A universal algorithm for Krull's theorem

Thomas Powell[1], Peter Schuster[2], and Franziskus Wiesnet[2,3,4]

[1]Department of Computer Science, University of Bath
[2]Department of Computer Science, University of Verona
[3]Department of Mathematics, Università degli Studi di Trento
[4]Department of Mathematics, Ludwig-Maximilians Universität

April 23, 2021

Abstract

We give a computational interpretation to an abstract formulation of Krull's theorem, by analysing its classical proof based on Zorn's lemma. Our approach is inspired by proof theory, and uses a form of update recursion to replace the existence of maximal ideals. Our main result allows us to derive, in a uniform way, algorithms which compute witnesses for existential theorems in countable abstract algebra. We give a number of concrete examples of this phenomenon, including the prime ideal theorem and Krull's theorem on valuation rings.

Keywords: Krull's theorem, maximal ideals, program extraction, constructive algebra

1 Introduction

Krull's theorem for prime ideals is a fundamental result from abstract algebra. It can be formulated as follows: Let $F \subseteq R$ be an arbitrary subset of some commutative ring R. Then whenever $r \in R$ lies in the intersection of all prime ideals containing F, the element r also lies in the radical ideal $\sqrt{(F)}$ generated by F, or in other words:

$$\bigcap\{P \,:\, F \subseteq P \text{ and } P \text{ a prime ideal}\} \subseteq \sqrt{(F)}.$$

The standard proof of this fact appeals to Zorn's lemma. More specifically, we assume for contradiction that $r \notin \sqrt{(F)}$ and consider an ideal which is maximal among all ideals I such that $F \subseteq I$ but $r \notin I$. We conclude by demonstrating that this maximal ideal must be prime.

The second author, together with Rinaldi, has shown that the basic idea behind Krull's theorem can be presented in a generalised way, as a universal Krull–Lindenbaum theorem [39], so that it subsumes a large collection of important results in abstract algebra and beyond, including Krull's theorem for valuation rings, the Artin–Schreier theorem, and Lindenbaum's lemma for complete theories. This is achieved by abstracting prime ideals from commutative rings to the context of finitary coverings and binary operations, a move in the vein of formal topology [44] which cannot be thought of without the time-honoured point-free presentation of the Zariski spectrum as a distributive lattice [14]; for details we refer to [46].

In this article, we give a computational interpretation to this universal form of Krull's theorem by analysing its proof. This is challenging, because the proof is non-constructive,

and in particular invokes maximal ideals via Zorn's lemma. We tackle this problem by using ideas from applied proof theory, where in particular we employ a form of update recursion in the sense of [3, 32] - which in turn dates back to Spector's pioneering work on bar recursion [56] - to eliminate the use of Zorn's lemma and compute an 'approximate' maximal ideal in its place.

By instantiating the parameters of our abstract computational interpretation of Krull's theorem in a suitable way, algorithms for computing witnesses for existential statements in a range of concrete settings can be derived in a uniform manner. We present several examples in the second part of the paper. Our paper extends some initial ideas in this direction presented in [36]: there, we focus on a very simple instance of Krull's theorem, whereas our more abstract framework here not only allows us to consider a range of different applications, but could be readily applied to other case studies in future work.

Our results can be viewed as a new application of proof theory in the spirit of Kreisel [17, 18], in which we use proof-theoretic techniques to give finitary formulations to infinitary reasoning. Most existing work in this direction, particularly the so-called 'proof mining' program, focuses on areas of analysis (see the standard text [15] and also the recent survey [16]), but in the last few years some exciting case studies have been produced in algebra (notably [54]). We too seek to bring ideas such as the Dialectica interpretation to bear on proofs in abstract algebra, but while [54] focuses on achieving new effective bounds from proofs, we emphasise on the other hand general algorithmic patterns which correspond to the use of Zorn's lemma in a countable setting. Similar work in this direction but in the context of infinitary combinatorics can be found in [30, 35].

In making explicit how proof theoretic techniques can be used to obtain concrete algorithms in commutative algebra, we hope that our work opens the way to a more detailed investigation of the connections between constructive algebra and more traditional proof-theoretic techniques such as proof interpretations. While this is a question that we leave open for now, it is nevertheless important that we not only highlight related work in constructive mathematics but also emphasise how elements of our work owe a debt to this area.

As compared to intuitionistic algebra [59] or algebra in the style of Bishop's constructive mathematics [22], the idea of tackling transfinite methods in algebra, which nowadays typically come in the guise of Zorn's Lemma, is more recent. This has only become possible by using dynamical methods [11, 12], which now are well established - see e.g. the survey articles [8, 20] and the comprehensive monographs [21, 63].

Incidentally, dynamical methods have been applied to Krull's theorem for prime ideals, the main focus of our work, only very recently [52], which however has immediately prompted a systematic presentation of these methods: a dynamical counterpart [50] of the syntactical conservation criterion [40, 41] the semantics of which include the universal Krull–Lindenbaum theorem [39], the latter being crucial for the present paper as indicated above. With the axioms-as-rules paradigm [24, 25, 43], this conservation criterion further subsumes [42, 45, 60] and a wealth of cases from the literature, e.g. [4, 10, 19, 23, 26]. The latter development, which carries over from prime to maximal ideals [49, 51], rests upon the idea of viewing entailment as a relation between arbitrary objects [53], and using this as a tool to syntactically simulate the 'ideal' objects one encounters in abstract mathematics [4].

A paper directly relevant to our work is [62], which appeals to dynamical reasoning to eliminate a specific use of maximal ideals and instead replace them with a backtracking algorithm; for a related approach to prime ideals we refer to [47, 48]. Our main result in Section 4.2 is based on a similar idea, and replaces maximality principles in the countable

setting with a kind of 'update recursion'. This form of recursion essentially goes back to Spector's classic paper [56] on interpreting the axiom of countable choice via bar recursion, and has been already studied in the context of open induction [3, 5, 33, 37] which is nothing but a contrapositive formulation of Zorn's lemma.

All of the concrete applications of our general framework have already been analysed from the point of view of constructive or dynamical algebra, and given explicit proofs. For instance, that invertible polynomials have nilpotent non-constant coefficients (Section 5.1) is studied in [2, 7, 21, 29, 38, 47, 48, 63]. Similarly, Krull's theorem for valuation rings and Kronecker's theorem (Section 6) are treated in [10] and [19], have given rise to the celebrated paper [6], and more recently have been studied in the light of Lorenzen's ground-breaking but hitherto neglected work [9, 27].

We do not claim that the algorithms given in this paper are in any way superior to those which result from the aforementioned works. In particular, our algorithms rely in a crucial way on an enumeration of the underlying structure, which is typically not the case in constructive algebra. (The countable case, however, often suffices for applications by way of the method of indeterminate coefficients [21]: to deduce new equations about elements $c_1, \ldots, c_N$ of an arbitrary ring, work instead in the polynomial ring $\mathbb{Z}[c_1, \ldots, c_N]$ modulo the given relations between those elements.) Our aim is simply to investigate nonconstructive reasoning in commutative algebra from a different perspective, using a different set of techniques which are not often applied in this area.

2 A universal Krull theorem

We begin by introducing a variant of the abstract Krull-Lindenbaum lemma presented in [39], and give a formal treatment of this result in the countable setting, where in particular we show that its usual proof based on Zorn's lemma (which in [39] is formulated in the guise of open induction) can be reduced to an instance of dependent choice for $\forall$-formulas. This formalisation inspires our use of an algorithm based on *update recursion* to give a computational interpretation to the proof of the lemma in Section 4.

2.1 Basic notions

Before we begin, we recall some basic concepts from ring theory. Let R be a commutative ring. Then an *ideal* I is a subset of R which contains zero, is closed under addition, and satisfies the property that

$$a \in I \Rightarrow ab \in I$$

for any $a, b \in R$. Given an arbitrary subset $U \subseteq R$, we write (U) for the ideal generated by U, that is

$$(U) = \{a_1 u_1 + \ldots + a_k u_k \ : \ k \in \mathbb{N},\ a_1, \ldots, a_k \in R,\ u_1, \ldots, u_k \in U\}$$

where we use the convention that the empty sum i.e. $k = 0$ is equal to the zero element of R. An ideal is *proper* if $1_R \notin I$, and is *prime* if it satisfies

$$ab \in I \Rightarrow a \in I \vee b \in I$$

for any $a, b \in R$. In the remainder of this section, we will abstract these basic notions in terms of arbitrary *finitary coverings* $\triangleright$, and will talk about $\triangleright$-ideals and so on. Ring ideals in the usual sense are then just instances of this more general phenomenon.

2.2 Finitary coverings and ideals

The notion of a *finitary covering* goes back to Tarski's concept of consequence operator [57] and also the axiom systems of Hertz [13], and is fundamental to the abstract approach of [39] (see Section 3), which is in turn based on ideas from universal algebra and point-free or formal topology. For the remainder of this section, we take S to be an arbitrary set, although from Section 2.4 onwards this will be countable.

Notation. Throughout the article, for sets $U, V \subseteq S$ and an element $x \in S$ we write U, V and U, x as shorthands for $U \cup V$ and $U \cup \{x\}$, and the like.

Definition 2.1. A *finitary covering* $\rhd$ is a binary relation $A \rhd a$ on *finite* subsets $A \subseteq S$ and elements $a \in S$, which satisfies the following two conditions:

- *Reflexivity*: $\{a\} \rhd a$;
- *Transitivity*: If $B \rhd b$ and $A, b \rhd a$ then $A \cup B \rhd a$.

Remark 2.2. By iterating transitivity we obtain, more generally, that whenever $\{a_1, \ldots, a_k\} \rhd a$ and $B_i \rhd a_i$ then $\bigcup_{i=1}^{k} B_i \rhd a$.

Remark 2.3. We could extend the relation $\rhd$ to $\mathcal{P}(S) \times S$ by defining

$$U \rhd a :\Leftrightarrow A \rhd a \text{ for some finite } A \subseteq U.$$

This would then coincide with the usual notion of a finitary covering in formal topology, also used in [39].

Definition 2.4. For any $U \subseteq S$ we define the closure $\langle U \rangle$ of U with respect to some finitary covering $\rhd$ by

$$\langle U \rangle := \{a \in S \ : \ A \rhd a \text{ for some } A \subseteq U\}.$$

One can view $\langle - \rangle$ as an algebraic closure operator (in the sense of universal algebra) on the subsets of S. In particular, $\langle - \rangle$ has the following properties:

Lemma 2.5. *Let $\rhd$ be a finitary covering. Then the following hold:*

(i) $U \subseteq \langle U \rangle$.

(ii) If $U \subseteq \langle V \rangle$ *then* $\langle U \rangle \subseteq \langle V \rangle$.

Proof. The first part $U \subseteq \langle U \rangle$ follows from reflexivity of $\rhd$, since $a \in U$ implies $U \supseteq \{a\} \rhd a$ and thus $a \in \langle U \rangle$. For the second part, suppose that $U \subseteq \langle V \rangle$ and $a \in \langle U \rangle$. Then $A = \{a_1, \ldots, a_k\} \rhd a$ for $a_i \in U \subseteq \langle V \rangle$, which in turn implies that $B_i \rhd a_i$ for some finite $B_i \subseteq V$ for each $i = 1, \ldots, k$. By transitivity (cf. Remark 2.2) we have $V \supseteq \bigcup_{i=1}^{k} B_i \rhd a$ and thus $a \in \langle V \rangle$. This establishes $\langle U \rangle \subseteq \langle V \rangle$. □

Remark 2.6. As a direct result of Lemma 2.5 we obtain $\langle U \rangle = \langle \langle U \rangle \rangle$ for any $U \subseteq S$.

Definition 2.7. Let $\rhd$ be a finitary covering.

- A $\rhd$-*ideal* is a set $I \subseteq S$ satisfying $I = \langle I \rangle$. An ideal I is *proper* if $I \subsetneq S$.
- For $U \subseteq S$ we say that $\langle U \rangle$ is the ideal *generated* by U.
- An ideal I is *finitely generated* if $I = \langle \{a_1, \ldots, a_k\} \rangle$ for some $a_1, \ldots, a_k \in S$.

Definition 2.8. Let $\rhd$ be a finitary covering. A *multiplication operation* (w.r.t. $\rhd$) is a binary operation $\circ : S \times S \to S$ which satisfies the following condition:

– *Encoding*: $A, a \rhd c$ and $B, b \rhd c$ implies $A \cup B, a \circ b \rhd c$

The importance of Encoding has been noted in [39, 40, 41]. We can extend $\circ$ to a binary relation on subsets of S by defining

$$U \circ V := \{a \circ b \ : \ a \in U, b \in V\}.$$

Definition 2.9. Let $\rhd$ be a finitary covering and $\circ$ a multiplication operation. We say that an ideal I is *prime* if it satisfies

$$a \circ b \in I \Rightarrow a \in I \vee b \in I.$$

2.3 Krull's theorem

We now state and prove our abstract Krull theorem. For the remainder of this section, we fix some S equipped with a finitary covering $\rhd$ and multiplication operation $\circ$. We first need a suitable formulation of Zorn's lemma.

Definition 2.10. Let θ be an arbitrary predicate on finite subsets $A \subseteq S$. We define the predicate $\theta^{\rhd}$ on arbitrary subsets $U \subseteq S$ as follows:

$$\theta^{\rhd}(U) :\Leftrightarrow \theta(A) \text{ holds for all finite } A \subseteq \langle U \rangle.$$

We call a predicate Θ on subsets $U \subseteq S$ *open* if

$$\Theta(U) \Leftrightarrow \theta^{\rhd}(U)$$

for a suitable predicate θ on finite subsets of S.

