ISSN 0105-8517

Proceedings of the

CLICS Workshop – Part I

Aarhus University, 23-27 March 1992

Glynn Winskel, ed.

DAIMI PB – 397-I
May 1992

COMPUTER SCIENCE DEPARTMENT
AARHUS UNIVERSITY
Ny Munkegade, Building 540
DK-8000 Aarhus C, Denmark

CLICS WORKSHOP
Aarhus University, Denmark

PROGRAMME

[1]There is no contribution for this talk.

References

R. D. Tennent. Semantical analysis of specification logic. *Information and Computation*, 85(2):135–162, 1990.

P. W. O'Hearn and R. D. Tennent. Semantical analysis of specification logic, part 2. Technical Report 91-304, Department of Computing and Information Science, Queen's University, Kingston, Canada, 1991. To appear in revised form in *Information and Computation*.

P. W. O'Hearn and R. D. Tennent. Semantics of local variables. Technical Report ECS-LFCS-92-192, Laboratory for Foundations of Computer Science, Department of Computer Science, University of Edinburgh, 1992. To appear in *Applications of Categories in Computer Science* (M. P. Fourman, P. T. Johnstone and A. M. Pitts, editors), the Proceedings of the London Mathematical Society Symposium on Applications of Categories in Computer Science, Durham, England, July 20–30, 1991, to be published by Cambridge University Press.

THIERRY COQUAND ①

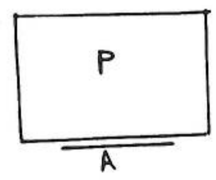
. Intuitionistic analysis of classical logic

. Analysis of the "computational content" of classical proofs

. Motivated by the first consistency proof of arithmetic by Gentzen (1936)

" 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 "

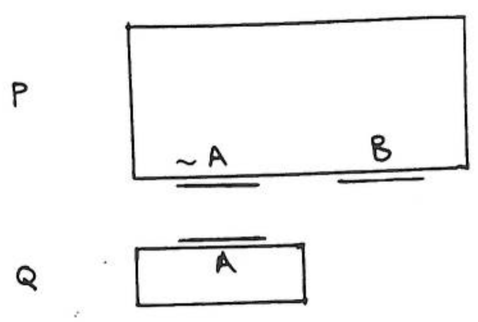
Here the "finitist sense" of a proposition will be an interactive program, a strategy for a game associated to the proposition



A: "interface" of P

(2)

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

(3)

. Intuitionistic meaning of quantifiers

. an intuitionistic proof of a formula

$\forall x \; \exists y \; \forall z \; \exists t \quad R(x, y, z, t)$ (R: decidable relation)

can be seen as a winning strategy for ∃loise in a game between two players

{ ∀belard
{ ∃loïse

∀	$x = a$			
∃		$y = b$		
∀			$z = c$	
∃				$t = d$

does $R(a,b,c,d)$ hold ?

yes → ∃ wins

no → ∀ wins

(4)

$$\exists x \ \forall y \ [D(x) \Rightarrow D(y)]$$
$$\exists x \ \forall y \ [f(x) \leq f(y)]$$

where $f : N \to N$ is an "oracle"

There is no <u>computable</u> winning strategy

For ∃loïse

We allow ∃loïse to "change her mind"

∃	$x = 0$		
∀		$y = b_1$	
∃	$x = b_1$		if $f(b_1) < f(0)$
∀		$y = b_2$	
∃	$x = b_2$		if $f(b_2) < f(b_1)$

⋮

∃loïse wins eventually because N is well-founded

$$f(0) > f(b_1) > f(b_2) > \dots$$

<u>Remarks:</u> . ∃loïse "learns" from the environment

. the first move $x = 0$ is a "guess"

successive approximation towards a solution

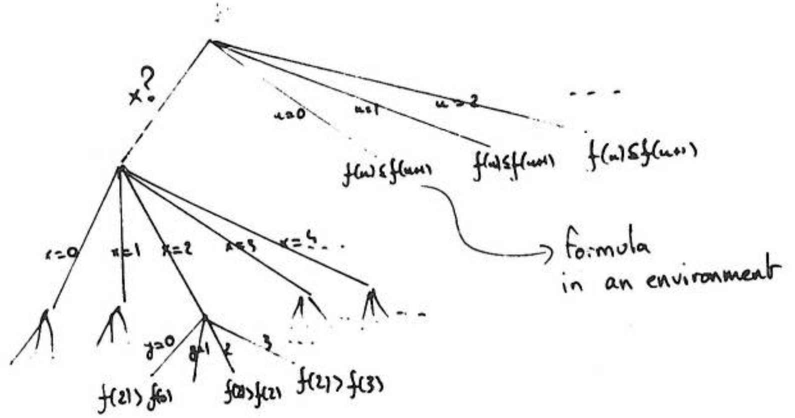
(5)

In general ∨ ∃loïse
∧ ∀belard

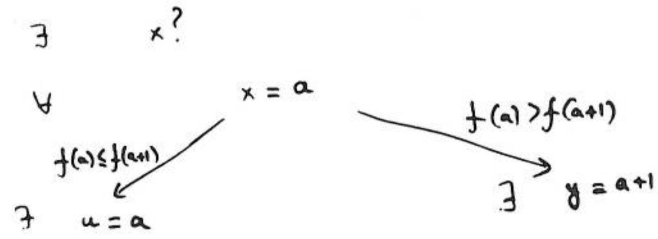
and a formula is a ∧ ∨ tree, possibly infinitely branching where leaves are decidable closed formulae

$$[\exists x \ \forall y \ [f(x) \leq f(y)]] \Rightarrow \exists u [f(u) \leq f(u+1)]$$

$$\forall x \ \exists y \ [f(x) > f(y)] \ \vee \ \exists u [f(u) \leq f(u+1)]$$



Strategy for ∃loïse



(6)

