Formal power series in Second-Order Arithmetic

Chris J. Conidis[1]

College of Staten Island, Staten Island, New York, USA
chris.conidis@csi.cuny.edu

1 Introduction

If $\mathbb{N} = \{0, 1, 2, \ldots\}$ denotes the set of natural numbers, then a well-known algebraic fact says that, for any field F[1], the (finitely generated polynomial) ring $F[\vec{X}_N] = F[X_1, X_2, \ldots, X_n]$ is Noetherian (i.e. satisfies the ascending chain condition on its ideals) for any natural number n. Classically, this result is known as the Hilbert Basis Theorem (HBT), and was established by Hilbert [8] via nonconstructive methods. Later on, Buchberger's Algorithm [6, Theorem 15.9] for computing Gröbner Bases in $F[\vec{X}_N]$ yielded a constructive (computable) proof of the Hilbert Basis Theorem for polynomial rings. After Buchberger's results, Simpson [12] showed that, in the context of Reverse Mathematics, HBT for $F[\vec{X}_N]$ is logically equivalent to the First-Order statement asserting the well-ordering of the ordinal number $\mathbb{N}^{\mathbb{N}}$ that corresponds (i.e. is isomorphic) to finite $\mathbb{N}-$sequences with the length-lexicographic ordering. This article is a precursor to a follow-up article that seeks to examine and classify the computability-theoretic properties of HBT for polynomial rings and its consequences such as the Artin-Rees Lemma, Krull Intersection Theorem, and related results concerning rings of formal power series.

In particular, we aim to exhibit the central role that the standard proof of HBT for the ring $R[\vec{X}_N]$ of polynomials plays in establishing similar results in the context of rings of formal power series. More specifically, Theorem 3.1 below formalizes [10, Theorem 3.3] in the context of RCA_0, and in so doing essentially establishes an effective reduction between the Hilbert Basis Theorem in the contexts of rings of polynomials and formal power series, and is the basis of all of our main results. Afterwards, Section 4 applies the basic module of Theorem 3.1 to show that, in the context of Reverse Mathematics, all known implications concerning HBT for polynonmial rings also hold for HBT in the context of formal power series.

2 Preliminaries

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

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

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

$$\vec{X}_N = \{X_0, X_1, \ldots, X_N\}$$

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

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

[1]Recall that a field is essentially any "number system" with commutative addition and multiplication operations such that any nonzero element has a multiplicative inverse.

so that each $\vec{X}_N$−monomial m is uniquely determined by its exponents $m \sim \langle \alpha_i : 0 \le i \le N \rangle \in \mathbb{N}^{\mathbb{N}+1}$. Now, if we define the *degree* of m to be $\sum_{i=0}^{N} \alpha_i \in \mathbb{N}$, then for each $n \in \mathbb{N}$, there are only finitely many monomials of degree n, and it follows that if we denote the set of $\vec{X}_N$−monomials by $\mathcal{M}$, then there is an $\mathcal{M}$−enumeration of nondecreasing degree. Moreover, we say that a monomial m_0 *divides* a monomial m_1 whenever the m_1−exponent of the indeterminate factor X_i is at least as large as that of m_0, for each $i = 0, 1, \dots, N$. Also recall that, while polynomials consisting of finitely many summand terms always have a leading term of *maximal degree*, for formal power series consisting of infinite sums containing unbounded exponents the leading term is taken to be the $\mathcal{M}$−least one having *minimal degree*.

We assume a familiarity with basic Commutative Ring Theory, as found in [4, 1, 6, 10]. 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. For any finite sequence $a_0, a_1, \dots, a_n \in R$, $n \in \mathbb{N}$, define

$$\langle a_0, a_1, a_2, \dots, a_n \rangle_R = \left\{ \sum_{i=0}^{n} r_i \cdot a_i : r_i \in R \right\};$$ [2]

this is the smallest R−ideal containing $a_0, a_1, \dots, a_N$. Recall that R is *Noetherian* if it satisfies the ascending chain condition (ACC) on its ideals. This is equivalent to saying that for any given infinite sequence $\{a_i\}_{i \in \mathbb{N}} \subseteq R$ there exists $N_0 \in \mathbb{N}$ such that the first N_0−many elements of A, $A_0 = \{a_0, a_1, \dots, a_{N_0}\} \subseteq A$, generates A, i.e. each a_i, $i \in \mathbb{N}$, can be written as an R−linear combination of the elements of A_0. If R is a ring, then its *generalized division algorithm* is the relation

$$x \in \langle a_0, a_1, \dots, a_N \rangle_R, \; N \in \mathbb{N}, \; x, a_0, a_1, \dots, a_N \in R.$$

