THE JOURNAL OF SYMBOLIC LOGIC
Volume 60, Number 1, March 1995

A SEMANTICS OF EVIDENCE FOR CLASSICAL ARITHMETIC

THIERRY COQUAND

Introduction. If it is difficult to give the exact significance of consistency proofs from a classical point of view, in particular the proofs of Gentzen [2, 6], and Novikoff [14], the motivations of these proofs are quite clear intuitionistically[1]. Their significance is then less to give a mere consistency proof than to present an intuitionistic explanation of the notion of classical truth. Gentzen for instance summarizes his proof as follows [6]: "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." From this point of view, the main part of both Gentzen's and Novikoff's arguments can be stated as establishing that modus ponens is valid w.r.t. this interpretation ascribing a "finitist sense" to classical propositions.

In this paper, we reformulate Gentzen's and Novikoff's "finitist sense" of an arithmetic proposition as a winning strategy for a game associated to it. (To see a proof as a winning strategy has been considered by Lorenzen [10] for intuitionistic logic.) In the light of concurrency theory [7], it is tempting to consider a strategy as an interactive program (which represents thus the "finitist sense" of an arithmetic proposition). We shall show that the validity of modus ponens then gets a quite natural formulation, showing that "internal chatters" between two programs end eventually[2].

We first present Novikoff's notion of *regular* formulae, that can be seen as an intuitionistic truth definition for classical infinitary propositional calculus. We use this in order to motivate the second part, which presents a game-theoretic interpretation of the notion of regular formulae, and a proof of the admissibility of modus ponens which is based on this interpretation. Proofs of regularity of a formula then get identified with winning strategies for a certain game associated to this formula. Another possible way of making intuitionistic sense of classical propositions is the double negation translation, which can be seen as giving a functional interpretation of classical proofs (see for instance [13]). We compare the two approaches on a special problem of composition of proofs.

Received February 7, 1992; revised March 17, 1993.

This is a revised version of a paper with the same title presented at the Basic Research Action Logical Framework meeting, Edinburgh, May 1991.

[1]The meaning of "intuitionistic" here will be close to the one described in Kleene's book [8]. Particularly relevant is the discussion after the proof of Theorem 61 [8], which presents a truth definition for Heyting arithmetic. This term is used with a similar meaning in [14].

[2]A similar point of view is presented in the different framework of classical linear logic in [1].

0022-4812/95/6001-0018/$02.30

§1. Novikoff's calculus. In order to motivate the introduction of interaction sequences, and our game-theoretical description of classical provability, we think that it may be helpful to present briefly the calculus of Novikoff [14]. Notice that this can be seen as a variation of the notion of *statable* sequent [6] of Gentzen.

The formulae of this system are of two sorts, existential and universal, and are inductively defined:

- the atomic formulae 0 and 1 are both existential and universal,
- if (A_i) is a family of universal formulae, then ΣA_i is an existential formula,
- if (A_i) is a family of existential formulae, then ΠA_i is a universal formula.

We may write a formula $\Sigma_i(\Sigma_j A_{ij})$ instead of $\Sigma_{(i,j)}A_{ij}$, and similarly $\Pi_i(\Pi_j A_{ij})$ instead of $\Pi_{(i,j)}A_{ij}$. It is possible also, and direct, to define a sum of two formulae $A + B$. As in [15], we also leave imprecise the exact form of the index sets over which we can form sum and product of a family of formulae. In what follows we only use for these sets decidable subsets of the set of natural numbers.

Negation is defined by the usual de Morgan rules.

Alternatively, we can think of any such formula simply as a tree, with a "polarity", that says whether or not this tree is considered as an existential or universal formulae. We shall use this presentation in the next section.

It is quite straightforward to represent any formula of Peano arithmetic in this infinitary propositional calculus. We do not do it in detail here, but refer to Tait's or Novikoff's paper [14, 15]. We hope, however, that the examples presented below give a clear idea of this transformation.

The notion of *provable* or *regular* formulae, according to Novikoff's terminology [14], is defined inductively as follows:

- 1 is provable,
- ΠA_i is provable iff each A_i is provable,
- ΣA_i is provable iff there exists i_0 such that $A_{i_0} = 1$ or $A_{i_0} = \Pi A_{i_0 j}$ and, for all j, the formula $\Sigma_{i \neq i_0} A_i + A_{i_0 j}$ is provable.

Except for the non-redundancy condition $i \neq i_0$, we can recognize in this definition the usual definition of cut-free provability in sequent calculus [15].

This notion can be compared to the definition of intuitionistic truth:

- 1 is intuitionistically true,
- ΠA_i is intuitionistically true iff each A_i is intuitionistically true,
- ΣA_i is intuitionistically true iff there exists i_0 such that $A_{i_0} = 1$ or $A_{i_0} = \Pi A_{i_0 j}$ and, for all j, the formula $A_{i_0 j}$ is intuitionistically true.

In the definition of regularity, we take our meta-language to be intuitionistic. We can then consider this definition of regularity as an intuitionistic explanation of classical truth. It can be seen as a "semantics of evidence" for classical truth, following Constable's terminology [5].

