Resolving Finite Indeterminacy

A Definitive Constructive Universal Prime Ideal Theorem

Peter Schuster[1]
Daniel Wessel[2]

[1]Dipartimento di Informatica, Università di Verona
[2]Mathematisches Institut, Universität München

partially based on joint work with
Giulio Fellin, Verona, and Ihsen Yengui, Sfax

BLAST, NMSU, Las Cruces, 9–13 June 2021

in memoriam Ray Mines, 1938-2013

Situation

Abstract algebra abounds with *ideal objects* and the invocations of *transfinite methods*, typically Zorn's Lemma, that grant those objects' existence. From a logical point of view, this means to invoke *model extension* for proving indirectly the *semantic conservation* of additional *non-deterministic sequents*, that is, with finite but not necessarily singleton succedents.

Dynamical methods in algebra (Coste–Lombardi–Roy, Coquand, Yengui et al.) allow to eliminate the ideal objects by shifting focus from semantic model extension to *syntactical conservation*. This partial realisation of *Hilbert's programme* has shaped modern constructive algebra, not least because *coherent logic* predominates in algebraic settings: the use of a non-deterministic axiom corresponds to a *finite branching* of the proof tree. Coherent theories lend themselves to *automated theorem proving* (Bezem, Coquand et al.)

Krull's Lemma

A paradigmatic case—hitherto somewhat neglected in dynamical algebra—is *Krull's Lemma*: a multiplicative subset R of a commutative ring meets a given ideal $\mathfrak{a}$ if and only if R meets every prime ideal $\mathfrak{p} \supseteq \mathfrak{a}$. Prompted by a novel treatment of valuative dimension (Kemper–Yengui 2019), Krull's Lemma has seen a constructive treatment only recently (Sch.–W.–Yengui 2019). The latter has brought us to eventually unearth the underlying general phenomenon:

Given a claim of computational nature usually proved by the semantic conservation of non-deterministic axioms, there is a finite labelled tree in an inductively generated class which tree encodes the desired computation.

Our result works in the fairly universal setting of *abstract consequence relations* $\rhd$ (Hertz, Tarski, Scott, Coquand, et al.), which here serve to capture the *basic structures* (ideals/filters, logical theories, partial orders, etc.) on top of which certain *non-deterministic axioms* describe the *ideal objects* refining those structures (prime ideals/filters, complete theories, linear orders, etc.).

Achievements

Decisive will be the notion of a *regular set* for non-deterministic axioms over a fixed consequence relation. Abstracted from the multiplicative subsets of Krull's Lemma, regular sets calibrate precisely the gearing of our *Universal Prime Ideal Theorem* UPIT, and account for its constructive version CUPIT.

We thus *uniformise* many of the known instances of the dynamical method, and *generalise* the proof-theoretic conservation criterion (Rinaldi–Sch.–W. 2017–18) for entailment relations à la Gentzen–Lorenzen–Scott, which in turn unifies numerous phenomena present in the literature (extension as conservation).

As compared to dynamical algebra, CUPIT is not only constructive but also *definitive* and *universal*: by passing to the logical setting of consequence we unearth the one *common pattern* of how the related trees are to be grown. Our approach is ready for use in customary *mathematical practice* without any need to adapt first the axioms, which would be not untypical for dynamical algebra. Last but not least, we identify regularity as both *sufficient* and *necessary* for (C)UPIT, and link the *syntactical* with the *semantic* approach: every ideal object can be approximated by a branch of the appropriate tree.

Deterministic consequence

Unless specified otherwise as occasion demands, we work in in (a fragment of) Constructive Zermelo–Fraenkel Set Theory **CZF** (Aczel, Rathjen).