Remark 2.11. Note that whenever Θ is open, by Lemma 2.5 and Remark 2.6 we have

$$\Theta(U) \Leftrightarrow \Theta(\langle U \rangle) \qquad \text{and} \qquad U \subseteq V \Rightarrow \Theta(U) \subseteq \Theta(V)\,.$$

The following is a tailor-made variant of what is known as the Teichmüller–Tukey Lemma:

Theorem 2.12 (Existence of maximal ideals)**.** *Let Θ be an open predicate and $F \subseteq S$ an arbitrary set satisfying $\Theta(F)$. Then there exists an ideal $M \supseteq F$ satisfying $\Theta(M)$, which is maximal in the sense that $\neg\Theta(M, a)$ for any $a \notin M$.*

Proof. The proof uses Zorn's lemma in the usual way. Define

$$Z := \{U \subseteq S \ : \ F \subseteq U \text{ and } \Theta(U)\}.$$

Then Z is nonempty since $F \in Z$. We show that every chain in Z has an upper bound in Z. To this end, take an arbitrary nonempty chain γ in Z and define $W := \bigcup_{U \in \gamma} U$. Then $F \subseteq W$ by nonemptyness of γ, and it remains to show that $\Theta(W)$ holds. Since Θ is open, we have $\Theta(U) \Leftrightarrow \theta^{\rhd}(U)$ for some predicate θ. Let $A = \{a_1, \ldots, a_k\}$ and suppose that $A \subseteq \langle W \rangle$, which means that for each $i = 1, \ldots, k$ we have $A_i \rhd a_i$ for some finite $A_i \subseteq W$. Now there is some $U \in \gamma$ such that $A_i \subseteq U$ and thus $a_i \in \langle U \rangle$ for each $i = 1, \ldots, k$ (note that for $A = \emptyset$ and thus $k = 0$ this follows by nonemptyness of γ). In other words, we have $A \subseteq \langle U \rangle$, and

since $\Theta(U)$ holds we must have $\theta(A)$. But we have therefore shown that $\theta(A)$ holds for any finite $A \subseteq \langle W \rangle$, which establishes $\Theta(W)$. Therefore γ has an upper bound $W \in Z$.

We can now apply Zorn's lemma to Z, which asserts the existence of some maximal element $M \in Z$. By Remark 2.11 we have $\Theta(\langle M \rangle)$ and thus $\langle M \rangle \in Z$, since also $F \subseteq M \subseteq \langle M \rangle$. Hence $M = \langle M \rangle$ by maximality of M. Finally, suppose that $a \notin M$. Then by maximality we have $M, a \notin Z$, and since $F \subseteq M, a$ this must imply that $\neg\Theta(M, a)$. □

We are now ready to present the abstract Krull theorem which will be analysed in the remainder of the paper. The result is essentially a reformulation of Theorem 14 from [39].

Theorem 2.13 (Krull's theorem)**.** *Let $F \subseteq S$ be an arbitrary set. Then we have*

$$\bigcap \{P \ : \ F \subseteq P \text{ and } P \text{ a prime ideal}\} \subseteq \langle F \rangle.$$

Proof. It suffices to show that for any $r \notin \langle F \rangle$ there exists at least one prime ideal P with $F \subseteq P$ but $r \notin P$. To this end we apply Theorem 2.12 with

$$\Theta(U) :\equiv r \notin \langle U \rangle \,,$$

which is clearly open since

$$r \notin \langle U \rangle \Leftrightarrow \neg(A \rhd r) \text{ for any finite } A \subseteq \langle U \rangle$$

From the assumption that $r \notin \langle F \rangle$, there exists by Theorem 2.12 some ideal $M \supseteq F$ with $r \notin \langle M \rangle = M$ but $r \in \langle M, a \rangle$ for any $a \notin M$. We now show that M is prime, which completes the proof.

Suppose for contradiction that there are some a, b with $a \circ b \in M$ but $a, b \notin M$. From $a \notin M$ and maximality of M it follows that $r \in \langle M, a \rangle$ i.e. $A' \rhd r$ for a finite $A' \subseteq M, a$. Moreover, it must be the case that $a \in A'$, i.e. $A' = A, a$ for some finite $A \subseteq M$, since otherwise we would have $M \rhd a$ and thus $r \in \langle M, a \rangle = \langle M \rangle$. Similarly, from $b \notin M$ it follows that $B, b \rhd r$ for some finite $B \subseteq M$. Therefore by encoding it follows that $A \cup B, a \circ b \rhd r$ from which we have $r \in \langle M, a \circ b \rangle$. But then we must have $a \circ b \notin M$, a contradiction. Therefore M is prime. □

A simple and well-known consequence of this theorem is the following, which was already analysed in [36] and will be examined in more generality in Section 5.

Corollary 2.14. *Let S be a commutative ring (with ideals now defined in the usual sense). Then*

$$\bigcap \{P \ : \ P \text{ a prime ideal}\} \subseteq \sqrt{0}$$

where for an ideal $I \subseteq S$, $\sqrt{I}$ denotes its radical*, that is, the ideal*

$$\sqrt{I} := \{a \in R \ : \ \exists e > 0 \ (a^e \in I)\}.$$

Proof. We instantiate $\circ$ as ring multiplication, and define

$$A \rhd a :\Leftrightarrow (\exists \vec{x} \in S^{|A|}, e > 0)(A \cdot \vec{x} = a^e),$$

where for $A := \{a_1, \ldots, a_k\}$ with $|A| = k$ and $\vec{x} = (x_1, \ldots, x_k)$ we define $A \cdot \vec{x}$ as shorthand for $a_1 x_1 + \ldots + a_k x_k$. To see that $\rhd$ constitutes a finitary covering, first observe that we

trivially have $\{a\} \rhd a$ since $a1_S = a^1$. For transitivity, supposing that $B \rhd b$ and $A, b \rhd a$ i.e. $B \cdot \vec{x} = b^{e_1}$ and $A \cdot \vec{y} + bz = a^{e_2}$ for some $\vec{x}, \vec{y}, z, e_1, e_2$, then it follows that

$$a^{e_1 e_2} = (A \cdot \vec{y} + bz)^{e_1} = A \cdot \vec{u} + b^{e_1} z^{e_1} = A \cdot \vec{u} + (B \cdot \vec{x})\ z^{e_1} = (A \cup B) \cdot \vec{v}$$

for suitable $\vec{u}$ and $\vec{v}$, which establishes $A \cup B \rhd a$. Finally, to see that ring multiplication is a multiplication operation w.r.t. $\rhd$, suppose that $A, a \rhd c$ and $B, b \rhd c$, in other words, $A \cdot \vec{x} + au = c^{e_1}$ and $B \cdot \vec{y} + bv = c^{e_2}$ for some $\vec{x}, \vec{y}, u, v, e_1, e_2$. Then we have

$$c^{e_1+e_2} = (A \cdot \vec{x} + au)(B \cdot \vec{y} + bv) = (A \cup B)\vec{z} + (ab)uv$$

for suitable $\vec{z}$, and therefore $A \cup B, ab \rhd c$.

Now, letting (U) denote the ideal generated by U in the usual sense, we observe that for any $U \subseteq S$ we have

$$\begin{aligned} \langle U \rangle &= \{a \in S \ :\ \exists k \in \mathbb{N}, \vec{a} \in U^k, \vec{x} \in S^k, e > 0\ (\vec{a} \cdot \vec{x} = a^e)\} \\ &= \{a \in S \ :\ \exists e > 0\ (a^e \in (U))\} \\ &= \sqrt{(U)}. \end{aligned}$$

In particular, I is an $\rhd$-ideal precisely when $I = \sqrt{(I)}$, and since this makes I an ideal in the usual sense we have $I = \sqrt{I}$ i.e. $\rhd$-ideals are precisely the radical ideals of S. Applying Theorem 2.13 for $F := \{0\}$ we obtain

$$\bigcap \{P \ :\ P \text{ is a prime } \rhd\text{-ideal}\} \subseteq \sqrt{0},$$

and since all prime ideals are radical, the result follows. □

Similar arguments for reflexivity, transitivity and encoding in the case of a commutative ring have been used elsewhere, e.g. in [46, 47, 48].

2.4 Formalising Krull's theorem in the countable setting

We now focus on the special case that our underlying set S is countable, and fix some enumeration

$$S := \{s_n \ :\ n \in \mathbb{N}\}.$$

We will show that in this case, Theorem 2.13 can be formalised using countable dependent choice, an observation which inspires our computational interpretation of the theorem in the next section. This subsection is **not essential for what follows**. In particular, Sections 3 and 4 are self-contained and do not rely on results of this subsection. We include them simply to give the proof-theoretically inclined reader some insight into where the algorithmic version of Krull's theorem comes from.

Our first result demonstrates that in the countable setting, maximality in the sense of Theorem 2.12 can be phrased in a sequential manner. The proof adapts a standard trick from reverse mathematics, see e.g. [55, Chapter III.5]. For the rest of this section, we take for granted that everything can be formalised over the base theory PA^ω of Peano arithmetic in all finite types (for details of this theory see e.g. [15], though precise details are not important for the sketch which follows).

Definition 2.15. Given some $U \subseteq S$ we define U_n to be the *initial segment* of U of length $n \in \mathbb{N}$, by which we mean

$$U_n := U \cap \{s_i \ : \ i < n\},$$

Note that $U_0 = \emptyset$ and $U = \bigcup_{n\in\mathbb{N}} U_n$.

Lemma 2.16. *Let Θ be an open predicate and $F \subseteq S$ an arbitrary set satisfying $\Theta(F)$. Define the predicate Θ_F by*

$$\Theta_F(U) :\Leftrightarrow \Theta(F \cup U).$$

Suppose that $M \subseteq S$ satisfies

$$s_n \in M \Leftrightarrow \Theta_F(M_n, s_n) \tag{1}$$

for all $n \in \mathbb{N}$. Then M is a maximal ideal in the sense of Theorem 2.12, in other words, it satisfies $F \subseteq M$, $\Theta(M)$ and $\neg\Theta(M, a)$ for any $a \notin M$.

Proof. We first show by induction that for any $n \in \mathbb{N}$ we have

$$(*) \quad F_n \subseteq M_n \text{ and } \Theta_F(M_n).$$

For $n = 0$ this means $\Theta(F)$. For the induction step there are two possibilities. If $s_n \in M$, then $M_{n+1} = M_n, s_n$ and thus $\Theta_F(M_{n+1})$ is equivalent to $\Theta_F(M_n, s_n)$, which is true by (1). Moreover, we have $F_{n+1} \subseteq F_n, s_n \subseteq M_n, s_n = M_{n+1}$ by induction. On the other hand, if $s_n \notin M$ then $M_{n+1} = M_n$ and thus $\Theta_F(M_{n+1})$ is equivalent to $\Theta_F(M_n)$, which holds by the induction hypothesis. To see that $F_{n+1} \subseteq M_{n+1} = M_n$ whenever $s_n \notin M$, by induction it suffices to show that $s_n \notin F$, i.e. $F_n = F_{n+1}$. But if $s_n \in F$ then $\Theta_F(M_n, s_n) \Leftrightarrow \Theta_F(M_n)$, and since the latter is true, by (1) this would contradict $s_n \notin M$. We now show that M has each of the desired conditions.

First of all, it is clear from $(*)$ that

$$F = \bigcup_{n\in\mathbb{N}} F_n \subseteq \bigcup_{n\in\mathbb{N}} M_n = M.$$

To see that M is an ideal, suppose for contradiction that $s_n \in \langle M\rangle$ but $s_n \notin M$ for some $n \in \mathbb{N}$. Then we have $A \rhd s_n$ for some finite $A \subseteq M$ but $\neg\Theta_F(M_n, s_n)$ by (1). Observe that since A is finite there is some $k \in \mathbb{N}$ sufficiently large such that $A \subseteq M_k$. We now consider two cases: If $k \leq n$ then $A \subseteq M_n$ and thus

$$\langle F \cup M_n, s_n\rangle = \langle F \cup M_n\rangle$$

by transitivity of $\rhd$. By Remark 2.11, in particular, $\neg\Theta_F(M_n, s_n)$ would imply $\neg\Theta_F(M_n)$, contradicting $(*)$. Similarly, on the other hand, if $n < k$ then $M_n, s_n \subseteq M_k, s_n$ and thus $\neg\Theta_F(M_n, s_n)$ implies $\neg\Theta_F(M_k, s_n)$, which in turn means $\neg\Theta_F(M_k)$ since $\langle F \cup M_k, s_n\rangle = \langle F \cup M_k\rangle$, and thus contradicts $(*)$. Here we repeatedly use Remark 2.11.

To see that $\Theta(M)$, i.e. that $\Theta_F(M)$ follows from $(*)$ it is enough to observe, for every finite A, that if $A \subseteq \langle F \cup M\rangle$ then $A \subseteq \langle F \cup M_n\rangle$ for sufficiently large n. Finally, for maximality, suppose that $a = s_n \notin M$. Then $\neg\Theta_F(M_n, s_n)$ by $(*)$, and since $\langle F \cup M_n, s_n\rangle \subseteq \langle F \cup M, s_n\rangle$ it follows that $\neg\Theta_F(M, s_n)$, again by Remark 2.11. □

Definition 2.17. A formula Q on $\vec{X}$, where here $\vec{X}$ is some tuple of types in PA^ω, is primitive recursive if there exists some primitive recursive functional $t_Q : \vec{X} \to \{0,1\}$ such that

$$Q(\vec{x}) \Leftrightarrow t_Q(\vec{x}) = 1$$

A formula $P(\vec{x})$ on some tuple of typed variables is a $\exists$- resp. $\forall$-formula when it can be expressed in the form $\exists \vec{y}\, Q(\vec{x}, \vec{y})$ resp. $\forall \vec{y}\, Q(\vec{x}, \vec{y})$ for primitive recursive Q.

