Some contributions of Lorenzen to constructive mathematics

Thierry Coquand

Konstanz, 8 March 2018

Lorenzen as a mathematician

The school of mathematics in Germany between the two wars was truly exceptional (Noether, Herglotz, Artin, Schmidt, Krull, Hasse, ...)

See e.g. P. Roquette's survey on *The Riemann hypothesis in characteristic* p which describes in particular the importance of the work of Hasse

Lorenzen was Hasse's student

Lorenzen as a mathematician

A new feature was the use of highly non effective methods in *algebra*

At working with the uncountable, in particular with the well-ordering theorem, I always had the feeling that one uses fictions there that need to be replaced some day by more reasonable concepts. But I was not getting upset over it, because I was convinced that at a careful application of the common "fictions" nothing false comes out, and because I was firmly counting on the man who would some day put all in order. Lorenzen has now found according to my conviction the right way...

Krull (letter to Scholz, 1953)

Lorenzen as a mathematician and a logician

Lorenzen was also aware of works in logic, in particular the work of Gentzen

He was able to connect his work in algebra (lattice theory, Dedekind) with proof theory

Lorenzen as a mathematician and a logician

Connections between lattice theory and logic were known but connections between lattice theory and *proof theory* were quite original (except for the previous work of Skolem)

Theorem: *A lattice is* distributive *if, and only if, it satisfies the (cut) rule*

$$\frac{a \wedge c \leqslant b \qquad a \leqslant b \vee c}{a \leqslant b}$$

Implicit in *Algebraische und logistische Untersuchungen über freie Verbände*, Journal of Symbolic Logic 1951

Lorenzen's analysis of Gentzen's work

Gentzen's consistency proof is presented as a proof about an infinitary calculus showing that the cut rule is *admissible* ("zulässing")

Two highly original features

(1) The metatheory is *constructive* allowing generalised inductive definitions

(2) no ordinal analysis

At about the same time, and independently, P.S. Novikov had a similar analysis, and also introduced the notion of admissible/derivable rule

Lorenzen's analysis of Gentzen's work

Apart from Novikov, most treatments in proof theory (Gentzen, Schütte) involve ordinal analysis

From a *constructive* point of view (and for me personally) the purely inductive presentation is much clearer

For stronger calculus, one can even argue that the ordinal analysis is a diversion (cf. Kreisel's review of Takeuti's proof which explains that ordinal diagrams are well-founded in an intuitionistic theory of inductive definitions)

Lorenzen's analysis of Gentzen's work

To allow generalized inductive defined objects in a constructive setting was highly original

Lorenzen-Myhill *Constructive Definition of Certain Analytic Sets* 1959 goes beyond "predicative" mathematics (cf. analysis of Cantor-Bendixson Theorem)

Apart from Novikov, the only example I could find are proofs in *Notes on Constructive Mathematics*, P. Martin-Löf, 1968, but there, infinitary objects are not represented directly but only via coding as recursively enumberable sets (which arguably obscures the main ideas)

Lorenzen's logic

Lorenzen and Myhill's paper analyses different ways to define subsets of natural numbers

They introduce the following stratification

Lorenzen's logic

1. By explicit definition, quantifying only over natural numbers.

2. By inductive definition, quantifying only over natural numbers.

3. By explicit definition, quantifying only over the (denumerable) totality of sets previously obtained.

4. By inductive definition, with the same restriction on quantifiers.

5. By uninhibited use of function-quantifiers.

Lorenzen's logic

Use of generalized inductive definitions (4) is presented as the "method of Lorenzen" *Einführung in die operative Logik und Mathematik*, Berlin 1955, with the comment that this "exhausts those means of definition at present known which are acceptable from a standpoint which rejects the actual infinite"

The last method (5) is impredicativity which has no constructive justification

Lorenzen's logic

This analysis is quite similar to the one of Martin-Löf for instance in the paper *The Hilbert-Brouwer controversy resolved?* (2008)

We have a calculus of inductively defined objects and inductive proofs/recursively defined functions on these objects