A *consequence relation* on a set S is a relation $\rhd$ between finite subsets and elements of S, which is *reflexive, monotone* and *transitive*:

$$\frac{U \ni a}{U \rhd a}\ (\mathrm{R}) \qquad \frac{U \rhd a}{U, V \rhd a}\ (\mathrm{M}) \qquad \frac{U \rhd b \quad U, b \rhd a}{U \rhd a}\ (\mathrm{T})$$

where the usual shorthand notations are in place. The *ideals* of a consequence relation are the subsets $\mathfrak{a}$ of S which are *closed* under $\rhd$: that is, if $\mathfrak{a} \supseteq U$ and $U \rhd a$, then $a \in \mathfrak{a}$. If U is a finite subset of S, then its closure

$$\langle U \rangle = \{\, a \in S \mid U \rhd a \,\}$$

is an ideal, and so is, more generally, the closure of an arbitrary subset T of S:

$$\langle T \rangle = \{\, a \in S \mid (\exists U \subseteq T)\, U \rhd a \,\}$$

Hence $\rhd$ is nothing but an *algebraic closure operator* $\langle \_ \rangle$ on the subsets of S:

$$T \rhd a \equiv \langle T \rangle \ni a$$

Think of $T \rhd a$ as "T proves a", "T generates a" or the like.

Finite indeterminacy

By a *non-deterministic axiom* on a set S we understand a pair (A, B) of finite subsets of S, and often write $A \vdash B$. A subset $\mathfrak{p}$ of S is *closed* under $A \vdash B$ whenever $A \subseteq \mathfrak{p}$ implies $\mathfrak{p} \between B$: that is, $\mathfrak{p}$ and B have an element in common.

Let $\mathcal{E}$ be a set of non-deterministic axioms, and $\rhd$ a consequence relation on a set S. A *prime ideal* is an ideal of $\rhd$ that is closed under every element of $\mathcal{E}$.

For instance, if $\rhd$ denotes deduction, and $\mathcal{E}$ consists of all pairs $(\emptyset, \{ \varphi, \neg\varphi \})$ or, alternatively, $\vdash \varphi, \neg\varphi$, then the (prime) ideals are the (complete) theories.

We say that a subset R of S is *regular* if for every $A \vdash B$ in $\mathcal{E}$

$$\frac{(\forall b \in B)\, \langle U, b \rangle \between R}{\langle U, A \rangle \between R}$$

and that $r \in S$ is *regular* if so is $\{ r \}$, i.e. for every $a_1, \dots, a_k \vdash b_1, \dots, b_\ell$ in $\mathcal{E}$

$$\frac{U, b_1 \rhd r \quad \dots \quad U, b_\ell \rhd r}{U, a_1, \dots, a_k \rhd r}$$

All $r \in S$ are regular iff every $a_1, \dots, a_k \vdash b_1, \dots, b_\ell$ in $\mathcal{E}$ is conservative over $\rhd$.

Semantic conservation

On a set S, let $\mathcal{E}$ be a set of non-deterministic axioms, and $\triangleright$ a consequence relation. The following is an abstraction of the usual proof of Krull's Lemma.

Lemma *Let $R \subseteq S$ be regular and let $\mathfrak{a}$ be an ideal. In **ZFC**, if $R \cap \mathfrak{a} = \emptyset$, then there is a prime ideal $\mathfrak{p} \supseteq \mathfrak{a}$ such that $R \cap \mathfrak{p} = \emptyset$.*

In fact, if R is regular, then every ideal which is maximal among those avoiding R is prime. It is necessary for this that R be regular.

Universal Prime Ideal Theorem (UPIT) *In **ZFC**, a subset R of S is regular if and only if for every ideal $\mathfrak{a}$ we have $R \between \mathfrak{a}$ precisely when $R \between \mathfrak{p}$ for all prime ideals $\mathfrak{p} \supseteq \mathfrak{a}$.*

UPIT is a form of the Axiom of Choice, equivalent in **ZF** to the Prime Ideal Theorem for distributive lattices; and UPIT entails Restricted Excluded Middle.

Trees for computation

Given an ideal $\mathfrak{a}$, we define inductively a collection $T_{\mathfrak{a}}$ of *finite* labelled trees such that the root of every $t \in T_{\mathfrak{a}}$ be labelled with a finite subset U of $\mathfrak{a}$, and the non-root nodes with elements of S.

