THE ARITHMETIC THEORY OF HILBERT'S BASIS THEOREM FOR MODULES

CHRIS J. CONIDIS

Abstract. We examine the strength of the Hilbert Basis Theorem for finitely generated modules (HBTM) and the stronger version pertaining to finitely generated polynomial rings (HBT) in the context of Reverse Mathematics and First-Order Arithmetic. More specifically, we show that the first-order consequences of HBTM for modules with a span-relation are equivalent to those of the Infinite Pigeonhole Principle ($\mathsf{B}\Sigma_2$); this implies that the first-order theory of HBTM for modules is incomparable with the Hilbert Basis Theorem for finitely generated polynomial rings over fields, studied by Simpson in [Sim88]. Finally, after noticing that HBTM for modules is reducible to the Hilbert Basis Theorem for multivariate polynomials with ring coefficients (HBT), we obtain that HBT also implies the Infinite Pigeonhole Principle, and (via some previously known results in [Con]) allows us to characterize the strength of HBT as the conjunction of the Infinite Pigeonhole Principle ($\mathsf{B}\Sigma_2$) equivalent to HBTM and the principle that asserts the well-foundedness of the ordinal number $\mathbb{N}^{\mathbb{N}}$ ($\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$) equivalent to the Hilbert Basis Theorem for finitely generated polynomial rings with field coefficients.

1. Introduction

One of the oldest nonconstructive mathematical arguments is the Hilbert Basis Theorem [Hil90], which says that the polynomial ring $R[X]$ with coefficients in a Noetherian (commutative) ring R and indeterminate variable X is Noetherian.[1] The effective content of the Hilbert Basis Theorem was examined first by Buchberger [Buc74], and his algorithm was subsequently translated to the proof-theoretic context for finitely generated polynomial rings with field coefficients (HBTF) by Simpson [Sim88] and others [Hat94]. By induction it easily follows from the Hilbert Basis Theorem that if R is a Noetherian commutative ring then the multivariate polynomial ring $R[X_1, X_2, \ldots, X_n]$ is Noetherian, for any natural number $n \in \mathbb{N}$. An even more general form of the theorem pertains to finitely generated modules over Noetherian rings. The standard proof of the Hilbert Basis Theorem essentially takes an infinite sequence of polynomials in $R[X]$ such that no polynomial is generated via its sequential predecessors (over $R[X]$), and produces a corresponding infinite sequence of "minimal" leading $R-$coefficients (i.e. coefficients corresponding to polynomials of minimal degree, modulo sequential predecessor polynomials) such that no coefficient is in the $R-$span of its sequential predecessors. Finding these minimal coefficients in general necessitates the use of nonconstructive methods.

Buchberger presented an algorithm for computing what are called Gröbner bases for ideals in multivariate polynomial rings. More precisely, for any ideal I in the multivariate polynomial ring $R[X_1, X_2, \ldots, X_n]$, $n \in \mathbb{N}$, R a Noetherian ring, a Gröbner basis (for I) is a finite generating set for I. In this way, Gröbner bases are essentially witnesses for the Hilbert

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

Key words and phrases. Computability Theory, Reverse Mathematics, Proof Theory, Hilbert Basis Theorem, Artin-Rees Lemma, Krull Intersection Theorem.

[1] A ring R is *Noetherian* if every ascending chain of ideals eventually stabilizes. More background on Algebra is given in the following section.

Basis Theorem. However, Buchberger's algorithm is iterative and to show its convergence Buchberger used the fact that the ordinal number $\mathbb{N}^{\mathbb{N}}$ is well-ordered. Later, in [Sim88], Simpson showed the necessity of Buchberger's hypothesis by showing that if R is a field then the proof of the Hilbert Basis Theorem for $R[X_1, X_2, \ldots, X_n]$, $n \in \mathbb{N}$, is necessarily nonconstructive because it is equivalent to (and therefore requires) the well-ordering of the ordinal $\mathbb{N}^{\mathbb{N}}$, denoted $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$.

More recently, in [Con], the author has shown that the first-order consequences of the Hilbert Basis Theorem for a multivariate polynomial ring $R[X_1, X_2, \ldots, X_n]$ with finitely many indeterminates $\vec{X}_n = \{X_1, X_2, \ldots, X_n\}$, $n \in \mathbb{N}$, and coefficients in Noetherian ring R, are contained within those of a principle called the Monomial Division Chain (principle) MDC which says that "every infinite sequence of $\vec{X}-$monomials of strictly increasing degree $\{m_i\}_{i=1}^{\infty}$ has an infinite subset corresponding to some $I \subseteq \mathbb{N}$ that forms a division chain such that for all $i, j \in I$, $i < j$, m_i divides m_j." Moreover, MDC is equivalent to the conjunction of $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ mentioned in the previous paragraph, along with the Infinite Pigeonhole Principle, deonted $\mathsf{B\Sigma_2}$, which we formally introduce in the following section and essentially says every finite partition of $\mathbb{N}$ must contain an infinite member.