Finally, recall that the Hilbert Basis Theorem (HBT) says that, for each ring R and $n \in \mathbb{N}$, the polynomial ring

$$R[\vec{X}_N] = R[X_0, X_1, \dots, X_n]$$

is Noetherian whenever R is Noetherian.

We will be examining HBT in the context of Reverse Mathematics for rings of formal power series over various coefficient rings R and sets of indeterminate variables $\vec{X}_N = \{X_0, X_1, \dots, X_N\}$, $N \in \mathbb{N}$. Formal power series are infinitary objects, and so we will formally represent them in the context of Reverse Mathematics and $\mathsf{RCA_0}$ numerically via their Turing (Gödel) codes. More specifically, a formal power series ring is a set $X \subseteq \mathbb{N}$ such that every $x \in X$ is the code of a formal power series, and X is closed under addition, subtraction, and multiplication of power series (codes). Other algebraic definitions, such as ideals and generating sets, are also defined via codes. The reader should keep in mind that, for us, specifying a formal power series amounts to giving an algorithm for computing its infinitely many coefficients, one coefficient for each monomial summand.

2.0.1 Reverse Mathematics, $\mathsf{RCA_0}$, and induction

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 [14, Chapter 4] or [5, Section 5.2]. Throughout this article we work in the context of Reverse Mathematics and Subsystems of Second-Order Arithmetic[3] that always assumes a hypothesis denoted $\mathsf{RCA_0}$ which, generally

[2] Note the subscript R on the lefthand side; for us, it distinguishes *ideals* from *sequences*.

[3] The program of Reverse Mathematics was first introduced by H. Friedman in the 1970s. More information on this modern branch of Mathematical Logic, including an introduction and historical remarks, can be found in [13, 5].

speaking, validates computable mathematical constructions via a Δ^0_1-comprehension axiom, 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. For more information on the formalism of Reverse Mathematics and $\mathsf{RCA_0}$, we refer the reader to either [13, Chapter II] or [5, Chapter 5]. Induction schemes are arithmetical axioms that only pertain to the first-order theory of any subsystem of Second-Order Arithmetic. Throughout this article we will only work with arithmetical subsystems of Second-Order Arithmetic over $\mathsf{RCA_0}$ that follow from Σ_2-induction ($\mathsf{I\Sigma_2}$); the next subsection describes these specific axioms in more detail.

2.1 Preliminary Combinatorics: the Infinite Pigeonhole Principle, the Well-Ordering of $\mathbb{N}^{\mathbb{N}}$, and the existence of monomial division chains

2.1.1 The Infinite Pigeonhole Principle

Recall the Infinite Pigeonhole Principle says that if $f : A \to B$ is a function with infinite domain A and finite range B, then for some $b \in B$ the fiber

$$f^{-1}(b) = \{a \in A : f(a) = b\}$$

is infinite. In the context of Reverse Mathematics (i.e. over $\mathsf{RCA_0}$) a theorem of Hirst [9] says that the Infinite Pigeonhole Principle is equivalent to a bounding principle for Σ_2-formulas that produces uniform bounds for finite sets of existential witnesses to Σ_2-formulas, and so over $\mathsf{RCA_0}$ we denote the Infinite Pigeonhole Principle by $\mathsf{B\Sigma_2}$.