A quite similar approach is taken in Martin-Löf's monograph [11], for explaining intuitionistically the classical meaning of inclusion between Borel sets over Cantor's space.

1.1. Game-theoretic formulation. The inductive definition of regularity of a formula has a natural game theoretic interpretation. A formula can be thought of as specifying a perfect information game between two players that are called ∃loise, who plays for existential formulae, and ∀belard, who plays for universal formulae.

We present first the game which corresponds to the notion of intuitionistic validity of a formula A. This formula describes the **configuration** of the game. If ∃loise (resp. ∀belard) has to play and the formula is atomic, then ∃loise (resp. ∀belard) wins if the formula is 1 (resp. 0) and looses if the formula is 0 (resp. 1). If the formula is non-atomic, there are two cases. If $A = \Sigma A_i$ is existential, then ∃loise has to play by choosing an index i_0, the configuration becomes A_{i_0} and it is ∀belard's turn to play. If $A = \Pi A_i$ is universal, then ∀belard has to play by choosing an index i_0, the configuration becomes A_{i_0} and it is ∃loise's turn to play. It is clear in this case that ∃loise has a winning strategy for the game of configuration A iff A is an intuitionistically true formula.

To get the corresponding notion of classical truth, analyzed intuitionistically, we break the symmetry between ∀belard and ∃loise. Intuitively, the game becomes rather unfair to ∀belard: now ∃loise can change her mind, and can backtrack in her choice, and can even resume a position that she had for a while taken back! Poor ∀belard, on the contrary, is forced to answer to ∃loise's latest move.

More precisely, the rules of the game are defined as before for an atomic configuration. If the formula is non-atomic, there are two cases. If $A = \Pi A_i$ is universal, then ∀belard has to choose an index i_0, the configuration becomes A_{i_0} and it is ∃loise's turn to play. If $A = \Sigma A_i$ is existential, then ∃loise chooses an index i_0, wins if A_{i_0} is atomic and is 1, looses if it is 0, and ∀belard must choose an index of the universal formula $A_{i_0} = \Pi A_{i_0 j}$ in the other case. The formula becomes then $\Sigma_{i \neq i_0} A_i + A_{i_0 j_0}$ and it is ∃loise's turn to play.

It is easy to see that ∃loise has a winning strategy for the game of configuration A iff A is regular.[3]

1.2. Examples. The following arithmetical formula (with a parameter f denoting an arbitrary function)

$$E_1 = \exists x. \forall y. f(x) \leq f(y)$$

expresses that any function has a minimum. It is understood that $f(x) \leq f(y)$ is 1 if $f(x)$ is less or equal than $f(y)$, and is 0 if $f(x)$ is strictly bigger than $f(y)$. It is standard that there is no computable functional $\Phi(f)$ which computes a value on which f is minimum, so that the formula E_1 cannot be proved intuitionistically.

However E_1 is a regular formula. This is most easily seen by describing a winning strategy for ∃loise in the game of configuration $E_1 = \Sigma_x \Pi_y f(x) \leq f(y)$:

- ∃loise starts by choosing $x = 0$,
- ∀belard has to answer by choosing $y = y_1$; if $f(0) \leq f(y_1)$ then ∃loise wins,
- otherwise, $f(y_1) < f(0)$ and ∃loise changes her mind by playing $x = y_1$,
- ∀belard has to answer by choosing $y = y_2$; if $f(y_1) \leq f(y_2)$ then ∃loise wins,
- otherwise, $f(y_2) < f(y_1)$ and ∃loise changes her mind by playing $x = y_2$, etc.

∃loise will win eventually if she follows this strategy because $<$ is well-founded on integers.

[3]A similar kind of game has been also considered by A. Blass [3], who gives a game-theoretic interpretation of propositional intuitionistic logic.

By a similar argument, the formula

$$E_2 = \forall x \exists y \geq x \forall z \geq x . f(y) \leq f(z)$$

is regular. The formula

$$E_3 = \exists M \forall x . f(x) \leq M + \forall N \exists y . N < f(y)$$

which expresses that f is either bounded or unbounded is also directly seen to be not valid intuitionistically.

But E_3 is regular. It is enough to describe a winning strategy for ∃loise:

- ∃loise starts by asking a value for N,
- ∀belard has to answer a value $N = N_0$,
- ∃loise changes her mind and plays $M = N_0$,
- ∀belard must give a value $x = x_0$,
- if $f(x_0) \leq N_0$, then ∃loise wins; otherwise ∃loise wins by playing $y = x_0$.

Notice that, in this case, we can give a bound a priori of the length of the game. This was not the case for the two other examples.

1.3. Markov's principle. There are two important cases where the notion of classical truth and intuitionistic truth coincides: if the formula is Σ_1^0 or Π_2^0. This fact was used by Novikoff's [14] to derive a form of closure under Markov's rule: if a Σ_1^0 formula is derivable classically, then it is valid intuitionistically. This nice proof seems to have been curiously unnoticed for a long time in the West (see Church's review [4] of Novikoff's article and Mints' survey article [12], which contains a presentation of Novikoff's paper).

