A Semantics of Evidence for Classical Arithmetic

Thierry Coquand

Chambery, June 5, 2009

Intuitionistic analysis of classical logic

This work is motivated by the first consistency proof of arithmetic by Gentzen (1936)

Unpublished by Gentzen (criticisms from Bernays, Gödel, Weyl), but can be found in his collected works

I learnt about this from a paper by Bernays (in *Intuitionism and Proof Theory*, 1970)

Can be formulated as a game semantics for classical arithmetic (discovered also independently by Tait, also from Bernays paper)

Intuitionistic analysis of classical logic

Thus propositions of actualist mathematics seem to have a certain utility, but no sense. The major part of my consistency proof, however, consists precisely in ascribing a finitist sense to actualist propositions

Similar motivations in the work of P. Martin-Löf *Notes on constructive mathematics*

Explains the notion of Borel subsets of Cantor space as infinitary propositional formulae

(Classical) inclusion between Borel subsets is explained constructively by sequent calculus

Intuitionistic analysis of classical logic

Here the "finitist sense" of a proposition will be an *interactive program*

A *winning strategy* for a game associated to the proposition

Lorenzen had an analysis of *intuitionistic* logic in term of games

What may be new here is the notion of backtracking and learning (but it was already present in Hilbert's ϵ-calculus)

Cohen: forcing motivated by work on consistency proof for analysis (R. Platek)

Intuitionistic analysis of classical logic

New analysis of modus-ponens

modus-ponens = internal communication = parallel composition + hiding

cut-elimination = “internal chatters” end eventually

new proof of cut-elimination

The finiteness of interaction is proved by a direct combinatorial reasoning about sequences of integers

Intuitionistic analysis of classical logic

Different from Gentzen's proofs. It would actually be quite interesting to go back to Gentzen's argument

Implicit use of the bar theorem?

Influence of Brouwer? Brouwer-Kleene ordering

No explicit reference to Brouwer. However the criticism was about implicit use of the bar theorem

Intuitionistic analysis of classical logic

Difference between R well-founded, i.e. all elements are R-accessible i.e. the following induction principle is valid

$$(\forall x.\ (\forall y.\ R(y,x) \rightarrow \varphi(y)) \rightarrow \varphi(x)) \rightarrow \forall z.\varphi(z)$$

and the fact that R has no infinite decreasing sequence

$$(*) \qquad \forall f.\exists n.\ \neg R(f(n+1), f(n))$$

The equivalence between these two formulations is the content of Brouwer's bar Theorem. Classically provable with dependent choice (so it is a principle of intuitionistic mathematics *compatible* with classical logic)

Intuitionistic analysis of classical logic

ω-logic: we express that we have a *well-founded* derivation tree

We can do induction on the structure of this tree

Instead Gentzen expresses that any branch is finite

This is only equivalent to the tree being well-founded modulo Brouwer's bar Theorem

It seems that Gentzen's argument goes through without the need of Brouwer's bar Theorem

Intuitionistic analysis of classical logic

Intuitionistic meaning of quantifiers: a proof of

$$\forall x.\exists y.\forall z.\exists t.\ P(x, y, z, t)$$

where $P(x, y, z, t)$ is decidable can be seen as a winning strategy for $\exists$loise in a game between two players $\forall$belard and $\exists$loise

$$\forall \quad x = a \quad \exists \quad y = b \quad \forall \quad z = c \quad \exists \quad t = d$$

Does $P(a, b, c, d)$ hold?

Intuitionistic analysis of classical logic

For the games

$$\exists x. \forall y.\ D(x) \rightarrow D(y)$$

$$\exists n. \forall m.\ f(n) \leqslant f(m)$$

there is no *computable* strategy for $\exists$loise

There would be a strategy for an *actualist* interpretation of quantifiers (Gentzen's terminology)

Intuitionistic analysis of classical logic

We allow ∃loise to "change her mind"

∃loise chooses first $x = 0$, then if $y = b_1$ is the choice of ∀belard, she changes her mind for $x = b_1$ if $f(b_1) < f(0)$

∃lois wins eventually since $\mathbb{N}$ is well-founded

Remark: ∃loise *learns* from her environment

The first move $x = 0$ can be seen as a "guess" and we have a successive approximation towards a solution (we are never sure we have the "right" solution)

Intuitionistic analysis of classical logic

Gödel (1938) presents Gentzen's proof in a lecture, that we can now read in Collected Works, III

Clearly refers to Gentzen's unpublished proof, and refers to Suslin's schema instead of bar's theorem

Presents it as no-counterexample interpretation

Counter-example: function g witness of $\forall n.\exists m.\ f(m) < f(n)$ i.e. $\forall n.\ f(g(n)) < f(n)$

We should have a function Φ such that $f(\Phi(g)) \leqslant f(g(\Phi(g)))$

Formulae as trees

In general we represent a formula as a $\wedge \vee$ tree, possibly infinitely branching, the leaves being 0 or 1