Problem for representing modus - ponens

" truth semantics " for classical logic ?

strategies described so far $\longleftrightarrow$ cut-free proofs

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

tree picture

" cooperation " betwen proofs via modus-ponens

P $\exists x \forall y \; [f(x) \le f(y)]$

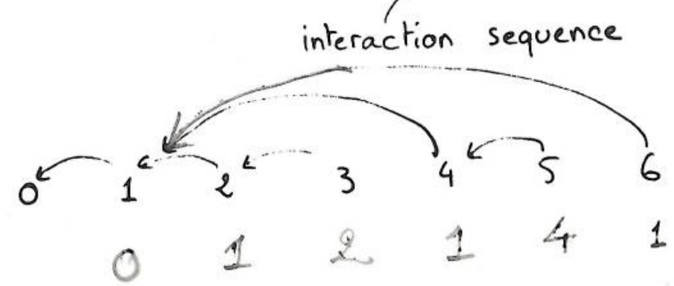
Q $\forall x \exists y \; [f(x) > f(y)] \;\vee\; \exists u \; f(u) \le f(u$

P and Q together

Q (P) $\exists u \; f(u) \le f(u+1)$

$f(0) = 10$ $f(1) = 0$ $f(2) = 5$ $f(3) = 2 \cdots$ (+)

1	Q	x ?	answers 0
2	P	$x = 0$	answers 1
3	Q	$y = 1$	answers 2
4	P	$x = 1$	answers 1
5	Q	$y = 2$	answers 4
6	P	$x = 2$	answers 1
7	Q	$u = 3$	



(8)

Interaction sequences first interaction of 2 cut-free proofs

$\varphi(1)$ $\varphi(2)$ $\varphi(3)$ ...

- $\varphi(1) = 0$
- $\varphi(n) < n$ φ changes parity

If one defines inductively

$$V(0) = \emptyset \qquad V(1) = \{0\}$$

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

then $\varphi(n) \in V(n)$

Examples $\varphi(1) = 0$ $\varphi(2) = 1$ $\varphi(3) = 2$ or 0 ...

The case where the environment does not change its mind

$$\varphi(n) = n-1 \quad \text{if } n \text{ is even}$$

(9)

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

They both can change their mind

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

(10)

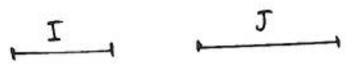
Analysis of one interaction

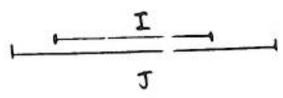
$\varphi(1)$ $\varphi(2)$ $\varphi(3)$ $\varphi(4)$ .... $\varphi(n)$ ....

Definitive interval $[\varphi(n), n]$ $n \notin \mathrm{Im}\,\varphi$
arguments that are not refuted

(1) The definitive intervals form a nest structure

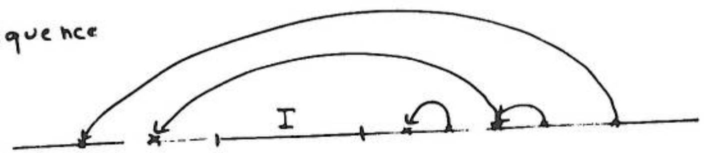
disjoint





follows from

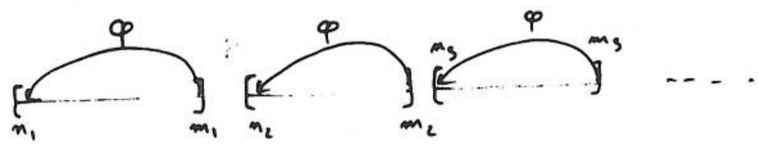
(2) If we take away a definitive interval, what is left is an interaction sequence



Main proposition

If $\varphi(1)$ $\varphi(2)$ $\varphi(3)$ ... infinite interaction sequence, then there exists

$n_1 = \varphi(m_1)$, $n_2 = m_1 + 1 = \varphi(m_2)$, ...



$$n_k = \varphi(n_{k+1} - 1)$$

this gives the finiteness of interaction of cut-free proofs.

(12)

A is a formula

total element of $[\![A]\!]$? → may be partial

strategy for the debate of topic A

which is "winning" in the sense that if the debate game goes on forever

$\varphi(1) \quad \varphi(2) \quad \varphi(3) \quad \ldots$

There is no infinite sequence (n_k)

$$\begin{cases} n_k = \varphi(n_{k+1} - 1) \\ n_k \text{ odd} \end{cases}$$

i.e. the relation $n = f(m-1)$ between odd integers is well-founded

$\left.\begin{array}{l} P \in [\![A]\!] \\ Q \in [\![\sim A]\!] \end{array}\right\}$ if the interaction sequence is infinite, then P or Q is not a total object

(13)

(1) If $P \in [\![\sim A \vee B]\!]$

$Q \in [\![A]\!]$

we can define $P(Q) \in [\![B]\!]$ and it is total if P, Q are total

(This is reduced to a proposition about interaction sequences)

(2) If $P \in [\![A]\!]$ is total, then

P, "by restriction", gives a cut-free proof of A

simply apply P against an environment that does not change its mind.