1.4. Admissibility of modus ponens. The principal result of Novikoff's paper is an intuitionistic proof that, if both $\neg A + B$ and A are regular, then B is regular. According to standard proof-theoretic terminology, this expresses that modus ponens is *admissible*. We present a short version of this argument in an appendix, which is quite remarkable in that it does not use any induction on the cut-formula (contrary to the argument presented in [15], or in [11]).

The examples show that it is convenient and intuitive to present proofs of regularity of a formula as the description of a winning strategy. We thus expect that a game-theoretic formulation will provide interesting new light on the admissibility of cut.

In what follows, we shall do this analysis in the case where B is Σ_1^0. We suppose given a winning strategy σ for A and a winning strategy τ for $\neg A + B$. The problem is now to build a witness for the Σ_1^0 formula B from σ and τ. Intuitively, this will be done by "letting σ play against τ." In the special case where B is Σ_1^0, we prefer to look at τ as a partial strategy for A : indeed, as soon as τ provides us with a move in B, we get a witness and we have finished our construction.

The problem is thus reduced to the following. Define a **partial strategy** as a strategy that may fail to indicate a move in some situations. Say that such a strategy is **non-losing** if, for any given game, this strategy eventually either wins or fails to suggest any move. (In particular, a winning strategy is non-losing.) Given a non-losing strategy σ for a formula ΣA_i and for each i a non-losing strategy τ_i for $\neg A_i$, we want to produce a game in which one τ_i or σ fails to answer. In the next section, we show that this can be done in a systematic way, providing us with a new proof of

the elimination of modus ponens. We shall define generally a particular sequence of games between σ and (τ_i), and express a combinatorial property of this sequence that implies that it must terminate if σ and τ_i are non-losing.

§2. Games, strategies and interaction sequences.

2.1. Trees, occurrences. We recall first our inductive definition of tree (or formula without indication of its polarity, existential or universal):

(1) 0 and 1 are trees,
(2) if (A_i) is a family of trees, then $\mathbf{sup}(A_i)$ is a tree.

The tree $\neg A$ is defined inductively. We have $\neg 0 = 1$, $\neg 1 = 0$ and $\neg\mathbf{sup}(A_i)$ is $\mathbf{sup}(\neg A_i)$.

We associate with any tree A its set of **occurrences**, that can be seen as a set of finite sequences of indexes. We use the letters $t, u, v, \ldots$ for denoting occurrences in a tree. This set is defined inductively: the empty sequence $<>$ is an occurrence of any tree, and if u is an occurrence of A_i, then the sequence iu is an occurrence of the tree $\mathbf{sup}(A_i)$. We write $f()$ instead of $f(<>)$ when the empty occurrence $<>$ is used as an argument of a function. To any occurrence u in A, we can associate a tree A_u, called **subtree** of A at occurrence u : we have $A_{<>} = A$ and if $A = \mathbf{sup}(A_i)$, then $A_{iu} = (A_i)_u$. If $u = i_1 \ldots i_n$, then n is the **length** of u. We say that a sequence v **extends** the sequence u iff v is of the form $uj_1 \ldots j_p$. A **direct** extension of u occurrence in A is an occurrence in A of the form uj_1.

2.2. Strategies. Given a tree A, a **partial strategy** for the game of configuration A is a function ϕ defined on a set $\mathbf{Dom}(\phi)$ of sequences $u_1 \ldots u_n$ of non-empty occurrences of even length in A. If $\phi(u_1 \ldots u_n)$ is defined, it has to be an occurrence $v \in A$ satisfying two properties

(1) it is a direct extension of exactly one of the u_i or of $<>$ (in particular, $\phi()$ is an occurrence of length 1),
(2) none of $u_1, \ldots, u_n$ is an extension of v.

Furthermore, if $u_1 \ldots u_{n+1} \in \mathbf{Dom}(\phi)$, then $u_1 \ldots u_n \in \mathbf{Dom}(\phi)$ and u_{n+1} is a direct extension of $\phi(u_1 \ldots u_n)$.

An element of $\mathbf{Dom}(\phi)$ is called a **branch** of ϕ. We use letters $L, M, N, \ldots$ for denoting branches of a strategy. A branch L is **directly winning** iff $\phi(L)$ is an occurrence of the form $u1$. A branch L is **directly losing** iff $\phi(L)$ is of the form $u0$, or the direct extension $\phi(L)1$ of $\phi(L)$ is an occurrence of A. A branch of ϕ represents a possible beginning of a game played by the strategy ϕ.

We define inductively when a branch is **winning**:

(1) It is winning if it is directly winning, or
(2) it is winning if all its extensions in $\mathbf{Dom}(\phi)$ are winning.

In the same way, we define inductively when a branch L is **non-losing**:

(1) It is non-losing if it is not directly losing, or
(2) it is non-losing if all its extensions in $\mathbf{Dom}(\phi)$ are non-losing.

Notice that a winning branch is necessarily non-losing.

We say that ϕ is **non-losing** iff $<>$ is a non-losing branch of $\mathbf{Dom}(\phi)$. A strategy ϕ is **winning** iff $<>$ is a winning branch in $\mathbf{Dom}(\phi)$. (Notice that a winning strategy is automatically non-losing.)

