# A semantics of evidence for classical arithmetic

Thierry Coquand*
Chalmers University

Preliminary version, June 1991

## Introduction

This note presents some remarks connected to Gentzen's first proof of consistency of arithmetic, that was actually never published by Gentzen himself, but instead appeared first in a paper of Bernays [1] (but see also [3]). As emphasized by Bernays, this argument is easier to follow than the first published proof. It can be read directly as a game-theoretic analysis of the notion of classical truth: a formula is classically true iff there is a winning strategy for a game defined by this formula. This provides a semantics of evidence for classical first-order arithmetic (the term "semantics of evidence" seems due to B. Constable, see [2]). Furthermore, Gentzen's proof leads directly to the result that an existential statement provable in classical arithmetic is provable intuitionistically.

More importantly, when expressed game-theoretically, the dynamic aspect of cut-elimination becomes clearer. We believe indeed that the main object of study here is the analysis of the possible sequence of moves in the strategies corresponding to classical proofs.

Such an analysis suggests strongly that it should be possible to find a cut-elimination proof of a different nature than Gentzen's which reflects and is inspired by this dynamic aspect. We try to motivate this point by presenting such a proof for cuts of a low level of logical complexity, and by a conjecture expressing the termination of an internal communication, result that would refine Gentzen's cut-elimination.

We discuss next a concrete example, due to Gabriel Stolzenberg, which suggests that it can be computationally inefficient to break a multiple cut in its component. In the simplest possible case that departs from usual cut-elimination, we sketch a way to do this "multiple cut-elimination." Here also, it is directly checked that this "protocol for multiple cuts" works for cuts of low logical complexity.

At the end of the paper we present an inductive formulation of $\omega$-logic, very close to Tait's formulation [9], which is readily seen to provide a computational content of classical arithmetical truth.

The contributions of this (preliminary) paper are:

- an "historical" contribution: we think it will be fair to attribute the result that an existential statement proved in Peano arithmetic has an intuitionsitic proof at least partially to Gentzen, since this is a direct corollary of his first proof of normalisation [1],

*coquand@margaux.inria.fr

[1] we conjecture that it is because Gentzen's interpretation of a proof was in general a non deterministic algorithm that his first proof was for a while forgotten

- a formulation of a conjecture that refines Gentzen's cut-elimination, with a proof in a restricted case (that hopefully will be completed for the less preliminary version of this paper),
- the analysis of a concrete example where it is clear that the "mutiple-conclusion" logic we manipulate cannot be simulated in a functional way, and so, the discovery of features of multiple-conclusion logic that are typical of parallel algorithms. We sketch then how to extend this to a truly parallel cut-elimination for classical arithmetic.

I would like to thank Gabriel Stolzenberg, Lars Hallnäs, Jan Smith, Peter Dybjer, Hugo Herbelin and Chet Murthy for enjoyable discussions on this topic. Karlis Cerans provided crucial critics.

# 1 A semantics of evidence

We start with a fixed language for arithmetic that contains (computable) functions like addition, multiplication and (decidable) basic relations, like equality, $\leq, \ldots$ We suppose that whenever an atomic relation $R$ is in this language we have another one $R^*$ which represents its complement, in such a way that $(R^*)^*$ is $R$.

The formulae are built inductively form atomic formulae by conjunction &, disjunction $\vee$, universal and existential quantification. The negation $\varphi^*$ is defined inductively from $\varphi$ as usual.

To simplify things, we will suppose that all formulae are prenex formulae in which universal and existential quantifications alternate, that is of the form $\forall x \exists y \forall z \ldots$, in which case we say that the formula is **universal**, or of the form $\exists x \forall y \exists z \ldots$, in which case we say that the formula is **existential.** All quantifier free formulae are decidable.

## 1.1 The intuitionistic case

We recall first what is a possible game-theoretic semantics of evidence for intuitionistic logic, as presented for instance in A. Ranta's thesis [8]. We consider the following game between Nature and Myself, which consists in making **moves,** that are existential or universal instantiations, in a given formula $\varphi$, which is called the **configuration** of the game. Myself is trying to establish the truth of formula $\varphi$, and Nature tries to produce a counter-example. If the formula is atomic, then it is decidable: if it is false, Nature wins, otherwise, Myself wins. If the formula is of the form $\exists n\ A[n]$, Myself should produce an integer $n_0$ and the game goes on with $A[n_0]$. If the formula is of the form $\forall n\ A[n]$, Nature produces an integer $n_0$ and the game goes on with the formula $A[n_0]$.

For this game, a formula $A$ can be defined to be intuitionistically true iff there is a winning strategy for Myself.

