Dynamic evaluation of integrity and the computational content of Krull's lemma

Peter Schuster[a,*], Daniel Wessel[a], Ihsen Yengui[b]

[a] *Dipartimento di Informatica, Università degli Studi di Verona, Strada le Grazie 15, 37134 Verona, Italy*
[b] *Department of Mathematics, Faculty of Sciences of Sfax, University of Sfax, 3000 Sfax, Tunisia*

Abstract

A multiplicative subset of a commutative ring contains the zero element precisely if the set in question meets every prime ideal. While this form of Krull's Lemma takes recourse to transfinite reasoning, it has recently allowed for a crucial reduction to the integral case in Kemper and the third author's novel characterization of the valuative dimension. We present a dynamical solution by which transfinite reasoning can be avoided, and illustrate this constructive method with concrete examples. We further give a combinatorial explanation by relating the Zariski lattice to a certain inductively generated class of finite binary trees. In particular, we make explicit the computational content of Krull's Lemma.

Keywords: prime ideal, Krull dimension, valuative dimension, dynamical algebra, Zariski lattice, constructive mathematics
2010 MSC: 03F65

1. Introduction

In 2002 Lombardi [12] characterized constructively the Krull dimension of a commutative ring $\mathbf{A}$ by means of certain relations between the elements of $\mathbf{A}$. More precisely, he showed that for a positive integer n, we have $\dim(\mathbf{A}) < n$ if and only if any given elements $a_1, \ldots, a_n \in \mathbf{A}$ are *dependent* with respect to the lexicographic monomial order. This is to say that they satisfy a relation $P(a_1, \ldots, a_n) = 0$ where $P \in \mathbf{A}[X_1, \ldots, X_n]$ is such that $\mathrm{lc}_{\mathrm{lex}}(P) = 1$, i.e., the smallest monomial of P with respect to the lexicographic order lex has coefficient 1. For example, a ring $\mathbf{A}$ has dimension $\leqslant 0$ if and only if

$$(\forall x \in \mathbf{A})(\exists n \in \mathbb{N})(\exists a \in \mathbf{A})(x^n = ax^{n+1}). \tag{1}$$

Recently, Kemper and the third author [10] have obtained a constructive characterization of the valuative dimension, in the vein of Lombardi's characterization of the Krull dimension, only by replacing the lexicographic monomial order with the graded (reverse) lexicographic order or, in fact, with any graded rational monomial order.

Recall that the *valuative dimension* of a domain $\mathbf{A}$, denoted by $\dim_{\mathrm{v}}(\mathbf{A})$, is the supremum of the Krull dimensions of all overrings of $\mathbf{A}$, where an *overring* of $\mathbf{A}$ is a subring $\mathbf{B}$ of the quotient field $\mathrm{Quot}(\mathbf{A})$ of $\mathbf{A}$ such that $\mathbf{B} \supseteq \mathbf{A}$. As pointed out by Gilmer [7, Theorem 30.9], $\dim_{\mathrm{v}}(\mathbf{A}) \leqslant n$ if and only if $\dim(\mathbf{A}[t_1, \ldots, t_n]) \leqslant n$ for all $t_1, \ldots, t_n \in \mathrm{Quot}(\mathbf{A})$. In the case of an integral domain, this can be interpreted as a constructive characterization of the valuative dimension, and it is in fact the definition adopted by Lombardi and Quitté in the integral case [13]. If $\mathbf{A}$ is a ring which need not be a domain, $\dim_{\mathrm{v}}(\mathbf{A})$ is defined as the supremum of all $\dim_{\mathrm{v}}(\mathbf{A}/\mathfrak{p})$, where $\mathfrak{p}$ ranges over the class $\mathrm{Spec}(\mathbf{A})$ of prime ideals of $\mathbf{A}$ (see Jaffard [8, p. 56]).

