Ideal Objects for Finite Methods

Peter Schuster
Department of Pure Mathematics, University of Leeds

Constructive Mathematics: Foundation and Practice
Faculty of Mechanical Engineering, University of Niš
24–28 June 2013

What About

Partial realisation in algebra (Coquand, Lombardi)
of a revised Hilbert Programme (Kreisel, Feferman)

— Get rid of 'ideal objects':
handle subsets with care, work predicatively

— Get by with 'finite methods':
do constructive proofs, use intuitionistic logic

— Work rather locally than globally:
consider single theories, individual theorems

Putative principal obstacle: the Axiom of Choice
Widely considered as obscuring computational information

Zorn's Lemma allegedly is 'constructively neutral' (J.L. Bell)
In fact it frequently occurs within a proof by contradiction

Let's turn such proofs upside down: use Open Induction instead
Ultimate goal: reduction of transfinite to finite methods

Mathematical Induction

Consider complementary $S, T \subseteq \mathbb{N}$

$0 \in S \,\&\, \forall n\,(n \in S \rightarrow n + 1 \in S) \rightarrow S = \mathbb{N}$

$\forall n\,[\forall m < n\ (m \in S) \rightarrow n \in S] \rightarrow S = \mathbb{N}$

If $T \neq \emptyset$, then T has a least element

$\mathbb{N}$ *well-ordered*

Well-Founded Induction

X partial order; $U, V \subseteq X$ complementary

$\forall x\,[\forall y < x\ (y \in U) \rightarrow x \in U] \rightarrow U = X$

If $V \neq \emptyset$, then V has a minimal element

X *well-founded*

well-ordered = well-founded + totally ordered

Transfinite Induction: along the ordinal numbers, a well-ordered class

In practice, quite a few partial orders are well-founded, also called *Noetherian*

Induction on any set whatsoever: with the **Well-Ordering Theorem**

WO *Every set can be well-ordered*

Stated by Cantor 1883 as a *Denkgesetz:* a law of thought

Reduced by Zermelo 1904 to the **Axiom of Choice AC**

Some History

Induction on sets well-ordered by WO soon became utterly popular
Prime example: algebraic closure of an abstract field (Steinitz 1910)

"*The theorems of Steinitz concerning algebraic closure . . . are barred, from the algebraic point of view, by the well-ordering theorem*" (Zorn 1935)

"*questionable set-theoretic reasoning in algebra*" (van der Waerden 1937)

"*AC is utterly acceptable . . . I would hate to accept WO as an axiom.*"
(Kaplansky 1972)

More History

Zorn's Lemma (1935; Kuratowski 1922; Teichmüller 1939; Tukey 1940)

"make the proofs shorter and more algebraic" (Zorn 1935)

"remplace avantageusement le théorème de Zermelo" (Bourbaki 1951)

"durch erheblich kürzere Schlußweisen zu ersetzen gestattet" (Witt 1951)

"quite simply, a useful piece of order theory" (Leinster 2012)

Open Induction (Raoult 1988): sometimes an improvement ...

Zorn's Lemma

Let X be a *directed-complete* partial order, for short a *dcpo*: i.e., every directed (and non-empty) subset $D \subseteq X$ has a sup $\bigvee D$ in X

A subset V of X is *closed* à la Zorn if, for every directed $D \subseteq X$,

$$D \subseteq V \to \bigvee D \in V$$

Zorn's Lemma reads as follows:

ZL *If V is closed and $V \neq \emptyset$, then V has a maximal element*

Classical Equivalent of ZL

If V is closed and V is unbounded, then $V = \emptyset$

Here V is *unbounded* if, for every $x \in X$,

$$x \in V \rightarrow \exists y > x \, (y \in V)$$

This is to say that V has no maximal element

Open Induction

A subset U of X is *open* à la Scott if, for every directed $D \subseteq X$,

$$\bigvee D \in U \to D \between U$$

Open Induction can be put as follows:

OI *If U is open and progressive, then $U = X$*

Here U is *progressive* if, for every $x \in X$,

$$\forall y > x\, (y \in U) \to x \in U$$

With U and V as complements, OI and ZL are classically equivalent

Classical Equivalence of OI and ZL

If $U \cup V = X$ and $U \cap V = \emptyset$, then

— $U = X$ if and only if $V = \emptyset$
— U is open if and only if V is closed
— U is progressive if and only if V is unbounded

OI If U is open and U is progressive, then $U = X$
ZL If V is closed and V is unbounded, then $V = \emptyset$