## 1.2 Extension to "multigames"

We can complicate this by allowing the configuration of the game to be a finite multiset of formulae. We write + the addition on multisets. The game stops when at least one formula is atomic and true, in which case Myself wins. In the other cases, Myself should make an instantiation whenever all formulae are existential, and Nature should make a move whenever

at least one formula is universal, by instantiating the universal formulae. If all formulae are atomic and false, then Nature wins.

In this version, there is a winning strategy for Myself for the configuration of "excluded middle" $A + A^*$, for any formula $A$ : Myself simply waits for Nature to move, and mimics her move in the dual formula.

For this notion of game however, it is not the case that there is a winning strategy for $\exists n \forall m\ [A[n]\ \vee\ A^*[m]]$ even in the case where $A$ is decidable. Indeed, suppose that Myself has such a winning strategy. Myself has to give a value $n_0$ for $n$, because the formula is existential. We know that if $A[n_0]$ does not hold, then we have $\forall m\ A^*[m]$. Otherwise, Nature can win by playing $m_0$ such that $A[m_0]$ holds. By checking whether $A[n_0]$ holds or not, we would thus extract a decision algorithm for $\exists n\ A[n]\ \vee\ \forall m\ A^*[m]$.

Notice however that, as pointed out already, there is a winning strategy for the "equivalent" multiset formula $\exists n\ A[n] + \forall m\ A^*[m]$ : Myself waits for an instantiation $m = m_0$ from Nature, and if $A^*[m_0]$ does not hold, win by playing $n = m_0$ (if $A^*[m_0]$ holds, then Myself wins already after Nature's move).

### 1.3 Games with "backtracking"

For getting a notion of game such that (intuitionistic) winning strategy contains classical provability, we allow backtracking for moves of Myself. This means that Myself can choose to complicate a configuration $M + \exists n\ A[n]$ where all the formulae are existential by both instantiating the formula $\exists n\ A[n]$ and keeping it, which produces the configuration $M + \exists n\ A[n] + A[n_0]$ where $n_0$ is the integer chosen by Myself. The moves of Nature are the same as before.

For this notion of game, there is a winning strategy for Myself for the configuration $\varphi$ iff $\varphi$ is classically true.

Instead of showing formally this equivalence, we will limit ourselves to show that if there is a winning strategy for the configuration $M + A + A$, then there is a winning strategy for the configuration $M + A$, and if there is a winning strategy for the configuration $M + A$ and a winning strategy for the configuration $N + A^*$, then there is a winning strategy for the configuration $M + N$.

This is enough to show that the notion of truth defined by the existence of a winning strategy has good properties. For instance, if we have a winning strategy for $N + A[0]$ and, for all $n$, a winning strategy for $M + A[n]^* + A[n + 1]$, then we deduce from these two closure properties that there is a winning strategy for all $n$ for $M + N + A[n]$.

The first claim is seen by simulating directly the moves of a strategy for $M + A + A$ by moves for the configuration $M + A$.

The second claim is more difficult, and we will present it as the proof of termination of some internal communications between two players following winnning strategies.

### 1.4 Two examples

There is now for instance a winning strategy for $\exists n \forall m\ [A[n]\ \vee\ A^*[m]]$. Myself chooses any instantiation for $n$, for instance $n = 0$, and keeps the formula, waiting for a $m = m_0$ given by Nature. If $A^*[m_0]$, then Myself wins, and if $A[m_0]$ then Myself chooses $n = m_0$ for its next move.

Another example, which shows that we cannot bound a priori the number of backtracking in Myself's guess, is the following strategy for the statement

$$\exists n \forall m\ [f(n) \leq f(m)],$$

seeing $f$ as an oracle. Myself starts by guessing an arbitrary value for $n$, for instance $n = 0$, and allows himself to backtrack. Nature plays then $m = u_1$. If $f(0) \leq f(u_1)$, Myself wins. If $f(u_1) < f(0)$, Myself backtracks and plays $n = u_1$, and allows himself to backtrack. Nature plays then $m = u_2$. If $f(u_1) \leq f(u_2)$, Myself wins. Otherwise, Myself backtracks and plays $n = u_2$, and allows himself to backtrack, and so on.

This will stop eventually, because $<$ is well-founded, but it is not possible to bound a priori (without knowing anything about $f$) the number of times that Myself will have to backtrack.

This explanation of classical truth is inspired by the first consistency proof for arithmetic by Gentzen, see [3, 1]. Note that Bernays, in [1], presents this proof using choice sequences, for representing the sequence of moves of Nature. We can use inductive definitions instead to represent the notion of choice sequence, as done for instance in [6].