Proposition 2.18. *Suppose that $\rhd$ is an $\exists$-formula i.e. is of the form*

$$A \rhd a \Leftrightarrow \exists x \in X\ (A \rhd_x a)$$

where the ternary relation $A \rhd_x a$ is primitive recursive and X is some type in PA^ω*. Then Theorem 2.12 applied to an open predicate of the form $\Theta(U) \Leftrightarrow \theta^{\rhd}(U)$ for primitive recursive $\theta(A)$ can be formalised in* $\mathrm{PA}^\omega + \forall$-DC*, where the latter stands for the axiom of countable dependent choice for $\forall$-formulas.*

Proof. We first observe that

$$a \in \langle U \rangle \Leftrightarrow (\exists A \subseteq U, x \in X)(A \rhd_x a)$$

and so $a \in \langle U \rangle$ is an $\exists$-formula. By coding variables into tuples, it follows more generally that the formula $A \subseteq \langle U \rangle$ for finite A is also an $\exists$-formula. But then since

$$\Theta(U) \Leftrightarrow (\forall A)(A \subseteq \langle U \rangle \Rightarrow \theta(A)),$$

it follows that $\Theta(U)$ is a $\forall$-formula, since the premise of the implication above is an $\exists$-formula and the conclusion is primitive recursive.

Now, let $F \subseteq S$ be an arbitrary set satisfying $\Theta(F)$. For a binary sequence $b_0, \ldots, b_{n-1}$ let $[b_0, \ldots, b_{n-1}] \subseteq S$ denote the finite subset $\{s_i \ : \ i < n \wedge b_i = 1\}$. Construct the function $f : \mathbb{N} \to \{0,1\}$ as follows: If $f(0), \ldots, f(n-1)$ have already been defined then

$$f(n) := \begin{cases} 1 & \text{if } \Theta_F([f(0), \ldots, f(n-1)], s_n) \\ 0 & \text{otherwise.} \end{cases}$$

Then the set $M := \{s_n \ : \ f(n) = 1\}$ satisfies the premise (1) of Lemma 2.16, and is therefore a maximal ideal. But the proof of Lemma 2.16 uses only induction and thus can be formalised in PA^ω. The above instance of dependent choice involves a decision on a $\forall$-formula and thus an instance of $\exists\forall$-DC, which by introducing dummy variables can be reduced to an instance of $\forall$-DC (see e.g. [15, p. 208]). □

Corollary 2.19. *Suppose that $\rhd$ is an $\exists$-formula. Then Theorem 2.13 can be formalised in* $\mathrm{PA}^\omega + \forall$-DC*.*

Proof. The proof of Theorem 2.13 uses Theorem 2.12 for $\Theta(U) \Leftrightarrow \theta^{\rhd}(U)$ for $\theta(A) :\Leftrightarrow r \notin A$, which is primitive recursive since this involves checking the code of r against the finite number of elements in A. Thus by Proposition 2.18, the existence of a maximal ideal in this case is provable in $\mathrm{PA}^\omega + \forall$-DC. Since the remainder of the proof of Theorem 2.13 uses simple classical logic and so can clearly be formalised in PA^ω, we are done. □

3 A computational formulation of Krull's theorem

In this and the following section we present the central result of the paper, namely a computational interpretation of the universal Krull theorem (Theorem 2.13). Our first step is to formulate precisely a computational problem corresponding to Krull's theorem, which we do below. In the next section, we present an algorithm which solves this problem. Though we use ideas from proof theory, particularly proof interpretations such as realizability and algorithmic ideas based on variants of bar recursion, everything that follows is presented in a self-contained manner, and requires no prior knowledge of the aforementioned concepts. From now on, we make the following key assumptions, which correspond to those in Section 2.4. These are that:

1. the underlying set $S := \{s_n \ : \ n \in \mathbb{N}\}$ is countable,
2. the covering relation $\rhd$ is an $\exists$-formula, i.e. $A \rhd a \Leftrightarrow (\exists x)(A \rhd_x a)$ for some primitive recursive ternary relation $A \rhd_x a$.

Krull's theorem as stated in Theorem 2.13 can be reformulated in a more explicit manner as follows: Fixing some arbitrary $F \subseteq S$ and $r \in S$, from the assumptions

(A) $\rhd$ is a finitary covering and $\circ$ a multiplication operator,

(B) $r \in \bigcap\{P \ : \ F \subseteq P \text{ and } P \text{ a prime ideal}\}$,

we can conclude that

(C) $r \in \langle F \rangle$.

Thus, in the spirit of realizability, our aim is to find a procedure which transforms *realizers* for the assumptions (A) and (B) into a realizer for the conclusion (C). The remainder of this section is dedicated to carefully outlining exactly what constitutes a realizer in each case.

3.1 Realizing (A) via a cover structure

The assumption (A) consists of three components: that the relation $\rhd$ is reflexive and transitive (Definition 2.1), and that the multiplication operator $\circ$ satisfies the encoding property (Definition 2.8). Let's first consider reflexivity. Bearing in mind that $\rhd$ is an $\exists$-formula, this corresponds to the following logical statement:

$$(\forall a \in S)(\exists x \in X)(\{a\} \rhd_x a).$$

A computational interpretation of this statement would then be a function $\iota(a)$ which for any $a \in S$ returns some $\iota(a) \in X$ satisfying $\{a\} \rhd_{\iota(a)} a$. Here we implicitly associate the element $a \in S$ with its code s_n for some $n \in \mathbb{N}$. Transitivity, on the other hand, takes the following logical form:

$$(\forall A, B, a, b)((\exists x)(A \rhd_x a) \wedge (\exists y)(B, a \rhd_y b) \Rightarrow (\exists z)(A \cup B \rhd_z b))$$

Its computational interpretation would be a function $\tau(A, B, a, b, x, y)$ such that whenever $A \rhd_x a$ and $B, a \rhd_y b$, we have $A \cup B \rhd_z b$ for $z := \tau(A, B, a, b, x, y)$. Encoding is similar. We now turn this idea into a formal definition, which we take to be a realizer for the assumption (A).

Definition 3.1 (Cover structure). A cover structure for $\rhd$ and $\circ$ is a triple of functions (ι, τ, η) satisfying the following properties:

- $\forall a\ (\{a\} \rhd_{\iota(a)} a)$,
- $\forall A, B, a, b, x, y\ (A \rhd_x a \wedge B, a \rhd_y b \Rightarrow A \cup B \rhd_{\tau(A,B,a,b,x,y)} b)$,
- $\forall A, B, a, b, c, x, y\ (A, a \rhd_x c \wedge B, b \rhd_y c \Rightarrow A \cup B, a \circ b \rhd_{\eta(A,B,a,b,c,x,y)} c)$.

In concrete cases studied in later sections, these functions often only depend on some of their arguments, and so we simply drop those arguments which do not play a role.

3.2 Realizing (B) via a 'Krull functional'

The assumption (B) states that for any $P \subseteq S$, if both $F \subseteq P$ and P is a prime ideal, then we must have $r \in P$. An equivalent formulation is the following:

$$(\forall P \subseteq S)(F \not\subseteq P \vee P \text{ not a prime ideal} \vee r \in P)$$

A computational interpretation of this statement can be taken to be a functional $\psi(P)$, which takes some arbitrary $P \subseteq S$ as its input (which we assume is given as a characteristic function, so that membership of P is a decidable property), and returns as output evidence that at least one of the disjuncts holds. Let us now consider each of the disjuncts in turn. Since $r \in P$ is decidable, no further evidence is needed to justify this. On the other hand, the statement $F \subseteq P$ has the form

$$(\forall a \in S)(a \in F \Rightarrow a \in P)$$

In other words, in order to justify $F \not\subseteq P$ we must provide as evidence a concrete element $a \in S$ such that $a \in F$ but $a \notin P$. Next, P being a prime ideal is actually the conjunction of two properties: namely being an ideal (Definition 2.7) and being prime (Definition 2.9). Since $P \subseteq \langle P \rangle$ trivially follows from reflexivity of $\rhd$ (Lemma 2.5), the property of being an ideal can be reduced to the inclusion $\langle P \rangle \subseteq P$, which from a logical point of view corresponds to

$$(\forall A, x, a)(P \supseteq A \rhd_x a \Rightarrow a \in P).$$

Therefore to justify the claim that P is not an ideal, we must exhibit some A, x, a such that $P \supseteq A \rhd_x a$ but $a \notin P$. Finally, since being prime corresponds to

$$(\forall a, b, c)(c = a \circ b \in P \Rightarrow a \in P \vee b \in P)$$

as evidence for non-primality of P we require a, b, c such that $c = a \circ b$ and $c \in P$, but both $a \notin P$ and $b \notin P$. Bringing everything together, our functional $\psi(P)$ will return two things: A marker which informs us which of the disjuncts we are seeking to verify, and the corresponding evidence for this. We call such a functional a 'Krull functional'. From now on we implicitly associate subsets of S with their representation as objects of type $S \to \{0, 1\}$, which taking into account the enumeration of S can be reduced to an object of type $\mathbb{N} \to \{0, 1\}$.

Definition 3.2 (Krull functional). Fixing parameters F and r, a *Krull functional* $\psi : \{0, 1\}^S \to \{0, 1, 2, 3\} \times \mathbb{N}$ is a functional which for any input $P \in \{0, 1\}^S$ satisfies

$$\begin{aligned}
&\psi(P) = (0, a) \Rightarrow a \in F \wedge a \notin P \\
&\psi(P) = (1, 0) \Rightarrow r \in P \\
&\psi(P) = (2, [A, x, a]) \Rightarrow A \subseteq P \wedge A \rhd_x a \wedge a \notin P \\
&\psi(P) = (3, [a, b, c]) \Rightarrow a \circ b = c \in P \wedge a \notin P \wedge b \notin P
\end{aligned}$$

where $[x_1, \ldots, x_n] \in \mathbb{N}$ denotes some coding of $x_1, \ldots, x_n$ as a single natural number, and we implicitly associate elements $a, b, c \in S$ with indices representing their enumeration.

Note that if the first component of $\psi(P)$ is 0, 1, 2 or 3, then $F \not\subseteq P$, $r \in P$, P is not an ideal and P is not prime, respectively.

3.3 The computational challenge

In order to realize our conclusion (C) that $r \in \langle F \rangle$, we simply need to exhibit some $A \subseteq F$ and x such that $A \rhd_x r$. Thus our overall challenge is to compute A and x in terms of realizers for our two main assumptions (A) and (B), in other words to give a pair of functionals $A(\iota, \tau, \eta, \psi)$ and $x(\iota, \tau, \eta, \psi)$ such that fixing $F \subseteq S$ and r

$$\begin{aligned}&(\iota, \tau, \eta) \text{ a cover structure} \wedge \psi \text{ a Krull functional w.r.t. } F \text{ and } r\\ &\Rightarrow F \supseteq A(\iota, \tau, \eta, \psi) \rhd_{x(\iota,\tau,\eta,\psi)} r.\end{aligned}$$

This will be the goal of the next section.

4 The main algorithm

We now present our algorithm for solving the computational problem outlined in the previous section. Just as the main component of the proof of Krull's theorem is the use of a maximal ideal, our algorithm is based around the step-by-step construction of an 'approximate' maximal ideal. As we will see, an approximation suffices for finding some A and x which satisfy $F \supseteq A \rhd_x r$, and in this way, the use of Zorn's lemma is eliminated in favour of a finitistic process, in a similar spirit to e.g. [62]. Our algorithm is essentially a variant of update recursion, a well-known method for constructing approximations to choice sequences which has appeared in many different guises over the years. This goes back at least as far as Spector [56] (Section 12.1), and has more recently played a role in learning realizability of Aschieri et al. [1], modified realizability [3] and the functional interpretation [28, 32, 33], and has also been studied as a recursion scheme in its own right [31]. In particular, the algorithm carries out recursion by successively extending a current approximation with new elements, and termination is shown using a continuity argument, as is standard for algorithms of this kind.

Our construction has some precedent in constructive algebra. For example, [22, Lemma VI.3.2] presents a simplified construction whereby a maximal ideal is built step-by-step relative to some enumeration of the underlying ring. However, in this case there is an additional assumption that all finitely generated ideals are detachable (i.e. decidable), and so the maximal ideal itself can be recursively constructed. We make no such assumption and must instead build approximations, via a more complex procedure. The backtracking procedure of Yengui [62] appears to be closer in spirit to ours, and it would be interesting to establish a more precise connection with his construction.

4.1 Specifying the algorithm

We will describe our algorithm as a sequential computation on states $\{\pi_i\}_{i \in \mathbb{N}}$, which starts in some empty state π_0 and successively updates $\pi_0 \mapsto \pi_1 \mapsto \ldots \mapsto \pi_k$ until it terminates in some final state π_k. This final state will contain the information we need for computing A

and x. We begin by defining the structure of our states. We let $[S]$ denote the set of all *finite* subsets of S, and by X we mean the type of x in $A \rhd_x a$.

Definition 4.1. A *state* is a partial function $\pi : \mathbb{N} \rightharpoonup [S] \times X$. We write $\pi_L : \mathbb{N} \rightharpoonup [S]$ and $\pi_R : \mathbb{N} \rightharpoonup X$ to denote the projections of π. Furthermore, we define:

(i) $\mathrm{dom}(\pi) := \{n \in \mathbb{N} \ : \ \pi(n) \text{ is defined}\} \subseteq \mathbb{N}$,

(ii) $U(\pi) := \{s_n \ : \ n \notin \mathrm{dom}(\pi)\} \subseteq S$.

Remark 4.2. Formally, we envisage partial functions $f : \mathbb{N} \rightharpoonup Y$ being represented as total functions $f' : \mathbb{N} \to \{0,1\} \times Y$, where $f'(n) = (1, f(n))$ on $\mathrm{dom}(f)$ and $f'(n) = (0, 0_Y)$ otherwise, for some canonical element $0_Y \in Y$. Thus, membership of $\mathrm{dom}(f)$ is a decidable property.

For everything that follows, we now fix some $F \subseteq S$ and element $r \in S$ as universal parameters. In addition to these, the algorithm we describe below will depend on a cover structure (ι, τ, η) and a Krull functional ψ.

Definition 4.3. We say that a state π is *partially maximal* if

(a) $F \subseteq U(\pi)$,

(b) if $s_n \notin U(\pi)$, i.e. $n \in \mathrm{dom}(\pi)$, then $\pi_L(n) \subseteq F \cup U(\pi)_n$ and $\pi_L(n), s_n \rhd_{\pi_R(n)} r$.

where we recall the notation $U(\pi)_n = U(\pi) \cap \{s_i \mid i < n\}$ (cf. Definition 2.15). Note that the empty partial function is trivially partially maximal.

