On the existence of infinite monomial division chains with finitely many indeterminates

Chris J. Conidis[1]

College of Staten Island

Abstract. Let R be a ring, and let $\overrightarrow{X} = \{X_0, X_1, \ldots, X_N\}$, $N \in \mathbb{N}$, finitely many indeterminate variables. We introduce a combinatorial principle in this context called MDC that produces, for any given infinite sequence of monomials

$$Z_0, Z_1, Z_2, \ldots, Z_k, \ldots \in R[\overrightarrow{X}],\ k \in \mathbb{N},$$

of strictly increasing degree, an infinite subsequence

$$Z_{k_0}, Z_{k_1}, \cdots, Z_{k_n}, \cdots,\ n \in \mathbb{N},$$

such that for each n we have that Z_{k_n} divides $Z_{k_{n+1}}$. We show that, in the context of Reverse Mathematics and Subsystems of Second-Order Arithmetic, MDC is an arithmetical principle equivalent to $\mathsf{B\Sigma}_2 + \mathsf{WO}(\mathbb{N}^{\mathbb{N}})$, where $\mathsf{B\Sigma}_2$ is a bounding principle for Σ_2 formulas equivalent to the Infinite Pigeonhole Principle (over RCA_0), and $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ asserts that finite sequences of natural numbers $\mathbb{N}^{\mathbb{N}}$ are well-ordered via the length-lexicographic ordering.

1 Introduction

If $\mathbb{N} = \{0, 1, 2, \ldots\}$ denotes the set of natural numbers, then a well-known algebraic fact called the Hilbert Basis Theorem (HBT) says that, for any field F[1], the (finitely generated polynomial) ring $F[\overrightarrow{X}] = F[X_1, X_2, \ldots, X_n]$ is Noetherian (i.e. satisfies the ascending chain condition on its ideals) for any natural number n. This classic result was first established by Hilbert [7] via nonconstructive methods. Later on, Buchberger's Algorithm [6, Theorem 15.9] for computing Gröbner Bases in $F[\overrightarrow{X}]$ yielded a constructive (computable) argument for the Hilbert Basis Theorem using the well-foundedness of the ordinal $\mathbb{N}^{\mathbb{N}}$. After Buchberger's results, Simpson [12] showed that, in the context of Reverse Mathematics and subsystems of Second-Order Arithmetic (see [13, 5] for more details), the Hilbert Basis Theorem for $F[\overrightarrow{X}]$ is logically equivalent to the First-Order statement asserting the well-ordering of $\mathbb{N}^{\mathbb{N}}$. The main aim of this article is to:

1. introduce a combinatorial principle called MDC, that assserts the existence of infinite monomial division chains in any infinite sequence of monomials, and is employed in the standard proof of the Hilbert Basis Theorem for finitely generated polynomial rings with coefficients in a given Noetherian ring,
2. catalog the relationship between MDC and other combinatorial principles previously studied in the context of Reverse Mathematics, and finally
3. give two different proofs of MDC from two incomparable axiom systems in the context of Reverse Mathemaics.

In particular, we will show that the strength of MDC is strictly stronger than the one for polynomial rings over fields characterized by Simpson in [12]. Moreover, in addition to classifying its strength in the context of Reverse Mathematics and subsystems of Second-Order Arithmetic, we will show (see Section 2.3 below for more details) exactly how this principle is related to (i.e. yields) the Hilbert Basis Theorem in the context of polynomial rings with coefficients in a given Noetherian ring R possessing a (generalized) division algorithm that effectively determines when a given ring element is in the ideal generated by finitely many elements. A final open question asks whether MDC is *necessary* to prove this version of the Hilbert Basis Theorem. Along the way we observe that, under the assumption that $\mathbb{N}^{\mathbb{N}}$ is well-ordered, monomials under the division relation form well-quasi-orderings. Moreover, a consequence of our main result characterizing MDC shows that it is equivalent to a combinatorial principle for well-quasi-orderings called wqo(set) introduced and studied by Cholak, Marcone, and Solomon in [2].

[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.

