $J$ is an ideal of $R$.

**Definition 3.3.** A subset $S \subseteq R$ is *t-nilpotent* if for any sequence of elements $x_0, x_1, \ldots, x_n, \ldots \in S$, there exists $N \in \mathbb{N}$ such that $\prod_{k=0}^{N} x_k = 0$.

This section is devoted to proving half of the following theorem.

**Theorem 3.4** ($\mathsf{RCA}_0+\mathsf{I}\Sigma_2$)**.** *The following are equivalent.*

1. $\mathsf{WKL}_0$.
2. *If $R$ is Artinian and an integral domain, then $R$ is a field.*
3. *If $R$ is Artinian, then every prime ideal of $R$ is maximal.*
4. *If $R$ is Artinian, then the Jacobson radical $J \subset R$ and nilradical $N \subset R$ exist and are equal.*
5. *If $R$ is Artinian and $J$ exists, then $J \subset R$ is $t$-nilpotent.*
6. *If $R$ is Artinian and $N$ exists, then $R/N$ is Noetherian.*

*Proof.* We shall show that 2–6 are true in $\mathsf{WKL}_0+\mathsf{I}\Sigma_2$. However, the axiom $\mathsf{I}\Sigma_2$ is only used to conclude that 1 implies 6. The reverse implications (i.e. 2–6 imply 1) all hold in $\mathsf{RCA}_0$, and are all proven in Section 4.4.

We reason in $\mathsf{WKL}_0+\mathsf{B}\Sigma_2$. Let $R$ be an Artinian ring. Before we proceed with the proof of Theorem 3.4, we prove a useful lemma, which we shall use repeatedly.

**Lemma 3.5.** *For any infinite sequence of elements $x_0, x_1, x_2, \ldots$ in $R$, we have that, for some $n \in \mathbb{N}$, $x_n$ is an $R$-linear combination of the set $\{x_{n+1}, x_{n+2}, x_{n+3}, \ldots\}$.*

*Proof.* Suppose, for a contradiction, that there exists a sequence of elements $x_0, x_1, x_2, \ldots$ in $R$ such that, for every $n \in \mathbb{N}$, $x_n$ is not an $R$-linear combination of the set $\{x_{n+1}, x_{n+2}, x_{n+3}, \ldots\}$. We shall use this assumption and the power of $\mathsf{WKL}_0$ to construct an infinite strictly descending chain of ideals in $R$, contradicting the fact that $R$ is Artinian. First, we construct a tree $T \subset 2^{<\mathbb{N}}$ such that the paths through $T$ code infinite strictly descending chains of ideals. The construction is as follows.

Let $T \subseteq 2^{<\mathbb{N}}$ be the set of all $\sigma \in 2^{<\mathbb{N}}$ such that

(1) For all $n \in \mathbb{N}$, $\sigma(\langle n, x_{n+1}\rangle) = 1$ if $|\sigma| > \langle n, x_{n+1}\rangle$.
(2) For all $n \in \mathbb{N}$, $\sigma(\langle n, x_n\rangle) = 0$ if $|\sigma| > \langle n, x_n\rangle$.
(3) For all $n \in \mathbb{N}$, if $|\sigma| > \langle n+1, b\rangle$ and $\sigma(\langle n+1, b\rangle) = 1$, then $\sigma(\langle n, b\rangle) = 1$.

(4) For all $n \in \mathbb{N}, b, c \in R$, if $\sigma(\langle n, b\rangle) = \sigma(\langle n, c\rangle) = 1$ and $b +_R c < |\sigma|$, then $\sigma(\langle n, b +_R c\rangle) = 1$.
(5) For every natural number $n$, and elements $, r, b \in R$, if $\sigma(\langle n, b\rangle) = 1$, $r < |\sigma|$, and $r \cdot_R b < |\sigma|$, then $\sigma(\langle n, r \cdot_R b\rangle) = 1$.

The subtree $T \subseteq 2^{<\mathbb{N}}$ exists by $\Delta^0_1$-comprehension. If $f \in 2^{\mathbb{N}}$ is an infinite path through $T$, then the sets $J_n = \{m \in \mathbb{N} : f(\langle n, m\rangle) = 1\}$ code an infinite descending chain of ideals $J_0 \supset J_1 \supset J_2 \supset \cdots$. (1) says that for every $n \in \mathbb{N}$, $x_{n+1} \in J_n$; (2) says that for every $n \in \mathbb{N}$, $x_n \notin J_n$ (note that this implies $1_R \notin J_n$); (3) says that $J_{n+1} \subseteq J_n$ (and so by (1) and (2) we have that $J_{n+1} \subset J_n$); (4) says that if $b, c \in J_n$, then $b +_R c \in J_n$; (5) says that if $b \in J_n$, and $r \in R$, then $r \cdot_R b \in J_n$. From these facts, it follows that the sets $J_n$, $n \in \mathbb{N}$, form an infinite decreasing chain of ideals. All that is left to prove is that $f$ exists, and, since we are assuming Weak König's Lemma, it suffices to show that $T$ is infinite.

Classically, we know that $T$ is infinite since, by hypothesis, we know that the ideals $\langle x_0, x_1, x_2, \ldots\rangle \supset \langle x_1, x_2, \ldots\rangle \supset \langle x_2, x_3, \ldots\rangle \supset \cdots$ form an infinite strictly descending chain in $R$. The same is true in $\mathsf{WKL}_0$. Let $m \in \mathbb{N}$. By bounded $\Sigma^0_1$-comprehension and the fact that for every $n \in \mathbb{N}$, $x_n$ is not an $R$-linear combination of the set $\{x_{n+1}, x_{n+2}, x_{n+3}, \ldots\}$, we can form the string $\sigma \in 2^{<\mathbb{N}}$, $|\sigma| = m$, such that

$$(\forall \langle n, i\rangle < |\sigma|)[\sigma(\langle n, i\rangle) = 1 \leftrightarrow (\exists N > n, \exists r_{n+1}, \ldots, r_N \in R)[i = \sum_{k=n+1}^{N} r_k \cdot_R x_k]].$$

By construction of $\sigma$ and $T$, it follows that $\sigma \in T$. Hence $T$ is infinite and so $f$ exists. This completes the proof of the lemma. □

**Corollary 3.6.** *Let $V$ be a vector space over the field $F$. Then, if $V$ contains an infinite sequence of vectors, $v_0, v_1, v_2, \ldots$, such that for every $n \in \mathbb{N}$, $v_{n+1}$ is not a $F$-linear combination of $\{v_0, v_1, v_2 \ldots, v_n\}$, then $V$ contains an infinite sequence of subspaces $V_0 \supset V_1 \supset V_2 \supset \cdots$.*

*Proof.* The proof is similar to that of Lemma 3.5, and uses the fact that, over $\mathsf{RCA}_0$ the set $\{v_0, v_1, \ldots, v_n\}$ is linearly independent if and only if $\{0\} \subset V^0_0 \subset V^1_0 \subset V^2_0 \subset \cdots \subset V^n_0$, where $V^j_i$ denotes the span of the vectors $\{v_i, v_{i+1}, \ldots, v_j\}$, for any $0 \leq i \leq j \leq n$. □

Now we show that, among other things, $1 \to 2$.

3.1. **1→2.** Suppose that

$$(\exists a \in R)(\forall k \in \mathbb{N})(\forall r \in R)[ra^{k+1} \neq a^k].$$

Then we can construct the infinite sequence of elements $a, a^2, a^3, \ldots$ which contradicts Lemma 3.5. Therefore, we must have that

$$(\forall a \in R)(\exists k \in \mathbb{N})(\exists r \in R)[ra^{k+1} = a^k]. \tag{1}$$

We assume (1) throughout the rest of this section.

To show that $1 \to 2$, suppose that $R$ is an integral domain and fix $a \in R$, $a \neq 0$. We shall show that $a$ is invertible. By (1) above, we have that

$$(\exists k \in \mathbb{N})(\exists r \in R)[ra^{k+1} = a^k],$$

from which it follows that $a^k(ra - 1) = 0$. Now, since $R$ is an integral domain and $a \neq 0$, we have that $a^k \neq 0$, and so we must have that $ra - 1 = 0$, or $ra = 1$. Hence, $a \in R$ is invertible. We now turn our attention to showing that $1 \to 3$.

3.2. **1→3.** In general, it is difficult to prove statements about maximal ideals in $\mathsf{WKL}_0$, because, as is shown in [20], the existence of maximal ideals is equivalent to $\mathsf{ACA}_0$. However, it is usually possible to prove statements about prime ideals in $\mathsf{WKL}_0$, since $\mathsf{WKL}_0$ can prove that every ring has a prime ideal. With this in mind, we prove the following lemma which says that $1 \to 3$.

**Lemma 3.7.** *Every prime ideal $P \subset R$ is maximal.*

*Proof.* Let $P \subset R$ be a prime ideal. We aim to show that $P$ is also maximal. In other words, we shall show that for any $x \notin P$, we have that $1 \in \langle x, P\rangle$.

Suppose that $x \notin P$. Then, by (1), we know that there exist $k \in \mathbb{N}, r \in R$ such that

$$x^k(1 - rx) = 0.$$

Now, since $P$ is prime, and $0 \in P$, (by $\Delta^0_0$-induction on $k$) it follows that either $x \in P$, or $1 - rx \in P$. By hypothesis we know that $x \notin P$, hence $1 - rx \in P$. Therefore, there is some $p \in P$ such that $1-rx = p$. Now, it follows that $p+rx = 1$, and hence $1 \in \langle x, P\rangle$, as required. □

3.3. **1→4.** We now show that $1 \to 4$.

**Lemma 3.8.** *The nilradical $N \subset R$ exists.*

*Proof.* We use $\Delta^0_1$-comprehension to construct $N$. It is clear that the set of nilpotent elements in $R$ is $\Sigma^0_1$-definable; we shall show that the complement is also $\Sigma^0_1$-definable. We claim that the set

$$N^c = \{x \in R : (\exists n \in \mathbb{N}, r \in R)[(x^n = r \cdot x^{n+1}) \wedge (x^n \neq 0)]\}$$

defines the complement of $N$. Since we know that (1) holds, it is clear that if $x \notin N^c$ then $x \in N$. Thus, it suffices to show that no element of $N^c$ is nilpotent. To prove this, let $x \in N^c$. Since $x \in N^c$, there exists a number $n \in \mathbb{N}$ such that $x^n = rx^{n+1} \neq 0$. Now, by $\Delta^0_0$-induction, it follows that for all $m \geq n$ we have $0 \neq x^n = r^{m-n}x^m$ and so $x^m \neq 0$. Hence $x$ is not nilpotent. This completes the proof. □

**Lemma 3.9.** *The intersection of all prime ideals $P \subset R$ is equal to the nilradical of $R$.*

*Proof.* It is clear that if $x \in R$ is nilpotent, then $x$ must be contained in every prime ideal $P \subset R$. Therefore, it suffices to show that, for every $x \in R$, if $x$ is not nilpotent then there is a prime ideal $P \subset R$ with $x \notin P$. The construction of such a prime ideal $P \subset R$ is similar to the construction in [20] (Lemma IV.6.2), which shows that in $\mathsf{WKL}_0$ every countable commutative ring with identity contains a prime ideal.

Let $\{a_i : i \in \mathbb{N}\}$ be an enumeration of the elements of $R$, and fix $x \in R$ such that for all $n \in \mathbb{N}$, $x^n \neq 0$. Then, using primitive recursion, define a sequence of codes for finite sets $X_\sigma \subseteq R$, $\sigma \in 2^{<\mathbb{N}}$, beginning with $X_\emptyset = \{0_R\}$ as follows. Let $\sigma \in 2^{<\mathbb{N}}$ be given, and suppose that $X_\sigma$ has been defined. Let

$$|\sigma| = 4 \cdot \langle i, j, m\rangle + k,\ 0 \leq k < 4.$$

Case 1: $k = 0$. If $a_i \cdot a_j \in X_\sigma$, put $X_{\sigma 0} = X_\sigma \cup \{a_i\}$ and $X_{\sigma 1} = X_\sigma \cup \{a_j\}$. Otherwise, put $X_{\sigma 0} = X_\sigma$ and $X_{\sigma 1} = \emptyset$.

Case 2: $k = 1$. Put $X_{\sigma 0} = \emptyset$. If $a_i, a_j \in X_\sigma$, put $X_{\sigma 1} = X_\sigma \cup \{a_i + a_j\}$. Otherwise, put $X_{\sigma 1} = X_\sigma$.