Lorenzen's logic

For instance we describe inductively natural numbers by two production rules

$$\to \quad | \qquad\qquad x \quad \to \quad x\,|$$

We describe inductively the equality

$$\to \quad | = | \qquad\qquad x = y \quad \to \quad x\,| = y\,|$$

Lorenzen's logic

It is then direct that

$$| = x | \quad \rightarrow \quad \bot$$

is provable (inversion principle)

This is used extensively for expressing and proving properties of semantics of programming language (natural semantics, G. Kahn) in interactive proof systems

Just to give an example, the paper *Über endliche Mengen*, Math. Annalen 1951 could almost be written as it is in proof systems for type theory

Lorenzen's logic

In 1992, we noticed that this inversion principle corresponds to the notion of *pattern-matching* in functional programming. This provides a convenient notation for inductive proofs (this is closely connected to the work of L. Hallnäs and P. Shroeder-Heister on definitional reflection)

More recent works in this direction are N. Zeilberger's PhD thesis (2008) and J. Cockx Ph.D. thesis (2017)

Proof theoretic analysis of point-free spaces

An *entailment relation* is a relation $a_1, \ldots, a_n \vdash b_1, \ldots, b_m$ between finite subsets of an abstract set such that

(1) $X \vdash Y$ if X and Y intersect

(2) $X \vdash Y$ if $X' \vdash Y'$ and $X' \subseteq X$ and $Y' \subseteq Y$

(3) $X \vdash Y$ if $X, a \vdash Y$ and $X \vdash Y, a$

Entailment relation is the key notion for presenting distributive lattice/spectral spaces in an elegant way

This notion already appears in Lorenzen 1951 paper

Proof theoretic analysis of point-free spaces

On a given domain R, we want an entailment relation which describes the (spectral) space of valuation of R

If $x_1, \ldots, x_n$ are elements in the fraction field of R we write $(x_1, \ldots, x_n)$ the R-module generated by $x_1, \ldots, x_n$

$$a_1, \ldots, a_n \vdash b_1, \ldots, b_m \quad \leftrightarrow \quad 1 \in \Sigma_{i>0}(a_1 b_1^{-1}, \ldots, a_n b_m^{-1})^i$$

In term of valuation rings, this expresses that any valuation ring (containing R) containing all a_i contains at least one b_j

For instance $a \vdash b$ holds if, and only if, b is integral over a

Proof theoretic analysis of point-free spaces

Die Erweiterung halbgeordneter Gruppen zu Verbandsgruppen Math. Zeitschr. 1953

Rediscovered in *Valuations and Dedekind's Prague Theorem* (C., Persson 1998) but Lorenzen's analysis is much more perspicious

Key lemma

For any R*-module* I *if* 1 *in* $I[c]$ *and in* $I[c^{-1}]$ *then* 1 *in* I

Proof theoretic analysis of point-free spaces

Example: Cantor space

As a set of points: set Ω of infinite binary sequences $\omega = \omega_0, \omega_1, \omega_2, \ldots$

As a point-free space: Boolean algebra of propositional logic, i.e. the Boolean algebra freely generated by countably many formal atoms written $\omega_k = 1$ (of formal complement $\omega_k = 0$)

E.g. $\omega_1 = 0 \wedge \omega_3 = 1$ represents a compact open subset of Ω, namely all sequences ω such that $\omega_1 = 0$ and $\omega_3 = 1$

An *open* subset of Ω corresponds to an *ideal* of C

Proof theoretic analysis of point-free spaces

Cantor-Bendixson

Logical Reflection and Formalism, Journal of Symbolic Logic, 1958

If U represents an open set of Cantor space in a point free way, so that U is an ideal on the corresponding Boolean algebra C, then the complement F of U (as a set of points) is a closed set

Lorenzen explains how to define, by a *generalized* inductive definition, a new ideal which corresponds to the kernel of F

This result is used in Kreisel's analysis of Cantor-Bendixson (1959)

Proof theoretic analysis of point-free spaces

If for each n we enumerate the 2^n elements $b_{i_0 \ldots i_{n-1}} = \omega_0 = i_0 \wedge \cdots \wedge \omega_{n-1} = i_{n-1}$ one possible way to inductively define the extension S of U is