### 1.5 The case of existence statement

Let us look at the special case of a winning strategy for a configuration $\exists n\ A[n]$, where $A[n]$ is a (decidable) atomic formula. We see the decision procedure for $A[n]$ as an oracle. To have a winning strategy in this case means that Myself will do a finite number of wrong guesses for $n$, until he eventually finds a $n_0$ such that $A[n_0]$. We can actually suppose that Myself always is doing some "auto-censure" by himself, so that he checks internally whether or not his guess is correct for an existential formula $\exists n\ A[n]$, where $A$ is atomic. With this assumption, a winning strategy for an existence statement is exactly a witness.

We thus get that the result "if an existence statement is provable in classical first-order arithmetic, then it is provable intuitionistically" follows from the identification of classical truth with the existence of a winning strategy.

### 1.6 Simple backtracking

In all the examples we have presented so far, the backtracking that Myself uses is of a particular nature. Myself never changes his mind about a value he has considered as wrong (we will precise this notion later). We call this behaviour of Myself **simple backtracking**.

This notion of simple backtracking is interesting because it does involve backtracking, but it is however a simple enough behaviour so that we can give a complete analysis of what is happening in the case where all players follow simple backtracking. In particular, we will be able to analyse later the case of multi-cuts for simple backtraking, that involves already real concurrency.

In order to analyse a little more this notion of simple backtracking, we introduce the following notations. In the history of configurations of a game which has $M + A$ as an initial configuration, where $A$ is existential, we follow the moves in $A$ by writing $A_1$, $A_2$, ... the instantiations of $A$ (due to Myself), and then $A_{11}$, $A_{21}$, ... the respective instantiations of these instantiations (due to Nature), and so on. If a formula $B$ is of the form $A_{n_1 \ldots n_p}$, or $A^*_{n_1 \ldots n_p}$, we say that $n_1 \ldots n_p$ is the **index** of the formula $B$, and we write $n_1 \ldots n_p = \mathsf{ind}(B)$. We say that

a sequence $n_1 \dots n_p$ is a **direct extension** of a sequence $m_1 \dots m_q$ iff $p = q + 1$, and $n_i = n_i$ for $i < p$.

To say that the backtracking is **simple for** the formula $A$ is to say that once we have observed the sequence of moves

$$A,\ A + A_1,\ A + A_{11},\ A + A_{11} + A_2, \dots, A + \dots + A_{n_1 \dots n_p}, \dots$$

with $p$ even, then the next move of Myself will be $A + \dots + A_{m_1 \dots m_q}$, where $m_1 \dots m_q$ is strictly bigger than $n_1 \dots n_p$ for the alphabetical ordering on sequence of integers.

This is the case if the formula $A$ is of the form $\exists x \forall y\ B[x, y]$, where $B$ is atomic, simply because in this case, Myself cannot play $A_{111}$. Simple backtracking holds thus when we consider formulae of low logical complexity.

If Myself follows a strategy that uses only simple backtracking for an existential formula $A$, then we can represent Myself's moves in $A$ (for a given game against nature) as a sequence of the form

$$A,\ A_1,\ A_{11},\ A_{111},\ A_{1111},\ A_{112},\ A_{1121},\ A_{113}, \dots$$

Such a sequence can be read as follows (if the sequence of quantifiers of $A$ is $\exists x \forall y \exists z \forall t \dots$): Myself makes a first guess $x = x_1$ about the value of $x$. Nature then answers $y = y_{11}$. Myself persists in his choice by guessing $z = z_{111}$, this choice being refuted by Nature, who plays $t = t_{1111}$. At this point, Myself changes his mind about the choice of $z$ (he considers that Nature has really refutated it and does not persist in his choice, leaving the last refutation of Nature $t_{1111}$ without answers). He tries then $z = z_{112}$. This is refuted by Nature who plays $t = t_{1121}$.

One can well imagine a strategy where Myself changes his mind also about the fact that he was wrong. This is a more subtle kind of behaviour.

The analogy with learning theory, that Myself makes successive guesses according to the moves of Nature, seems clear here and should be precised. We will limit ourselves here to point out this analogy.

It would be nice if we can insure that for all classically true multiset $M$, it is possible to find a winning strategy using only simple backtracking. Though we don't have any concrete counter-example, we suspect that this is not the case, since we don't see how to get a strategy for the configuration $M + A$ from a strategy for the configuration $M + A + A$ if we impose strategies to use only simple backtracking. Any strategy for $M + A + A$ can be simulated by a strategy for $M + A$. Even if for both $A$, a strategy for $M + A + A$ uses only simple backtracking, this may not be the case for the simulated strategy for $M + A$.