(14)

$\vdash A$

- Classical logic $\supseteq$ Intuitionistic logic

  $\urcorner$

  higher-order computations ?

- connections between the idea of "resuming a point in a debate" and the use of dump in SECD evaluation ?

  proof of normalisation?

more examples ?

variable for <u>functions</u> ?

$\exists f$ ---

→ conjectures a law?

gives a finite partial information about the function ?

- too sequential ?

Interaction Sequences

Thierry Coquand
Department of Computer Science, University of Göteborg/Chalmers
S-412 96 Göteborg, Sweden

March 20, 1992

Introduction

We present an abstract version of the notion of cuts between proofs. This leads to an argument of normalisation based on an analysis of what happens during the process of cut-elimination (and not on an induction on the complexity of the cut formula).

This paper is mathematically self-contained. A knowledge of infinitary propositional calculus, as presented in [5], may be useful for reading section 6.

1 Motivations

The idea of identifying a proof with a winning strategy for a game seems to come from Lorenzen [1, 2][1]. This identification is especially clear if we consider intuitionistic provability of arithmetical prenex formulae. For example, the game defined by a formula

$$\exists x.\forall y.\exists z.A(x, y, z).$$

where $A(x, y, z)$ is decidable, is that a player chooses a value for x, the opponent a value for y and then the player chooses a value for z. The player wins iff the formula $A(x, y, z)$ becomes true for this choice of values for x, y, z. In this case, it is clear that a winning strategy for this game corresponds exactly to an intuitionistic proof of the above formula.

[1] The author was lead to this identification by reading [1]

Looking at examples of prenex formulae that are classically valid, it seems natural to try to extend this analogy between proofs and winning strategy in the case of classical logic by allowing the proof, when it has to make a move, to answer to any previous move of its opponent, or to play a new initial move. One can then hope to identify classical proofs with winning strategy for such games. This was suggested by Lorenz [2].

Another idea, that comes from concurrency theory [3], is to interpret a strategy as an interactive programs and modus ponens as internal communication: given a winning strategy for $A \Rightarrow B$ and a winning strategy for A, one hopes to get a winning strategy for the game corresponding to B by letting the strategy for $A \Rightarrow B$ play against the strategy for A whenever its play concerns A. One expects then that the result of cut-elimination will be replaced by a proof showing that "internal chatters" end eventually.

When trying to put these ideas together, the difficulty is in the exact definition of what it means to "let two strategies play against each other". Trying to precise this leads to the notion of interaction sequence, which is a purely combinatorial notion.

One surprise is then that the main concepts about proofs, like the one of normal proofs, can be lifted at the level of interaction sequence. Basic facts about proofs, like cut-elimination, can also be expressed and proved at the level of interaction sequences.

We first present the notion of interaction sequence, and some of its basic properties. These are directly applied to a definition of classical provability for infinitary propositional formulae [5], for which modus ponens can be interpreted by internal communication.

2 Interaction Sequences

An **interaction sequence** is a pair (V, f) such that $V(0)$ is empty, $V(1) = \{0\}$, $f(1) = 0$, the function f is defined on an initial segment $[1, N]$ and for $n < N$

$$V(n+1) = \{n\} \cup V(f(n)), \quad f(n+1) \in V(n+1).$$

If (V, f) is defined for all positive integers, and for all N, (V, f) is an interaction sequence on $[1, N]$, we say that (V, f) is an **infinite interaction sequence**.

Notice that, if (V, f) is an interaction sequence, we always have $f(n) < n$ and $f(n), n$ are of distinct parity.

We let $y \prec x$ mean that $x \in f(V(y))$. By a direct induction on y, $y \prec x$ iff there exists a sequence $y_1, \ldots, y_n$ such that $y_1 = f(y-1)$, $y_{k+1} = f(y_k - 1)$ and $y_n = x$. Hence $\prec$ is transitive.

Lemma 1 *If $y \prec x$, then $V(x)$ is a strict initial segment of $V(y)$.*

Proof: By the alternative definition of $\prec$. □

We shall need a slight generalisation of the notion of interaction sequence. If $A = \{n_0, \ldots, n_k\}$, with $n_0 < \ldots < n_k$ and f is a function defined at least on $\{n_1, \ldots, n_k\}$, we say that f **defines an interaction** on A iff there exists an interaction sequence (V, g) defined on $[1, k]$ such that $f(n_p) = n_{g(p)}$ for $p = 1, \ldots, k$.

If $p = g(i)$, $q = g(j)$, we write $q \prec p$ (f, A) for the fact that $j \prec i$ relatively to the interaction sequence (V, g).

It can be seen directly that the following algorithm checks whether or not a function f defines an interaction on $\{n_0, \ldots, n_k\}$.

- If $k = 0$, then f does define an interaction on $\{n_0\}$.
- If $k > 0$, check recursively whether or not f defines an interaction on the set $\{n_0, \ldots, n_{k-1}\}$:
  - if not, then f does not define an interaction on $\{n_0, \ldots, n_k\}$.
  - if yes, we know that $f(n_{k-1})$ is of the form n_p, with $p < k-1$. If furthermore $f(n_k) = n_{p-1}$, then f defines an interaction on $\{n_0, \ldots, n_k\}$. Otherwise, f defines an interaction on $\{n_0, \ldots, n_k\}$ iff $f(n_k) \in \{n_0, \ldots, n_{p-1}\}$ and f defines an interaction sequence on the set $\{n_0, \ldots, n_{p-1}, n_k\}$.