Case 3: $k = 2$. Put $X_{\sigma 0} = \emptyset$. If $a_i, a_j \in X_\sigma$, put $X_{\sigma 1} = X_\sigma \cup \{a_i \cdot a_j\}$. Otherwise, put $X_{\sigma 1} = X_\sigma$.

Case 4: $k = 3$. Put $X_{\sigma 0} = \emptyset$. If $x^m \in X_\sigma$, put $X_{\sigma 1} = \emptyset$. Otherwise, put $X_{\sigma 1} = X_\sigma$.

Let $S \subseteq 2^{<\mathbb{N}}$ be the set of all $\sigma$ such that $X_\sigma \neq \emptyset$. Clearly, $S$ is a tree.

We claim that, for each $m, n \in \mathbb{N}$, there exists $\sigma \in S$ of length $n$ such that $x^m \notin \langle X_\sigma \rangle$. For $n = 0$, this claim is trivial since by hypothesis we have that, for all $m \in \mathbb{N}$, $x^m \neq 0$. If $n \equiv 1, 2, 3 \mod 4$ and the claim holds for $n$ then it also holds for $n+1$. Suppose that $n \equiv 0 \mod 4$ and the claim holds for $n$. We shall show that it also holds for $n+1$. Let $\sigma \in S$ be of length $n$ such that $x^m \notin \langle X_\sigma \rangle$, for all $m \in \mathbb{N}$, and let $n = 4\langle i, j, m \rangle$. If $a_i \cdot a_j \notin X_\sigma$, then the claim trivially holds for $n+1$. On the other hand, if $a_i \cdot a_j \in X_\sigma$, then we make a subclaim that $X_{\sigma 0} = X_\sigma \cup \{a_i\}$ and $X_{\sigma 1} = X_\sigma \cup \{a_j\}$ do not both generate elements $x^{m_0}, x^{m_1} \in R$. If they did, then we would have

$$x^{m_0} = c + ra_i \text{ and } x^{m_1} = d + sa_j,$$

where $r, s \in R$ and $c, d$ are finite linear combinations of elements of $X_\sigma$ with coefficients from $R$. Then,

$$x^{m_0+m_1} = cd + csa_j + dra_i + rsa_ia_j,$$

and so $x^{m_0+m_1} \in \langle X_\sigma \rangle$, a contradiction. This proves the subclaim, and hence our claim holds for $n+1$. The claim now follows for all $n \in \mathbb{N}$ by $\Pi^0_1$-induction on $n$.

We have that $S \subset 2^{<\mathbb{N}}$ is infinite. Hence, by Weak König's Lemma, $S$ has an infinite path, $f \in [S]$. Now, using $f$ and bounded $\Sigma^0_1$-comprehension, we construct the desired prime ideal $P \subset R$ such that $x \notin P$.

Without loss of generality, assume that $a_0 = 0$ and $a_1 = x$. We construct a tree $T \subseteq 2^{<\mathbb{N}}$ such that every infinite path through $T$ codes a prime ideal $P \subset R$ such that $x \notin P$. Let $T$ be the set of all $\tau \in 2^{<\mathbb{N}}$ such that

(1) $0 < |\tau|$ implies $\tau(0) = 1$.
(2) $1 < |\tau|$ implies $\tau(1) = 0$.
(3) If $i, j, k < |\tau|$, $\tau(i) = \tau(j) = 1$, and $a_i +_R a_j = a_k$ then $\tau(k) = 1$.
(4) If $i, j, k < |\tau|$, $\tau(i) = 1$, and $a_i \cdot_R a_j = a_k$ then $\tau(k) = 1$.
(5) If $i, j, k < |\tau|$, $\tau(i) = \tau(j) = 0$, and $a_i \cdot_R a_j = a_k$ then $\tau(k) = 0$.

Condition (1) says that every subset of $R$ coded by a path through $T$ contains $0 \in R$. Condition (2) says that every subset of $R$ coded by a path through $T$ does not contain $x \in R$. Condition (3) says that every subset of $R$ coded by a path through $T$ is closed under $+_R$. Condition (4) says that every subset of $R$ coded by a path through $T$ is closed under multiplication by elements from $R$. Condition (5) says that the complement of every subset coded by a path through $T$ is closed under $\cdot_R$. When taken together, conditions (1)-(5) above imply that every path through $T$ codes a prime ideal not containing $x \in R$. Formally (i.e. in $\mathsf{WKL}_0$), the proof is as follows.

By construction, it follows that $T \subset 2^{<\mathbb{N}}$ is closed downwards, and thus $T$ is a tree. We claim that $T$ is also infinite. To see why $T$ is infinite, let $m \in \mathbb{N}$ be given, and by bounded $\Sigma^0_1$ comprehension let $Y$ be the set of all $i < m$ such that $(\exists n)[a_i \in X_{F(n)}]$, where $F(n) = \langle f(0), f(1), \cdots, f(n-1) \rangle \in 2^{<\mathbb{N}}$. Now, define $\tau \in 2^{<\mathbb{N}}$, $|\tau| = m$, by setting $\tau(i) = 0$, if $i \in Y$, and $\tau(i) = 1$, if $i \notin Y$. Then we have that $\tau \in T$ and $|\tau| = m$. Hence, $T$ is infinite. Therefore, applying weak König's Lemma to $T$ yields an infinite path $g \in [T]$, and letting $P = \{a_i \in R : i \in \mathbb{N}, g(i) = 1\}$ constructs the desired prime ideal $P \subset R$ such that $x \notin P$. This completes the proof of the corollary. □

By Lemmas 3.8 and 3.9, we know that the intersection of all prime ideals in $R$ exists and is equal to $N$, the nilradical of $R$. Also, by Lemma 3.7, we know that $N = J$, where $J$ is the Jacobson radical of $R$. Thus, we have that $1 \to 4$. We now show that $1 \to 5$.

3.4. **1→5.** Suppose that $x_0, x_1, x_2, \ldots, x_n, \ldots \in N$ is an infinite sequence of (not necessarily distinct) nilpotent elements in $R$ such that, for every $n \in \mathbb{N}$, $y_n = \prod_{i=0}^{n} x_i \neq 0$. Then we claim that for every $n \in \mathbb{N}$ and $r \in R$, $ry_{n+1} \neq y_n$. Suppose, for a contradiction, that there exists an element $r \in R$ such that $ry_{n+1} = y_n$. By definition of $y_{n+1}$, we have that $y_{n+1} = x_{n+1}y_n$. Hence, it follows that $y_n(1 - rx_{n+1}) = 0$. But $x_{n+1} \in N$ is nilpotent, and therefore $1 - rx_{n+1}$ is a unit (with inverse $\sum_{k=0}^{\infty}(rx_{n+1})^k$). Thus, $y_n = 0$, a contradiction. Thus, we have constructed a sequence of elements of $R$, $y_0, y_1, y_2, \ldots$, such that for every $n \in \mathbb{N}$, $y_n$ is not an $R$-linear combination of $\{y_{n+1}, y_{n+2}, y_{n+3}, \ldots\}$, contradicting Lemma 3.5. This proves that $N \subset R$ is in fact $t$-nilpotent, and hence $1 \to 5$.

3.5. **1→6.** We now turn our attention to proving that $1 \to 6$. Since $\mathsf{RCA}_0$ proves that if $R$ is an Artinian ring, then any quotient of $R$ is also Artinian, we can assume that $J = \{0\}$. Let $I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots$ be an infinite strictly increasing chain of ideals in $R$. We aim to show that there is an infinite strictly decreasing chain of ideals $R \supseteq J_0 \supset J_1 \supset J_2 \supset \cdots$.

3.5.1. *Constructing an infinite strictly decreasing chain of ideals in R.* We wish to use $\mathsf{WKL}_0$ to construct a set $X$ such that, for every $n \in \mathbb{N}$ the set $X_n = \{k \in \mathbb{N} : \langle n, k\rangle \in X\}$ is a prime (and hence maximal) ideal that does not contain some element $x \in (\cap_{i=0}^{n-1} X_i) \setminus J$. There are two cases to consider. The first case says that for any $n \in \mathbb{N}$, and any sequence of maximal ideals $M_0, M_1, \cdots, M_n \subset R$, there is a maximal ideal $M \subset R$ such that $M \cap M_0 \cap M_1 \cap \cdots \cap M_n \subset M_0 \cap M_1 \cap \cdots \cap M_n$, and the second case says that there exists some number $n \in \mathbb{N}$, and a sequence of maximal ideals $M_0, M_1, M_2, \cdots M_n$, such that $M_0 \cap M_1 \cap \cdots \cap M_n = 0$ (by definition of $J$, it follows that the negation of case 2 is case 1).

**Case 1.** Suppose that we are in the first case, and let $x_0, x_1, x_2, \ldots$ be an enumeration of elements of $R \setminus \{0\}$. Via an argument similar to the proof of Lemma 3.9, we can construct a sequence of prime (and hence maximal) ideals $M_0, M_1, M_2, \ldots$ such that, for every $k \in \mathbb{N}$, $x_k \notin M_k$. Then, via $\Delta^0_1$-comprehension and the fact that we are in case 1, we can construct an infinite sequence of numbers $c_0 < c_1 < c_2 < \cdots$ such that for every $k \in \mathbb{N}$, we have that $\cap_{i=0}^{k} M_{c_i} \supset \cap_{i=0}^{k+1} M_{c_i}$. It follows that $M_{c_0} \supset M_{c_0} \cap M_{c_1} \supset M_{c_0} \cap M_{c_1} \cap M_{c_2} \supset \cdots$ is an infinite strictly decreasing sequence of ideals in $R$. This ends the proof of case 1.

Observe that in the previous paragraph we did not use the hypothesis that the chain of ideals $I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots \subseteq R$ exists. This observation is used in Section 5 to show that $\mathsf{ACA}_0$ proves the existence of finitely many maximal ideals whose intersection is the Jacobson radical of $R$ (i.e. we are in case 2).

**Case 2.** Let $R = M_0$, and $M_1, M_2, \cdots, M_T$ be maximal ideals such that $\cap_{i=0}^{T} M_i = J = 0$. Using bounded $\Sigma^0_1$-comprehension, we can assume, without loss of generality, that $M_0, M_1, M_2, \ldots, M_T$ are distinct ideals. Now, since $M_1, M_2, \ldots, M_T$ are distinct maximal ideals, we have that for every $i = 0, 1, 2, \cdots, T-1$, $M_0 \cap M_1 \cap \cdots \cap M_i + M_{i+1} = R$, and hence it follows that $M_1 \cap M_2 \cap \cdots \cap M_i = M_1 M_2 \cdots M_i$. For every $i = 0, 1, 2, \ldots T-1$, define $V_i$ to be the $R/M_{i+1}$-vector space $M_0 M_1 \cdots M_i / M_0 M_1 \cdots M_{i+1}$.

Recall that $I_0 \subset I_1 \subset I_2 \subset \cdots$ is an infinite strictly increasing chain of ideals in $R$. Using bounded $\Sigma^0_2$-comprehension (which is equivalent to $\Sigma^0_2$-induction), find the greatest number $n < T$ such that the set

$$\{m \in \mathbb{N} : (I_{m+1} \setminus I_m) \cap M_0 M_1 M_2 \cdots M_n \neq 0\}$$

is not finite (note that $n = 0$ satisfies this condition, since $M_0 = R$). By definition of $n$, there is a number $m_0 \in \mathbb{N}$ such that for all $m \geq m_0$ we have $(I_{m+1} \setminus I_m) \cap M_0 M_1 M_2 \cdots M_n M_{n+1} = \emptyset$. Without loss of generality (i.e. by passing to an infinite subsequence of $\{I_m\}_{m\in\mathbb{N}}$), assume that $m_0 = 0$. By $\Delta^0_1$-comprehension, we can construct an infinite sequence of numbers, $a_0 < a_1 < a_2 < \cdots < a_m < \cdots$, such that for every $m \in \mathbb{N}$ there exists an element $0 \neq x_{m+1} \in (I_{a_m+1} \backslash I_{a_m}) \cap M_0M_1 \cdots M_n$. Without loss of generality (i.e. by passing to an infinite subsequence of $\{I_m\}_{m\in\mathbb{N}}$), assume that for every $m \in \mathbb{N}$, $a_m = m$. Now, for every $m \geq 0$, let $v_m \in V_n$ be the image of $x_m \in M_0M_1 \cdots M_n$ under the canonical quotient map $\varphi : M_0M_1 \cdots M_n \to V_n$.