Here is an example of a sequence of move that uses more than simple backtracking:

$$A,\ A + A_1,\ A + A_{11},\ A + A_{11} + A_2,$$
$$A + A_{11} + A_{21},\ A + A_{11} + A_{21} + A_{111},$$
$$A + A_{11} + A_{21} + A_{1111},\ \ A + A_{11} + A_{21} + A_{1111} + A_{211}, \dots$$

The intuition is that Myself, when he plays $A_{111}$, changes his mind about his first backtracking, and does not answer to the refutation $A_{21}$ of his last play. But when Nature refutes this last play $A_{111}$ by playing $A_{1111}$, Myself changes his mind again and comes back to the choice of his second instantiation of $A$. Myself tries by playing $A_{211}$ to refute the previous refutation of Nature $A_{21}$ he had left without answers.

## 2 A dynamic view of cut-elimination

Let us imagine that we are playing against Nature for a given configuration. We can see a strategy for this configuration as a player we have at our disposition. Each time Nature plays, we transmit her move to this player. When all formulae are existential, we wait to see what is the move of this player on this configuration. We follow the strategy by copying his move.

With this picture in mind, we can conceive that it takes more or less time for the player to answer our question. We can consider a strategy to be **total** if we are sure that, eventually, after a finite amount of time, the player will answer. It is then natural to consider also **partial** strategies, that are like players who stay mute, thinking for a too long time about their next move.

Given two strategies for $M + A$ and $N + A^*$, we show how to build a "partial" strategy for $M + N$. The situation is exactly the same as in concurrency theory where partial processes appear when we use internal communication: a deadlock due to "infinite internal chatter" can happen when we combine these two strategies. But, and this is what the cut-elimination result expresses, if both strategies are winning strategies, then we do get a total strategy which is a winning strategy.

It seems possible to give a definition of this compound strategy by following Gentzen's argument. This corresponds to a direct study of the following property of a multiset of formulae $M$ "there exists a winning strategy for $M$". One gives a direct inductive definition of this property, and one shows that if both $M + A$ and $N + A^*$ have this property, then so does $M + N$. The argument is a double induction, first on the complexity of the cut-formula, and then on the proof that the strategies are winning. Such a proof is presented in the last section. If we follow this approach however, it is not so clear what is the "structure" of the algorithm we get.

It seems much more interesting to see if a direct termination argument can be given, based on an analysis of what are the possible interactions between two players $I$ and $II$.

### 2.1 Definition of the compound strategy

Here is an informal description of how this compound stategy is built. We assume that Myself has at his disposition two coplayers $I$ and $II$. The player $I$ represents a strategy for the game of configuration $M + A$ and the player $II$ a strategy for the game of configuration $N + A^*$. Myself follows then the following protocol for the game against Nature of configuration $M + N$.

As long as one formula in $M$ or $N$ is universal, Myself waits for an instantiation coming from Nature. It transmits then this instantiation to the player $I$ or $II$ that is concerned with it.

After a finite number of such moves, both $M$ and $N$ have only existential formulae, so that Nature is waiting for an existential instantiation by Myself. Myself noticed that at least $A$ or $A^*$ is existential. Let us say that $A$ is existential. In this case, Myself asks to the player $I$ what is his move. Myself knows that $I$ will answer, because all the formulae in the configuration of the player $I$ are existential. There are two cases:

- $I$ instantiates a formula in $M$, then Myself does the same move and the game goes on,
- $I$ instantiates the formula $A$. This is the difficult case.

In the second difficult case, Myself has not yet available any play against Nature. Indeed, Nature does not "see" the formula $A$ and so, cannot transmit $I$'s move as in the first case.

There is a simple subcase however for which it is clear what Myself should do: if the player $I$ instantiates the formula $A$ without keeping it. In this case, the formula $A$ becomes $A_1$, and Myself transmits this move to the player $II$. The configuration of $I$ is then $M + A_1$, and the configuration of $II$ is $N + A_1^*$. The situation is the same as before, except that Myself is now waiting for $II$'s move. This "ping-pong" kind of play between $I$ and $II$ (via Myself) goes on for a finite amount of time, because the formula $A$ is finite.

If during this internal communication, the formula $A$ (resp. $A^*$) becomes true, then the dual formula becomes false, and the game goes on with only the player $II$ (resp. $I$), since this player follows then a winning strategy for $N$ (resp. $M$), the other player becoming inactive. If both players follow a winning strategy, it is then clear that Myself follows a winning strategy by copying one of these two players.

The only remaining subcase is when Myself gets to a position where, let say, $I$ has a move in $A$, but this move is such that $I$ keeps the formula $A$ (allowing backtracking). In such a case, it is not so clear what Myself can do. Here is a possibility, that we shall analyse (and which corresponds to Gentzen's solution).

Myself transmits the move to the player $II$, the formula $A^*$ becoming $A_1^*$, but also Myself *keeps a copy* of the player $II$ in its initial configuration. The motivation is that Myself does not know whether or not the choice of the player $I$ is definitive, and so, it makes sure that he can continue in case of a change of mind of the player $I$.