2 Preliminaries

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.

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 [5] 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 [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 $a_0, a_1, \ldots, a_n \in R$, $n \in \mathbb{N}$, define

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

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

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

If R is a ring, then its *division algorithm* is the relation

$$x \in \langle a_0, a_1, \ldots, a_N \rangle_R,$$

$N \in \mathbb{N}$, $x, a_0, a_1, \ldots, a_N \in R$. Finally, recall that the Hilbert Basis Theorem (HBT) says that, for each ring R and $n \in \mathbb{N}$, the polynomial ring

$$R[\overrightarrow{X}] = R[X_0, X_1, \ldots, X_n]$$

is Noetherian whenever R is Noetherian.

2.1 Reverse Mathematics

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 [14, Chapter 4] or [5, 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 [13, Chapter II] or [5, 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.

$\mathsf{B\Sigma_2}$ and the Infinite Pigeonhole Principle There is another logical 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.

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 [12, 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 HBT for polynomial rings of the form

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

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 [6, Chapter 15] for computing Gröbner Bases via multivariate polynomial division in $\mathsf{RCA_0}$. One consequence of Simpson's result is that, over $\mathsf{RCA_0}$, $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ proves that if

$$Z_0, Z_1, \ldots, Z_k, \ldots,\ k \in \mathbb{N},$$

is an infinite sequence of $\overrightarrow{X}-$monomials, then for some $k \neq \ell$, $k, \ell \in \mathbb{N}$, we have that Z_k divides Z_ℓ. We will use this fact later on to show that $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ along with the Chain-Antichain Principle for infinite partial orders implies MDC over $\mathsf{RCA_0}$.

2.2 Preliminary Combinatorics related to MDC

We begin this section by formally stating MDC, the combinatorial principle whose proof-theoretic strength the following section examines in detail.

Theorem 1 (MDC). *Fix a finite set of indeterminates $\overrightarrow{X} = \{X_0, X_1, \ldots, X_N\}$, $N \in \mathbb{N}$, and suppose that*

$$Z_0, Z_1, Z_2, \ldots, Z_k, \ldots,\ k \in \mathbb{N},$$

is an infinite sequence of $\overrightarrow{X}-$monomials of strictly increasing degree. Then there is a subsequence of natural numbers

$$k_0 < k_1 < k_2 < \cdots < k_n < \cdots,\ n, k_n \in \mathbb{N},$$

such that

$$Z_{k_n} \mid Z_{k_{n+1}}$$

for all $n \in \mathbb{N}$.

We call $\{Z_{n_k}\}_{n \in \mathbb{N}}$ a monomial division chain *(for $\{Z_k\}_{k \in \mathbb{N}}$).*

Monomials under the division relation form a Well-Partial-Order, which is also a Well-Quasi-Order

Definition 1. *A partial order is a pair $\mathcal{P} = (P, \leq_P)$ such that $P \subseteq \mathbb{N}$ and $\leq_P$ is a binary reflexive antisymmetric and transitive relation on P.*

Definition 2. *A quasi-order is a pair $\mathcal{Q} = (Q, \leq_Q)$ such that $Q \subseteq \mathbb{N}$ and $\leq_Q$ is a binary reflexive transitive relation on Q.*

It is trivial to see that every partial order is a quasi-order.

Definition 3. *A partial order $\mathcal{P} = (P, \leq_P)$ is a* well partial order *(WPO) if for each function $f : \mathbb{N} \to P$ we have that $f(n) \leq_P f(m)$ for some $n \leq_{\mathbb{N}} m$.*

A quasi-order $\mathcal{Q} = (Q, \leq_Q)$ is a well-quasi-order *(WQO) if for each function $f : \mathbb{N} \to Q$ we have that $f(n) \leq_Q f(m)$ for some $n \leq_{\mathbb{N}} m$.*

It is trivial to see that every well partial order is a well-quasi-order. Therefore, every claim about all well-quasi-orders is also true for all well partial orders.