The intuition here is that the set $U(\pi)$ represents an approximation from above/outside to a maximal ideal M in the sense of the proof of Theorem 2.13, while the partial function π provides justification for *excluding* an element from $U(\pi)$ - this is the rationale for defining $U(\pi)$ to be the complement of the domain of π. To be more precise, recall that the object M in the proof of Theorem 2.13 satisfies

(i) $F \subseteq M$

(ii) M is a $\rhd$-ideal

(iii) $r \notin \langle M \rangle = M$

(iv) if $a \notin M$ then there is some finite $A \subseteq M$ and $x \in X$ with $A, a \rhd_x r$.

In comparison, if a state π is partially maximal, then $U(\pi)$ satisfies both (i) and *a computationally explicit* form of (iv) above, but not necessarily (ii) or (iii). For instance, the 'empty' state $\epsilon : \mathbb{N} \rightharpoonup [S] \times X$ undefined everywhere gives rise to $U(\epsilon) = S$, and is thus trivially partially maximal, but on the other hand satisfies $r \in \langle U(\epsilon) \rangle$. Our algorithm's strategy is to start with the full set S and remove elements step-by-step, in a way that is guided by the Krull functional ψ. Though we can never construct the full maximal object, at some point we arrive at a sufficiently good partially maximal state which encodes some $A \subseteq F$ and $x \in X$ with $A \rhd_x r$.

Informally, the following result says that assuming that r lies in the intersection of all prime ideals containing F, then $r \in \langle U(\pi) \rangle$ whenever a state π is partially maximal. We then use this fact to exclude some new element from $U(\pi)$, thus updating our approximation to a maximal ideal with one that is 'better'.

Lemma 4.4. *Suppose that (ι, τ, η) is a cover structure and ψ a Krull functional. Then there exists a functional $g_{\iota,\tau,\eta,\psi}(\pi) \in [S] \times X$ such that whenever π is partially maximal, then $(A, x) := g_{\iota,\tau,\eta,\psi}(\pi)$ satisfies $U(\pi) \supseteq A \rhd_x r$.*

Proof. We consider $\psi(U(\pi))$ and show that in each possible case we can produce some (A, x) satisfying $U(\pi) \supseteq A \rhd_x r$. First note that $\psi(U(\pi)) = (0, a)$ is not possible, since by partial maximality of π we have $F \subseteq U(\pi)$.

- If $\psi(U(\pi)) = (1, 0)$ then $r \in U(\pi)$ and thus $A := \{r\}$ and $x := \iota(r)$ work.
- If $\psi(U(\pi)) = (2, [B, y, s_i])$ then $B \rhd_y s_i$ for $B \subseteq U(\pi)$ and $s_i \notin U(\pi)$. Since π is partially maximal, the latter implies $\pi_L(i), s_i \rhd_{\pi_R(i)} r$ for $\pi_L(i) \subseteq F \cup U(\pi)_i \subseteq U(\pi)$. Thus it follows that $A := B \cup \pi_L(i)$ and $x := \tau(B, \pi_L(i), s_i, r, y, \pi_R(i))$ do the trick.
- If $\psi(U(\pi)) = (3, [s_i, s_j, c])$ then $s_i \notin U(\pi)$, $s_j \notin U(\pi)$ but $c \in U(\pi)$, and thus $\pi_L(i), s_i \rhd_{\pi_R(i)} r$ and $\pi_L(j), s_j \rhd_{\pi_R(j)} r$. Therefore we have

  $$\pi_L(i) \cup \pi_L(j), c \rhd_{\eta(\pi_L(i),\pi_L(j),s_i,s_j,c,\pi_R(i),\pi_R(j))} r$$

  and since $\pi_L(i), \pi_L(j) \subseteq U(\pi)$ and also $c \in U(\pi)$ we see that $A := \pi_L(i) \cup \pi_L(j), c$ and $x := \eta(\pi_L(i), \pi_L(j), c, s_i, s_j, \pi_R(i), \pi_R(j))$ do the trick.

Putting all this together, we have $A \subseteq U(\pi)$ and $A \rhd_x r$ for $(A, x) = g_{\iota,\tau,\eta,\psi}(\pi)$, where $g_{\iota,\tau,\eta,\psi}(\pi)$ is the functional which simply decides which case we are in and returns the relevant witness. □

Lemma 4.5. *Suppose that $F \subseteq U$. Then whenever A, x are such that $U \supseteq A \rhd_x r$, one of the following two cases holds:*

(a) $A \subseteq F$, or

(b) $A \nsubseteq F$ and setting $n := \max\{i \ : \ s_i \in A \backslash F\}$ and $B := A \backslash \{s_n\}$ we have $s_n \in U \backslash F$ and $B \subseteq F \cup U_n$ and $B, s_n \rhd_x r$,

where we recall that $U_n := U \cap \{s_i \ : \ i < n\}$.

Proof. We have $s_n \in U \backslash F$ by the assumption $A \subseteq U$. To see that $B \subseteq F \cup U_n$, suppose that $s_i \in B$. If $i > n$ then $s_i \in F$ by maximality of n, and otherwise if $i < n$ then we must have $s_i \in U_n$, since $s_i \in A \subseteq U$. But since $B, s_n = A$ we also have $B, s_n \rhd_x r$. □

Having established some basic properties relating to states and cover structures, we are now ready to define our main algorithm.

Definition 4.6. The binary operation $\uplus$ takes as input a state π together with a tuple $(n, B, x) \in \mathbb{N} \times [S] \times X$ and returns a new state given by

$$\pi \uplus (n, B, x) := m \mapsto \begin{cases} \pi(m) & \text{if } m < n \text{ and } m \in \mathrm{dom}(\pi) \\ (B, x) & \text{if } m = n \\ \text{undefined} & \text{otherwise} \end{cases}$$

Note in particular that we have

$$U(\pi \uplus (n, B, x)) = U(\pi)_n \cup \{s_m \ : \ m > n\}.$$

We are now ready to define the main update recursive algorithm.

Definition 4.7. The sequential algorithm $(\pi_k)_{k\in\mathbb{N}}$ is defined as follows. Let π_0 be the empty partial function, and given that we have reached state π_k:

1. Let $A_k \in [S]$ and $x_k \in X$ be defined by $(A_k, x_k) := g_{\iota,\tau,\eta,\psi}(\pi_k)$, for $g_{\iota,\tau,\eta,\psi}$ as in Lemma 4.4.
2. If $A_k \subseteq F$, the algorithm terminates in state π_k.
3. Otherwise, let $n_k \in \mathbb{N}$ and $B_k \in [S]$ be given by

$$n_k := \max\{i \ : \ s_i \in A_k \backslash F\}$$
$$B_k := A_k \backslash \{s_{n_k}\}$$

define $\pi_{k+1} := \pi_k \uplus (n_k, B_k, x_k)$, and repeat steps 1-3 for $k \mapsto k+1$.

4.2 Termination and correctness

Having specified our algorithm, there are two things left to do: We need to demonstrate that whatever we choose as our parameters, the algorithm eventually terminates, and moreover, we must show that our final state contains the desired output. We begin by dealing with termination. For this, we make use of a continuity argument.

Definition 4.8. Let $f : (\mathbb{N} \rightharpoonup [S] \times X) \to Y$ be some functional from states π to objects $y \in Y$, and suppose that X, Y are both equipped with an coding into the natural numbers $\mathbb{N}$. Then in particular, since states can be represented as total functions $\mathbb{N} \to \{0,1\} \times [S] \times X$ (see Remark 4.2), which can in turn be encoded as functions $\mathbb{N} \to \mathbb{N}$, then f can be encoded as an object of type $(\mathbb{N} \to \mathbb{N}) \to \mathbb{N}$. We say that f is *computable* if its underlying representation can be computed on an oracle Turing machine.

Definition 4.9. A functional $g : (\mathbb{N} \rightharpoonup [S] \times X) \to [S] \times X$ from states to pairs in $[S] \times X$ is *continuous* if for any state π there exists some N such that

$$\forall \pi'(\pi =_N \pi' \Rightarrow g(\pi) = g(\pi')).$$

Here, $\pi =_N \pi'$ is shorthand for $\forall i < N(\pi(i) = \pi'(i))$, and $\pi(i) = \pi'(i)$ means that both sides are either undefined, or defined and equal to the same value. Note that $\pi =_0 \pi'$ for any π, π'.

Whenever a functional g is computable in the sense of Definition 4.8, it must also be continuous: The intuition here is that given some oracle Turing machine which simulates g, for any input π the output $g(\pi)$ is computed in a finite number of steps, during which the input state π can only be queried a finite number of times. In particular, if g can be defined within certain restricted calculi such as Gödel's System T, a so-called *modulus of continuity* can even be computed in this case (see [58], or [34, 61] for a more recent treatment of this fact).

Lemma 4.10. *Suppose that the cover structure (ι, τ, η) consists of computable functions, and the Krull functional ψ is computable in the sense of Definition 4.8. Then the functional $g_{\iota,\tau,\eta,\psi}$ given in Lemma 4.4 is also computable, and therefore continuous.*

Proof. Since membership of $\mathrm{dom}(\pi)$ is decidable, it is clear that the functional $\pi \mapsto \psi(U(\pi))$ is computable. Once we have computed $\psi(U(\pi))$, the functional $g_{\iota,\tau,\eta,\psi}$ is nothing more than a simple case distinction, which is computable in the cover structure (ι, τ, η). □

Theorem 4.11. *Fixing global parameters F and r, let (ι, τ, η) be a computable cover structure and ψ a computable Krull functional. Then running our algorithm from Definition 4.7, there is some sufficiently large $K \in \mathbb{N}$ such that $A_K \subseteq F$ and thus the algorithm terminates in state π_K.*

Proof. We begin by showing that for each $n \in \mathbb{N}$, the value of $\pi_k(n)$ can change only finitely many times as $k \to \infty$. To this end, we define a sequence $j_0 \leq j_1 \leq \ldots$ satisfying $\forall m \in \mathbb{N}$:

$$\forall k \geq j_m \ (\pi_k =_m \pi_{j_m}).$$

This by induction on m. We set $j_0 := 0$, and assuming that j_m has been defined, we split our construction into two cases:

- If $\pi_k(m)$ is undefined for all $k \geq j_m$ then $j_{m+1} := j_m$ does the trick.
- Otherwise $\pi_j(m) = (A, x)$ for some $j \geq j_m$, and we set $j_{m+1} := j$. To see that this works, it suffices to show that $\pi_k(m) = (A, x)$ for all $k \geq j_{m+1}$. Suppose that this were not the case, and take the minimum $k \geq j_{m+1}$ with $\pi_k(m) = (A, x)$ but $\pi_{k+1}(m) \neq (A, x)$. But by definition, as $m \in \mathrm{dom}(\pi_k)$ this can only happen if $m \geq n_k$ (cf. Definitions 4.6–4.7), and since $s_{n_k} \in A_k \subseteq U(\pi_k)$ and thus $\pi_k(n_k)$ is undefined, we cannot have $m = n_k$ and therefore $m > n_k$. But now - again by definition - we have $\pi_{k+1}(n_k) = (B_k, x_k) \neq \pi_k(n_k)$ (the latter being undefined), and since $n_k < m$ this contradicts $\pi_{k+1} =_m \pi_k$ and thus the construction of j_m.

Next, we define the state π_∞ to be the limit of the π_{j_m} i.e. $\pi_\infty(m) := \pi_{j_{m+1}}(m)$. In particular, we have $\pi_\infty =_m \pi_{j_m}$ for all $m \in \mathbb{N}$. Now, by continuity of $g_{\iota,\tau,\eta,\psi_{F,r}}$ (which follows from Lemma 4.10) there exists some $N \in \mathbb{N}$ such that setting $(A, x) := g_{\iota,\tau,\eta,\psi_{F,r}}(\pi_\infty)$ we have

$$\forall \pi' \ (\pi_\infty =_N \pi' \Rightarrow (A, x) = g_{\iota,\tau,\eta,\psi_{F,r}}(\pi')).$$

In particular, for all $k \in \mathbb{N}$ we have

$$\pi_\infty =_N \pi_k \Rightarrow (A, x) = (A_k, x_k). \tag{2}$$

Let $M := \max(\{i + 1 \ : \ s_i \in A\} \cup \{N\})$ and define $K := j_M$ so that

$$\pi_\infty =_M \pi_K \quad \text{and} \quad \forall k \geq K \ (\pi_k =_M \pi_K). \tag{3}$$

We claim that $A_K \subseteq F$. If this were not the case, then we would have $\pi_{K+1} = \pi_K \uplus (n_K, B_K, x_K)$ for $s_{n_K} \in A_K \backslash F \subseteq U(\pi_K)$ and so in particular $\pi_{K+1}(n_K) = (B_K, x_K)$ while $\pi_K(n_K)$ is undefined. Now, since $N \leq M$, and $\pi_\infty =_M \pi_K$ by (3), then also $\pi_\infty =_N \pi_K$ and thus by (2) we have $(A, x) = (A_K, x_K)$. But this implies that $s_{n_K} \in A_K = A$ and thus $n_K < M$, but since by (3) it follows that $\pi_{K+1} =_M \pi_K$, this contradicts $\pi_{K+1}(n_K) \neq \pi_K(n_K)$. Thus we have established $A_K \subseteq F$ and we're done. □

In all of the examples that follow, we consider instances of (ι, τ, η) and ψ which are clearly computable, and so termination of our algorithm in each case follows directly from the above theorem. It remains, however, to show that the algorithm is correct, which follows by demonstrating that all reachable states are partially maximal.

