Classical and Intuitionistic Arithmetic with Higher Order Comprehension Coincide on Inductive Well-Foundedness

Stefano Berardi

Università di Torino, Italy

Abstract

Assume that we may prove in Arithmetic with Comprehension axiom that a primitive recursive binary relation R is well-founded, using the inductive definition of well-founded. In this paper we prove that the proof that R is well-founded may be made intuitionistic. Our result generalizes to any implication between such formulas. We conclude that if we are able to formulate any mathematical problem as the fact that some primitive recursive relation is well-founded, then intuitionistic and classical provability coincide, and for such a statement we may always find an intuitionistic proof, if we may find a proof at all.

1998 ACM Subject Classification F.4.1 Mathematical Logic

Keywords and phrases Intuitionism, Inductive Definitions, Proof Theory, impredicativity, omega rule

Digital Object Identifier 10.4230/LIPIcs.CSL.2015.343

1 Introduction. A conservativity result for the statements of inductive well-foundedness

The proof principle of induction, originally called *transfinite induction*, is credited to the founder of intuitionism, Brouwer ([19]). In 1967 Howard and Kreisel [10] remarked that (transfinite) induction is the most useful formulation of well-foundedness in an intuitionistic context. In 1971, P. Martin-Löf studied an intuitionistic natural deduction version of transfinite induction [13]. By building over their work, many classical theorems, whose original version is not intuitionistically provable, have been reformulated in such a way to become intuitionistically provable. For some primitive recursive relations $R_1, \ldots, R_n$, R over `Nat`, the new statements have the following form:

(1) "if $R_1, \ldots, R_n$ are inductively well-founded, then R is inductively well-founded"

Among many examples we recall: Higman Lemma [5], [7], compactness results in formal topology [6], Ramsey Theorem in Combinatorial Mathematics, the Termination Theorem and the Size-Change Termination Theorem in Computer Science [3], [20].

The results of this paper are an *a posteriori* justification of the existence of these intuitionistic results. We guarantee, in the case of a classical proof of a statement of the form (1), that constructivization is always possible in principle, at least for the arithmetical proofs using Comprehension of all finite orders: second order arithmetic, third order and so forth. Comprehension axiom for sets of natural numbers says that any predicate on natural numbers defines a set, Comprehension axiom for sets of sets of natural numbers says that any predicate on sets of natural numbers defines a set of sets, and so forth, for all finite orders. Let us call *impredicative* a proof possibly using Comprehension axiom of some finite

24th EACSL Annual Conference on Computer Science Logic (CSL 2015).
Editor: Stephan Kreutzer; pp. 343–358
Leibniz International Proceedings in Informatics
LIPICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

order. We prove that any impredicative proof of a statement of the form (1) may avoid the use of Excluded Middle. Often the resulting proof will be intuitionistic but impredicative.

We claim having an effective method for transforming classical proofs into intuitionistic ones, however, we do not claim that this method is feasible in practice. We do not claim we found an optimal proof, either. Our meta-proof that a result is intuitionistically provable uses intuitionistic but impredicative meta-reasoning. We are not yet able to define some simple effective procedure to turn classical proofs of well-foundedness into intuitionistic ones. We tried with Gödel's $\neg\neg$-translation and with Friedman's A-translation [8], but they did not work.

There are results along the same direction. Sieg proved in his ph.d. thesis that whenever ω-iterated inductive definitions prove that a primitive recursive ordinal is well-founded, then the ordinal belongs to some primitive recursive denotation system, which may be proved to be well-founded intuitionistically. An account of his proof may be found in [18].

Here we address a more general case: a classical proof using the Comprehension axioms of all finite orders. The conclusion of the classical proof has the more general form: if R_1, $\ldots$, R_n are inductively well-founded, then R is inductively well-founded, with $R_1, \ldots, R_n, R$ primitive recursive relations over $\mathtt{Nat}$.

Our result may be seen as a generalization of the well-known result of conservativity of classical analysis w.r.t. intuitionistic analysis for Π^0_2-formulas by Kreisel [12]. This conservativity results generalizes to any implications between Π^0_2-formulas (this is an old remark, for a proof see for instance [4]). We extend the conservativity result to all implications among Π^1_1-formulas, provided these formulas may be expressed through the well-foundedness of some primitive recursive relation, and using the inductive definition of well-foundedness. The predicate "being the code of a primitive recursive well-founded relation" is Π^1_1-complete (see for instance [9]). Thus, our result allows to reformulate any classical theorem which is an implication between Π^1_1-formulas by some classically equivalent and intuitionistically provable implication between statements of inductive well-foundedness. The original classical theorem may be not intuitionistically provable.

This is the plan of the paper. In Section 2 we introduce $\mathtt{PA}^\omega$, classical arithmetic with Comprehension of order ω, the formal system we deal with in this paper. In Section 3 we describe the inductive definition of well-founded relation and its basic properties in Intuitionistic Arithmetic. In Section 4 we sketch the proof idea for the conservativity result, and in §5 we prove it. In Section 6 we draw our conclusions and we provide some examples. The acknowledgments are in Paragraph 6.1.

2 The conservativity result and the formal system for Classical Higher Order Arithmetic

Assume $R_1, \ldots, R_n, R$ are some primitive recursive binary relations on $\mathtt{Nat}$. Let us denote with $\mathtt{WF}(R)$ the statement "R is inductively well-founded" (to be defined later). We want to prove: whenever we have a proof of $\mathtt{WF}(R_1), \ldots, \mathtt{WF}(R_n) \implies \mathtt{WF}(R)$ in Classical Peano Arithmetic with Comprehension axiom of order ω, then we may prove $\mathtt{WF}(R_1), \ldots, \mathtt{WF}(R_n) \implies \mathtt{WF}(R)$ in the "Theory of Species" [14]. The "Theory of Species" is a natural deduction with higher order predicate variables, and Comprehension axiom of level ω hidden in the $\forall$-elimination rule. Comprehension of level two (for sets of natural numbers) proves Paris-Harrington Theorem, the Theorem about Goodstein Sequences, Higman Lemma, Kruskal Lemma, which are not provable in first order arithmetic (classical or intuitionistic). Each level of comprehension adds new theorems. In spite of these strong assumptions, the "Theory of Species" is an intuitionistic logic, because it has the disjunctive property and the witness property ([14], p. 231, Section 11.1, 11.2). In fact, it may be considered as *the Intuitionistic Arithmetic with Comprehension axiom of order* ω.

