FORMAL TOPOLOGY AND PROOF THEORY

Thierry Coquand

Prague, August 1998

Proof Theory

Infinitary methods are often used to give elegant derivations of purely combinatorial statement.

1. topological dynamics; for instance van der Waerden's theorem: use that an endomap on a compact space has a minimal invariant subspace, then instanciate it to $\{0, 1\}^Z$, and deduce the theorem by compactness,

2. Ramsey theorem: use a non principal ultrafilter (which selects the colour "most often used") to prove the infinite version; then deduce the finite version by compactness,

3. Wiener's theorem on invertible series: use the notion of spectrum of a commutative Banach algebra to prove that a serie has an inverse.

Question: is it possible to give constructive meaning to such proofs? Do they have any computational content?

Formal Topology

Most of infinitary arguments use topological spaces:

- the space $\{0, 1\}^Z$,
- compact subspace of a compact space,
- spectrum of a commutative ring or of a Banach algebra,

and show the existence of suitable points of these space.

The non effective aspect of these arguments is often concentrated in these non constructive existence (often reduced to the axiom of choice in the form of Zorn's lemma).

Menger has suggested a more concrete approach to topology (topology without points): use only $observable$ notions.

Claim: using formal topology, we can make constructive sense of some infinitary reasoning. Often, these interpretations can be carried out in a proof-theoretically weak meta-language.

We shall give constructive meaning also of non combinatorial statements such as Hahn-Banach's theorem.

Some History of Formal Topology

Whitehead (around 1910); then exposed and further analysed by Russell, Wiener and Nicod. For instance, they analyse how to define the (ideal) notion of points in time from the notion of events.

Weyl (1921) M.Z., 10: inspired by Brouwer, a point-free presentation of the real line and a sketch of a point-free definition of manifolds. ("Ueber die neue Grundlagenkrise der Mathematik".)

Stone (around 1935): equivalence of Boolean algebra and totally disconnected compact spaces.

Menger (1940) "Topology without Points"; survey of previous attempts, "all the physicist can observe are pieces of space, and the individual points are merely given as the result of approximations".

de Bruijn, van der Meiden (1967): point-free analysis of the spectrum of a Banach algebra.

Theory of locales (around 1970): difference between locale and spaces; connections with the theory of choice sequences.

Martin-Löf, Sambin started a systematic development of these notions in Type Theory. Allows applications to proof theory.

Example: Boolean Algebra

Stone's representation theorem gives a kind of dictionary between topological (infinitary) notions and algebraic (finitary) notions.

- a space becomes an algebra,
- a continuous map becomes an algebraic morphism,
- an open subset becomes an ideal,
- $\{0, 1\}^N$ becomes the (Tarksi-)Lindenbaum algebra of propositional logic,
- the product becomes the tensor product.

Compare the

- $semantical$ and
- $syntactical$

compactness of propositional calculus.

Formal Space

A *formal space* will be given by a set S of (concrete) objects representing basic neighbourhood.

An open U will be a subset of S (in term of points, the union of its element).

We need to define when an open U is *covered* by another open V. We write it $U \lhd V$.

The "complexity" of the space can be measured by the complexity of this covering relation $\lhd$. It can be defined in a constructive (often weak) meta-language.

Opens form a complete Heyting algebra. We can consider *topological models* where truth-values are (formal) open sets of the space S. Concretely this corresponds to defining a forcing relation bewteen basic neighbourhoods and formulae.

Two examples of Formal Spaces

In this talk, I will limit myself to:

Sambin's representation of complete boolean algebra: S is a meet-semi lattice with a downward closed subset Z. Defines an orthogonality relation: $x \perp y$ iff $xy \in Z$. Then $U \lhd V$ means $V^{\perp} \subseteq U^{\perp}$.

Distributive lattices: if S is a distributive lattice, defines $U \lhd V$ by $x \leq v_1 \vee \ldots \vee v_k$ for some $v_1, \ldots, v_k \in V$ for any $x \in U$. (Variation: compact Hausdorff spaces using *regular* lattices.)

I: Minimal Invariant Spaces

We have a compact space X (Hausdorff) with a endomap $f : X \to X$. There exists a minimal compact non empty $K \subseteq X$ such that $f(K) \subseteq K$.

Such a subset does not exist constructively.

If X totally disconnected, such a formal space is a boolean algebra B, and f is represented by an endomorphism $g : B \to B$. The subset K is represented by a predicate on B.

It is possible to define Z the set of "empty" basic open, directly: $x \epsilon Z$ iff there exists k such that $xg(x) \ldots g^k(x) = 0$.

We can build *effectively* a minimal invariant subspace in a suitable topological model. This gives a constructive meaning to the topological proof of van der Waerden's theorem.

II: Some Classical Systems

Let EL_1 be the system with quantifications over functions and natural numbers, with only primitive recursion, and only Σ_1^0 induction.

It is not possible to interpret $EL_1 + EM$ in EL_1 by negative translation.

Take the semi-lattice of functions $f : N \rightarrow N$ with $T(f) = (\exists n)[f(n) = 0]$ and $f \leq g$ defined as $T(g) \Rightarrow T(f)$. Define Z the subset of f such that $T(f)$ holds.