1.1. The Hilbert Basis Theorem for Modules.

A different version of the Hilbert Basis Theorem says that if R is Noetherian and M is a finitely generated $R-$module, then M is Noetherian, and we will denote this principle by HBTM throughout the rest of the paper. The main purpose of this article (see Section 3 below) is to show that the first-order consequences of HBTM for rings R that possess a "generalized division algorithm" (which we describe in the following section) are the same as those of the Infinite Pigeonhole Principle ($\mathsf{B\Sigma_2}$). A consequence of this result, in the context of some previous results of Simpson [Sim88, Sim], shows that the first-order consequences of our HBTM neither include, nor are included in, the first-order consequences of the Hilbert Basis Theorem for polynomial rings with field coefficients[2].

1.2. The General Hilbert Basis Theorem for Finitely Generated Polynomial Rings.

The strongest and most general form of the Hilbert Basis Theorem says that if R is a Noetherian ring, then the finitely generated polynomial ring $R[\vec{X}_n] = R[X_1, X_2, \ldots, X_n]$, $n \in \mathbb{N}$, in the n indeterminate variables $X_1, X_2, \ldots, X_n$ is also a Noetherian ring. We focus on the first-order consequences of HBT by assuming that the coefficient ring R has a generalized division algorithm, and we denote the resulting principle HBT. We will eventually observe that HBT implies HBTM (over $\mathsf{RCA_0}$), and therefore also implies the equivalent principle $\mathsf{B\Sigma_2}$. By definition, HBT trivially implies the version of the theorem where $R = K$ is a field, examined by Simpson in [Sim88], who showed that this weaker form of HBT is equivalent to $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$. Therefore, our main theorem pertaining to HBTM will allow us to decompose the more general and stronger Hilbert Basis Theorem for Noetherian rings HBT into the conjunction of two strictly weaker and incomparable versions:

- HBTM, equivalent to the Infinite Pigeonhole Principle $\mathsf{B\Sigma_2}$; and
- HBTF, equivalent to the Well-Ordering Principle for $\mathbb{N}^{\mathbb{N}}$.

Moreover, via [Con], this decomposition implies that HBT is equivalent to the Monomial Division Chain Principle MDC.

[2] Note that, by definition, the (generalized) division algorithm for a field is trivial. Therefore, fields always possess such an algorithm over $\mathsf{RCA_0}$, although a ring may not.

2. Background

To begin with, let $\mathbb{N} = \{0, 1, 2, \ldots\}$ denote a possibly nonstandard set of natural numbers, and for any $N \in \mathbb{N}$, define

$$\mathbb{N}^N = \underbrace{\mathbb{N} \times \mathbb{N} \times \cdots \times \mathbb{N}}_{N}.$$

We identify $N \in \mathbb{N}$ with the set of natural numbers preceding it

$$N = \{0, 1, \ldots, N-1\}.$$

Since we are working exclusively in the context of Second-Order Arithmetic, all of the structures that we will consider are countable.

2.1. **Basic Commutative Algebra.**

For any $N \in \mathbb{N}$,

$$\overrightarrow{X} = \{X_0, X_1, \ldots, X_N\}$$

is a set of indeterminate variables, and we can speak of $\overrightarrow{X}-$monomials that are products of the form

$$\prod_{i=0}^{N} X_i^{\alpha_i}, \ \alpha_i \in \mathbb{N}.$$

We can identify a monomial m with its sequence of exponents

$$m \sim \langle \alpha_0, \alpha_1, \ldots, \alpha_N \rangle = \langle \alpha_i : i \in N+1 \rangle \in \mathbb{N}^{N+1}.$$

We say that a monomial $m_0 \sim \langle \alpha_{i,0} : i \in N+1 \rangle$ *divides* a monomial $m_1 \sim \langle \alpha_{i,1} : i \in N+1 \rangle$ whenever we have that

$$\alpha_{i,0} \leq \alpha_{i,1}, \ i = 0, 1, \ldots, N,$$

and this corresponds to division in polynomial rings (see [DM22] for basic definitions and facts about polynomial rings). We write $x \,|\, y$ to mean that x divides y. Recall that the *degree* of the monomial $m = \langle \alpha_i : i \in N+1 \rangle$ is

$$\deg(m) = \sum_{i=0}^{N} \alpha_i \in \mathbb{N}.$$

We assume a familiarity with basic Commutative Ring Theory, as found in [DF99, AM69, Eis95, Mat04]. For us, R will always refer to a countable commutative ring with identity element $1 = 1_R \in R$. Recall that an *ideal* of R ($R-$ideal) is a subset of R closed under addition, subtraction, and multiplication by all $R-$elements. Recall that:

- an ideal $P \subseteq R$ is *prime* whenever we have that $a \cdot_R b \notin I$, for all $a, b \notin P$;
- an ideal $M \subseteq R$ is *maximal* whenever there is no ideal $I \subsetneq R$ such that $M \subsetneq I$;
- if M is a maximal ideal, then M is also prime;
- we say that $S \subseteq R$ is a *subring* if it contains $0_R, 1_R$ and is closed under $+_R, \cdot_R$;
- $x \in R$ is a *zero divisor* whenever $x \cdot y =_R 0$, for some $0 \neq_R y$;
- $u \in R$ is a *unit* whenever there exists $x \in R$ such that $x \cdot_R u = 1_R$;
- R is an *integral domain* whenever it contains no zero divisors, i.e. whenever $\{0_R\}$ is a prime ideal; and finally
- x *divides* y, denoted by $x \,|\, y$, whenever there exists $a \in R$ such that $a \cdot_R x = y$.

For any finite sequence $a_0, a_1, \ldots, a_n \in R$, $n \in \mathbb{N}$, define

$$\langle a_0, a_1, a_2, \ldots, a_n \rangle_R = \left\{ \sum_{i=0}^{n} r_i \cdot a_i : r_i \in R \right\} \subseteq R;$$

this is the smallest $R-$ideal containing $a_0, a_1, \ldots, a_n$. For a fixed R, the relation $x \in \langle y \rangle_R$ is called the *division algorithm*; while the relation

$$x \in \langle y_1, y_2, \ldots, y_n \rangle_R, \ n \in \mathbb{N},$$

is called the *generalized division algorithm.* Although we may not always have access to a (generalized) division algorith when working over $\mathsf{RCA_0}$, we take it as an assumption in our HBTM. If R is an integral domain and every ideal I possesses an element x_I such that $\langle x_I \rangle_R = I$, then R is called an *principal ideal domain.* If $U \subseteq R$ is multiplicative(ly closed) and does not contain any zero divisors, then it is always possible to (effectively) construct the localization $R[U^{-1}]$ in which R embeds via an injective ring homomorphism $\psi : R \to R[U^{-1}]$ and such that every $\psi(u)$, $u \in U$, has an $R[U^{-1}]-$inverse. Recall that R is *Noetherian* if it satisfies the ascending chain condition (ACC) on its ideals. This means that R is not Noetherian whenever it contains an infinite strictly ascending chain of ideals

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_k \subsetneq \cdots \subsetneq R, \ k \in \mathbb{N}.$$

An $R-$module M is an abelian group on which R acts both associatively and distributively in each action-factor; modules are generalizations of vector spaces and the two notions are equivalent whenever R is a field. A submodule $N \subseteq M$ is closed under the action of R on M. It follows that R is always a module over itself, and in this case the submodules correspond to ideals. We say that M is *finitely generated* whenever there are finitely many elements of M that span M via the $R-$action. We can also speak of chains of submodules, i.e. sequences of submodules ordered by inclusion. We say that M is *Noetherian* if it contains no infinite strictly ascending submodule chains; i.e. whenever every infinite ascending chain of submodules eventually stabilizes.

2.2. **Reverse Mathematics.**

In this article we work exclusively in the context of Reverse Mathematics and Second-Order Arithmetic; a good introduction to these topics is given in the first two parts of [DM22]. More specifically, we will always assume an axiom system known as $\mathsf{RCA_0}$ that allows for the construction of sets of natural numbers defined by computable predicates, along with an induction scheme for formulas of sufficiently simple arithmetic complexity; more details are given below.

2.2.1. *Induction over* $\mathsf{RCA_0}$*.* We assume familiarity with the arithmetical hierarchy consisting of the Σ_n and Π_n arithmetic formulas; more information on this topic can be found in either [Soa16, Chapter 4] or [DM22, Section 5.2]. Throughout this article we will always assume a hypothesis denoted $\mathsf{RCA_0}$ that, generally speaking, validates computable mathematical constructions via Δ^0_1-comprehension, along with a restricted induction scheme called $\mathsf{I\Sigma_1}$ that grants induction for arithmetic formulas of complexity Σ_1 consisting of a Δ^0_1-predicate preceded by a single existential quantifier. It is well-known that, over $\mathsf{RCA_0}$, the Σ_n-induction scheme is equivalent to the Π_n-induction scheme, and moreover the $\Sigma_{n+1}-$induction scheme is strictly stronger than the Σ_n-induction scheme. For more information on the formalism of Reverse Mathematics and $\mathsf{RCA_0}$, we refer the reader to either [Sim09, Chapter II] or [DM22, Chapter 5]. For us, Σ_1-induction is subsumed in $\mathsf{RCA_0}$, and $\mathsf{I\Sigma_2}$ will be the strongest arithmetical principle that we refer to throughout this article.