In this paper we are interested in the mere existence of an intuitionistic formal proof, and not in an efficient way of writing of it. We prove our result using intuitionistic but impredicative meta-reasoning. For the moment, we do not have a meta-proof using first order arithmetical reasoning.

We first define a sequent calculus version of the Intuitionistic Theory of Species plus Excluded Middle. We call this system *the Classical Arithmetic with Comprehension axiom of order* ω. Following [13], [16], we use a superscript to denote the level of comprehension, and we call this system $\mathtt{PA}^\omega$. $\mathtt{PA}^\omega$ should not be confused with $\mathtt{PA}_\omega$, the system for first order classical arithmetic having higher order functions and no Comprehension axiom. We do not have higher order functions instead. We do have higher order predicate types: $\mathtt{Nat} \to \mathtt{Prop}$ (the type of sets of natural numbers), $(\mathtt{Nat} \to \mathtt{Prop}) \to \mathtt{Prop}$ (the type of sets of sets of natural numbers), and so forth. Comprehension for second order, third order, ..., arithmetic is the statement $\exists X^{\sigma \to \mathtt{Prop}}.(\forall x^\sigma.X(x) \Leftrightarrow P)$, for $\sigma = \mathtt{Nat}, (\mathtt{Nat} \to \mathtt{Prop}), \ldots$. Comprehension is not an axiom of our sequent calculus $\mathtt{PA}^\omega$, but we will express it through left-introduction rules for universal quantifiers: $\forall X^{\mathtt{Nat}\to\mathtt{Prop}}.A$, $\forall X^{(\mathtt{Nat}\to\mathtt{Prop})\to\mathtt{Prop}}.A$, ... This is analogous to the way Martin-Lof expresses Comprehension axiom through the $\forall$-elimination rule. We choose this formalization of Comprehension in order to use Girard's candidate method for deriving normalization of $\mathtt{PA}^\omega$.

▶ **Definition 1** (The Language of $\mathtt{PA}^\omega$)**.** $\mathtt{PA}^\omega$ is the formal system having:

1. One numeral for each $n \in \mathtt{Nat}$, one symbol for each primitive recursive function, infinitely many variables $x^{\mathtt{Nat}}, y^{\mathtt{Nat}}, z^{\mathtt{Nat}}, \ldots$ of type $\mathtt{Nat}$. All terms we may define from them.
2. *Predicates* types: the type $\mathtt{Prop}$ of formulas, and with σ, τ also $\sigma \to \tau$ and $\mathtt{Nat} \to \tau$. If σ is a predicate type, its degree $\deg(\sigma)$ is inductively defined by $\deg(\mathtt{Nat}) = 1$, $\deg(\mathtt{Prop}) = 2$ and $\deg(\sigma \to \tau) = \max(\deg(\sigma) + 1, \deg(\tau))$.
3. One predicate constant p for each primitive recursive predicate on $\mathtt{Nat}$ of any arity, infinitely many variables $X^\sigma, Y^\sigma, Z^\sigma, \ldots$ for each predicate type σ.
4. All formulas we may define from the atomic formulas $p(t_1, \ldots, t_n), X(t_1, \ldots, t_n)$ using the connective $\to$, and two kinds of $\forall$: quantification over $\mathtt{Nat}$, and for any predicate type σ, quantification over σ.
5. All predicates we may define from formulas by simply typed λ-abstraction.
6. As predicate equality, the smallest equivalence relation including: the β-reduction and the reduction replacing a closed term $t : \mathtt{Nat}$ by the numeral it denotes.
7. Two-sided sequents $\Gamma \vdash \Delta$, for any finite sets of formulas Γ, Δ.

The degree of a type is inductively defined by $\deg(\mathtt{Nat}) = 1$, $\deg(\mathtt{Prop}) = 2$, $\deg(\sigma \to \tau) = \max(1 + \deg(\sigma), \deg(\tau))$. The order of a formula is the maximum degree of the types of its variables: first order formulas have integer variables, second order formulas have integer variables and variables on sets of integers, and so forth. For any predicate type σ, the formula $\exists X^\sigma.A$ is not a primitive formula of the language but it is expressed through its canonical higher order definition: $\forall Z^{\mathtt{Prop}}.(\forall X^\sigma.(A \to Z^{\mathtt{Prop}})) \to Z^{\mathtt{Prop}}$, for $Z^{\mathtt{Prop}}$ not free in A. In the same way we define $A \vee B$ as $\forall Z^{\mathtt{Prop}}.(A \to Z^{\mathtt{Prop}}), (B \to Z^{\mathtt{Prop}}) \to Z^{\mathtt{Prop}}$, and $A \wedge B$ as $\forall Z^{\mathtt{Prop}}.(A, B \to Z^{\mathtt{Prop}}) \to Z^{\mathtt{Prop}}$, for $Z^{\mathtt{Prop}}$ not free in A, B, and $A \Leftrightarrow B$ as $(A \to B) \wedge (B \to A)$. Thus, we may now write Comprehension $\exists X^{\sigma\to\mathtt{Prop}}.(\forall x^\sigma.X(x) \Leftrightarrow P)$ as a defined formula. If $\deg(\sigma) = n$ we say that this formula is Comprehension of order n.

We will identify a numeral with the number it denotes. We often skip the type superscript of a variable, but we always use lower case letters $x, y, z, \ldots$ for natural number variables and upper case letters $X, Y, Z, \ldots$ for predicate variables. We consider any recursively enumerable set of basic arithmetical axioms. Any basic arithmetical axiom should have the form $\alpha_1, \ldots, \alpha_n \vdash \alpha$ or $\beta_1, \ldots, \beta_n \vdash$, with each formula of the form $p(t_1, \ldots, t_n)$ for some primitive recursive p and some terms $t_1, \ldots, t_n$. Basic arithmetical axioms should include $t+1 = u+1 \vdash t = u$ and $0 = t+1 \vdash \emptyset$, all rules making $=$ an equivalence relation, and all definition rules for all primitive recursive maps and relations. Basic arithmetical axioms should be true, and should be closed under substitution and cut. The last clause is required if we want to have full cut-elimination for $\mathtt{PA}^\omega$, otherwise cuts between axioms cannot be eliminated.

Proof rules are those of two-sided sequent calculus, with left-introduction rules for $\forall X^\sigma.A$ expressing comprehension of any finite order.