Once this is done, the configuration is almost like the previous subcase, except that Myself allows $I$ to backtrack in his choice.

How is the game going on?? Myself asks to the latest copy of the player $II$, who plays now with a configuration $N + A_1^*$, what is his move. If this move is in $N$, it is transmitted to Nature. If this move is in $A_1^*$, Myself proceeds as before, i.e.:

- if this move is without backtracking ($II$ is sure of his guess), then the configuration of $II$ becomes $N + A_{11}^*$, and Myself transmits this move to the player $I$, whose configuration becomes $M + A + A_{11}$,
- if this move is with possible backtracking, then Myself does as before. The configuration of $II$ becomes $N + A_1^* + A_{11}^*$, and Myself transmits this move to the player $I$, whose configuration becomes $M + A + A_{11}$, but Myself also keeps a copy of the player $I$ in his configuration $M + A + A_1$, in case of a possible backtracking of $II$, and so on.

This finishes the description of the cut-elimination process.

A concrete instance of such a situation is the problem where we have a proof of a $\Sigma_0^1$ statement $C$ by proving $C, A^*$ and $C, A$ (for instance, $C$ is Littlewood's theorem, and $A$ is Riemann's hypothesis). This cut-elimination process, if it terminates, gives a way of computing a witness for $C$ from the two given proofs of $C, A^*$ and $C, A$.

## 2.2 Analysis of the problem of termination

The partial correctness of the compound strategy described in the previous subsection is clear. That is, if the players $I$ and $II$ follow a winning strategy for their respective configuration, it is clear that, if a game between Nature and Myself terminates, then Myself wins. However, it is not clear that the internal moves between the two players $I$ and $II$ terminate. In this subsection, we want to analyse the nature of the problem of termination.

First, it is not restrictive to assume that both players $I$ and $II$, when they make a move in $A$, are doing an instantiation with possible backtracking. Second, we can suppose that there is no moves by $I$ in $M$ and no moves by $II$ in $N$, so that we can restrict our attention to the moves in the formula $A$ only. That is, we suppose that we have a (partial) strategy for $A$ and a (partial) strategy for $A^*$, and we analyse what happens if we let the strategy for $A$ play against the strategy for $A^*$. We can then analyse the possible "interaction paths": we are sure that we will observe the moves

$$A + A_1,\ A_1^* + A_{11}^*,$$

and for the next move, there is a choice: $A + A_{11}$ can become $A + A_{11} + A_{111}$ or $A + A_{11} + A_2$, and so on.

What we have to show is that if these moves come from winning strategies, then this interaction path is finite.

The problem appears then to be the following. We know that a winning strategy (for the player $I$) will win against any player that does not backtrack (and hence, in any such game, the player $I$ will backtrack only a finite number of time). We want to generalise this to a play against a winning strategy (of $II$), which may backtrack. It is possible to show that if the strategy for $II$ bactracks only a finite number of time, then the game will stop (because we have then a finitely branching tree, which has finite branches). The problem is that, a priori, the only way to be sure that this will happen is to show that $I$ will backtrack a finite number of time. So there is a circularity here.

We can however formulate this problem as a pure problem of termination. The interaction can be represented as a sequence of formulae

$$B_0 = A^*,\ B_1 = A + A_1,\ B_2 = A_1^* + A_{11}^*,\ B_3 = A + A_{11} + A_2, \ldots$$

such that each $B_k$ is a sum of formulae $C_1 + \ldots + C_n$ where

1. all $C_i$ are existential for $i < n$, and $C_n$ is universal, we call $C_n$ the **end formula** of $B_k$, and we write $h(B_k) = C_n$, $t(B_k) = C_1 + \ldots + C_{n-1}$,
2. there is exactly one $i < n$ such that $\mathsf{ind}(C_n)$ is a direct extension of $\mathsf{ind}(C_i)$. Furthermore, $\mathsf{ind}(C_n)$ is the least direct extension of $\sigma$ for the lexicographical ordering that does not occur already in $B_0, \ldots B_{k-1}$; we say then that $i$ is **answered** in $B_k$,
3. for each $i < n$, the dual $C_i^*$ appears as the end formula of exactly one $B_j$, for one $j < k$,
4. if $i$ is answered in $B_k$, then $t(B_{k+1}) = t(B_i) + h(B_k)$.

The formulae $B_0, \ldots, B_k$ corresponds to the copies of the players $I$ and $II$. We call such a sequence $B_0, \ldots, B_k$ an **interaction sequence.**

The refinement of Gentzen's cut-elimination is that such an interaction sequence is finite, if the players follow a winning strategy. Gentzen's argument (see the last section) provides only the existence of a winning strategy, without describing it. It does seem possible however to use a similar argument to show that the interaction sequence is finite, as will be shown in the next version of this paper.