*Corresponding author
Email addresses: peter.schuster@univr.it (Peter Schuster), daniel.wessel@univr.it (Daniel Wessel), ihsen.yengui@fss.rnu.tn (Ihsen Yengui)

In their aforementioned constructive characterization of the valuative dimension à la Lombardi, the only non-constructive argument that Kemper and the third author have employed is a reduction to the integral case. This goes as follows: fix a monomial order $<$ and consider, for any given $a_1, \ldots, a_n \in \mathbf{A}$, the multiplicative set

$$S := \{ P(a_1, \ldots, a_n) \mid P \in \mathbf{A}[X_1, \ldots, X_n] \text{ with } \mathrm{lc}_<(P) = 1 \} \subseteq \mathbf{A}.$$

Assume then that for every $\mathfrak{p} \in \mathrm{Spec}(\mathbf{A})$ the sequence $a_1, \ldots, a_n$ is $<$-dependent in $\mathbf{A}/\mathfrak{p}$, whence $S \cap \mathfrak{p} \neq \emptyset$. By a well-known non-constructive argument with Zorn's Lemma, this means $0 \in S$, which is to say that $a_1, \ldots, a_n$ are $<$-dependent in $\mathbf{A}$. To constructivize this is the initial motivation for the present note: we transform and reshape that non-constructive argument—in fact, any sufficiently concrete instance of the general method to show that a multiplicative subset S of a ring $\mathbf{A}$ contains 0 by showing that it meets any prime ideal of $\mathbf{A}$—into a constructive one.[1]

More specifically, we show that $0 \in S$ means that there is a finite binary tree labelled by finitely generated ideals such that S meets each of the ideals sitting at the leaves. The class of those trees, moreover, is inductively generated with the only branching rule corresponding to the characteristic axiom of ring without zero-divisors. We thus prove constructively a combinatorial version of Krull's Lemma [11] in the form that $0 \in S$ precisely when S meets every prime ideal.

On method and foundations

This note is written in Bishop-style constructive algebra [13, 14]. Its content can be formalized, e.g., in an appropriate fragment of Aczel's constructive set theory [1].

2. A dynamical solution

Recall that $\mathbf{A}$ is said to be *without zero-divisors* [13] if

$$(\forall a, b \in \mathbf{A})(ab = 0 \;\to\; a = 0 \vee b = 0).$$

Constructively, this is a special case of integrity. To carry over a proof from the case in which $\mathbf{A}$ is without zero-divisors to the general case of an *arbitrary* ring $\mathbf{A}$, start with $\mathbf{A} = \mathbf{A}/\langle 0 \rangle$. At each disjunction

$$a = 0 \;\vee\; b = 0,$$

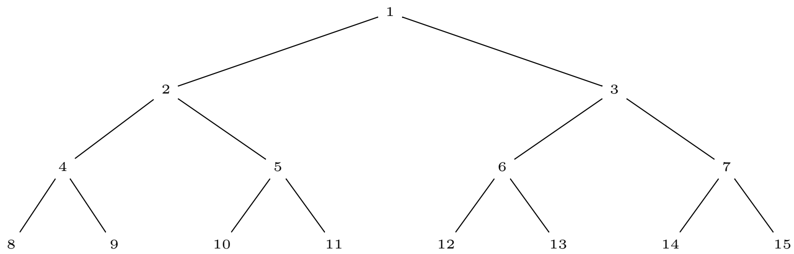
as given rise to by elements a, b such that $ab = 0$, and produced when computing in the integral case, replace the "current" ring $\mathbf{A}/\langle c_1, \ldots, c_r \rangle$ with $\mathbf{A}/\langle c_1, \ldots, c_r, a \rangle$ and $\mathbf{A}/\langle c_1, \ldots, c_r, b \rangle$, in each of which the computations can be carried on. Note that if

$$r \in S \cap \langle c_1, \ldots, c_r, a \rangle \text{ and } s \in S \cap \langle c_1, \ldots, c_r, b \rangle, \text{ then } rs \in S \cap \langle c_1, \ldots, c_r \rangle \tag{2}$$

as $ab = 0$. If the proof given modulo a generic prime ideal is sufficiently "uniform", then there is a bound for the depth of the (*a priori* infinite) binary tree we thus obtain. Hence the tree is finite and we get an algorithm. At the end of this rereading, a finite family of rings $(\mathbf{A}/\langle c_{1,j}, \ldots, c_{r_j,j} \rangle)_{1 \leqslant j \leqslant k}$ (rings at leaves) along with $s_j \in S \cap \langle c_{1,j}, \ldots, c_{r_j,j} \rangle$ will have been obtained, witnessing $0 = \prod_{1 \leqslant j \leqslant k} s_j \in S$ by construction of the tree, especially by (2).

