# An algorithmic approach to the existence of ideal objects in commutative algebra *

Thomas Powell[1], Peter Schuster[2], and Franziskus Wiesnet[3]

[1] Technische Universität Darmstadt
[2] University of Verona
[3] University of Trento

**Abstract.** The existence of ideal objects, such as maximal ideals in nonzero rings, plays a crucial role in commutative algebra. These are typically justified using Zorn's lemma, and thus pose a challenge from a computational point of view. Giving a constructive meaning to ideal objects is a problem which dates back to Hilbert's program, and today is still a central theme in the area of dynamical algebra, which focuses on the elimination of ideal objects via syntactic methods. In this paper, we take an alternative approach based on Kreisel's no counterexample interpretation and sequential algorithms. We first give a computational interpretation to an abstract maximality principle in the countable setting via an intuitive, state based algorithm. We then carry out a concrete case study, in which we give an algorithmic account of the result that in any commutative ring, the intersection of all prime ideals is contained in its nilradical.

**Keywords:** Proof theory · Program extraction · Commutative algebra · No-counterexample interpretation.

## 1 Introduction

This paper is an application of proof theory in commutative algebra. To be more precise, we use proof theoretic methods to give a computational interpretation to a general maximality principle (Theorem 1), which in particular implies the existence of maximal ideals in commutative rings (Krull's lemma). In the context of second order arithmetic, the latter statement is equivalent to arithmetical comprehension [41, Chapter III.5], and thus Theorem 1 is a genuinely strong principle, and highly non-trivial from a computational perspective.

The extraction of programs from proofs has a long and rich history, dating back to Kreisel's pioneering work on the 'unwinding' of proofs [17, 18]. In the ensuing decades, the application of proof interpretations in particular has become

* The first, second and third author were supported by the German Science Foundation (DFG Project KO 1737/6-1); by the John Templeton Foundation (ID 60842) and by a Marie Skłodowska-Curie fellowship of the Istituto Nazionale di Alta Matematica, respectively. The opinions expressed in this paper are those of the authors and do not necessarily reflect the views of the John Templeton Foundation.

a major topic in proof theory, and today encompasses both *proof mining* [12–14], which focuses on obtaining quantitative information primarily from proofs in areas of mathematical analysis, and the mechanized synthesis of programs from proofs, which has found many concrete applications in discrete mathematics and computer science [3, 4, 40].

Though as far back as the 1950s Kreisel already discusses the use of proof theoretic techniques to extract quantitative information from proofs in abstract algebra [19], specifically Hilbert's 17th problem together with his *Nullstellensatz*, to date there are comparatively few formal applications of proof interpretations in algebra, the computational analysis of which is done largely on a case by case basis. This typically involves replacing *semantic* conservation theorems with appropriate *syntactic* counterparts both sufficient for proofs of elementary statements and provable by elementary means. This method has proved possible in numerous different settings [5, 6, 21, 22, 34, 44], and in the context of *commutative* algebra the so-called dynamical method is especially dominant [7, 20, 45, 46].[4] In dynamical algebra one deals with a supposed ideal object (such as a maximal ideal) only by means of concrete, finitary approximations (such as finitely generated ideals, or rather the finite sets of generators), where the latter provide partial but sufficiently complete information about the former.

Interestingly, the idea of replacing ideal objects with suitable finitary approximations is already implicit in Kreisel's unwinding program, and is captured by his famous no-counterexample interpretation (n.c.i.). The n.c.i. plays an important role in proof mining, where in particular it corresponds to the notion of *metastability* [11, 15, 16], which has been made popular by Tao [43] and more recently has featured in higher order computability theory [35].

In this article, we take a new approach to eliminating ideal objects in abstract algebra, by solving an appropriate metastable reformulation of our general maximality principle. We then use this solution to extract *direct witnesses* from a variant of Krull's lemma.

The novelty of our approach lies not just in our use of the n.c.i., but in our description of its solution as a state based algorithm, inspired by recent work of the first author [23, 24, 26–28] which focuses on the algorithmic meaning of extracted programs. This form of presentation allows us to bridge the gap between the *rigorous* extraction of programs from proofs as terms in some formal calculus, and the more algorithmic style of dynamical algebra.

It also enables us to present our results in an entirely self-contained manner, without needing to introduce any heavy proof theoretic machinery. Though behind the scenes at least, aspects of our work are influenced by Gödel's functional interpretation [8] and Spector's bar recursion [42], neither of these make an official appearance, and we have endeavoured to make everything as accessible to the non-specialist as possible.

Our first main contribution, given as Theorems 3 and 4, is a time sequential algorithm (in the sense of Gurevich [9]), whose states evolve step by step until

[4] The second author has contributed to a universal conservation criterion [31–33] that includes many of the those cases [30, 36, 39].

they terminate in some final state $s_j$ which represents a solution to the n.c.i. of Theorem 1. Each step in this process represents an *improvement* to our construction of an approximate ideal object, and so can also be viewed as a learning procedure in the style of [1].

We then present a concrete application of our abstract result, in which we analyse a classic maximality argument used to prove the well known fact that in any commutative ring, if some element $r$ is contained in intersection of all prime ideals, then it must be nilpotent. We show that an instance of our sequential algorithm can be used to directly compute an exponent $e > 0$ such that $r^e = 0$, and thus our case study is another illustration of how the proof theoretic analysis of a highly nonconstructive proof can yield direct, computational information. We conclude by instantiating our algorithm in case of nonconstant coefficients of invertible polynomials. This is a well known example which has been widely studied from a computational perspective [25, 29, 37, 38], thus facilitating a future analysis of our work with other approaches.

## 2 A general maximality argument

We begin by presenting our abstract maximality principle, which forms the main subject of the paper. Let $X$ be some set (which for now is arbitrary but later will be countable), and denote by $\mathcal{P}_{fin}(X)$ the set of all finite subsets of $X$. Simple lemmas are stated without proof.

**Definition 1.** *Let $\triangleright$ be some subset of $\mathcal{P}_{fin}(X) \times X$. We treat $\triangleright$ as a binary relation and say that the element $x$ is generated by the finite set $A$ whenever $A \triangleright x$. We extend $\triangleright$ to arbitrary (not necessarily finite) $S \subseteq X$ by defining $S \triangleright^* x$ whenever there exists some finite $A \subseteq S$ such that $A \triangleright x$.*

**Definition 2.** *Given some $S \subseteq X$, define the sequence $(S_i)_{i\in\mathbb{N}}$ of sets by*

$$S_0 := S \quad \text{and} \quad S_{i+1} := \{x \mid \bigcup_{j\leq i} S_j \triangleright^* x\}$$

*and let $\langle S\rangle := \bigcup_{i\in\mathbb{N}} S_i$. We say that $\langle S\rangle$ is the closure of $S$ w.r.t. $\triangleright$, since whenever $\langle S\rangle \triangleright^* x$ then $x \in \langle S\rangle$.*

**Definition 3.** *For any $S \subseteq X$ and $x \in X$, $S \oplus x := \langle S \cup \{x\}\rangle$ denotes the closed extension of $S$ with $x$.*

**Lemma 1.** *Suppose that $S \triangleright^* x$. Then $S \oplus x = \langle S\rangle$.*

**Definition 4.** *Let $Q(x)$ be some predicate on $X$. For $S \subseteq X$ write $Q(S)$ for $(\forall x \in S)Q(x)$. Note in particular that $Q(S)$ and $S \supseteq T$ implies $Q(T)$.*

**Definition 5.** *We say that $M \subseteq X$ is maximal w.r.t. $\triangleright$ and $Q$ if*

*(i) $M$ is closed w.r.t. $\triangleright^*$,*
*(ii) $Q(M)$,*

*(iii)* $\neg Q(M \oplus x)$ *for any* $x \notin M$.

