Constructivization via Approximations and Examples

Stefano Baratella
Dipartimento di Matematica Università di Trento
Via Sommarive 14, 38050 Povo (TN), Italy
baratell@science.unitn.it

Stefano Berardi
Dipartimento di Informatica Università di Torino
Corso Svizzera 185, 10149 Torino, Italy
stefano@di.unito.it

1 Introduction

From a logician's or computer scientist's viewpoint it is natural to ask whether there are general procedures which transform classical results with classical proofs into constructive results with constructive proofs.

By *constructivization technique* we mean a systematic way of obtaining intuitionistic interpretations of classical proofs.

Among the ways of making intuitionistic sense of classical proofs, we recall Gödel's *double-negation translation* of classical predicate calculus (cf. [7, §81]). Via Curry-Howard correspondence between programs and proofs, it can be regarded as a functional interpretation of classical proofs (see [11]).

We recall that, by extending the double negation translation, Friedman [4] showed how to translate a classical arithmetic proof of a Π^0_2-sentence into a constructive arithmetic proof of the same. Friedman provided also a double negation translation for Zermelo-Fraenkel set theory [5].

For a discussion on the reduction of classical proofs to constructive ones under the additional assumption that atomic statements are decidable and the connection between proofs and λ-terms used in functional interpretations of intuitionistic systems, see [15, II.2, IV]. In this regard, Parigot's *$\lambda\mu$-calculus* [13] yields an extension of the correspondence between intuitionistic proofs and functional programs to second order classical proofs.

Obtaining intuitionistic translations of classical proofs can be viewed as a preliminary step in order to perform code extraction from proofs. The latter has become very important because of the development of proof assistants like Coq, which are based on intuitionistic logic (in this regard, see [14]).

In this paper, we give a survey of a constructivization technique presented in [1] that applies to theorems of classical first-order arithmetic. The examples that we present in the first part are very simple in order to put emphasis on the technique, rather than on the proven theorem.

In the second part, we give two examples on how to deal with theorems of classical real analysis. Rather than performing step-by-step proof-transformation, we use a direct method. Namely, we try to make intuitionistic sense of a classical proof from the proof itself: this for the sake of having a method that works faster.

We begin with some well-known facts, a partial historical account of constructivization techniques and a discussion on how our technique fits into the existing framework.

Proofs and Constructions. Call *EM* the Excluded Middle Principle and *Intuitionistic Logic* the logic without *EM*. It is known that an intuitionistic proof of existence of a mathematical object can interpreted as a construction actually providing us with such an object [16]. Proofs using *EM* (classical proofs) cannot be constructively interpreted in the same way (i.e. as constructions). The reason is that *EM* is not intuitionistically derivable.

Beginning with Kreisel [9] almost fifty years ago, the constructive content of proofs in first order arithmetic of *simply existential statements* (i.e.those concerning the existence of an object with a decidable property) was investigated. One main result is that intuitionistic first order arithmetic is closed under *Markov's Rule* for decidable predicates; i.e., whenever P is a decidable predicate on natural numbers and $\neg\neg\exists x.P(x)$ is intuitionistically provable, then $\exists x.P(x)$ is also intuitionistically provable (see [18]). Kreisel introduced a proof-transformation technique, known as *no counterexample interpretation*, by means of which every classical proof of a simply existential statement $\exists x.P(x)$ can be turned into an intuitionistic proof of the same $\exists x.P(x)$, which can be seen as a construction of a witness x such that $P(x)$.

In general, the resulting construction is not just blind search through all possible values of the domain under consideration, and it can often be used to devise a more efficient search algorithm.

A variant of Kreisel's technique. In practice, Kreisel's no counterexample interpretation suffers some drawbacks (see [1] and [2] for a thorough discussion). In particular, Kreisel's use of negations of counterexamples of a formula conceptually leads to the introduction of two nested negations. We avoid this complication by dealing with *approximations* of formulas (see below).

Here we present a variant of Kreisel's interpretation that we call ψ. For the reader acquainted with Kreisel's interpretation, we anticipate that ψ does not apply only to statements in prenex form and that contraction rule will be interpreted by means of multi-valued counterexamples.

Indeed, ψ is a map turning an arbitrary first order statement A into a statement $\psi(A)$ (the "intuitionistic interpretation of A"), and any classical proof of A into an intuitionistic proofs of $\psi(A)$. The statement $\psi(A)$ is intuitionistically equivalent to

Kreisel's interpretation of A and is, in our opinion, simpler to understand and to prove. The definition of ψ was inspired by works of Novikov [12] and Coquand [3].

We call *simply existential* a formula free from universal quantifications over infinite domains.

We identify statements with trees and we topologize the family of trees as follows: let $\beta_1, \ldots, \beta_n$ be finitely many branches; the basic open sets are of the form $O_{\beta_1,\ldots,\beta_n} = \{T : T \text{ is a tree and } \beta_1, \ldots, \beta_n \in T\}$ (*Brouwer's topology*).

If $EM_0 = \forall x.(P(x) \vee \neg P(x))$ is any instance of EM, then $\psi(EM_0)$ is a family of simply existential statements whose limit is EM_0.

Similarly, if A is any classically provable statement, then $\psi(A)$ is a family of constructively provable statements "approximating" A. An *approximation* of A is obtained by restricting the range of every universal quantifier in A to a finite subdomain by means of an *approximation map*. Indeed, in the tree topology, the limit of (the tree forms of) all approximations of A is (the tree form of) A itself. The formal definitions of approximation of A and $\psi(A)$ are given in section 2 and 3, respectively.

Technically, Kreisel's interpretation can be obtained from ours by considering unary approximation maps only: these are maps taking only singletons as values. However, differences with Kreisel are relevant in practice, namely in the interpretation of proofs because of Kreisel's use of negations of counterexamples of a formula: that amounts to dealing with two nested negations, as we have already remarked.

Complete interpretations. The statement $\psi(A)$ turns out to be equivalent to the classical provability of A (in an infinitary classical logic à la Tait). We will refer to such equivalence as *intuitionistic completeness* of ψ. Completeness tells us that our interpretation (and Kreisel's) are "as close as possible" to the original meaning of the classical statements. Completeness of ψ has been proved in [1], indeed by showing that classical proofs of A can directly be "seen" as intuitionistic proofs of $\psi(A)$ and conversely. This fact argues in favor of the simplicity of use of ψ.

Notice that not all constructive interpretations of classical logic are intuitionistically complete. For instance, Gödel's *Dialectica interpretation* is not (see the appendix in [1]). In our opinion, lack of completeness makes Gödel's interpretation less natural. The only other interpretation known to be complete was Coquand's *game interpretation* [3], whose completeness was proved in [6]. Since Coquand's deeply influenced our interpretation, we will now compare the two.

Coquand's interpretation [3] is defined in a game-theoretic framework. Informally, in his approach, a (possibly wrong) argument in favour of the truth of a formula like $\exists x \in \mathbf{N}.P(x)$, where P is any predicate, is a program returning a temporary guess x_0, and a (possibly wrong) argument p_0 in favour of the truth of $P(x_0)$. If a counterexample for the argument p_0 is found, the program makes a new guess x_1 together with a new argument p_1 in favour of the truth of $P(x_1)$, and so on.... Eventually the program terminates (the underlying assumption being that the tree of all possible computations is well-founded), either giving up, or because no further counterexample was found for its argument. A proof of $\exists x \in \mathbf{N}.P(x)$ is an argument for $\exists x \in \mathbf{N}.P(x)$ never giving up. An argument (proof) for $\forall x \in \mathbf{N}.P(x)$

is a family of arguments (proofs), one for each $P(x)$.

Coquand formally interprets arguments and counterexamples as strategies for suitable games. Proofs are interpreted as winning strategies for those games. Computations arising from his interpretation are described much in detail. For this very reason, which makes his work so interesting, the meaning of the formula being interpreted is somewhat hidden.

In our interpretation, we still appeal to Coquand's game terminology, but only in an informal way, in order to motivate and explain interpretations of proofs (see last sections of this paper). By removing game terminology from formal definitions, we achieved a deep simplification in the interpretation of statements, at the price of skipping detailed descriptions of the computations involved.

Outline of the paper. After setting the framework in which we will operate (section 2), we first describe our constructive interpretation (section 3). Then we give examples of its application to simple classical proofs (section 4). Eventually, we suggest how to directly interpret statements rather than proofs, namely we try to get an intuitionistic proof of an approximation of a given statement without translating a classical proof of the statement (section 5). As already mentioned, the direct method is supposed to work faster than the step-by-step proof transformation.

2 Preliminaries

The reader is referred to [1] and [2] for an extended presentation of these preliminaries. The metatheory of the preliminaries (and of the whole paper, indeed) is intuitionistic.

We work in a language with a countable number of atomic formulas either affirmed (denoted by $a, b, c, \ldots$) or negated ($a^\perp, b^\perp, c^\perp, \ldots$), and connectives $\vee$ and $\wedge$ over finite or countable domains. Atomic formulas are to be thought as decidable statements of first order arithmetic.

Universal and existential quantifier will be freely used in place of conjunction and disjunction, respectively.

Subformulas of a formula of the form $\forall x \in I.A(x)$ ($\exists x \in I.A(x)$) are inductively defined as the formula itself and all the subformulas of $A(x)$, for some $x \in I$. The only subformula of an atomic formula is the formula itself.

The language is *predicative*, in the sense that quantifications over functions, sets, real numbers ...are not allowed. For, they would lead to disjunctions and conjunctions over *uncountable* sets, that are forbidden. This restriction makes the constructive interpretation far easier and still does not prevent us from interpreting theorems of classical analysis (see section 5).

Propositional formulas are those free from quantifications over infinite domains. They are decidable, because atomic formulas are. *Simply existential (universal)* formulas are those free from universal (existential) quantifications over infinite domains.

Negation is performed by the map the map $A \mapsto A^\perp$ that switches $a, \vee, \exists$ with $a^\perp, \wedge, \forall$, respectively. We write $A \to B$ as shorthand for $A^\perp \vee B$.

An *approximation (example)* of a formula A is obtained by hereditarily restricting all domains of universal (existential) quantifiers in A to finite subdomains. Notice that Kreisel uses the word *counterexample* for approximation as a reminder of the fact that if an approximation of a formula is false, then the formula itself is false.

Formally, let σ be a map such that $\sigma(\forall x \in I.B(x))$ is a finite subset of I, for every occurrence $\forall x \in I.B(x)$ of a universal subformula of A, quantifying over a domain I. We call σ an *approximation map.*

We recursively define an approximation $\sigma[B]$ of a subformula B of A as follows:

- if B is an atom or a negated atom, then $\sigma[B]$ is B;
- if B is a disjunction $\exists x \in I.C(x)$ then $\sigma[B]$ is $\exists x \in I.\sigma[C(x)]$;
- if B is a conjunction $\forall x \in I.C(x)$ and $I_0 = \sigma(B)$, then $\sigma[B]$ is $\forall x \in I_0.\sigma[C(x)]$.