### 2.3 Total correctness in some restricted cases

A termination argument is readily given if $A$ is of low logical complexity, for instance of the form $\exists x\ B[x]$, or $\exists x \forall y\ B[x,y]$. This becomes more complicated in the case $\exists x \forall y \exists z\ B[x,y,z]$, and we leave to the reader an analysis of all possible behaviours of cut-elimination in this case.

We conjecture the termination of the algorithm in the general case. We will prove here only the case of simple backtracking.

With this added assumption, we use that $A$ is finite, of depth $n$, and we remark that the number of formulae extension of $A_{n_1 \ldots n_p}$ occuring in the interaction sequence is finite, by induction on $n - p$.

### 2.4 No-counter example interpretation

Another method (maybe inspired by Gentzen's proof) of giving a computational meaning of arithmetical truth is the no-counter example interpretation due to Kreisel. This is described for instance in the introduction of [6]. One can see the present "interaction approach" as an attempt towards the analysis of a computation at higher-type, in the spirit of Kleene 78 [5].

## 3 Towards a "symmetric" cut-elimination

We will analyse now a "multiple cut". We will limit ourselves to the case of a cut of the following form: we suppose to have a strategy for the games of configurations $M + A$, $N + A^* + B^*$ and $L + B$, and we try to build from these strategies a strategy for the game of configuration $M + N + L$.

It appears that there is only one choice if $A$ or $B$ is universal. If both $A$ and $B$ are existential however, there are several choices. The main point of this paper is to show that the usual two choices: first eliminate the cut between $M + A$ and $N + A^* + B^*$, then between $M + N + B^*$ and $L + B$, or the opposite solution, first eliminate the cut between $L + B$ and $N + A^* + B^*$, then between $L + N + A^*$ and $M + A$, not only lead to distinct results in general, but also are not natural w.r.t. the present game-theoretical analysis of cut-elimination.

### 3.1 A concrete example

This phenomena is particularly clear for the following concrete exemple, which is due to Gabriel Stolzenberg. It involves a typically classical lemma: the "infinite box principle".

The example is the following. We suppose given as an "oracle" a stream of 0 and 1. Classically, there are infinitely many 0, or infinitely many 1. The question is about a possible computational meaning of this assertion.

Let us represent the stream of 0 and 1 by a parameter $f$ which is a unary function symbol. We represent a computational meaning of the infinite box principle as a winning strategy for the game of configuration

$$\forall x_0 \exists y_0\ [x_0 \leq y_0\ \&\ f(y_0) = 0]\ + \forall x_1 \exists y_1\ [x_1 \leq y_1\ \&\ f(y_1) = 1],$$

that we will write $A(0) + A(1)$. Here is such a winning strategy: Myself waits for two instantiations $x_0 = u_0$ and $x_1 = u_1$ from Nature. When Myself gets these values, he computes the value of $u = \max(u_0, u_1)$ and asks to the oracle the value of $f(u)$. If $f(u) = 0$ Myself wins by playing $y_0 = u$ and if $f(u) = 1$, Myself wins by playing $y_1 = u$.

This interpretation seems very natural.

The question now is to see how to use this "computational" interpretation to do some effective computation. Let us analyse a trivial use of this lemma: from the infinite box principle, we deduce that there are at least two 0s or at least two 1s. Indeed, if there are infinitely many 0, there are two 0s (by picking the first two 0s), and similarly in the other case.

We have so a winning strategy for the configuration

$$\exists a_0 \exists b_0\ [a_0 < b_0\ \&\ f(a_0) = f(b_0) = 0]\ + \exists x_0 \forall y_0\ [y_0 < x_0\ \vee\ f(y_0) = 1],$$

i.e. if there are infinitely many 0s, then there are two 0s. We will write $M(0) + A(0)^*$ this configuration. and a winning strategy for the configuration

$$\exists a_1 \exists b_1\ [a_1 < b_1\ \&\ f(a_1) = f(b_1) = 1]\ + \exists x_1 \forall y_1\ [y_1 < x_1\ \vee\ f(y_1) = 0].$$

i.e. if there are infinitely many 1s, then there are two 1s. We will write $M(1) + A(1)^*$ this configuration.

Let us precise this winning strategy for the configuration $M(0) + A(0)^*$. Myself starts by instantiating $x_0 = 0$, keeping the formula $A(0)^*$. Nature answers then by giving $y_0 = u$. If we have $u < 0\ \vee\ f(u) = 1$, then Myself wins. If we have $f(u) = 0$, then Myself backtracks in his choice of $x_0$, and choses now $x_0 = u + 1$. Nature answers by giving $y_0 = v$. If we have $v < u + 1\ \vee\ f(v) = 1$, then Myself wins. If we have $u + 1 \leq v$ and $f(v) = 0$, then Myself wins by playing $a_0 = u$ and $b_0 = v$.