These definitions can be seen as a precise intuitionistic counterpart of the informal presentation contained in the previous section. In particular, there is a winning strategy for a tree A, iff this tree is regular, seen as an existential formula.

2.3. Debate. Let A be a formula and (A_i) the family of its immediate subtrees. Given a strategy σ for A and a family of strategies τ_i for $\neg A_i$, we are going to define a sequence of branches alternatively in $\mathbf{Dom}(\sigma)$ and in one of $\mathbf{Dom}(\tau_i)$. This sequence will be finite if σ and all τ_i are non-losing, and furthermore, in this case, it gives an algorithm for computing an extremal branch of σ or one of the τ_i which is not directly winning.

We define the **debate** associated to σ and τ_i. A debate consists in a sequence of **moves**: (f_1, u_1), $(f_2, u_2), \ldots$ where the nth move (f_n, u_n) is a pair of an integer $f_n < n$ and an occurrence u_n in A. The integers f_n and n are of different parity, and f_n indicates to what move the nth move is answering.

This sequence is built by steps, using values of σ and τ_i. The debate stops as soon as one strategy fails to answer. First, we compute $\sigma() = i_1$ and $(0, i_1)$ is the first move. Next, let us suppose that we have already computed the first n moves, and we try to compute the $(n+1)$th move. There are two cases:

- n is even: we compute the sequence $n_1 = n$, $n_2 = f_{n_1} - 1, \ldots$ until we find n_p such that $f_{n_p} = 1$, and compute $\sigma(u_{n_p} \ldots u_{n_2} u_{n_1}) = u_{n+1}$ which is a direct extension of exactly one of u_{n_k} or of $<>$. If it is a direct extension of $<>$ we take $f_{n+1} = 0$. If it is a direct extension of u_{n_k}, we take $f_{n+1} = n_k$,
- n is odd: similarly, we compute the sequence $n_1 = n, n_2 = f_{n_1} - 1, \ldots$ until we find n_{p+1} such that $f_{n_{p+1}} = 0$. Inductively, all values $u_{n_1}, u_{n_2}, \ldots$ start with the same index i and we define v_{n_k} by $iv_{n_k} = u_{n_k}$. We compute then $\tau_i(v_{n_p} \ldots v_{n_2} v_{n_1}) = v_{n+1}$, which is a direct extension of exactly one of v_{n_k} or of $<>$. If it is a direct extension of $<>$, we take $f_{n+1} = n_{p+1}$. If it is a direct extension of v_{n_k}, we take $f_{n+1} = n_k$. In both cases, we take $u_{n+1} = iv_{n+1}$.

It may help the intuition of the reader to think about what happens during a real debate on a given topic between two persons. Both defend arguments, can change for a while their position, but also, at any point, can resume the debate at a point it was left before. This is what happens here, the integer f_n representing to what move the nth move is answering. (By convention, we take $f_1 = 0$ for the first move.) The topic of discussion is represented by the formula A.

2.4. Example. Given a function f on integers as a parameter, both formulae

$$E_2(x) = \exists y \geq x. \forall z \geq x. [f(y) \leq f(z)]$$

and

$$E_4 = \exists x \neg E_2(x) \vee \exists u_3 > u_2 > u_1. [f(u_1) \leq f(u_2) \leq f(u_3)]$$

are regular. The second formula is even provable intuitionistically, if we read it as

$$(\forall x E_2(x)) \Rightarrow \exists u_3 > u_2 > u_1. [f(u_1) \leq f(u_2) \leq f(u_3)]$$

but as we have seen, $E_2(x)$ holds only classically.

We define a family of winning strategies τ_x for $E_2(x)$ and a winning strategy σ for E_4. This strategy σ will also be considered as a non-losing strategy for the formula

$$(\exists x) \neg E_2(x) = \exists x. \forall y \geq x. \exists z \geq x. [f(y) > f(z)]$$

We shall write the debate between these two strategies that produces a witness for

$$\exists u_3 > u_2 > u_1.[f(u_1) \leq f(u_2) \leq f(u_3)].$$

The strategy τ_x for $E_2(x)$ has been already described above. Here is a description of a winning strategy σ for the formula E_4.

- σ chooses $x = 0$,
- the opponent chooses a value $y = a_1$,
- σ changes its mind and plays $x = a_1 + 1$,
- the opponent chooses a value $y = a_2$, such that $a_2 > a_1$,
- if $f(a_1) > f(a_2)$, σ resumes the game with its initial value 0 for x, and wins by playing $z = a_2$. If $f(a_1) \leq f(a_2)$, σ changes its mind and plays $x = a_2 + 1$,
- the opponent chooses a value $y = a_3$, such that $a_3 > a_2$,
- if $f(a_3) > f(a_2)$, σ resumes the game with the value $a_1 + 1$ for x, and wins by playing $z = a_3$. Otherwise, $f(a_1) \leq f(a_2) \leq f(a_3)$, and σ wins by playing $u_1 = a_1, u_2 = a_2, u_3 = a_3$.