2.1.2 The well-ordering of $\mathbb{N}^{\mathbb{N}}$

There is an arithmetical principle that follows from $\mathsf{I\Sigma_2}$ and says that the ordinal number $\mathbb{N}^{\mathbb{N}}$ is well-ordered. This is equivalent to saying that the length-lexicographic ordering on finite sequences of natural numbers is a well-order. We denote this principle by $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$. Simpson [12] has shown that $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ is equivalent to saying that the finitely generated polynomial ring $F[\vec{X}_N] = F[X_0, X_1, \dots, X_N]$, $N \in \mathbb{N}$, with coefficients in a field F is Noetherian. Along the way Simpson also shows the equivalence between $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ and the Noetherian criterion for monomials that says if $M = \{m_i\}_{i\in\mathbb{N}} \subseteq F[\vec{X}_N]$ is an infinite sequence of $\vec{X}_N-$monomials (i.e. finite products of indeterminates in $\vec{X}_N$) then there exists $n_0 \in \mathbb{N}$ such that for all $n \in \mathbb{N}$ we have that m_n is divisible by some element of $M_0 = \{m_i\}_{i=0}^{n_0}$, i.e. M_0 generates M.

2.1.3 The existence of monomial division chains

Recently in [3] the author has studied a combinatorial principle that plays a key role in the proof of the Hilbert Basis Theorem, called MDC, that says if $M = \{m_i\}_{i=0}^{\infty}$ is an infinite sequence of $\vec{X}_N = \{X_0, X_1, \dots, X_N\}-$monomials, $N \in \mathbb{N}$, then there exists an infinite subsequence $\{i_k\}_{k=0}^{\infty} \subseteq \mathbb{N}$ such that for each $k \in \mathbb{N}$ we have that m_{i_k} divides $m_{i_{k+1}}$. Moreover, building on results of Simpson [12] and Chong, Slaman and Yang [2], the author has shown MDC to be equivalent to $\mathsf{B\Sigma_2} + \mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ over $\mathsf{RCA_0}$, while Simpson [11] has shown that $\mathsf{B\Sigma_2} + \mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ is strictly stronger than either $\mathsf{B\Sigma_2}$ or $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$, and that $\mathsf{B\Sigma_2} + \mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ is strictly weaker than $\mathsf{I\Sigma_2}$.

3 Transfering the Division Algorithm from $R[\vec{X}_N]$ to $R[[\vec{X}_N]]$

The following theorem is the essential key to all of our results. Its proof is essentially a formalization of [10, Theorem 3.3] in RCA_0.

Theorem 3.1 (The Division Algorithm for power series rings with Noetherian coefficients, RCA_0)**.** *Suppose that R is a ring, $n \in \mathbb{N}$, and let*

- $\vec{X}_N = \{X_0, X_1, \dots, X_n\}$ *be a set of $n-$many indeterminates corresponding to rings $R[\vec{X}_N]$ and $R[[\vec{X}_N]]$, and such that*
  - $\mathcal{M} = \{m_i\}_{i=0}^{\infty}$ *is an enumeration of the $\vec{X}_N-$monomials in nondecreasing order of $\mathbb{N}-$degree,*
- $F = \{f_k\}_{k\in\mathbb{N}} \subseteq R[[X]]$ *be an enumeration of an $R[[\vec{X}_N]]-$ideal with*

$$f_k = \sum_{i=0}^{\infty} a_{k,i} m_i,\ a_{k,i} \in R,$$

and such that $\ell_k \in \mathbb{N}$ is ($\mathbb{N}-$)least such that $a_{k,\ell_k} \neq_R 0$. In this case we have that $s_k = a_{k,\ell_k} m_{\ell_k}$ denotes the leading summand of f_k.

Now, suppose that there exists some $N_0 \in \mathbb{N}$ that witnesses the Noetherian property that says:

$$\langle s_k : k \in \mathbb{N}\rangle_{R[\vec{X}_N]} = \langle s_0, s_1, \dots, s_{N_0}\rangle_{R[\vec{X}_N]}, \tag{1}$$

then we also have that

$$F = \langle f_k : k \in \mathbb{N}\rangle_{R[[\vec{X}_N]]} = \langle f_k : 0 \leq k \leq N_0\rangle_{R[[\vec{X}_N]]}.$$