Lemma 4.12. *Suppose that (ι, τ, η) is a cover structure and ψ a Krull functional. For each $k \in \mathbb{N}$ the state π_k is partially maximal.*

Proof. Induction on k. For $k = 0$ we have $U(\pi_0) = S$ and thus π_0 is trivially partially maximal. Let's now suppose that π_k is partially maximal, and appeal to the notation of Definition 4.7. By Lemma 4.4 we have $U(\pi_k) \supseteq A_k \rhd_{x_k} r$. Assume that $A_k \nsubseteq F$ (else the algorithm terminates and we're done). By Lemma 4.5, we see that $B_k, s_{n_k} \rhd_{x_k} r$ for $B_k, s_{n_k} \subseteq F \cup U(\pi_k)_n$. But since $s_{n_k} \notin F$ we have (as π_k is partially maximal):

$$F \subseteq U(\pi_k) \backslash \{s_{n_k}\} \subseteq U(\pi_k)_{n_k} \cup \{s_m \ : \ m > n_k\} = U(\pi_k \uplus (n_k, B_k, x_k)) = U(\pi_{k+1}).$$

Now take some $s_m \notin U(\pi_{k+1})$. There are two possibilities. Either $m < n_k$ and so $s_m \notin U(\pi_k)$, in which case by the induction hypothesis we have

$$\pi_{k+1,L}(m) = \pi_{k,L}(m) \subseteq F \cup U(\pi_k)_m = F \cup U(\pi_{k+1})_m$$

and similarly $\pi_{k+1,L}(m), s_m \rhd_{\pi_{k+1,R}(m)} r$. On the other hand, if $m \geq n_k$, then we must have $m = n_k$. Then (using Lemma 4.5 (b)) we have

$$\pi_{k+1,L}(n_k) = B_k \subseteq F \cup U(\pi_k)_{n_k} = F \cup U(\pi_{k+1})_{n_k}$$

and $\pi_{k+1,L}(n_k), s_{n_k} \rhd_{\pi_{k+1,R}(n_k)} r$ follows directly from $B_k, s_{n_k} \rhd_{x_k} r$ and the fact that $\pi_{k+1}(n_k) = (B_k, x_k)$. □

We now come to the main result of this section.

Theorem 4.13 (Main theorem)**.** *Fixing F and r, let (ι, τ, η) be a computable cover structure and ψ a computable Krull functional, and consider the algorithm given in Definition 4.7. Consider the pair (A_K, x_K) where π_K is the algorithm's final state (which always exists by Theorem 4.11). Then $F \supseteq A_K \rhd_{x_K} r$.*

Proof. By Lemma 4.12, the final state π_K is partially maximal, and thus by Lemma 4.4, we have $A_K \rhd_{x_K} r$. But since π_K is the final state, the condition $A_K \subseteq F$ must be satisfied. This completes the proof. □

Looking back to the computational challenge outlined in Section 3.3, our main theorem states that the problem is solved by setting

$$A(\iota, \tau, \eta, \psi), x(\iota, \tau, \eta, \psi) := A_K, x_K$$

which are in turn obtained from the final state π_K of our sequential algorithm. In the remainder of the paper, we now turn our attention to concrete instantiations of our algorithm. We focus on two main case studies in which our relation $\rhd$ and cover structure are implemented in a particular way. In each of these case studies we give specific examples where a Krull functional is introduced.

5 Case study I: Radical ideals in commutative rings

In this section we develop the study of radical ideals already briefly mentioned in Corollary 2.14. Here we take $S := \{s_n \ : \ n \in \mathbb{N}\}$ to be some countable commutative ring whose ring operations can all be represented by computable functions on natural numbers. We also adopt the convention that finite subsets $A \subseteq S$ are uniquely represented by finite sequence $[a_0, \ldots, a_{k-1}]$, containing no repetitions and ordered in terms of their coding.

Definition 5.1. For the remainder of this section, we define $X := S^* \times \mathbb{N}_{>0}$ where S^* denotes the set of all finite sequences of elements of S, and define our main relation $A \rhd_{x,e} a$ as

$$A \rhd_{x,e} a :\Leftrightarrow (|A| = |x|) \wedge (A \cdot x = a^e)$$

where $|A|$ denotes the length of A i.e. for $A = [a_0, \ldots, a_{k-1}]$ we have $|A| := k$ (the same for x), $A \cdot x = a_0 x_0 + \ldots + a_{k-1} x_{k-1}$, and $A \cdot [] = 0_S$ in the case that $A = \emptyset$.

Let A, B be finite subsets of S represented by $[a_0, \ldots, a_{k-1}]$ and $[b_0, \ldots, b_{l-1}]$ respectively. Then the representation of $A \cup B$ is obtained from $[a_0, \ldots, a_{k-1}]$ and $[b_0, \ldots, b_{l-1}]$ by merging both lists, sorting them and deleting repeated elements (for the case $A \cap B \neq \emptyset$). In a similar fashion, if $x, y \in S^*$ satisfy $|A| = |x|$ and $|B| = |y|$, there is some $z \in S^*$ computable from x, y, A, B such that $|A \cup B| = |z|$ and

$$(A \cup B) \cdot z = A \cdot x + B \cdot y.$$

We use the operator $*$ to denote the function which takes x, y, A, B and returns such a z, so that

$$(A \cup B) \cdot (x *_{A,B} y) = A \cdot x + B \cdot y.$$

Lemma 5.2. *Let $\circ$ denote the ring multiplication in S. Then relations $\rhd$ and $\circ$ can be given a computable cover structure (ι, τ, η).*

Proof. We deal with each property in turn.

- Since $a 1_S = a^1$ we clearly have $\{a\} \rhd_{\iota(a)} a$ for $\iota(a) := ([1_S], 1)$.
- Assume that $A \rhd_{x,e_1} a$ and $B, a \rhd_{y',e_2} b$ and so in particular $A \cdot x = a^{e_1}$ and there is some $y \in S^*$ and $u \in S$ computable from y' such that $B \cdot y + au = b^{e_2}$. Now we claim for each $n \in \mathbb{N}$ there is some $y_n \in S^*$ computable in a, b, y, u, e_2 satisfying $B \cdot y_n + a^n u^n = b^{ne_2}$. For $n = 1$ we just set $y_1 := y$, whereas for the induction step we note that

$$\begin{aligned} b^{(n+1)e_2} &= (B \cdot y_n + a^n u^n) b^{e_2} \\ &= B \cdot b^{e_2} y_n + a^n u^n (B \cdot y + au) \\ &= B \cdot (b^{e_2} y_n + a^n u^n y) + a^{n+1} u^{n+1} \end{aligned}$$

  and so we can set $y_{n+1} = b^{e_2} y_n + a^n u^n y$. Now, in particular we have

$$b^{e_1 e_2} = B \cdot y_{e_1} + a^{e_1} u^{e_1} = B \cdot y_{e_1} + A \cdot u^{e_1} x = (A \cup B) \cdot (u^{e_1} x *_{A,B} y_{e_1})$$

  and so we can set

$$\tau(A, B, a, b, x, e_1, y', e_2) := (u^{e_1} x *_{A,B} y_{e_1}, e_1 e_2).$$

- Assume that $A, a \rhd_{x',e_1} c$ and $B, b \rhd_{y',e_2} c$ and so in particular there are x, u computable from x' and y, v computable from y' such that $A \cdot x + au = c^{e_1}$ and $B \cdot y + bv = c^{e_2}$. Then we have

$$\begin{aligned} c^{e_1 + e_2} &= (A \cdot x + au) c^{e_2} \\ &= A \cdot c^{e_2} x + au (B \cdot y + bv) \\ &= (A \cup B) \cdot (c^{e_2} x *_{A,B} auy) + abuv \\ &= (A \cup B, ab) \cdot (c^{e_2} x *_{A,B} auy) *_{A \cup B, ab} [uv] \end{aligned}$$

  and therefore we can set

$$\eta(A, B, a, b, c, x', y') := ((c^{e_2} x *_{A,B} auy) *_{A \cup B, ab} [uv], e_1 + e_2).$$

This completes the proof. □

Theorem 5.3. *Suppose that for parameters $F \subseteq S$ and $r \in S$ we are given a computable Krull functional $\psi_{F,r}$. Then instantiating the algorithm from Definition 4.7 on the cover structure (ι, τ, η) above and $\psi_{F,r}$, the algorithm terminates in some state π_k from which we obtain $(A_k, (x_k, e_k))$ (as in step 1 of Definition 4.7) with $A_k \subseteq F$, $|A_k| = |x_k|$ and $A_k \cdot x_k = r^{e_k}$.*

Remark 5.4. In the case that $F = \{0_S\}$ the algorithm terminates in some state with $A_k \subseteq \{0_S\}$ in which case we must have $r^{e_k} = 0_S$.

We now give some examples of situations giving rise to a concrete Krull function, which then yield fully determined algorithms for computing witnesses for existential statements.

5.1 Nilpotent coefficients of invertible polynomials

Our first example has been studied from the perspective of dynamical algebra in [21, cf. II.2 Lemma 2.6] and in a more general form in [63], and was already discussed in [36]. We recall it here and describe it using our new notation.

> Let S be a commutative ring and $f = \sum_{i=0}^{n} a_i X^i$ be a unit in $S[X]$. Then a_i is nilpotent for each $i > 0$.

This fact is traditionally established by showing that $a_i \in P$ for each prime ideal $P \subseteq S$ and then using Corollary 2.14. To this end, assume for contradiction that $a_i \notin P$ for some prime ideal P and $i > 0$, and let $g = \sum_{i=0}^{m} b_i X^i$ be an inverse of f. Let us write $gf = \sum_{i=0}^{m+n} c_i X^i$. Then we have $a_0 b_0 = c_0 = 1$ and for any $i > 0$

$$0 = c_i = a_0 b_i + \ldots + a_{i-1} b_1 + a_i b_0$$

and therefore

$$a_i = -a_0(a_0 b_i + \ldots + a_{i-1} b_1)$$

from which it follows that $b_j \notin P$ for some $0 < j \leq i$. Pick k, l to be the maximum indices such that $a_k, b_l \notin P$, noting in particular that $k + l > 0$. This implies that

$$0 = c_{k+l} = a_0 b_{k+l} + \ldots + a_{k-1} b_{l+1} + a_k b_l + a_{k+1} b_{l-1} + \ldots + a_{k+l} b_0$$

and from maximality of k, l it follows that $a_k b_l \in P$, a contradiction.

A closer inspection of this argument allows us to produce a Krull functional $\psi_{\{0_S\},a_i}$ for any $i > 0$ witnessing that for any P either P is not a prime ideal or $a_i \in P$. We now describe such a functional $\psi_{\{0_S\},a_i}$ as an algorithm, assuming that f together with an inverse g as above are given explicitly. Note that whenever the basic ring operations together with membership of P are computable, the functional is computable.

Lemma 5.5. *Let S be a countable commutative ring. Suppose that $f = \sum_{i=0}^{n} a_i X^i \in S[X]$ has an inverse $g \in \sum_{i=0}^{m} b_i X^i \in S[X]$. For $i > 0$ define the functional $\phi(i, P)$ by the following algorithm:*

1. *Check if $0_S \notin P$. If so, return $(0, 0_S)$.*
2. *Check if $a_i \in P$. If so, return $(1, 0)$.*

3. *Check if* $b_1, \ldots, b_i \in P$. *If so then* $[b_1, \ldots, b_i] \cdot [-a_0 a_{i-1}, \ldots, -a_0^2] = a_i \notin P$ *and from this we can directly compute* x *such that* $\{b_1, \ldots, b_i\} \rhd_{x,1} a_i$. *Return* $(2, [\{b_1, \ldots, b_i\}, (x, 1), a_i])$.

4. *Compute* k, l *maximal with* $a_k, b_l \notin P$.

5. *Check if* $a_k b_l \in P$. *If so return* $(3, [a_k, b_l, a_k b_l])$.

6. *Else* $[b_{k+l}, \ldots, b_{l+1}, a_{k+1}, \ldots, a_{k+l}] \cdot [-a_0, \ldots, -a_{k-1}, -b_{l-1}, \ldots, -b_0] = a_k b_l$ *and thus we can compute* x *such that* $A := \{b_{k+l}, \ldots, b_{l+1}, a_{k+1}, \ldots, a_{k+l}\} \rhd_{x,1} a_k b_l$. *Return* $(2, [A, (x, 1), a_k b_l])$.

Then $\psi_{\{0_S\},a_i}(P) := \phi(i, P)$ *is a Krull functional w.r.t.* $\{0_S\}$ *and* a_i.

Proof. A straightforward checking of each case. The first two cases are trivial, and the third follows from the assumption that $\{b_1, \ldots, b_i\} \in P$ and $a_i \notin P$. Step 4 is well defined since $a_i \notin P$ and $b_j \notin P$ for some $0 < j \leq i$. For the final case, we have $\{b_{k+l}, \ldots, b_{l+1}, a_{k+1}, \ldots, a_{k+l}\} \subseteq P$ by maximality of k and l. □

Corollary 5.6. *Let* S *be a countable commutative ring. Suppose that* $f = \sum_{i=0}^{n} a_i X^i \in S[X]$ *has an inverse* $g \in \sum_{i=0}^{m} b_i X^i \in S[X]$ *and take some* $i > 0$. *Suppose the algorithm from Definition 4.7 is instantiated on the cover structure from Lemma 5.2 and the functional* $\psi_{\{0_S\},a_i}$ *defined in Lemma 5.5. Then the algorithm terminates in some state* π_k *from which we obtain* e_k *with* $a_i^{e_k} = 0_S$.

5.2 The theorem of Gauss-Joyal

We consider a second construction, this time arising from the following result, see e.g. [2], which is commonly called the Gauss-Joyal theorem [6, 7, 21]:

> Let S be a commutative ring and $f = \sum_{i=0}^{n} a_i X^i, g = \sum_{i=0}^{m} b_i X^i \in S[X]$ be two polynomials with $fg = \sum_{i=0}^{n+m} c_i X^i$. Then
>
> $$a_i b_j \in \sqrt{(c_0, \ldots, c_{i+j})}$$
>
> for all $i = 0, \ldots, n$ and $j = 0, \ldots, m$.