We are going now to show an example of the debate between these two strategies, in the case where the values of f are given by

$$f(0) = 10,\ f(1) = 5,\ f(2) = 3,\ f(3) = 7,\ f(4) = 4,\ f(5) = 11,\ f(6) = 29, \ldots$$

(1) σ plays $x = 0$,
(2) τ_0 plays $y = 0$, responding to the move 1,
(3) σ changes its mind, plays $x = 1$, starting with a new opening,
(4) τ_1 plays $y = 1$, responding to the move 3,
(5) $f(0) > f(1)$, hence σ plays $z = 1$, responding to the move 2,
(6) τ_0 plays $y = 1$, responding to the move 1,
(7) σ plays $x = 2$, starting with a new opening,
(8) τ_2 plays $y = 2$, responding to the move 7,
(9) $f(1) > f(2)$, hence σ plays $z = 2$, responding to the move 6,
(10) τ_0 plays $y = 2$, responding to the move 1,
(11) σ plays $x = 3$, starting with a new opening,
(12) τ_3 plays $y = 3$, responding to the move 11,
(13) $f(3) \geq f(2)$, hence σ plays $x = 4$, starting with a new opening,
(14) τ_4 plays $y = 4$, responding to the move 13,
(15) $f(4) < f(3)$, hence σ plays $z = 4$, responding to the move 12,
(16) τ_3 plays $y = 4$, responding to the move 11,
(17) $f(4) \geq f(2)$, hence σ plays $x = 5$, starting a new opening,
(18) τ_5 plays $y = 5$, responding to the move 17,
(19) $f(5) \geq f(4)$, hence σ plays $u_1 = 2,\ u_2 = 4,\ u_3 = 5$.

The computation of (u_1, u_2, u_3) consists of an exchange of values between τ_x and σ, until a value $(u_1, u_2, u_3) = (2, 4, 5)$ is found by σ.

2.5. Interaction sequences. For proving that a debate between non-losing strategies terminates eventually, we single out one special property of the sequence of integers $f_1 f_2 \ldots$ associated with a possible debate. We define an **interaction sequence** as a sequence $f_1 f_2 \ldots$ such that $f_1 = 0$ and the integer f_{p+1} is one of the values $p, f_p - 1, f_{f_p - 1} - 1, \ldots$

It is clear by construction that if $(f_1, u_1)(f_2, u_2), \ldots$ is a debate between strategies, then $f_1 f_2 \ldots$ is an interaction sequence. The following lemma is proved directly from the definition.

LEMMA 1. *Let $f_1 f_2 \ldots f_n$ be an interaction sequence. If all values $f_{p+1}, f_{p+2}, \ldots, f_n$ are different from p, then $f_1 \ldots f_{f_p - 1} f'_{p+1} \ldots f'_n$, where $f'_q = f_q$ if $f_q < f_p$ and $f'_q = f_q - (p - f_p + 1)$ if $f_q > p$, is an interaction sequence.*

Given an interaction $f_1 f_2 \ldots f_n$, let us call a **definite interval** an interval $[f_p, p]$ such that p is different from all values $f_{p+1}, \ldots, f_n$. (In terms of debate, this corresponds to a move that has not yet been "refuted".) The previous lemma can be stated by saying that if we take away a definite interval from an interaction sequence, what is left is still an interaction sequence. From this, we deduce:

LEMMA 2. *The definite intervals of an interaction sequence form a nest structure.*

This means that any two distinct definite intervals are either disjoint or one is included strictly in the other, where $[a, b]$ is included strictly in $[c, d]$ iff $c < a$ *and* $b < d$.

In order to simplify our treatment, we suppose now that the formula A is of bounded depth[4], that is, such that there exists a bound N to the length of all occurrences in A. In terms of interaction sequence, this means that we can suppose that there exists a bound N to the length of sequences $i, f_i, f_{f_i}, \ldots$ The length of this sequence is the **depth** of i and we say then that the interaction sequence $f_1 f_2 \ldots$ is of bounded depth $\leq N$. Notice that, in such a case, any interval $[f_p, p]$ where p is of maximal depth N is definite.

PROPOSITION 3. *Let N be an integer. Given any well-founded ordering $<$, the tree built of sequences $(f_1, \alpha_1) \ldots (f_n, \alpha_n)$ such that $f_1 \ldots f_n$ is an interaction sequence of depth $\leq N$ and $\alpha_n < \alpha_m$ whenever $m = f_n - 1$, is well-founded.*

PROOF. By induction on N. This is direct for $N = 1$. If the proposition holds for $N-1$, we associate to any sequence $s = (f_1, \alpha_1) \ldots$ the sequence $\phi(s) = (g_1, \beta_1) \ldots$ that we get from s by taking away all intervals $[f_p, p]$ where p is of depth N. The lemmas above show that $g_1 \ldots$ is an interaction sequence, which is of depth $\leq N - 1$ and it is straightforward that $\beta_n < \beta_m$ whenever $m = g_n - 1$.