▶ **Definition 2** (Proofs of $\mathtt{PA}^\omega$)**.** Proof trees of $\mathtt{PA}^\omega$ are exactly the *finite trees* built by the rules below, where Γ, Δ are finite sets of formulas, A, B are formulas, $\alpha_1, \ldots, \alpha_n \vdash \alpha$ and $\beta_1, \ldots, \beta_n \vdash$ are basic arithmetical axioms.

$$\frac{}{\Gamma, \alpha_1, \ldots, \alpha_n \vdash \Delta, \alpha}\ (\mathtt{axiom})$$

$$\frac{}{\Gamma, \beta_1, \ldots, \beta_n \vdash \Delta}\ (\mathtt{axiom})$$

$$\frac{}{\Gamma, A \vdash \Delta, A}\ (\mathtt{id})$$

$$\frac{\Gamma_1 \vdash \Delta_1, A \quad \Gamma_2, A \vdash \Delta_2}{\Gamma_1, \Gamma_2 \vdash \Delta_1, \Delta_2}\ (\mathtt{cut})$$

$$\frac{\Gamma, A \implies B \vdash \Delta, A \quad \Gamma, A \implies B, B \vdash \Delta}{\Gamma, A \implies B \vdash \Delta}\ (\implies_l)$$

$$\frac{\Gamma, A \vdash \Delta, A \implies B, B}{\Gamma \vdash \Delta, A \implies B}\ (\implies_r)$$

$$\frac{\Gamma, \forall x A, A[t/x] \vdash \Delta}{\Gamma, \forall x A \vdash \Delta}\ (\text{First Order } \forall_l)$$

$$\frac{\Gamma \vdash \Delta, \forall x A, A[z/x] \quad (z \notin \mathtt{FV}(\Gamma \vdash \Delta, \forall x A))}{\Gamma \vdash \Delta, \forall x A}\ (\text{First Order } \forall_r)$$

$$\frac{\Gamma, \forall X^\sigma A, A[P/X^\sigma] \vdash \Delta}{\Gamma, \forall X^\sigma A \vdash \Delta}\ (\text{Higher Order } \forall_l)$$

$$\frac{\Gamma \vdash \Delta, \forall X A, A[Z/X] \quad (Z \notin \mathtt{FV}(\Gamma \vdash \Delta, \forall X A))}{\Gamma \vdash \Delta, \forall X A}\ (\text{Higher Order } \forall_r)$$

$$\frac{\Gamma \vdash \Delta, \forall x A, A[0/x] \quad \Gamma, A[z/x] \vdash \Delta, \forall x A, A[z+1/x] \quad (z \notin \mathtt{FV}(\Gamma \vdash \Delta, \forall x A))}{\Gamma \vdash \Delta, \forall x A}\ (\mathtt{ind})$$

We say that a $\forall_l$-rule for a formula $\forall X^\sigma A$ has order n if $\deg(\sigma) = n$. Choose any predicate type σ with $\deg(\sigma) = n$. Then the sequent $\vdash \exists X^{\sigma \to \mathtt{Prop}}.(\forall x^\sigma.X(x) \Leftrightarrow P)$ expresses Comprehension axiom of level n. We claim that there is a proof of this sequent using $\forall_l$-rules of order $\leq n+1$ only. For instance, the rules $\forall_l$ of order ≤ 2 derive Comprehension of order 1, or Comprehension for sets of integers. We call order n Peano Arithmetic, and we denote by $\mathtt{PA}^n$, the system with $\forall_l$ restricted to the order $\leq n$. For instance, First Order Arithmetic $\mathtt{PA}^1$ derives no Comprehension axiom, while Second Order Arithmetic $\mathtt{PA}^2$ only derives Comprehension of order 1 (for sets of natural numbers).

In the identity rule and in the cut rule, formulas are identified up to predicate equality (Def. 1.5). In all rules but $\mathtt{cut}$ the conclusion of the rule is included in each premise (if any).

The relation R we fixed, being a primitive recursive binary predicate, is a symbol of the language of $\mathtt{PA}^\omega$. Let us assume $\mathtt{PA}^n \vdash \mathtt{WF}(R)$. We will intuitionistically prove $\mathtt{WF}(R)$ using Comprehension of order $n+1$.

This is the proof idea. We first define an infinitary semi-formal proof system, then we interpret the finitary proof system in the infinitary one and we use the infinitary system to derive our result.

▶ **Definition 3** (ω-rule)**.** Let $\mathtt{PA}^\omega$ + recursive ω-rule be the semi-formal system obtained from $\mathtt{PA}^\omega$ by:

1. considering only the sequents with *no free number variables*,
2. replacing the rules $\mathtt{ind}$ and $\forall_r$ for $\mathtt{Nat}$ with the recursive ω-rule: derive $\Gamma \vdash \Delta, \forall x^{\mathtt{Nat}}.A$ from a recursively given family of proof-trees, one proof of $\Gamma \vdash \Delta, \forall x A, A[m/x^{\mathtt{Nat}}]$ for each numeral $m \in \mathtt{Nat}$.

We write $\pi : \Gamma \vdash \Delta$ for: π is a well-founded recursive proof-tree with ω-rule of conclusion $\Gamma \vdash \Delta$. Let $n > 0$. $\mathtt{PA}^n$ + recursive ω-rule is $\mathtt{PA}^\omega$ + recursive ω-rule with the $\forall_l$-rules restricted to all orders $\leq n$.

The ω-rule may be represented as follows:

$$\frac{\ldots \quad \Gamma \vdash \Delta, \forall x A, A[m/x] \quad \ldots \quad (\text{for all } m \in \mathtt{Nat})}{\Gamma \vdash \Delta, \forall x A} \ (\omega\text{-rule})$$

Proofs of $\mathtt{PA}^\omega$ + recursive ω-rule are at most countable well-founded recursive trees decorated with the rules of the system. A proof tree is called *normal* if it has no cut rule. It is well-known that there is an effective method for turning any proof of any A in $\mathtt{PA}^n$ into a proof of A in $\mathtt{PA}^n$ + recursive ω-rule. It is also well-known that the system $\mathtt{PA}^n$ + recursive ω-rule has a normalization algorithm, turning any proof-tree of $\Gamma \vdash \Delta$ into a normal proof-tree, and that the proof may be expressed using order $n + 1$ Comprehension.