Proof. Let

$$S_0 = \{s_0, s_1, \dots, s_{N_0}\},\quad F_0 = \{f_0, f_1, \dots, f_{N_0}\},$$

and $k = k_0 \in \mathbb{N}$. By hypothesis we have that

$$f_{k_0} = a_{k_0,\ell_{k_0}} m_{\ell_{k_0}} + \sum_{\ell > \ell_{k_0}} a_{k_0,\ell} m_\ell = s_{k_0} + \sum_{\ell > \ell_{k_0}} a_{k_0,\ell} m_\ell,$$

and moreover we can write the leading summand $s_{k_0} = a_{k_0,\ell_{k_0}} m_{\ell_{k_0}} \in R[\vec{X}]$ of f_{k_0} as an $R[\vec{X}_N]-$linear combination of $\{s_0, s_1, \dots, s_{N_0}\}$. Therefore, if we have that

$$s_{k_0} = \sum_{i=0}^{N_0} c_{k_0,i} s_i,\ c_{k_0,i} \in R[\vec{X}_N],$$

then it follows that

$$f_k - \sum_{i=0}^{N_0} c_{k,i} f_i = f_{k_1} \in F$$

is such that $\ell_{k_1} > \ell_{k_0}$. Furthermore, we can repeat the argument, in infinitely many stages indexed by $i \in \mathbb{N}$, to obtain an infinite sequence of numbers $\{k_i\}_{i\in\mathbb{N}}$ corresponding to power series $\{f_{k_i}\}_{i\in\mathbb{N}} \subseteq F$ such that for every $i \in \mathbb{N}$ we have that

$$\ell_{k_{i+1}} > \ell_{k_i};$$

in other words, the $\mathcal{M}-$index of the leading summand of $f_{k_{i+1}}$ is strictly greater than that of f_{k_i}. Now, the degrees of the monomials in any enumeration of $\mathcal{M}$ always grow uniformly, and thus we have that $\lim_i \deg(m_i) = \infty$. Also, because our sets S_0 and F_0 are fixed thorughout the construction, at each stage $i \in \mathbb{N}$, in order to obtain the cancellation required for $\ell_{i+1} > \ell_i$, we must have that

$$\lim_j \deg(c_{k_j,i}) = \infty,$$

uniformly in $i = 0, 1, \ldots, N_0$. Finally, by our construction it follows that if we set

$$c_i = \sum_{j=0}^{\infty} c_{k_j,i}, \; i = 0, 1, \ldots, N_0,$$

then $c_i \in R[[\vec{X}_N]]$ and

$$f_k = \sum_{i=0}^{N_0} c_i f_i.$$

□

Remark 3.2. *The key assumption in the previous theorem is the existence of $N_0 \in \mathbb{N}$, which essentially assumes a division algorithm for $R[\vec{X}_N]$, $N \in \mathbb{N}$. It would benefit the reader to keep in mind that the hypotheses in the theorems that follow, all of which utilize Theorem 3.1, are chosen so as to guarantee the existence of the number N_0 in the previous proof, and that the necessary hypotheses for producing N_0 depend upon the properties of R and N.*

4 Transfering the Noetherian property from R to $R[[\vec{X}_N]]$ (via $R[\vec{X}_N]$)

Let F be a field and R be a ring with a generalized division algorithm. The goal of this section is to apply Theorem 3.1 to successively more general power series rings of the form $R[[X]]$, $F[\vec{X}_N]$, and finally $R[[\vec{X}_N]]$. Each application corresponds to a different subsystem of Second-Order Arithmetic.

In the proofs of each of the theorems below $F = \{f_k\}_{k\in\mathbb{N}}$ will always denote the ideal of $R[[\vec{X}_N]]$, $\vec{X}_N = \{X_0, X_1, \ldots, X_n\}$, $n \in \mathbb{N}$, for which we produce a finite set of generators via Theorem 3.1 above. Also, as in Theorem 3.1, recall that $\mathcal{M} = \{m_i\}_{i\in\mathbb{N}}$ denotes an enumeration of $\vec{X}_N-$monomials of nondecreasing $\mathbb{N}-$degree, and for each $k \in \mathbb{N}$, $\ell_k \in \mathbb{N}$ is least such that the leading summand of f_k is of the form $a_{\ell_k} \cdot m_{\ell_k}$ for some $0 \neq_R a_k$. With all of this notation and definitions in mind and out of the way, the main focus of our proofs will be the construction of the number N_0 mentioned in the hypothesis of Theorem 3.1 above.