2.2.2. $\mathsf{B\Sigma_2}$ *and the Infinite Pigeonhole Principle.* There is another more relevant combinatorial principle, denoted $\mathsf{B\Sigma_2}$, that is implied by $\mathsf{I\Sigma_2}$ and says that for any Δ^0_1 formula ϕ with free variables A, x, y, $A \subseteq \mathbb{N}$, $x, y \in \mathbb{N}$, and corresponding Σ_2-predicate

$$\varphi = (\exists x)(\forall y > x)\phi,$$

for any given $N \in \mathbb{N}$ there exists $x_N \in \mathbb{N}$ such that

$$\varphi(a) \text{ if and only if } (\forall y > x_N)\phi(a), \text{ for all } a \in N+1.$$

$\mathsf{B\Sigma_2}$ is called the Σ_2-Bounding Principle, or simply Σ_2-Bounding. Moreover, a well-known result of Hirst says that, over $\mathsf{RCA_0}$, $\mathsf{B\Sigma_2}$ is equivalent to the Infinite Pigeonhole Principle that says for any $N \in \mathbb{N}$ and function $f : \mathbb{N} \to N$ there exists $n \in N$ such that the fiber $f^{-1}(n) \subseteq \mathbb{N}$ is infinite. In light of Hirst's result, we will use $\mathsf{B\Sigma_2}$ to refer to the Infinite Pigeonhole Principle.

2.2.3. *The well-ordering of* $\mathbb{N}^{\mathbb{N}}$. Recall that a linearly ordered set is *well-ordered* if it does not contain any infinite strictly descending sequences. We use $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ to denote the principle that says, for each $n \in \mathbb{N}$, the (standard) lexicographic ordering on set of length-n sequences of natural numbers $\mathbb{N}^n$ is a well-ordering. By [Sim88, Proposition 2.6], this is equivalent to saying that the length-lexicographic ordering on finite sequences of natural numbers $\mathbb{N}^{\mathbb{N}}$ is a well-ordering. Moreover, Simpson has analyzed the reverse mathematical strength of HBTM for polynomial rings of the form

$$K[\overrightarrow{X}] = K[X_0, X_1, \dots, X_N], \ N \in \mathbb{N},$$

where K is a field, and found that, over $\mathsf{RCA_0}$, $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ is equivalent to the assertion that for any field K and $N \in \mathbb{N}$, $K[\overrightarrow{X}]$ is a Noetherian ring. The proof is essentially a formalization of Buchberger's Algorithm [Eis95, Chapter 15] for computing Gröbner Bases via multivariate polynomial division in $\mathsf{RCA_0}$.

2.3. **The Hilbert Basis Theorem for modules (i.e. HBTM).**

The main theorem in this article characterizes the first-order part (i.e. the arithmetical consequences) of the following theorem in the context of Reverse Mathematics.

Theorem 2.1 (Hilbert Basis Theorem for modules (HBTM))**.** *Let R be a Noetherian ring possessing a generalized division algorithm, and let M be a finitely generated $R-$module. Then M is Noetherian.*

From a constructive point of view such as that of Reverse Mathematics and $\mathsf{RCA_0}$, it is more useful to rephrase HBTM via the following contrapositive.

Theorem 2.2 ((HBTM))**.** *Let R be a ring possessing a generalized division algorithm, and let M be a finitely generated non-Noetherian $R-$module. Then R is not Noetherian; i.e. there exists an infinite strictly ascending chain of $R-$ideals*

$$J_0 \subsetneq J_1 \subsetneq J_2 \subsetneq \cdots \subsetneq J_n \subsetneq \cdots \subsetneq R, \ n \in \mathbb{N}.$$

2.4. **The Significance of Our Main Theorem for the General Hilbert Basis Theorem HBT.**

Our main theorem, i.e. Theorem 3.1 in the following section, says that in the context of Reverse Mathematics $\mathsf{RCA_0} + \mathsf{HBTM}$ implies $\mathsf{B\Sigma_2}$. We will present a proof of HBTM via $\mathsf{B\Sigma_2}$ in the following subsection. Taken together, these results say that HBTM and $\mathsf{B\Sigma_2}$ are equivalent over $\mathsf{RCA_0}$. This is interesting because Simpson has shown [Sim88] that, the Hilbert Basis Theorem for polynomial rings with field coefficients HBTF is equivalent to $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$, and moreover in [Sim] Simpson shows that $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ and $\mathsf{B\Sigma_2}$ are incomparable principles over $\mathsf{RCA_0}$. Therefore, in the context of Simpson's prior work, our work shows that HBTM has incomparable first-order strength with Hilbert's original version of the theorem studied by Simpson in [Sim88]. We now discuss how these results relate to the more general Hilbert Basis Theorem for finitely generated polynomial rings.