We claim that for every number $m \geq 0$, $v_m \in V_n$ is not in the subspace generated by $\{v_0, v_1, \ldots, v_{m-1}\}$. For suppose that we had $v_m = \sum_{k=0}^{m-1} r_k v_k$. It follows that $v_m - \sum_{k=0}^{m-1} r_k v_k = 0 \in V_n$, and thus $x_m - \sum_{k=0}^{m-1} r_k x_k \in (I_m \setminus I_{m-1}) \cap M_0M_1 \cdots M_nM_{n+1}$, a contradiction. Therefore, we have that for every number $n \in \mathbb{N}$, $v_n$ is not an $R/M_{n+1}$-linear combination of $\{v_0, v_1, \ldots, v_{n-1}\}$, and so, by Corollary 3.6, $V$ contains an infinite strictly decreasing sequence of subspaces $V \supseteq \hat{J}_0 \supset \hat{J}_1 \supset \hat{J}_2 \supset \cdots \supset \hat{J}_m \supset \cdots$.

Now, if for every $m \in \mathbb{N}$ we let $J_m = \varphi^{-1}(\hat{J}_m)$, then we have that $R \supseteq J_0 \supset J_1 \supset J_2 \supset \cdots$ is an infinite strictly decreasing chain of ideals in $R$. Thus, we have shown that $1 \to 6$. □

## 4. $\mathsf{WKL}_0$ Lower Bound

The main goal of this section is to prove that, over $\mathsf{RCA}_0$, each of the properties 2–6 in Theorem 3.4 implies $\mathsf{WKL}_0$, as does Theorem 1.9. Achieving this goal consists mostly of proving the following theorem.

**Theorem 4.1.** *There is an integral domain $R$ containing an infinite uniformly computable increasing sequence of ideals $I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_N \subset \cdots$, and such that every infinite decreasing sequence of ideals $J_0 \supset J_1 \supset J_2 \supset \cdots$ in $R$ contains some $J_n$ of PA degree.*

*Proof.* The proof consists of four parts. First, we describe the basic idea behind the proof, and give the basic module of the construction of $R$. Next, we construct the ring $R$. Afterwards, we show that $R$ contains a uniformly computable increasing chain of ideals, and finally, we verify that every infinite decreasing sequence of ideals in $R$ contains an element that is of PA degree.

Let $R_0 = \mathbb{Q}[X_{\langle N,k\rangle} : \langle N, k\rangle \in \mathbb{N}]$. The ring $R$ shall be of the form $R_0[\mathfrak{Y}]$, for a set of (dependent) variables $\mathfrak{Y}$ which we shall define in Section 4.2. Before we give the full construction of $R$, which is rather technical, we describe its first step in complete detail. By thoroughly examining the first step of the construction of $R$, we shall give the reader the motivation and main ideas behind the entire construction.

Let $R$ and $S$ be rings such that $R \subset S$. Then, if $I$ is either a subset of $R$, or a sequence of elements in $R$, the notation $\langle I\rangle_R$ denotes the ideal generated by $I$ *in the ring $R$*.

We start by extending $R_0$ to a computable ring $R_1$, with the following properties.

1. There is a uniformly computable, strictly increasing sequence of ideals $I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_N \subset \cdots$ in $R_1$.
2. Every ideal $J \subset R_1$ that is not of PA degree satisfies
$$J \cap R_0 = \langle X_{\langle N',k\rangle} : N' \leq N, k \in \mathbb{N}\rangle_{R_0}, \text{ for some } N \in \mathbb{N} \cup \{\infty\}.$$

The motivation behind property 1 is obvious. To motivate property 2, let $J_0 \supset J_1 \supset J_2 \supset \cdots$ be an infinite strictly decreasing chain of ideals in $R_1$ such that the sequence of ideals $J_0 \cap R_0 \supset J_1 \cap R_0 \supset J_2 \cap R_0 \supset \cdots$ is also strictly decreasing. We claim that property 2 implies that at least one of the $J_N \cap R_0$, $N \in \mathbb{N}$, is of PA degree. To see why this is the case, suppose that $R_1$ satisfies 2, and note that either

$J_2 \cap R_0$ is of PA degree, or else we have that $J_2 \cap R_0 = \langle X_{\langle N',k\rangle} : N' \leq N, k \in \mathbb{N}\rangle_{R_0}$, for some $N \in \mathbb{N}$. In the former case we are done, so suppose that we are in the latter case. Then it follows that one of the ideals $J_3 \cap R_0, J_4 \cap R_0, \ldots, J_{N+3} \cap R_0$ is not equal to $\langle X_{\langle N',k\rangle} : N' \leq M, k \in \mathbb{N}\rangle_{R_0}$, for any $M \in \mathbb{N}$, and hence (by property 2) must be of PA degree.

If we could show that every infinite strictly decreasing chain of ideals in $R_1$ contains a member of PA degree, then we could set $R = R_1$ and we would be done. However, the best that we can show for now is that for every infinite strictly decreasing chain of ideals $J_0 \supset J_1 \supset J_2 \supset \cdots$ in $R_1$, if the chain $J_0 \cap R_0 \supset J_1 \cap R_0 \supset J_2 \cap R_0 \supset \cdots$ is also strictly decreasing then it contains a member of PA degree. To overcome this current shortcoming, we shall make infinitely many (uniformly computable) ring extensions $R_0 \subset R_1 \subset R_2 \subset \cdots$, and set $R = \cup_{s\in\mathbb{N}} R_s$. Furthermore, we shall be careful in maintaining the fact that $R$ satisfies property 1.

4.1. **Constructing the ring $R_1 \supset R_0$.** First, we need some definitions. Fix disjoint c.e. sets $A$ and $B$ such that any set $C$ with $A \subseteq C$ and $C \cap B = \emptyset$ is of PA degree, and let $\alpha, \beta : \mathbb{N} \to \mathbb{N}$ be computable 1-1 functions with range $A$ and $B$, respectively. Also, for any quotient of polynomials, $q \in \mathbb{Q}(X_{\langle N,k\rangle} : \langle N, k\rangle \in \mathbb{N})$, let $M(q)$ be the value of the largest pair $\langle N, k\rangle \in \mathbb{N}$ such that $X_{\langle N,k\rangle}$ appears in $q$, and for any polynomial $p \in R_0$, let $N(p)$ be the least number $N \in \mathbb{N}$ such that $p$ can be written in the form $p = C + p'$ with $C \in \mathbb{Q}$ and $p' \in \langle X_{\langle N',k\rangle} : N' \leq N, k \in \mathbb{N}\rangle_{R_0}$.

To construct $R_1$ from $R_0$, let

$$\mathfrak{Y}_{-1} = \{Y_{\langle N,N',k,l\rangle} : N, N', k, l \in \mathbb{N}, l < \beta(k), N' \leq N\}, \text{ and}$$

$$\mathfrak{Z} = \{Z_{\langle p,i\rangle} : 0 \neq p \in R_0, \alpha(i) > M(p)\}$$

be sets of formal symbols. Now set $\mathfrak{Y}_0 = \mathfrak{Z} \cup \mathfrak{Y}_{-1}$, and define $R_1 = R_0[\mathfrak{Y}_0]/\cong$, where $\cong$ is an equivalence relation that is defined in the next paragraph. Note that, for every $r \in R_1$, we can write $r$ in the form

$$r = \sum_{k=0}^{n} f_k Y_k,$$

where $f, f_k \in R_0$ and $Y_k$ is a product of elements from $\mathfrak{Y}_0$, $0 \leq k \leq n$. We call such an expression a *code* for $r \in R_1$.

Let $\varphi_0 : R_1 \to \mathbb{Q}(X_{\langle N,k\rangle} : \langle N, k\rangle \in \mathbb{N})$ be the unique (computable) homomorphism of rings that fixes $R_0$, and such that

$$\varphi_0(Y_{\langle N,N',k,l\rangle}) = \frac{X_{\langle N',l\rangle}}{X_{\langle N,\beta(k)\rangle}}, \text{ and}$$

$$\varphi_0(Z_{\langle p,i\rangle}) = \frac{X_{\langle N(p),\alpha(i)\rangle}}{p}.$$

Note that $\varphi_0$ is injective on the set $\mathfrak{Y}_0$. For any two elements $r, s \in R_1$, we define $r \cong s$, and write $r = s$, if $\varphi_0(r) = \varphi_0(s)$. It follows that $R_1$ is a computable ring. We shall sometimes identify the elements of $\mathfrak{Y}_0$ with their images under $\varphi_0$. In particular, we shall refer to the numerators and denominators of these elements.

The idea behind the definitions of $\varphi_0(Z_{\langle p,i\rangle})$ and $\varphi_0(Y_{\langle N,N',k,l\rangle})$ above is as follows. Suppose that some element $r_1 \in R_1$ is contained in an ideal $J \subsetneq R_1$ not of PA degree. Then, since $J$ is an ideal, we have that there is also some $r_0 \in R_0$ in $J$ ($r_0 \in R_0$ is such that $\varphi(r_0)$ is equal to the numerator of $\varphi_0(r_1)$). Now, since $\mathfrak{Z} \subset R_1$, then for $N = N(r_0) \in \mathbb{N}$ and large enough $i \in \mathbb{N}$ we have that $X_{\langle N,\alpha(i)\rangle} \in J$. Now, since $J$ is not of PA degree, $J$ must also contain infinitely many elements of the form $X_{\langle N,\beta(j)\rangle}$, $j \in \mathbb{N}$. Otherwise, the set $\{k \in \mathbb{N} : X_{\langle N,k\rangle} \in J\} \leq_T J$

would be a separator for $\operatorname{ran}(\alpha)$ and $\operatorname{ran}(\beta)$ on some cofinal interval of $\mathbb{N}$. Now, since $\mathfrak{Y}_{-1} \subset R_1$, it follows that every element of the form $X_{\langle N',k\rangle}$, $N' \leq N, k \in \mathbb{N}$, is contained in $J$, and so $J \supseteq \langle X_{\langle N',k\rangle} : N' \leq N, k \in \mathbb{N}\rangle_{R_0}$. Hence, we have shown that if $J \subseteq R_1$ is an ideal that is not of PA degree, then $J$ must contain $\langle X_{\langle N',k\rangle},\ N' \leq N, k \in \mathbb{N}\rangle_{R_0}$ for every number $N = N(r_0)$ such that $r_0 \in R_0$ is the numerator of some $\varphi_0(r_1)$, $r_1 \in R_1$. It follows that $J \cap R_0 = I_N \cap R_0$, where $N \in \mathbb{N} \cup \{\infty\}$ is such that $N = \sup\{N(p) : p \in R_0 \cap J\}$ and $I_\infty = \cup_{M \in \mathbb{N}} I_M$. Note that $I_\infty$ is a maximal ideal of $R_1$.

Now, let $J_0 \supset J_1 \supset J_2 \supset \cdots \supset J_n \supset \cdots$ be an infinite strictly decreasing chain of ideals in $R_1$ such that the chain of ideals $J_0 \cap R_0 \supset J_1 \cap R_0 \supset J_2 \cap R_0 \supset \cdots$ is also strictly decreasing. Then, by the results in the previous paragraph, we have that $J_2$ must either be of PA degree, or equal to some $I_N$, $N \in \mathbb{N}$. If $J_2$ is of PA degree, then we have property 2. Otherwise, $J_2 = I_N$ for some $N \in \mathbb{N}$. Since the chain of ideals $J_0 \cap R_0 \supset J_1 \cap R_0 \supset J_2 \cap R_0 \supset \cdots$ is strictly decreasing, then one of the ideals $J_3 \cap R_0, J_4 \cap R_0, \ldots, J_{N+3}$ is of PA degree. Therefore, $R_1$ satisfies property 2.

Proving that $R_1$ satisfies property 1 is no simpler than proving the following lemma, whose proof we defer to later.