Theorem 4.1 (RCA_0)**.** *$R[[X]]$ is Noetherian whenever R is a Noetherian ring possessing a generalized division algorithm.*

Proof. To construct N_0 in the current context, there are two cases to consider. The first case says that

$$a_{k+1} \notin \langle a_0, a_1, \ldots, a_k \rangle_R$$

for infinitely many $k \in \mathbb{N}$. In this case it follows that R is not Noetherian, which is a contradiction. So we are in the second case which says that there exists $N_0 \in \mathbb{N}$ such that for all $k \in \mathbb{N}$, $k \geq N_0$, we have that

$$a_k \in \langle a_0, a_1, \ldots, a_{N_0} \rangle_R.$$

The hypothesis of the current theorem says that $\vec{X}_N = \vec{X} = \{X\}$, and it is not difficult to verify that the current N_0 satisfies the hypothesis of Theorem 3.1 above. □

Recall that fields are a subclass of rings, all of which possess the same trivial division algorithm, and in which division is always possible unless the divisors are all zero. The following result is also contained in [7, Corollary 3].

Theorem 4.2 ($\mathsf{RCA}_0 + \mathsf{WO}(\mathbb{N}^{\mathbb{N}})$)**.** *$F[[\vec{X}_N]]$ is Noetherian whenever F is a field.*

Proof. Simpson [12] has shown that, over RCA_0, $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ implies that $F[\vec{X}_N]$ is Noetherian, which is equivalent to saying that for any infinite sequence of $\vec{X}_N-$monomials $\{m_k\}_{k\in\mathbb{N}}$ there exists $N_0 \in \mathbb{N}$ such that for any $k \in \mathbb{N}$, $k \geq N_0$,

$$m_k \in \langle m_0, m_1, \ldots, m_{N_0}\rangle_{F[\vec{X}_N]}.$$

Finally, since F is a field it follows that N_0 satisfies the hypothesis of Theorem 3.1. □

Theorem 4.3 ($\mathsf{RCA}_0 + \mathsf{MDC}$)**.** *$R[[\vec{X}_N]]$ is Noetherian whenever R is a Noetherian ring possessing a generalized division algorithm.*

Proof. First of all, recall that MDC implies $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ and $\mathsf{B\Sigma}_2$ (the Infinite Pigeonhole Principle). As in the proof of the previous theorem above, it follows from our implicit assumption $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ that there exists $N_1 \in \mathbb{N}$ such that for all $k \geq N_1$, $k \in \mathbb{N}$, we have

$$m_k \in \langle m_0, m_1, \ldots, m_{N_1}\rangle_{R[\vec{X}_N]};$$

i.e. one of the monomials $m_0, m_1, \ldots, m_{N_1}$ divides m_k. For each $k = 0, 1, \ldots, N_1$, let

$$A_k = \{a_\ell : m_k \,|\, m_\ell\}.$$

Now, since R is Noetherian and possesses a generalized division algorithm, it follows that for each $k = 0, 1, 2, \ldots, N_1$ there exists $N_{k+2} \in \mathbb{N}$ such that $A_k \cap \{a_i : i \leq N_{k+2}\}$ is a finite generating set for A_k (or else, under the current hypothesis, we could construct an infinite strictly ascending chain of ideals in R), and MDC implies $\mathsf{B\Sigma}_2$ which says that there exists a uniform upper bound N_0 on $\{N_i : 1 \leq i \leq N_1 + 2\}$. By our construction of the $\{N_i : 0 \leq i \leq N_1 + 2\}$, it follows that N_0 satisfies the hypothesis of Theorem 3.1 above. □

References

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

[2] C. T. Chong, T. A. Slaman, and Y. Yang. Π^1_1-conservation of combinatorial principles weaker than Ramsey's theorem for pairs. *Advances in Mathematics*, 230(3):1060–1077, 2012.

[3] C. J. Conidis. On the existence of infinite monomial division chains. To appear.

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

[5] D. D. Dzhafarov and C. Mummert. *Reverse Mathematics*. Springer, 2022.

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

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

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

[9] J.L. Hirst. Combinatorics in subsystems of second order arithmetic. PhD Thesis, Pennsylvania State University, 1987.

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

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

[12] S. G. Simpson. Ordinal numbers and the hilbert basis theorem. *J. Symbolic Logic*, 53(3):961–974, 1988.

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

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