To illustrate this in the case of the valuative dimension [10] recalled before, suppose that for $a_1, \ldots, a_n \in \mathbf{A}$, fixing a monomial order $<$, the tree produced by the dynamical method we have just sketched is the following, with depth 3:

[1] The overall strategy bears a certain resemblance to the third author's method to make the use of maximal ideals constructive [25, 26]. The later part of this note owes to the approach taken in dynamical algebra [6], has grown out of [18–20], and takes some clues from [24]. For a recent algorithmic approach to the existence of prime ideals in (countable) commutative rings we refer to [16].

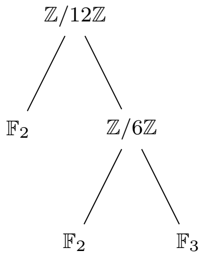


This means that at the leaves (corresponding to rings $\mathbf{A}/\langle c_{1,j}, c_{2,j}, c_{3,j}\rangle$) we have computed polynomials $P_j \in \mathbf{A}[X_1, \ldots, X_n]$ ($8 \leqslant j \leqslant 15$) such that $\mathrm{lc}_<(P_j) = 1$ and $P_j(a_1, \ldots, a_n) \equiv 0 \mod \langle c_{1,j}, c_{2,j}, c_{3,j}\rangle$. It follows that $P := \prod_{8 \leqslant j \leqslant 15} P_j$ vanishes at $a_1, \ldots, a_n$ with $\mathrm{lc}_<(P) = 1$, as desired.

3. Examples

Example 1. Consider 10 in the zero-dimensional ring $\mathbf{A} = \mathbb{Z}/12\mathbb{Z}$, and let us try to find $P \in \mathbf{A}[X]$ such that $P(10) = 0$ and $\mathrm{lc}_<(P) = 1$ (as in (1)) using the dynamical method described above.

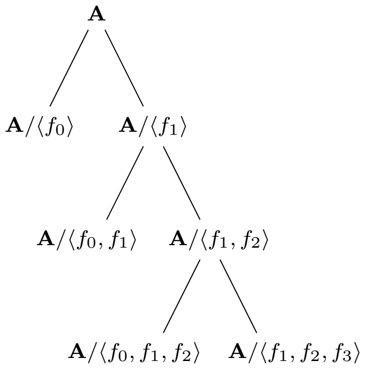
We will do as if $\mathbf{A}$ were integral (and thus a field), i.e., as if 12 were prime (its gcd with another integer is either 1 or 12). Computing $\gcd(12, 10) = 2 \notin \{1, 12\}$ yields a partial factorization $12 = 2 \times 6$. Hence $\mathbf{A}$ gets replaced with $\mathbf{A}_1 := \mathbf{A}/\langle 2\rangle \cong \mathbb{F}_2$ and $\mathbf{A}_2 := \mathbf{A}/\langle 6\rangle \cong \mathbb{Z}/6\mathbb{Z}$. Since $\mathbf{A}_1$ is a field, we are done: $P_1 = X$ is a solution to our problem ($10 = 0$ in this ring). Next continue with $\mathbf{A}_2$ as if 6 were prime. Computing $\gcd(6, 10) = 2 \notin \{1, 6\}$ yields a factorization $6 = 2 \times 3$. Now $\mathbf{A}_2$ gets replaced with $\mathbf{A}_3 := \mathbf{A}_2/\langle 2\rangle \cong \mathbb{F}_2$ and $\mathbf{A}_4 := \mathbf{A}_2/\langle 3\rangle \cong \mathbb{F}_3$. As before, a solution in $\mathbf{A}_3$ is $P_3 = X$. In the field $\mathbf{A}_4$ a solution is $P_4 = 1 - X$ (10 is invertible with inverse 1). We conclude that $P = P_1P_3P_4 = X^2(1 - X)$ is a solution to our problem. The dynamical evaluation tree we obtain is the following, at the three leaves of which 10 is either zero (two leaves) or invertible (one leaf).