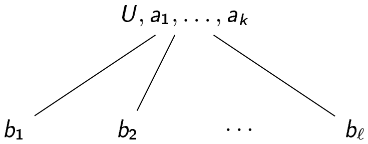
We understand paths, which necessarily are finite, to lead from the root of a tree to one of its leaves. Given a path π of $t \in T_{\mathfrak{a}}$, we write $\pi \triangleright a$ whenever $U, b_1, \dots, b_n \triangleright a$ where U labels the root of t and $b_1, \dots, b_n$ are the labels occurring at the non-root nodes of π. We define $T_{\mathfrak{a}}$ inductively as follows:

1. For every finite $U \subseteq \mathfrak{a}$, the trivial tree (i.e., the root-only tree) labelled with U belongs to $T_{\mathfrak{a}}$.
2. If $A \vdash B$ is in $\mathcal{E}$ and if $t \in T_{\mathfrak{a}}$ has a path π such that $\pi \triangleright a$ for every $a \in A$, then add, for every $b \in B$, a child labelled with b at the leaf of π.

Paths for prime ideals

As in dynamical algebra, the given ideal $\mathfrak{a}$ can be thought as a set of initial data, of which just a finite amount U be used for computation; with this we label the root. The paths of a tree $t \in T_{\mathfrak{a}}$ then represent the possible courses of a computation which proceed *as if* the ideal $\mathfrak{a}$ were prime.

For instance, if $a_1, \ldots, a_k \vdash b_1, \ldots, b_\ell$ is in $\mathcal{E}$ and U is a finite subset of S, then the following tree is in $T_{\langle U, a_1, \ldots, a_k \rangle}$:



Proposition *Let $\mathfrak{a}$ be an ideal, and $t \in T_{\mathfrak{a}}$ a tree. For every prime ideal $\mathfrak{p} \supseteq \mathfrak{a}$ there is a path π in the tree t such that $\mathfrak{p} \supseteq \langle \pi \rangle$.*

The paths of $t \in T_{\mathfrak{a}}$ thus are finite approximations of the prime ideals $\mathfrak{p} \supseteq \mathfrak{a}$.

Syntactical conservation

We say that a tree $t \in T_{\mathfrak{a}}$ *terminates* in $R \subseteq S$ if for *every* (!) path π of t there is $r \in R$ such that $\pi \triangleright r$. E.g., $R \between \mathfrak{a}$ iff some trivial tree in $T_{\mathfrak{a}}$ terminates in R.

The following lemma goes by induction on the construction of the tree $t \in T_{\mathfrak{a}}$.

Lemma *Let $R \subseteq S$ be regular and let $\mathfrak{a}$ be an ideal. If some $t \in T_{\mathfrak{a}}$ terminates in R, then $R \between \mathfrak{a}$.*

Constructive Universal Prime Ideal Theorem (CUPIT) *A subset R of S is regular if and only if for every ideal $\mathfrak{a}$ we have $R \between \mathfrak{a}$ precisely when there is a tree $t \in T_{\mathfrak{a}}$ which terminates in R.*

By reading “(prime) ideal” literally, one instantiates CUPIT as a constructive version of Krull's Lemma for commutative rings, with paths in place of prime ideals. This version is ready to use for proving constructively the facts of computational nature for which one would normally do an indirect proof with Krull's Lemma for prime ideals, i.e. the corresponding instance of UPIT.

But of course this is by far not the only application . . .

A relatively simple case, with (complete) theories as (prime) ideals as alluded to above, yields (a variant of) Lindenbaum's Lemma for propositional logic and Glivenko's Theorem as instances of UPIT and CUPIT, respectively.