Lemma 2 *If f defines an interaction on $\{n_0, \ldots, n_r\}$, $f(n_q) = n_p$ and n_q is not in the set $f(\{n_{q+1}, \ldots, n_r\})$, then f defines an interaction on the set $\{n_0, \ldots, n_{p-1}, n_{q+1}, \ldots, n_r\}$.*

Proof: By induction on $r - q$, using the previous algorithm. □

If A is an infinite subset $\{n_0, n_1, \ldots\}$, and f is a function defined at least on A, we say that f **defines an interaction** on A iff f defines an interaction on each $\{n_0, \ldots, n_k\}$.

Let us define $\mathsf{depth}(f, 0) = 0$, $\mathsf{depth}(f, n) = \mathsf{depth}(f, f(n)) + 1$ for $n > 0$. The integer $\mathsf{depth}(f, n)$ is called the **depth** of n for f. We say that (V, f) is of **bounded depth** iff there exists N such that $\mathsf{depth}(f, n) < N$ for all n.

The following definitions will not be needed in the next two sections, but are needed for the definition of classical provability. We say that an interaction sequence f is **cut-free** iff $f(2p) = 2p - 1$ whenever $2p$ is in the domain of f.

We define inductively $\mathsf{index}(f, n)$ for n in the domain of f by

- $\mathsf{index}(f, n) = n$ if $f(n) = 0$.
- otherwise, $\mathsf{index}(f, n) = \mathsf{index}(f, f(n))$.

3 Main Proposition

In this section, we suppose given an infinite interaction sequence (V, f).

Lemma 3 *if $f(x) > 0$, then $x \prec f(f(x))$.*

Proof: We have $f(x) \in V(x)$, hence $f(f(x)) \in f(V(x))$. □

If $A \subseteq \mathbf{N}$, $S_A(x)$ denotes $A \cap V(x)$.

An infinite subset $A = \{n_k\}$ is called **good** iff $f(A) \subseteq A$ and $S_A(n_{k+1}) = \{n_k\} \cup S_A(f(n_k))$.

Notice that $A = \mathbf{N}$ is good. Also, if A is good, then f defines an interaction on A.

Lemma 4 *If $A = \{n_k\}$ is good, either, for all q there exists $r > q$ such that $n_q = f(n_r)$, or there exists a good subset $\{m_l\}$ and p such that $n_i = m_i$ for $i < p$ and $m_p \prec n_p$.*

Proof: If A is good, n_q not in $f(A)$, and $n_p = f(n_q)$, let (m_l) be defined by $m_i = n_i$ for $i < p$, and $m_{p+i} = n_{q+1+i}$. It is clear that (m_l) is strictly increasing. Let $B = \{m_l\}$. Lemma 2 shows that $f(B) \subseteq B$. Furthermore

$$S_A(n_{q+1}) = \{n_q\} \cup S_A(n_p) = \{n_q, n_{p-1}\} \cup S_A(f(n_{p-1}))$$

and hence

$$S_B(m_p) = \{m_{p-1}\} \cup S_B(f(m_{p-1})).$$

It follows that B is good.

Notice also that $m_p \prec n_p$ because $n_q \in V(n_{q+1})$. □

Proposition 1 *Given an infinite interaction sequence (V, f), there exists an infinite sequence $u_1 < u_2 < u_3 \ldots$ such that $f(u_{p+1} - 1) = u_p$ for all p.*

Proof: This can be reformulated by saying that $\prec$ is not well-founded. Were $\prec$ well-founded, we could find a good subset $\{n_k\}$ such that n_{k+1} is $\prec$-minimal for good subsets starting with $n_0, \ldots, n_k$. By lemma 4, we have that for all p, there exists $q > p$ such that $n_p = f(n_q)$, and we get a contradiction by lemma 3. □

In the important special case of bounded depth sequences, we can build effectively a sequence (u_p) such that $u_{p+1} \prec u_p$. The algorithm is built by induction on a bound N of the depth. If $\mathsf{depth}(f, n)$ is always $< N$, we apply the induction hypothesis. Otherwise, lemma 2 shows that two segments of the form $[f(n), n]$ with $\mathsf{depth}(f, n) = N$ are such that they are disjoint or one is strictly included into another. We progressively remove all these segments that are maximal. In this way, either we are left with an infinite subset, which is a good subset $\{n_k\}$ where all $\mathsf{depth}(f, n_k)$ are $< N$, and we apply the induction hypothesis, or we are left with a finite subset, and the left extremity of the segments form a sequence (u_p) such that $u_{p+1} \prec u_p$ for all p.

4 Cut-elimination

An infinite interaction sequence (V, f) is said to be **winning** iff $\prec$ is well-founded over odd integers. If $A \subseteq N$ is infinite, we define in a corresponding way when f defines a winning interaction on A.

Lemma 5 *If (V, f) is an interaction sequence on $[1, n_k]$ and $\{n_0, \ldots, n_k\}$ is a set X such that $f(n_j) \in X$ for $j = 1, \ldots, k$ and $f(n) \in \{n_1, \ldots, n_k\}$ implies $n \in X$, then f defines an interaction sequence on X.*

Proof: By induction on k.