For instance

$$(\exists n.\forall m.\ f(n) \leqslant f(m)) \rightarrow \exists u.\ f(u) \leqslant f(u+1)$$

will be represented as a $\wedge \vee$ tree

$$(\forall n.\exists m.\ f(n) > f(m)) \vee \exists u.\ f(u) \leqslant f(u+1)$$

Formulae as trees

Winning strategy

$\exists$loise asks for x

$\forall$belard answers $x = a$

If $f(a) \leqslant f(a+1)$ then $\exists$loise takes $u = a$

If $f(a) > f(a+1)$ then $\exists$loise takes $y = a + 1$

Winning strategy and the length of a play is 2

Cut-free proofs

truth semantics for classical arithmetic

The concept of the "statability of a reduction rule" for a sequent will serve as the formal replacement of the informal concept of truth*; it provides us with a special finitist interpretation of propositions and take place of their* actualist interpretation

Example: classical existence of gcd by looking at $\langle a, b\rangle = \langle g\rangle$

Modus Ponens

The strategies we have considered so far corresponds to *cut-free proofs*

tells the proof how to behave in an environment that does not change its mind

Modus-ponens = "cooperation" between proofs

Modus Ponens

$A \quad \exists n. \forall m.\ f(n) \leqslant f(m)$

$B \quad (\forall n. \exists m.\ f(n) > f(m)) \vee\ \exists u.\ f(u) \leqslant f(u+1)$

A and B interacts to produce a proof of

$\exists u.\ f(u) \leqslant f(u+1)$

Modus Ponens

$f(0) = 10 \quad f(1) = 8 \quad f(2) = 3 \quad f(3) = 27 \quad \ldots$

1	B	$n?$
2	A	$n = 0$ answers move 1
3	B	$m = 1$ answers move 2
4	A	$n = 1$ answers move 1
5	B	$m = 2$ answers move 4
6	A	$n = 2$ answers move 1
7	B	$u = 3$

Modus Ponens

We have an *interaction sequence* (pointer structure)

$\varphi(1) = 0 \quad \varphi(2) = 1 \quad \varphi(3) = 2 \quad \varphi(4) = 1 \quad \varphi(5) = 4 \quad \varphi(6) = 1$

Modus Ponens

Behaviour of a proof against an environment that can "change its mind"

Notion of *debate*

The formula seen as a tree is the "topic of the debate"

argument counter-argument counter-counter-argument ...

Two opponents who *both* can change their mind

At any point they can *resume* the debate at a point it was left before

Modus Ponens

Analysis of modus-ponens, the cut-formulae is P

$\exists x. \forall y. \ \neg P(x, y)$

$\forall x. \exists y. \ P(x, y)$

In general

$\exists x. \forall y. \exists z. \ldots \ \neg P(x, y, z, \ldots)$

$\forall x. \exists y. \forall x. \ldots . \ P(x, y, z, \ldots)$

How does Gentzen proceed?

Modern formulation

$$\frac{\Gamma, \neg P(n), \exists x. \neg P(x)}{\Gamma, \exists x. \neg P(x)} \qquad \frac{\ldots \ \Delta, P(m) \ \ldots}{\Delta, \forall x. P(x)}$$

First $\Delta, \forall x. P(x)$ and $\Gamma, \neg P(n), \exists x. \neg P(x)$ by cut we get $\Delta, \Gamma, \neg P(n)$

Then $\Delta, \Gamma, \neg P(n)$ and $\Delta, P(n)$ by cut we get Δ, Δ, Γ and hence Δ, Γ

Analysis of the interaction?

Depth 2 $\quad A \quad \exists x.\forall y.\ \neg P(x,y) \quad B \quad \forall x.\exists y.\ P(x,y)$

$A \quad x = a_1$

$B \quad y = b_1$

$A \quad x = a_2$

$B \quad y = b_2$

We can assume $P(a_1, b_1) = P(a_2, b_2) = \cdots = 1$ so that the value $x = a_i$ is *definitively* refuted by the move $y = b_i$

Analysis of the interaction?

Depth 3 A $\exists x.\forall y.\exists z.\ \neg P(x,y,z)$ B $\forall x.\exists y.\forall z.\ P(x,y,z)$

A $x = a_1$

B $y = b_1$

A $x = a_2$

B $y = b_2$

Key idea: whenever there is a move A $z = c$ it *definitively* refutes the corresponding move B $y = b$ and one can forget all that has happened between these two moves