**Lemma 4.2.** *Fix $N \in \mathbb{N}$. Then for every $z \in R$, if $z \in I_N$ and $z = g + \sum_{j=0}^{m} g_j Z_j$ is a code for $z$, then the numerators of $g, g_j Y_j$, $j = 0, 1, \ldots, m$, belong to the ideal $\langle X_{\langle N',k\rangle} : N' \leq N, k \in \mathbb{N}\rangle_{R_0}$.*

For every $N \in \mathbb{N}$, let $I_N \subset R_1$ be the set of elements $r \in R_1$ such that $r$ can be written as $r = \sum_{k=0}^{n} f_k Y_k$ and such that the numerator of $f, f_k Y_k$ is in $\langle X_{\langle N',k\rangle} : N' \leq N, k \in \mathbb{N}\rangle_{R_0}$ for every $0 \leq k \leq n$. Briefly speaking, Lemma 4.2 says that if $r \in I_N$, then *every* expression for $r$, $r = \sum_{k=0}^{n} f_k Y_k$, is such that the numerators of $f, f_k Y_k$, $0 \leq k \leq n$, belong to $\langle X_{\langle N',k\rangle} : N' \leq N, k \in \mathbb{N}\rangle_{R_0}$. We now verify that Lemma 4.2 implies that the ideals $I_0 \subset I_1 \subset \cdots I_N \subset \cdots$ form a uniformly computable infinite strictly increasing chain in $R_1$. First, to determine whether or not a given $r \in R$, $r = \sum_{k=0}^{n} f_k Y_k$, is in $I_N$ one simply checks to see if the numerators of $f, f_k Y_k$ belong to $\langle X_{\langle N',k\rangle} : N' \leq N, k \in \mathbb{N}\rangle_{R_0}$, for every $0 \leq k \leq n$. Hence the chain is uniformly computable. Secondly, to verify that the chain is strictly increasing, note that by Lemma 4.2, for every $N \geq 1$, $X_{\langle N,0\rangle} \in I_N$, but $X_{\langle N,0\rangle} \notin I_{N-1}$.

A brief intuition as to why Lemma 4.2 is true is as follows. For every $y_0 \in \mathfrak{Y}_0$, we have chosen the element $\varphi_0(y_0)$ carefully so that if its numerator is of the form $X_{\langle N,k\rangle}$, then for every monomial $m$ occurring its denominator, we have that $m$ is either constant (in the case $y_0 = Z_{\langle p,i\rangle}$, for some $p \in R_0$ with a nontrivial constant term), or else $m$ contains an occurrence of some $X_{\langle N',k'\rangle}$ with $N' \geq N$. This makes it impossible for $y_0 r \in I_{N'}$, $N < N'$, unless $r \in I_{N'}$. Hence, $R_1 I_N = I_N$.

4.2. **Constructing the ring $R$.** Having now seen the first step in the construction and verification of the ring $R$, we are ready to proceed with the full construction. Recall that the reason why we cannot simply set $R = R_1$ is that we cannot prove an analogous version of property 2 for ideals in the ring $R_1$ (property 2 talks about descending chains of ideals in $R_1$ restricted to $R_0$). We shall spend the rest of this section constructing the ring $R \supset R_1$ without such a deficiency.

The key fact that allowed us to show $R_1$ satisfies property 2 is that if $J \subset R_1$ is an ideal that is not of PA degree, then $J \cap R_0 = I_N = \langle X_{\langle N',k\rangle} : N' \leq N, k \in \mathbb{N}\rangle$. Furthermore, to show this, we used the fact that $\mathfrak{Y}_0 \in R_1$. We would like to prove a similar statement about ideals of the form $J \cap R_1$, but, in order to do so, we must extend $R_1$ to a new ring $R_2$ (in the same way we extended $R_0$ to $R_1$), and so on. Therefore, to construct the ring $R$, we shall make countably many extensions

$R_0 \subset R_1 \subset R_2 \subset \cdots \subset R_n \subset \cdots$ (and set $R = \cup_{s\in\mathbb{N}} R_s$), so that the subring $R_n \subset R_{n+1}$ satisfies property 2 in the same way that $R_0 \subset R_1$ satisfies property 2. Moreover, our extensions shall be done carefully, so that in the end $R$ also satisfies property 1.

We are now in good shape to construct the ring $R = \cup_{s\in\mathbb{N}} R_s$. But, before we do, we need some definitions. Let $\mathbb{N}^*$ be the set of all finite sequences of natural numbers, and for any $\sigma = \langle\sigma(0), \sigma(1), \ldots, \sigma(n-1)\rangle \in \mathbb{N}^*$ let $\beta(\sigma) = \langle\beta(\sigma(0)), \beta(\sigma(1)), \ldots, \beta(\sigma(n-1))\rangle$. Let $|\sigma|$ denote the length of $\sigma$, and write $\sigma^-$ for the sequence $\langle\sigma(0), \sigma(1), \cdots, \sigma(|\sigma|-2)\rangle$. We say that $\sigma \in \mathbb{N}^*$ is strictly increasing if, for every $0 \le i < |\sigma| - 1$, we have that $\sigma(i) < \sigma(i+1)$. Let $\mathbb{N}^<$ be the set of strictly increasing elements of $\mathbb{N}^*$. Furthermore, for $\sigma \in \mathbb{N}^*, N \in \mathbb{N}$, let $\sigma > N$ if $\min\{\sigma(i) : i < |\sigma|\} > N$ (similarly define $\sigma \ge N$). Also, for any $\sigma, \tau \in \mathbb{N}^*$ such that $|\tau| = |\sigma|$, define $X_{\langle\tau,\sigma\rangle}$ to be the monomial $\prod_{i=0}^{n-1} X_{\langle\tau(i),\sigma(i)\rangle} \in R_0$. If $\tau = \sigma = \emptyset$, then set $X_{\langle\tau,\sigma\rangle} = 1$.

Now, fix $s \ge 0$, and define

$$\mathfrak{Y}_s = \{Y_{\langle N',l,\tau,\sigma\rangle}\} \cup \{Z_{\langle p,i,\tau,\sigma\rangle}\},$$

where $\langle N', l, \tau, \sigma\rangle$ ranges over all 4-tuples such that:

(1) $N', l \in \mathbb{N},\ \tau, \sigma \in \mathbb{N}^*$, $\beta(\sigma) \in \mathbb{N}^<$.
(2) $|\tau| = |\sigma| \le s + 1$.
(3) $N' \le \tau$.
(4) $l < \beta(\sigma)$.

and $\langle p, i, \tau, \sigma\rangle$ ranges over all 4-tuples such that:

(1) $0 \ne p \in R_0,\ i \in \mathbb{N},\ \tau, \sigma \in \mathbb{N}^*,\ \beta(\sigma) \in \mathbb{N}^<$.
(2) $|\tau| = |\sigma| \le s + 1$.
(3) $M(p) < \alpha(i) < \beta(\sigma)$.
(4) $N(p) \le \tau$.

We set $R_{s+1} = R_0[\mathfrak{Y}_s]/\cong$, where $\cong$ is an equivalence relation on $R_{s+1}$ that is defined in the next paragraph. By definition of $\cong$, we will have that $R_s$ is a subring of $R_{s+1}$.

Let $\varphi_s : R_{s+1} \to \mathbb{Q}(X_{\langle N,k\rangle} : \langle N, k\rangle \in \mathbb{N})$ be the unique (computable) homomorphism of rings that fixes $R_0$, and such that

$$\varphi_s(Y_{\langle N',l,\tau,\sigma\rangle}) = \frac{X_{\langle N',l\rangle}}{X_{\langle\tau,\beta(\sigma)\rangle}}, \text{ and}$$

$$\varphi_s(Z_{\langle p,i,\tau,\sigma\rangle}) = \frac{X_{\langle N(p),\alpha(i)\rangle}}{pX_{\langle\tau,\beta(\sigma)\rangle}}.$$

Note that although we have redefined $\mathfrak{Y}_0$ and $\varphi_0$, the new definitions are equivalent to the old ones. Also, note that $\varphi_s \subset \varphi_{s+1}$. For any two elements $r, s \in R_{s+1}$, we let $r \cong s$, and write $r = s$, if $\varphi_s(r) = \varphi_s(s)$. Hence, $R_{s+1}$ is a computable integral domain, since $\mathbb{Q}(X_{\langle N,k\rangle} : \langle N, k\rangle \in \mathbb{N})$ is a computable integral domain. In practice we shall sometimes identify the elements of $\mathfrak{Y}_s$ with their images under $\varphi_s$. In particular, we shall refer to the numerators and denominators of these elements. By a *code* for an element $r \in R$, we shall mean an expression (i.e. sum) of the form

$$S = f + \sum_{k=0}^{n} f_k Y_k,$$

such that $r = S$, $f, f_k \in R_0$, and $Y_k$ is a product of elements from $\mathfrak{Y} = \cup_{s=0}^{\infty} \mathfrak{Y}_s$, for all $0 \le k \le n$. We now verify that $R$ satisfies the criteria of Theorem 4.1. Let $\varphi : R \to \mathbb{Q}(X_{\langle N,k\rangle} : \langle N, k\rangle \in \mathbb{N})$ be defined as $\varphi = \cup_{s\in\mathbb{N}} \varphi_s$, and let $\mathfrak{Y} = \cup_{s\in\mathbb{N}} \mathfrak{Y}_s$.

4.3. **Verifying that $R$ has the desired properties.** In this section we complete the proof of Theorem 4.1 by verifying that $R$ satisfies the following two properties.

(1) $R$ contains a uniformly computable, infinite strictly increasing chain of ideals.
(2) Every infinite strictly decreasing chain of ideals in $R$ contains a member that is of PA degree.

To show that $R$ satisfies property 1, we exhibit an infinite uniformly computable increasing sequence of ideals $I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_N \subset \cdots$ in $R$.

For every $N \in \mathbb{N}$, let $I_N \subset R$ be the set of elements $r \in R$ such that $r$ has a code of the form $r = \sum_{k=0}^{n} f_k Y_k$ and such that the numerator of $f$, and of $f_k Y_k$, $k = 0, 1, 2, \ldots, n$, is in $\langle X_{\langle N', k \rangle} : N' \leq N, k \in \mathbb{N} \rangle_{R_0}$, for every $0 \leq k \leq n$. Also, define $I_\infty = \cup_{s \in \mathbb{N}} I_s$. By construction, it is clear that $I_N \subset R$ is an ideal for every $N \in \mathbb{N}$. Also, by the construction of $\mathfrak{Y}_s,\ s \in \mathbb{N}$, we have the following proposition.

**Proposition 4.3.** *Fix $s \in \mathbb{N}$. If $y \in \mathfrak{Y}_s$, then $y \in I_\infty$. Also, if the numerator of $y$ is not in $I_N \cap R_0$, then neither is the denominator of $y$.*

We now prove Lemma 4.2, which says that for every $z \in R$, if $z \in I_N$ and $z = g + \sum_{j=0}^{m} g_j Z_j$ is a code for $z$, then the numerators of $g, g_j Z_j,\ j = 0, 1, \ldots, m$, belong to the ideal $\langle X_{\langle N', k \rangle} : N' \leq N, k \in \mathbb{N} \rangle_{R_0}$. It was shown earlier that a consequence of this lemma is that the ideals $I_0 \subset I_1 \subset I_2 \subset \cdots I_N \subset \cdots$ form a uniformly computable infinite strictly increasing chain in $R$, and hence $R$ satisfies property 1.

The inspiration for the proof of Lemma 4.2 is derived from that of Theorem 3.2 in [5]. In this proof, Downey, Lempp, and Mileti show that certain elements $x_k,\ k \in \mathbb{N}$, of a ring $R$ are not invertible. To do this, the authors examine the largest index of a variable occurring in an expression for $\frac{1}{x_k} \in R$.

*Proof of Lemma 4.2.* Let $z, g, g_j, Z_j, g_j',\ j = 0, 1, \ldots, m$, be as in the statement of the lemma, and such that $g, g_j \in \langle X_{\langle N', k \rangle} : N' \leq N, k \in \mathbb{N} \rangle_{R_0}$ for all $j = 0, 1, 2, \ldots, m$. Furthermore, suppose for a contradiction that we can write

$$(*) \qquad z = g + \sum_{j=0}^{m} g_j Z_j = f + \sum_{i=0}^{n} f_i Y_i = y,$$

for some $f, f_i \in \mathbb{Q}[X_{\langle N', k' \rangle} : \langle N', k' \rangle \in \mathbb{N}]$, such that one of the elements $f, f_0', f_1', \ldots, f_n'$ ($f_i'$ denotes the numerator of $f_i Y_i$) is not in the ideal $\langle X_{\langle N', k' \rangle} : N' \leq N, k' \in \mathbb{N} \rangle_{R_0}$. We shall henceforth refer to the sum $f + \sum_{i=0}^{n} f_i Y_i$ by $y$, and the sum $g + \sum_{j=0}^{m} g_j Z_j$ by $z$; these sums are different codes for the same element of $R$.

Without loss of generality, we assume the following.