**Theorem 1.** *Suppose that* $Q(\langle\emptyset\rangle)$. *Then there exists some* $M \subseteq X$ *which is maximal w.r.t.* $\rhd$ *and* $Q$.

*Proof.* Define $\mathcal{S} := \{S \subseteq X \mid S \text{ is closed w.r.t } \rhd^* \text{ and } Q(S)\}$. We show that $\mathcal{S}$ is nonempty and chain complete w.r.t. set inclusion. Nonemptyness follows from the fact that $\langle\emptyset\rangle \in \mathcal{S}$, so it remains to prove chain completeness. Let $\gamma$ be a chain in $\mathcal{S}$. Then $\hat{S} := \bigcup_{S\in\gamma} S$ is clearly closed, and moreover, if $x \in \hat{S}$ then $x \in S$ for some $S \in \gamma$, and therefore $Q(x)$. This establishes $\hat{S} \in \mathcal{S}$.

Thus by Zorn's lemma, $\mathcal{S}$ has some maximal element $M$, which by definition satisfies (i) and (ii). But for $x \notin M$ we have $M \subset M \oplus x$ and thus $M \oplus x \notin \mathcal{S}$. But since $M \oplus x$ is closed, it follows that $\neg Q(M \oplus x)$.

**Corollary 1.** *Any commutative ring* $X$ *with* $0 \neq 1$ *has a maximal ideal.*

*Proof.* We follow the standard proof. Define $\rhd$ by $A \rhd x$ iff $x = x_1 \cdot a_1 + \ldots + x_k \cdot a_k$ for some $a_1, \ldots, a_k \in A$ and $x_1, \ldots, x_k \in X$. Note that $\emptyset \rhd 0$ by the convention that an empty sum is equal to zero. In addition, define $Q(x) :\equiv (x \neq 1)$. Then $S \subseteq X$ is closed iff it is an ideal, with $Q(S)$ iff $S$ is proper. Now $\langle\emptyset\rangle = \{0\}$ (since $\emptyset \rhd 0$) and if $0 \neq 1$ then $Q(\{0\})$, thus by Theorem 1 there exists some maximal structure $M$. To see that $M$ is a maximal ideal, if there were some $M \subset I \subseteq X$ then we would have $M \subset M \oplus x \subseteq I$ for some $x \notin M$, and by $\neg Q(M \oplus x)$ we would have $1 \in M \oplus x$ and thus $I = X$.

## 3 A logical analysis of Theorem 1

From now on, we assume that $X$ is countable and comes equipped with some explicit enumeration $\{x_n \mid n \in \mathbb{N}\}$. Given some $S \subseteq X$, the initial segment of $S$ of length $n$ is defined by $[S](n) := S \cap \{x_m \mid m < n\}$. Note that $S = \bigcup_{n\in\mathbb{N}} [S](n)$. We define $\mathrm{dom}(S) \subseteq \mathbb{N}$ by $\mathrm{dom}(S) := \{n \in \mathbb{N} \mid x_n \in S\}$.

**Theorem 2.** *Suppose that* $M \subseteq X$ *satisfies*

$$x_n \in M \Leftrightarrow Q([M](n) \oplus x_n) \tag{1}$$

*for all* $n \in \mathbb{N}$. *If* $Q(\langle\emptyset\rangle)$ *then* $M$ *is maximal w.r.t.* $\rhd$ *and* $Q$.

*Proof.* Let $M_n := \langle [M](n)\rangle$. We first observe that $Q(M_n)$ for all $n \in \mathbb{N}$, which follows by induction: For $n = 0$ we have $M_0 = \langle\emptyset\rangle$ and so $Q(M_0)$ is true by assumption. Now supposing that $Q(M_n)$ holds for some $n \in \mathbb{N}$ there are two possibilities: If $Q([M](n) \oplus x_n)$ then $x_n \in M$ and hence $M_{n+1} = \langle [M](n) \cup \{x_n\}\rangle = [M](n) \oplus x_n$, and if $\neg Q([M](n) \oplus x_n)$ then $x_n \notin M$ and hence $M_{n+1} = \langle [M](n)\rangle = M_n$. Either way we have $Q(M_{n+1})$.

We now establish each of the maximality conditions in turn. For closure, suppose that $M \rhd^* x_n$ but $x_n \notin M$, and so by definition $\neg Q([M](n) \oplus x_n)$. Since $M \rhd^* x_n$ we have $[M](k) \rhd^* x_n$ for some $k \in \mathbb{N}$. First, let $k \leq n$. Then

$[M](k) \subseteq [M](n)$ and thus $[M](n) \rhd^* x_n$, which implies that $x_n \in M_n$ and thus by Lemma 1

$$[M](n) \oplus x_n = \langle [M](n) \rangle = M_n.$$

Since $Q(M_n)$ this contradicts $\neg Q([M](n) \oplus x_n)$. But if $n < k$ then $[M](n) \oplus x_n \subseteq [M](k) \oplus x_n$ and thus $\neg Q([M](n) \oplus x_n)$ implies $\neg Q([M](k) \oplus x_n)$. But $[M](k) \rhd^* x_n$ and thus by Lemma 1 again, $[M](k) \oplus x_n = M_k$, contradicting $Q(M_k)$.

That $Q(M)$ holds is straightforward: For if $x_n \in M$ then $x_n \in [M](n+1) \subseteq M_{n+1}$ and thus $Q(x_n)$ follows from $Q(M_{n+1})$. Finally, to show that $\neg Q(M \oplus x_n)$ for $x_n \notin M$, note that $x_n \notin M$ implies $\neg Q([M](n) \oplus x_n)$, and since $[M](n) \oplus x_n \subseteq M \oplus x_n$ the result follows.

The purpose of the above theorem was to give a more syntactic formulation of Theorem 1 in the countable setting: If $Q(\langle \emptyset \rangle)$ then the existence of a some maximal $M \subseteq X$ is implied by the existence of some $M$ satisfying (1). In order to proceed, we will now take a closer look at the structure of (1) and make some restrictions on the logical complexity of certain parameters.

**Lemma 2.** *Suppose that the relation $A \rhd x$ can be encoded as a $\Sigma_1^0$-formula. Then the membership relation $x \in \langle A \rangle$ can also be encoded as a $\Sigma_1^0$-formula.*

*Remark 1.* The reader may assume that we are working in some reasonable base theory, and that formulas can be expressed in the language of Peano arithmetic: Thus a $\Sigma_1^0$-formula is a formula of the form $(\exists y)P(y)$ where $P(y)$ is primitive recursive.