Theorem 2.3 (General Hilbert Basis Theorem)**.** *Let R be a Noetherian ring, $N \in \mathbb{N}$, and $R[\vec{X}_N] = R[X_1, X_2, \ldots, X_N]$ be the finitely generated polynomial ring with coefficients in R and indeterminate varaibles $\{X_i\}_{i=1}^N$. Then $R[\vec{X}_N]$ is a Noetherian ring.*

In our constructive context of $\mathsf{RCA_0}$, a more useful rephrasing of the previous theorem is obtain via the following contrapositive form.

Theorem 2.4 ((HBT))**.** *Let R be a ring, $N \in \mathbb{N}$, and let $R[\vec{X}_N]$ denote the polynomial ring in the finitely-many indeterminates $X_1, X_2, \ldots, X_N$. Then, if $R\vec{X}_N$ contains an infinite strictly ascending chain of ideals, so does R.*

After proving Theorem 3.1, we will observe exactly how HBT is more general than HBTM, and almost trivially implies it over $\mathsf{RCA_0}$. Thus, a consequence of our main theorem (Theorem 3.1) will say that HBT implies $\mathsf{B\Sigma_2}$ over $\mathsf{RCA_0}$. Meanwhile, in [Con] the author has previously shown that MDC is equivalent to $\mathsf{WO}(\mathbb{N}^\mathbb{N}) + \mathsf{B\Sigma_2}$ and implies HBTM. Hence, after our main theorem is proven, we will be able to cite Simpson's result [Sim88] to conclude that HBT is equivalent to MDC and also equivalent to $\mathsf{WO}(\mathbb{N}^\mathbb{N}) + \mathsf{B\Sigma_2}$, over $\mathsf{RCA_0}$. Moreover, a result of Simpson [Sim] that is also referred to diagrammatically in [HP16, page 69], says that $\mathsf{B\Sigma_2}$ and $\mathsf{WO}(\mathbb{N}^\mathbb{N})$ are incomparable principles over $\mathsf{RCA_0}$, and therefore each has a strength that is strictly weaker than the conjunction $\mathsf{B\Sigma_2} + \mathsf{WO}(\mathbb{N}^\mathbb{N})$. Thus, when combined, all of these results produce a decomposition of HBT into two related weaker principles, one of which is HBTM.

2.5. HBTM via the Infinite Pigeonhole Principle.

Lemma 2.5 ($\mathsf{RCA_0}$)**.** *Assume that $\mathsf{B\Sigma_2}$ holds. Let R be a ring with a division algorithm, and let M be a non-Noetherian finitely generated $R-$module. Then R is not Noetherian.*

Proof. Let M be generated by $\eta_1, \eta_2, \ldots, \eta_n$, $n \in \mathbb{N}$. Then we can think of any $m \in M$ as a vector

$$m = (r_1, r_2, \ldots, r_n) \equiv \sum_{k=1}^{n} r_k \eta_k \in M,\ r_k \in R.$$

Moreover, since R possesses a generalized division algorithm and M is finitely generated, M also possesses a generalized division algorithm that says whether one element of M is the $R-$span of several other given $M-$elements. Even more, we can use M's generalized division algorithm to effectively row-reduce $M-$vectors in the following way: given a sequence $m_0, m_1, \ldots, m_k \in M$, $k \in \mathbb{N}$, and $m_{k+1} \in M$, via M's generalized division algorithm, we can effectively produce a linear combination of $m_0, m_1 \ldots, m_k$ via coefficients $a_0, a_1, \ldots, a_k \in R$ such that:

- $m_{k+1} + \sum_{\ell=0}^{k} a_\ell m_\ell = \sum_{i=1}^{j_{k+1}} x_i \eta_i$, $j_{k+1} \in \mathbb{N}$, $j_{k+1} \leq k$, such that
  - $j_{k+1} = 0$ if and only if $m_{k+1} \in \langle m_0, m_1, \ldots, m_k \rangle_R$; and otherwise
  - $j_{k+1} \geq 1$ and and $x_{j_{k+1}} \neq_R 0$.

  Furthermore,
- for any coefficients $c_1, c_2, \ldots, c_k \in R$ there do not exist corresponding coefficients $x_1, x_2, \ldots, x_{j_{k+1}-1} \in R$ such that

$$m_{k+1} + \sum_{\ell=1}^{k} c_\ell m_\ell = \sum_{i=1}^{j_{k+1}-1} x_i \eta_i.$$

Now, since M is not Noetherian it has an infinite sequence $\{m_k\}_{k \in \mathbb{N}}$ such that $m_0 \neq 0_M$ and

$$m_{k+1} \notin \langle m_0, m_1, \ldots, m_k \rangle_R \subset M,\ k \in \mathbb{N}.$$