Example 2. Let $\mathbf{A} = \mathbf{K}[\underline{x}] = \mathbf{K}[x_1, \ldots, x_n] = \mathbf{K}[X_1, \ldots, X_n]/I = \mathbf{K}[\underline{X}]/I$ be the coordinate ring of a zero-dimensional algebraic variety $V(I)$, where $I = \langle g_1, \ldots, g_s\rangle \subseteq \mathbf{K}[\underline{X}]$ and $\mathbf{K}$ is a field. The Krull dimension of $\mathbf{A}$ is zero.

Let us conceive an algorithm that for any $f_0(\underline{x}) \in \mathbf{A}$ finds a *collapse* as in (1), applying the dynamical method described above, combined with the fact that any nonzero element in $\mathbf{A}$ is either invertible or a zero-divisor. If $f_0(\underline{x}) = 0$ (that is, $f_0(\underline{X}) \in I$) or $f_0(\underline{x}) \in \mathbf{A}^\times$ (that is $1 \in \langle f_0(\underline{X}), g_1(\underline{X}), \ldots, g_s(\underline{X})\rangle$) then we are clearly done. Else compute an $f_1(\underline{x}) \in \mathbf{A} \setminus \{0\}$ such that $f_0(\underline{x})f_1(\underline{x}) = 0$ (this can be done via computing an element of $[I : \langle f_0(\underline{X})\rangle]$ which is not in I). Now the ring $\mathbf{A}$ gets replaced with $\mathbf{A}_1 := \mathbf{A}/\langle f_1(\underline{x})\rangle = \mathbf{K}[\underline{X}]/\langle f_1(\underline{X}), g_1(\underline{X}), \ldots, g_s(\underline{X})\rangle$ and $\mathbf{B}_1 := \mathbf{A}/\langle f_0(\underline{x})\rangle = \mathbf{K}[\underline{X}]/\langle f_0(\underline{X}), g_1(\underline{X}), \ldots, g_s(\underline{X})\rangle$. If $f_0(\underline{x}) = 0$ in $\mathbf{A}_1$ or $f_0(\underline{x}) \in \mathbf{A}_1^\times$ then we are done. Else compute $f_2(\underline{x}) \in \mathbf{A}_1 \setminus \{0\}$ such that $f_0(\underline{x})f_2(\underline{x}) = 0$, and so on. After a finite number of iterations (mind that $\mathbf{A}$ is Noetherian), we find $f_N(\underline{x}) \in \mathbf{A}$ such that either $f_0(\underline{x}) \in \langle f_1(\underline{x}), \ldots, f_N(\underline{x})\rangle$ or $f_0(\underline{x})$ is invertible modulo $\langle f_1(\underline{x}), \ldots, f_N(\underline{x})\rangle$. In the first case, the desired collapse in $\mathbf{A}$ is $f_0^{N+1} = 0$; in the second case, denoting by h the inverse of $f_0(\underline{x})$ modulo $\langle f_1(\underline{x}), \ldots, f_N(\underline{x})\rangle$, the desired collapse in $\mathbf{A}$ is $f_0^N(1 - hf_0) = 0$.

To give a concrete example, let $\mathbf{A} = \mathbb{Q}[x, y] = \mathbb{Q}[X, Y]/I$ be the coordinate ring of the algebraic variety $V(I)$ with $I = \langle X^2 - Y^2 - 1, X^4Y^2 - 2X^3Y^3 + Y^6 + Y^4 \rangle$. With Buchberger's algorithm we find $G = \{Y^4 + Y^2, X^2 - Y^2 - 1\}$ as reduced Gröbner basis for I according to the lexicographic order with $X > Y$. Thus, $\mathrm{LT}(I) = \langle Y^4, X^2 \rangle$ (the leading terms ideal of I), and the dimension of the variety $V(I)$ (which is also the Krull dimension of the ring $\mathbf{A}$) is zero since $\mathbf{A}$ has finite dimension as a $\mathbb{Q}$-vector space. Taking $f_0 = x^2y^2 + xy$, the obtained f_i's are: $f_1 = y^3 + y$, $f_2 = y^2 + 1$, and finally $f_3 = x$ with $f_0 \in \langle f_1, f_2, f_3 \rangle$. The desired collapse in $\mathbf{A}$ is $f_0^4 = 0$. It corresponds to the following binary tree, at all leaves of which f_0 is zero.