Trees for classical proofs by cases

Let $\vdash_i$ and $\vdash_c$ stand for intuitionistic and classical logic in a propositional language S. For any given $\Gamma \cup \{\varphi\} \subseteq S$ it is known that $\Gamma \vdash_c \varphi$ precisely when

$$\Gamma, \psi_1 \vee \neg\psi_1, \ldots, \psi_k \vee \neg\psi_k \vdash_i \varphi$$

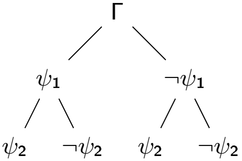
where $\psi_1, \ldots, \psi_k$ are the propositional variables occurring in $\Gamma \cup \{\varphi\}$.

Let $\rhd = \vdash_i$ on S and consider on top of $\rhd$ the non-deterministic axiom of excluded middle, i.e., let $\mathcal{E}$ consist of all the $\vdash \psi, \neg\psi$ with $\psi \in S$.

For simplicity's sake we only do the case $k = 2$. If $\Gamma \vdash_c \varphi$ means

$$\Gamma, \psi_1 \vee \neg\psi_1, \psi_2 \vee \neg\psi_2 \vdash_i \varphi\,,$$

then the following tree belongs to $T_{\langle\Gamma\rangle}$ and terminates in φ:



If, in addition, φ is regular, then $\Gamma \rhd \varphi$, i.e. $\Gamma \vdash_i \varphi$, by CUPIT.

But which formulas are regular?

Lemma *A formula* φ *is regular if and only if it is* stable: *that is,* $\neg\neg\varphi \vdash_i \varphi$.

We thus regain from CUPIT the following version of a time-honoured result:

Glivenko's Theorem *If* φ *is a stable formula, then*

$$\Gamma \vdash_c \varphi \Longrightarrow \Gamma \vdash_i \varphi \, .$$

Needless to say, proofs of Glivenko's theorem usually go along similar lines.

But what has Glivenko's Theorem to do with transfinite methods?

The above variant is the syntactical core of the following form of UPIT:

Proposition *In **ZFC**, if* φ *is a stable formula, then*

$$\varphi \in \bigcap \{\Theta \subseteq S : \Theta \text{ complete theory} \supseteq \Gamma\} \implies \Gamma \vdash_i \varphi \, .$$

This implies a variant (Fellin–Sch.–W. 2019) of another time-honoured result:

Lindenbaum's Lemma *In **ZFC**,*

$$\bigcap \{\Theta \subseteq S : \Theta \textit{ complete theory} \supseteq \Gamma\} = \{ \varphi \in S \mid \Gamma \vdash_i \neg\neg\varphi \} \, .$$

J. Cederquist and T. Coquand. Entailment relations and distributive lattices. In S. R. Buss, P. Hájek, and P. 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.

M. Coste, H. Lombardi, and M.-F. Roy. Dynamical method in algebra: Effective Nullstellensätze. *Ann. Pure Appl. Logic*, 111(3):203–256, 2001.

G. Fellin, P. Schuster, and D. Wessel. The Jacobson radical of a propositional theory. 2019. Submitted.

V. Glivenko. Sur quelques points de la Logique de M. Brouwer. *Acad. Roy. Belg. Bull. Cl. Sci. (5)*, 15:183–188, 1929.

G. Kemper and I. Yengui. Valuative dimension and monomial orders. *J. Algebra*, 557:278–288, 2020.

W. Krull. Idealtheorie in Ringen ohne Endlichkeitsbedingung. *Math. Ann.*, 101:729–744, 1929.

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

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

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

D. Rinaldi, P. Schuster, and D. Wessel. Eliminating disjunctions by disjunction elimination. *Indag. Math. (N.S.)*, 29(1):226–259, 2018. Communicated first in *Bull. Symb. Logic* 23 (2017), 181–200.

P. Schuster and D. 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, pages 820–830, New York, NY, USA, 2020. Association for Computing Machinery.

P. Schuster, D. Wessel, and I. Yengui. Dynamic evaluation of integrity and the computational content of Krull's lemma. *J. Pure Appl. Algebra*, 226(1), 2022. paper 106794, available online 17 May 2021.

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

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