Furthermore, via the uniform row reductions described in the items above, we can assume that each m_{k+1} is reduced via its predecessors, and that $j_k \in \mathbb{N}$, $1 \leq j_k \leq n$ is as above. Moreover, $\mathsf{B}\Sigma_2$ says that for some $1 \leq n_0 \leq n$, $n_0 \in \mathbb{N}$, there is an infinite subsequence of the $\{j_k\}_{k\in\mathbb{N}}$ such that $j_k = n_0$. Without any loss of generality (i.e. by passing to an infinite subsequence and re-indexing the row-reduced $M-$elements) we may assume that $j_k = n_0$ for all $k \in \mathbb{N}$. Furthermore, for each $k \in \mathbb{N}$, let $x_{k,n_0} \in R$ denote the $R-$coefficient of $\eta_{n_0} = \eta_{j_k}$ in (the row-reduced) m_k. Then by our construction of j_k it follows that for each $k \in \mathbb{N}$ we have that

$$x_{k+1} \notin \langle x_0, x_1, \ldots, x_k \rangle_R.$$

From which it follows that R is not Noetherian, since if we define

$$J_k = \langle x_0, x_1, \ldots, x_k \rangle_R$$

then we have that

$$J_0 \subsetneq J_1 \subsetneq \cdots \subsetneq J_k \subsetneq \cdots \subsetneq R, \ k \in \mathbb{N}.$$

□

2.5.1. *The base ring $R_{0,N}$.* In this section we construct, for each $N \in \mathbb{N}$, $N \geq 1$. a general ring $R_0 = R_{0,N}$ that will form the basis of the construction of our main theorem. Fix a natural number $N \geq 1$, and let

$$\vec{X} = \vec{X}_N = \{X_{k,\ell} : 1 \leq k \leq N, \ k, \ell \in \mathbb{N}\}$$

be a set of indeterminate variables. Define

$$\mathbb{Q}_\infty = \mathbb{Q}_{N,\infty} = \mathbb{Q}[\vec{X}]$$

to be the polynomial ring with $\mathbb{Q}-$coefficients and indeterminate variables $\vec{X}$. For each $k = 1, 2, \ldots, N$ it is not difficult to see that the ideal

$$P_k = P_{N,k} = \langle X_{k,\ell} : \ell \in \mathbb{N} \rangle \subseteq \mathbb{Q}_\infty$$

is prime since its complement

$$\overline{P_k} = \mathbb{Q}_\infty \setminus P_k$$

is multiplicatively closed; it follows that

$$U = U_N = \bigcap_{k=1}^{N} \overline{P_k} \subseteq \mathbb{Q}_\infty$$

is multiplicatively closed and consists of those $\mathbb{Q}_\infty-$polynomial elements x such that for each $k = 1, 2, \ldots, N$ there exists a nonzero $x-$monomial summand consisting only of indeterminates of the form $X_{k,\ell}$, $\ell \in \mathbb{N}$. Since $\mathbb{Q}_\infty$ is an integral domain and hence U contains no zero divisors, we can construct the localization $\mathbb{Q}_\infty[U^{-1}]$ in which $\mathbb{Q}_\infty$ embeds and every $x \in U$ is invertible.

Now, for any given $x \in Q_\infty$, if m denotes the greatest common divisor of the monomial summands of x (after all possible cancellations) then m is a $\vec{X}-$monomial and after factoring m out of each monomial summand of x we obtain a factorization of the form

$$x = m \cdot u,$$

where $u \in U$. In other words, every element of the localized $Q_\infty[U^{-1}]$ is the product of a unit and a $\mathbb{Q}_\infty-$monomial. Furthermore, if $I \subseteq \mathbb{Q}_\infty[U^{-1}]$ is an ideal, then it follows that there is a unique $Q_\infty-$monomial m such that $m \in I$ and m divides every $x \in I$; in other words I is generated by m and $\mathbb{Q}_\infty[U^{-1}]$ is a principal ideal domain. These arguments will also hold for our ring R_N in the following paragraph, although R_N is not an integral domain.

Finally, the construction of $R_N = R_{0,N}$ from $\mathbb{Q}_\infty[U^{-1}]$ requires introducing the following R_N-indeterminate multiplication relations:

(a) $X_{k_1,\ell_1} \cdot X_{k_2,\ell_2} =_{R_N} 0$, $k_1, k_2, \ell_1, \ell_2 \in \mathbb{N}$, $k_1 \neq k_2$; and
(b) $X^2_{k,\ell+1} =_{R_N} X_{k,\ell}$, $1 \leq k \leq N$, $k, \ell \in \mathbb{N}$.