4. Zariski lattice and trees

In this final section we put the reduction trick once more under constructive scrutiny, yet from a slightly different angle. Let $\mathbf{A}$ again be a commutative ring. The *Zariski lattice* [2, 9] $\mathrm{Zar}(\mathbf{A})$ of $\mathbf{A}$ is the distributive lattice generated by symbols $D(a)$ for $a \in \mathbf{A}$, subject to the so-called *support relations*

$$D(0) = 0, \quad D(1) = 1, \quad D(ab) = D(a) \wedge D(b), \quad D(a + b) \leqslant D(a) \vee D(b).$$

For elements $b_1, \dots, b_n$ of $\mathbf{A}$ it is common to write $D(b_1, \dots, b_n)$ as a shorthand for $D(b_1) \vee \cdots \vee D(b_n)$. By way of the support relations, every element of $\mathrm{Zar}(\mathbf{A})$ can be written in the form $D(b_1, \dots, b_n)$ for suitable elements b_i of $\mathbf{A}$. What is sometimes known as the *formal Nullstellensatz* provides proper control over $\mathrm{Zar}(\mathbf{A})$ by asserting that [4]

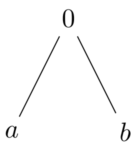
$$D(a) \leqslant D(b_1, \dots, b_n) \quad \text{if and only if} \quad a \in \sqrt{\langle b_1, \dots, b_n \rangle}. \tag{3}$$

Next we generate a collection $\mathcal{T}$ of finite binary trees T, the nodes of which are labelled with elements of $\mathbf{A}$. Given a path π of such a tree T, we write $\langle \pi \rangle$ for the ideal generated by the elements labelling the nodes of π. Similarly, $D(\pi)$ is meant to denote the join of the $D(a)$'s for labels a that occur along π. Note here that we understand paths to lead from the root of a tree to one of its leaves.

Definition 3. *We generate $\mathcal{T}$ inductively according to the following rules.*

1. *The trivial tree (i.e., the root-only tree) labelled with* 0 *belongs to* $\mathcal{T}$.
2. *If $a, b \in \mathbf{A}$ and $T \in \mathcal{T}$ has a path π such that $ab \in \langle \pi \rangle$, then the tree obtained from T by adding at the leaf of π two children labelled with a and b, respectively, also belongs to $\mathcal{T}$.*

For instance, any pair a, b such that $ab = 0$ yields a member of $\mathcal{T}$:



The dynamical method described in Section 2 generates trees which correspond to those in $\mathcal{T}$. Branchings, as given rise to by dynamic evaluation, can now be "folded up" by computation in $\mathrm{Zar}(\mathbf{A})$.

Lemma 4. *Let $\pi_1, \dots, \pi_n$ be the distinct paths of $T \in \mathcal{T}$. If $s_1, \dots, s_n \in \mathbf{A}$ are such that $D(s_i) \leqslant D(\pi_i)$ for $1 \leqslant i \leqslant n$, then $D(s_1 \cdots s_n) = 0$.*

Proof. By induction on the construction of $T \in \mathcal{T}$. The base case is trivial. Consider next the case in which T has been extended at the leaf of one of its paths π by children labelled with a and b, respectively, where $ab \in \langle \pi \rangle$. Suppose now that $r, s \in \mathbf{A}$ are such that $D(r) \leqslant D(\pi) \vee D(a)$ and $D(s) \leqslant D(\pi) \vee D(b)$. Distributivity and the third support relation imply that

$$D(rs) = D(r) \wedge D(s) \leqslant (D(\pi) \vee D(a)) \wedge (D(\pi) \vee D(b)) \leqslant D(\pi) \vee D(ab).$$

Since $D(ab) \leqslant D(\pi)$, it follows that $D(rs) \leqslant D(\pi)$, whence the induction hypothesis applies. □

Now let S be a multiplicative subset of $\mathbf{A}$, and let $T \in \mathcal{T}$. Let us say (for lack of a better term) that T *terminates in* S if, for every path π of T, we can find $s \in S$ for which $D(s) \leqslant D(\pi)$, which is to say that S meets $\langle \pi \rangle$.