(1) By adding some $z' \in I_N$ to both sides of $(*)$ above, assume that $f_i'$ is not in $P = \langle X_{\langle N', k' \rangle} : N' \leq N, k' \in \mathbb{N} \rangle$ for *every* $0 \leq i \leq n$. Hence, by Proposition 4.3, none of the denominators of the $Y_i,\ 0 \leq i \leq n$, are in $P$ either.
(2) Assume that the denominator $d \in R_0$ of some $Z_{\langle p, i, \tau, \sigma \rangle}$ is not contained in $P$. One can always express such a $d \in R_0$ as a (unique) sum $d = d_1 + d_2,\ d_1, d_2 \in R_0$, such that $d_1 \in P$ and every monomial occurring in $d_2$ is not in $P$. Now, upon multiplying both sides of $(*)$ by $d$, and then adding $-d_1 R_*$ to both sides of $(*)$, where $R_*$ represents the right-hand side of $(*)$, we can rewrite $(*)$ as another equation of the same form but such that $d$ does not occur in the denominator of any $Z_{\langle p, i, \tau, \sigma \rangle}$. By repeating this argument, we can assume (without loss of generality) that the denominator of *every* $Z_{\langle p, i, \tau, \sigma \rangle}$ occurring in the left-hand side of $(*)$ is contained in $P$.

(3) By computably rewriting the codes $y$ and $z$ with different coefficients $f_i$, assume that for no $0 \leq j \leq m,\ 0 \leq i \leq n$, does the term $X_{\langle N',k'\rangle}$ appear in $f_i', g_j'$ if it divides the denominator of $Y_i, Z_j$, respectively. Furthermore, since the c.e. sets $A$ and $B$ are disjoint, it follows that if some $g_j'$ is divisible by $X_{\langle N,\alpha(i)\rangle}$, for some $N, i \in \mathbb{N}$, then after rewriting the sum in this fashion, $g_j'$ is divisible by $X_{\langle N,\alpha(i')\rangle}$, for some $i' \in \mathbb{N}$ such that $\alpha(i') \geq \alpha(i)$.

(4) By computably rewriting the codes $y$ and $z$, assume that there do not exist sets $I \subseteq \{0, 1, 2, \ldots, n\},\ J \subseteq \{0, 1, 2, \ldots, m\}$ such that

$$\sum_{i\in I} f_i Y_i = 0 \text{ or } \sum_{j\in J} g_j Z_j = 0.$$

Let $C, D \in R_0$ be the least common multiple for the denominators of the fractions $Y_0, Y_1, \ldots, Y_n$ and $Z_0, Z_1, \ldots, Z_m$, respectively. Then we have that $D(Cy) = C(Dz)$, where $C, D, Cy, Dz \in R_0$. Note that since $P = \langle X_{\langle N',k'\rangle} : N' \leq N, k' \in \mathbb{N}\rangle_{R_0}$ is a prime ideal (in the ring $R_0$), and none of the denominators of the $Y_i$ are in $P$, then $C \notin P$.

We have now made the necessary preliminary observations. The rest of the proof is as follows. First, by examining a variable of large index, we show that none of the factors in the monomials $Z_j,\ j = 0, 1, \ldots, m$, are of the form $Z_{\langle p,i,\tau,\sigma\rangle} \in \mathfrak{Y}$, for some $p \in R_0$. Then, via a similar argument, we show that none of the factors in the monomials $Z_j,\ j = 0, 1, \ldots, m$, are of the form $Y_{\langle N',l,\tau,\sigma\rangle} \in \mathfrak{Y}$, for some $N' \leq N$. Finally, we consider the case where none of the numerators of $Z_j,\ j = 0, 1, \ldots, m$, are in $P$, and derive a contradiction.

First, we claim that for all monomials $Z_j$ occurring in the sum $\sum_{j=0}^m g_j Z_j = z$, $Z_j$ is not divisible by any variable of the form $Z_{\langle p,i,\tau,\sigma\rangle} \in \mathfrak{Y}$. Suppose otherwise, and let $0 \leq j_0 \leq m$ be such that $Z_j$ is divisible by some $Z_{\langle p_0,i_0,\tau_0,\sigma_0\rangle}$ with $N(p_0) \leq N$ and $\alpha(i_0)$ maximal. First notice that by (1), no variable of the form $X_{\langle N_0,\alpha(i_0)\rangle},\ N_0 = N(p),\ i_0 \in \mathbb{N}$, appears in $f_i'$, for any $0 \leq i \leq n$. It now follows from (4) that $X_{\langle N_0,\alpha(i_0)\rangle}$ appears in the denominator of some $Z_{j_1},\ 0 \leq j_1 \leq m$. Now, by (2) and the construction of $\mathfrak{Y} = \cup_{s\in\mathbb{N}}\mathfrak{Y}_s$, it follows that $Z_{j_1}$ is divisible by some $Z_{\langle p_1,i_1,\tau_1,\sigma_1\rangle}$, for some $p_1 \in R_0$ such that $N(p_1) \leq N$ and with $X_{\langle N_0,\alpha(i_0)\rangle}$ occurring in $p_1$. Now, by the comment in (3) above and the construction of $Z_{\langle p,i,\tau,\sigma\rangle} \in \mathfrak{Y}$, it follows that $g_{j_1}'$ is divisible by some $X_{\langle N,\alpha(i')\rangle}$ such that $\alpha(i') > \alpha(i_0)$, which is a contradiction since $\alpha(i_0)$ was chosen to be maximal.

Now, suppose that there is a $0 \leq j_0 \leq m$ such that $Z_{j_0}$ is divisible by some variable of the form $Y_{\langle N_0',l_0,\tau_0,\sigma_0\rangle}$, such that $N_0' \leq N$ and $l_0 \in \mathbb{N}$ is minimal. Then, by similar reasoning as in the previous paragraph, we can derive a contradiction in this case also, as follows. Notice that, by (1), no variable of the form $X_{\langle N_0',l_0\rangle}$ appears in $f_i'$, for any $0 \leq i \leq n$. It now follows from (3) and (4) that $X_{\langle N_0',l_0\rangle}$ appears in the denominator of some $Z_{j_1},\ 0 \leq j_0 \neq j_1 \leq m$. However, by the previous paragraph we know that $Z_{j_1}$ is not divisible by any element of the form $Z_{\langle p,i,\tau,\sigma\rangle}$, and hence, by construction of $R$ and $\mathfrak{Y} = \cup_{s\in\mathbb{N}}\mathfrak{Y}_s$, and by a similar argument as in the comment in (3) above, it follows that the only way that $X_{\langle N_0',l_0\rangle}$ can appear in the denominator of $Z_{j_1}$ is if some $X_{\langle N_1',l_1\rangle}$ appears in the numerator of $Z_{j_1}$, for some $l_1 < l_0$, and this is a contradiction since we chose $l_0$ to be minimal.

We have now reduced ourselves to the case which says that, for every $j = 0, 1, 2 \ldots, m$, the numerator of $Z_j$ is not in $P$. In this case, however, we can derive a contradiction as follows. Since none of numerators of $Z_j,\ j = 0, 1, \ldots, m$, are in $P$, by Proposition 4.3, it follows that neither are the denominators of $Z_j,\ j = 0, 1, \ldots, m$. However, this contradicts (2) above, and so it follows that $(*)$ must be an equality of the form

$$A = \frac{B}{C} \Leftrightarrow CA = B,\ C \neq 0,$$

where $A, B, C$ are elements of $R_0$, $A$ is in $P$, and $B, C$ are not in $P$, a contradiction. □

**Corollary 4.4.** *The ideals $I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_N \subset \cdots$ form a strictly increasing, uniformly computable chain of ideals in the ring $R$.*

Now that we have constructed the computable ring $R$ and the infinite uniformly computable increasing chain of ideals $I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_N \subset \cdots \subset R$, we prove a lemma which will help us to show that every infinite decreasing chain of ideals in $R$ contains an element that is of PA degree. This is analogous to the verification that $R_1$ satisfies property 2.

**Lemma 4.5.** *If an ideal $J_0 \subseteq R$ is not of PA degree, then one of the following holds:*

(1) $J_0 = 0$.
(2) $J_0 = I_N$, *for some* $N \in \mathbb{N}$.
(3) $J_0 = I_\infty = \cup_{N=0}^{\infty} I_N$.
(4) $J_0 = R$.

*Proof.* Assume that $J_0 \neq 0$. We shall show that $J_0$ satisfies one of (2)–(4) above. First, we show that if $J_0 \nsubseteq I_\infty$, then $J_0 = R$. Then we show that if $J_0 \subseteq I_\infty$, then either $J_0 = I_\infty$, or else $J_0 = I_N$ for some $N \in \mathbb{N}$.

Assume that $J_0 \nsubseteq I_\infty$, and let $F \in J_0 \setminus I_\infty$. Then, since $F \in J_0 \setminus I_\infty$, $F$ must have a nontrivial constant term and hence $0 \neq F$. Also, since $J_0$ is an ideal, without loss of generality we can assume that $0 \neq F \in J_0 \cap R_0$. Now, since $\mathfrak{Z} \subset R$ and $\mathfrak{Z}$ contains elements of the form $Z_{\langle F,i \rangle}$, $i > M(F)$, it follows that $J_0$ contains elements of the form $X_{\langle N(F),\alpha(i) \rangle} = F \cdot Z_{\langle F,i \rangle}$, for (cofinitely many) $i \in \mathbb{N}$, $i > M(F)$. Since $J_0$ is not of PA degree, this means that $J_0$ must also contain elements of the form $X_{\langle N,\beta(j) \rangle}$ for infinitely many $j \in \mathbb{N}$. Now, since $\mathfrak{Y}_0 \subset R$, we have that $J_0$ contains the ideal $\langle X_{\langle N',k \rangle} : N' \leq N(F), k \in \mathbb{N} \rangle_{R_0}$, and from this it follows that $J_0$ contains the constant term of $F$, which is nonzero by assumption. Thus, we have shown that if $J_0 \nsubseteq I_\infty$, then $J_0 = R$.

We now show that if $J_0 \subseteq I_\infty$, then either $J_0 = I_\infty$ or $J_0 = I_N$ for some $N \in \mathbb{N}$. To do this, we prove that if $0 \neq F \in J_0 \cap R_0$ and $N = N(F_0)$, then $I_N \subseteq J_0$. From this it follows that $J_0 = I_N$, where $N \in \mathbb{N} \cup \{\infty\}, N = \sup\{N(F_0) : 0 \neq F = \frac{F_0}{F_1} \in J_0\}$.

Let $0 \neq F \in J_0 \cap R_0$. Now, since $\mathfrak{Z} \subset R$ we have that $J_0$ contains elements of the form $X_{\langle N,\alpha(i) \rangle}$ for $N = N(F)$ and cofinitely many $i \in \mathbb{N}$. Now, since $J_0$ is not of PA degree we must have that $J_0$ contains elements of the form $X_{\langle N,\beta(j) \rangle}$ for $N = N(F)$ and infinitely many $j \in \mathbb{N}$. Now, by construction of $\mathfrak{Y} = \cup_{s \in \mathbb{N}} \mathfrak{Y}_s$, if an ideal $J_0$ contains $X_{\langle N,\beta(j) \rangle}$ for infinitely many $j \in \mathbb{N}$, then we have that $\mathfrak{Y} J_0 \supseteq I_N$. Hence we have that $I_{N(F)} \subseteq J_0$. This completes the proof of the lemma. □

We now show that $R$ cannot contain a descending chain of ideals $R \supseteq J_0 \supset J_1 \supset J_2 \supset \cdots \supset J_n \supset \cdots$ unless some $J_N$, $N \in \mathbb{N}$ is of PA degree. Let $R \supseteq J_0 \supset J_1 \supset J_2 \supset \cdots \supset J_n \supset \cdots$ be an infinite strictly descending chain of ideals in $R$. By Lemma 4.5, we know that for every $n \in \mathbb{N}$, either $J_n$ is of PA degree, or else $J_n$, $n \in \mathbb{N}$, is equal to one of $\{0\}$,$R$, $I_\infty$, $I_N$, $N \in \mathbb{N}$. Now, since $I_\infty$ is a maximal ideal, then we have that either $J_2$ is of PA degree, or $J_2 \subset I_\infty$. Hence, if $J_2$ is not of PA degree, then there exists a number $M \in \mathbb{N}$ such that $J_2 = I_M$. Now, since the chain $R \supseteq J_0 \supset J_1 \supset J_2 \supset \cdots \supset J_n \supset \cdots$ is infinite and strictly decreasing, there must exist a number $k \in \{2, \ldots, M+2\}$ such that the ideal $J_k$ is not equal to $I_N$, for any $N \in \mathbb{N}$. But, by Lemma 4.5, this implies that $J_k$ must be of PA degree. Thus, every infinite strictly decreasing chain of ideals $R \supseteq J_0 \supset J_1 \supset J_2 \supset \cdots \supset J_n \supset \cdots$ contains an element of PA degree. This completes the proof of the theorem. □

We wish to make a remark about the last paragraph of the proof of Theorem 4.1. In particular, we wish to note that $\mathrm{RCA}_0 + \Sigma^0_1$-induction suffices to make the argument in this paragraph. To see why this is the case, first assume (for a contradiction) that $J_0 \supset J_1 \supset J_2 \supset \cdots$ is an infinite strictly decreasing sequence of ideals in $R$, none of which are of PA degree. Furthermore, note that $\mathsf{RCA}_0$ proves Lemma 4.5, and it follows that $J_2 = I_M$, for some $M \in \mathbb{N}$. Next, note that "$J_n \subseteq I_{M-n+2}$" is a $\Pi^0_1$ statement, and can be proved via $\Pi^0_1$-induction on $n \in \mathbb{N}$. This proves that $J_{M+2} = \{0\}$, which is a contradiction since we assumed that the chain $J_0 \supset J_1 \supset J_2 \supset \cdots$ was strictly decreasing. Therefore, $J_n$ must be of PA degree for some $n \in \mathbb{N}$, and so, over $\mathsf{RCA}_0$, Theorem 4.1 implies $\mathsf{WKL}_0$. This completes the proof of the lower bound in Theorem 1.12. The proof of the upper bound (in Theorem 1.12) is given in Section 5.