In the last case of the definition it may be the case that $\sigma(B) = I$, when I is finite. We then say that σ is *trivial on* B. We also say that σ is *trivial* if it is trivial on all universal subformulas of A involving quantifications over finite domains (a trivial σ may still be non-trivial over infinite domains).

We introduce now the notion of *example* of a formula A, by "dualizing" the definition of approximation. Let τ be a map such that $\tau(\exists x \in I.C(x))$ is a finite subset of I, for every occurrence of existential subformula of A. It is clear how one can inductively define, for every such occurrence B, an *example* $\tau\{B\}$ of B. In examples, we hereditarily restrict to finite subdomains the domains of disjunctions. The map τ is trivial if $\tau(\exists x \in I.C(x)) = I$ for every existential subformula $\exists x \in I.C(x)$ of A on some finite I. Since examples are duals of counterexamples with respect to negation, examples of A can be identified with counterexamples of $A^{\perp}$.

Every formula A is classically equivalent to $\forall\sigma.\sigma[A]$. Assuming the Axiom of Choice, A is intuitionistically equivalent to $\exists\tau.\tau\{A\}$.

Notice that the truth of an example $\tau\{A\}$ is more informative than the truth of A. Loosely speaking, if $\tau\{A\}$ holds then the map τ embodies the construction hidden inside an intuitionistic proof of A. For instance, if $\tau\{\exists x \in I.a_x\}$ holds, then $\exists x \in I_0.a_x$ holds for some finite I_0. Hence we have additional information: a finite upper bound on the number of tests needed for finding x such that a_x holds.

Approximations (examples) are simply existential (universal) formulas. Notice also that an example of an approximation of a formula is a propositional formula.

As described in [1], once fixed a decidable subset of the set of atoms containing those atoms that we want to interpret as true atoms, we can inductively define a predicate ($\_$ is true) on formulas such that, for every formula A, (A is true) is a metalinguistic interpretation of A. Indeed, by choice of an intuitionistic metatheory, (A is true) holds if and only if A is intuitionistically true.

We introduce now Tait's cut-free deductive system for predicative classical logic [17]. We assume that a *complete* set Σ of Post rules of the form $a_1, \ldots, a_n \vdash a$, where $a_1, \ldots, a_n$ and a are atoms, is given. Completeness of Σ means that $\vdash a$ is derivable from Σ if and only if a is true, and that $a \vdash$ is derivable from Σ if and only if a is false. Deduction rules infer finite sequences $A_1, \ldots, A_n$ of formulas, or *contexts*. Contexts (also called *sequents*) are denoted by $\Gamma, \Delta, \ldots$ Context Γ is true if some $A \in \Gamma$ is true. The deduction rules are:

i. $\dfrac{a, \Gamma}{\Gamma}$ if the rule $a \vdash$ is in Σ.

ii. $\dfrac{a_1, a, \Gamma \quad \ldots \quad a_n, a, \Gamma}{a, \Gamma}$ if the rule $a_1, \ldots, a_n \vdash a$ is in Σ.

iii. $\dfrac{}{a^{\perp}, \Gamma}$ if $a \in \Gamma$.

iv. $\dfrac{\{A(x), \Gamma\}_{x \in I}}{\forall x \in I.A(x), \Gamma}$

v. $\dfrac{A(t), \exists x \in I.A(x), \Gamma}{\exists x \in I.A(x), \Gamma}$

We call **CL** (a shortening for *Predicative Classical Logic*) the system whose formulas and deduction rules have been just presented. All the rules of **CL** are intuitionistically sound, with the exception of $\forall$- introduction over countable domains, whose justification relies on *EM*.

We say that **CL** *proves* Γ (notation: $\mathbf{CL} \vdash \Gamma$) if there exists a well-founded proof of Γ in **CL**. Notation $\mathbf{CL} \vdash A$ will be used for $\mathbf{CL} \vdash \{A\}$.

A sequent Γ is simply existential if all its formulas are. If Γ is simply existential, then we claim that every proof of Γ is finite and intuitionistically sound. To prove the claim, argue by induction on the proof-tree. The crucial case is when the proof-tree ends with a $\forall$- introduction over a domain I, say. Then I is finite, hence the $\forall$-introduction is intuitionistically sound and its premise is still a simply existential sequent.

The previous claim can be strengthened to show that there exist a computable map from proofs in **CL** of any simply existential formula A to true examples of A, and a computable map in the opposite direction.

A list of further properties of the relation $\vdash$ is given in [1].

The system **CL** is *classically complete*, that is

$$(\mathbf{CL} \vdash A) \leftrightarrow (A \text{ is true})$$

holds classically for every formula A (see [17]). All logical rules are conditionally derivable in **CL**, including cut rule [17]. Indeed, we may prove in a purely syntactic way that if $\mathbf{CL} \vdash \Gamma, A$ and $\mathbf{CL} \vdash A^{\perp}, \Delta$, then $\mathbf{CL} \vdash \Gamma, \Delta$.

3 The constructive interpretation

Call *level* 1 *function* (briefly: *function*) any map whose domain and range are countable sets. Call *level* 2 *function*, or *functional*, any map with domain some set of functions and range a countable set.

Our interpretation ψ of classical logic is based over the notion of *continuous* functional. Roughly speaking, a functional is continuous if each value of it is determined by a finite amount of information about its function argument. Continuous functionals are also known as *countable* functionals in the literature [8]. We will now introduce them in a formal way.

Definition 3.1 Let I, J and K be effectively enumerated sets. Let $H \subseteq I \to J$ and let $F \in H \to K$ be a functional.

1. A question/answer pair (briefly: q/a pair) for the functional F is a pair $\langle i, j\rangle$, with $i \in I$ and $j \in J$. Intuitively, a q/a pair for F represents a request of F, during a computation of $F(f)$, for the value $j = f(i)$. If f_0 is any finite list of q/a pairs, then we write $f_0 \subseteq f$ if $j = f(i)$ for all $\langle i, j\rangle$ in f_0.

2. Roughly speaking, a question/answer tree for F is made of all possible sequences of q/a pairs between F and some of its inputs f. Recall that a tree T on $I \times J$ is a set of finite sequences of elements $I \times J$ that is closed under predecessor and contains the empty list $\langle\ \rangle$.

   The tree T is a q/a tree for F if and only if, for any $f_0 \in T$, either f_0 is a leaf in T (i.e. a maximal sequence in T with respect to the predecessor relation), or the branching from f_0 consists, for some $i \in I$, of all nodes $f_0\langle i, j\rangle$ for some $j \in J$. If f_0 is a leaf in T, we further require that $F(f) = F(g)$ for all $f, g \in H$ such that $f_0 \subseteq f, g$.

3. A functional $F \in H \to K$ is *continuous* if and only if there exists a well-founded q/a tree for F.

We recall that the collection WF of well-founded trees is the smallest collection X of trees such that, if every immediate subtree of a tree T is in X, then T is in X. For instance, the tree $\{\langle\ \rangle\}$ is well-founded, because it has *no* immediate subtree.

Intuitionistically, continuity of F implies the following, known as *weak continuity*: for every $f \in H$ there exist some $k \in K$, and some finite $f_0 \subseteq f$, such that $F(g) = k$ for all $g \in H$ including f_0. The proof that continuity implies weak continuity is by induction over a well-founded q/a tree of F.

Weak continuity more explicitly defines the property we wanted to formalize: *the value of $F(f)$ depends only on a finite amount of information about f.*

Assuming the Axiom of Choice, continuity and weak continuity are classically equivalent. Intuitionistically, the former is stronger than the latter. This is why we chose the former to formalize our informal notion of "continuity".

Having introduced a notion of continuity for functionals, we are now ready to define our interpretation map ψ.

Given a formula A, we say that F a continuous functional *associated to* A if F is defined on approximation maps σ of A and, for every σ, $F(\sigma)$ is a (finite intuitionistic) proof of $\sigma[A]$ in $\mathbf{CL}$[1] . For every formula A, $\psi(A)$ is now the metalinguistic statement

There exists a continuous functional F associated to A.

As we already mentioned in the introduction, roughly speaking $\psi(A)$ says that there is a family F of proofs, one for each approximation of A, and that the family is indexed in a "continuous" way.

The following is proved in [1]:

Lemma 3.2 For every $A \in \mathbf{L}$ we have:

1. $(\mathbf{CL} \vdash A) \rightarrow \psi(A)$.
2. $\psi(A) \leftrightarrow (A$ is true) for simply existential A. In general, $\psi(A)$ is intuitionistically strictly weaker than the truth of A.
3. Suppose either (A is true) or ($A^{\perp}$ is true). Then (A is true) $\leftrightarrow \psi(A)$.

Point 1 in lemma 3.2 says that the interpretation ψ is sound. This means that we can effectively turn a classical proof of A into an intuitionistic proof of $\psi(A)$. The formula $\psi(A)$ is, in general, intuitionistically strictly weaker than A.

From point 3, we get that $\psi(A)$ is classically equivalent to (A is true), for every formula A. Hence, from a classical viewpoint, $\psi(A)$ is just a reformulation of A, chosen to bypass applications of *EM* in any proof of A. By point 2, $\psi(A)$ and (A is true) are also intuitionistically equivalent, if A is simply existential.

The main result in [1] is intuitionistic completeness of ψ, namely $\psi(A)$ and $(\mathbf{CL} \vdash A)$ are intuitionistically equivalent, for every formula A. Such a result is a consequence of lemma 3.2 and of the following:

Theorem 3.3 For every formula A we have $\psi(A) \leftrightarrow (\mathbf{CL} \vdash A)$.

As already mentioned in the introduction, the previous equivalence is a sort of identity, in the sense that each proof-tree of A in **CL** can be viewed as a well-founded q/a tree of some continuous functional F associated to A. Thus, after a mere linguistic reformulation, each classical proof of A can be regarded as an intuitionistic proof of $\psi(A)$.

The converse is "almost" true: there is a subclass of continuous functionals F associated to A, the *connected* functionals, whose well-founded q/a trees can be viewed as classical proofs of A in **CL**. So there is a strong connection between continuous functionals associated to A, namely intuitionistic proofs of $\psi(A)$, and classical proofs of A. Such a connection is of much importance since it makes the constructivization of classical proofs easier.

[1] The formula $\sigma[A]$ is simply existential, hence *all* its proofs in **CL** are necessarily finite and intuitionistic.