This is proven using Theorem 2.13 for $F := \{c_0, \ldots, c_{i+j}\}$, observing (cf. Corollary 2.14) that

$$\langle \{c_0, \ldots, c_{i+j}\} \rangle = \sqrt{(c_0, \ldots, c_{i+j})}.$$

It therefore suffices to show that $a_i b_j \in P$ for each prime ideal P with $F \subseteq P$. Suppose for contradiction that $a_i b_j \notin P$ and thus $a_i, b_j \notin P$ and define k, l to be the minimum such that $a_k, b_l \notin P$. Since P is prime we also have $a_k b_l \notin P$. Observe as in Section 5.1 that

$$c_{k+l} = a_0 b_{k+l} + \ldots + a_{k-1} b_{l+1} + a_k b_l + a_{k+1} b_{l-1} + \ldots + a_{k+l} b_0.$$

Noting that $k + l \leq i + j$ we have $c_{k+l} \in F \subseteq P$, and by minimality of k, l it therefore follows that $a_k b_l \in P$, a contradiction.

Lemma 5.7. *Let* S *be a countable commutative ring. Suppose that* $f = \sum_{i=0}^{n} a_i X^i, g = \sum_{i=0}^{m} b_i X^i \in S[X]$ *are polynomials with* $fg = \sum_{i=0}^{n+m} c_i X^i$. *Define the functional* $\phi(i, j, P)$ *by the following algorithm:*

1. *Check if $c_k \notin P$ for some $k = 0, \dots, i+j$. If so, return $(0, c_k)$.*
2. *Check if $a_i b_j \in P$. If so, return $(1, 0)$.*
3. *Check if either $a_i \in P$ or $b_j \in P$. If so, return in the first case $(2, [\{a_i\}, ([b_j], 1), a_i b_j])$ and in the second $(2, [\{b_j\}, ([a_i], 1), a_i b_j])$.*
4. *Compute k, l minimal with $a_k, b_l \notin P$.*
5. *Check if $a_k b_l \in P$. If so return $(3, [a_k, b_l, a_k b_l])$.*
6. *Else $[c_{k+l}, a_0, \dots, a_{k-1}, b_{l-1}, \dots, b_0] \cdot [1_S, -b_{k+l}, \dots, -b_{l+1}, -a_{k+1}, \dots, -a_{k+l}] = a_k b_l$ and thus we can compute x such that*

$$A := \{c_{k+l}, a_0, \dots, a_{k-1}, b_{l-1}, \dots, b_0\} \rhd_{x,1} a_k b_l.$$

Return $(2, [A, (x, 1), a_k b_l])$.

Then for all $i = 0, \dots, n$ and $j = 0, \dots, m$ the functional $\psi_{\{c_0,\dots,c_{i+j}\},a_i b_j}(P) := \phi(i, j, P)$ is a Krull functional w.r.t $\{c_0, \dots, c_{i+j}\}$ and $a_i b_j$.

Proof. Another straightforward case distinction. For the final case, the inclusion

$$\{c_{k+l}, a_0, \dots, a_{k-1}, b_{l-1}, \dots, b_0\} \subseteq P$$

follows by minimality of k, l and the fact that $k + l \leq i + j$ and thus $c_{k+l} \in P$ by the failure of the first case. □

Corollary 5.8. *Let S be a countable commutative ring. Suppose that $f = \sum_{i=0}^{n} a_i X^i, g = \sum_{i=0}^{m} b_i X^i \in S[X]$ are polynomials with $fg = \sum_{i=0}^{n+m} c_i X^i$ and take some $0 \leq i \leq n$ and $0 \leq j \leq m$. Suppose the algorithm from Definition 4.7 is instantiated on the cover structure from Lemma 5.2 and the functional $\psi_{\{c_0,\dots,c_{i+j}\},a_i b_j}$ defined in Lemma 5.7. Then the algorithm terminates in some state π_k from which we obtain $(A_k, (x_k, e_k))$ with $A_k \subseteq \{c_0, \dots, c_{i+j}\}$ and $A_k \cdot x_k = (a_i b_j)^{e_k}$.*

6 Case study II: Valuation rings and integral closures

We now give a very different application of our main computational results, focusing on valuation rings. For the rest of the section, we let S be some countable *field* whose operations are computable, and fix some subring $E \subseteq S$ whose members can be constructed in an explicit way. Given any subset $U \subseteq S$, as usual $E[U]$ denotes the subring of S containing E which is generated by U. An element $a \in S$ is called *integral* over some arbitrary subring $R \subseteq S$ if there exists some monic polynomial $p \in R[X]$ such that $p(a) = 0$. We denote by $\overline{R} \subseteq S$ the integral closure of R in S, i.e. the set of all elements of S which are integral over R.

Definition 6.1. We now instantiate our main relation by

$$A \rhd_p a :\Leftrightarrow p \text{ monic} \wedge p(a) = 0$$

where here $p \in E[A][X]$ ranges over all polynomials with coefficients in $E[A]$.

Note that for $A = \{a_1, \ldots, a_k\}$, the elements of $E[A]$ are precisely those of the form $f(a_1, \ldots, a_k)$, where $f \in E[X_1, \ldots, X_k]$ is some multivariable polynomial with coefficients in E. Thus polynomials $p \in E[A][X]$ are formally represented by tuples of polynomials over E, which are in turn represented by tuples of objects in E. However, in this section we do not go into detail as to how everything is formally encoded, and from now on, whenever we write $A \rhd_p x$ we work directly with some $p \in E[A][X]$ rather than its formal representation.

Lemma 6.2. *For any $U \subseteq S$ we have $\langle U \rangle = \overline{E[U]}$. In particular, the $\rhd$-ideals of S are precisely the integrally closed subrings $R \subseteq S$ which contain E.*

Proof. Suppose that $a \in \overline{E[U]}$. Then there is some monic polynomial $p(X) = X^n + b_{n-1}X^{n-1} + \cdots + b_0 \in E[U][X]$ such that $p(a) = 0$. Now, for any coefficient $b_i \in E[U]$ it follows that $b_i \in E[A_i]$ for some finite $A_i \subseteq U$, and thus $p \in E[A][X]$ for $A := \bigcup_{i=0}^{n-1} A_i$. So we conclude $a \in \overline{E[U]}$ iff $A \rhd_p a$ for some finite $A \subseteq U$, or in other words $a \in \langle U \rangle$. □

We recall that P is a prime ideal iff P is an integrally closed subring $E \subseteq P \subseteq K$ with the additional property that $c \in P \vee c^{-1} \in P$ for all $c \in K \setminus \{0\}$. To see this, in one direction from $cc^{-1} = 1 \in P$ we have $c \in P \vee c^{-1} \in P$, and in the other, if $ab \in P$ for $a, b \neq 0$ (otherwise it is trivial) then either $a \in P$ and we are done, or $a^{-1} \in P$ and thus $b = a^{-1}ab \in P$.

Subrings $P \subseteq K$ with the property $c \in P \vee c^{-1} \in P$ are called *valuation rings*. Note that a valuation ring P is automatically integral closed, since if $c^n + a_{n-1}c^{n-1} + \cdots + a_1c + a_0 = 0$ is an integral equation for an element $c \in K \setminus \{0\}$ and $a_0, \ldots, a_{n-1} \in P$, then either $c \in P$ and we are done or $c^{-1} \in P$. But then multiplying the integral equation with $c^{-n+1} \in P$ gives: $c = -a_{n-1} - \cdots - a_1c^{-n+2} - a_0c^{-n+1} \in P$.

Lemma 6.3. *Let $\circ$ denote multiplication in S. Then $\rhd$ and $\circ$ can be given a computable cover structure (ι, τ, η).*

Proof. We deal with each property in turn.

- We clearly have $\{a\} \rhd_{\iota(a)} a$ for $\iota(a) := X - a$.
- Suppose that $A \rhd_p a$ and $B, a \rhd_q b$ where $\deg(p) = n$ and $\deg(q) = m$. Then we have

  $$p(a) = a^n + p_{n-1}a^{n-1} + \cdots + p_1a + p_0 = 0,$$

  where $p_i \in E[A]$, and similarly

  $$q(b) = b^m + \tilde{q}_{m-1}b^{m-1} + \ldots + \tilde{q}_1b + \tilde{q}_0 = 0,$$

  for $\tilde{q}_j \in E[B, a]$. In particular, from the $\tilde{q}_j$ we can compute some $l \in \mathbb{N}$ and $q_0, \ldots, q_l \in E[B][X]$ with $\deg(q_j) < m$ and

  $$P_2(a) := q_l(b)a^l + \cdots + q_1(b)a + b^m + q_0(b) = 0,$$

  where now $P_2 \in E[B, b][X]$ is a polynomial of degree l. This means that the resultant $\mathrm{res}(p, P_2) = 0$ because p and P_2 have a as common root. Recall that the resultant is

the determinant of the Sylvester matrix given by

$$\left.\begin{pmatrix} 1 & p_{n-1} & \dots & p_0 & & 0 \\ & \ddots & \ddots & & \ddots & \\ 0 & & 1 & p_{n-1} & \dots & p_0 \\ q_l(b) & \dots & q_1(b) & b^m + q_0(b) & & 0 \\ & \ddots & \ddots & & \ddots & \\ 0 & & q_l(b) & q_{l-1}(b) & \dots & b^m + q_0(b) \end{pmatrix}\right\} \begin{matrix} l \text{ rows} \\ \\ \\ \\ \\ n \text{ rows} \end{matrix}$$

Considering the resultant as a polynomial in b we obtain a polynomial $r \in E[A, B][X]$ with $r(b) = 0$. To see that this polynomial is monic, observe that each summand of the determinant of the Sylvester matrix selects l elements from $\{1, p_{n-1}, \dots, p_1, p_0\}$ and n elements from $\{q_l(b), \dots, q_1(b), b^m + q_0(b)\}$. The p_i are constant in b and the degree of the q_i is smaller than m. So each non-zero summand has degree smaller than mn, except for the product of the diagonal entries which is given by

$$1^l(b^m + q_0(b))^n = b^{mn} + \dots$$

and thus r is monic.

– Suppose that $A, a \rhd_p c$ and $B, b \rhd_q c$ with $\deg(p) = n$ and $\deg(q) = m$. Then similarly to the previous part, we can compute from p some $k \in \mathbb{N}$ and $p_0, \dots, p_k \in E[A][X]$ such that

$$P_1(c) := p_k(c)a^k + \dots + p_1(c)a + c^n + p_0(c) = 0$$

where $\deg(p_i) < n$. Similarly from q we can compute some $l \in \mathbb{N}$ and $q_0, \dots, q_l \in E[B][X]$ with

$$P_2(b) := q_l(c)b^l + \dots + q_1(c)b + c^m + q_0(c) = 0$$

where $\deg(q_j) < m$. Now, multiplying $P_1(c)$ by b^k and defining $\overline{p}_i := p_i \cdot (ab)^i$, where now $\overline{p}_i \in E[A, ab][X]$ but still $\deg(\overline{p}_i) < n$, we obtain

$$P_3(b) := (c^n + p_0(c))b^k + \overline{p}_1(c)b^{k-1} + \dots + \overline{p}_{k-1}(c)b + \overline{p}_k(c) = 0.$$

Since $P_3(b) = P_2(b) = 0$, the resultant $\mathrm{res}(P_3, P_2) \in E[A, B, ab][c]$ is equal to zero. From this resultant we can compute a polynomial $Q \in E[A, B, ab][X]$ with $Q(c) = \mathrm{res}(P_3, P_2) = 0$. Thus $A \cup B, ab \rhd_Q c$ provided we can show that Q is monic. Here the relevant Sylvester matrix is given by

$$\begin{pmatrix} c^n + p_0(c) & \overline{p}_1(c) & \dots & \overline{p}_k(c) & & 0 \\ & \ddots & \ddots & & \ddots & \\ 0 & & c^n + p_0(c) & \overline{p}_1(c) & \dots & \overline{p}_k(c) \\ q_l(c) & \dots & q_1(c) & c^m + q_0(c) & & 0 \\ & \ddots & & \ddots & \ddots & \\ 0 & & q_l(c) & \dots & q_1(c) & c^m + q_0(c) \end{pmatrix}$$

Each non-zero summand of the determinant of this matrix involves the multiplication of l coefficients from P_3 and k coefficients from P_2 and thus the degree in c of each summand bounded by $nl + mk$. But since $deg(\overline{p}_i) < n$ and $deg(q_j) < m$ this degree is

actually smaller than $nl + mk$, except for the product of the diagonal entries with is given by

$$(c^n + p_0(c))^l (c^m + q_0(c))^k = c^{nl+mk} + ...$$

and thus the determinant is monic when considered as a polynomial in c. □

In this setting of valuation rings and integral closures we have the following formulation of Theorem 4.13:

Theorem 6.4. *Suppose that for $F \subseteq S$ and $r \in S$ we have a computable Krull functional $\psi_{F,r}$. Then the algorithm of Definition 4.7 on the computable cover structure given in Lemma 6.3 and $\psi_{F,r}$ terminates in some state π_k from which we obtain (A_k, p_k) with $A_k \subseteq F$ and such that $p_k \in E[A_k][X]$ is monic with $p_k(r) = 0$.*

6.1 Kronecker's Theorem

We now conclude by giving a concrete example of a Krull functional, which we obtain by analysing a proof of Kronecker's theorem due to Coquand and Persson [10] which was revised by Lombardi [19]. Kronecker's theorem is stated as follows:

> Let E be some subring of S and $a_0, \ldots, a_m, b_0, \ldots, b_n$ be nonzero elements of S and $c_k := \sum_{i+j=k} a_i b_j$. Then any $a_k b_l$ is integral over $E[c_0, \ldots, c_{m+n}]$.

We prove this result using Theorem 6.4 with $F = \{c_0, \ldots, c_{m+n}\}$. It suffices to show that $a_k b_l \in P$ for any valuation ring P containing F. So we fix such a valuation ring P and we first prove the following lemma:

> For any $u_1, \ldots, u_n \in S \setminus \{0\}$ with $(u_1 + \cdots + u_n)^{-1} \in P$ it follows that $u_i^{-1} \in P$ for at least one i.