*Proof.* We only sketch the proof, since explicit encodings will be given in the case studies that follow. We have $x \in \langle A \rangle$ iff there exists some finite derivation tree for $x$ whose leaves are elements of $A$ and whose nodes represent instances of $\rhd$. Given that $\rhd$ can be encoded as a $\Sigma_1^0$-formula, it is clear that the existence of a derivation trees can in turn be represented as $\Sigma_1^0$-formula via a suitable encoding.

**Lemma 3.** *Suppose that $Q(x)$ is a $\Pi_1^0$-formula and that $A \rhd x$ can be encoded as a $\Sigma_1^0$-formula. Then $Q(\langle A \rangle)$ is a $\Pi_1^0$-formula i.e. $Q(\langle A \rangle) \Leftrightarrow (\forall p) R_A(p)$ for some decidable predicate $R_A(p)$ on $\mathcal{P}_{fin}(A) \times \mathbb{N}$.*

*Proof.* We can write $Q(x) \Leftrightarrow (\forall e) Q_0(x, e)$ for some decidable $Q_0(x, e)$, and by Lemma 2, $x \in \langle A \rangle \Leftrightarrow (\exists t) G_A(x, t)$ for some decidable $G_A(x, t)$. Then

$$\begin{aligned} Q(\langle A \rangle) &\Leftrightarrow (\forall m)(x_m \in \langle A \rangle \Rightarrow Q(x_m)) \\ &\Leftrightarrow (\forall m)((\exists t) G_A(x_m, t) \Rightarrow (\forall e) Q_0(x_m, e)) \\ &\Leftrightarrow (\forall m, t, e)(G_A(x_m, t) \Rightarrow Q_0(x_m, e)) \end{aligned}$$

and the latter formula can be encoded as $(\forall p) R_A(p)$ for suitable $R_A(p)$ and using some pairing function for the tuple $m, t, e$.

**Lemma 4.** *Under the conditions of Lemma 3, (1) holds iff for all $n \in \mathbb{N}$:*

$$x_n \in M \Leftrightarrow (\forall p) R_{[M](n) \cup \{x_n\}}(p) \tag{2}$$

*Proof.* By Lemma 3 setting $A = [M](n) \cup \{x_n\}$, so that $\langle A \rangle = [M](n) \oplus x_n$.

Written out in full, the existence of some $M$ satisfying (2) becomes

$$(\exists M)(\forall n)((x_n \in M \Rightarrow (\forall p)R_{[M](n)\cup\{x_n\}}(p)) \wedge (x_n \notin M \Rightarrow (\exists q)R_{[M](n)\cup\{x_n\}}(q)))$$

and so written out in Skolem normal form, this becomes

$$(\exists M, f)(\forall n, p)(x_n \in M \Rightarrow R_{[M](n)\cup\{x_n\}}(p) \wedge x_n \notin M \Rightarrow R_{[M](n)\cup\{x_n\}}(f(n))). \tag{3}$$

This motivates our final version of maximality, which is now in a form where we can directly apply the no-counterexample interpretation.

**Definition 6.** *An explicit maximal object w.r.t. $\rhd$ and $Q$ is a set $M \subseteq X$ together with a function $f : \mathrm{dom}(X \backslash M) \to \mathbb{N}$ such that*

- $x_n \in M \Rightarrow R_{[M](n)\cup\{x_n\}}(p)$
- $x_n \notin M \Rightarrow \neg R_{[M](n)\cup\{x_n\}}(f(n))$

*for all $n, p \in \mathbb{N}$.*

The idea here is that the function $f$ provides concrete evidence for why $x_n$ is excluded from the maximal structure $M$: in other words, it encodes an element $x_m$ together with some tree $t$ and $e$ such that $x_m \in [M](n) \oplus x_n$ with respect to $t$ but $Q(x_m)$ fails relative to $e$.

## 4 An approximating algorithm for maximal objects

In general, it is impossible to effectively compute a set $M$ together with an $f$ satisfying Definition 6. However, we demonstrate how an *approximate*, or *metastable*, formulation of maximality in the spirit of Kreisel's no-counterexample interpretation, can be directly witnessed via an intuitive stateful procedure.

For a detailed and modern account of the n.c.i., the reader is encouraged to consult e.g. [10, 13]. The rough idea is the following: Given some prenex formula of the form $A :\equiv (\exists x \in X)(\forall y \in Y)P_0(x, y)$, a functional $\Phi : (X \to Y) \to X$ is said to witness the n.c.i. of $A$ if it witnesses $(\forall \omega : X \to Y)(\exists x)P_0(x, \omega(x))$ i.e. $(\forall \omega)P_0(\Phi\omega, \omega(\Phi\omega))$. This definition generalises in the obvious way to prenex formulas of arbitrary complexity. In this section, we give an algorithmic description of such an $\Phi$ for $A$ being the statement that an explicit maximal object exists, as in Definition 6.

**Definition 7.** *Let $(\omega, \phi)$ be functionals which take as input $M$ and $f$ and each return as output a natural number. An* approximate *explicit maximal object w.r.t $\rhd$, $Q$ and $(\omega, \phi)$ is a set $M \subseteq X$ together with a function $f$ such that*

- $x_n \in M \Rightarrow R_{[M](n)\cup\{x_n\}}(p)$
- $x_n \notin M \Rightarrow \neg R_{[M](n)\cup\{x_n\}}(f(n))$

*but now only for $n \leq \omega(M, f)$ and $p = \phi(M, f)$.*

Note that Definition 7 is slightly stronger than the n.c.i. of (3), since it works for all $n \leq \omega(M, f)$ and not just $n = \omega(M, f)$.

Approximate maximal objects are useful because when a proof of a pure existential statement relies on the existence of some maximal $M$, we are typically able to find functionals $(\omega, \phi)$ which calibrate exactly how this maximal object is used, and thereby construct a witness to the existential statement in terms of an approximate maximal object relative to $(\omega, \phi)$. For a more detailed discussion of this phenomenon in the context of sequential algorithms the reader is directed to [28, Section 4.5]. We will see a concrete example in Section 5.

### 4.1 The algorithm

We now present our algorithm, which computes approximate maximal objects given some input functionals $(\omega, \phi)$. Our algorithm will be described as an evolving sequence of states

$$s_0 \mapsto s_1 \mapsto \cdots \mapsto s_k.$$

The basic idea is as follows: We start in some initial state $s_0$ which contains no information and gives rise to an 'empty' approximation. In each step of the computation we query our mathematical environment to asses whether or not our current approximation is good enough. If it is, the computation terminates in that state. If not, we use the information gained from this query to *improve* our approximation. The hope is that our algorithm always terminates on some reasonable set of inputs. In this section we describe how the states evolve, and in the next we deal with termination.