The reason for introducing connected functionals is that, in a q/a tree relative to a functional, every branch can be identified with a finite approximation map only if the set of its nodes satisfies the usual condition of functionality. In general, there are branches not corresponding to any approximation. For, it may be that a branch contains two different answers relative to a same instance of a universal formula. Of course, those branches do not correspond to any computation, nevertheless they may appear in a q/a tree.

Formally:

Definition 3.4 Let σ be an approximation map.

1. σ is *unary* if $\sigma(B)$ is a singleton for every $B \in \mathrm{dom}(\sigma)$. Notice that all universal formulas occurring in the domain of a unary approximation map have nonempty domain.

2. The formula B_z is a *σ-instance* of $B = \forall y \in I.B_y$ if $B \in \mathrm{dom}(\sigma)$ and $z \in \sigma(B)$.

3. Let B be a subformula of A, and $A = B_1, \ldots, B_n = B$ be the subformula path from A to B. We say that B is *connected by σ* if whenever $i < n$ and B_i is universal then B_{i+1} is a σ-instance of B_i. σ is *connected* if all points in $\mathrm{dom}(\sigma)$ are connected by σ.

4. A *finite approximation map* is a restriction of an approximation map to a finite domain.

5. A continuous functional

$$F : \{\text{approximation maps of } A\} \to \{\text{finite proofs in } \mathbf{CL}\}$$

is *connected* if it has a well-founded q/a tree whose branches are connected finite approximation maps.

One can directly recover a classical proof of formula from a continuous functional, when the functional is connected. Hence the following result is crucial (see [1] for a proof).

Lemma 3.5 Let A be a formula and let F be a continuous functional such that $F(\sigma)$ is a proof of $\sigma[A]$, for every approximation map σ of A. Then there exists a connected functional G defined only on unary approximations such that $G(\sigma)$ is a proof of $\sigma[A]$, for every $\sigma \in \mathrm{dom}(G)$.

Thanks to the previous lemma, the proof of theorem 3.3 reduces to show that from a connected functional defined only on unary approximation maps we can recover a proof of A in **CL**. This is done in [1].

4 Step-by-step proof interpretation

In this section we consider a second equivalent formulation of the interpretation ψ which, for every formula A, says

There exists a continuous functional G mapping every approximation map σ on A to a true example of $\sigma[A]$.

The original formulation of ψ is better suited for the theory, the present one is more adequate for practical use. The equivalence between the two formulations is easily proved. We claimed in section 2 that there exist a computable map θ from proofs in **CL** of any simply existential formula B to true examples of B, and a computable map χ in the opposite direction.

Thus, if F is a continuous functional from approximations σ of A to proofs of $\sigma[A]$, we obtain G as in the second formulation by letting $G = \theta \circ F$. The functional G is still continuous, with same q/a trees as F.

Conversely, from G as in the second formulation of ψ, we define F with required domain and range by $F = \chi \circ G$.

Notice that the results obtained so far hold even if we replace formulas by sequents, after making the necessary changes.

Assume that Γ is a classically derivable sequent, namely that $\psi(\Gamma)$ holds. From a classical proof of Γ, we want to obtain an explicit definition functional G as in the second formulation of ψ. With little abuse, we still say that G is a functional associated to Γ.

We begin by defining an ordering between approximations.

If σ and σ' are approximation maps for a formula A, we let $\sigma \preceq \sigma'$ if and only if $\sigma(B) \subseteq \sigma'(B)$ for every B in their common domain. Then we let $\sigma[A] \preceq \sigma'[A]$ if and only if $\sigma \preceq \sigma'$.

The relation $\preceq$ is a directed partial order on approximations of a formula A: if A_1 and A_2 are approximations of A, by induction on A one can define an approximation A_3 of A such that $A_1 \preceq A_3$ and $A_2 \preceq A_3$. The approximation A_3 can even be chosen to be the least upper bound of A_1 and A_2.

In the same way we define $\preceq$ on examples.

Notice that if $A_1 \preceq A_2$ are approximations of a same formula then A_2 implies A_1. The converse implication holds for examples.

Let us return to the definition of G.

Given a proof of Γ in **CL**, for any approximation map σ of Γ we define a true example of $\sigma[\Gamma]$. For a proof of continuity of G, we refer the reader to [1]. We proceed by induction on the given classical proof.

- $\exists$-introduction. Let $A(t)^\sim, (\exists x \in I.A(x))^\sim, \Gamma^\sim$ be an approximation of $A(t)$, $\exists x \in I.A(x), \Gamma$. Suppose we already interpreted a proof of $A(t), \exists x \in I.A(x), \Gamma$ as a proof of an example $A(t)', (\exists x \in I.A(x))', \Gamma'$ of $A(t)^\sim, (\exists x \in I.A(x))^\sim, \Gamma^\sim$.

  Then $(\exists x \in I.A(x))'$ is $\exists x \in K.(A(x))'$ for some finite $K \subseteq I$. We interpret an $\exists$- introduction

$$\frac{A(t),\ \exists x \in I.A(x),\ \Gamma}{\exists x \in I.A(x),\ \Gamma}$$

by a $\vee$-introduction

$$\frac{A(t)',\ \exists x \in K.(A(x))',\ \Gamma'}{\exists x \in \{t\} \cup K.(A(x))',\ \Gamma'},$$

where $\exists x \in \{t\} \cup K.(A(x))'$ is still an example of $(\exists x \in I.A(x))^\sim$. Intuitively, we first look for an intuitionistic proof of $A(t)'$. If we fail, we try to prove the sequent $\exists x \in K.(A(x))', \Gamma'$.

- $\forall$-introduction. For all $x \in I$, let $A(x)^\sim, \Gamma(x)^\sim$ be an approximation of $A(x), \Gamma$. Suppose we already interpreted a proof of $A(x), \Gamma$ as a proof of an example $A(x)', \Gamma(x)'$ of $A(x)^\sim, \Gamma(x)^\sim$. Fix an approximation $(\forall x \in I.A(x))^\sim = \forall x \in K.(A(x))^\sim$ of $\forall x \in I.A(x)$, where K is a finite subset of I. Then a $\forall$-introduction

$$\frac{A(x),\ \Gamma \qquad (\text{for all } x \in I)}{\forall x \in I.A(x),\ \Gamma}$$

is interpreted as a $\wedge$-introduction

$$\frac{A(x)',\ \Gamma(x)' \qquad (\text{for all } x \in K)}{\forall x \in K.A(x)',\quad \Gamma'},$$

where Γ' any sequent of examples of Γ such that $\Gamma(x)' \preceq \Gamma'$ for all $x \in K$. Notice that such a Γ' does exist because the componentwise extension of $\preceq$ to sequents is still a directed partial order.

Intuitively, this means we first look for for an intuitionistic proof of $A(x)'$, for all $x \in K$. If we fail for some $y \in K$, we return an intuitionistic proof of some formula in $\Gamma(y)'$, hence of some formula of Γ'.

- We interpret the axiom $a^\perp, \Gamma$ (when $a \in \Gamma$) as a process waiting either for a proof of a or for a proof of $a^\perp$, and then sending it back, in the first case as a counterexample to $a^\perp$, in the second case as a counterexample to a.

In the sequel, we provide some examples of application of the technique outlined above. They are taken from [2].

In each example, we first give a classical proof in sequent calculus of a statement A, and describe the general form of an approximation $A^\sim$ of A. Then, we interpret the classical proof of A as an intuitionistic proof of some example A' of $A^\sim$. Eventually, we exhibit the example A' obtained from the classical proof of A.

4.1 Interpretation of a classical proof of $\exists x.\forall y.(p(x) \to p(y))$

In this example, p is a decidable unary predicate over natural numbers.

Classical proof (top-down).

We start from the axiom $p(y) \vee p(y)^{\perp}$ and argue by cases. If $p(y)^{\perp}$ holds of some $y \in \mathbf{N}$, then we have $p(y) \to p(z)$, for all $z \in \mathbf{N}$, and $\forall z.(p(y) \to p(z))$ (by $\forall$-introduction). We can deduce $A = \exists x.\forall y.(p(x) \to p(y))$, (by $\exists$-introduction, after renaming of bound variables) and we now have a proof of the sequent $p(y), A$, for all $y \in \mathbf{N}$.

We still have to consider the case when $p(y)$ holds for a generic $y \in \mathbf{N}$. In this case we choose an arbitrary $x_0 \in \mathbf{N}$, and from $p(y)$ we deduce $p(x_0) \to p(y)$ (by $\vee$-introduction). From it we deduce $\forall y.(p(x_0) \to p(y))$ (by $\forall$-introduction), and then A (by $\exists$-introduction). In this way we get a proof of A. Here is its proof-tree:

$$\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{\dfrac{}{p(y),\ p(y)^{\perp}}}{p(y),\ p(y) \to p(z)}}{p(y),\ \forall z.(p(y) \to p(z))}}{p(y),\ A}}{p(x_0) \to p(y),\ A}}{\forall y.(p(x_0) \to p(y)),\ A}}{A}$$

Intuitionistic Interpretation.

The classical argument can be restricted to an intuitionistic one for an approximation

$$\sigma[A] = \exists x \in \mathbf{N}.\forall y \in \mathbf{N}_x.(p(x) \to p(y))$$

of A depending continuously on

$$\sigma : \ \forall y \in \mathbf{N}.(p(x) \to p(y)) \mapsto \mathbf{N}_x,$$

where $\mathbf{N}_x$ is a finite subset of $\mathbf{N}$. The meaning of $\sigma[A]$ is that we can find a natural number x on which p takes a least truth value, provided we choose to check it only against a finite subset of $\mathbf{N}$ given by the map σ.

We now interpret the classical proof of A by means of an intuitionistic proof of $\sigma[A]$ in a way depending continuously on σ.

1. We first try to prove $A_{x_0} = \forall y \in \mathbf{N}_{x_0}.(p(x_0) \to p(y))$ (interpretation of the last $\exists$-introduction).

2. Let $\mathbf{N}_{x_0} = \{y_1, \ldots, y_n\}$. Then we try to prove $p(x_0) \to p(y_i)$, for all $1 \leq i \leq n$, starting from $i = 1$ (interpretation of the last $\forall$-introduction).

3. For every $1 \leq i \leq n$, we try to deduce $p(x_0) \to p(y_i)$ from $p(y_i)$ (interpretation of the last $\vee$- introduction).

4. We temporary drop the attempt at proving $p(y_i)$ and we try again to prove A from $A_{y_i} = \forall z \in \mathbf{N}_{y_i}.(p(y_i) \to p(z))$ (interpretation of the first $\exists$-introduction).

5. Let $\mathbf{N}_{y_i} = \{z_1, \ldots, z_m\}$. Then we try to prove $p(y_i) \to p(z_j)$, $1 \leq j \leq m$, starting from $j = 1$ (interpretation of the last $\forall$-introduction).