Remark 1. Let $\overrightarrow{X} = \{X_0, X_1, \ldots, X_N\}$, $N \in \mathbb{N}$, be a finite set of indeterminates generating the monomial set M, and let $\leq_M$ denote the binary division relation such that for all $m_1, m_2 \in M$, we have that $m_1 \leq_M m_2$ if and only if m_1 divides m_2. Then it follows that

$$\mathcal{M} = (M, \leq_M)$$

is both a partial order and a quasi-order. Moreover, Simpson [12] has shown that, under the assumption of $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$, $\mathcal{M}$ is a WPO and WQO. Thus, any statement pertaining to all WQOs is also true of $\mathcal{M}$.

We now give two proofs of MDC that we will eventually make use of in the following section that proves our main results. The first proof of MDC is essentially [2, Lemma 3.4], which says that the Chain-Antichain Principle for infinite partial orders (CAC) implies that every infinite WQO has an infinite nondescending sequence of elements; the reader can consult [8] for more details on the computational aspects of this interesting combinatorial principle that is implied by the Ramsey's Theorem for pairs. Our second proof of MDC is more direct and follows from the relatively benign axiom that is $\mathsf{RCA}_0 + \mathsf{I}\Sigma_2$. More specifically, our second proof of MDC uses the Σ_2-induction axiom $\mathsf{I}\Sigma_2$ in its RCA_0-equivalent form of Π^0_2-comprehension for finite (i.e. bounded) sets.

Definition 4. *Let $\mathcal{P} = (P, \leq_P)$ be a parial order with universe P and order relation $\leq_P$, and let $X \subseteq P$. We call X a* chain *if for any $x, y \in P$ we have that either $x \leq_P y$ or $y <_P x$. On the other hand, we say that X is an* antichain *if for any $x, y \in X$, neither $x \leq_P y$ nor $y \leq_P x$ whenever $x \neq y$.*

Note that there is an infinite partial order that is neither a chain nor an antichain.

Theorem 2 (Chain-Antichain Theorem for Infinite Partial Orders (CAC)). *Let $\mathcal{P} = (\mathbb{N}, \leq_P)$ be an infinite partial order. Then there is an infinite $X \subseteq \mathbb{N}$ such that the partial (sub)order $\mathcal{X} = (X, <_X)$, where $<_X$ is the restriction of $<_P$ to X, is either a chain or an antichain.*

Proof (First proof of Theorem 1; [2, Lemma 3.4]). Let $\overrightarrow{X} = \{X_0, X_1, \ldots, X_N\}$, $N \in \mathbb{N}$, be given, and let $\{Z_k\}_{k \in \mathbb{N}}$ be an infinite sequence of $\overrightarrow{X}-$monomials of strictly increasing degree. Define a partial order $\mathcal{P} = (\mathbb{N}, <_P)$ via

$$k <_P \ell, \quad \text{whenever} \quad Z_k \,|\, Z_\ell.$$

Now, CAC says that $\mathcal{P}$ contains an infinite suborder $\mathcal{X} = (X, <_X)$ that is either a chain or an antichain. However, Buchberger's Algorithm for computing Gröbner Bases [6, Chapter 15], which follows from $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ (see [13, Section 3] for more details), implies that in any infinite sequence of monomials there exist two monomials one of which divides the other. This excludes the possibility that $\mathcal{X}$ is an antichain, and so $\mathcal{X}$ is a chain and (by our construction of $<_X$) we have that

$$Z_x \,|\, Z_y$$

for any $x, y \in X$, $x < y$. In other words X corresponds to an infinite monomial division chain of $\{Z_k\}_{k \in \mathbb{N}}$.