We have now three winning strategies for the respective configurations $M(0)+A(0)$, $A(0)^*+A(1)^*$ and $A(1) + M(1)$, and we want a winning strategy for the configuration $M(0) + M(1)$. Notice indeed that such a winning strategy will provide us with two 0s or two 1s.

One way to solve this problem is to "put parenthesis". We analyse this way first.

### 3.2 "Usual" cut-elimination is not symmetric

It consists in reducing the problem of multiple cuts to the problem of simple cut. Symbolically, we want to do

$$\mathbf{CUT}(M(0) + A(0), A(0)^* + A(1)^*, A(1) + M(1))$$

and we do this by doing either

$$(*) \qquad \mathbf{CUT}(\mathbf{CUT}(M(0) + A(0), A(0)^* + A(1)^*), A(1) + M(1))$$

or by doing

$$(**) \qquad \mathbf{CUT}(M(0) + A(0), \mathbf{CUT}(A(0)^* + A(1)^*, A(1) + M(1))),$$

using the algorithm described above.

We will not do it explicitely here, leaving this as an exercise for the reader. The important points are that

- we *do not* get the same algorithm doing (*) and doing (**),
- both algorithms (*) and (**) are not symmetric w.r.t. 0/1, that is, they do not provide the same answer if we interchange 0 and 1 in the values of the oracle $f$.

### 3.3 A symmetric cut-elimination

It is remarkable that, on this simple example, a way of doing cut-elimination suggested by "common sense", which is neither (*) nor (**), furnishes an algorithm that is symmetric w.r.t. 0/1.

More generally, in the case of a cut between $A$, $A^* + B^*$ and $B$ where $A$ and $B$ are existential, there seems to be a canonical way of doing the cut-elimination in the case of simple backtracking. This way differs from the one where we put parenthesis in general.

We will analyse this on one possible interaction sequence (which corresponds to one possible interaction sequence for the example described above).

Since $A$ and $B$ are existential, the corresponding strategies guess first values for them, with possible backtracking: $A_1$ and $B_1$. Then, Myself asks what is the move for $A_1^* + B_1^*$. Let say it is $A_{11}^*$. In this case, we consider that the choice $A_1$ has been refuted, and Myself transmits this refutation to the corresponding player. This player can either persist in his choice playing $A_{111}$, or changes his mind, playing $A_2$. In this last choice, since only simple backtracking is allowed, Myself can naturally consider that the choice $A_1$ has been definitively refuted and will never come back to this choice again. So, Myself asks what is the move for $A_2^* + B_1^*$. If the answer is $B_{11}$, and the move for $B_1 + B_{11}$ is $B_2$, it is natural that Myself asks what is the move for $A_2^* + B_2^*$, and so on.

But this is not what will happen if Myself tries to evaluate

$$\mathbf{CUT}(\mathbf{CUT}(A, A^* + B^*), B).$$

For this "protocol", Myself asks instead what is the move for $A_1^* + B_2^*$, forgetting completely what happened about $A$.

One can generally expect inefficiency (at least in the case of simple backtracking) if Myself follows the protocol

$$\mathbf{CUT}(\mathbf{CUT}(A, A^* + B^*), B).$$

In this case indeed, whenever the player associated with the formula $B$ tries a new instantiation $B_i$ for $B$, Myself comes back to the first instantiation for $A$, and asks what is the move for $A_1^* + B_i^*$.

Symmetrically, if Myself follow the protocol

$$\mathbf{CUT}(A, \mathbf{CUT}(A^* + B^*, B)).$$

In this case, whenever the player associated with the formula $A$ tries a new instantiation $A_i$ for $A$, Myself comes back to the first instantiation for $B$, and asks what is the move for $A_i^* + B_1^*$.

The symmetric protocol, which seems natural, is instead that Myself asks systematically the move for $A_i^* + B_j^*$ where $A_i$ (resp. $B_j$) is the last instantiation of $A$ (resp. $B$) that has been played. Furthermore, if Myself follows this protocol, then a given game can be analysed as two sequences of interaction for $A$ and $B$ that are interleaved, hence a direct termination argument.

Notice that this is a new "ternary" way of doing cut-elimination, which is not reducible to a combination of two "binary" cuts.

In the case where $A$ or $B$ is universal, then the "ternary" cut-elimination is equivalent to a combination of "two" cuts (except of doing less copies.) This is what happened, in a iterated way, with the cut-elimination procedure presented above compared to Gentzen's cut-elimination.