6. For every $1 \leq j \leq m$, we try to deduce $p(y_i) \to p(z_j)$ from $p(y_i)^{\perp}$ (interpretation of the first $\vee$-introduction).

7. We wait for a proof of $p(y_i)$ or for a proof of $p(y_i)^{\perp}$ (interpretation of the axiom $p(y_i), p(y_i)^{\perp}$).

   There are two cases to examine now.

7a. If we get a proof of $p(y_i)$, we fail in proving $p(y_i)^{\perp}$ for the first value z_1 of z in $\mathbf{N}_{y_i}$ (point 6). Then we fail in proving A from A_{y_i} (point 4). In this case we succeed with $p(x_0) \to p(y_i)$, and make one step forward in proving A_{x_0} (starting again from point 6).

7b. If we always obtain a proof of $p(y_i)^{\perp}$, then we definitively fail in proving A from A_{x_0}. So we make an attempt at proving A just from A_{y_i}. In this case we prove A from A_{y_i} and A_{y_i} from each $p(y_i) \to p(z)$, for $z \in N_{y_i}$. Eventually, we prove the latter from $p(y_i)^{\perp}$.

8a. If we always fail with $p(y_i)^{\perp}$, then we succeed with A_{x_0} and hence with A, by using the random witness x_0 we started with in the classical proof.

8b. As as soon as we succeed with $p(y_i)^{\perp}$, we have a proof of A from A_{y_i}.

To summarize: by decidability of p, if $\forall y \in \mathbf{N}_{x_0}.p(y)$ holds then

$$\forall y \in \mathbf{N}_{x_0}.(p(x_0) \to p(y))$$

holds as well, and we are done. Otherwise, $p(y)^{\perp}$ holds for some $y \in \mathbf{N}_{x_0}$, and then $\forall z \in \mathbf{N}_y.(p(y) \to p(z))$ holds. In both cases we deduce $\sigma[A]$.

Notice that who N_y is and the truth value of $p(x_0)$ are not relevant for the computation. In fact, we have proved the example

$$\tau\{\sigma[A]\} = \exists x \in \mathbf{N}_{\sigma}.\forall y \in \mathbf{N}_x.(p(x) \to p(y))$$

of $\sigma[A]$, with $\mathbf{N}_{\sigma} = \{x_0\} \cup \mathbf{N}_{x_0}$.

4.2 Interpretation of a classical proof of $\exists x.\forall y.f(x) \leq f(y)$

In this example, f is a function from natural numbers to natural numbers.

Classical proof (bottom-up). We assume that, for all $x, y \in \mathbf{N}$, we have either a proof of $f(x) \leq f(y)$, or a proof of $f(x) > f(y)$, according to the case.

We choose an arbitrary integer x_0. We can deduce $A = \exists x.\forall y.f(x) \leq f(y)$ by a $\forall$-introduction and an $\exists$-introduction from all the sequents

$$\Gamma_y = f(x_0) \leq f(y),\ A \qquad (y \in \mathbf{N}).$$

Now we have to prove all Γ_ys. If $f(x_0) \leq f(y)$ holds, we get a proof of Γ_y. If $y = x_1$ is such that $f(x_0) > f(x_1)$, we can prove Γ_{x_1} by a $\forall$- introduction and an $\exists$-introduction from all the sequents Γ_{x_1}, y of the form

$$f(x_0) \leq f(x_1),\ f(x_1) \leq f(y),\ A \qquad (y \in \mathbf{N}).$$

Again, if $f(x_1) \leq f(y)$ we have a proof of $\Gamma_{x_1,y}$. If $y = x_2$ is such that $f(x_1) > f(x_2)$, we can prove Γ_{x_1,x_2} by a $\forall$-introduction and a $\exists$-introduction from all the sequents $\Gamma_{x_1,x_2,y}$ of the form

$$f(x_0) \leq f(x_1),\ f(x_1) \leq f(x_2),\ f(x_2) \leq f(y),\ A \qquad (y \in \mathbf{N}),$$

and so on. Clearly, this process eventually stops by well- foundedness of $\mathbf{N}$.

The proof-tree of A is:

$$\dfrac{\dfrac{\dfrac{\Pi_y}{f(x_0) \leq f(y),\ A}}{\forall y.f(x_0) \leq f(y),\ A}}{\exists x.\forall y.f(x_0) \leq f(y),\ A}$$

The proof tree Π_y is given by hypothesis if $f(x_0) \leq f(y)$ holds. For all $y = x_1$ such that $f(x_1) > f(x_0)$, the proof-tree Π_y is defined by:

$$\dfrac{\dfrac{\dfrac{\dfrac{\Pi_{x_1,y}}{f(x_0) \leq f(x_1), f(x_1) \leq f(y),\ A}}{f(x_0) \leq f(x_1), \forall y.f(x_1) \leq f(y),\ A \qquad (n \in \mathbf{N})}}{f(x_0) \leq f(x_1), \exists x.\forall y.f(x_1) \leq f(y),\ A}}{f(x_0) \leq f(x_1),\ A}$$

The proof tree $\Pi_{x_1,y}$ is given by hypothesis if $f(x_1) \leq f(y)$ holds. It is defined in the same way as Π_y, otherwise. And so on.

Intuitionistic interpretation. The classical argument can be restricted to an intuitionistic one for

$$\sigma[A] = \exists x \in \mathbf{N}.\forall y \in \mathbf{N}_x.f(x) \leq f(y)$$

that depends continuously on $\sigma : \forall y \in \mathbf{N}.f(x) \leq f(y) \mapsto \mathbf{N}_x$. The meaning of $\sigma[A]$ is that we can find a natural number x that is a minimum point for the restriction of f to the finite set $\{x\} \cup \mathbf{N}_x$, where $\mathbf{N}_x$ is provided by σ.

Now we interpret the classical proof of A into an intuitionistic proof of $\sigma[A]$ that depends continuously on σ.

1. We start by trying to prove the instance $A_{x_0} = \forall y \in \mathbf{N}_{x_0}.f(x_0) \leq f(y)$ of A (corresponding to the last $\exists$-introduction).
2. For each $y \in \mathbf{N}_{x_0}$ we try to prove $f(x_0) \leq f(y)$ (corresponding to the last $\forall$-introduction).
3. If $f(x_0) \leq f(y)$ for all $y \in \mathbf{N}_{x_0}$, then we succeed in proving A_{x_0} and hence A.
4. If not, let $y = x_1$ be the first element in an enumeration of $\mathbf{N}_{x_0}$ such that $f(x_0) > f(x_1)$. We drop the attempt at proving A_{x_0} and we try to prove the instance $A_{x_1} = \forall y \in \mathbf{N}_{x_1}.f(x_1) \leq f(y)$ of A.
5. We repeat the previous steps until we succeed in proving some A_{x_i}.

To summarize: either $\forall y \in \mathbf{N}_{x_0}.f(x_0) \leq f(y)$ holds, or its negation $\exists x_1 \in \mathbf{N}_{x_0}.f(x_0) > f(x_1)$ does. In the latter case, either $\forall y \in \mathbf{N}_{x_1}.f(x_1) \leq f(y)$ or $\exists x_2 \in \mathbf{N}_{x_1}.f(x_1) > f(x_2)$ hold and so on, until the sequence of natural numbers

$$f(x_0) > f(x_1) > f(x_2) > f(x_3) > \ldots$$

stops and we find some x_i such that $\forall y \in \mathbf{N}_{x_i}.f(x_i) \leq f(y)$. Indeed, we have provided an intuitionistic argument for

$$\exists x \in \mathbf{N}_\sigma.\forall y \in \mathbf{N}_x.f(x) \leq f(y),$$

with $\mathbf{N}_\sigma = \{x_0\} \cup \mathbf{N}_{x_0}$.

4.3 Interpretation of a proof with cut of $\forall x.\exists y_1 \ldots \exists y_n.(x < y_1 < \ldots < y_n \wedge f(y_1) \leq \ldots \leq f(y_n))$

In this example, f is a function from natural numbers to natural numbers.

Notice that so far we did not provide an interpretation of cut rule

$$\frac{\Gamma, A \qquad A^\perp, \Delta}{\Gamma, \Delta}.$$

Suppose we have a continuous functional F from approximation maps σ of Γ, A to true examples of $\sigma[\Gamma, A]$ and a continuous functional F' from approximation maps σ' of $A^\perp, \Delta$ to true examples of $\sigma'[A^\perp, \Delta]$. We must show that there exists a continuous functional G from approximation maps ν of Γ, Δ to true examples of $\nu[\Gamma, \Delta]$. The proof is by triple induction over A, a well-founded q/a tree of F and

a well-founded q/a tree of F'. It is just a reformulation of Tait's Normalization Theorem for an infinitary sequent calculus [17] that makes use of the properties of F and F'. We do not include such a proof here: in this example we explain how to interpret concrete instances of cut rule case by case.

Classical proof (top-down). Let $A_n(x, \mathbf{y})$ be

$$x < y_1 < \ldots < y_n \wedge f(y_1) \leq \ldots \leq f(y_n)$$

and let C_n be $\forall x.\exists y_1 \ldots . \exists y_n . A_n(x, \mathbf{y})$.

The proof of C_n is by induction on n. The case $n = 1$ is trivial. Assume we have a proof of C_n and we prove C_{n+1}.

Let x be a natural number and let $\mathbf{y}^0$ be a n-tuple of natural numbers. Recall that $\Gamma \vdash \Delta$ stands for $\Gamma^{\perp}, \Delta$ and consider the following proof tree, where Δ is the sequent $f(x+1) \leq f(y_1^0), f(x+1) > f(y_1^0)$:

$$\dfrac{\dfrac{x < x+1 \qquad A_n(x+1, \mathbf{y}^0) \vdash A_n(x+1, \mathbf{y}^0)}{A_n(x+1, \mathbf{y}^0) \vdash (x < x+1) \wedge A_n(x+1, \mathbf{y}^0)} \qquad \Delta}{A_n(x+1, \mathbf{y}^0) \vdash A_{n+1}(x, x+1, \mathbf{y}^0), f(x+1) > f(y_1^0)}$$

Notice that in the previous proof-tree we skipped some minor steps involving associativity and commutativity of $\wedge$.