-b is in S if b is in U

-b is in S if for each n, at least $2^n - 1$ elements $b \wedge b_{i_0 \ldots i_{n-1}}$ are in S

We see that this is a *generalised* inductive definition

Proof theoretic analysis of point-free spaces

The same paper

Logical Reflection and Formalism, Journal of Symbolic Logic, 1958

contains a key remark explaining how formulae involving universal quantification on sets of natural numbers can be interpreted by a generalised inductive definition

$\forall X\ (X(3) \to X(3))$ is valid since $X(3) \to X(3)$ is valid, where X is a *variable*

Measure theory

Lorenzen (1951) was able to describe the σ-complete Boolean algebra generated by a given Boolean algebra

More generally, given an entailment relation $E, \vdash$ he builds a σ-complete Boolean algebra B with an interpretation $v : E \to B$ universal for this property, and then show

$$a_1, \ldots, a_n \vdash b_1, \ldots, b_m \quad \leftrightarrow \quad v(a_1) \wedge \cdots \wedge v(a_n) \leqslant v(b_1) \vee \cdots \vee v(b_m)$$

This result is cited in Beth's book "Foundations of Mathematics"

Measure theory

If we start from the Boolean algebra C of *propositional logic* which is the Boolean algebra generated from countably many atoms we get a σ-complete Boolean algebra B

C can be seen as a point-free presentation of *Cantor space*, which is the set Ω of all infinite binary sequences $\omega = \omega_0, \omega_1, \ldots$

B can be seen as a point-free presentation of the σ-complete Boolean algebra of *Borel sets* on Cantor space

This was noticed by P. Martin-Löf *Notes on Constructive Mathematics*

Borel sets

A Borel set X is given inductively:

-X is a propositional formula or

-X is of the form $\bigvee_n X_n$ or

-X is of the form $\bigwedge_n X_n$

Lorenzen defines a sequent calculus $X_1, \ldots, X_n \vdash Y_1, \ldots, Y_m$ and proves that the cut-rule is admissible

Borel sets

We can define $X \subseteq Y$ by $X \vdash Y$

We have $X \subseteq X$ and $X \subseteq Z$ if $X \subseteq Y$ and $Y \subseteq Z$

We can define the formal complement X' of X and we have $\vdash X, X'$ by induction on X

Borel sets

An example is the set of *normal* binary sequences $\bigwedge_k \bigvee_m \bigwedge_{n \geqslant m} b_{n,k}$ with $b_{n,k}$ a point-free representation of

$$\{\ \omega \in \Omega \mid\ -\frac{1}{k} \leqslant \frac{\Sigma_{i<n}(2\omega_i - 1)}{n} \leqslant \frac{1}{k}\ \}$$

In the classical approach this is thought of as a set of points (the complement of which is not countable and of measure 0)

Here it is a purely symbolic expression (which should be of measure 1)

Measure theory

If we start from the Boolean algebra with two elements we get the σ-complete Boolean algebra of *hyperarithmetical propositions*

Borel's measure problem

Borel sets can be described inductively

Can we define the measure $\mu(X)$ of a Borel set X by induction on X?

Borel's own formulation: we design a formal theory which describes how the measure should work, and we have to prove that this formal theory is *consistent*

This is actually a *coherence problem*: we have to show that

$$X \vdash Y \;\rightarrow\; \mu(X) \leqslant \mu(Y)$$

Borel's measure problem

Lusin in his book "Leçons sur les Ensembles Analytiques et leurs Applications" asked for a purely inductive solution of this problem

The usual definition of measure (Lebesgue, Daniell, Bourbaki) goes *beyond* inductive reasonings

Here I explain how to define recursively $r < \mu(X)$ as a *hyperarithmetical* proposition by induction on X

We take the usual measure on Cantor space: if X is a propositional formula $\mu(X)$ is a rational and $r < \mu(X)$ is 0 or 1

E.g. $\mu(\omega_1 = 0 \wedge \omega_3 = 1) = 1/4$

Borel's measure problem

For instance if we define

$$X_{n+1} = \wedge_{i<n}[\omega_i = 0] \wedge [\omega_n = 1]$$

$$X_0 = \bigwedge_k [\omega_k = 0]$$

we have $1 = \bigvee_n X_n$

and $\mu(1) = 1$ and $\mu(X_0) = 0$ and $\mu(X_{n+1}) = 1/2^{n+1}$

$$1 = 0 + 1/2 + 1/4 + \ldots$$

Borel's measure problem

Main difficulty: how to define $r < \mu(X)$ if X is a disjunction or conjunction?