4.4. **Reversals in Theorem 3.4.** We now use the proof of Theorem 4.1 to show that, over $\mathsf{RCA}_0$, statements 2–6 in Theorem 3.4 imply $\mathsf{WKL}_0$. Throughout the rest of this section we assume $\mathsf{RCA}_0$.

To show that 2 implies $\mathsf{WKL}_0$, assume that 2 holds, and note that the ring $R$ of Theorem 4.1 is not a field, but it is an integral domain. Therefore, if 2 holds, $R$ cannot be Artinian. But, as we have seen in the proof of Theorem 4.1, the fact that $R$ is not Artinian implies the existence of a separating set for $\mathrm{ran}(\alpha)$ and $\mathrm{ran}(\beta)$. Hence, we have $\mathsf{WKL}_0$.

To show that 3 implies $\mathsf{WKL}_0$, assume that 3 holds, and note that, since $R$ is an integral domain, $\{0\}$ is a prime ideal in $R$ that is not maximal. Hence, $R$ cannot be Artinian, and so, as in the previous paragraph, we have $\mathsf{WKL}_0$.

To show that 4 implies $\mathsf{WKL}_0$, assume that 4 holds, and note that, since $R$ is an integral domain and not a field, the set of nilpotent elements in $R$ is equal to $\{0\}$. Therefore, 4 implies that either $R$ is not Artinian, in which case we can deduce $\mathsf{WKL}_0$ as above, or else there must be a maximal ideal $M \subset R$, $M \neq I_\infty$. But, by Lemma 4.5, we know that the existence of such an ideal also implies $\mathsf{WKL}_0$.

To show that 5 implies $\mathsf{WKL}_0$, assume that 5 holds, and note that the only $t$-nilpotent set in $R$ is $\{0\}$. Hence, 5 implies that either $R$ is not Artinian, in which case we can deduce $\mathsf{WKL}_0$, or else there is a maximal ideal $M \subset R$, $M \neq J$. As in the previous paragraph, this also implies $\mathsf{WKL}_0$.

To show that 6 implies $\mathsf{WKL}_0$, assume that 6 holds, and note that the set of nilpotent elements in $R$ is equal to $\{0\}$. Now, since $R$ contains a uniformly computable increasing sequence of ideals, $R$ is not Noetherian. Hence, by 6, $R$ is not Artinian either. In this case we have already shown that we can deduce $\mathsf{WKL}_0$.

## 5. $\mathrm{ACA}_0$ Upper Bound

In Sections 5 and 6 we turn our attention to showing that, over $\mathsf{RCA}_0+\mathsf{B}\Sigma_2$, Theorem 1.11 is equivalent to $\mathsf{ACA}_0$. Our first step toward achieving this goal is the proof of the following theorem.

**Theorem 5.1** ($\mathsf{ACA}_0$)**.** *Every Artinian ring is strongly Noetherian.*

*Proof.* We reason in $\mathsf{ACA}_0$. Our proof of Theorem 5.1 is very similar to the standard proof given in texts such as [6, 17].

Before we proceed with the proof of Theorem 5.1, we require two standard facts from commutative algebra. Let $J \subset R$ be the Jacobson radical of $R$.

**Lemma 5.2.** *We have that $x \in J$ if and only if for every $a \in R$, $1 - ax \in R$ is a unit.*

*Proof.* First, suppose that $1 - ax \in R$ is a unit for every $a \in R$, and suppose for a contradiction that $x \notin J$. Now, let $M \subset R$ be a maximal ideal such that $x \notin M$. We can write

$$1 = ax + m,$$

for some $m \in M, a \in R$. Hence, $1 - ax \in M$, and so $1 - ax$ is not a unit, a contradiction. Therefore, $x \in J$.

Secondly, suppose that there is an element $a \in R$ such that $1 - ax \in R$ is not a unit. Then, using $\mathsf{ACA}_0$, construct a maximal ideal $M \subset R$ containing $1 - ax$. Now, we cannot have that $x \in J$, or else we would have that $x \in M$ and so $(1 - ax) + (ax) = 1 \in M$, a contradiction. Hence, $x \notin J$. □

Note that one consequence of Lemma 5.2 is that $\mathsf{ACA}_0$ proves the existence of $J$. Applying $\mathsf{ACA}_0$ relative to $J$ also shows that for any $R$-module $M$, the submodule $JM \subseteq M$ exists.

In the literature, the following theorem is referred to as *Nakayama's Lemma.*

**Theorem 5.3.** *If $M$ is an $R$-module such that $M \neq 0$ and $JM = M$, then $M$ is not finitely generated.*

*Proof.* The proof is by $\Pi^0_3$-induction relative to $J$ and $JM$, with $M$ as a parameter. For the base case, suppose that $M$ is generated by a single element $m \in M,\ m \neq 0$. Then, since $M = JM$ we have that

$$m = am,\ a \in J.$$

From this it follows that

$$(1 - a)m = 0.$$

Since $a \in J$, by Lemma 5.2 we have that $1 - a \in R$ is a unit, and thus $m = 0$, a contradiction. This proves the base case.

For the induction step, suppose that $M \neq 0,\ M = JM$, and let $m_0, m_1, \ldots, m_n \in M$ be given. Using the fact that $m_0, m_1, \ldots, m_{n-1}$ does not generate $M$ (i.e. the induction hypothesis), we shall show that $m_0, m_1, \ldots, m_n$ does not generate $M$.

Suppose, for a contradiction, that $m_0, m_1, \ldots, m_n$ generates $M$, then we can write

$$m_n = a_0 m_0 + a_1 m_1 + \cdots + a_n m_n,\ a_0, a_1, \ldots, a_n \in J,$$

which implies that

$$(1 - a_n)m_n = a_0 m_0 + a_1 m_1 + \cdots + a_{n-1} m_{n-1}.$$

Now, since $a_n \in J$, we can apply Lemma 5.2 to conclude that $1 - a \in R$ is a unit. Thus, $M$ is generated by $m_0, m_1, \ldots, m_{n-1}$, which contradicts the induction hypothesis. □

### 5.1. **Finishing the proof of Theorem 5.1.**

We now have all the necessary ingredients to complete the proof of Theorem 5.1.

Since $\mathsf{ACA}_0$ implies $\mathsf{WKL}_0$, by our results in Section 3.5 we know that there exist finitely many maximal ideals $M_1, M_2, \ldots, M_n \subset R$ such that $J = \cap_{i=0}^n M_i = M_1 M_2 \cdots M_n$ is the Jacobson radical of $R$. We shall show that $J$ is nilpotent. In other words, there exists $m \in \mathbb{N}$ such that $J^m = \underbrace{J \cdot J \cdot \ldots \cdot J}_{m} = 0$.

5.1.1. *J is nilpotent.* Since we are working in $\mathsf{ACA}_0$, we have that the infinite (non-strictly) decreasing sequence of ideals $J \supseteq J^2 \supseteq \cdots \supset J^m \supseteq \cdots$ exists. Now, since $R$ is an Artinian ring, it follows that there is some $m \in \mathbb{N}$ such that $J^m = J^{m+1}$. We shall prove that $J^m = 0$.

Assume (for a contradiction) that $J^m \neq 0$, and use arithmetic comprehension to construct a sequence of elements $x_0, x_1, x_2, \ldots, x_n, \ldots$ such that for every $n \in \mathbb{N}$ we have $x_n J^m \neq 0$ and $\langle x_n \rangle \supset \langle x_{n+1} \rangle$. Since $R$ is Artinian, the sequence $x_0, x_1, x_2, \ldots x_n, \ldots$ must in fact be finite. Let $N \in \mathbb{N}$ be such that $x_N$ is the last element in the sequence. By construction, we have that the ideal $I_N = \langle x_N \rangle$ is minimal among all ideals $I$ such that $IJ^m \neq 0$.

Let $I = I_N$, and $x = x_N$. By the construction of $I$ and definition of $x$, it follows that $((xJ)J^m) = xJ^{m+1} = xJ^m \neq 0$, and hence, by the minimality of $I = \langle x \rangle$, it follows that $\langle x \rangle = xJ$. Then, by Nakayama's Lemma, we must have that $x = 0$, a contradiction since $xJ^m \neq 0$. Hence, $J^m = 0$.

5.1.2. *R has finite length.* Now, using arithmetic comprehension, construct the chain of ideals

$$\begin{aligned} R = M_0 \supset M_1 \supset M_1M_2 \supset \cdots \supset M_1M_2\cdots M_{n-1} \supset J \supset \\ JM_1 \supset JM_1M_2 \supset \cdots \supset JM_1M_2\cdots M_{n-1} \supset J^2 \supset \cdots \\ \cdots \supset J^{m-1}M_1 \supset J^{m-1}M_1M_2 \supset \cdots \supset J^{m-1}M_1M_2\cdots M_{n-1} \supset J^m = 0. \end{aligned}$$

Note that, as an $R$-module, the quotient of any two consecutive terms in the chain above is a vector space $V$ over the field $R/M_i$, for some $0 \leq i \leq N$. Furthermore, since $R$ is Artinian, $V$ is finite dimensional (otherwise we could use $\mathsf{ACA}_0$ to construct an infinite strictly decreasing sequence of subspaces in $V$ and then lift these subspaces via a quotient map to get an infinite strictly decreasing chain of ideals in $R$, which contradicts the fact that $R$ is Artinian). Let $S$ denote the sum of the dimensions of all such $V$.

Now, let $I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_S$ be a strictly increasing chain of ideals of length $S$ in $R$. Furthermore, let $0 \leq l < nm$, $l = pn + r$, $0 \leq r < n$, be such that if $V = J^pM_0M_1M_2\cdots M_r/J^pM_0M_1M_2\cdots M_{r+1}$, $d_0 = \dim(V)$, and $\varphi : J^pM_0M_1M_2\cdots M_r \to V$ is the canonical homomorphism, then there is a set $D \subseteq \{0, 1, 2, \ldots, S\}$, $|D| > d_0$, such that for every $d' \in D$, $(I_{d'+1} \setminus I_{d'}) \cap J^pM_0M_1M_2\cdots M_r \neq \emptyset$ but $(I_{d'+1} \setminus I_{d'}) \cap J^pM_0M_1M_2\cdots M_rM_{r+1} = \emptyset$. The fact that such a set $D \subseteq \{0, 1, 2, \ldots, S-1\}$ exists follows from the definition of $S$.

Now, using the definition of $l$ and $D$, and via an argument similar to the one given in Section 3.5.1 (case 2), we can show that if for every $k \in D$ we define $v_k$ to be any nonzero element of $(J^{d'+1} \setminus J^{d'}) \cap J^pM_0M_1M_2\cdots M_r$, then $\{v_k \in V : k \in D\}$ is a linearly independent set of vectors in $V$. But this contradicts the definition of $d_0 = \dim(V)$. Therefore, the length of any strictly increasing chain of ideals in $R$ is bounded by $S$, and hence $R$ is strongly Noetherian. □

We have now proven Theorem 1.12. We have also proven the upper bound of Theorem 1.13. In Section 6, we complete the proof of Theorem 1.13 by showing that, over $\mathsf{RCA}_0$+$\mathsf{B}\Sigma_2$, Theorem 1.11 implies $\mathsf{ACA}_0$.