Let Γ_0 be the "sequent" obtained at the root of the above proof-tree. Since from $A_n(x+1, \mathbf{y}^0), \ldots, A_n(y_1^{i-1}, \mathbf{y}^i)$ we can prove

$$x < x+1 \wedge x+1 < y_1^0 \wedge y_1^0 < y_1^1 \wedge \ldots \wedge y_1^{i-1} < y_1^i,$$

by transitivity of the order relation we get

$$A_n(x+1, \mathbf{y}^0), \ldots, A_n(y_1^{i-1}, \mathbf{y}^i) \vdash x < y_1^i.$$

Thus, similarly to above, we can prove the "sequent" Γ_{i+1} given by

$$A_n(x+1, \mathbf{y}^0), A_n(y_1^0, \mathbf{y}^1), \ldots, A_n(y_1^i, \mathbf{y}^{i+1}) \vdash A_{n+1}(x, y_1^i, \mathbf{y}^{i+1}), f(y_1^i) > f(y_1^{i+1})$$

for every $i, x \in \mathbf{N}$ and every $\mathbf{y}^0, \ldots, \mathbf{y}^{i+1} \in \mathbf{N}^n$.

By combining together the proofs of $\Gamma_0, \ldots, \Gamma_{i+1}$, we get a proof of

$$A_n(x+1, \mathbf{y}^0), A_n(y_1^0, \mathbf{y}^1), \ldots, A_n(y_1^i, \mathbf{y}^{i+1}) \vdash \Theta_i, B_i$$

where Θ_i is the sequent

$$A_{n+1}(x, x+1, \mathbf{y}^0), A_{n+1}(x, y_1^0, \mathbf{y}^1), \ldots, A_{n+1}(x, y_1^i, \mathbf{y}^{i+1})$$

and B_i is the formula $f(x+1) > f(y_1^0) \wedge \ldots \wedge f(y_1^i) > f(y_1^{i+1})$.

By well-foundedness of natural numbers, B_i must be false for some i (notice that a definite i can be obtained since f is fixed). Hence we have:

$$\frac{A_n(x+1,\mathbf{y}^0), A_n(y_1^0,\mathbf{y}^1),\ldots,A_n(y_1^i,\mathbf{y}^{i+1}) \vdash \Theta_i, B_i \qquad B_i^\perp}{A_n(x+1,\mathbf{y}^0), A_n(y_1^0,\mathbf{y}^1),\ldots,A_n(y_1^i,\mathbf{y}^{i+1}) \vdash \Theta_i}$$

Now we can prove the sequent $A_n^\perp, A_{n+1}$ by means of an adequate sequence of $\exists$- and $\forall$-introductions. After existential quantifications of the last $n+1$ variables in each formula of Θ_i, we obtain a proof of

$$A_n(x+1,\mathbf{y}^0), A_n(y_1^0,\mathbf{y}^1),\ldots,A_n(y_1^i,\mathbf{y}^{i+1}) \vdash \exists \mathbf{z} A_{n+1}(x,\mathbf{z}),$$

where $\mathbf{z}$ is a $n+1$-tuple of variables.

So, expanding our abbreviations, we obtain a proof of the sequent

$$A_n(x+1,\mathbf{y}^0)^\perp, A_n(y_1^0,\mathbf{y}^1)^\perp,\ldots,A_n(y_1^i,\mathbf{y}^{i+1})^\perp, \exists \mathbf{z} A_{n+1}(x,\mathbf{z}).$$

We universally quantify $\mathbf{y}^{i+1}$ in $A_n(y_1^i,\mathbf{y}^{i+1})^\perp$, then $\mathbf{y}^i$ in $A_n(y_1^{i-1},\mathbf{y}^i)^\perp$, down to $\mathbf{y}^0$ in $A_n(x+1,\mathbf{y}^0)^\perp$.

After further $\exists$-introductions, we get $A_n^\perp, A_{n+1}(x)$ and, as result of a last $\forall$-introduction, we prove

$$A_n^\perp, A_{n+1}.$$

Eventually we get:

$$\frac{A_n \qquad A_n^\perp, A_{n+1}}{A_{n+1}}$$

Intuitionistic interpretation. Inductively assume that we have an intuitionistic proof of

$$\forall x \in J. \exists y_1 \ldots \exists y_n \in \mathbf{N}_x. (x < y_1 < \ldots < y_n \wedge f(y_1) \leq \ldots \leq f(y_n)) \qquad (1)$$

for every finite subset J of $\mathbf{N}$, where $\mathbf{N}_x$ is a finite subset of $\mathbf{N}$ depending on x.

Let I be a nonempty finite subset of $\mathbf{N}$ and let x be an arbitrary element of I. We apply (1) to $J = \{x+1\}$. We apply (1) again to $J = \{z_1\}$, where z_1 is a value for y_1 as given by (1). We continue and we generate a sequence $z_0 = x+1, z_1, z_2, \ldots, z_k, z_{k+1}$, where k is the least natural number l such that $f(z_l) \leq f(z_{l+1})$ holds. Then we get an intuitionistic proof of

$$\forall x \in I. \exists y_1 \ldots \exists y_{n+1} \in \mathbf{N}_x. (x < y_1 < \ldots < y_{n+1} \wedge f(y_1) \leq \ldots \leq f(y_{n+1})),$$

with $\mathbf{N}_x = \{z_0,\ldots,z_k\} \cup \mathbf{N}_{z_0} \cup \ldots \cup \mathbf{N}_{z_k}$.

5 Direct interpretation

In this section, we give examples on how to avoid the lengthy step-by-step proof transformation so to get a constructive interpretation of a classical proof directly from the proof itself. Clearly, this technique assumes practice with the step-by-step method. It works faster, in particular when the classical proof to be transformed is not as simple as in the previous section.

5.1 Approximating the square root

We represent reals as (equivalence classes of) rational Cauchy sequences. Thus, quantification over reals is indeed quantification over functions. We do not know, yet, how to approximate statements including quantification over functions, i.e. impredicative statements. This requires a notion of continuity for third order functionals, currently under joint development by S. Berardi and U. de' Liguoro. Therefore we consider first order versions of such statements parametrized over function constants, but containing no explicit quantification over functions. According to [10], this is not a severe restriction in most theorems of classical analysis.

We first recall the *Monotonicity Lemma* (briefly: *ML*).

Lemma 5.1 *(ML)* Let (a_n) be a weakly decreasing rational sequence bound below by some real number L. Then (a_n) is Cauchy.

Proof *(Classical)* For the sake of contradiction suppose that, for some $\epsilon \in \mathbf{Q}^+$ and for all $n \in \mathbf{N}$, there exists $m > n$ with $a_n - a_m > \epsilon$. We define a subsequence (a_{n_i}) of (a_n) by letting

$$\begin{aligned} n_0 &= 0; \\ n_{i+1} &= \text{any natural number } j > n_i \text{ such that } a_{n_i} - a_j > \epsilon. \end{aligned}$$

By construction we have $a_0 - a_{n_i} > i\epsilon$. Let k be such that $k\epsilon > a_0 - L$. Then $a_0 - a_{n_k} > k\epsilon > a_0 - L$ and so $a_{n_k} < L$: contradiction. □

Indeed, for arbitrary sequence (a_n) as in the statement of *ML*, there is no effective way of finding, for every $\epsilon \in \mathbf{Q}^+$, a natural number n such that $a_n - a_m \leq \epsilon$ for all $m > n$. This is equivalent to saying that *ML* is not intuitionistically provable, as the following argument shows: to any function $f : \mathbf{N} \to \mathbf{N}$ associate a sequence $a^f = (a^f_n)$ defined by

$$a^f_n = \begin{cases} 1 & \text{if } f(m) > 1 \text{ for all } m \leq n; \\ 0 & \text{otherwise.} \end{cases}$$

The sequence a^f is weakly decreasing and bound below by 0. Yet, there is no effective method of finding, for every f, a natural number n such that $a^f_n - a^f_m$ is less than, say, 0.1 for all $m > n$. Such an effective method would amount to effectively knowing the value of $\lim_{n\to\infty} a^f_n$, that is, whether $f(n) > 1$ for all n or not. Clearly, there is no effective way of deciding such a property uniformly on f.

An intuitionistic interpretation of ML

Let (a_n) be as in the statement of *ML*. For simplicity, let us use *ML* also to refer to its first order formalization.

The meaning of $\psi(ML)$ is that (a_n) satisfies, in a continuous way, any approximation of the property of "being Cauchy". So, for any $\epsilon > 0$, $\psi(ML)$ implies

$$\exists n.\forall m \in \sigma(n).(a_n - a_m \leq \epsilon) \tag{2}$$

for any map

$$\begin{array}{rccc} \sigma: & \mathbf{N} & \to & \mathcal{P}_{fin}(\mathbf{N}) \\ & n & \mapsto & \sigma(n) \subset]n, \infty[. \end{array}$$

With the restriction to the domain of $\forall m$ imposed by σ, the classical proof becomes effective: fix $\epsilon \in \mathbf{Q}^+$ and define a sequence (n_i) of natural numbers by letting $n_0 = 0$ and

$$n_{i+1} = \begin{cases} n_i & \text{if } a_{n_i} - a_m \leq \epsilon \text{ for all } m \in \sigma(n); \\ \text{any } m \in \sigma(n) \text{ such that } a_{n_i} - a_m > \epsilon & \text{otherwise.} \end{cases}$$

Let k be the least integer i such that $i\epsilon > a_0 - L$. The argument used in the classical proof of *ML* ensures the existence of a least $j \leq k$ such that $n_j = n_{j+1}$. The natural number n_j is a witness for the existential in (2).

The given intuitionistic interpretation looks weak, because we find a_n which satisfies $a_n - a_m \leq \epsilon$ for finitely many m's only. Yet, it is classically equivalent to the original *ML*. Intuitionistically, it is strong enough to replace *ML* when proving simply existential statements, as we see in the following example.

Given any $r \in \mathbf{Q}^+$, we want to define a rational sequence (a_n) approximating the square root of r. Let $s \in \mathbf{Q}^+$ be such that $s^2 > r$. Define

$$a_0 = s; \qquad a_{n+1} = \frac{1}{2}(a_n + \frac{r}{a_n}) = \frac{a_n^2 + r}{2a_n}. \tag{3}$$

Using *ML*, we first give a classical proof of (a_n^2) converging to r. We want to interpret it constructively and get a bound on the number of steps needed to have $|a_n^2 - r| < \epsilon$, for $\epsilon \in \mathbf{Q}^+$.

Lemma 5.2 Let (a_n) be the sequence defined in (3). Then $a_n^2 \to r$.