Proof (Second proof of Theorem 1). First note that, since $|\overrightarrow{X}| = N+1$ it has $2^{N+1}-$many subsets. We identify each indeterminate $X \in \overrightarrow{X}$ with its index, essentially identifying $\overrightarrow{X}$ with $N+1 \subset \mathbb{N}$, and, as we previously discussed, every $\overrightarrow{X}-$monomial m can be identified with a finite sequence of natural numbers

$$Z_k \sim \langle \alpha_{0,k}, \alpha_{1,k}, \ldots, \alpha_{N,k} \rangle \in \mathbb{N}^N, \text{ where } Z_k = \prod_{i=0}^{N} X_i^{\alpha_{i,k}}.$$

Now (via $\mathsf{I}\mathbf{\Sigma}_2$ in the guise of Bounded $\mathit{\Pi}_2-$Comprehension) let $I \subseteq \mathcal{P}(N+1)$ be defined as follows:

$$I = \{S \subseteq N+1 : (\forall n)(\exists k)(\forall i \in S)[\alpha_{i,k} \geq n]\}.$$

In other words I contains those subsets $S \subseteq \overrightarrow{X}$ for which there exist infinitely many numbers $k \in \mathbb{N}$ such that the coordinates (exponents) of those (indeterminate) indices in S strictly increase, uniformly in k. Moreover, since $\deg(Z_k) > k$, by the Infinite Pigeonhole Principle it follows that there exists an indeterminate index $i \in N+1$ with a corresponding infinite strictly increasing sequence of natural numbers $\{k_n\}_{n\in\mathbb{N}}$ such that for each $n \in \mathbb{N}$ we have that

$$\alpha_{i,k_n} \geq n.$$

Thus, I contains some nonempty element $\{i\} \subseteq \overrightarrow{X}$.

Let $Y \in I$, $Y \subseteq N+1$, be maximal with respect to inclusion. By our construction of I there is an infinite strictly increasing sequence $\{k_n\}_{n\in\mathbb{N}}$ such that for each n,

$$\alpha_{y,k_n} \geq n, \ y \in Y,$$

and by the maximality of $Y \in I$, for each $i \in (N+1) \setminus Y$ there exists $\alpha_i \in \mathbb{N}$ such that

$$\alpha_{i,k_n} \leq \alpha_i, \ n \in \mathbb{N}.$$

Now, since $Y \subset N+1$ is finite, by $\mathsf{B}\mathbf{\Sigma}_2$ there exists an exponent $\alpha \in \mathbb{N}$ such that for each $i \in (N+1) \setminus Y$ and $n \in \mathbb{N}$ we have that

$$\alpha_{i,k_n} \leq \alpha.$$

Furthermore, via the Infinite Pigeonhole Principle applied to "monomial pigeons" Z_{k_n}, $n \in \mathbb{N}$, and pigeonholes made up of the finitely many $\alpha-$bounded sequences of (natural numbers) exponents corresponding to indeterminate indices in $(N+1) \setminus Y$ appearing in Z_{k_n}, we can assume that α_{i,k_n} is independent of $n \in \mathbb{N}$ (i.e. constant), for each $i \in (N+1) \setminus Y$. Finally, it follows from our construction of I and the fact that $Y \in I$, that for each $n \in \mathbb{N}$ and $i \in N+1$ we can refine $\{k_n\}_{n\in\mathbb{N}}$ by taking an infinite computable subsequence if required so that without any loss of generality the following two conditions are satisfied:

- $\alpha_{i,k_n} < \alpha_{i,k_{n+1}}$ when $i \in Y$, and
- $\alpha_{i,k_n} = \alpha_{i,k_{n+1}}$ when $i \notin Y$,

from which it follows that the $\{Z_{k_n}\}_{n\in\mathbb{N}}$ are an infinite monomial division chain.

2.3 The significance of monomial division chains in the context of the Hilbert Basis Theorem

We show the signficance of MDC by revealing its role in the standard proof of the Hilbert Basis Theorem first espoused by Hilbert, and now found throughout the field. Recall that the Hilbert Basis Theorem [4, Section 9.6, Theorems 21 & 22] says that if R is a Noetherian ring, $N \in \mathbb{N}$, and $\overrightarrow{X} = \{X_0, X_1, \ldots, X_N\}$, then the polynomial ring

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

in the indeterminates $\overrightarrow{X}$ with coefficients in R is also Noetherian. This is equivalent to saying that R is not Noetherian whenever $R[\overrightarrow{X}]$ is not a Noetherian ring, or that R contains an infinite strictly ascending chain of ideals whenever $R[\overrightarrow{X}]$ contains such a chain. We prove this via MDC in the following paragraphs. Before that, however, recall that we can linearly (well) order the $\overrightarrow{X}-$monomials based on the lexicographic ordering on exponents, and this gives rise to the notion of the *leading monomial* and corresponding *leading coefficient* of any nonzero $R[\overrightarrow{X}]-$polynomial.