For us, states $s_i$ are defined to be a functions of type $\mathbb{N} \to \{(*)\} + \mathbb{N}$ i.e. $s_i$ is an array, whose $n$th entry $s_i(n)$ is either a natural number or some default value $(*)$. Any given state encodes a current approximation $(M[s_i], f[s_i])$ to an explicit maximal object by defining the set $M[s_i] \subseteq X$ as

$$M[s_i] := \{x_n \in \mathbb{N} \mid s_i(n) = (*)\}$$

and the function $f[s_i] : \mathrm{dom}(X \backslash M[s_i]) \to \mathbb{N}$ by

$$f[s_i](n) := s_i(n) \in \mathbb{N}$$

where $s_i(n) \in \mathbb{N}$ follows from the assumption that $n \notin M[s_i]$. Fixing some input functionals $(\omega, \phi)$, we imagine for convenience that these now act directly on states, and write $\omega(s_i)$ as shorthand for $\omega(M[s_i], f[s_i])$.

We now need to explain how our state evolves. As an initial state, we set

$$s_0(m) := (*)$$

and so $M[s_0] = X$ and $f[s_0]$ has an empty domain. Now, supposing that we are in the $i$th state, we define

$$(n_i, p_i) := (\omega, \phi)(s_i).$$

and carry out the following steps:

– Search from 0 up to $n_i$ until some $0 \leq n \leq n_i$ is found such that each of the following hold
  - $x_n \in M[s_i]$,
  - $\neg R_{[M[s_i]](n) \cup \{x_n\}}(p_i)$
– If no such $n$ is found, the algorithm terminates in state $s_i$.
– Otherwise, define

$$s_{i+1}(m) := \begin{cases} s_i(m) & \text{if } m < n \\ p_i & \text{if } m = n \\ (*) & \text{if } m > n \end{cases}$$

and so in particular

$$M[s_{i+1}] = [M[s_i]](n) \cup \{x_k \in \mathbb{N} \mid k > n\}$$

and $x_n \notin M[s_{i+1}]$.

**Lemma 5.** *For all states $s_i \in \mathbb{N}$ and $n \in \mathbb{N}$ we have*

$$x_n \notin M[s_i] \Rightarrow \neg R_{[M[s_i]](n) \cup \{x_n\}}(f[s_i](n)).$$

*Proof.* Induction on $i$. For $i = 0$ the statement is trivially true, since $M[s_0] = X$. So suppose the statement is true for some $i$, and that $x_n \notin M[s_{i+1}]$. Since $M[s_{i+1}] = [M[s_i]](n') \cup \{x_k \in \mathbb{N} \mid k > n'\}$ for some $n' \leq n_i$ there are two possibilities. Either $n < n'$ and $x_n \notin M[s_i]$ and so the result follow by the induction hypothesis since $f[s_{i+1}](n) = s_{i+1}(n) = s_i(n) = f[s_i](n)$ and $[M[s_{i+1}]](n) = [M[s_i]](n)$. Or $n = n'$ and so $f[s_{i+1}(n)] = p_i$ which is defined to satisfy $\neg R_{[M[s_i]](n) \cup \{x_n\}}(p_i)$, and thus the result follows since $[M[s_{i+1}]](n) = [M[s_i]](n)$.

**Theorem 3.** *Suppose that the algorithm terminates in state $s_j$. Then $s_j$ forms an approximate explicit maximal object w.r.t. $\rhd, Q$ and $(\omega, \phi)$.*

*Proof.* If the algorithm terminates, then by definition it holds that for all $n \leq n_j = \omega(s_j)$, if $x_n \in M[s_j]$ then $R_{[M[s_j]](n) \cup \{x_n\}}(p_j)$ where $p_j = \phi(s_j)$. But if $x_n \notin M[s_j]$ then $\neg R_{[M[s_j]](n) \cup \{x_n\}}(f[s_j](n))$ by Lemma 5, and so we're done.

### 4.2 Termination

It remains, then, to show that our algorithm actually terminates on some reasonable set of parameters! Here, we make an additional standard assumption, namely that the functionals $(\omega, \phi)$ are *continuous*.

**Definition 8.** *We say that $(\omega, \phi)$ are continuous if for all states $s : \mathbb{N} \to \{*\} + \mathbb{N}$ (which encode $M, f$) there exists some natural number $L$ such that for any other input state $s'$, if $[s](L) = [s'](L)$ then*

$$(\omega, \phi)(s) = (\omega, \phi)(s').$$

Note that whenever $(\omega, \phi)$ are instantiated by computable functionals, they will automatically be continuous, so restricting ourselves to the continuous setting is entirely reasonable.

**Theorem 4.** *Whenever the algorithm runs on continuous parameters $(\omega, \phi)$, it terminates after a finite number of steps.*

*Proof.* Suppose that the algorithm does not terminate and thus results in an infinite run $\{s_i\}_{i\in\mathbb{N}}$. We first show that for each $n \in \mathbb{N}$, the value of $s_i(n)$ can only change finitely many times as $i \to \infty$. More precisely, we define a sequence $j_0 \leq j_1 \leq j_2 \leq \ldots$ satisfying

$$(\forall i \geq j_n)([s_i](n) = [s_{j_n}](n)). \tag{4}$$

The $(j_n)_{n\in\mathbb{N}}$ are defined inductively as follows: We let $j_0 := 0$, and if $j_n$ has been defined, either there exists some $j \geq j_n$ such that $x_n \notin M[s_j]$, in which case we define $j_{n+1} = j$, or $x_n \in M[s_j]$ for all $j \geq j_n$ and we set $j_{n+1} := j_n$. To see that this construction satisfies (4) we use induction on $n$. The base case is trivial, so let's fix some $n$. By the induction hypothesis and the fact that $j_{n+1} \geq j_n$ we have $[s_i](n) = [s_{j_{n+1}}](n)$ for all $i \geq j_{n+1}$, and so we only need to check point $n$. Now, in the case $x_n \in M[s_i]$ for all $i \geq j_n = j_{n+1}$ we're done since this means that $s_i(n) = (*)$ for all $i \geq j_{n+1}$. In the other case, if $x_n \notin M[s_{j_{n+1}}]$ then $s_{j_{n+1}}(n) = p \in \mathbb{N}$ and observing the manner in which the states evolves at each step, the only way this can change is if $x_m$ is removed from to $s_i$ for some $i \geq j_{n+1}$ and $m < n$. But this contradicts the induction hypothesis.

The second part of the proof is where we make use of continuity. Define $s_\infty$ to be the limit of the $[s_{j_n}](n)$, and let $L$ be a point of continuity for $(\omega, \phi)$ on this input. Define

$$j := j_N \quad \text{for} \quad N := \max\{L, \omega(s_\infty) + 1\}$$

Then in particular, since $[s_\infty](L) = [s_j](L)$ we must have

$$n_j := \omega(s_j) = \omega(s_\infty) < N.$$

But since the algorithm does not terminate, there is some $0 \leq n \leq n_j$ with $x_n \in M[s_j]$ but $x_n \notin M[s_{j+1}]$. But by definition of $j = j_N$, since $n < N$ then $x_n \in M[s_j]$ implies that $x_n \in M[s_i]$ for all $i \geq j$, a contradiction.