This allows us to phrase, and prove constructively, the following combinatorial version of Krull's Lemma:

Proposition 5. *Let S be a multiplicative subset of $\mathbf{A}$. The following are equivalent.*

1. $0 \in S$.
2. *There is $T \in \mathcal{T}$ which terminates in S.*

Proof. If $0 \in S$, then the trivial tree terminates in S. Conversely, if $T \in \mathcal{T}$ terminates in S, then by Lemma 4 there is $s \in S$ such that $D(s) = 0$, which in view of (3) is tantamount to $0 \in S$. □

Remark 6. *Let $T \in \mathcal{T}$. For every prime ideal $\mathfrak{p}$ of $\mathbf{A}$ there is a path π through T such that $\mathfrak{p} \supseteq \langle \pi \rangle$.*

Proof. The path can be constructed by induction, keeping in mind that $0 \in \mathfrak{p}$ to begin with. Once the path has arrived at a certain node, the prime ideal axiom ensures that one of the successors can be added to the path so as to stay within $\mathfrak{p}$. □

In particular, if T terminates in S, then $\mathfrak{p}$ meets S for every prime ideal $\mathfrak{p}$. As recalled before, non-constructively this entails $0 \in S$. Proposition 5 thus underpins constructively the reduction method around which the present note revolves.

Last but not least, it is worth pointing out the resulting computational content of a variant of Krull's Lemma.

Corollary 7. *For every $a \in \mathbf{A}$, the following are equivalent.*

1. *a is nilpotent.*
2. *There is $T \in \mathcal{T}$ which terminates in $\{ a^n \mid n \in \mathbb{N} \}$.*

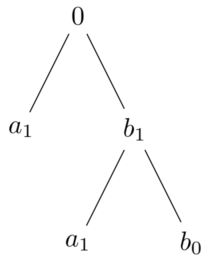
In particular, $\mathbf{A}$ is trival if and only if there is $T \in \mathcal{T}$ terminating in 1.

Proof. Direct consequence of Proposition 5. For the particular case, set $a = 1$. □

The litmus test for Corollary 7 is the well-known theorem that every nonconstant coefficient of an invertible polynomial is nilpotent.[2] On a case by case basis, this can indeed be read off a corresponding tree of coefficients, for which [21, 22] is instructive.

[2]This theorem, which admits an elegant proof by reduction to the integral case, has already seen many a constructive treatment in the literature, among which [3, 5, 15–17, 21, 22], as well as, most recently, [23], which the present note has given rise to.

Example 8. For sake of a simple illustration, let $f = a_0 + a_1X$ and $g = b_0 + b_1X$ in $\mathbf{A}[X]$, and suppose that $fg = 1$, which information amounts to $a_0b_0 = 1$ and $a_0b_1 + a_1b_0 = a_1b_1 = 0$. Branching out from the latter, and since $a_1b_0 \in \langle b_1 \rangle$, we obtain a corresponding member of $\mathcal{T}$:



Note that the rightmost path generates $\mathbf{A}$ as b_0 is invertible. Thus, according to Corollary 7, this tree tells us that a_1 is indeed nilpotent.

Acknowledgements

The present study was carried out within the project "A New Dawn of Intuitionism: Mathematical and Philosophical Advances" (ID 60842) funded by the John Templeton Foundation; the final version was then prepared within the project "Reducing complexity in algebra, logic, combinatorics - REDCOM" belonging to the programme "Ricerca Scientifica di Eccellenza 2018" of the Fondazione Cariverona. The authors Schuster and Wessel are members of the "Gruppo Nazionale per le Strutture Algebriche, Geometriche e le loro Applicazioni" (GNSAGA) of the Istituto Nazionale di Alta Matematica (INdAM).[3] Further financial assistance through the ICTP-INdAM "Research in Pairs"-programme is gratefully acknowledged. The third author's collaboration with Kemper at Technische Universität München, during which the impetus to the present note had been given, was supported by the Alexander-von-Humboldt Foundation. Numerous hints by the anonymous referees have helped to improve the presentation.