Proof *(Classical)* We show that (a_n) is weakly decreasing and bound below by $L = r/a_0$. We first prove inductively that $a_n^2 \geq r$. We have $a_0^2 \geq r$ by hypothesis. Let us deal with the inductive step: we assume

$$a_0^2 \geq a_1^2 \geq \cdots \geq a_n^2$$

and prove $a_n^2 \geq a_{n+1}^2 \geq r$. We have

$$a_{n+1}^2 \geq r \quad \Leftrightarrow \quad \frac{a_n^4 + 2ra_n^2 + r^2}{4a_n^2} \geq r \quad \Leftrightarrow \quad (a_n^2 - r)^2 \geq 0$$

and the latter is clearly true: this proves ${a_n}^2 \geq r$. So $a_n \geq r/a_n$ and, since a_{n+1} is the arithmetic mean of a_n and r/a_n, we get $a_n \geq a_{n+1} \geq r/a_n$. Eventually, we get $a_0 \geq a_n$ and

$$a_n \geq \frac{r}{a_n} \geq \frac{r}{a_0} = L.$$

By *ML*, (a_n) is Cauchy. Therefore, for every $\epsilon \in \mathbf{Q}^+$, there exists $n \in \mathbf{N}$ such that $a_n - a_m \leq \epsilon/2a_0$, for all $m > n$. By choosing $m = n + 1$, we have

$$\frac{a_n^2 - r}{2a_n} = \frac{1}{2}(a_n - \frac{r}{a_n}) = a_n - a_{n+1} \leq \frac{\epsilon}{2a_0},$$

hence $a_n^2 - r \leq 2a_n(\epsilon/2a_0) \leq \epsilon$. Being (a_n) weakly decreasing, we also have $a_m^2 - r \leq \epsilon$, for all $m \geq n$. Therefore $a_n^2 \to r$. □

Admittedly, the previous proof is unnecessarily detailed. We did it on purpose, just to point out its key step, namely the argument showing the existence of n such that $a_n^2 - r \leq \epsilon$, for every $\epsilon \in \mathbf{Q}^+$. Notice that, for fixed ϵ, the statement

$$\exists n.(a_n^2 - r \leq \epsilon)$$

is simply existential, hence the proof itself implicitly provides a construction of an upper bound for the least n such that $a_n^2 - r \leq \epsilon$.

However, it is by no means obvious where the construction lies, due to the intuitionistic unprovability of *ML*.

An intuitionistic interpretation of the classical proof of $\forall\epsilon.\exists n.(a_n^2 - r \leq \epsilon)$

Fix $\epsilon \in \mathbf{Q}^+$. In the classical proof of $\exists n.(a_n^2 - r \leq \epsilon)$, we applied *ML* to prove that (a_n) is Cauchy, but indeed we needed just to find n such that $a_n - a_{n+1} \leq \epsilon/2a_0$, because the sequence is weakly decreasing. Formally, this means that we only used the approximation of the property of being Cauchy given by the map $\sigma : n \mapsto \{n+1\}$. Such an approximation is intuitionistically provable, as we showed when intuitionistically interpreting *ML*.

In the intuitionistic interpretation of *ML*, we find n such that $a_n - a_{n+1} \leq \epsilon/2a_0$ as follows: we first get the sequence $n_0 = 0$, $n_{i+1} \in \{n_i + 1\}$, that is $n_i = i$, for all i. Then we keep on testing the required condition on it, until true.

The argument also contains a bound m on the number of steps: the least natural number k such that $(\epsilon\ 2a_0)k > (a_0 - L)$, i.e. the least natural number greater than $2a_0(a_0 - L)/\epsilon$.

It is interesting to compare m with the number of steps actually needed to a_n^2 to get closer than ϵ to r. Take $r = 750$ and $a_0 = 30$; then $L = 25$ and m is the least integer greater than $300/\epsilon$. For $\epsilon = 10^{-n}$, we get $m = 3 \cdot 10^{n+2} + 1$. Yet, direct calculation shows that we already have $a_4^2 - r < 10^{-10}$.

The classical proof is not responsible for the inaccuracy of the bound, though. The point is that, when using a general result like *ML*, we do not exploit at all the way (a_n) was defined in (3). Notice that (a_n) is obtained by applying Newton's tangent method to the function $y = x^2 - r$.

What the classical proof does not know is that (a_n) converges very rapidly to the square root of r. If we proved that (a_n^2) converges to r by means of auxiliary results including a description of the behavior of (a_n) (for instance, the theorem proving correctness of Newton's method), we would get more precise information about the convergence speed of (a_n^2) to r.

5.2 Uniform continuity

We recall some well-known facts in order to motivate the next example. It is a theorem of classical real analysis that every continuous map $f : [a, b] \to \mathbf{R}$ is uniformly continuous. As a consequence, for every rational $\epsilon > 0$, we can find a step function g on $[a, b]$ (i.e. the union of finitely many constant functions defined on disjoint subintervals of $[a, b]$) approximating f pointwise up to ϵ. Therefore $|\int_a^b f(x)\mathrm{d}x - \int_a^b g(x)\mathrm{d}x| < \epsilon$. The interest of this fact from the viewpoint of numerical computation is clear: the value of $\int_a^b f(x)\mathrm{d}x$ can be approximated up to any degree of accuracy by means of $\int_a^b g(x)\mathrm{d}x$, which is indeed a finite sum.

In order to retrieve a construction of step function g from the proof of uniform continuity of f, we must restrict ourselves to the case when f is computable and when the statement "g is a step function approximating f up to ϵ" is decidable. Under these assumptions the classical proof of existence of g is the proof of a simply existential statement. Thus, it provides a construction of a step function g as above, for every $\epsilon > 0$.

Throughout this section, the following *main assumptions* are in force:

- $f : [a, b] \to \mathbf{R}$ is a computable continuous function such that $f(\mathbf{Q} \cap [a, b]) \subseteq \mathbf{Q}$. If the latter were not satisfied, computability of f would yield a family $(f_\epsilon)_{\epsilon \in \mathbf{Q}^+}$ of functions $f_\epsilon : [a, b] \to \mathbf{R}$, with f_ϵ approximating f up to ϵ and $f_\epsilon(\mathbf{Q} \cap [a, b]) \subseteq \mathbf{Q}$. Dealing with such a family would make notation very cumbersome, with no real gain in generality.

- f is monotonic (weakly increasing or weakly decreasing) on $[a, b]$. If not, it is usually possible to split $[a, b]$ into smaller intervals on which f is monotonic. We actually assume that f is weakly increasing on $[a, b]$ (only trivial changes are needed in what follows if f is weakly decreasing).

- $a = 0$ and $b = 1$, the general case being easily recovered by means of affine transformations.

We will see that, under the previous assumptions, the statement "g is a step function approximating f up to ϵ" is decidable.

Recall that f is *uniformly continuous* if

$$UC : \quad \forall \epsilon \in \mathbf{Q}^+ . \exists \delta \in \mathbf{Q}^+ . \forall x, y \in [0, 1] . (|x - y| < \delta \to |f(x) - f(y)| < \epsilon).$$

Representing each real number $x \in [0, 1]$ as a unary predicate on $\mathbf{N}$, with $x(i)$ saying "the i-th digit in the binary expansion of x is 0", as done in [10], would introduce second order quantifications in the predicative translation of *UC*. Indeed, we may circumvent the problem by restricting ourselves to reals that are definable in first order arithmetic but, for simplicity, we express *UC* in its equivalent form *DUC* (abbreviation for *Discretized Uniform Continuity*). Equivalence of *UC* and *DUC* for continuous monotonic f can easily be proved. *DUC* formally states, under

the main assumptions, the existence of step functions approximating f up to any degree of accuracy.

$$DUC: \quad \forall \epsilon \in \mathbf{Q}^+.\exists n \in \mathbf{N}^+.\forall 0 \leq i < n.(f((i+1)/n) - f(i/n) < \epsilon)$$

So DUC says that, for n corresponding to a given ϵ, the step function g defined by

$$g(x) = \begin{cases} f(x) & \text{if } x = 0; \\ f(i/n) & \text{if } x \in]i/n, (i+1)/n] \text{ and } 0 \leq i < n \end{cases}$$

is an approximation of f up to ϵ.

We now introduce a classical proof of DUC that is an adaptation of one of the well-known proofs. Then we turn it into a constructive proof, obtained by applying our constructivization technique to the statement that f is continuous.

A classical proof of DUC

We first want to give a nonconstructive proof that DUC holds for any weakly increasing continuous function f defined on $[0,1]$. As in the previous section, we choose a classical proof that is better suited for constructivization.

Let $2 = \{0,1\}$. We denote by 2^n the set of binary sequences of length n, and we let $2^* = \cup_{n \in \mathbf{N}} 2^n$. We write $\sharp\alpha$ for the length of $\alpha \in 2^*$. $\alpha_{|n}$ stands for the prefix of α of length n, with $\alpha_{|n} = \alpha$ if $\sharp\alpha \leq n$. By $\alpha < \beta$ we mean that α is smaller than β in the lexicographic order. We use the same notation for infinite binary sequences, whose set is denoted by 2^ω.

Every element of 2^* can be identified with an element of $\mathbf{Q} \cap [0,1[$, in the usual way. In the sequel, we will freely use this identification.

Proposition 5.3 Let $f : [0,1] \to \mathbf{R}$ be a weakly increasing continuous function. Then f satisfies DUC.

Proof *(Classical)* Fix $\epsilon \in \mathbf{Q}^+$. We consider the following subtree T_ϵ of the full binary tree: the leaves of T_ϵ are the least $\alpha \in 2^*$ (with respect to length) such that $f(\alpha + 2^{-(\sharp\alpha+1)}) - f(\alpha) < \epsilon$.

We claim that T_ϵ has no infinite branch. For, let α be a branch of T_ϵ. Notice that α represents a real number in $[0,1]$.

By continuity of f at α, there exists $\delta \in \mathbf{Q}^+$ such that

$$\forall x \in]\alpha - \delta, \alpha + \delta[\cap [0,1].(|f(x) - f(\alpha)| < \epsilon/2).$$

Let k be the least natural number j such that $2^{-j} < \delta$. By applying continuity twice, we get

$$f(\alpha_{|k} + 2^{-(k+1)}) - f(\alpha_{|k}) < \epsilon.$$

So T_ϵ has no infinite branch and, by *König's Lemma*, there is a finite bound m on the length of branches of T_ϵ. Put $n = 2^m$. □

A constructive proof of DUC

We want to give a constructive proof of DUC for a function f satisfying the main assumptions previously stated. It suffices to provide, for all $\epsilon \in \mathbf{Q}^+$, a constructive proof of finiteness of the tree T_ϵ introduced in the classical proof of DUC. Notice that the tree T_ϵ is decidable.

Let us introduce the binary predicate $P(\alpha, j)$ on $2^* \times \mathbf{N}$ saying "there are at least j levels of T_ϵ below α." Formally:

$$P(\alpha, j) = \exists \beta \in 2^j.(\alpha \star \beta \in T_\epsilon),$$

where $\star$ stands for juxtaposition. The predicate P is decidable: in the sequel we will treat it as an atomic formula.