3 The inductive definition of a well-founded relation

In Intuitionistic Arithmetic, we define well-founded relations through an inductive definition. Let R be any binary relation over a set I. Classically, the usual definition of "R is well-founded" says: "there is no infinite R-decreasing chain", or: "all R-decreasing chains are finite". In Intuitionistic Arithmetic, these statements are not informative enough, and we prefer the inductive definition of well-foundedness, which runs as follows. A predicate X over a set I is called R-inductive if X contains x whenever X contains all y such that yRx. We say that I, R (or just R for short) is inductively well-founded, and we write $\mathtt{WF}(R)$, if all R-inductive properties X are true for all $x \in I$. By definition unfolding, we obtain:

$$\mathtt{WF}(R) = \forall x \in I.\forall X.(\forall y \in I.(\forall z \in I.zRy \implies X(z)) \implies X(y)) \implies X(x)$$

From now on, we will often write "well-founded" as a shorthand for "inductive well-founded". If (I, R) is well-founded, then, in order to prove that $\forall x \in I.P(x)$, it is enough to prove that P is R-inductive. This well-known proof method is called "by induction on x and R". For instance, when R is the successor relation on $\mathtt{Nat}$, we re-obtain induction on $\mathtt{Nat}$. Induction may be nested. In order to prove $P(x)$ we may use induction again, over some set I_x and some relation R_x, possibly depending on $x \in I$. In this case we speak of "secondary induction on $y \in I_x$ and R_x".

Our conservativity proofs deals with the sub-formulas of $\mathtt{WF}(R)$. Now we will list them, just skipping the atomic sub-formulas and the implications of atomic formulas. If we list the sub-formulas of $\mathtt{WF}(R)$ from right to left, the first four sub-formulas we find are atomic, or implications of atomic. The fifth sub-formula, and the first in our list, is: *(1)* $\forall z \in I.zRy \implies X(z)$. Then we find, in this order: *(2)* $(\forall z \in I.zRy \implies X(z)) \implies X(y)$, then *(3)* $\forall y \in I.(\forall z \in I.zRy \implies X(z)) \implies X(y)$, then *(4)* $(\forall y \in I.(\forall z \in I.zRy \implies X(z)) \implies X(y)) \implies X(x)$, then *(5)* $\forall X.(\forall y \in I.(\forall z \in I.zRy \implies X(z)) \implies X(y)) \implies X(x)$, and eventually *(6)* the formula $\mathtt{WF}(R)$ itself. These 6 expressions are cumbersome, therefore we will introduce a name for each of them. There is nothing to understand here: we assign 6 names (including $\mathtt{WF}(R)$ itself) we will use later.

▶ **Definition 4** (Formal definition of (inductive) well-foundedness)**.** Let R be any binary relation over a set I and $X : I \to \mathtt{Prop}$ any variable of unary predicate over I.

1. $\mathtt{IH}(y, X) = \forall z \in I.(zRy \implies X(z))$ *(R-inductive hypothesis in y for X)*
2. $\mathtt{Ind}(y, X) = (\mathtt{IH}(y, X) \implies X(y))$ *(X is R-inductive in y)*
3. $\mathtt{IND}(X) = \forall y \in I.\mathtt{Ind}(y, X)$ *(X is R-inductive)*
4. $\mathtt{wf}(x, X) = (\mathtt{IND}(X) \implies X(x))$ *(x is R-well-founded w.r.t. X)*
5. $\mathtt{Wf}(x) = \forall X.\mathtt{wf}(x, X)$ *(x is R-well-founded)*
6. $\mathtt{WF}(R) = \forall x \in I.\mathtt{Wf}(x)$ *((I, R) is well-founded)*

We abbreviate "(I, R) is well-founded" by "R is well-founded" when I is clear from the context. The predicates defined in the points $1 - 5$ above, to be accurate, should be written with an extra argument R. We skipped R because it is fixed and would clutter our formulas uselessly. We left the argument X, even if X is fixed, as a memo for the name of the variable X denoting a generic unary predicate on I in the formula $\mathtt{WF}(R)$.

ω-rule is complete w.r.t. the statements of the form $\mathtt{WF}(R)$.We may state this fact as follows. Recall that $\pi : \Gamma \vdash \Delta$ denotes that π is a well-founded recursive proof-tree of conclusion $\Gamma \vdash \Delta$.

▶ **Lemma 5** (ω-rule is complete for $\mathtt{WF}(R)$)**.** *There is some recursive family of trees indexed over binary primitive recursive relations over* $\mathtt{Nat}$*, of the form* $\{\pi_R | R$ *bin.prim.rec.*$\}$*, such that:*

$$\mathtt{WF}(R) \implies \pi_R : \mathtt{WF}(R)$$

This fact is provable in Second Order Intuitionistic Arithmetic.

Classically and using choice, the inductive definition of $\mathtt{WF}(R)$ is equivalent to the classical formulation which says "all descending R-chains are finite". This equivalence is not provable in Higher Order Intuitionistic Arithmetic.

A method for proving well-foundedness is the simulation of a relation into another well-founded relation. Informally, we may simulate $x \in I$ by $y \in J$ using a relation $\sim$ if, by moving from I to J using $\sim$, we may simulate R-chains through S-chains. Our method is an intuitionistic and simplified version of the method used for proving that a labeled state transition systems strongly terminates [15], if we take as set of labels of a transition a singleton.

▶ **Definition 6** (Simulation)**.** Assume R is a binary relation over a set I and S is a binary relation over a set J. Assume $\sim \subseteq I \times J$.

1. $\sim$ is a simulation of (I, R) into (J, S) if whenever $x{\sim}y$ and $x'Rx$ then for some $y' \in J$ we have $y'Sy$ and $x'{\sim}y'$.
2. $\sim$ is a bisimulation if both $\sim$ and $\sim^{-1}$ are simulations.
3. $\sim$ is a weak simulation of (I, R) into (J, S) if whenever $x{\sim}y$ and $x'Rx$ then for some $y' \in J$ we have: $y'Sy$ and either $x{\sim}y'$ or $x'{\sim}y'$.

In the rest of the paper we will use some well-known definitions and facts about well-founded relations and simulations.

We first state the Kleene-Brouwer Theorem. We denote by $\sigma{*}\tau$ the concatenation of two finite sequences σ, τ, and with $\sigma@n = \sigma{*}\langle n \rangle$ the appending of an element to a list. We denote the one-step extension relation on finite sequences by $\prec_1$, and we define it by $\sigma@n{\prec_1}\sigma$. We denote by $\prec$ the strict prefix relation, and we define it by $\sigma{*}\langle n \rangle{*}\tau{\prec}\sigma$. We denote by

$\prec\!\!\!\prec$ the post-order, a total order over the finite sequences over `Nat`. $\prec\!\!\!\prec$ is defined as follows: $\sigma@n{*}\tau \prec\!\!\!\prec \sigma$, and if $n' < n$ then $\sigma@n'{*}\tau \prec\!\!\!\prec \sigma@n{*}\rho$. Then the Kleene-Brouwer Theorem may be stated as follows: "if $(T, \prec_1)$ is a well-founded tree of finite sequences over `Nat`, then $(T, \prec\!\!\!\prec)$ is well-founded".