If $k = 1$, then we have $f(n_1) = n_0$ and hence f defines an interaction on $\{n_0, n_1\}$.

If $1 < k$, and the lemma holds for all $p < k$, let (V, f) and X satisfying the hypothesis of the lemma. By induction hypothesis, f defines an interaction on $\{n_0, \ldots, n_{k-1}\}$.

If $f(n_k) = n_{k-1}$ then f defines an interaction on $\{n_0, \ldots, n_k\}$.

Otherwise, we have $f(i) \neq n_{k-1}$ for $i \in]n_{k-1}, n_k]$, and hence, by lemma 2, if we let n_p be $f(n_{k-1})$ we have $f(n_k) < n_p$. The hypothesis of lemma 5 apply then to the set $\{n_i, \ldots, n_{p-1}, n_k\}$ and hence f defines an interaction on this set. This implies that f defines an interaction on $\{n_0, \ldots, n_k\}$. □

We suppose given an interaction sequence (V, f).

Let $I \subset N$ be the set of integers i such that $f(i) = 0$. If $i \in I$, let A_i be the set of integers n such that $\mathsf{index}(f, n) = i$. The set A_i satisfies the two conditions of lemma 5, and so f defines an interaction sequence on A_i.

Lemma 6 *If $i \in I$, and n is even, then $n \in A_i$ iff i is the least element of $V(n)$. If n is odd and $n \in A_i$, then $n + 1 \in A_i$.*

Proof: First, it is clear that i is odd, and that $i + 1 \in A_i$. Let $n > 0$ be even. The least integer k such that $f^k(n) = 0$ is even. Let $i = f^{k-1}(n) = \mathsf{index}(f, n)$. By lemma 1 and lemma 3, $V(f^{k-2}(n)) = \{i\}$ is an initial segment of $V(n)$, and hence i is the least element of $V(n)$. If $n > i$ is odd, and $n \in A_i$, then $f(n) \in A_i$ and $f(n)$ is even, $i \in V(f(n))$. Hence $i \in V(n + 1)$ and $n + 1 \in A_i$. □

Corollary 1 *If $i \in I$, and n is even, $m \prec n$, and $n \in A_i$, then $m \in A_i$, and $m \prec n$ (f, A_i).*

If $J \subseteq I$ and X_J denotes the complement of the union of all sets A_i for $i \in J$, then X_J satisfies the two conditions of lemma 5, and so f defines an interaction sequence on X_J.

Proposition 2 (cut-elimination) *Let $J \subseteq I$ be such that f defines a winning interaction sequence on each infinite A_i for $i \in J$. If (V, f) is a winning interaction sequence, then f defines a winning interaction on X_J.*

Proof: Proposition 1 and the corollary of lemma 6 show that X_J is infinite, because otherwise, $\prec$ will be well-founded both on odd and even integers.

If f does not define a winning interaction on X_J, then there exists two infinite increasing sequences (x_k) and (y_k) in X_J such that $f(y_k) = x_k$, and x_{k+1} is the next element coming after y_k in X_J.

For each k, we show by induction on $l \leq k$ that f defines an interaction on $Y_l = [0, x_{k+1}[\setminus \cup_{i<l}[x_{k-i}, y_{k-i}]$. Indeed, we have $f(p) \neq y_{k-l}$ for $p \in Y_l$ and $y_{k-l} < p$. Hence, by lemma 2, if f defines an interaction on Y_l, for $l < k$, then it defines an interaction on Y_{l+1}.

It follows that f defines an interaction on $Y = [0, x_1[\cup \bigcup]y_k, x_{k+1}[$. Since $f(y_k) = x_k$ for all k, we have that $n \prec m$ (f, Y) implies $n \prec m$. It follows that $\prec$ (f, Y) is well-founded on odd integers. Since $X_J \cap Y$ is finite, the corollary of lemma 6 shows that $\prec$ (f, Y) is also well-founded on even integers. We get then a contradiction from proposition 1. □

5 Games

We use capital letters $A, B, S, \ldots$ for denoting finite sequences (or words). We denote by Sx the concatenation of S and x, and $<>$ denotes the empty sequence. If $S = x_1 \ldots x_n$, then n is the **length** of S. We say that a sequence T **extends** the sequence S iff T is of the form $Sx_1 \ldots x_p$.

All the objects we consider here, games and strategies, are considered given intuitionistically. In particular, they are computable objects.

5.1 Games and Strategies

A **game** G is a set of sequences which is such that $<> \in G$ and $S \in G$ whenever $Sx \in G$. The elements of G are called **game history**. If $S \in G$, the set $M_G(S) = \{x \mid Sx \in G\}$ is called the set of **possible moves from** S.

A **strategy** is a function o defined on some elements of G of even length, and such that $o(S) \in M_G(S)$ whenever $o(S)$ is defined. The strategy is exactly defined on elements of G of even length that **follow the strategy** o, where $s_1 \ldots s_n$ follows the strategy o iff $o(s_1 \ldots s_{2k})$ is defined and is s_{2k+1} for all k such that $2k < n$.

Given a strategy o, we say that an infinite sequence $s_1 s_2 \ldots$ **follows the strategy** o iff $s_1 \ldots s_n$ follow the strategy o for all n.