## 6. $\mathrm{ACA}_0$ Lower Bound

This section is mostly devoted to proving the following theorem, which we then use to show that, over $\mathsf{RCA}_0$+$\mathsf{B}\Sigma_2$, Theorem 1.11 implies $\mathsf{ACA}_0$.

**Theorem 6.1.** *There exists a computable ring $R$ such that for all $N \in \mathbb{N}$, $R$ has a finite strictly increasing chain of ideals $I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_N \subseteq R$ of length*

*$N$, and such that every infinite strictly decreasing sequence of ideals $R \supseteq J_0 \supset J_1 \supset \cdots \supset J_k \supset \cdots$ computes the halting set $\emptyset'$.*

*Proof.* We begin by fixing an infinite computably enumerable set, $A \subset \mathbb{N}$, and a 1-1 computable function $\alpha : \mathbb{N} \to \mathbb{N}$ whose range is $A$, such that the characteristic function of the complement of $A$, $A^c = \{0 = a_0 < a_1 < a_2 < \cdots < a_n < \cdots\}$, dominates the modulus function for the halting set $\emptyset'$ ($A$, and hence $A^c$, can be constructed via a movable marker construction [21], which we give at the end of Section 6). By definition of $A$, it follows that every infinite subset of $A^c$ also computes $\emptyset'$. We now construct the computable ring $R$.

$R$ will be of the form $\mathbb{Q}[X_N : N \in \mathbb{N}]/I$, where $I \subset \mathbb{Q}[X_N : N \in \mathbb{N}]$ is a computable ideal. Therefore, to construct the computable ring $R$, it suffices to construct the ideal $I$, which we shall do in stages.

First, define $I_0 = \langle X_i X_j : i, j \in \mathbb{N}\rangle$. Thus, $I_0$ is the unique computable ideal generated by all monomials of degree 2. We shall let $I_0 \subset I$, and $R = \mathbb{Q}[X_N : N \in \mathbb{N}]/I$. Hence, to construct $R$ it suffices to construct a computable ideal $I$ in the computable ring $R_0 = \mathbb{Q}[X_N : N \in \mathbb{N}]/I_0$, such that $R = R_0/I$. Before constructing the ideal $I$, we wish to make some simple observations about the ring $R_0$.

It follows from the definition of $I_0$ that every element in the quotient ring $R_0 = \mathbb{Q}[X_N : N \in \mathbb{N}]/I_0$ is equal to the image of a linear polynomial in $\mathbb{Q}[X_N : N \in \mathbb{N}]$ under the canonical quotient map $\varphi : \mathbb{Q}[X_N : N \in \mathbb{N}] \to R_0$. We shall code the elements of $R_0$ and $R$ via linear representatives for each equivalence class, and for any two elements $f, g \in R_0$ of the form

$$f = a + \sum_{k=0}^{n} a_i X_i,\ \ g = b + \sum_{j=0}^{m} b_j X_j \in R_0,\ \ a, b, a_i, b_j \in \mathbb{Q},$$

it follows from the definition of $I_0$ that the product $fg$ is equal to

$$fg = ab + a\sum_{j=0}^{m} b_j X_j + b\sum_{i=0}^{n} a_i X_i.$$

Note that for every $n \in \mathbb{N}$, $X_n \in R_0$, we have that $X_n^2 = 0$. Furthermore, if $p \in R_0$, $p = a + \sum_{k=0}^{n} a_i X_i \in R_0$, then $p$ is a unit if and only if $a \neq 0$ and $p^{-1} = a^{-1} - \sum_{k=0}^{n} a_i X_i$. Furthermore, for any nonunits $x_0, x_1, \ldots, x_n \in R_0$ we have

$$\langle x_0, x_1, \ldots, x_n\rangle = \{r \in R_0 : r = \sum_{k=0}^{n} q_k x_k,\ \ q_k \in \mathbb{Q}\}.$$

Hence, determining whether or not any given $y \in R_0$ belongs to $\langle x_0, x_1, \ldots, x_n\rangle$ is a matter of solving a finite system of linear equations in finitely many variables, which can be done computably. This shows that any finitely generated ideal $J \subset R_0$ is computable. Having now made the necessary observations about the ring $R_0$, we now turn our attention to constructing the ideal $I \subset R_0$ in stages.

6.1. **Constructing** $I$. Let $0 = p_0, p_1, p_2, \ldots$ be an effective listing of the noninvertible elements of $R_0$. Rather than constructing the ideal $I \subset R_0$, we shall construct a generating set $D = \cup_{s\in\mathbb{N}} D_s \subset R_0$ in stages such that $\langle D\rangle = I$ is the ideal that we want. Afterwards, we will verify that both $D$ and $\langle D\rangle$ are in fact computable. At stage $s = 0$, define $D_0 = 0 = p_0$. At stage $s+1$, we are given $D_s$, and add to $D_s$ an element of the form $Z_s^n = nX_{\alpha(s)} - X_{\alpha(s)+1} \in R_0$, for some $n \in \mathbb{N}$, to get $D_{s+1}$. We do this in such a way (i.e. we choose $n$ so) that we guarantee that for every $0 \le i \le s$, if $p_i \notin \langle D_s\rangle$, then $p_i \notin \langle D_{s+1}\rangle$. But first, we need a lemma.

**Lemma 6.2.** *Fix a stage $s+1 \geq 1$. If for every $q \in \mathbb{Q}$ we define $Z_s^q = qX_{\alpha(s)} - X_{\alpha(s)+1}$, and $Z_s = X_{\alpha(s)}$, then we have that $Z_s^q, Z_s \notin \langle D_s \rangle$, for any $q \in \mathbb{Q}$. Also, for every $n_0, n_1 \in \mathbb{N}$, $n_0 \neq n_1$, we have $\langle D_s, Z_s^{n_0} \rangle \cap \langle D_s, Z_s^{n_1} \rangle = \langle D_s \rangle$.*

*Proof.* Let $Z$ be equal to $Z_s^q$, for some $q \in \mathbb{Q}$, or equal to $Z_s$. Suppose, for a contradiction, that $Z \in \langle D_s \rangle$. Then, there exist $n_0, n_1, \ldots, n_{s-1} \in \mathbb{N}$, and $q_0, q_1, \ldots, q_{s-1} \in \mathbb{Q}$, such that

$$Z - \sum_{k=1}^{s-1} q_k Z_k^{n_k} = 0.$$

It is clear that $Z \neq 0$, and so $s-1 \geq 0$. Now, let $N, M \in \mathbb{N}$ be such that $X_M, X_N$ both appear in the expression above and such that $N$ is maximal, and $M$ is minimal (one can show that $M$ and $N$ exist via $\Delta_0^0$-induction). Since $s-1 \geq 0$, it follows that $N \neq M$. Furthermore, by the construction of the elements $Z_t^m$, $m, t \in \mathbb{N}$, it follows that $X_N$ cannot be canceled by any of the other summands, unless $Z = Z_s = X_{\alpha(s)}$, in which case both $X_M$ and $X_N$ cannot be canceled by any of the other summands. Thus, we have a contradiction. Therefore, $Z \notin \langle D_s \rangle$.

To prove the second part of the lemma, first note that $\langle D_s, Z_s^{n_0} \rangle \cap \langle D_s, Z_s^{n_1} \rangle \supseteq \langle D_s \rangle$. Now, suppose $r \in \langle D_s, Z_s^{n_0} \rangle \cap \langle D_s, Z_s^{n_1} \rangle$, we shall show that $r \in \langle D_s \rangle$. By hypothesis, we have that there exist $n_0, n_1, \ldots, n_{s-1} \in \mathbb{N}$ and $q_0, q_1, \ldots, q_s, q'_0, q'_1 \ldots, q'_s \in \mathbb{Q}$ such that

$$r = q_s Z_s^{n_0} + \sum_{k=1}^{s-1} q_k Z_k^{n_k} = q'_s Z_{s-1}^{n_1} + \sum_{k=1}^{s-1} q'_k Z_k^{n_k},$$

from which it follows that

$$q_s Z_s^{n_0} - q'_s Z_s^{n_1} \in \langle D_s \rangle.$$

By definition of $Z_t^m$, $m, t \in \mathbb{N}$, it follows that either $Z_s^{\frac{q_s n_0 - q'_s n_1}{q_s - q'_s}} \in \langle D_s \rangle$, if $q_s \neq q'_s$, or $Z_s \in \langle D_s \rangle$, if $q_s = q'_s \neq 0$, or else $r \in \langle D_s \rangle$, if $q_s = q'_s = 0$. The first two cases contradict the first part of the lemma, and so we must be in the third case, i.e. $r \in \langle D_s \rangle$. This completes the proof Lemma 6.2. □

We now claim that there is a number $n \in \mathbb{N}$ such that for all $p_k$, $0 \leq k \leq s$, if $p_k \notin \langle D_s \rangle$, then $p_k \notin \langle D_s, Z_s^n \rangle$. By Lemma 6.2 we have that for any $n_0 \neq n_1 \in \mathbb{N}$, $\langle Z_s^{n_0}, D_s \rangle \cap \langle Z_s^{n_1}, D_s \rangle = \langle D_s \rangle$. This implies that, as $n \in \mathbb{N}$ varies, the (infinite collection of) ideals $\langle D_s, Z_s^n \rangle$ are all distinct, and so we can (uniformly and computably) find one not containing any $p_k$, for every $0 \leq k \leq s$ such that $p_k \notin D_s$. This ends the construction of $D$. For every $x \in R_0$, we let $\overline{x} \in R = R_0/I$ denote the image of $x$ under the canonical quotient map $\varphi : R_0 \to R_0/I = R$.

Note that $\langle D \rangle \subset R_0$ is a computable set, since, if $\overline{p_i} \in R_0$ a noninvertible polynomial, then $\overline{p_i} \in \langle D \rangle$ if and only if $\overline{p_i} \in \langle D_i \rangle$.

It follows from the construction of $R = R_0/I$ that for every $N \in \mathbb{N}$ we have the following equality of sets in $R$:

$$\langle \overline{X_0}, \overline{X_1}, \overline{X_2} \cdots, \overline{X_N} \rangle = \langle \overline{X_0}, \overline{X_{a_0}}, \overline{X_{a_1}}, \cdots, \overline{X_{a_n}} \rangle,$$

where $a_n \in \mathbb{N}$ is the least number in $A^c$ greater than or equal to $N$.

6.2. **Verifying that $R$ has the desired properties.** We now verify that $R$ satisfies the following properties.

(1) For each $n \in \mathbb{N}$, $R$ contains an increasing chain of computable ideals $I_0 \subset I_1 \subset \cdots \subset I_N$.
(2) Every infinite decreasing chain of ideals $R \supseteq J_0 \supset J_1 \supset \cdots \supset J_k \supset \cdots$ computes an infinite subset of $A^c$.

For any $p \in R_0$, let $\overline{p} = \varphi(p)$ be the image of $p$ under the canonical quotient map $\varphi : R_0 \to R$. To verify that $R$ has property 1, let $N \in \mathbb{N}$ be given, and let $A^c = \{0 = a_0 < a_1 < a_2 < \cdots < a_k < \cdots\}$. If we define $I_k = \langle \overline{X_{a_0}}, \overline{X_{a_1}}, \cdots, \overline{X_{a_k}} \rangle$, $k \in \mathbb{N}$, then it follows that the ideals $I_0 \subset I_1 \subset \cdots \subset I_N$ form an increasing chain of computable ideals. To show this note that, for all $k \in \mathbb{N}$, $I_k$ is computable since it is finitely generated. We now show that for every $k \in \mathbb{N}$, $I_k \subset I_{k+1}$, by proving that the elements $\overline{X_{a_0}}, \overline{X_{a_1}}, \overline{X_{a_2}}, \ldots \in R$ are linearly independent over $\mathbb{Q}$.

It follows from the construction of $R = R_0/\langle I \rangle$ that every $r \in R$ can be expressed as a $\mathbb{Q}$-linear combination of $\overline{1}, \overline{X_{a_0}}, \overline{X_{a_1}}, \overline{X_{a_2}}, \ldots$. To show that the sequence $\overline{X_{a_0}}, \overline{X_{a_1}}, \overline{X_{a_2}}, \ldots$ is linearly independent over $\mathbb{Q}$, it suffices to show that this representation is unique. Suppose that $c, c_0, c_1, \ldots, c_n, b, b_0, b_1, \ldots, b_m \in \mathbb{Q}$ are such that

$$f = c + \sum_{k=0}^{n} c_k X_{a_k}, \;\; g = b + \sum_{j=0}^{n} b_j X_{a_j} \in R_0,$$

and $\overline{f} = \overline{g}$. It follows that

$$f - g = c - d + \sum_{k=0}^{n} (c_k - d_k) X_{a_k} \in \langle I \rangle.$$

By construction of $I$, it follows that $c = d$.