The main property of simulations we need to prove is: if $y \in J$ simulates some $x \in I$ and y is S-well-founded, then x is R-well-founded. Recall that "well-founded" is short for "inductively well-founded" here.

All these results have an intuitionistic proof, included in the next Lemma.

▶ **Lemma 7.** *Properties of well-founded relations] Assume T is any tree of finite sequences over some set K, with x child of y if and only if $x \prec_1 y$. Assume I, J are any sets, and R, S are any binary relations, respectively, on I and on J.*

1. **(a)** *Well-foundedness is an inductive predicate: for any $x \in I$ we have* $\forall y.(yRx \implies y \text{ is } R\text{-well-founded }) \implies x \text{ is } R\text{-well-founded}$
   (b) *The converse holds: for any $x \in I$ we have* $x \text{ is } R\text{-well-founded } \implies \forall y.(yRx \implies y \text{ is } R\text{-well-founded })$
2. **(a)** *A tree is well-founded if and only if all proper descendants of the root of the tree are well-founded.*
   (b) *A tree is well-founded if and only if its root is.*
3. *Assume $\sim$ is a simulation relation from I, R to J, S. If $x \sim y$ and $y \in J$ is S-well-founded, then $x \in I$ is R-well-founded.*
4. Kleene-Brouwer Theorem. *If $(T, \prec_1)$ is a tree of sequences over `Nat`, and $(T, \prec_1)$ is well-founded, then $(T, \prec\!\!\!\prec)$ is well-founded.*
5. *A relation R is well-founded if and only if the tree of all R-decreasing sequences is well-founded. $x \in I$ is R-well-founded if and only if the tree of all R-decreasing sequences from x is well-founded.*
6. *Assume $\sim$ is a weak simulation relation from a set I with a relation R to a set J with a relation S. If (J, S) is well-founded and S is transitive then $\sim$ is a simulation.*

Proof.

1. **(a)** *Well-foundedness is inductive.* Assume $\forall y.(yRx \implies y$ is R-well-founded), in order to prove that x is R-well-founded, that is, that for any inductive predicate X we have $x \in X$. Since X is inductive, then our thesis follows by proving $\forall z.(zRx \implies z \in X)$. In order to prove it, let z be such that zRx. Then by hypothesis z is R-well-founded, hence, by the assumption that X is inductive, we have $z \in X$, as we wished to show.
   (b) Assume (x is R-well-founded), in order to prove $\forall y.(yRx \implies y$ is R-well-founded), that is, that for any inductive predicate X and any $y \in I$ we have $y \in X$. If X is inductive, then we may prove by definition unfolding that $Y = \{x \in I | X(x) \land \forall y.(yRx) \implies y \in X\}$ is inductive. Then $x \in Y$ by R-well-foundation of x, and by definition of Y we have $\forall y.(yRx) \implies y \in X$, as wished.
2. **(a)** Assume T is a tree and all proper descendants of the root of T are $\prec_1$-well-founded. We have to prove that all nodes of T are $\prec_1$-well-founded: we only have to prove that the root is well-founded. All children of the root are $\prec_1$-well-founded by assumption, therefore the root is $\prec_1$-well-founded by point 1.*a* above.
   (b) Assume that the root of T is $\prec_1$-well-founded. Then all nodes of T, being reachable from the root, are $\prec_1$-well-founded by point 1.*b* above.
3. Assume J, S is well-founded and $x \sim y$ and y is S-well-founded in order to prove that x is R-well-founded. We prove that all $x \sim y$ are R-well-founded by induction on $y \in J$. By point 1, it is enough to prove that all zRx are R-well-founded. By definition of simulation

there is some $t \in J$ such that $z{\sim}t$ and tSy. By induction hypothesis on t we conclude that z is R-well-founded, as we wished to show.

4. *Kleene-Brouwer Theorem.* Assume that $(T, \prec_1)$ is well-founded and T is a tree of sequences over $\mathtt{Nat}$. For any $\sigma \in T$, denote with T_σ the set $\{\tau | \sigma{*}\tau \in T\}$. We prove that T_σ, $\lessdot\!\!\lessdot$ is well-founded by $\prec_1$-induction on σ. The thesis will follow by choosing $\sigma = \langle\rangle$: in this case we have $T_\sigma = T$. Assume that $(T_{\sigma'}, \lessdot\!\!\lessdot)$ is well-founded for all $\sigma' \prec_1 \sigma$, in order to prove that T_σ, $\lessdot\!\!\lessdot$ is well-founded. All $\sigma' \prec_1 \sigma$ have the form $\sigma@n$ for some $n \in \mathtt{Nat}$. All $\tau \in T_\sigma$ but the root $\langle\rangle$ are $\langle n\rangle{*}\rho$ for some $n \in \mathtt{Nat}$ and some $\rho \in T_{\sigma@n}$. Define $J = \{(n, \rho) | n \in \mathtt{Nat} \wedge \rho \in T_{\sigma@n}\}$. Let $(n', \rho')S(n, \rho)$ if and only if $n' < n$ or $n' = n$ and $\rho' \lessdot\!\!\lessdot \rho$. Then J is well-founded: the proof is by principal induction on n, $<$ and secondary induction on $\rho \in T_{\sigma@n}$, $\lessdot\!\!\lessdot$. For all $\tau \in T_\sigma$, we define a relation $\tau{\sim}(n, \rho)$ if and only if $\tau = \langle n\rangle{*}\rho$. $\sim$ is a simulation of T_σ, $\lessdot\!\!\lessdot$ in J, S. Indeed, if $\tau' \lessdot\!\!\lessdot \tau$ and $\tau{\sim}(n, \rho)$ then $\tau' = \langle n'\rangle{*}\rho'$. By definition of $\lessdot\!\!\lessdot$, either $n' < n$ or $n' = n$ and $\rho' \lessdot\!\!\lessdot \rho$. In both cases by definition of $\sim$ and S we have: $\tau'{\sim}(n', \rho')$ and $(n', \tau')S(n, \tau)$. Thus, by point 3 above τ is $\prec_1$-well-founded, for all $\tau = \langle n\rangle{*}\rho$, that is, for all $\tau \in T_\sigma$ different from the root $\langle\rangle$. By point 2 we conclude that T_σ is well-founded.