This is proved by induction: If $n = 0$, the premise $(u_1 + \cdots + u_n)^{-1} \in P$ is never true since $u_1 + \cdots + u_n = 0$ is not invertible. For the induction step, suppose that $w := (u_1 + \cdots + u_n + u_{n+1})^{-1} \in P$, note that

$$1 = (u_1 + \cdots + u_n)w + u_{n+1}w$$

and thus

$$u_{n+1}^{-1} w^{-1} = u_{n+1}^{-1} v + 1,$$

where $v := u_1 + \cdots + u_n$. If $v = 0$, we have directly $u_{n+1}^{-1} = w \in P$. If $v \neq 0$ then $v^{-1} w^{-1} = 1 + v^{-1} u_{n+1}$ and thus

$$(v^{-1} w^{-1} - 1)(u_{n+1}^{-1} w^{-1} - 1) = 1 \in P.$$

So either $(v^{-1} w^{-1} - 1) \in P$ and thus $v^{-1} \in P$, in which case we are done by the induction hypothesis, or $u_{n+1}^{-1} w^{-1} - 1 \in P$ and thus $u_{n+1}^{-1} \in P$.

Continuing with the proof of Kronecker's theorem, as in [10] we define the order $\leq_P$ on $S \setminus \{0\}$ by $x \leq_P y$ iff $yx^{-1} \in P$. Since P is a subring, this $\leq_P$ is reflexive and transitive, and since P is a valuation ring and we thus have either $yx^{-1} \in P$ or $xy^{-1} \in P$, the preorder $\leq_P$ is a total preordering on $S \setminus \{0\}$.

In particular, there exist i_0 and j_0 such that $a_{i_0} \leq_P a_i$ and $b_{j_0} \leq_P b_j$ for all i, j. We take i_0 and j_0 maximal with this property. As $x \leq_P y$ and $x' \leq_P y'$ imply $xx' \leq_P yy'$,

we have $a_{i_0}b_{j_0} \leq_P a_k b_l$ and so $a_k b_l \in P$ follows from $a_{i_0}b_{j_0} \in P$ (because if $x \leq_P y$ then $x \in P \Rightarrow y \in P$). Now, suppose for contradiction that $a_{i_0}b_{j_0} \notin P$, and note that

$$a_{i_0}b_{j_0} = c_{i_0+j_0} - \sum_{\substack{i+j=i_0+j_0 \\ i \neq i_0}} a_i b_j.$$

We have

$$c_{i_0+j_0}a_{i_0}^{-1}b_{j_0}^{-1} - \sum_{\substack{i+j=i_0+j_0 \\ i>i_0}} a_i b_j a_{i_0}^{-1}b_{j_0}^{-1} - \sum_{\substack{i+j=i_0+j_0 \\ j>j_0}} a_i b_j a_{i_0}^{-1}b_{j_0}^{-1} = 1 \in P$$

where all terms of the sum, except $c_{i_0+j_0}a_{i_0}^{-1}b_{j_0}^{-1}$, cannot be zero, since $a_i, b_j \neq 0$. We assume first $c_{i_0+j_0} \neq 0$, then we apply the lemma above to all the terms of the sum and get:

- If $c_{i_0+j_0}^{-1}a_{i_0}b_{j_0} \in P$ then $a_{i_0}b_{j_0} \in P$, a contradiction, because we have $c_{i_0+j_0} \in P$ by assumption.
- If $a_i^{-1}b_j^{-1}a_{i_0}b_{j_0} \in P$ for some $i > i_0$ then by $b_{j_0} \leq_P b_j$ we have $a_i \leq_P a_{i_0}$ but this is not possible by the maximality of i_0.
- If $a_i^{-1}b_j^{-1}a_{i_0}b_{j_0} \in P$ for some $j > j_0$ then by $a_{i_0} \leq_P a_i$ we have $b_j \leq_P a_{j_0}$ but this is not possible by the maximality of j_0.

In the other case we have $c_{i_0+j_0} = 0$ and therefore

$$\sum_{\substack{i+j=i_0+j_0 \\ i>i_0}} a_i b_j a_{i_0}^{-1}b_{j_0}^{-1} + \sum_{\substack{i+j=i_0+j_0 \\ j>j_0}} a_i b_j a_{i_0}^{-1}b_{j_0}^{-1} = 1 \in P.$$

Also here we use the lemma above to this sum but this time we only have to consider the cases $a_i^{-1}b_j^{-1}a_{i_0}b_{j_0} \in P$ for some $i > i_0$ or for some $j > j_0$. But in both cases we get a contradiction analogously to the first case.

Inspired by the proof above, we build a Krull functional which represents its computational content. We break down our construction into a series of lemma, whereby we denote by a *partial Krull functional* a Krull functional which is defined on some specified subset of $\{0,1\}^S$.

Lemma 6.5. *For $s = [u_1, \ldots, u_n] \in (S\backslash\{0\})^*$ and given $P \subseteq S$ with $u_i^{-1} \notin P$ for all i, $(u_1 + \ldots + u_n)^{-1} \in P$ and $1 \in P$ we define the functional $\phi_1(s, P) \in \{0,1,2,3\} \times \mathbb{N}$ recursively on the length of s as follows:*

1. *Set $w := (u_1 + \ldots + u_n)^{-1}$ and $v := u_1 + \ldots + u_{n-1}$, so that $1 = vw + u_n w$. Note that $v = 0$ implies that $u_n^{-1} = w \in P$, a contradiction, so v^{-1} exists.*
2. *Check if $u_n^{-1}w^{-1} - 1 \in P$. If so, return $(2, [\{u_n^{-1}w^{-1} - 1, w\}, X - (u_n^{-1}w^{-1} - 1)w - w, u_n^{-1}])$.*
3. *Check if $v^{-1}w^{-1} - 1 \in P$. If so, consider the following two cases:*
   (a) *If $v^{-1} \notin P$ return $(2, [\{v^{-1}w^{-1} - 1, w\}, X - (v^{-1}w^{-1} - 1)w - w, v^{-1}])$,*
   (b) *If $v^{-1} \in P$ then go back to Step 1 with $s = [u_1, \ldots, u_{n-1}]$.*
4. *Return $(3, [v^{-1}w^{-1} - 1, u_n^{-1}w^{-1} - 1, 1])$.*

Then for any given s the function $\phi_1(s,P)$ is a partial Krull functional in all such P as above.

Proof. The proof uses the computations which directly precede Lemma 6.5: We assume that $1 \in P$. For Step 1 we can assume that $n \geq 2$, else we would have $u_1^{-1} \notin P$ and $u_1^{-1} \in P$. In Step 2, if $u_n^{-1}w^{-1} - 1 \in P$ then $\{u_n^{-1}w^{-1} - 1, w\} \subseteq P$ and $X - (u_n^{-1}w^{-1} - 1)w + w = X - u_n^{-1}$ clearly works as output in this case. An entirely analogous argument deals with 3a. For 3b, from $v^{-1} = (u_1 + \ldots + u_{n-1})^{-1} \in P$ we can reason inductively: Note that we can still assume that $n-1 \geq 2$, since otherwise we would have $u_1^{-1} \in P$, a contradiction. The final case follows from $(u_n^{-1}w^{-1} - 1)(v^{-1}w^{-1} - 1) = 1 \in P$. □

Lemma 6.6. *Define the functional $\phi_2(s,P) \in \{0,1,2,3\} \times \mathbb{N}$ recursively on the length of $s := [u_1, \ldots, u_n]$ and for all P satisfying $1 \in P$, $u_i \neq 0$ for all i and $\forall_i \exists_j u_i \not\leq_P u_j$.:*

1. *Search for some $i \leq n$ such that $u_i \leq_P u_j$ for all $j < n$. If none exists, repeat this process with input $[u_1, \ldots, u_{n-1}]$ and P. Take also $k < n$ with $u_n \not\leq_P u_k$ (exists by the third property of P).*
2. *Check $u_n \not\leq_P u_i$ i.e. $u_i u_n^{-1} \notin P$. If so, return $(3, [u_i u_n^{-1}, u_n u_i^{-1}, 1])$.*
3. *Otherwise return $(2, [\{u_i u_n^{-1}, u_k u_i^{-1}\}, X - u_k u_i^{-1} \cdot u_i u_n^{-1}, u_k u_n^{-1}])$.*

Then for any $s := [u_1, \ldots, u_n]$ the function $\phi_2(s,P)$ is a partial Krull functional in all P with the three properties from above.

Proof. Let s and P be given with the properties as in the lemma. By Step 1, we can assume, that there is some $i \leq n$ with $u_i \leq_P u_j$ for all $j < n$. By the third property of P, we must have $u_i \not\leq_P u_n$. As $1 \in P$ and therefore $u_n \leq_P u_n$, there exists $k < n$ with $u_n \not\leq_P u_k$, where we again used the third property of P. If now $u_i u_n^{-1} \notin P$ then neither $u_i u_n^{-1}$ nor $u_i^{-1} u_n$ are in P and therefore P is not prime with witness $(u_i u_n^{-1})(u_i^{-1} u_n) = 1$ and so the output of Step 2 is justified. If $u_i u_n^{-1} \in P$ then $u_k u_i^{-1}, u_i u_n^{-1} \in P$ but $(u_k u_i^{-1})(u_i u_n^{-1}) = u_k u_n^{-1} \notin P$ so P cannot be an ideal, and this justifies the output in Step 3. □

Lemma 6.7. *For $0 \leq k \leq m$ and $0 \leq l \leq n$ define the functional $\phi(k,l,P)$ by the following algorithm.*

1. *Check if $c_i \notin P$ for some $i = 0, \ldots, m+n$. If so, return $(0, c_i)$.*
2. *Check if $1 \notin P$. If so, return $(2, [\emptyset, X - 1, 1])$.*
3. *Check if $a_k b_l \in P$. If so, return $(1, 0)$.*
4. *Search for the maximal i_0 such that $a_{i_0} \leq_P a_i$ for all i. If this doesn't exist, return $\phi_2([a_0, \ldots, a_m], P)$.*
5. *Search for the maximal j_0 such that $b_{j_0} \leq_P b_j$ for all j. If this doesn't exist, return $\phi_2([b_0, \ldots, b_n], P)$.*
6. *Check if $a_{i_0} b_{j_0} \in P$. If so, return*
   (a) $(2, [\{a_{i_0}^{-1} a_{j_0}^{-1} a_k b_l, a_{i_0} b_{j_0}\}, X - a_k b_l, a_k b_l])$ if $a_{i_0}^{-1} a_{j_0}^{-1} a_k b_l \in P$;
   (b) $(2, [\{a_k a_{i_0}^{-1}, b_l b_{j_0}^{-1}\}, X - a_{i_0}^{-1} b_{j_0}^{-1} a_k b_l, a_{i_0}^{-1} b_{j_0}^{-1} a_k b_l])$ otherwise.

7. *Check if* $c_{i_0+j_0} \neq 0$ *and* $a_{i_0}b_{j_0}c_{i_0+j_0}^{-1} \in P$. *If so, return* $(2, [\{c_{i_0+j_0}, a_{i_0}b_{j_0}c_{i_0+j_0}^{-1}\}, X - a_{i_0}b_{j_0}, a_{i_0}b_{j_0}])$.

8. *Check if* $-a_{i_0}b_{j_0}(a_ib_j)^{-1} \in P$ *for some* i, j *with* $i + j = i_0 + j_0$ *and either* $i > i_0$ *or* $j > j_0$.

   (a) *If* $i > i_0$ *and* $a_i \not\leq_P a_{i'}$ *(such an* i' *exists by maximality of* i_0*), return*

   $$(2, [\{-a_{i_0}b_{j_0}(a_ib_j)^{-1}, a_{i'}a_{i_0}^{-1}, b_jb_{j_0}^{-1}\}, X - a_{i_0}b_{j_0}(a_ib_j)^{-1} \cdot a_{i'}a_{i_0}^{-1} \cdot b_jb_{j_0}^{-1}, a_{i'}a_i^{-1}]).$$

   (b) *Analogously if* $j > j_0$ *and* $b_j \not\leq_P b_{j'}$.

9. *If* $c_{i_0+j_0} \neq 0$, *return* $\phi_1(c_{i_0+j_0}a_{i_0}b_{j_0}^{-1} :: s, P)$ *where* :: *is the list concatenation and the list* s *enumerates all elements* $-a_ib_j(a_{i_0}b_{j_0})^{-1}$ *for* $i + j = i_0 + j_0$ *but either* $i > i_0$ *or* $j > j_0$. *If* $c_{i_0+j_0} = 0$ *just return* $\phi_1(s, P)$.

Then for any k, l *the functional* $\psi_{\{c_0,\ldots,c_{m+n}\},a_kb_l}(P) := \phi(k, l, P)$ *is a Krull functional in* P *relative to* $F := \{c_0, \ldots, c_{m+n}\}$ *and* $r := a_kb_l$.

Proof. Cases 1-3 are clear, while for cases 4 and 5 we appeal to Lemma 6.6: The premise of the lemma holds for the a_i and b_i, respectively, in place of the u_i, since nonexistence of a maximal i_0 in particular means that there is no i with $a_i \leq_P a_j$ for all j, and similarly for j_0. From cases 6 onwards, we therefore may assume that i_0 and j_0 are maximal indices with the desired properties, namely $a_{i_0} \leq_P a_i$ for all $i \in \mathbb{N}$, but for $i > i_0$ we have $a_i \not\leq_P a_{i'}$ for some i', and similarly for j_0.

Case 6 follows by definition, noting that for (b) we have $\{a_ka_{i_0}^{-1}, b_lb_{j_0}^{-1}\} \subseteq P$ by the defining property of i_0, j_0, and case 7 is similarly straightforward. Now we have $a_{i_0}b_{j_0} \notin P$. For case 8 (a) we use in addition to maximality of i_0 and j_0 also that $a_{i_0} \leq_P a_{i'}$ and $b_{j_0} \leq_P b_j$, and analogously for (b).