Let $\{I_k\}_{k\in\mathbb{N}}$ be an infinite strictly ascending chain of ideals in $R[\overrightarrow{X}]$, and for each $k \in \mathbb{N}$ let $x_k \in I_{k+1} \setminus I_k \subseteq R[\overrightarrow{X}]$. It follows that for each $k \in \mathbb{N}$,

$$x_k \notin \langle x_0, x_1, \ldots, x_{k-1}\rangle_{R[\overrightarrow{X}]} \subseteq I_k.$$

For each $k \in \mathbb{N}$, let $r_k \in R$ be the leading coefficient of x_k, and let m_k be its leading monomial, so that $r_k m_k$ is its *leading summand*. Under the assumption that R possesses a division algorithm we can take for granted that, for each $k \in \mathbb{N}$, we have that

$$r_k m_k \notin \langle r_0 m_0, r_1 m_1, \ldots, r_{k-1} m_{k-1}\rangle_{R[\overrightarrow{X}]}.$$

There are now two cases to consider.

The first case says that $\{\deg(m_k) : k \in \mathbb{N}\}$ is bounded (i.e. finite), then by the Infinite Pigeonhole Principle[2] there is an infinite set of natural numbers $\{k_n\}_{n\in\mathbb{N}}$ such that the monomial $m_{k_n} = m$ does not depend on n. Now, since

$$r_{k_{n+1}} m_{k_{n+1}} \notin \langle r_{k_0} m_{k_0}, r_{k_1} m_{k_1}, \ldots, r_{k_n} m_{k_n}\rangle_{R[\overrightarrow{X}]},$$

or in this case

$$r_{k_{n+1}} m \notin \langle r_{k_0} m, r_{k_1} m, \ldots, r_{k_n} m\rangle_{R[\overrightarrow{X}]},$$

it follows that

$$r_{k_{n+1}} \notin \langle r_{k_0}, r_{k_1}, \ldots, r_{k_n}\rangle_R,$$

for each $n \in \mathbb{N}$, and so the ideals

$$J_n = \langle r_{k_0}, r_{k_1}, \ldots, r_{k_n}\rangle_R,\ n \in \mathbb{N},$$

form an infinite strictly ascending $R-$chain.

The second case says that $\{\deg(m_k) : k \in \mathbb{N}\}$ is unbounded. In this case there is an infinite subsequence of $\{m_k\}_{k\in\mathbb{N}}$ of strictly increasing degree. Furthermore we can apply MDC to this subsequence to obtain an infinite sequence of natural numbers $\{k_n\}_{n\in\mathbb{N}}$ such that $\{m_{k_n}\}_{n\in\mathbb{N}}$ is an infinite division chain of $\overrightarrow{X}-$monomials, i.e. we have that

$$m_{k_a} \,|\, m_{k_b}$$

for all $a, b \in \mathbb{N}$, $a < b$. Similar to the previous paragraph, since

$$r_{k_{n+1}} m_{k_{n+1}} \notin \langle r_{k_0} m_{k_0}, r_{k_1} m_{k_1}, \ldots, r_{k_n} m_{k_n}\rangle_{R[\overrightarrow{X}]},$$

and

$$m_{k_0}, m_{k_1}, \ldots, m_{k_n} \,|\, m_{k_{n+1}},$$

it follows that

$$r_{k_{n+1}} \notin \langle r_{k_0}, r_{k_1}, \ldots, r_{k_n}\rangle_R$$

for each $n \in \mathbb{N}$, and so

$$J_n = \langle r_{k_0}, r_{k_1}, \ldots, r_{k_n}\rangle_R$$

forms an infinite strictly ascending $R-$chain.