Now, either $c_k = d_k$, for every $k = 0, 1, 2, \ldots, n$, or else there is some $k \in \{0, 1, 2, \ldots, n\}$ such that $c_k \neq d_k$. If we are in the former case, then the proof is complete, so suppose that we are in the latter case, and let $k \in \{0, 1, 2, \ldots, n\}$ be such that $c_k \neq d_k$. We shall derive a contradiction. By $\Pi^0_1$-induction on $s$, one can show that for every $h \in \langle I_s \rangle \subset R_0$, $f - g + h$ must contain a nonzero rational coefficient in front of $X_l$, for some $a_{k-1} < l \leq a_k$. Thus, $f - g + h \neq 0$. Therefore, we can conclude that for every $s \in \mathbb{N}$, $f - g \notin \langle I_s \rangle$, from which it follows that $f - g \notin \langle I \rangle$, a contradiction. We have now proven that the sequence $\overline{X_{a_0}}, \overline{X_{a_1}}, \overline{X_{a_2}}, \ldots$ is linearly independent over $\mathbb{Q}$, and hence the ideals $I_k$, $k \in \mathbb{N}$, are strictly increasing in $k \in \mathbb{N}$.

Before we can prove that $R$ has property 2, we need the following lemma.

**Lemma 6.3.** *Fix $N \in \mathbb{N}$, and let $\langle 0 \rangle \subset I_1 \subset I_2 \subset \cdots \subset I_k \subseteq \mathbb{Q}[X_0, X_1, \cdots, X_N]/(I_0 \cap \mathbb{Q}[X_0, X_1, \cdots, X_N]) = S$ be a strictly increasing chain of ideals. Then $k \leq N + 1$.*

*Proof.* Note that $S$ is a finite dimensional $\mathbb{Q}$-vector space, with basis $1, X_0, X_1, X_2, \ldots, X_N$. Since any ideal $I \subset S$ is a $\mathbb{Q}$-subspace of $S$, it follows that the length of any chain of ideals in $S$ is bounded by $N + 1$. □

**Corollary 6.4.** *Let $\langle 0 \rangle = I_0 \subset I_1 \subset I_2 \subset \cdots \subset I_k$ be a strictly increasing chain of ideals in $\langle \overline{X_0}, \overline{X_1}, \cdots, \overline{X_N} \rangle$. Then $k \leq a_n$, where $a_n \in \mathbb{N}$ is the least number in $A^c$ greater than or equal to $N$.*

Suppose, for a contradiction, that there exist numbers $m_0, b_0 \in \mathbb{N}$ such that for every $m \geq m_0$, if $p \in R_0$ and $\overline{p} \in I_{m_0} \setminus I_m$, then $X_b$ does not occur in $p$ for any $b \geq b_0$. Then it follows that the ideal $\langle \overline{X_0}, \overline{X_1}, \cdots, \overline{X_{b_0}} \rangle$ contains an infinite strictly descending chain of ideals, which contradicts Corollary 6.4. Thus, we have proven the following fact which we shall use in the next paragraph to construct a set $B = \{b_1 < b_2 < \cdots < b_n < \cdots\}$ such that, for every $n \in \mathbb{N}$, $b_n > a_n$.

**Proposition 6.5.** *Given any numbers $m_0, b_0 \in \mathbb{N}$, there exist numbers $m > m_0, b > b_0$, and $p \in R_0$ with $X_b$ occurring in $p$, and $p \in I_{m_0} \setminus I_m$.*

We now construct the set $B$ in stages using the proposition. At stage $s = 0$ compute numbers $m_0, b_0 \in \mathbb{N}$ such that $\overline{X_{b_0}} \notin J_{m_0}$. At stage $s + 1$, given $m_s, b_s$, define $m_{s+1} = b_s + 1$, and compute a finite set $K_{s+1} = \{k_{m_s+1}, k_{m_s+2}, \cdots, k_{m_{s+1}}\}$ such that for $k = m_s+1, m_s+2, \cdots, m_{s+1}$ we have that $J_{k-1} \setminus J_k$ contains an element $\overline{f = \sum_{i=0}^{n} c_i X_i} \in R$ with $n \geq k$ and $c_k \neq 0$. Now, let $b_{s+1}$ be the maximum of the finite set $K_{s+1}$, and put $b_{s+1}$ into $B_{s+1}$. By Corollary 6.4, and the definition of $m_{s+1}$, we must have that $b_{s+1} > b_s$, and there exists a number $a \in A^c$, $b_s < a \leq b_{s+1}$. From this it follows that the set $B = \{b_1 < b_2 < \cdots < b_{s+1}\}$ majorizes the set $A^c = \{0 = a_0 < a_1 < \cdots < a_s\}$, and hence $B$ computes the halting set $\emptyset'$. □

We now use Theorem 6.1 to show that, over $\mathsf{RCA}_0 + \mathsf{B}\Sigma_2$ (i.e. $\mathsf{RCA}_0$, plus induction for all $\Sigma_2$ formulas), Theorem 1.11 implies $\mathsf{ACA}_0$. First, however, we review the standard construction (i.e. computable approximation) of the set $A^c = \{0 = a_0 < a_1 < a_2 < \cdots < a_n < \cdots\}$.

Let $\emptyset'_s$, $s \in \mathbb{N}$, be a computable approximation to $\emptyset'$ such that for every stage $s \in \mathbb{N}$, there exists $x \in \mathbb{N}$ such that $\emptyset'_{s+1}(x) \neq \emptyset'_s(x)$. The standard stage-by-stage computable (movable marker) approximation of $A^c$ is as follows.

(1) At stage $s = 0$, initialize (markers) $\Gamma^x_0 = x$, for every $x \in \mathbb{N}$.
(2) At stage $s + 1$, assume that $\Gamma^x_s$ is defined for every $x \in \mathbb{N}$, and search for the least $x \in \mathbb{N}$ such that $\emptyset'_{s+1}(x) \neq \emptyset'_s(x)$. Then define $\Gamma^y_{s+1} = \Gamma^y_s$ for every $y < x$, and for every $y \geq x$, define $\Gamma^y_{s+1} = \Gamma^{y+M}_s$, where $\Gamma^{x+M}_s$ is the least number of the form $\Gamma^{x+M'}_{s'}$, $M', s' \in \mathbb{N}$, that is greater than $s$.

Assume $\mathsf{RCA}_0 + \mathsf{B}\Sigma_2$, and fix a number $n \in \mathbb{N}$. We shall show that the ring $R$ has an increasing sequence of ideals of length $n$. Since the approximation $\emptyset'_s(x)$ comes to a limit for every $x \in \mathbb{N}$, we have that for every $x \in \mathbb{N}$ there exists a stage $M_x \in \mathbb{N}$ such that for every stage $s > M_x$, $\emptyset'_s(x) = \emptyset'_{M_x}(x)$. Therefore, by $\mathsf{B}\Sigma_2$, it follows that

$$(\forall x \in \mathbb{N})(\exists M_x \in \mathbb{N})(\forall s > M_x)[\emptyset'_s \restriction x = \emptyset'_{M_x} \restriction x].$$

In other words, for every natural number $x$ there is a stage $M_x$ by which the first $x$ bits of our computable approximation to $\emptyset'$ have settled. Now, by the construction of $A^c$ above and $\Sigma_0$-induction (on $s$), it follows that, for every number $x \in \mathbb{N}$, and every stage $s > M_x$, we have that $\Gamma^k_s = \Gamma^k_{M_x}$, for all $k \leq x$. In other words, for all $k \leq x$, the markers $\Gamma^k_s$ have come to a limit by stage $M_x$.

This fact allows us to verify that for every $n \in \mathbb{N}$, there exists a strictly increasing chain of ideals of length $n$ in $R$. In particular, (as in the proof of Theorem 6.1) the chain may be taken to be of the form $Y_0 \subset Y_1 \subset Y_2 \subset \cdots \subset Y_n$, where $Y_k = \langle X_{a_0}, X_{a_1}, \cdots, X_{a_k}\rangle$ and $a_x = \lim_{s\to\infty} \Gamma^x_s$, for every $x \in \mathbb{N}$. Now, since we are assuming that Theorem 1.11 holds, then there exists an infinite strictly decreasing chain of ideals in $R$, which we can use to construct the halting set $\emptyset'$, as in the last two paragraphs of the proof of Theorem 6.1. Hence, over $\mathsf{RCA}_0 + \mathsf{B}\Sigma_2$, Theorem 1.11 implies the existence of the halting set $\emptyset'$, and therefore it also implies $\mathsf{ACA}_0$. This completes the proof of Theorem 1.13.

## References

1. Y. Akizuki, *Teilerkettenatz und vielfachensatz*, Proc. Phys.–Math. Soc. Japan **17** (1935), 337–345.
2. M.F. Atiyah and I.G. MacDonald, *Introduction to commutative algebra*, Perseus, 1969.
3. A.W. Baur, *Rekursive algebren mit kettenbedingungen*, Zeits. Math. Logik Grundl. Math. **20** (1974), 37–46.
4. R.G. Downey, D.R. Hirschfeldt, A.M. Kach, S. Lempp, J.R. Mileti, and A. Montalbán, *Subspaces of computable vector spaces*, J. Algebra **314** (2007), 888–894.
5. R.G. Downey, S. Lempp, and J.R. Mileti, *Ideals in computable rings*, J. Algebra **314** (2007), 872–887.
6. D.S. Dummit and R.M. Foote, *Abstract algebra*, John Wiley & Sons, 1999.

7. H.M. Friedman, S.G. Simpson, and R.L. Smith, *Countable algebra and set existence axioms*, Ann. Pure and Appl. Logic **25** (1983), 141–181.
8. ———, *Addendum to: "countable algebra and set existence axioms"*, Ann. Pure and Appl. Logic **28** (1985), 319–320.
9. A. Frölich and J.C. Shepherdson, *Effective procedures in field theory*, Philosophical Transactions of the Royal Society of London. Series A, Mathematical and Physical Sciences **248** (1956), 407–432.
10. P. Hájeck and P. Pudlák, *Metamathematics of first order arithmetic (second printing), perspect. math. logic*, Springer-Verlag, Berlin, 1998.
11. G. Hermann, *Die frage der endichen vielen schritte in der theorie der plynomideale*, Math. Ann. **95** (1926), 736–738.
12. P. Hingston, *Effective decomposition in noetherian rings*, Aspects of Effective Algebra, Upside Down A. Book Co., Yarra Glen, Vic., 1981, pp. 122–127.
13. C. Hopkins, *Rings with minimum condition for left ideals*, Ann. Math. **40** (1939), 712–730.
14. C.G. Jockusch and R.I. Soare, $\Pi^0_1$*-classes and degrees of theories*, Trans. Amer. Math. Soc. **173** (1972), 33–56.
15. L. Kronecker, *Grundzüge einer arithmetischen theorie der algebraischen groössen*, J. Reine Angew. Math. **92** (1882), 1–122.
16. S. Lang, *Algebra*, Springer-Verlag, 1993.
17. H. Matsumura, *Commutative ring theory*, Cambridge University Press, 2004.
18. J.B. Paris and L.A.S. Kirby, $\Sigma_n$*-collection schemas in arithmetic*, Logic Colloquium '77, Stud. Logic Foundations Math., vol. 96, North-Holland, Amsterdam–New York, 1977.
19. S.G. Simpson, *Degrees of unsolvability: A survey of results*, Handbook of Mathematical Logic (J. Barwise, ed.), North-Holland (Elsevier) 1977.
20. ———, *Subsystems of second order arithmetic*, Springer-Verlag, 1999.
21. R.I. Soare, *Recursively enumerable sets and degrees*, Springer-Verlag, 1987.
22. V. Stoltenberg-Hansen and J.V. Tucker, *Computable rings and fields*, Handbook of Computability Theory (E.R. Griffor, ed.), North-Holland (Elsevier) 1999.
23. B.L. van der Waerden, *Algebra, vol. 1*, Springer-Verlag, 2003.

Department of Mathematics, University of Chicago, Chicago, IL 60637, USA