One solution is provided by F. Riesz *Sur la décomposition des opérations fonctionnelles linéaires* (1928)

We instead define recursively $r < \mu(b \wedge X)$ for each propositional formula b

We introduce a new relation $r < \mu(X, b)$ which represents $r < \mu(b \wedge X)$

This can be defined inductively on X and we recover $r < \mu(X)$ as $r < \mu(X, 1)$

Borel's measure

The insight of Riesz was that, if $X = \bigvee_n X_n$ then

$$\mu(b \wedge X) = \bigvee_{\substack{b=b_1,\ldots,b_k \\ n_1<\cdots<n_k}} \mu(b_1 \wedge X_{n_1}) + \cdots + \mu(b_k \wedge X_{n_k})$$

Here $b = b_1, \ldots, b_k$ is a *partition* of b

So $\mu(b \wedge X)$ is defined in term of $\mu(c \wedge X_n)$ for some $c \leqslant b$

Borel's measure

If $X = c$ then we can compute $r < \mu(b \wedge c)$ and this is the value of $r < \mu(X, b)$

If $X = \bigvee_n X_n$ then $r < \mu(X, b)$ is the formula

$$\bigvee_{\substack{b=b_1,\ldots,b_k \\ r=r_1+\cdots+r_k \\ n_1<\cdots<n_k}} r_1 < \mu(X_{n_1}, b_1) \ \wedge \ \ldots \ \wedge \ r_k < \mu(X_{n_k}, b_k)$$

Borel's measure

For $X = \bigwedge_n X_n$ we should have $\mu(b \wedge X) = \mu(b) - \mu(b \wedge \bigvee_n X'_n)$ and

$$\mu(b \wedge \bigvee_n X'_n) = \bigvee_{\substack{b=b_1,\ldots,b_k \\ n_1<\cdots<n_k}} \mu(b_1 \wedge X'_{n_1}) + \cdots + \mu(b_k \wedge X'_{n_k})$$

From this, we deduce the value of $r < \mu(X, b)$

Borel's measure

This defines recursively $r < \mu(X, b)$ as a hyperarithmetical formula

It is then possible to show *purely inductively* that if we have $X \vdash Y$ then

$$[r < \mu(X, b)] \quad \leqslant \quad [r < \mu(Y, b)]$$

This shows the consistency of our definition: if X and Y represent the *same* Borel set then $r < \mu(X, b)$ and $r < \mu(Y, b)$ are equal

We then show, purely inductively, that $r < \mu(N, 1)$ is provable for each $r < 1$, where N is the symbolic representation of the set of normal binary sequences. We get in this way a proof of $\mu(N) = 1$ which only involves inductive reasoning

Game semantics

By lack of time I can only briefly mention the work on game semantics, interpreting a proof as a *winning strategy*

In particular, Lorenzen has a suggestive analysis of

$$\neg\neg a \quad \rightarrow \quad a$$

and why it is not intuitionistically valid, or even of

$$\wedge_x(A \vee B(x)) \ \rightarrow \ A \vee \wedge_x B(x)$$

Game semantics

An extension of this interpretation to analysis is described in Berardi, Bezem, C. (1994), providing in particular a different interpretation than Spector (1961). See also the work of T. Hida (2012) interpreting of the axiom of determinacy

I suggested (1991) an analysis of cut-elimination based on this interpretation, describing cut-elimination as an interaction between two strategies that both can backtrack. This has recently been used by F. Aschieri (2015) for proving a non trivial refinement of Gentzen's upper bound (with a tower of exponential) in term of the level of *backtracking* of the strategies.

For instance, if *one* strategy has only one level of backtracking then we have a single exponential (whatever the complexity of the cut formula).