Notice next that if s' extends s, then either $\phi(s')$ extends $\phi(s)$ or else $\phi(s') = (g'_1, \beta'_1)(g'_2, \beta'_2) \ldots$ is such that $\beta'_1 \beta'_2 \cdots < \beta_1 \beta_2 \ldots$ for the lexicographic ordering. The proposition for N follows then by standard arguments from the induction hypothesis. ⊣

The example of the previous subsection is a debate of depth ≤ 3. The interaction sequence associated with this interaction is the following sequence of integers:

$$0, 1, 0, 3, 2, 1, 0, 7, 6, 1, 0, 11, 0, 13, 12, 11, 0, 17.$$

The maximal intervals are [2, 5], [6, 9] and [12, 15]. If we take away these intervals, what is left is the interaction sequence 0, 1, 0, 3, 0, 5 of depth ≤ 2.

[4]It would be possible to extend our treatment to the general case. The main ideas however are present in this special case, which is enough for representing arithmetical formulae.

COROLLARY 4. *Any debate between non-losing strategies ends eventually.*

If σ and τ_i are all non-losing, no strategy can be directly winning in the debate and the debate must end because σ, or one of the τ_i, fail to answer.

The notion of debate gives an algorithm for solving the following problem:

PROBLEM 1. *Given a Σ^0_1 formula B, and winning strategies for the formulae $\neg A + B$ and A, to compute a witness for B.*

It works as well if we have a winning strategy for $\neg A + B$ and $A + B$, which corresponds to a situation which occurs in mathematical practice [9]: we prove the formula B both from the hypothesis that A holds and from the hypothesis that $\neg A$ holds, and we deduce (classically) that B holds[5]. Notice that the algorithm is non-deterministic in the trivial case where both strategies give directly a witness for B. We have then to choose arbitrarily one of these two witnesses.

The solution of the more general problem, where we compute a winning strategy for a formula B, not necessarily Σ^0_1, from a winning strategy for A and $\neg A + B$, will involve similar non-canonical choices. Rather than presenting this generalization, we prefer to analyze in the next section a situation which seems to require such a generalization: B is Σ^0_1 and given winning strategies for $A_0 + A_1$, $\neg A_0$ and $\neg A_1 + B$, we want to compute a witness for B.

§3. Non-functional composition of strategies. In this section, we compare the present intuitionistic explanation of classical proofs with the double negation interpretation on a particular problem of composition of strategies.

3.1. Distributivity law. The composition problem we consider is the following:

PROBLEM 2. *Given a proof of $A = \Sigma A_i$ and a proof of $B = \Sigma B_j$, how to produce a proof of $\Sigma_{(i,j)}\, A_i B_j$?*

This expresses one direction of the distributivity law, and we refer to this problem as the "distributivity problem". We shall see that there are essentially three ways to do this composition of strategy.

We need first a general lemma about well-founded ordering.

LEMMA 5. *Let X and Y be two well-founded orderings. The following operations define a well-founded ordering on the product $X \times Y$:*

- *$(x_1, y_1) < (x_2, y_2)$ iff $x_1 < x_2$ or both $x_1 = x_2$ and $y_1 < y_2$,*
- *$(x_1, y_1) < (x_2, y_2)$ iff $y_1 < y_2$ or both $y_1 = y_2$ and $x_1 < x_2$,*
- *$(x_1, y_1) < (x_2, y_2)$ iff both $x_1 < x_2$ and $y_1 = y_2$ or both $x_1 = x_2$ and $y_1 < y_2$ or both $x_1 < x_2$ and $y_1 < y_2$.*

This is standard. Notice that the third ordering is included in the two other orderings and is symmetric in X and Y.[6]

We suppose now given a winning strategy σ for ΣA_i and a winning strategy τ for ΣB_j. We try to build a winning strategy δ for $\Sigma_{(i,j)}\, A_i B_j$.

---

[5] In Kreisel's example [9], B is Littlewood's theorem, and A is Riemann's hypothesis.

[6] The usual argument for proving that the third ordering is well-founded breaks this symmetry. I have not been able to produce an argument symmetric in X and Y for showing that the third ordering is well-founded.

In order to simplify the notations, we suppose that the indexes in the "A part" are disjoint from the ones in the "B part". Any occurrence in $\Sigma_{(i,j)} A_i B_j$ can thus be written $(i, j)k_2 \dots k_n$ and, if this occurrence is of length > 1, we associate to it an occurrence in A if k_2 is an index of the A part, namely $ik_2 \dots k_n$, or an occurrence in B if k_2 is an index in the B part, namely $jk_2 \dots k_n$.

In this way, to any sequence L of occurrences of length > 1 in $\Sigma_{(i,j)} A_i B_j$, we associate a *pair* $(p(L), q(L))$ of sequences of occurrences in A and B.

We define now the strategy δ. First, $\delta() = (i_0, j_0)$, where $\sigma() = i_0$ and $\tau() = j_0$. Next, a sequence L of non-empty occurrences, whose last element is an occurrence in the A part (resp. B part), is in the domain: of δ iff

(1) $p(L)$ is in the domain of σ,
(2) $q(L)$ is in the domain of τ,
(3) $\tau(q(L)) = j_L$ is a sequence of length 1 (resp. $\sigma(p(L)) = i_L$ is a sequence of length 1).