3 Our main results: Two different proofs of MDC over $\mathsf{RCA_0}$ via two incomparable subsystems of Second-Order Arithmetic

Theorem 3 ($\mathsf{RCA_0} + \mathsf{I\Sigma_2}$)**.** ($\mathsf{MDC}$) *Fix a finite set of indeterminates $\overrightarrow{X} = \{X_0, X_1, \ldots, X_N\}$, $N \in \mathbb{N}$, and suppose that*

$$Z_0, Z_1, Z_2, \ldots, Z_k, \ldots,\ k \in \mathbb{N},$$

is an infinite sequence of $\overrightarrow{X}-$monomials of strictly increasing degree. Then there subsequence of natural numbers

$$n_0 < n_1 < n_2 < \cdots < n_k < \cdots,\ k, n_k \in \mathbb{N},$$

such that

$$Z_{n_k} \,|\, Z_{n_{k+1}}$$

for all $k \in \mathbb{N}$.

[2] Later on we will show that MDC implies $\mathsf{B\Sigma_2}$ over $\mathsf{RCA_0}$. Therefore, our use of the Infinite Pigeonhole Principle can be thought of as an implicit utilization of MDC.

Proof. The reader can verify that our second proof of Theorem 1 in the previous section utilizes

- Bounded Π^0_2-Comprehension (equivalent to $\mathsf{I}\Sigma_2$);
- $\mathsf{B}\Sigma_2$ (which follows from $\mathsf{I}\Sigma_2$); and
- the Infinite Pigeonhole Principle (equivalent to $\mathsf{B}\Sigma_2$ which follows from $\mathsf{I}\Sigma_2$);

and is therefore valid in $\mathsf{RCA}_0 + \mathsf{I}\Sigma_2$.

The following theorem is a consequence of [2, Lemma 3.20], which is a more general statement regarding WQOs. The proof given there is essentially the same as the one that follows here.

Theorem 4 (RCA_0)**.** MDC *implies* $\mathsf{B}\Sigma_2$.

Proof. Assume that $\mathsf{B}\Sigma_2$ fails via finitely many finite sets

$$A_0, A_1, A_2, \ldots, A_N,\ N \in \mathbb{N},$$

that partition $\mathbb{N}$. Let $R = \mathbb{Q}[\overrightarrow{X}] = \mathbb{Q}[X_0, X_1, \ldots, X_N]$, and define an infinite sequence of $R-$monomials $Z_0, Z_1, Z_2, \ldots, Z_n, \ldots, n \in \mathbb{N}$, via

$$Z_n = X_j^n$$

for the unique $j \in \mathbb{N}$, $0 \leq j \leq N$, such that $n \in A_j$. Since each Z_n is the power of some indeterminate X_j, it follows that

$$Z_k \,|\, Z_\ell$$

only if $k, \ell \in A_j$, and since A_j is finite there cannot exist an infinite monomial division chain.

A proof of the following theorem is also given in [2, Lemma 3.4] in the more general context of WQOs.

Theorem 5 ($\mathsf{RCA}_0 + \mathsf{WO}(\mathbb{N}^{\mathbb{N}})$)**.** CAC *implies* MDC.

Proof. The reader can verify that our first proof of Theorem 1 in the previous section above is valid in $\mathsf{RCA}_0 + \mathsf{CAC} + \mathsf{WO}(\mathbb{N}^{\mathbb{N}})$. Recall that a consequence of [12, Lemma 3.4] is that $\mathsf{RCA}_0 + \mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ can prove that in any infinite sequence of monomials there must exist a pair of monomials one of which divides the other.

The following corollaries summarize our work so far.

Corollary 1 (RCA_0)**.** MDC *is implied by both the arithmetic axiom* $\mathsf{I}\Sigma_2$*, as well as the second-order axiom* $\mathsf{CAC} + \mathsf{WO}(\mathbb{N}^{\mathbb{N}})$.

Corollary 2 (RCA_0)**.** MDC *implies* $\mathsf{B}\Sigma_2$ *and* $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$.