## 5 Case study: The nilradical as the intersection of all prime ideals

We now use our algorithm to carry out a computational analysis of the following well known fact [2, Proposition 1.8], which is a frequently used form of Krull's lemma. Recall that a ring element $r$ is nilpotent if $r^e = 0$ for some integer $e > 0$.

**Theorem 5.** *Let $X$ be a countable commutative ring. Suppose that $r$ lies in the intersection of all prime ideals of $X$. Then $r$ is nilpotent.*

We first show how the standard proof follows from our general maximality principle Theorem 1. Now our countable set $X$ comes equipped with a ring structure, which will be used to instantiate our parameters $\rhd$ and $Q$.

*Proof.* Define $\rhd$ as in Corollary 1, but now let $Q(x) := (\forall e)(e > 0 \Rightarrow x \neq r^e)$. Then $S \subseteq X$ is closed w.r.t $\rhd$ and satisfies $Q(S)$ iff it is an ideal which does not contain $r^e$ for any $e > 0$. Suppose for contradiction that $r$ is not nilpotent, which would mean that $Q(\{0\})$ and thus $Q(\langle\emptyset\rangle)$ hold. By Theorem 1 there is some $M$ which is maximal w.r.t. $\rhd$ and $Q$, and in this case $M \oplus x = \langle M \cup \{x\}\rangle$ is just the ideal generated by $M$ and $x$.

Take $x, y \notin M$. Then $\neg Q(M \oplus x)$ and hence there exists some $e_1 > 0$ such that $r^{e_1} \in M \oplus x$. Similarly, there exists some $e_2 > 0$ with $r^{e_2} \in M \oplus y$. But then $r^{e_1+e_2} \in M \oplus xy$ and thus $xy \notin M$. This would mean that $M$ is prime, but then $Q(M)$ contradicts the assumption that $r \in M$.

**Lemma 6.** *For $\rhd$ and $Q$ defined as in the proof of Theorem 5, we have*

$$Q(\langle A\rangle) \Leftrightarrow (\forall b \in X^*, e)(\underbrace{|b| = k \wedge e > 0 \Rightarrow a_1 \cdot b_1 + \ldots + a_k \cdot b_k \neq r^e}_{R_A(b,e)})$$

*where $A := \{a_1, \ldots, a_k\}$, $X^*$ as usual denotes the set of lists over $X$ and $|b|$ is the length of $b$.*

Our aim will be to address the following computational challenge, given any fixed $X$ and $r$,

- **Input.** Evidence that $r$ lies in the intersection of all prime ideals
- **Output.** An exponent $e > 0$ such that $r^e = 0$

The first question is what we take to be evidence that $r$ lies in all prime ideals. Note that this assumption is logically equivalent to the statement

$$(\forall S \subseteq X)(S \text{ is not a prime ideal} \vee r \in S),$$

so for a computational interpretation of the above it would be reasonable to ask for a procedure which takes some $S \subseteq X$ as input, and either confirms that $r \in S$ or demonstrates that $S$ is not a prime ideal.

Let's now fix some enumeration of $X$, where we assume for convenience that $x_0 = 0_X$, $x_1 = 1_X$ and $x_2 = r$. This assumption is not essential, and is there merely to simplify some of the bureaucratic details which follow. From now on we assume that we have some function

$$\psi : \mathcal{P}(X) \to \{0, 1, 2\} + (\{3, 4, 5\} \times \mathbb{N}^3)$$

which for any $S \subseteq X$ satisfies

- $\psi(S) = 0 \Rightarrow 0_X \notin S$
- $\psi(S) = 1 \Rightarrow 1_X \in S$
- $\psi(S) = 2 \Rightarrow r \in S$

- $\psi(S) = (3, i, j, k) \Rightarrow (x_i + x_j = x_k) \wedge (x_i, x_j \in S) \wedge (x_k \notin S)$
- $\psi(S) = (4, i, j, k) \Rightarrow (x_i \cdot x_j = x_k) \wedge (x_i \in S) \wedge (x_k \notin S)$
- $\psi(S) = (5, i, j, k) \Rightarrow (x_i \cdot x_j = x_k) \wedge (x_i, x_j \notin S) \wedge (x_k \in S)$

The functional $\psi$ witnesses the statement that $r \in S$ or $S$ is not a prime ideal.

**Lemma 7.** *Suppose that $M \subseteq X$ and $f$ satisfy*

$$x_n \notin M \Rightarrow \neg R_{[M](n) \cup \{x_n\}}(f_1(n), f_2(n)) \tag{5}$$

*where $R_A(b, e)$ is as in Lemma 6 and if $f(n) = \langle b, e \rangle$ then $f_1(n) = b$ and $f_2(n) = e$. Whenever $\psi(M) \neq 0$ there exists some nonempty $A = \{a_1, \ldots, a_l\} \subseteq M$ together with a sequence $[b_1, \ldots, b_l]$ of elements of $X$ and $e > 0$ such that*

$$a_1 \cdot b_1 + \ldots + a_l \cdot b_l = r^e.$$

*Moreover, $e, A$ and $b$ are computable in $\psi$, $M$ and $f$.*

*Remark 2.* Note that here $\langle b, e \rangle$ denotes the encoding of the pair $b, e$ as a single natural number, so that the type of $f$ matches that of Section 4.

*Proof.* This is a fairly routine case analysis. Since $\psi(M) \neq 0$ there are five remaining possibilities:

- $\psi(M) = 1$, i.e. $x_1 = 1_X \in M$ and so we set $e := 1$, $A := \{x_1\}$ and $b := [x_2]$ (recall that $x_2 = r$).
- $\psi(M) = 2$, i.e. $x_2 = r \in M$ and so $e := 1$, $A := \{x_2\}$ and $b := [x_1]$ work.
- $\psi(M) = (3, i, j, k)$. Since $x_k \notin M$, by (5) for $b' = f_1(k)$ we have
$$x_{\alpha_1} \cdot b'_1 + \ldots + x_{\alpha_p} \cdot b'_p + x_k \cdot b'_{p+1} = r^{f_2(k)}$$
for $\{x_{\alpha_1}, \ldots, x_{\alpha_p}\} = [M](k)$. But then
$$x_{\alpha_1} \cdot b'_1 + \ldots + x_{\alpha_p} \cdot b'_p + (x_i + x_j) \cdot b'_{p+1} = r^{f_2(k)}$$
and so $e := f_2(k)$, together with $A := \{x_{\alpha_1}, \ldots, x_{\alpha_p}, x_i, x_j\} \subseteq M$ and $b := [b'_1, \ldots, b'_p, b'_{p+1}, b'_{p+1}]$ work.
- $\psi(M) = (4, i, j, k)$. Entirely analogously, but this time we have
$$x_{\alpha_1} \cdot b'_1 + \ldots + x_{\alpha_p} \cdot b'_p + x_i \cdot (x_j \cdot b'_{p+1}) = r^{f_2(k)}$$
and so $e := f_2(k)$, $A := \{x_{\alpha_1}, \ldots, x_{\alpha_p}, x_i\}$ and $b := [b'_1, \ldots, b'_p, x_j \cdot b'_{p+1}]$ work.
- $\psi(M) = (5, i, j, k)$. For $b' = f_1(i)$ and $b'' = f_1(j)$ we have $x_{\alpha_1} \cdot b'_1 + \ldots + x_{\alpha_p} \cdot b'_p + x_i \cdot b'_{p+1} = r^{f_2(i)}$ and $x_{\beta_1} \cdot b''_1 + \ldots + x_{\beta_q} \cdot b''_q + x_j \cdot b''_{q+1} = r^{f_2(j)}$ where $\{x_{\alpha_1}, \ldots, x_{\alpha_p}\} = [M](i)$ and $\{x_{\beta_1}, \ldots, x_{\beta_q}\} = [M](j)$, and therefore
$$\begin{aligned}&(x_{\alpha_1} \cdot b'_1 + \ldots + x_{\alpha_p} \cdot b'_p) \cdot r^{f_2(j)} + x_i \cdot b'_{p+1} \cdot (x_{\beta_1} \cdot b''_1 + \ldots + x_{\beta_q} \cdot b''_q) \\ &+ x_i \cdot x_j \cdot b'_{p+1} \cdot b''_{q+1} = r^{f_2(i) + f_2(j)}\end{aligned}$$
and so $e := f_1(i) + f_2(j)$, $A := \{x_{\alpha_1}, \ldots, x_{\alpha_p}, x_{\beta_1}, \ldots, x_{\beta_q}, x_i \cdot x_j\}$ and the corresponding $b$ from the above equation work.