5. Assume T is the tree of all R-decreasing sequences on I (all $\langle x_1, \ldots, x_n\rangle$ such that $x_n R x_{n-1} R \ldots R x_1$). We may define a simulation $\sim$ of (I, R) into $(T, \prec_1)$ by $x \sim \langle x_1, \ldots, x_n\rangle$ if and only if $n > 0$ and $x = x_n$. $\sim$ is a bisimulation. Indeed, assume that $x{\sim}\langle x_1, \ldots, x_n\rangle$, that is, $n > 0$ and $x = x_n$. If yRx then $\langle x_1, \ldots, x_n, y\rangle$ is R-decreasing and $y{\sim}\langle x_1, \ldots, x_n, y\rangle$. Conversely, if $\langle x_1, \ldots, x_n, y\rangle$ is R-decreasing then $yRx_n = x$. For all $x \in I$ we have $\langle x\rangle \in T$ and $x{\sim}\langle x\rangle$. Thus, if T is $\prec_1$-well-founded then all $x \in I$ are R-well-founded by point 3. If R is well-founded then all sequences in T with one or more points are well-founded by 3, therefore $(T, \prec_1)$ is well-founded by point 2 above.
Assume T_x is the tree of all R-decreasing sequences $\langle x_1, \ldots, x_n\rangle$ on I such that $n > 0$ and $x_n = x$. Define $\sim'$ by restricting $\sim$ to the set of all pairs $(y, \langle x_1, \ldots, x_n\rangle)$ such that $\langle x_1, \ldots, x_n\rangle \in T_x$ (that is, such that $n > 0$ and $x_n = x$ and $x_1 = x$). Then a reasoning similar to the previous one shows that $\sim'$ is a bisimulation, therefore x is R-well-founded if and only if $\langle x\rangle$ is well-founded in T_x. By point 2, since $\langle x\rangle$ is the root of T_x, this is equivalent to the fact that T_x is well-founded.

6. Assume $\sim$ is a weak simulation relation from a set I with a relation R to a set J with a relation S. Assume $x{\sim}y$ and zRx in order to prove that for some tSy we have $z{\sim}t$. We argue by induction on y w.r.t. S. By definition of weak simulation, for some tSy we have either $x{\sim}t$ or $z{\sim}t$. In the second case we have the thesis. In the first case by induction hypothesis on t there is some uSt such that $z{\sim}u$. By transitivity of S and uSt, tSy we have uSy: we conclude our thesis. ◀

4 The proof idea for the conservativity result

Assume π is a proof of $\mathtt{PA}^\omega$ or of $\mathtt{PA}^\omega$ + recursive ω-rule. Recall that we write $\pi : \Gamma \vdash \Delta$ for "π has conclusion $\Gamma \vdash \Delta$", and that a proof is cut-free if it includes no cut rule. We consider the notion of sub-formula in which the sub-formulas of $\forall x.A$ (quantification over $\mathtt{Nat}$) are all $A[n/x]$ with $n \in \mathtt{Nat}$. A proofs of $\mathtt{PA}^\omega$ + recursive ω-rule satisfies the sub-formula property if all formulas in any sequent of the proof are a sub-formula of some formula in the conclusion and they occur in the left-hand-side if they are negative sub-formulas, in the right-hand-side if they are positive sub-formulas.

Let $R, R_1, \ldots, R_n$ be primitive recursive binary predicates on $\mathtt{Nat}$. We assume $\mathtt{PA}^\omega \vdash \mathtt{WF}(R)$ in order to intuitionistically derive $\mathtt{WF}(R)$. Then we will generalize the result to a statement of the form $\mathtt{WF}(R_1), \ldots, \mathtt{WF}(R_n) \implies \mathtt{WF}(R)$. We first recall some well-known intuitionistic results about $\mathtt{PA}^n$ and $\mathtt{PA}^n$ + recursive ω-rule.

Our first step is to prove that if $\mathtt{PA}^n \vdash \mathtt{WF}(R)$, then $\mathtt{PA}^n$ + recursive ω-rule $\vdash \mathtt{WF}(R)$ with some normal proof.

▶ **Lemma 8** (Embedding and Normalization). *Let $\Gamma \vdash \Delta$ be a sequent and π be a proof of $\mathtt{PA}^\omega$. Assume σ be any substitution of the first order free variables of $\Gamma \vdash \Delta$ with numerals.*

1. *There is a recursive map f taking any proof $\pi : \Gamma \vdash \Delta$ in $\mathtt{PA}^\omega$, any first order substitution σ, and returning a proof $\Pi = f(\pi, \sigma) : \sigma(\Gamma \vdash \Delta)$ in $\mathtt{PA}^\omega$ + recursive ω-rule.*
2. *Let $n > 0$. There is a recursive map g, taking any infinitary proof-tree $\pi : \Gamma \vdash \Delta$ in $\mathtt{PA}^n$ + recursive ω-rule, and returning some cut-free proof $\Pi = g(\pi) : \Gamma \vdash \Delta$ in the same system. This fact has an intuitionistic proof using Comprehension of order $n + 1$.*
3. *Any normal proof of $\mathtt{PA}^\omega$ + recursive ω-rule satisfies the sub-formula property.*

Proof.