Furthermore, in this case, $\delta(L)$ is defined as follows: we compute first $\sigma(p(L)) = i_1 \dots i_n$, and take $\delta(L) = (i_1, j_L)i_2 \dots i_n$. In the case where the last occurrence of L is in the B part, then we compute $\tau(q(L)) = j_1 \dots j_m$ and we take $\delta(L) = (i_L, j_1)j_2 \dots j_m$.

In this way, we see that any branch of δ is an interwoven sequence of a branch of σ and a branch of τ, that is, it is of the form $M_1 N_1 M_2 \dots$ where $M_1 M_2 \dots$ is a branch of σ and $N_1 N_2 \dots$ a branch of τ. The map:

$$\begin{aligned} \mathbf{Dom}(\delta) &\to \mathbf{Dom}(\sigma) \times \mathbf{Dom}(\tau) \\ L &\longmapsto (p(L), q(L)) \end{aligned}$$

is then increasing if the product is given the third possible ordering of lemma 5. By this lemma, δ is a winning strategy.

We can formulate this result as follows:

LEMMA 6. *If ΣA_i and ΣB_j are regular, then so is $\Sigma_{(i,j)} A_i B_j$.*

This formulation, however, fails to emphasize the main point that our construction of δ is symmetric in σ and τ.

By contrast, two other non-symmetric constructions of δ are also possible. One of them "favors" σ : each time the last occurrence of L is in the A part, and $\sigma(p(L)) = i_1 \dots i_n$, then $\delta(L)$ is $(i_1, j_0)i_2 \dots i_n$ where $j_0 = \tau()$ is the first move of τ. In the case where the last occurrence of L is in the B part, $\delta(L)$ is defined as above: we compute $\tau(q(L)) = j_1 \dots j_m$ and take $\delta(L) = (i_L, j_1) \dots j_m$ with $i_L = \sigma(p(L))$. A branch of δ is of the form: $M_1 N_1 M_2 N_2 \dots$ where $M_1 M_2 \dots$ is a branch of σ but now *each* $N_1, N_2, \dots$ is a branch of τ. By lemma 5, δ so defined is still a winning strategy. There is a similar construction that "favors" τ instead.

In this way, we get three different solutions for the following problem:

PROBLEM 3. *Given $(A_i), (B_j)$ two families of existential formulae, C a Σ_1^0 formula, for all i, j a winning strategy for $A_i + B_j$, and winning strategies for the formulae $\Sigma\neg A_i$, and $C + \Sigma\neg B_j$, to compute a witness for the formula C.*

Therefore this can be seen as an example of "multiple" cut-elimination: from a proof of $\Pi_{ij}(A_i + B_j)$, a proof of $\Sigma\neg A_i$ and of $C + \Sigma\neg B_j$, we compute a witness for C.

3.2. Comparison with the double-negation interpretation. The double negation interpretation is another possible intuitionistic explanation of classical provability. We do not recall it here, but refer for instance to [13]. Via Curry-Howard correspondence between functional programs and proofs, it can be seen essentially as an interpretation of classical proofs as functional programs (see [13]). We find it interesting to analyze what the "distributivity problem" becomes in this framework: we get in a natural way two possible compositions of proofs, that are not symmetric. It seems furthermore quite difficult to get a symmetric composition.

Via double negation, the problem of distributivity becomes: given a proof f of $\neg(\Pi_i\neg A_i')$ and a proof g of $\neg(\Pi_j\neg B_j')$, how to produce a proof of $\neg(\Pi_{(i,j)}\neg(A_i'B_j'))$? (We denote by C' the double negation translation of C.) It is very convenient to use functional notations to analyze this problem, using λ terms for representing proofs in natural deduction. Recall that $\neg C$ is an abbreviation for $C \Rightarrow \bot$. Two ways are possible for combining f and g in order to produce a proof of $\neg(\Pi_{(i,j)}\neg(A_i'B_j'))$:

(1) One is $\lambda h.f(\lambda i\lambda u.g(\lambda j\lambda v.h((i,j),(u,v))))$,
(2) the other is $\lambda h.g(\lambda j\lambda v.f(\lambda i\lambda u.h((i,j),(u,v))))$.

These two ways are non-symmetric. There does not seem to be any functional way to get a symmetric composition which solves the distributivity problem. If this conjecture holds, there appears to be a fundamental difference between functional interpretation of classical logic (based on double negation interpretation) and our present explanation based on the notion of regular formulae and interaction between strategies.

Conclusion. We have presented a game-theoretic semantics of evidence for classical arithmetic, and a proof of validity of modus ponens based on this analysis. A natural extension, much needed for analyzing mathematical arguments, will be the treatment of quantification over function symbols. It is likely that, for such a generalization, in the case of an existential quantification $\exists\alpha\ldots$, $\exists$loise has to conjecture a law for α, law that may be refined according to the moves of $\forall$belard.

Appendix: Novikoff's proof. In this section, we present briefly Novikoff's proof (slightly modified) of the validity of modus ponens.