5.2 Debate associated to a game

Let f be an interaction on $[1, n]$ and S a sequence $x_1 \ldots x_n$ of length n, we define for each $k \leq n$ a sequence $I(f, S, k)$ of length $\mathsf{depth}(f, k)$ by

- $I(f, S, 0) = <>$.
- $I(f, S, k)$ is the concatenation $I(f, S, f(k))x_k$ if $m > 0$.

Given a game G we let G^* be the set of sequences $(f(1), s_1) \ldots (f(n), s_n)$ such that

- f is an interaction on $[1, n]$ and
- for all $k \leq n$ we have $I(f, s_1 \ldots s_n, k) \in G$.

It is direct that this defines a game, called the **debate associated** to the game G.

We say that a strategy for G^* is **winning** iff for any infinite sequence $(f(1),s_1)(f(2),s_2)\ldots$, that follows this strategy, the infinite interaction sequence f is winning.

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 the game G^* represents, where G can be said to represent the "topic" of the debate.

5.3 Cut-Free Strategy

If G is a game, an element $(f(1),s_1)\ldots(f(n),s_n) \in G^*$ is **cut-free** iff f is cut-free.

A **cut-free strategy** for a game G^* is a function φ defined on some elements of G^* of even length that are cut-free. Such a strategy φ is defined exactly on sequences that **follow the strategy** φ and the sequence $(f(1),s_1)\ldots(f(n),s_n)$ follows the strategy φ iff f is cut-free and $(f(p+1),s_{p+1})$ is equal to $\varphi((f(1),s_1)\ldots(f(p),s_p))$ for all even $p < n$.

It is clear that any strategy for G^* defines a cut-free strategy by restriction.

Intuitively, a cut-free strategy tells how to behave in a debate against an opponent that never changes in mind.

We recall that, if f is an interaction sequence on $[1,n]$, we have written $V(n+1)$ the set inductively defined $\{n\} \cup V(f(n))$. The following is the motivation behind the introduction of the set $V(n)$.

If $S = (f(1),s_1)\ldots(f(n),s_n) \in G^*$ is of even length, we define inductively a cut-free sequence $C(S) = (g(1),t_1)\ldots(g(l),t_l) \in G^*$ of even length and a strictly increasing function $F(S):[1,l] \to [1,n]$ such that $s_{F(S)(j)} = t_j$, $F(S)(l) = n$, $V(n+1)$ is exactly the image $F(S)(\{1,3,\ldots,l-1\})$ and $f \circ F(S) = F(S) \circ g$:

- $C(<>) = <>$, and $I(<>)$ is the identity on the empty set,
- otherwise, we have $f(n) = p$ where $p < n$ is odd. We let T be $(f(1),s_1)\ldots(f(p-1),s_{p-1})$ and $C(T)$ be $(g(1),t_1)\ldots(g(l),t_l)$. We know by induction hypothesis that $f(p)$ is of the form $F(T)(q)$ for an odd $q \in [1,l]$. We define then $C(S)$ to be $C(T)(q,s_p)(l+1,s_n)$, and let $F(S)$ be the extension of $F(T)$ defined by $F(S)(l+1) = p$ and $F(S)(l+2) = n$.

Let φ be a cut-free strategy. We define a strategy $F(\varphi)$ for G^* by computing $(q,s) = \varphi(C(S))$ and letting $F(\varphi)(S)$ be $(F(S)(q),s)$ for S of even length. The strategy $F(\varphi)$ is called the **extension** of the cut-free strategy φ.

A cut-free strategy is said to be **winning** iff the relation of extension is well-founded on sequences that follow this strategy.

Lemma 7 *A winning strategy for G^* defines a winning cut-free strategy by restriction. Conversely, the extension of a winning cut-free strategy is a winning strategy.*

Proof: Direct from the definition. □

6 Classical provability

6.1 Classical Formulae

The formulae are defined inductively by the unique rule:

- if A_i, $i \in I$ is a family of formulae, then $A = |(A_i, i \in I)$ is a formula.

Intuitively, | is a generalised Scheffer connective, and A says that the formulae A_i are incompatible, i.e. A holds iff at least one A_i does not hold.

In particular, the formula $0 = |(A_i, i \in \emptyset)$, is false under this interpretation. We write $|A$ for $|(A)$ where (A) is a family with one formula A. It represents the negation of A. Thus the formula $1 = |0$ is true under this interpretation.

If $A = |(A_i, i \in I)$ is a formula, and K is a subset of I, we let $A(K)$ be the formula $|(A_i, i \in K)$.

This language is directly seen to be equivalent to infinitary propositional calculus as described in [5]. As shown in Tait's paper [5], this calculus contains naturally Peano arithmetic.

6.2 Classical Games

Each formula can be seen as a tree. To each formula A, we associate the game G_A where, intuitively, each player chooses alternatively a subtree of the tree already chosen by the opposite player. Formally, if $A = |(A_i, i \in I)$, then G_A is the set with the empty sequence and the sequences of the form iS, with $i \in I$ and $S \in G_{A_i}$.

We define a **proof** of A to be a winning strategy for the game G^*_A. We say that A is **provable** iff it has a proof.

Notice that the formula 0 is not provable with this definition. There is only one strategy for G^*_A if $A = 1$, and it is a winning strategy, so that $1 = |0$ is provable.

A winning cut-free strategy of G^*_A can directly be seen as a normal proof of A in the sense of Tait in [5] where rules of or-introduction and rules of and-introduction are forced to alternate.