Relation (a) is not essential to our construction but helps to simplify R_N by eliminating unnecessary monomial products, while (b) essentially says that for any $1 \leq k \leq N$, $k, \ell \in \mathbb{N}$, $X_{k,\ell+1}$ is the square root of $X_{k,\ell}$. It follows that, for each $k \in \mathbb{N}$, $1 \leq k \leq N$, the R_N-ideal

$$P_k = P_{R,N,k} = \langle X_{k,\ell} : \ell \in \mathbb{N} \rangle_{R_N}$$

is maximal, and every R_N-prime ideal is of this form. By our construction of $\mathbb{Q}_\infty[U^{-1}]$ it follows that if $I \subseteq R_N$ is an ideal then there exists $k \in \mathbb{N}$, $1 \leq k \leq N$, such that either:

- $I = P_k$; or else
- $I = \langle X_{k,\ell} \rangle$ for some $\ell \in \mathbb{N}$.

It now follows that if

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_j \subsetneq \cdots \subsetneq R_N, \; j \in \mathbb{N},$$

is an infinite strictly ascending chain of ideals then, since each $P_k \subsetneq R_n$, $1 \leq k \leq N$, $k \in \mathbb{N}$, is maximal and $P_{k_0} \cap P_{k_1} = 0$ whenever $k_0 \neq k_1$, there exists an infinite strictly increasing sequence of natural numbers

$$\ell_0 < \ell_1 < \ell_2 < \cdots < \ell_j < \cdots, \; j \in \mathbb{N},$$

and $1 \leq k_0 \leq N$, $k_0 \in \mathbb{N}$, such that for each $j \in \mathbb{N}$ we have that

$$I_j = \langle X_{k_0,\ell_j} \rangle \subsetneq R_N.$$

Moreover, since R_N is effective and in the case that $\{I_k\}_{k\in\mathbb{N}}$ has a uniformly effective presentation then $\{\ell_k\}_{k\in\mathbb{N}}$ can be effectively determined (via search) as well. The same conclusions can be drawn (via the same arguments) for any subring $S_N \subseteq R_N$ such that $u^{-1} \in S$ whenever $x = m \cdot u \in S$, $m \in Q_\infty$ a monomial, $u \in U$.

3. Our main result

Theorem 3.1 (RCA_0). HBTM *implies* $\mathsf{B}\Sigma_2$.

Proof. We will prove the Infinite Pigeonhole Principle $\mathsf{B}\Sigma_2$ via $\mathsf{RCA}_0 + \mathsf{HBTM}$. To do this, first suppose that $f : \mathbb{N} \to N$, for some $N \in \mathbb{N}$, $N \geq 1$; we will prove $\mathsf{B}\Sigma_2$ by establishing the existence of a number $1 \leq k_0 \leq N$ such that the fibre $f^{-1}(k_0)$ is infinite.

First of all, let R_N be as in Section 2.5.1 above. Using f, we will construct a computable subring $R \subseteq R_N$ and corresponding finitely generated $R-$module M such that M has an infinite strictly ascending chain of submodules and so HBTM says that R must have an infinite ascending chain of ideals. To construct R:

(I) for each $x = 0, 1, 2, \ldots$, enumerate the indeterminate $X_{k,\ell} \in \vec{X_N} \subset R_N$, $1 \leq k \leq N$, $\ell \in \mathbb{N}$, into R whenever $f(x) = k$ and

$$|f^{-1}(k) \cap \{0, 1, 2, \ldots, x-1\}| = \ell,$$

as well as all polynomials $p \in \mathbb{Q}_\infty$ in which $X_{k,\ell}$ appears. Also,

(II) for each polynomial $p \in \mathbb{Q}_\infty \subseteq R_N$ currently in R with factorization $p = m \cdot u$, $u \in U$, monomial (GCD) $m \in \mathbb{Q}_\infty$, enumerate $u^{-1} \in U^{-1}$ into R as well.

Let M be the free $R-$module generated by $\{\omega_1, \omega_2, \ldots, \omega_N\}$, and define

- $N_0 = \langle 0 \rangle_N$; and

- $N_{x+1} = N_j +_M \langle X_{k,\ell} \cdot_N \omega_k \rangle_N$, where $x, k, \ell \in \mathbb{N}$, $1 \leq k \leq N$, are such that $X_{k,\ell}$ is enumerated into R at stage x via item (I) above. By our construction of R and N_x it follows that $X_{k,\ell} \notin N_x$ since only $X_{k,0}, X_{k,1}, \ldots, X_{k,\ell-1}$ have been enumerated into R before stage x, and $X^2_{k,j+1} =_R X_{k,j}$ for each $j = 0, 1, \ldots, \ell - 1$.