Now, since $\mathsf{I}\Sigma_2$ is an arithmetic axiom system, there are models of RCA_0 in which $\mathsf{I}\Sigma_2$ holds, but CAC does not. On the other hand an eventual consequence of the following theorem is that there exist models of Second-Order Arithmetic in which $\mathsf{CAC} + \mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ is satisfied but $\mathsf{I}\Sigma_2$ is not. In summary, $\mathsf{I}\Sigma_2$ and CAC are incomparable subsystems of Second-Order Arithmetic in which (we have now seen that) MDC holds.

Corollary 3 (RCA_0)**.** *Let* $\mathbb{N}$ *be a model of First-Order Arithemtic in which* $\mathsf{B}\Sigma_2 + \mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ *holds. Then* $\mathbb{N}$ *is the first-order part of a model* $\mathcal{M}$ *of Second-Order Arithmetic in which* WQO *holds.*

Proof. Our second proof of Theorem 1 can be applied in the context of WQOs to show that WQO is implied by $\mathsf{I}\Sigma_2$. Meanwhile, [2, Lemma 3.4] (similar to our first proof of Theorem 1) explains why WQO follows from $\mathsf{CAC} + \mathsf{WO}(\mathbb{N}^{\mathbb{N}})$. Now, a result of Chong, Slaman, and Yang [3, Corollary 5.2] says that any model of $\mathsf{B}\Sigma_2$ can be extended to a model of CAC without changing its first-order part, and hence without changing its arithmetical theory. Thus, if we begin with a model $\mathcal{M}_1$ of $\mathsf{RCA}_0 + \mathsf{B}\Sigma_2 + \mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ with first-order part $\mathbb{N}$, then [3, Corollary 5.2] says that $\mathcal{M}_1$ can be extended to a model $\mathcal{M}_2$ of $\mathsf{RCA}_0 + \mathsf{B}\Sigma_2 + \mathsf{WO}(\mathbb{N}^{\mathbb{N}}) + \mathsf{CAC}$ with first-order part $\mathbb{N}$. Now, via our first proof of Theorem 1 in the previous section which also applies in the more general context of WQOs via [2, Lemma 3.4], it follows that WQO holds in $\mathcal{M}_2$.

Corollary 4 (RCA_0)**.** MDC *and* WQO *are each strictly stronger than either* $\mathsf{B}\Sigma_2$ *or* $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$*, and neither implies* $\mathsf{I}\Sigma_2$.

Proof. In an unpublished manuscript [11] Simpson has shown that $\mathsf{B\Sigma_2}$ and $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ are incomparable over $\mathsf{RCA_0}$, i.e. neither one implies the other and therefore the conjunction $\mathsf{B\Sigma_2}+\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ is strictly stronger than either individual principle $\mathsf{B\Sigma_2}$, $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$. In the same manuscript Simpson also shows that $\mathsf{B\Sigma_2}+\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ is strictly weaker than (i.e. does not prove) $\mathsf{I\Sigma_2}$.[3]

If we let $\mathbb{N}$ be a model of First-Order Arithmetic in which $\mathsf{B\Sigma_2}+\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ holds but $\mathsf{I\Sigma_2}$ does not, then Corollary 3 above says that $\mathbb{N}$ can be extended to a model of Second-Order Arithemtic $\mathcal{M}$ in which $\mathsf{CAC}+\mathsf{B\Sigma_2}+\mathsf{WO}(\mathbb{N}^{\mathbb{N}})+\neg\mathsf{I\Sigma_2}$ holds, and Theorems 3 and 5 above say that WQO (and hence MDC) is valid in $\mathcal{M}$. Therefore, $\mathcal{M}$ witnesses the fact that WQO and MDC do not imply $\mathsf{I\Sigma_2}$.

4 Avenues for further research

Our results here suggest the following two avenues of further research, one of which pertains to MDC, and another pertaining to HBT which we have not directly addressed here other than our remarks in Section 2.3 above that essentially show how HBT for rings that possess division algorithms follows from MDC over $\mathsf{RCA_0}$.