6.3 Principal Properties

Let $A = |(A_i, i \in I)$ and K be a subset of I. If $S \in G^*_A$ is the sequence $(f(1), s_1)\ldots(f(n), s_n)$, we say that a move $(f(p), s_p)$ **plays in** $A(K)$ iff $\mathbf{index}(f, p) \in K$. Let $(f(p_1), s_{p_1})\ldots(f(p_l), s_{p_l})$ be the subsequence of S of elements $(f(p), s_p)$ that play in K. By lemma 5, there exists an interaction sequence g on $[1, l]$ such that $f(p_i) = p_{g(i)}$ for $i = 1, \ldots, l$. We let $p_K(S) \in G^*_{A(K)}$ be the sequence $(g(1), s_{p_1})\ldots(g(l), s_{p_l})$.

If S is the sequence $(f(1), s_1)\ldots(f(n), s_n)$, and $k \leq n$ is such that $f(k) = 0$, let $(0, s_k)(f(p_1), s_{p_1})\ldots(f(p_l), s_{p_l})$ be the subsequence of S of elements $(f(p), s_p)$ such that $\mathbf{index}(f, p) = k$. By lemma 5, there exists an interaction sequence g on $[1, l]$ such that $f(p_i) = p_{g(i)}$ for $i = 1, \ldots, l$. We let $p_k(S) \in G^*_{A_{s_k}}$ be the sequence $(g(1), s_{p_1})\ldots(g(l), s_{p_l})$.

Proposition 3 (modus ponens) *If*

- $A = |(A_i, i \in I)$ *is provable.*
- $I = J \cup K$ *is a partition of* I.
- A_j *is provable for* $j \in J$.

then the formula $A(K) = |(A_i, i \in K)$ *is provable.*

Proof: Let σ be a winning strategy for A, and σ_j be a winning strategy for A_j, for $j \in J$. We say that a sequence $S \in G^*_A$ following σ is **correct** w.r.t. (σ_j) iff it is such that $p_k(S)$ follows σ_{s_k} whenever $f(k) = 0$ and $s_k \in J$.

Proposition 2 shows that the following extension $G(S)$ of S, for S sequence of even length $(f(1), s_1)\ldots(f(n), s_n)$ following σ and correct w.r.t. (σ_j), is well defined:

- if $\sigma(S) = (f(n+1), s_{n+1})$ and $\mathbf{index}(f, f(n+1)) = k$ is such that $s_k \in K$, then $G(S) = S(f(n+1), s_{n+1})$.
- otherwise, $\mathbf{index}(f, f(n+1)) = k$ is such that $s_k \in J$. Let $(0, s_k)(f(p_1), s_{p_1})\ldots(f(p_l), s_{p_l})$ be the subsequence of $S(f(n+1), s_{n+1})$ of elements $(f(p), s_p)$ such that $\mathbf{index}(f, p) = k$, and g such that $f(p_i) = p_{g(i)}$ for $i = 1, \ldots, l$. Since $p_k(S)$ follows σ_k, the element

$$\sigma_k(p_k(S(f(n+1), s_{n+1}))) = \sigma_k((g(1), s_{p_1})\ldots(g(l), s_{p_l})) = (m, s)$$

is well defined. We let $G(S)$ be $G(S(f(n+1), s_{n+1})(p_m, s))$.

Notice that $G(S)$ is of odd length, extends S and its last move plays in K.

We can now define simultaneously by induction a strategy τ for $A(K)$, and for any sequence S following τ, a sequence $F(S)$ such that $F(S)$ follows σ, is correct w.r.t. (σ_j) and $p_K(F(S)) = S$. If S is of even length, let (p, s) be the last element of $G(F(S))$. There exists then a unique q such that $p_K(G(F(S)) = S(q, s)$ and we let $\tau(S)$ be (q, s) and $F(S\tau(S))$ be $G(F(S))$. If S is of odd length, and $S(p, s) \in G_{A(K)}$, we take $F(S(p, s))$ to be $F(S)(p, s)$. □

Proposition 4 *(consistency) For any formula A, at least one formula A or $|A$ is not provable.*

Proof: Because 0 is not provable. This follows also directly from proposition 1. □

It is clear that if $A = |(A_i, i \in I)$ and $K \subseteq I$ is such that $A(K)$ is provable, then A is provable, because a winning strategy for $A(K)$ is also a winning strategy for A.

Proposition 5 *If $A = |(A_i, i \in I)$ is provable, $K \subseteq I$ and there is an onto map $p : I \to K$ such that $A_{p(i)} = A_i$ for all $i \in I$ and $p(i) = i$ for $i \in K$, then $A(K)$ is provable.*

Proof: If $S \in G^*_A$ is the sequence $(f(1), s_1)\ldots(f(n), s_n)$, let $G(S)$ be the sequence $(f(1), s'_1)\ldots(f(n), s'_n)$, where $s'_i = p(s_i)$ if $f(i) = 0$, and $s'_i = s_i$ if $f(i) \neq 0$. It is clear that $G(S) \in G^*_{A(K)}$.

Let σ be a winning strategy of A. We define by simultaneous induction a strategy v for $A(K)$ and for any sequence S following v, a sequence $F(S)$ such that $F(S)$ follows σ and $G(F(S)) = S$.

If S is of even length, we compute $\sigma(F(S)) = (p, s)$. If $p = 0$, we let $v(S)$ be $(p, \rho(s))$ and $F(S(p, s))$ be $F(S)(p, s)$. If $p \neq 0$, we let $v(S)$ be (p, s) and $F(S(p, s))$ be $F(S)(p, s)$.