Hence one can reduce depth 3 to depth 2

Combinatorial analysis

$a_1 \ b_{11} \ c_{11} \ \ldots \ b_{1(n_1-1)} \ c_{1(n_1-1)} \ b_{1n_1}$

$a_2 \ b_{21} \ c_{21} \ \ldots \ b_{2(n_2-1)} \ c_{2(n_2-1)} \ b_{2n_2}$

$\ldots$

$a_k \ b_{k1} \ c_{k1} \ \ldots \ b_{k(n_k-1)} \ c_{k(n_k-1)} \ b_{kn_k}$

The next move is either a_{k+1} or c_{ln_l} for some $l \leqslant k$

Combinatorial analysis

Interaction sequence $\varphi(1)\ \varphi(2)\ \varphi(3)\ \ldots$

$\varphi(n) < n$ and $\varphi(n)\quad n$ different partity

$V(0) = \emptyset \quad V(n+1) = \{n\} \cup V(\varphi(n))$

then $\varphi(n)$ has to be in $V(n)$

Cut-free proof: we have $\varphi(n) = n$ for n even

Depth: maximum length of chain $\varphi(n_1) = 0\ \ \varphi(n_2) = n_1\ \ \ldots\ \ \varphi(n_d) = n_{d-1}$

Combinatorial analysis

We consider an interaction sequence of depth d

A *definite* interval is an interval $[\varphi(n), n]$ with n of depth d

Lemma: *If we take away a definite interval what is left is still an interaction sequence*

Lemma: *The definite intervals form a nest structure*

If we have two definite intervals then either they are disjoint or one is well-inside the other

Combinatorial analysis

Heuristic why the interaction has to be finite by induction on the depth

We take away all maximal definite intervals

By induction on the depth we should have an infinite number of consecutive intervals $[m_0+1, m_1]$ $[m_1+1, m_2]$ $[m_2+1, m_2]$ ... with $\varphi(m_0+1) = \varphi(m_1+1) = \dots$

This contradicts that we have a winning strategy

Gentzen d to $1+d$, and here d to $d+1$

Cut-elimination

Combinatorial analysis of what happens during cut-elimination

Termination follows from this analysis

The termination argument seems different from Gentzen's

Further work: Countable choices

We quantify over functions: we conjecture "laws" that can be refined by learning

There is a natural strategy for countable choice (and dependent choice)

This is not well-founded any more

However, if we cut with a well-founded strategy we get a well-founded strategy

Further work: Countable choices

$(\exists n.\forall x.\ \neg P(n,x)) \vee \exists f.\forall n.\ P(n,f(n))$

$f = f_0$ opponent answers $n = n_0$

$n = n_0$ opponent answers $x = x_0$

$f = f_0 + n_0 \longmapsto x_0$ opponent answers $n = n_1$

$n = n_1$ opponent answers $x = x_1$

$f = f_0 + n_0 \longmapsto x_0 + n_1 \longmapsto x_1$ opponent answers $n = n_2$

Further work: Curien and Herbelin

Stack free version of Krivine Abstract Machine

$$M \;::=\; \lambda\vec{x}.\, W \qquad W \;::=\; y\ \vec{M} \qquad \rho, \nu \;::=\; () \mid \rho, \vec{x} = \vec{M}\nu$$

One reduction rule

$$(x\ \vec{M})\rho \quad \rightarrow W(\nu, \vec{z} = \vec{M}\rho)$$

where $\rho(x) = (\lambda\vec{z}.\ W)\nu$

Further work: Curien and Herbelin

Theorem: *This* always *terminates*

No direct proof known. *Types are not involved in the proof of termination. They only play a role in garanteeing that the final states correspond to (an abstract form of) head normal forms.*

Question: can we compute a bound on the length of the interaction (hyper-exponential)?

Simple backtracking

As "learning procedures" the cut-free proofs are quite complex since we may have "backtracking in the backtracking"

Non monotonic learning

As a first step one can analyse what happens with "simple" backtracking where we never consider again a position that has been rejected

For instance, the argument for $\exists n.\forall m.\ f(m) \leqslant f(n)$ only involves simple backtracking

Hilbert's basis theorem

Simple backtracking

Infinite box principle

$$(\forall n.\exists m \geqslant n.\ f(m) = 0) \vee (\forall n.\exists m \geqslant n.\ f(m) = 1)$$

needs more complex backtracking

Exactly the same notion occurs in the work of R. Harmer and P. Clairambault: cellular strategies

Infinite box principle

$(\exists n.\forall m \geqslant n.\ f(m) = 1) \vee \exists a < b.\ f(a) = f(b)$

$(\exists n.\forall m \geqslant n.\ f(m) = 0) \vee \exists a < b.\ f(a) = f(b)$

$(\forall n.\exists m \geqslant n.\ f(m) = 0) \vee (\forall n.\exists m \geqslant n.\ f(m) = 1)$

There is a symmetric interaction which proves

$\exists a < b.\ f(a) = f(b)$

Further work: Berardi

All these lemmas are valid if we change the notion of definite interval

$[\varphi(n), n]$ is definite iff there is no m such that $\varphi(m) = n$

View on $[0, n]$: partition in intervals $\ldots [n_2+1, n_1]$ $[n_1+1, n]$ where $n_1+1 = \varphi(n),\ n_2+1 = \varphi(n_1), \ldots$

S. Berardi noticed that this can be (classically) extended to ω and thus one can extend the notion of view to infinite plays

Theorem: (classical) *One has an unique partition of* $[0, \omega[$ *in (definite) intervals* $[\varphi(n), n]$

So we can extend the interaction transfinitely