We have a topological model (over a complete boolean algebra) which gives a model of $EL_1 + EM$.

This can be rewritten as a direct interpretation of $EL_1 + EM$ into EL_1. (Hence conservativity of $I\Sigma_1^0$ over primitive recursive arithmetic.)

(with Martin Hofmann) A proof that if an existential statement is provable in PV^ω then it is provable in IPV^ω.

Lattices and Entailment Relations

Dana Scott has introduced the notion of *entailment relation*. See "Completeness and Axiomatizability in Many-Valued Logic", Tarski Symposium.

Abstract presentation of Gentzen's multi-conclusion sequent calculus.

A set S (of abstract sentences) and a binary relation $\vdash$ between finite subsets of S such that

$$\mathcal{A} \vdash \mathcal{B} \; if \; \mathcal{A} \cap \mathcal{B} \neq \emptyset \tag{R}$$

$$\frac{\mathcal{A} \vdash \mathcal{B}}{\mathcal{A}, \mathcal{A}' \vdash \mathcal{B}, \mathcal{B}'} \tag{M}$$

$$\frac{\mathcal{A} \vdash s, \mathcal{C} \qquad \mathcal{A}, s \vdash \mathcal{C}}{\mathcal{A} \vdash \mathcal{C}} \tag{T}$$

Here, we denote by $\mathcal{A}, \mathcal{B}, \mathcal{C}, \ldots$ arbitrary finite subsets of S. We write $\mathcal{A}, \mathcal{B}$ for $\mathcal{A} \cup \mathcal{B}$ and $\mathcal{A}, s$ for $\mathcal{A} \cup \{s\}$.

Read $x_1, \ldots, x_n \vdash y_1, \ldots, y_m$ as $x_1 \ldots x_n \leq y_1 \vee \ldots \vee y_m$.

Quite suggestive way of defining distributive lattices (hence formal spaces).

Spectrum of a ring

Let A be a commutative ring. Define

$$x_1, \ldots, x_n \vdash y_1, \ldots, y_m$$

as "the product $y_1 \ldots y_m$ is in the radical of the ideal generated by $x_1, \ldots, x_n$."

This is an *entailment relation*.

This defines hence a distributive lattice, hence a formal space, which corresponds to the space of prime ideals (spectrum).

$$x_1, \ldots, x_n \vdash y_1, \ldots, y_m$$

can be read as

$$if\ x_1 \in P\ and\ \ldots\ and\ x_n \in P\ then\ y_1 \in P\ or\ \ldots\ or\ y_m \in P$$

This is a form of elimination of choice sequences.

Dual Space

Let E be a normed space. We let $Fn\ E$ be the space of linear form over E of norm ≤ 1.

Take $S = Q \times E$ and define

$$p_1 < x_1, \ldots, p_n < x_n \vdash q_1 < y_1, \ldots, q_m < y_m$$

as "there exists $r_i \geq 0$, $s_j \geq 0$ and $r \geq 0$ z of norm ≤ 1 such that $r + \Sigma r_i > 0$ and

- $\Sigma r_i x_i + rx = \Sigma s_j y_j$ and
- $\Sigma r_i p_i - r = \Sigma s_j q_j$.

This defines an entailment relation. Hence a distributive lattice (which is regular). This defines a formal space, which is compact Hausdorff and is $Fn\ E$.

This means

$$if\ p_1 < u(x_1)\ and\ \ldots\ and\ p_n < u(x_n)\ then$$
$$q_1 < u(y_1)\ or\ \ldots\ or\ q_m < u(y_m)$$

Application: direct proof of the localic Hahn-Banach (and a new proof of the classical version).

The elements of S have a suggestive interpretation: what we can *observe* of a linear form.

General Theme: associate entailment relations to mathematical structures (linear space, ring, fields).

Reverse Mathematics

Compare to S. Simpson "Partial Realizations of Hilbert's Programs", JSL 53, 1988; some examples

- Heine-Borel,
- Hahn-Banach, Alaoglu, for separable Banach spaces
- Prime ideals for countable commutative rings.

Furthermore, axioms are justified as being "different ways of affirming the existence of enough points in continuous media."

These theorems are proved in a theory conservative over PRA for Π^2_0 statements.

Here the point-free version of compactness of $Fn\ E$ or Hahn-Banach can be carried out in very weak meta-language.

All the "proof-theoretic work" is contained in the establishing the connection with the pointwise versions (which here amounts to the fact that regular compact locales have enough points).

Conclusion

Formal topology allows for a constructive interpretation of some mathematical notions used in

- infinitary combinatorics: some topological dynamics,
- algebra: spectrum, valuations,
- functional analysis: Hahn-Banach theorem, spectrum of a commutative Banach algebra.

When interpreted in this way, some theorems get a direct and elementary proofs. These interpretations can be used as well for any concrete applications.

"Relative view": the truth-values are open of a space, that can itself vary.

One question: how to represent non separable spaces and non continuous maps (examples of Hindman's theorem)?