4.1 Problem 1: characterizing MDC over $\mathsf{RCA_0}$

In general we desire characterizations of MDC and WQO over $\mathsf{RCA_0}$.

Question 1 ($\mathsf{RCA_0}$). Is MDC equivalent to WQO? Or are there models of $\mathsf{MDC}+\neg\mathsf{WQO}$?

In the previous section we showed that our two proofs of Theorem 1 above are indeed different. More precisely our results show that WQO and MDC are each

- implied by $(\mathsf{CAC}+\mathsf{WO}(\mathbb{N}^{\mathbb{N}}))\wedge\mathsf{I\Sigma_2}$, and
- imply $\mathsf{B\Sigma_2}+\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$,

and thus raises the following question.

Question 2 ($\mathsf{RCA_0}$). Characterize the strengths of WQO and MDC by showing, for each principle, that it is either

- equivalent to $(\mathsf{CAC}+\mathsf{WO}(\mathbb{N}^{\mathbb{N}}))\wedge\mathsf{I\Sigma_2}$, or
- equivalent to $\mathsf{B\Sigma_2}+\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$, or else
- strictly between these upper and lower bounds.

Remark 2. Establising the first item would essentially involve a proof of CAC via $\mathsf{RCA_0}+\mathsf{WQO}+\neg\mathsf{I\Sigma_2}$, which would be interesting to see.

4.2 Problem 2: characterizing HBT over $\mathsf{RCA_0}$

Recall that HBT denotes the Hilbert Basis Theorem which says that for each $n\in\mathbb{N}$ and Noetherian ring R with a division algorithm, the polynomial ring $R[\vec{X}]=R[X_0,X_1,\ldots,X_N]$ is Noetherian.

Our analysis of MDC here is motivated by HBT because MDC plays the key role in every known proof of HBT. However, we do not yet know the exact reverse mathematical strength of HBT over $\mathsf{RCA_0}$, and therefore cannot say definitively whether or not MDC is an essential assumption in the proof of HBT. Simpson [12] has shows that HBT implies $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$, and our remarks in Subsection 2.3 above can be formalized in Second-Order Arithmetic to show that HBT follows from MDC over $\mathsf{RCA_0}$.

Theorem 6 ($\mathsf{RCA_0}$). HBT *implies* $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$*, and is implied by* $\mathsf{CAC}+\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ *(*MDC*).*

However, Simpson [11] has shown that $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ is not equivalent to $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})+\mathsf{B\Sigma_2}$, and thus the exact strength of HBT remains open.

Question 3. What is the exact strength of HBT over $\mathsf{RCA_0}$? Is HBT equivalent to $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$? Is it equivalent to $\mathsf{B\Sigma_2}+\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$? Or is it strictly in between?

Remark 3. It is interesting to note that a proof of HBT via $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})$ would require novel algebraic methods that do not filter through MDC. On the other hand, if HBT is equivalent to $\mathsf{WO}(\mathbb{N}^{\mathbb{N}})+\mathsf{B\Sigma_2}$ that would imply that MDC is necessary to prove HBT (as suggested thus far by empirical evidence).

[3] The results referred to in this paragraph were probably known prior to [11]; they are referred to diagrammatically in [9, page 69].

References

1. M.F. Atiyah and I.G. MacDonald. *Introduction to Commutative Algebra*. Perseus, 1969.
2. P. A. Cholak, A. Marcone, and D. R. Solomon. Reverse mathematics and the equivalence of definitions for well and better quasi-orders. *J. Symbolic Logic*, 69(3):683–712, 2004.
3. 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.
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. D. Hilbert. Über die theorie der algebraischen formen. *Mathematische Annalen*, 36(4):473–534, 1890.
8. D.R. Hirschfeldt and R.A. Shore. Combinatorial principles weaker than Ramsey's theorem for pairs. *Journal of Symbolic Logic*, 71:171–206, 2007.
9. P. Hájek and P. Pudlák. *The Metamathematics of First-Order Arithmetic*. Cambridge University Press, 2016.
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.