If $\alpha, \beta \in 2^*$, we write $\alpha \ll \beta$ as abbreviation for "α, β have the same length and α is to the left of β", that is:

$$\alpha \ll \beta = (\sharp\alpha = \sharp\beta) \wedge (\alpha < \beta).$$

We also introduce a predicate Q on natural numbers, the meaning of $Q(i)$ being "there is an infinite branch in T_ϵ and the node at level i in the leftmost infinite branch is 0" (levels are numbered starting from zero at the root). This is equivalent to saying: "there exists a sequence γ_1 of length i such that $\gamma_1 \star 0$ is the leftmost node at level i of T_ϵ and has successors at infinitely many levels below level i". Formally:

$$Q(i) = \exists \gamma_1 \in 2^i.(\forall j_1.P(\gamma_1 \star 0, j_1) \wedge \forall \beta_1 \ll \gamma_1 \star 0.\exists k_1.\neg P(\beta_1, k_1)).$$

Let us also explicitly write $\neg Q(i)$, after variable renaming, since we will refer to it in the sequel:

$$\neg Q(i) = \forall \gamma_2 \in 2^i.(\exists j_2.\neg P(\gamma_2 \star 0, j_2) \vee \exists \beta_2 \ll \gamma_2 \star 0.\forall k_2.P(\beta_2, k_2)).$$

From the assumption of continuity of f (classically understood), we can classically get a proof of

$$C: \ \exists \delta \in \mathbf{Q}^+.\forall \alpha \in 2^n.[\forall i < n.(\alpha_i = 0 \leftrightarrow Q(i)) \rightarrow R(\alpha)],$$

where n is the least positive natural number j such that $2^{1-j} < \delta$ and $R(\alpha)$ is $f(\alpha + 2^{-n}) - f(\alpha) < \epsilon$. The previous statement is just a consequence of the continuity argument applied at the end of the classical proof: roughly, it says that if α is closer than 2^{-n} to the leftmost infinite branch γ in T_ϵ (recall that α and γ "are" real numbers in $[0, 1]$), then the images of α and $\alpha + 2^{-n}$ are closer than ϵ (this is true because both lie in $]\gamma - \delta, \gamma + \delta[$, by choice of n).

Now we expand C. By logical identities, the formula in square brackets becomes

$$[\exists i < n.[(\alpha_i = 0 \wedge \neg Q(i)) \vee (\alpha_i = 1 \wedge Q(i))]] \vee R(\alpha)].$$

One can further expand $Q(i)$ and $\neg Q(i)$, according to their definitions.

We first examine the effect of application of an approximation map to C. Let us code a subformula in the expansion of C as follows: the a_k-th subformula of the a_{k-1}-th subformula ... of the a_0-th subformula of C is coded by $\langle a_0, \ldots, a_k \rangle$.

Here are two examples: $p_2 = \langle \delta, \alpha, i, 0, 1 \rangle$ is the position of $\neg Q(i)$ in C. The 0 digit tells us that $\neg Q(i)$ is in the left disjunct in

$$(\alpha_i = 0 \wedge \neg Q(i)) \vee (\alpha_i = 1 \wedge Q(i)).$$

The digit 1 tells us that $\neg Q(i)$ is the right conjunct in $(\alpha_i = 0 \wedge \neg Q(i))$. Similarly, $p_1 = \langle \delta, \alpha, i, 1, 1 \rangle$ is the position of $Q(i)$ in C.

Here and in the sequel we choose to remain informal about this sort of technicalities for sake of avoiding cumbersome notation.

Let σ be a unary approximation map for C. Recall that σ maps the position p of an arbitrary universal subformula $\forall x \in I.A(x)$ of C to an element $\sigma(p) \in I$. Let us describe the approximation $\sigma[C]$ defined by σ: we recursively replace every universal subformula $\forall x \in I.A(x)$ of C in position p, say, with $A(\sigma(p))$.

Let $\alpha = \sigma(\delta)$. Then $\sigma[C]$ is

$$\exists \delta \in \mathbf{Q}^+.[\exists i < n.[(\alpha_i = 0 \wedge \sigma[\neg Q(i)]) \vee (\alpha_i = 1 \wedge \sigma[Q(i)])] \vee R(\alpha)].$$

Let us compute $\sigma[\neg Q(i)]$. Let $\gamma_2 = \sigma(p_2)$ and $k_2 = \sigma(p_2, \gamma_2, 1, \beta_2)$. Then

$$\sigma[\neg Q(i)] = \exists j_2.\neg P(\gamma_2 \star 0, j_2) \vee \exists \beta_2 \ll \gamma_2 \star 0.P(\gamma_2, k_2).$$

For what concerns $\sigma[Q(i)]$, let $j_1 = \sigma(p_1, \gamma_1, 0)$ and $\beta_1 = \sigma(p_1, \gamma_1, 1)$. Then

$$\sigma[Q(i)] = \exists \gamma_1 \in 2^i.[P(\gamma_1 \star 0, j_1) \wedge \exists k_1.\neg P(\beta_1, k_1)].$$

By results mentioned in section 3, classical provability of C implies the existence of a connected functional F that, applied to a unary approximation map σ for C, returns a constructive proof $F(\sigma)$ of $\sigma[C]$. Therefore, for every σ, we can regard F as providing values for each existential variable in $\sigma[C]$ so that the quantifier-free sentence $F\{\sigma[C]\}$ obtained from $\sigma[C]$ by assigning to each existential variable the value computed for it by F is true. We write

$$F(\sigma) = \langle \delta, i, j_2, \beta_2, \gamma_1, j_1 \rangle.$$

Here is $\tau\{\sigma[C]\}$, with $\tau = F(\sigma)$:

$$[\alpha_i = 0 \wedge (\neg P(\gamma_2 \star 0, j_2) \vee P(\beta_2, k_2))] \vee [\alpha_i = 1 \wedge P(\gamma_1 \star 0, j_1) \wedge \neg P(\beta_1, k_1)] \vee R(\alpha).$$

Recall that our goal is to get a constructive proof that T_ϵ is finite. We know that F has a well-founded q/a tree T whose branches are connected finite approximation maps. We work with branches of T corresponding to certain approximation maps. Let $\nu \in 2^\omega$ be such that every branch τ in T_ϵ to the left of ν is finite. Clearly, the constant sequence zero satisfies the condition. To every such ν we want to associate an approximation map σ_ν for C satisfying the following condition: let n, i, k_1, j_2 be the values taken by the corresponding variables in $F\{\sigma_\nu[C]\}$ and let

$M = \max\{n, i+k_1, i+j_2\}$. We claim that $\nu_{|M}$ is a (not necessarily proper) extension of a leaf of T_ϵ. We refer to the previous claim as *Finiteness Claim* (briefly: *FC*).

Now we define $\sigma_\nu(p)$ for every position p of a universal formula in C so that σ_ν satisfies *FC*.

In order to simplify the definition of σ_ν, we give the following definition: let σ be an approximation map on C. We say that a position $p = \langle q_1, \ldots, q_r\rangle$ in C is *compatible with* σ if, for every $1 \leq i < r$ such that such that $p_{|i} = \langle q_1, \ldots, q_{i-1}\rangle$ is a position of a universal subformula, we have $q_i = \sigma(p_{|i})$.

Let ξ be the branch of the q/a tree T corresponding to the computation of $F(\sigma)$ and let p be a position in the domain of ξ (recall that branches of T are finite approximation maps, see [1]). Then connectedness of F implies that p is compatible with σ. Therefore it suffices to define $\sigma_\nu(p)$ only when p is compatible with σ. When p is not compatible with σ_ν, then $\sigma_\nu(p)$ can be arbitrarily defined since the pair $\langle p, \sigma_\nu(p)\rangle$ does not belong to any branch of T.

Let $\nu \in 2^\omega$ be such that for no infinite branch α in T_ϵ we have $\alpha < \nu$. We define $\sigma_\nu(p)$, when p is compatible with σ_ν. Given $\delta \in \mathbf{Q}^+$, recall that n always stands for the least positive natural number j such that $2^{1-j} < \delta$.

1. We let $\sigma_\nu(\delta) = \nu_{|n}$.
2. Let $\alpha = \sigma_\nu(\delta)$ and let $p_2 = \langle \delta, \alpha, i, 0, 1\rangle$.
   We let $\sigma_\nu(p_2) = \nu_{|i}$.
   Let $\gamma_2 = \sigma_\nu(p_2)$. Then, for every $\beta_2 \ll \gamma_2 \star 0$, we let
   $$\sigma_\nu(p_2, \gamma_2, 1, \beta_2) = \min\{k : \neg P(\beta_2, k)\}.$$
   The definition is correct since $\beta_2 \ll \nu_{|i+1}$ for every β_2, hence there exists k such that $\neg P(\beta_2, k)$, by choice of ν.
3. Let $\alpha = \sigma_\nu(\delta)$ and let $p_1 = \langle \delta, \alpha, i, 1, 1\rangle$.
   If $\alpha_i = \nu_i = 0$, we define $\sigma_\nu(p_1, \gamma_1, 0) = 0$ and
   $$\sigma_\nu(p_1, \gamma_1, 1) = \max\{\beta : \beta \in 2^{i+1} \text{ and } \beta \ll \gamma_1 \star 0\}.$$
   If $\alpha_i = \nu_i = 1$ and $\nu_{|i} \ll \gamma_1$, we define
   $$\sigma_\nu(p_1, \gamma_1, 0) = 0 \quad \text{and} \quad \sigma_\nu(p_1, \gamma_1, 1) = \nu_{|i+1}.$$
   The definition is correct since $\nu_{|i+1} \ll \gamma_1 \star 0$.
   If $\alpha_i = \nu_i = 1$ and $\gamma_1 \ll \nu_{|i}$ or $\gamma_1 = \nu_{|i}$, we define $\sigma_\nu(p_1, \gamma_1, 0) = \min\{j : \neg P(\gamma_1 \star 0, j)\}$ and
   $$\sigma_\nu(p_1, \gamma_1, 1) = \max\{\beta : \beta \in 2^{i+1} \text{ and } \beta \ll \gamma_1 \star 0\}.$$
   The definition is correct since, from $\gamma_1 \ll \nu_{|i}$ or $\gamma_1 = \nu_{|i}$, we get $\gamma_1 \star 0 \ll \nu_{|i+1}$ and so there exists j_1 such that $\neg P(\gamma_1 \star 0, j_1)$.

Lemma 5.4 Let $\nu \in 2^\omega$ be such that every branch $\tau < \nu$ in T_ϵ is finite. Then the approximation map σ_ν defined above satisfies FC.

Proof We know that $F(\sigma)\{\sigma_\nu[C]\}$ is intuitionistically provable. We examine three cases, according to the description of $F\{\sigma_\nu[C]\}$ previously given.