LEMMA 7. *If $B + A$ and $B + \Sigma C_i$ are regular then so is $B + \Sigma AC_i$.*

We refer to Novikoff's paper for a proof of this statement, which can also be proved directly using the notion winning strategy.

Let us say that a formula A is **eliminable** iff B is regular whenever $\neg A + B$ is. The core of Novikoff's argument is to show that A is eliminable whenever A is regular, by induction on the proof that A is regular.

LEMMA 8. *If $B + \Sigma\neg A_i$ is regular, and each A_i is an eliminable existential formula, then B is regular.*

PROOF. By induction on the proof that $B + \Sigma\neg A_i$ is eliminable. ⊣

COROLLARY 9. *If A_i is a family of eliminable existential formulae, then ΠA_i is regular.*

PROPOSITION 10. *Any regular formula is eliminable.*

PROOF. By induction on the proof that A is regular, we prove that it is eliminable. If A is universal, this follows from the corollary above. Otherwise, $A = \Sigma A_i$ and we prove by induction on the proof that $B + \Pi\neg A_i$ is regular that B is regular. This follows directly from lemmas 7 and 8. ⊣

We conjecture that, when we compare our notion of debate and this proof seen as an algorithm for computing a witness of a Σ_1^0 formula B from a winning strategy for A and $\neg A + B$, we get the same witness, and that both computations proceed actually in the same way (i.e., the values exchanged between the proofs are the same).

Acknowledgments. The starting point of this work was provided by an exercise of Gabriel Stolzenberg: to analyze the computational content of the proof that a boolean function on the natural numbers takes twice the same value considering it as a corollary of the (classical) fact that it takes infinitely many times the same value. He observed that doing this, using a double negation interpretation, revealed a surprising "break of symmetry" and this is analyzed in our last section. Important motivations for this work were also the original proof of Gentzen of consistency for number theory as presented in [2], talks of Jean-Yves Girard and Samson Abramsky on the "geometry of interactions," talks of Lennart Augustsson presenting very intuitively some results of [13] and several discussions with Hugo Herbelin on the problem of finding constructive contents of classical arguments. I would like also to thank Lars Hallnäs, Jan Smith, Bjorn von Sydow, Peter Dybjer, Chet Murthy and especially Karlis Cerans, Sergei Tupailo (who provided crucial criticisms) for enjoyable discussions on this topic.

Thanks finally to the anonymous referee.

REFERENCES

[1] S. ABRAMSKY, *Computational interpretations of linear logic*, ***Theoretical Computer Science*** (1993), pp. 3–57, Special issue for MFPS 1990.

[2] P. BERNAYS, *On the original Gentzen consistency proof for number theory*, ***Intuitionism and proof theory*** (A. Kino, J. Myhill, and J. E. Vesley, editors), North Holland, Amsterdam, 1970, pp. 409–417.

[3] A. BLASS, *Degrees of indeterminancy of games*, ***Fundamental Mathematicae***, vol. LXXVII (1972), pp. 151–166.

[4] A. CHURCH, *Review of Novikoff's article*, this JOURNAL, vol. 11 (1946), pp. 129–131.

[5] R. CONSTABLE, *The semantics of evidence*, ***Technical Report TR 85–684***, Cornell University, Department of Computer Science, Ithaca, New York, 1985.

[6] G. GENTZEN, ***The collected papers of Gerhard Gentzen***, North-Holland, Amsterdam, 1969, edited by M. E. Szabo.

[7] C.A.R. HOARE, ***Communicating sequential processes***, Prentice-Hall, 1985.

[8] S. C. KLEENE, ***Introduction to metamathematics***, North-Holland, 1952.

[9] G. KREISEL, *Interpretation of non-finitist proofs*, this JOURNAL, vol. 17 (1952), pp. 50–56.

[10] K. LORENZEN, *Ein dialogisches konskruktivitatskriterium*, ***Infinitistic methods***, Pergamon Press, 1962, Proceedings of the Symposium on the Foundations of Mathematics, PWN, Warszawa,1959, pp. 193–200.

[11] P. MARTIN-LÖF, ***Notes on constructive mathematics***, Almqvist and Wiksell, Stockholm, 1970.

[12] G. MINTS, *Proof theory in the USSR, 1925-1969*, this JOURNAL, vol. 56 (1991), pp. 385–424.

[13] C. MURTHY, *Extracting constructive content from classical proofs*, ***Ph.D. thesis***, Cornell University, 1990.

[14] P. S. NOVIKOFF, *On the consistency of certain logical calculus*, ***Matematiceskij sbornik (Recueil-Mathématique, T.12)***, vol. 54 (1943), pp. 230–260.

[15] W. W. TAIT, *Normal derivability in classical logic*, ***The syntax and semantics of infinitary languages*** (Jon Barwise, editor), Lecture Notes in Mathematics, vol. 72, Springer Verlag, 1968, pp. 204–236.

CHALMERS TEKNISKA HÖGSKOLA
AND UNIVERSITY OF GÖTEBORG
DEPARTMENT OF COMPUTER SCIENCES
S-41296 GÖTEBORG
SWEDEN

E-mail: coquand@cs.chalmers.se