For the final cases, we note that

$$1 = c_{i_0+j_0}(a_{i_0}b_{j_0})^{-1} + \sum_{\substack{i+j=i_0+j_0 \\ i\neq i_0 \\ j\neq j_0}} -a_ib_j(a_{i_0}b_{j_0})^{-1}.$$

If $c_{i_0+j_0} \neq 0$ then by the failure of case 7 we must have $a_{i_0}b_{j_0}c_{i_0+j_0}^{-1} \notin P$ and thus $c_{i_0+j_0}a_{i_0}b_{j_0}^{-1} :: s = [u_1, \ldots, u_p]$ where $(u_1 + \ldots + u_p)^{-1} = 1 \in P$ and for each q we have $u_q^{-1} \notin P$, where here we use the failure of case 8 that $a_{i_0}b_{j_0}(a_ib_j)^{-1} \notin P$ for $i > i_0$ or $j > j_0$. Thus the result follows from Lemma 6.5. If $c_{i_0+j_0} = 0$ then an analogous but simpler application of Lemma 6.5 does the trick. □

Corollary 6.8. *Let* E *be some subring of a field* S, *and* $a_0, \ldots, a_m, b_0, \ldots, b_n$ *be nonzero elements of* S *and* $c_k := \sum_{i+j=k} a_ib_j$. *Take some* k *and* l. *Suppose that the algorithm from Definition 4.7 is instantiated on the cover structure from Lemma 6.3 and the functional* $\psi_{\{c_0,\ldots,c_{m+n}\},a_kb_l}$ *defined in Lemma 6.7. Then the algorithm terminates in some state* π_k *from which we obtain* (A_k, p_k) *with* $A_k \subseteq \{c_0, \ldots, c_{m+n}\}$ *and* p_k *some monic polynomial with coefficients in* $E[A_k] \subseteq E[c_0, \ldots, c_{m+n}]$ *such that* $p(a_kb_l) = 0$.

Acknowledgements. The authors express their gratitude to the anonymous referees, whose detailed and insightful comments improved the paper considerably. In the case of the second author, the present study was carried out within the projects "A New Dawn of Intuitionism: Mathematical and Philosophical Advances" (ID 60842) funded by the John Templeton Foundation, and "Reducing complexity in algebra, logic, combinatorics - REDCOM" belonging to the programme "Ricerca Scientifica di Eccellenza 2018" of the Fondazione Cariverona. The second author is member of the Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni (GNSAGA) within the Italian Istituto Nazionale di Alta Matematica (INdAM), and the third author is Marie Skłodowska-Curie fellow of INdAM.[1]

References

[1] F. Aschieri and S. Berardi. Interactive learning-based realizability for Heyting arithmetic with EM1. *Logical Methods in Computer Science*, 6(3), 2010.

[2] B. Banaschewski and J. J. C. Vermeulen. Polynomials and radical ideals. *J. Pure Appl. Algebra*, 113(3):219–227, 1996.

[3] U. Berger. A computational interpretation of open induction. In *Proceedings of LICS 2004*, pages 326–334. IEEE Computer Society, 2004.

[4] J. Cederquist and T. Coquand. Entailment relations and distributive lattices. In *Logic colloquium '98. Proceedings of the annual European summer meeting of the Association for Symbolic Logic*, pages 127–139, 2000.

[5] T. Coquand. A note on the open induction principle. Technical report, Göteborg University, 1997.

[6] T. Coquand. Space of valuations. *Ann. Pure Appl. Logic*, 157:97–109, 2009.

[7] T. Coquand, L. Ducos, H. Lombardi, and C. Quitté. L'idéal des coefficients du produit de deux polynômes. *Revue des Mathématiques de l'Enseignement Supérieur*, 113(3):25–39, 2003.

[8] T. Coquand and H. Lombardi. A logical approach to abstract algebra. *Mathematical Structures in Computer Science*, 16(5):885–900, 2006.

[9] T. Coquand, H. Lombardi, and S. Neuwirth. Lattice-ordered groups generated by an ordered group and regular systems of ideals. *Rocky Mountain Journal of Mathematics*, 49(5):1449–1489, 2019.

[10] T. Coquand and H. Persson. Valuations and Dedekind's Prague theorem. *Journal of Pure and Applied Algebra*, 155(2-3):121–129, 2001.

[11] M. Coste, H. Lombardi, and M.-F. Roy. Dynamical method in algebra: Effective Nullstellensätze. *Annals of Pure and Applied Logic*, 111(3):203–256, 2001.

[1] The opinions expressed in this paper are those of the authors and do not necessarily reflect the views of those foundations and institutions.

[12] J. Della Dora, C. Dicrescenzo, and D. Duval. About a new method for computing in algebraic number fields. In *EUROCAL '85 European Conference on Computer Algebra*, volume 204 of *Lecture Notes in Computer Science*, pages 289–290. Springer, 1985.

[13] P. Hertz. Über Axiomensysteme für beliebige Satzsysteme. Teil II. Sätze höheren Grades. *Mathematische Annalen*, 89:76–102, 1923.

[14] A. Joyal. Les théoremes de Chevalley–Tarski et remarques sur l'algèbre constructive. *Cah. Topol. Géom. Différ. Catég.*, 16:256–258, 1976.

[15] U. Kohlenbach. *Applied Proof Theory: Proof Interpretations and their Use in Mathematics*. Monographs in Mathematics. Springer, 2008.

[16] U. Kohlenbach. Proof-theoretic methods in nonlinear analysis. In *Proc. ICM 2018*, volume 2, pages 79–100. World Scientific, 2019.

[17] G. Kreisel. On the interpretation of non-finitist proofs, Part I. *Journal of Symbolic Logic*, 16:241–267, 1951.

[18] G. Kreisel. On the interpretation of non-finitist proofs, Part II: Interpretation of number theory. *Journal of Symbolic Logic*, 17:43–58, 1952.

[19] H. Lombardi. Hidden constructions in abstract algebra (1): integral dependance. *Journal of Pure and Applied Algebra*, 167(2-3):259–267, 2002.

[20] H. Lombardi. Structures algébriques dynamiques, espaces topologiques sans points et programme de Hilbert. *Annals of Pure and Applied Logic*, 137(1–3):256–290, 2006.

[21] H. Lombardi and C. Quitté. *Commutative Algebra: Constructive Methods. Finite Projective Modules*, volume 20 of *Algebra and Applications*. Springer Netherlands, Dordrecht, 2015.

[22] R. Mines, F. Richman, and W. Ruitenburg. *A course in constructive algebra*. Springer Science & Business Media, 1988.

[23] C. Mulvey and J. Wick-Pelletier. A globalization of the Hahn–Banach theorem. *Adv. Math.*, 89:1–59, 1991.

[24] S. Negri. Proof analysis beyond geometric theories: from rule systems to systems of rules. *J. Logic Comput.*, 26(2):513–537, 2014.

[25] S. Negri and J. von Plato. Cut elimination in the presence of axioms. *Bull. Symb. Log.*, 4(4):418–435, 1998.

[26] S. Negri, J. von Plato, and T. Coquand. Proof-theoretical analysis of order relations. *Arch. Math. Logic*, 43:297–309, 2004.

[27] S. Neuwirth. Lorenzen's reshaping of Krull's Fundamentalsatz for integral domains (1938–1953). Preprint, available at `https://arxiv.org/abs/2007.08625`, 2020.

[28] P. Oliva and T. Powell. Spector bar recursion over finite partial functions. *Annals of Pure and Applied Logic*, 168(5):887–921, 2017.

[29] H. Persson. 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.

[30] T. Powell. Applying Gödel's Dialectica interpretation to obtain a constructive proof of Higman's lemma. In *Proceedings of Classical Logic and Computation '12*, volume 97 of *EPTCS*, pages 49–62, 2012.

[31] T. Powell. The equivalence of bar recursion and open recursion. *Annals of Pure and Applied Logic*, 165(11):1727–1754, 2014.

[32] T. Powell. Gödel's functional interpretation and the concept of learning. In *Proceedings of Logic in Computer Science (LICS '16)*, pages 136–145. ACM, 2016.

[33] T. Powell. On the computational content of Zorn's lemma. In *LICS '20: Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 768–781, 2020.

[34] T. Powell. A unifying framework for continuity and complexity in higher types. *Logical Methods in Computer Science*, 16(3):17:1 – 17:28, 2020.

[35] T. Powell. Well quasi-orders and the functional interpretation. In P. Schuster, M. Seisenberger, and A. Weiermann, editors, *Well-Quasi Orders in Computation, Logic, Language and Reasoning*, volume 53 of *Trends in Logic*, pages 221–269. Springer, 2020.

[36] T. Powell, P. Schuster, and F. Wiesnet. An algorithmic approach to the existence of ideal objects in commutative algebra. In *Proceedings of Wollic '19*, volume 11541 of *LNCS*, pages 533–549, 2019.

[37] J.-C. Raoult. Proving open properties by induction. *Information Processing Letters*, 29:19–23, 1988.

[38] F. Richman. Nontrivial uses of trivial rings. *Proc. Amer. Math. Soc.*, 103(4):1012–1014, 1988.

[39] D. Rinaldi and P. Schuster. A universal Krull-Lindenbaum theorem. *Journal of Pure and Applied Algebra*, 200:3207–3232, 2016.

[40] D. Rinaldi, P. Schuster, and D. Wessel. Eliminating disjunctions by disjunction elimination. *Bull. Symb. Logic*, 23(2):181–200, 2017.

[41] D. Rinaldi, P. Schuster, and D. Wessel. Eliminating disjunctions by disjunction elimination. *Indag. Math. (N.S.)*, 29(1):226–259, 2018.

[42] D. Rinaldi and D. Wessel. Extension by conservation. Sikorski's theorem. *Log. Methods Comput. Sci.*, 14(4:8):1–17, 2018.

[43] D. Rinaldi and D. Wessel. Cut elimination for entailment relations. *Arch. Math. Logic*, 58(5–6):605–625, 2019.

[44] G. Sambin. Intuitionistic formal spaces—a first communication. In D. Skordev, editor, *Mathematical Logic and its Applications, Proc. Adv. Internat. Summer School Conf., Druzhba, Bulgaria, 1986*, pages 187–204. Plenum, New York, 1987.

[45] K. Schlagbauer, P. Schuster, and D. Wessel. Der Satz von Hahn–Banach per Disjunktionselimination. *Confluentes Math.*, 11(1):79–93, 2019.

[46] P. Schuster. Formal Zariski topology: positivity and points. *Ann. Pure Appl. Logic*, 137(1–3):317–359, 2006.

[47] P. Schuster. Induction in algebra: a first case study. In *2012 27th Annual ACM/IEEE Symposium on Logic in Computer Science*, pages 581–585. IEEE Computer Society Publications, 2012. Proceedings, LICS 2012, Dubrovnik, Croatia.

[48] P. Schuster. Induction in algebra: A first case study. *Logical Methods in Computer Science*, 9(3:20):1–19, 2013.

[49] P. Schuster and D. Wessel. The computational significance of Hausdorff's maximal chain principle. In M. Anselmo, G. D. Vedova, F. Manea, and A. Pauly, editors, *Beyond the Horizon of Computability. 16th Conference on Computability in Europe*, volume 12098 of *Lect. Notes Comput. Sci.*, pages 239–250. Springer, 2020. Proceedings, CiE 2020, Fisciano, Italy, June 29–July 3, 2020.

[50] P. Schuster and D. Wessel. Resolving finite indeterminacy: a definitive constructive universal prime ideal heorem. In *Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS '20, pages 820–830, New York, NY, USA, 2020. Association for Computing Machinery.

[51] P. Schuster and D. Wessel. Radical theory of Scott-open predicates: the computational content of the Teichmüller–Tukey lemma. 2021. Preprint.

[52] P. Schuster, D. Wessel, and I. Yengui. Dynamic evaluation of integrity and the computational content of Krull's lemma. 2019. Preprint.

[53] D. Scott. Completeness and axiomatizability in many-valued logic. In L. Henkin, J. Addison, C. Chang, W. Craig, D. Scott, and R. Vaught, editors, *Proceedings of the Tarski Symposium (Proc. Sympos. Pure Math., Vol. XXV, Univ. California, Berkeley, Calif., 1971)*, pages 411–435. Amer. Math. Soc., Providence, RI, 1974.

[54] W. Simmons and H. Towsner. Proof mining and effective bounds in differential polynomial rings. *Advances in Mathematics*, 343:567–623, 2019.

[55] S. G. Simpson. *Subsystems of Second Order Arithmetic*. Perspectives in Mathematical Logic. Springer, Berlin, 1999.

[56] C. Spector. Provably recursive functionals of analysis: a consistency proof of analysis by an extension of principles in current intuitionistic mathematics. In F. D. E. Dekker, editor, *Recursive Function Theory: Proc. Symposia in Pure Mathematics*, volume 5, pages 1–27. American Mathematical Society, Providence, Rhode Island, 1962.

[57] A. Tarski. Fundamentale Begriffe der Methodologie der deduktiven Wissenschaften. I. *Monatsh. Math. Phys.*, 37:361–404, 1930.

[58] A. S. Troelstra. *Metamathematical Investigation of Intuitionistic Arithmetic and Analysis*, volume 344 of *Lecture Notes in Mathematics*. Springer, 1973.

[59] A. S. Troelstra and D. van Dalen. *Constructivism in Mathematics: an Introduction*, volume II of *Studies in Logic and the Foundations of Mathematics*. North-Holland, Amsterdam, 1988.

[60] D. Wessel. Ordering groups constructively. *Comm. Algebra*, 47(12):4853–4873, 2019.

[61] C. Xu. A syntactic approach to continuity of T-definable functionals. *Logical Methods in Computer Science*, 16(1), 2020.

[62] I. Yengui. Making the use of maximal ideals constructive. *Theoretical Computer Science*, 392:174–178, 2008.

[63] I. Yengui. *Constructive Commutative Algebra. Projective Modules over Polynomial Rings and Dynamical Gröbner Bases*, volume 2138 of *Lecture Notes in Mathematics*. Springer, Cham, 2015.