This analysis can be extended to the case of a "multi-cut" $A$, $A^* + B^*$, $B$, with $A$, $B$ of arbitrary complexity, but the players follow a strategy of simple backtracking.

# 4 An inductive presentation of $\omega$-logic

For sake of comparison, we reformulate usual definitions of $\omega$-logic in the framework of generalised inductive definitions.

We define inductively when a multiset $M$ of formulae is (classically) **true**. There are the following clauses:

- if $M$ contains a true atomic formulae, then $M$ is true,
- if there exists $n_0$ such that $M + A[n_0]$ is true, then $M + \exists n\ A[n]$ is true,
- if there exists $n_0$ such that $M + \exists n\ A[n] + A[n_0]$ is true, then $M + \exists n\ A[n]$ is true,
- if $M + A + B$ is true, then $M + A \ \vee \ B$ is true,
- if $M + A$ and $M + B$ are true, then $M + A \ \& \ B$ is true,
- if $M + A[n_0]$ is true for all integers $n_0$, then $M + \forall n\ A[n]$ is true.

Only the last clause is not finitary.

If we forget the point that in the game-theoretic presentation we consider only prenex formulae, the main difference is that in the game-theoretic presentation, we have to use the last rule whenever one formula is universal in the multiset of sequents. It follows that if there is a winning strategy for a configuration $M$, then $M$ is true with the present definition.

**Lemma 1** The following properties hold

- if $A$ is a false atomic formula, and $M + A$ is true, then $M$ is true,

- if $M + A \ \vee \ B$ is true, then $M + A + B$ is true,
- if $M + A \ \& \ B$ is true, then $M + A$ and $M + B$ are true,
- if $M + \forall n \ A[n]$ is true, then $M + A[n_0]$ is true for all integer $n_0$.

**Proof:** All these properties are of the form: if $M$ is true, then $M'$ is true, and they are proved directly by induction on the proof that $M$ is true.

**Lemma 2** If $M + A + A$ is true, then so is $M + A$.

**Proof:** By double induction: first on the formula $A$, and then by induction on the proof that $M + A$ is true, using the previous lemma 1.

**Proposition 1** If $M + A$ and $N + A^*$ are true, then so is $M + N$.

**Proof:** By double induction, first on the formula $A$, and then by induction on the proofs that $M + A$ and $N + A^*$ are true. Let us look at one case: $A$ is $\exists n \ B[n]$ and $M + A$ is true because $M + B[n_0] + A$ is true. Then, by lemma 1, we know that $N + B[n_0]^*$ is true. By induction hypothesis, by a cut between $N + A^*$ and $M + B[n_0] + A$, we get that $N + M + B[n_0]$ is true. By induction hypothesis, since $B[n_0]$ is less complex than $A$, we get that $N + N + M$ is true. By lemma 2, $N + M$ is true.

The important remark is that, with this definition, cut-elimination is not an associative operation.

## Conclusion

We have presented a conjecture of termination of an internal communication, that would refine Gentzen's cut-elimination. This conjecture is valid in the case of cuts of low logical complexity, and in a restricted case of "simple backtracking." The same idea in the case of multiple cuts leads to a protocole of cut-elimination distinct in general from the one where we decompose the multiple cut in binary cuts.

One important point to precise is the connection between the symmetric protocol we presented and the fact, noticed by Hugo Herbelin, that there does exist a Gentzen like cut-elimination procedure that lead to a symmetric answer. It is not clear at all yet what is the game-theoretical meaning of this procedure.

## References


[1] Bernays P. (1968) "On the original Gentzen consistency proof for number theory." In Intuitionism and Proof Theory, Kino, Myhill, Vesley eds.

[2] Constable, R. "The semantics of evidence." Technical Report TR 85-684, Cornell University, Department of Computer Science, Ithaca, New York, May 1985.

[3] Gentzen G. (1969) "Collected Works." North-Holland, Szabo ed.

[4] Isles, D. "A Finite Analog to the Lowenheim-Skolem Theorem." Draft, 1990.

[5] Kleene, S.C. (1978) "Recursive Functionals and Quantifiers of Finite Types Revisited II." in The Kleene Symposium, North-Hlland, J. Barwise, H.J. Keisler and K. Kunen eds.

[6] Martin-Löf P. (1968) "Notes on Constructive Mathematics." Almqvist & Wiksell ed.

[7] Martin-Löf P. "Hauptsatz for the Intuitionistic Theory of Iterated Inductive Definitions." in Proceedings of the Second Scandinavian Logic Symposium, North-Holland, J.E. Fenstad ed.

[8] Ranta A., Ph. D. Thesis (1990), Stockholm.

[9] Tait W.W. (1968) "Normal Derivability in Classical Logic." Springer Lecture Notes in Mathematics 72, J. Barwise ed.