**Lemma 8.** *Suppose that $M$ and $f$ satisfy (5) as in Lemma 7 and that $\psi(M) \neq 0$. Then there exists some $n \in \mathbb{N}$, sequence $b$ and $e > 0$ such that*

- $x_n \in M$,
- $\neg R_{[M](n)\cup\{x_n\}}(b, e)$

*and moreover, $n$, $b$ and $e$ are computable in $\psi$, $M$ and $f$.*

*Proof.* By Lemma 7 there exist, computable in $\psi$, $M$ and $f$, a nonempty $A = \{a_1, \ldots, a_l\} \subseteq M$ together with $b = [b_1, \ldots, b_l]$ and $e > 0$ satisfying $a_1 \cdot b_1 + \ldots + a_l \cdot b_l = r^e$. In particular, we can find some $n \in \mathbb{N}$ which is the maximal with $x_n \in A \subseteq M$, and thus $A \subseteq [M](n) \cup \{x_n\}$. But by expanding $b$ to some sequence $b'$ with zeroes added wherever needed, we have

$$x_{\alpha_1} \cdot b'_1 + \ldots + x_{\alpha_p} \cdot b'_p + x_n \cdot b'_{p+1} = r^e$$

where $\{x_{\alpha_1}, \ldots, x_{\alpha_p}\} = [M](n)$, and thus $\neg R_{[M](n)\cup\{x_n\}}(b', e)$ holds.

**Theorem 6.** *Given an input functional $\psi$ which for any $S$ witnesses that $r \in S$ or $S$ is not a prime ideal, define the functionals $\omega, \phi$ by*

$$(\omega, \phi)(M, f) := \begin{cases} n, \langle b, e\rangle & \text{if } \psi(M) \neq 0, \text{ where } n, b \text{ and } e \text{ satisfy Lemma 8} \\ 0, \langle [], 0\rangle & \text{otherwise} \end{cases}$$

*Suppose that the algorithm $\{s_i\}_{i\in\mathbb{N}}$ described in Section 4.1 is run on $(\omega, \phi)$, and for $R_A(b, e)$ as defined in Lemma 6. Then the algorithm terminates in some final state $s_j$ satisfying*

$$s_j(0)_2 > 0 \wedge r^{s_j(0)_2} = 0_X.$$

*Proof.* First of all, we note that $(\omega, \phi)$ are computable, and so in particular must be continuous in the sense of Definition 8. Therefore the algorithm terminates in some final state $s_j$. By Lemma 5 we have

$$x_n \notin M[s_j] \Rightarrow \neg R_{[M[s_j]](n)\cup\{x_n\}}(f_1[s_j](n), f_2[s_j](n)). \tag{6}$$

We claim that $\psi(M[s_j]) = 0$. If this were not the case, then by Lemma 8 and the definition of $(\omega, \phi)$ we would have $x_{n_j} \in M[s_j]$ and $\neg R_{[M[s_j]](n_j)\cup\{x_{n_j}\}}(b_j, e_j)$ for

$$(n_j, \langle b_j, e_j\rangle) = (\omega, \phi)s_j$$

and so by definition the algorithm cannot be in a final state. This proves the claim. But $\psi(M[s_j]) = 0$ implies that $x_0 = 0_X \notin M[s_j]$, and therefore by (6) we have $\neg R_{\{x_0\}}(b, e)$ where $\langle b, e\rangle = f[s_j](0) = s_j(0)$, which is just

$$|b| = 1 \wedge e > 0 \wedge x_0 \cdot b_0 = r^e.$$

But since $x_0 \cdot b_0 = 0_X \cdot b_0 = 0$ we have $r^e = 0$ i.e. $r^{s_j(0)_2} = 0_X$.

### 5.1 Informal description of the algorithm

The basic idea behind the algorithm in this section is the following.

- Each state $s_i$ encodes some $M[s_i] \subseteq X$, where $x_n \notin M[s_i]$ only if we have found evidence that $[M[s_i]](n) \cup \{x_n\}$ generates $r^e$ for some $e > 0$, in which case this evidence is encoded as $s_i(n) \in \mathbb{N}$.
- We start off at $s_0$ with the full set $M[s_0] = X$.
- At state $s_i$ we interact with our functional $\psi$, which provides us with evidence that either $M[s_i]$ is not a prime ideal, or $r \in M[s_i]$.
- If this evidence takes the form of anything other than $0_X \notin S$, then we are able to use this to find some $x_n \in M$ and evidence that $[M](n) \cup \{x_n\}$ generates $r^e$ for some $e > 0$. We exclude $x_n$ from $M[s_i]$ but add all $x_k$ for all $k > n$ (since now the evidence that $[M[s_i]](k) \cup \{x_k\}$ generates $r^{e'}$ could be falsified by the removal of $x_n$).

Eventually, using a continuity argument as in Theorem 4, the algorithm terminates in some state $s_j$. But the only way this can be is if $\psi(M[s_j]) = 0$, which indicates that $0_X \notin M[s_j]$. Thus $\{0_X\}$ generates $r^e$ for some $e > 0$ encoded in the state.

### 5.2 Example: Nilpotent coefficients of invertible polynomials

We conclude by outlining a simple and very concrete application [2, pp. 10–11] of Theorem 5, and sketching how our algorithm would be implemented in this case. Fixing our countable commutative ring $X$, let $f = \sum_{i=0}^{n} a_i T_i$ be a unit in the polynomial ring $X[T]$. Then each $a_i$ for $i > 0$ is nilpotent.