It follows that $\{N_x\}_{x\in\mathbb{N}}$ is uniformly effectively definable infinite strictly increasing sequence of $M-$submodules, which satisfies the hypothesis of our (contrapositive) principle HBTM. Therefore, our assumption of HBTM says that R cannot be a Noetherian ring and thus produces an infinite strictly ascending chain of ideals

$$I_0 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots \subsetneq I_j \subsetneq \cdots \subsetneq R, \ j \in \mathbb{N}.$$

However, we have already argued in Section 2.5.1 above that any such chain must be of the form

$$I_j = \langle X_{k,\ell_j} \rangle_R$$

for a fixed $k \in \mathbb{N}$ and an infinite strictly increasing sequence

$$\ell_0 < \ell_1 < \ell_2 < \cdots < \ell_j < \cdots, \ j, \ell_j \in \mathbb{N}.$$

By our construction of R it follows that the fibre $f^{-1}(k)$ must be infinite, thus witnessing the Infinite Pigeonhole Principle $\mathsf{B\Sigma_2}$ for the given function f. □

Now that we have proven our main result and established the equivalence of HBTM and $\mathsf{B\Sigma_2}$ over $\mathsf{RCA_0}$, we make an almost trivial observation of how HBTM follows from HBT in a strong way, even over $\mathsf{RCA_0}$. The easiest way to see the implication is to interpret the module-generators $\omega_1, \omega_2, \ldots, \omega_n$ as indeterminate variables of a polynomial ring

$$R_N[\vec{\omega}] = R_N[\omega_1, \omega_2, \ldots, \omega_N] \cong R_N[X_1, X_2, \ldots, X_N]$$

where "generator powers" of the form

$$\omega_k^\ell = \underbrace{\omega_k \cdot \omega_k \cdot \cdots \cdot \omega_k}_{\ell}, \ k, \ell \in \mathbb{N}, \ 1 \leq k \leq N,$$

exist. Under this interpretation, the infinite strictly ascending chain of $M-$submodules translates to an infinite strictly ascending chain of $R_N[\vec{\omega}]-$ideals, witnessing the non-Noetherianness of $R_N[\vec{\omega}]$. Our assumption of HBT then produces an infinite strictly ascending R_N-chain, which we explained in Section 2.5.1 above and utilized in previous proof, can be used in the context of $\mathsf{RCA_0}$ to construct a witness for the Infinite Pigeonhole Principle $\mathsf{B\Sigma_2}$.

We have now shown how the proof of the previous theorem can be reinterpreted to prove the following theorem.

Theorem 3.2 ($\mathsf{RCA_0}$). HBT *implies* $\mathsf{B\Sigma_2}$.

In [Sim88], Simpson shows that HBT implies $\mathsf{WO}(\mathbb{N}^\mathbb{N})$.

Corollary 3.3 ($\mathsf{RCA_0}$). HBT *implies* $\mathsf{B\Sigma_2} + \mathsf{WO}(\mathbb{N}^\mathbb{N})$.

In [Con] the author shows that the Monomial Division Chain Principle MDC is equivalent to $\mathsf{WO}(\mathbb{N}^\mathbb{N}) + \mathsf{B\Sigma_2}$, and proves HBT, over $\mathsf{RCA_0}$.

Corollary 3.4 ($\mathsf{RCA_0}$). HBT *is equivalent to both* MDC *and* $\mathsf{B\Sigma_2} + \mathsf{WO}(\mathbb{N}^\mathbb{N})$.

Simpson [Sim] and others [HP16, page 69] have shown that $\mathsf{B\Sigma_2}$ and $\mathsf{WO}(\mathbb{N}^\mathbb{N})$ are incomparable principles over $\mathsf{RCA_0}$, neither of which implies the other in this context. Our results here explain why HBTM is equivalent to $\mathsf{B\Sigma_2}$ over $\mathsf{RCA_0}$, while [Sim88] proves that HBTF is equivalent to $\mathsf{WO}(\mathbb{N}^\mathbb{N})$ over $\mathsf{RCA_0}$. Thus, when taken together all of these results yield a decomposition of HBT into two incomparable strictly weaker variants of the Hilbert Basis Theorem, namely HBTM (equivalent to $\mathsf{B\Sigma_2}$) and HBTF (equivalent to $\mathsf{WO}(\mathbb{N}^\mathbb{N})$), over $\mathsf{RCA_0}$.

References

[AM69] M.F. Atiyah and I.G. MacDonald. *Introduction to Commutative Algebra*. Perseus, 1969.

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

[Con] C.J. Conidis. On the existence of infinite monomial division chains with finitely many indeterminates. To appear in Lecture Notes in Computer Science.

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

[DM22] D. D. Dzhafarov and C. Mummert. *Reverse Mathematics: Problems, Reductions, and Proofs*. Springer-Verlag, 2022.

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

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

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

[HP16] P. Hájek and P. Pudlák. *The Metamathematics of First-Order Arithmetic*. Cambridge University Press, 2016.

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

[Sim] S. G. Simpson. Comparing $\mathrm{WO}(\omega^\omega)$ with Σ^0_2 induction. Unpublished. Available at https://arxiv.org/abs/1508.02655.

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

[Sim09] S.G. Simpson. *Subsystems of Second Order Arithmetic, second edition*. Cambridge University Press, 2009.

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

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

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