If S is of odd length, and $S(p, s) \in G_{A(K)}$, we let $F(S(p, s))$ be $F(S)(p, s)$. □

From proposition 3 and proposition 5 follows easily the equivalence of our notion of provable formulae with the usual definition of classical provability (as defined in [5]).

6.4 Example

A winning strategy can be seen as an interactive program, and proposition 3 interprets modus ponens as internal communication [3]. Here is an example of such a situation.

Given a function f on integer as a parameter, both formulae

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

and

$$B(f) = A(f) \Rightarrow \exists u_1, u_2, u_3.\ [u_1 < u_2 < u_3] \wedge [f(u_1) \leq f(u_2) \leq f(u_3)]$$

are provable. The second formula is even provable intuitionistically, but $A(f)$ holds only classically, if f is a parameter.

We will now define a winning cut-free strategy P for $A(f)$ and a winning cut-free strategy Q for $B(f)$. By lemma 7, this defines a winning strategy for $A(f)$ and $B(f)$ and proposition 3 leads then to a winning strategy for

$$\exists u_1, u_2, u_3.\ [u_1 < u_2 < u_3] \wedge [f(u_1) \leq f(u_2) \leq f(u_3)].$$

Such a winning strategy can be seen as a program computing u_1, u_2, u_3 such that $u_1 < u_2 < u_3$ and $f(u_1) \leq f(u_2) \leq f(u_3)$.

Rather than giving formally these winning cut-strategy, we will explain them heuristically.

The winning cut-free strategy P for $A(f)$ can be described as follows:

- the opponent gives a value for $x = a$.

- P answers $y = a$.
- the opponent gives a value for $z = a_1$. If $f(a) \leq f(a_1)$, P has won.
- If $f(a) > f(a_1)$, P changes its mind and plays $y = a_1$ instead.
- the opponent gives a value for $z = a_2$. If $f(a_1) \leq f(a_2)$, P has won.
- If $f(a_1) > f(a_2)$, P changes its mind and plays $y = u_2 \ldots$

Since **N** is well-founded, P is going to win eventually.

Here is a description of Q seen as a cut-free strategy for the formula

$$\exists x.\forall y \geq x.\exists z \geq x.[f(y) > f(z)] \vee (\exists u_1, u_2, u_3)[u_1 < u_2 < u_3 \wedge f(u_1) \leq f(u_2) \leq f(u_3)].$$

This is described informally:

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

We are going now to show an example of an interaction between these two proofs (identified with cut-free strategies), in the case where the values of f are given by

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

Here are the moves, as they are given by proposition 3:

1. Q plays $x = 0$.

2. P plays $y = 0$.

3. Q changes its mind, plays $x = 1$.

4. P plays $y = 1$.

5. $f(0) > f(1)$, hence Q plays $z = 1$.

6. P plays $y = 1$.

7. Q plays $x = 2$.

8. P plays $y = 2$.

9. $f(1) > f(2)$, hence Q plays $z = 2$.

10. P plays $y = 2$.

11. Q plays $x = 3$.

12. P plays $y = 3$.

13. $f(3) \geq f(2)$, hence Q plays $x = 4$.

14. P plays $y = 4$.

15. $f(4) < f(3)$, hence Q plays $z = 4$.

16. P plays $y = 4$.

17. $f(4) \geq f(2)$, hence Q plays $x = 5$.

18. P plays $y = 5$.

19. $f(5) \geq f(4)$, hence Q plays $u_1 = 2$, $u_2 = 4$, $u_3 = 5$.

The interaction sequence g associated to this interaction is given by:

$$g(1) = 0,\ g(2) = 1,\ g(3) = 0,\ g(4) = 3,\ g(5) = 2,\ g(6) = 1,$$

$$g(7) = 0,\ g(8) = 7,\ g(9) = 6,\ g(10) = 1,\ g(11) = 0,\ g(12) = 11,$$

$$g(13) = 0,\ g(14) = 13,\ g(15) = 12,\ g(16) = 11, g(17) = 0,\ g(18) = 17.$$

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

Conclusion

Our treatment seems to extend directly to the case of non necessarily well-founded formulae. We can even consider partial strategy, and prove for instance proposition 5 by a bissimulation argument.

The approach followed in this paper leads to a (may be new) proof of cut-elimination in a strictly deterministic framework. We think that it can be extended by allowing each player to play simultaneously a finite set of moves.

References

[1] Bernays P. (1968) "On the original Gentzen consistency proof for number theory." In Intuitionism and Proof Theory, Kino, Myhill, Vesley eds., pp. 409-417.

[2] Felsher, W. (1985) "Dialogues as a Foundation for Intuitionistic Logic" in D. Gabbay and F. Guenthner (eds.) Handbook of Philosophical Logic, Vol. III, pp. 341-372.

[3] Hoare, C.A.R. "Communicating Sequential Processes." Prentice-Hall, 1985.

[4] Lorenzen, K. (1958) "Ein dialogisches Konskruktivitatskriterium" in Infinistic Methods, Proceed. Symp. Found. of Math., PWN, Warszawa, pp. 193-200.

[5] Tait W.W. (1968) "Normal Derivability in Classical Logic." Springer Lecture Notes in Mathematics 72, J. Barwise ed. pp. 204-236.