To prove this, by Theorem 5 it suffices to show that $a_i \in P$ for all prime ideals $P$ of $X$. Let $g \in X[T]$ be such that $fg = 1$, and let $P$ be some arbitrary prime ideal. Then we also have $fg = 1$ in $(X/P)[T]$, but since $P$ is prime, $X/P$ is an integral domain, and thus $0 = \deg(fg) = \deg(f) + \deg(g)$. This implies that $\deg(f) = 0$ in $(X/P)[T]$ and thus $a_i \in P$ for all $i > 0$.

In order to obtain a concrete algorithm, which for any $a_i$ for $i > 0$, produces some $e > 0$ such that $r^e = 0$, we need to analyse the above argument to produce a specific functional $\psi$ which for any $S \subseteq X$, witnesses the statement that either $a_i \in S$ or $S$ is not a prime ideal. Fixing $i > 0$ and $S$, we define $\psi(S)$ via the following algorithm:

- Check in turn whether any of $0 \notin S$, $1 \in S$ or $a_i \in S$ are true. In the first case, return $\psi(S) = 0$, and in the others, $\psi(S) = 1$ and $\psi(S) = 2$ respectively.
- Otherwise, let $g = \sum_{j=0}^{m} b_j T^j \in X[T]$ be such that

$$1 = fg = \sum_{k=0}^{n+m} c_k T^k$$

for $c_k = \sum_{j=0}^{k} a_j b_{k-j}$. Then in particular, for $i > 0$ we have $0 = c_i = \sum_{j=0}^{i-1} a_j b_{i-j} + a_i b_0$ and so (using that $a_0 b_0 = c_0 = 1$):

$$a_i = -a_0 \sum_{j=0}^{i-1} a_j b_{i-j}. \tag{7}$$

There are now two subcases to consider.

- If all of $b_1, \ldots, b_i \in S$, then because $a_i \notin S$, an analysis of the r.h.s. of (7) allows us to find, in a finite number of steps, either some $x_u, x_v \in S$ and $x_w \notin S$ such that $x_w = x_u + x_v$, in which case we return $\psi(S) = (3, u, v, w)$, or some $x_u \in S, x_v$ and $x_w \notin S$ such that $x_w = x_u x_v$, in which case we return $\psi(S) = (4, u, v, w)$.
- Otherwise we have $b_j \notin S$ for some $1 \leq j \leq i$. Take $1 \leq k \leq n$ and $1 \leq l \leq m$ to be the maximal such that $a_k, b_l \notin S$ (note that because $a_i \notin S$ then this maximal $a_k$ also exists) and consider

  $$0 = c_{k+l} = a_k b_l + \sum_{p+q=k+l \wedge (p>k \vee q>l)} a_p b_q.$$

  Then, splitting into two further subcases: Either $a_k b_l \in S$, in which case we return $\psi(S) = (5, u, v, w)$ for $x_u = a_k$, $x_v = b_l$ and $x_w = a_k b_l$, or

  $$-\sum a_p b_q = a_k b_l \notin S$$

  and since for each summand $a_p b_q$ either $a_p \in S$ or $b_q \in S$, an analysis analogous to the previous case returns $\psi(S) = (3, u, v, w)$ or $(4, u, v, w)$ for suitable $u, v, w$.

Therefore, running our algorithm for $\psi$ as defined above results in a sequential algorithm which, by Theorem 6 terminates in some final state $s_j$ with $f[s_j] = \langle b, e \rangle$ for $e > 0$ and $a_i^e = 0$.

*Example 1.* In the very simple case where $X = \mathbb{Z}_4$ and $f = a_0 + a_1 T = 1 + 2T$, the corresponding run our algorithm for $a_1 = 2$ would be as follows;

- $M[s_0] = \mathbb{Z}_4$, and since $1 \in \mathbb{Z}_4$ we are in the first main case of the definition of $\psi$ above, and we have $\psi(\mathbb{Z}_4) = 1$. Therefore we remove 1 from $\mathbb{Z}_4$, citing $1 \cdot 2 = 2^1$ as evidence.
- $M[s_1] = \mathbb{Z}_4 \backslash \{1\}$, and since $a_1 = 2 \in \mathbb{Z}_4 \backslash \{1\}$ we are again in the first main case. Therefore we set $\psi(\mathbb{Z}_4 \backslash \{1\}) = 2$ and remove 2 with evidence $2 \cdot 1 = 2^1$.
- $M[s_2] = \mathbb{Z}_4 \backslash \{1, 2\}$. We now fall into the second main case. Picking $g = b_0 + b_1 T = 1 + 2T$ as our inverse for $f$, since in $\mathbb{Z}_4$:

  $$(1 + 2T)(1 + 2T) = 1,$$

  we have $b_1 = 2 \notin \mathbb{Z}_4 \backslash \{1, 2\}$. This puts us in the second subcase, where we observe that $a_1 = b_1 = 2$ are the maximal coefficients with $a_1, b_1 \notin \mathbb{Z}_4 \backslash \{1, 2\}$. Then $0 = c_2 = a_1 \cdot b_1 \in \mathbb{Z}_4 \backslash \{1, 2\}$, and thus $\psi(\mathbb{Z}_4 \backslash \{1, 2\}) = (5, 2, 2, 0)$, and so we remove 0 with evidence $0 = 2^2$.

– Finally, $M[s_3] = \mathbb{Z}_4\backslash\{0\}$ (since we now re-add both 1 and 2 to the approximation) and $\psi(\mathbb{Z}_4\backslash\{0\}) = 0$, and since we have already stored the evidence that $0 = 2^2$, the algorithm terminates with $e = 2$.

**Acknowledgements.** The authors are grateful to the anonymous referees for their detailed comments, which led to a much improved version of the paper.