1. If the disjunct $[\alpha_i = 0 \wedge (\neg P(\gamma_2 \star 0, j_2) \vee P(\beta_2, k_2))]$ is provable, then $\neg P(\beta_2, k_2)$ holds by definition of σ_ν and so $\neg P(\gamma_2 \star 0, j_2)$ does. Since $\gamma_2 \star 0 = \nu_{|i+1}$, by definition of the predicate P we have that $\nu_{|i+j_2}$ is or extends a leaf of T_ϵ. Since $i + j_2 \leq M$, the same is true for $\nu_{|M}$.

2. If the disjunct $[\alpha_i = 1 \wedge P(\gamma_1 \star 0, j_1) \wedge \neg P(\beta_1, k_1)]$ is intuitionistically provable, notice first that $\alpha_i = \nu_i$, so $\nu_i = 1$. Notice also that if it were $\gamma_1 \ll \nu_{|i}$ or $\gamma_1 = \nu_{|i}$, then, by definition of σ_ν, we would have $\neg P(\gamma_1 \star 0, j_1)$.

   So only $\nu_{|i} \ll \gamma_1$ can happen. Hence $\beta_1 = \nu_{|i+1}$ and $\neg P(\beta_1, k_1)$. Therefore $\nu_{|i+k_1}$ is or extends a leaf of T_ϵ. Since $i + k_1 \leq M$, the same is true for $\nu_{|M}$.

3. If $R(\alpha)$ is intuitionistically provable, then from $\alpha = \nu_{|n}$ it follows that $\nu_{|n}$ is or extends a leaf of T_ϵ. Given that $n \leq M$, the same is true for $\nu_{|M}$.

□

Let M_ν be the bound corresponding to a given $\nu \in 2^\omega$ having the property that every branch $\tau < \nu$ in T_ϵ is finite. If $\nu_{|M_\nu}$ is the constant sequence 1, then T_ϵ is finite because each of its branches is either extended (not necessarily properly) by $\nu_{|M_\nu}$ or is smaller than $\nu_{|M_\nu}$.

If $\nu_{|M_\nu} = \rho \star 0 \star 1 \ldots \star 1$, then we let $\nu' = \rho \star 1 \star 0^*$ as new value of ν, where 0^* is the infinite constant sequence 0. If $\nu_{|M_\nu}$ is the constant sequence 1, we let $\nu' = \nu$. Notice that every branch $\tau < \nu'$ in T_ϵ is finite.

Starting with $\nu(0) = 0^*$ and updating the value of ν as just described we get a sequence $(\nu(j))$ of elements of 2^ω. Notice that we have a proof of finiteness of T_ϵ if we show that there exists $j \in \mathbf{N}$ such that $\nu(j) = \nu(j+1)$: this is what we want to prove next.

We consider the subtree S of the well-founded q/a tree T of F whose branches are computations of F needed to compute $F(\sigma_{\nu(j)})$, for some j. Let ξ be a branch in S. We define a well-founded partial ordering $\lhd$ of the immediate successors of ξ in S (if any). Descendants are of the form $\xi \star \langle p, r \rangle$, where p is the position of a universal subformula $\forall x \in I.A(x)$ and $r \in I$.

If $I = \mathbf{N}$, we stipulate that $\xi \star \langle p, r \rangle \lhd \xi \star \langle p, 0 \rangle$, for all $r \in \mathbf{N}^+$.

If $I = 2^i$, for some i, then $\xi \star \langle p, r \rangle \lhd \xi \star \langle p, s \rangle$ if and only if $s < r$.

The set S and the set of immediate successors of each node in S are well-founded with respect to the extension relation and the partial order $\lhd$, respectively. Thus we can prove by induction over the (well-founded) q/a order of T that S is well-founded with respect to the order $\prec$ given by the transitive closure of the two partial orders.

Lemma 5.5 Let χ_j be the maximal branch in S corresponding to the computation of $F(\sigma_{\nu(j)})$. Then, for every j, $\chi_{j+1} \preceq \chi_j$.

Proof Notice that the sequence $(\nu(j))$ is strictly increasing in the lexicographic order Suppose $\chi_j \neq \chi_{j+1}$ for some j and let $\xi \star \langle p, r\rangle$ and $\xi \star \langle q, s\rangle$ be the nodes corresponding to the first point where the two disagree. Then $p = q$ since in a q/a tree p and q both depend only on ξ, and so $r \neq s$. We claim that $\xi\star\langle p, s\rangle \prec \xi\star\langle p, r\rangle$. We distinguish different cases, according to what position p is (and hence according to the definition of $\sigma_\nu(p)$).

1. If p is δ, then $r = \nu(j)_{|n}$ and $s = \nu(j+1)_{|n}$. So $\xi \star \langle p, r\rangle$ is greater or equal to $\xi \star \langle p, s\rangle$ with respect to $\prec$, because the the sequence $(\nu(j))$ is strictly increasing in the lexicographic order.

2. If p is p_2, then $r = \nu(j)_{|i}$ and $s = \nu(j+1)_{|i}$, the conclusion follows as in the previous case.

   If p is $\langle p_2, \gamma_2, 1, \beta_2\rangle$, then $r = \min\{k : \neg P(\beta_2, k)\} = s$.

3. Suppose p is $\langle p_1, \gamma_1, l\rangle$, with $l = 0, 1$. We follow the definition of $\sigma_\nu(p)$.

   Suppose $\alpha_i = \nu(j)_i = \nu(j+1)_i = 0$. For $l = 0$, we have $r = 0 = s$. For $l = 1$, we still have $r = s$, by definition of $\sigma_\nu(p)$.

   Suppose $\alpha_i = \nu(j)_i = \nu(j+1)_i = 1$.

   If $\nu(j+1)_{|i} \ll \gamma_1$, then for $l = 0$, we have $r = 0 = s$. For $l = 1$, we have

   $$r = \nu(j)_{|i+1} \ll \text{ (or equal to) } \nu(j+1)_{|i+1} = s$$

   and the conclusion follows by definition of $\prec$.

   The cases when $\gamma_1 \ll \nu(j+1)_{|i}$ or when equality holds are treated in a similar way.

   Let us consider the case when

   $$\nu(j)_{|i} \ll \gamma_1 \ll \text{ (or equal to) } \nu(j+1)_{|i}.$$

   For $l = 0$, we have $r = 0 \leq s$, and, for $l = 1$,

   $$r = \nu(j)_{|i+1} \ll \text{ (or equal to) } s.$$

   In both subcases the conclusion follows by definition of $\prec$.

□

Theorem 5.6 T_ϵ is finite.

Proof As already noticed, it suffices to show that $\nu(j) = \nu(j+1)$, for some $j \in \mathbf{N}$.
Consider the family $(X_i)_{i\in\mathbf{N}}$ of finite subsets of $\mathbf{N}$ defined by

$$X_i = [i, i + 2^{M_{\nu(i)}}].$$

By lemma 5.5 and by well-foundedness of $\prec$, there exists $k \in \mathbf{N}$ such that $\chi_j = \chi_k$, for all $j \in X_k$. For all $j \in X_k$ we also have $F(\sigma_{\nu(j)}) = F(\sigma_{\nu(k)})$ and so $M_{\nu(j)} = M_{\nu(k)} = K$, for some $K \in \mathbf{N}$. Since the sequence $(\nu(j)_{|K})_{j \geq k}$ can take at most 2^K different values and is weakly increasing with respect to $\ll$, it must be that $\nu(j)_{|K} = \nu(j+1)_{|K}$ for some $j \in X_k$. We conclude that $\nu(j) = \nu(j+1)$, for some $j \in X_k$. □

References

[1] S. Baratella and S. Berardi. *Yet Another Constructivization of Classical Logic,* Proc. Conference *Twenty-five Years of Constructive Type Theory,* G. Sambin and J.Smith eds., Oxford University Press (1998), pp. 1-20.

[2] S. Baratella and S. Berardi. *Approximating Classical Theorems,* to appear in Journal of Logic and Computation.

[3] T. Coquand. *A Semantics of Evidence for Classical Arithmetic.* Journal of Symbolic Logic, vol. 60-1 (1995), pp. 325-337.

[4] H. Friedman. *Classically and Intuitionistically Provably Recursive Functions.* In *Higher Set Theory,* D.S. Scott and G.H. Muller eds., Lecture Notes in Mathematics 699, Springer-Verlag (1978), pp. 21-28.

[5] H. Friedman. *The Consistency of Classical Set Theory relative to a Set Theory with Intuitionistic Logic.* Journal of Symbolic Logic, vol. 38 (1973), pp. 315-319.

[6] H. Herbelin. *Sequents qu'on Calcule,* Ph.D. Thesis, Université Paris VII, 1995.

[7] S.C. Kleene. *Introduction to Metamathematics.* Van Nostrand, Princeton NJ, 1950.

[8] S.C. Kleene. *Countable Functionals.* In *Constructivity in Mathematics.* Proc. Coll. Amsterdam (1957), pp. 81-100.

[9] G. Kreisel. *On the Interpretation of Non-finitist Proofs.* Journal of Symbolic Logic, vol. 16-4 (1951), pp. 241-267.

[10] A. Marcone. *Notes on Simpson's Reverse Mathematics.* Università di Torino, 1985.

[11] C. Murthy. *Extracting Constructive Content from Classical Proofs.* Ph.D. thesis, Cornell University, 1990.

[12] P.S. Novikov. *On the Consistency of certain Logical Calculus.* Matematiceskij Sbornik (Recueil-Mathématique T.12), vol. 54 (1943), pp. 230-260.

[13] M. Parigot. *Proofs as Programs.* In *Computational Logic and Proof Theory*, G. Gottlob et al. eds. Lecture Notes in Computer Science 713, Springer-Verlag (1993), pp. 263-276.

[14] C. Paulin-Mohring. *Extraction de Programmes dans le Calcul des Constructions.* Ph.D. Thesis, Université Paris VII, 1989.

[15] D. Prawitz. *Ideas and Results in Proof Theory.* Proc. *2nd Scandinavian Logic Symposium (Univ. Oslo, Oslo 1970).* Studies in Logic and the Foundation of Mathematics 63. North-Holland, Amsterdam (1971), pp. 235-307.

[16] D. Prawitz. *Natural Deduction.* Almqvist and Wiksell, Stockholm, 1965.

[17] W.W. Tait. *Normal Derivability in Classical Logic.* In *The Syntax and Semantics of Infinitary Languages.* J. Barwise editor. Lecture Notes in Mathematics n. 72. Springer-Verlag, Berlin (1968), pp. 204–236.

[18] A.S. Troelstra and D. van Dalen. *Constructivism in Mathematics - An Introduction, vol. II.* North-Holland, Amsterdam, 1988.