First Case Study: a Lemma due to Gauß

Let f, g be polynomials with coefficients in a commutative ring R with 1
This R need not be a reduced ring, let alone an integral domain

$$f = a_0+a_1T+a_2T^2+\ldots+a_nT^n\,, \quad g = b_0+b_1T+b_2T^2+\ldots+b_mT^m$$

Fix $0 < \overline{\imath} \leqslant n$, set $u = a_{\overline{\imath}}$, and consider a lemma on *nilpotent coefficients*

$$\textbf{NC} \quad fg = 1 \rightarrow \exists e\,(u^e = 0)$$

The hypothesis of NC is a finite conjunction of atomic formulas

$$a_0b_0 = 1\,,\ a_0b_1 + a_1b_0 = 0\,,\ \ldots\,,\ a_nb_m = 0$$

The logical form is simple, an elementary proof of NC must be possible

Why Bother

"... [NC] admits an elegant proof upon observing that each a_i with $i \geqslant 1$ must be in every prime ideal of R, and that the intersection of the prime ideals of R consists of the nilpotent elements of R. This proof gives no clue as to how to calculate n such that $a_i^n = 0$, while such a calculation can be extracted from the proof that we present." (Richman 1988)

"Nontrivial uses of trivial rings" yield a constructive proof (Richman 1988)
There anyway is a fully elementary proof, sometimes a textbook exercise
Formal topology: constructive interpretation of elegant proof (Persson 1999)
We equally extract the the exponent, keeping close to the elegant proof

Elegant Proof

The specific case is straightforward in which R is an *integral domain*:

$$xy = 0 \rightarrow x = 0 \vee y = 0$$

In this case, in particular, if $u^e = 0$, then already $u = 0$

The general case can be reduced to this particular case

To this end, work modulo any *prime ideal* P of R:

$$xy \in P \rightarrow x \in P \vee y \in P$$

An ideal P of R is prime iff the quotient ring R/P is an integral domain

Hence $u = 0$ in R/P or, equivalently, $u \in P$ for all prime ideals P of R

So one arrives at

$$fg = 1 \to \forall P\,(u \in P)$$

To get to NC one now uses the contrapositive

$$\textbf{KL} \quad \forall P\,(u \in P) \to \exists e\,(u^e = 0)$$

of what is usually called **Krull's Lemma**

$$\forall e\,(u^e \neq 0) \to \exists P\,(u \notin P)$$

This however is an instance of Zorn's Lemma

This route is 'short and elegant' but it does have defects,
both from a foundational and a pragmatic perspective:

— Zorn's Lemma is invoked without real need
— sweeping quantification over ideal objects P
— unnecessary use of proof by contradiction
— considerable loss of computational information
— gives no clue of how to compute the exponent e

But the hypothesis of NC carries more information than the one of KL

Direct Proof

With OI one can give a direct proof of KL
If R is Noetherian, then OI is unnecessary

To prove NC one can even get by with **Finite Induction**

FI *If X is finite, and U is progressive, then $U = X$*

where for a partial order X to be *finite* includes that $\leqslant$ be decidable

FI is fairly basic, only requires mathematical induction

To prove NC with FI, follow the route from OI to KL,
and apply the same manipulations as in the elegant proof

During the proof it turns out that one can stay within the given problem: take X to be the set (!) consisting of the ideals generated by some of the

$$a_1, \ldots, a_n, b_1, \ldots, b_m$$

Any element of X can be represented by a binary list of length $n + m$

Alongside the proof of NC by FI one can grow a finite tree
This encodes an algorithm to compute some e with $u^e = 0$
Enough computational information has been preserved

By basic proof theory the decidability assumptions can be eliminated: Gödel–Gentzen, Dragalin–Friedman, continuation translation; Gentzen's *Hauptsatz* (Ishihara, Leivant, Nadathur, Negri, Orevkov, Palmgren, Strahm)

Sketch of Direct Proof of NC with FI

X: the ideals H that are generated by some a_i, b_j with $i, j > 0$

$\exists e\,(u^e = 0)$? $\quad 0 = \bot_X \quad \bot_X \in U$? $\quad H \in U \equiv \exists e\,(u^e \in H)$

U upwards closed $\quad U$ progressive? $\quad$ Take any $H \in X$

Assume that $\forall G \in X\ (G > H \rightarrow G \in U)$ $\quad$ To prove: $H \in U$

Case 1 $\forall i > 0\ (a_i \in H) \quad u \in H \quad e = 1 \quad H \in U$

Case 2 $\exists i > 0\ (a_i \notin H)$ $\quad$ Then also $\exists j > 0\,(b_j \notin H)$

Pick i, j maximal

$$H \ni c_{i+j} = \underbrace{\sum_{q>j} a_p b_q}_{\in H} + a_i b_j + \underbrace{\sum_{p>i} a_p b_q}_{\in H} \qquad a_i b_j \in H$$

We have $a_i \notin H$ $b_j \notin H$ $a_i b_j \in H$

$K = H + Ra_i$ $L = H + Rb_j$ $K, L \in X$

$K, L \supsetneqq H$ $K \cap L = H + Ra_i b_j = H$

$K, L \in U$ by induction $u^k \in K$, $u^\ell \in L$

$u^{k+\ell} \in K \cap L = H$ $e = k + \ell$ $H \in U$ $\square$

This proof has revealed a pattern that can be detected in various proofs

Growing a Tree

Construct recursively a binary tree of elements of X as follows

— Define the root as $\perp_X$

— Assume that a node H has just been constructed.