References

[1] Peter Aczel and Michael Rathjen. Notes on constructive set theory. Technical report, Institut Mittag–Leffler, 2000. Report No. 40.

[2] Bernhard Banaschewski. Radical ideals and coherent frames. *Comment. Math. Univ. Carolin.*, 37(2):349–370, 1996.

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

[4] Jan Cederquist and Thierry Coquand. Entailment relations and distributive lattices. In Samuel R. Buss, Petr Hájek, and Pavel Pudlák, editors, *Logic Colloquium '98. Proceedings of the Annual European Summer Meeting of the Association for Symbolic Logic, Prague, Czech Republic, August 9–15, 1998*, volume 13 of *Lect. Notes Logic*, pages 127–139. A. K. Peters, Natick, MA, 2000.

[5] Thierry Coquand, Lionel Ducos, Henri Lombardi, and Claude Quitté. L'idéal des coefficients du produit de deux polynômes. *Revue des Mathématiques de l'Enseignement Supérieur*, 113(3):25–39, 2003.

[6] Michel Coste, Henri Lombardi, and Marie-Françoise Roy. Dynamical method in algebra: Effective Nullstellensätze. *Ann. Pure Appl. Logic*, 111(3):203–256, 2001.

[7] Robert Gilmer. *Multiplicative Ideal Theory.* Marcel Dekker, New York, 1972.

[8] Paul Jaffard. *Théorie de la Dimension dans les Anneaux de Polynomes.* Mémor. Sci. Math., Fasc. 146. Gauthier-Villars, Paris, 1960.

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

[10] Gregor Kemper and Ihsen Yengui. Valuative dimension and monomial orders. *J. Algebra*, 557:278–288, 2020.

[11] Wolfgang Krull. Idealtheorie in Ringen ohne Endlichkeitsbedingung. *Math. Ann.*, 101:729–744, 1929.

[12] Henri Lombardi. Dimension de Krull, Nullstellensätze et évaluation dynamique. *Math. Zeitschrift*, 242:23–46, 2002.

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

[14] Ray Mines, Fred Richman, and Wim Ruitenburg. *A Course in Constructive Algebra.* Springer, New York, 1988. Universitext.

[3]The opinions expressed in this paper are those of the authors and do not necessarily reflect the views of the John Templeton Foundation.

[15] Henrik 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.

[16] Thomas Powell, Peter Schuster, and Franziskus Wiesnet. An algorithmic approach to the existence of ideal objects in commutative algebra. In R. Iemhoff and M. Moortgat, editors, *26th Workshop on Logic, Language, Information and Computation (WoLLIC 2019), Utrecht, Netherlands, 2–5 July 2019, Proceedings*, volume 11541 of *Lect. Notes Comput. Sci.*, pages 533–549, Berlin, 2019. Springer.

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

[18] Davide Rinaldi and Peter Schuster. A universal Krull–Lindenbaum theorem. *J. Pure Appl. Algebra*, 220:3207–3232, 2016.

[19] Davide Rinaldi, Peter Schuster, and Daniel Wessel. Eliminating disjunctions by disjunction elimination. *Bull. Symb. Logic*, 23(2):181–200, 2017.

[20] Davide Rinaldi, Peter Schuster, and Daniel Wessel. Eliminating disjunctions by disjunction elimination. *Indag. Math. (N.S.)*, 29(1):226–259, 2018.

[21] Peter 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.

[22] Peter Schuster. Induction in algebra: a first case study. *Log. Methods Comput. Sci.*, 9(3):20, 2013.

[23] Peter Schuster and Daniel Wessel. Resolving finite indeterminacy: A definitive constructive universal prime ideal theorem. In *Proceedings of the 35th Annual ACM/IEEE Symposium on Logic in Computer Science*, LICS 20, page 820830, New York, NY, USA, 2020. Association for Computing Machinery.

[24] Daniel Wessel. A note on connected reduced rings. *J. Comm. Algebra*, 2019. Forthcoming. URL: `https://projecteuclid.org/euclid.jca/1561363253`.

[25] Ihsen Yengui. Making the use of maximal ideals constructive. *Theoret. Comput. Sci.*, 392:174–178, 2008.

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