## References

1. Aschieri, F., Berardi, S.: Interactive learning-based realizability for Heyting arithmetic with EM1. Logical Methods in Computer Science **6**(3) (2010)
2. Atiyah, M., Macdonald, I.: Introduction to Commutative Algebra. Addison-Wesley Publishing Co. (1969)
3. Berger, U., Lawrence, A., Forsberg, F., Seisenberger, M.: Extracting verified decision procedures: DPLL and resolution. Logical Methods in Computer Science **11**(1:6), 1–18 (2015)
4. Berger, U., Miyamoto, K., Schwichtenberg, H., Seisenberger, M.: Minlog - A tool for program extraction supporting algebras and coalgebras. In: Proceedings of CALCO 2011. LNCS, vol. 6859, pp. 393–399 (2011)
5. Cederquist, J., Coquand, T.: Entailment relations and distributive lattices. In: Buss, S.R., Hájek, P., Pudlák, P. (eds.) Logic Colloquium '98. Proceedings of the Annual European Summer Meeting of the Association for Symbolic Logic, Prague, Czech Republic, August 9–15, 1998, Lect. Notes Logic, vol. 13, pp. 127–139. A. K. Peters, Natick, MA (2000)
6. Cederquist, J., Negri, S.: A constructive proof of the Heine–Borel covering theorem for formal reals. In: Berardi, S., Coppo, M. (eds.) Types for Proofs and Programs, Lecture Notes in Computer Science, vol. 1158, pp. 62–75. Springer, Berlin (1996)
7. Coste, M., Lombardi, H., Roy, M.F.: Dynamical method in algebra: Effective Nullstellensätze. Ann. Pure Appl. Logic **111**(3), 203–256 (2001)
8. Gödel, K.: Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes. dialectica **12**, 280–287 (1958)
9. Gurevich, Y.: Sequential abstract-state machines capture sequential algorithms. ACM Transactions on Computational Logic (TOCL) **1**, 77–111 (2000)
10. Kohlenbach, U.: On the no-counterexample interpretation. Journal of Symbolic Logic **64**, 1491–1511 (1999)
11. Kohlenbach, U.: Some computational aspects of metric fixed point theory. Nonlinear Analysis **61**(5), 823–837 (2005)
12. Kohlenbach, U.: Some logical metatheorems with applications in functional analysis. Trans. Amer. Math. Soc. **357**, 89–128 (2005)
13. Kohlenbach, U.: Applied Proof Theory: Proof Interpretations and their Use in Mathematics. Monographs in Mathematics, Springer (2008)
14. Kohlenbach, U.: Proof-theoretic methods in nonlinear analysis. In: Proc. ICM 2018. vol. 2, pp. 79–100. World Scientific (2019)
15. Kohlenbach, U., Koutsoukou-Argyraki, A.: Rates of convergence and metastability for abstract Cauchy problems generated by accretive operators. J. Math. Anal. Appl. **423**, 1089–1112 (2015)
16. Kohlenbach, U., Leuştean, L.: Effective metastability of Halpern iterates in CAT(0) spaces. Advances in Mathematics **321**, 2526–2556 (2012)

17. Kreisel, G.: On the interpretation of non-finitist proofs, Part I. Journal of Symbolic Logic **16**, 241–267 (1951)
18. Kreisel, G.: On the interpretation of non-finitist proofs, Part II: Interpretation of number theory. Journal of Symbolic Logic **17**, 43–58 (1952)
19. Kreisel, G.: Mathematical significance of consistency proofs. Journal of Symbolic Logic **23**(2), 155–182 (1958)
20. Lombardi, H., Quitté, C.: Commutative Algebra: Constructive Methods: Finite Projective Modules. Springer Netherlands, Dordrecht (2015)
21. Mulvey, C., Wick-Pelletier, J.: A globalization of the Hahn–Banach theorem. Adv. Math. **89**, 1–59 (1991)
22. Negri, S., von Plato, J., Coquand, T.: Proof-theoretical analysis of order relations. Arch. Math. Logic **43**, 297–309 (2004)
23. Oliva, P., Powell, T.: A game-theoretic computational interpretation of proofs in classical analysis. In: Gentzen's Centenary: The Quest for Consistency, pp. 501–532. Springer (2015)
24. Oliva, P., Powell, T.: Spector bar recursion over finite partial functions. Annals of Pure and Applied Logic **168**(5), 887–921 (2017)
25. Persson, H.: An application of the constructive spectrum of a ring. In: Type Theory and the Integrated Logic of Programs. Chalmers University and University of Göteborg (1999), phD thesis
26. Powell, T.: On Bar Recursive Interpretations of Analysis. Ph.D. thesis, Queen Mary University of London (2013)
27. Powell, T.: Gödel's functional interpretation and the concept of learning. In: Proceedings of Logic in Computer Science (LICS 2016). pp. 136–145. ACM (2016)
28. Powell, T.: Sequential algorithms and the computational content of classical proofs (2018), preprint, available at https://arxiv.org/abs/1812.11003
29. Richman, F.: Nontrivial uses of trivial rings. Proc. Amer. Math. Soc. **103**(4), 1012–1014 (1988)
30. Rinaldi, D., Schuster, P.: A universal Krull–Lindenbaum theorem. J. Pure Appl. Algebra **220**, 3207–3232 (2016)
31. Rinaldi, D., Schuster, P., Wessel, D.: Eliminating disjunctions by disjunction elimination. Bull. Symb. Logic **23**(2), 181–200 (2017)
32. Rinaldi, D., Schuster, P., Wessel, D.: Eliminating disjunctions by disjunction elimination. Indag. Math. (N.S.) **29**(1), 226–259 (2018)
33. Rinaldi, D., Wessel, D.: Cut elimination for entailment relations. Arch. Math. Log. (2018), https://doi.org/10.1007/s00153-018-0653-0
34. Rinaldi, D., Wessel, D.: Extension by conservation. Sikorski's theorem. Log. Methods Comput. Sci. **14**(4:8), 1–17 (2018)
35. Sanders, S.: Metastability and higher-order computability. In: Logical foundations of computer science. LNCS, vol. 10703, pp. 309–330. Springer (2018)
36. Schlagbauer, K., Schuster, P., Wessel, D.: Der Satz von Hahn–Banach im Rahmen einer allgemeinen Idealtheorie. Confluentes Math. (201?), forthcoming
37. Schuster, P.: Induction in algebra: a first case study. In: 2012 27th Annual ACM/IEEE Symposium on Logic in Computer Science. pp. 581–585. IEEE Computer Society Publications (2012), proceedings, LICS 2012, Dubrovnik, Croatia
38. Schuster, P.: Induction in algebra: a first case study. Log. Methods Comput. Sci. **9**(3), 20 (2013)
39. Schuster, P., Wessel, D.: A general extension theorem for directed-complete partial orders. Rep. Math. Logic **53**, 79–96 (2018)

40. Schwichtenberg, H., Seisenberger, M., Wiesnet, F.: Higman's lemma and its computational content. In: Advances in Proof Theory, Progress in Computer Science and Applied Logic, vol. 28, pp. 353–375. Springer (2015)
41. Simpson, S.G.: Subsystems of Second Order Arithmetic. Perspectives in Mathematical Logic, Springer, Berlin (1999)
42. Spector, C.: Provably recursive functionals of analysis: a consistency proof of analysis by an extension of principles in current intuitionistic mathematics. In: Dekker, F.D.E. (ed.) Recursive Function Theory: Proc. Symposia in Pure Mathematics, vol. 5, pp. 1–27. American Mathematical Society, Providence, Rhode Island (1962)
43. Tao, T.: Soft analysis, hard analysis, and the finite convergence principle. Essay, published as Ch. 1.3 of T. Tao, *Structure and Randomness: Pages from Year 1 of a Mathematical Blog*, Amer. Math. Soc, original version available online at http://terrytao.wordpress.com/2007/05/23/soft-analysis-hard-analysis-and-the-finite-convergence-principle/ (2008)
44. Wessel, D.: Ordering groups constructively. Comm. Algebra (201?), forthcoming
45. Yengui, I.: Making the use of maximal ideals constructive. Theoret. Comput. Sci. **392**, 174–178 (2008)
46. Yengui, I.: Constructive Commutative Algebra. Projective Modules over Polynomial Rings and Dynamical Gröbner Bases, Lecture Notes in Mathematics, vol. 2138. Springer, Cham (2015)