Case 1 Declare H to be a leaf

Case 2 Endow H with the two children $H \vee a_i$ and $H \vee b_j$

Every branch is strictly increasing; whence the tree is finite

A node belongs to U if it is a leaf or if both children belong to U

Hence, by induction on the construction, the root $\perp_X$ belongs to U

The tree encodes the computation of e with $u^e = 0$ from $fg = 1$

Related Approaches

Open Induction for lexicographic orders (U. Berger, Coquand)
Nontrivial uses of trivial rings (Richman)

Dynamical methods in algebra (Coste, Roy, Lombardi)
Formal topology, specially the Basic Picture (Sambin)

Two-level foundations with forget-restore option (Maietti, Sambin)
Ideal objects for real mathematics—if conservative (Sambin)

Current Work

— Wiener's $1/f$ Theorem with(out) Gelfand theory (with M. Hendtlass)
— ZL and OI as reducibility and spatiality (with D. Rinaldi, G. Sambin)
— Further ideal objects: valuation rings, orders on fields (with D. Rinaldi)
— First-order completeness: Henkin sets (with F. Ciraulo, N. Gambino)
— The proof pattern: universal Krull–Lindenbaum (with D. Rinaldi)
— Eliminating maximal ideals from proofs in algebra (with S. Huber)
— Towards a systematic, syntactic treatment of ZL $\rightsquigarrow$ OI (with U. Berger)

References

Bell, J.L., Zorn's lemma and complete Boolean algebras in intuitionistic type theories. *J. Symb. Log.* 62 (1997) 1265–1279

Berger, U., A computational interpretation of open induction. In: F. Titsworth, ed., *Proceedings of the Nineteenth Annual IEEE Symposium on Logic in Computer Science (LICS), Turku, Finland, July 2004.* IEEE Computer Society Press (2004) 326–334

Coquand, T., Constructive topology and combinatorics.
In: J. Myers, M. O'Donnell, eds., *Constructivity in Computer Science*.
Springer *Lecture Notes in Computer Science* 613 (1992) 28–32

Coquand, T., A note on the open induction principle. Chalmers Institute of Technology and Göteborg University (1997)

Coquand, T. and H. Lombardi, A logical approach to abstract algebra.
Math. Struct. in Comput. Science 16 (2006) 885–900

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

Crosilla, L. and P. Schuster, Finite methods in mathematical practice.
In: M. Detlefsen, G. Link, eds., *Formalism and Beyond.* Ontos, Heusenstamm, 201?

Hendtlass, M. and P. Schuster, A direct proof of Wiener's theorem. In S. B. Cooper, A. Dawar, B. Löwe, eds., *How the World Computes. Turing Centenary Conference and Eighth Conference on Computability in Europe*, volume 7318 of *Lect. Notes Comput. Sci.*, pages 294–303, Berlin and Heidelberg, 2012. Springer. Proceedings, CiE 2012, Cambridge, UK, June 2012.

Maietti, M.E., A minimalist two-level foundation for constructive mathematics. *Ann. Pure Appl. Logic* 160(3): 319–354, 2009.

Maietti, M.E. and G. Sambin, Toward a minimalist foundation for constructive mathematics. In L. Crosilla, P. Schuster, editors, *From Sets and Types to Topology and Analysis*, volume 48 of *Oxford Logic Guides*, pages 91–114. Oxford: Oxford University Press, 2005.

Persson, H., An application of the constructive spectrum of a ring. In H. Persson, *Type Theory and the Integrated Logic of Programs*. PhD thesis. Chalmers University and University of Göteborg, 1999.

Raoult, J.-C., Proving open properties by induction. *Inform. Process. Lett.* 29 (1988) 19–23

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

Sambin, G., Steps towards a dynamic constructivism. In P. Gardenfors et al., editor, *In the Scope of Logic, Methodology and Philosophy of Science*, volume 315 of *Synthese Library*, pages 263–286, Dordrecht, 2002. Kluwer. 11th International Congress of Logic, Methodology and Philosophy of Science. Krakow, Poland, August 1999.

Sambin, G., Some points in formal topology.
Theoret. Comput. Sci., 305(2003), 347–408

Sambin, G., Real and ideal in constructive mathematics. In *Epistemology versus ontology*, volume 27 of *Log. Epistemol. Unity Sci.*, pages 69–85. Springer, Dordrecht, 2012.

Schuster, P., 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, June 2012.