1. We recursively define a map f taking any proof $\pi : \Gamma \vdash \Delta$ in $\mathtt{PA}^\omega$, any first order substitution σ, and returning a proof $f(\pi, \sigma) : \sigma(\Gamma \vdash \Delta)$ in $\mathtt{PA}^\omega$ + recursive ω-rule. The proof follows the pattern of the analogous result for $\mathtt{PA}^1$ obtained by Tait ([17], p. 277, Thm. 28.9). Any rule of $\mathtt{PA}^\omega$, different from the rule $\forall_r$ for `Nat` and from the rule `ind`, is translated in $\mathtt{PA}^\omega$ + recursive ω-rule by the rule itself . There are two cases left.
   - **a.** Assume π ends with some $\forall_r$-rule, whose unique assumption is $\pi_1 : \Gamma \vdash \Delta, \forall x A, A[z/x]$ in $\mathtt{PA}^\omega$, for some $z \notin \mathtt{FV}(\Gamma \vdash \Delta, \forall x.A)$. Let $\sigma[n/z]$ be any extension of the substitution σ to z with some numeral n. By assumption z is not free in $\Gamma, \Delta, \forall x A$, hence z may occur free in A only if $z = x$. σ is a closed substitution, therefore z occurs in no $\sigma(y)$. Thus, $\sigma[n/z](\Gamma \vdash \Delta, \forall x A) = \sigma(\Gamma \vdash \Delta, \forall x A)$ and $\sigma[n/z](A[z/x]) = \sigma(A[z/x][n/z]) = \sigma(A[n/x]) = \sigma(A)[n/x]$. Then by induction hypothesis we have $f(\pi_1, \sigma[n/z]) : \sigma[n/z](\Gamma \vdash \Delta, \forall x A, A[z/x]) = \sigma(\Gamma \vdash \Delta, \forall x A, A[n/x])$. Eventually, we define some proof $f(\pi, \sigma) : \sigma(\Gamma \vdash \Delta, \forall x.A)$ by recursive ω-rule.
   - **b.** Assume π ends with some `ind`-rule, whose assumptions are $\pi_1 : \Gamma \vdash \Delta, \forall x A, A[0/x]$ and $\pi_2 : \Gamma, A[z/x] \vdash \Delta, \forall x A, A[z + 1/x]$ in $\mathtt{PA}^\omega$, for some $z \notin \mathtt{FV}(\Gamma \vdash \Delta, \forall x.A)$. Let $\sigma[n/z]$ be any extension of the substitution σ to z with some numeral n. With the same reasoning we did on z in the previous case we obtain $\sigma[n/z](A[0/x]) = \sigma(A)[0/x]$ and $\sigma[n/z](A[z/x]) = \sigma(A)[n/x]$ and $\sigma[n/z](A[z + 1/x]) = \sigma(A)[n + 1/x]$. Then by induction hypothesis we have $f(\pi_1, \sigma[n/z]) : \sigma[n/z](\Gamma \vdash \Delta, \forall x A, A[0/x]) = \sigma(\Gamma \vdash \Delta, \forall x A, A[0/x])$ and $f(\pi_2, \sigma[n/z]) : \sigma[n/z](\Gamma, A[z/x] \vdash \Delta, \forall x A, A[z + 1/x]) = \sigma(\Gamma, A[n/x] \vdash \Delta, \forall x A, A[n + 1/x])$. We inductively define a recursive family $\Pi_n : \sigma(\Gamma \vdash \Delta, \forall x A, A[n/x])$ of proofs indexed by $n \in \mathtt{Nat}$ by $\Pi_0 = f(\pi_1, \sigma[n/z]) : \sigma(\Gamma \vdash \Delta, \forall x A, A[0/x])$ and Π_{n+1} = the cut of $\Pi_n : \sigma(\Gamma \vdash \Delta, \forall x A, A[n/x])$ and $f(\pi_2, \sigma[n/z]) : \sigma(\Gamma, A[n/x] \vdash \Delta, \forall x A, A[n + 1/x])$. Eventually, we define $f(\pi, \sigma) : \sigma(\Gamma \vdash \Delta, \forall x.A)$ by recursive ω-rule from $\{\Pi_n | n \in \mathtt{Nat}\}$.
2. (Proof Sketch). Using Girard's candidates, adapted to the sequent calculus. T. Altenkirch formalized Girard's candidates in LEGO using an inductive definition over second order formulas and third order quantifiers ([1], p.109). His idea may be easily generalized: defining Girard's candidates for $\mathtt{PA}^n$ + ω-rule requires Comprehension of order $n + 1$. We need Comprehension of order 3 for defining Girard's candidates for $\mathtt{PA}^2$, and so forth. We postpone the details to a journal version of this paper.
3. By induction over the normal proof. ◀

In order to derive $\mathtt{WF}(R)$, now it is enough to prove that for a normal proof π of $\mathtt{WF}(R)$ in $\mathtt{PA}^\omega$ + recursive ω-rule there is simulation relation $\sim$ between the R-decreasing sequences with the one-step extension relation, and the proof-tree π itself, with the post-order relation $\lll$. By Lemma 7.6, even a weak simulation relation is enough. Then our conservativity result will follow by Lemma 7.3. The proof is intuitionistic because Lemma 7 is.

5 Simulating a primitive recursive relation into a normal infinitary proof of its well-foundedness

In this section we will define a simulation relation $\sim$ between the tree of decreasing R-sequences and π, $\lll$, a normal proof-tree with ω-rule of the statement $\mathtt{WF}(R)$, with the post-order relation.

Let R be the relation we fixed, $I = \mathtt{Nat}$, $x, y \in I$. Assume X is any unary predicate variable. Assume that π is a normal proof in $\mathtt{PA}^\omega$ + recursive ω-rule of $\vdash \mathtt{WF}(R)$.

By the sub-formula property for normal proofs (Lemma 8.3), for any sequent $\Gamma \vdash \Delta$ occurring in π, all $A \in \Gamma$ are negative sub-formulas of $\mathtt{WF}(R)$, and all $B \in \Delta$ are positive sub-formulas of $\mathtt{WF}(R)$. We refer to Def. 4 for the names we assigned to the sub-formulas of $\mathtt{WF}(R)$. The immediate sub-formulas of $\mathtt{WF}(R) = \forall x.\mathtt{Wf}(x)$ are $\mathtt{Wf}(n)$ for all $n \in \mathtt{Nat}$ (positive). The immediate sub-formula of $\mathtt{Wf}(n) = \forall X.\mathtt{wf}(n, X)$ is $\mathtt{wf}(n, X)$ (positive). The sub-formulas of $\mathtt{wf}(n, X) = (\mathtt{IND}(X) \implies X(n))$ are: $X(n)$ (positive) $\mathtt{IND}(X) = \forall y.\mathtt{Ind}(y, X)$ (negative), for all $m \in \mathtt{Nat}$, $\mathtt{Ind}(m, X) = (\mathtt{IH}(m, X) \implies X(m))$ (negative), $X(m)$ (negative), $\mathtt{IH}(m, X) = \forall z.(zRm \implies X(z))$ (positive), for all $p \in \mathtt{Nat}$, $(pRm \implies X(p)$ (positive), $X(p)$ (positive), pRm (negative). All sub-formulas of $\mathtt{WF}(R)$ but those of the form $X(m)$ for some m have a unique sign. Summing up, we just proved:

▶ **Lemma 9** (Sequents in π). *Every formula F in every sequent $\Gamma \vdash \Delta$ in any normal proof π of $\vdash \mathtt{WF}(R)$ in $\mathtt{PA}^\omega$ + recursive ω-rule falls in at least one of the following cases, for some $n, m, p \in \mathtt{Nat}$:*

1. $F = \mathtt{WF}(R) = \forall x.\mathtt{Wf}(x) \in \Delta$
2. $F = \mathtt{Wf}(n) = \forall X.\mathtt{wf}(n, X) \in \Delta$
3. $F = \mathtt{wf}(n, X) = (\mathtt{IND}(X) \implies X(n)) \in \Delta$
4. $F = \mathtt{IND}(X) = \forall y.\mathtt{Ind}(y, X) \in \Gamma$
5. $F = \mathtt{Ind}(m, X) = (\mathtt{IH}(m, X) \implies X(m)) \in \Gamma$
6. *1.* $F = X(m) \in \Gamma$
   2. $F = X(m) \in \Delta$
3. $F = \mathtt{IH}(m, X) = \forall z.(zRm \implies X(z)) \in \Delta$
4. $F = ((pRm) \implies X(p)) \in \Delta$
5. $F = (pRm) \in \Gamma$

We apply the post-order relation $\lll$ to the proof-tree π, taking the same order among the premises of a rule we have in the proof (this order is fixed in Def. 2).

Let us denote with T the tree of R-decreasing sequences on $\mathtt{Nat}$. We will define a weak simulation relation of $(T, \prec_1)$ in $(\pi, \lll)$, relating any node of T with some node in π. From the well-foundedness of π, $\lll$ (Lemma 7.4) and the fact that $\lll$ is transitive we will deduce that $\sim$ is a simulation (Lemma 7.6), therefore any node of T is well-founded (Lemma 7.3). We will conclude that T is well-founded, and R itself is well-founded (Lemma 7.5).

If ν is any node of π, we write $\nu : \Gamma \vdash \Delta$ for "the sub-proof of π of root ν has conclusion $\Gamma \vdash \Delta$". Let $\sigma = a_k R a_{k-1} R \ldots R a_2 R a_1 \in T$ be any R-decreasing chain. We define a relation $\sigma \sim \nu$ between R-sequences and nodes of π.

Informally, $\sigma \sim \nu : \Gamma \vdash \Delta$ says that Δ is a property of the nodes $a_k, \ldots, a_1$ of the R-decreasing sequence σ, and in all formulas $aRb \in \Gamma$ and $aRb \implies X(a) \in \Delta$, the element a is the successor of b in σ. The precise definition follows.

▶ **Definition 10** (The relation $\sim$). Let T be the tree of R-decreasing sequences and $\sigma = a_k R a_{k-1} R \ldots R a_2 R a_1 \in T$ be any R-decreasing chain, with possibly $k = 0$. Let $\pi : \vdash \mathtt{WF}(R)$ be a normal proof in $\mathtt{PA}^\omega + \omega$-rule. We say that σ is simulated by a node $\nu : \Gamma \vdash \Delta$ in π, and we write $\sigma \sim \nu$, if:

1. every numeral m occurring in Δ is a_i for some $i = 1, \ldots, k$
2. every (closed) formula $(pRm) \in \Gamma$ and $(pRm) \implies X(p) \in \Delta$ is, respectively, $(a_{i+1} R a_i)$, $(a_{i+1} R a_i) \implies X(a_{i+1})$ for some $i = 1, \ldots, k-1$

ν is a node of π, therefore Lemma 9 lists all formulas which may occur in the conclusion $\Gamma \vdash \Delta$ of ν. Using Lemma 9 we may reformulate the definition of $\sim$ in the following equivalent form.

▶ **Lemma 11** (An alternative definition of $\sim$). *$\sigma \sim \nu : \Gamma \vdash \Delta$ if and only if every formula $F \in \Gamma \vdash \Delta$ falls in at least one of the following cases:*

1. $F = \mathtt{WF}(R) = \forall x.\mathtt{Wf}(x) \in \Delta$
2. $F = \mathtt{Wf}(a_i) = \forall X.\mathtt{wf}(a_i, X) \in \Delta$, *for some* $a_i \in \sigma$
3. $F = \mathtt{wf}(a_i, X) = (\mathtt{IND}(X) \implies X(a_i)) \in \Delta$, *for some* $a_i \in \sigma$
4. $F = \mathtt{IND}(X) \in \Gamma$
5. $F = \mathtt{Ind}(m, X) \in \Gamma$ *for some* $m \in \mathtt{Nat}$
6. *1.* $F = X(m) \in \Gamma$ *for some* $m \in \mathtt{Nat}$
   2. $F = X(a_i) \in \Delta$ *for some* $a_i \in \sigma$.
3. $F = \mathtt{IH}(a_i, X) \in \Delta$ *for some* $a_i \in \sigma$.
4. $F = ((a_{i+1} R a_i) \implies X(a_{i+1})) \in \Delta$ *for some* $a_i, a_{i+1} \in \sigma$.
5. $F = (a_{i+1} R a_i) \in \Gamma$ *for some* $a_i, a_{i+1} \in \sigma$.

The relation $\sim$ is closed under ancestor: if $\sigma \sim \nu$ and $\nu \prec \mu$ then $\sigma \sim \mu$. The reason is that all rules $\neq$ `cut` of $\mathtt{PA}^\omega$ + recursive ω-rule are contravariant w.r.t. the descendant relation $\prec$: if $\nu : \Gamma \vdash \Delta$, $\nu' : \Gamma' \vdash \Delta'$ and $\nu \prec \nu'$ then $\Gamma \vdash \Delta \supseteq \Gamma' \vdash \Delta'$, therefore $\nu' : \Gamma' \vdash \Delta'$ satisfies the clauses for σ if $\nu : \Gamma \vdash \Delta$ satisfies the clauses for σ.

The relation $\sim$ is total: for every $\sigma \in T$ there is some $\nu \in \pi$ such that $\sigma \sim \nu$. *Proof.* Let μ_0 be the root of π. Then we have $\mu_0 : \vdash \mathtt{WF}(R)$. Every F in $\vdash \mathtt{WF}(R)$ satisfies $F = \mathtt{WF}(R) \in \Delta$. By Lemma 11 we have $\sigma \sim \mu_0$ for every $\sigma \in T$.

We recall that $(\tau \prec_1 \sigma)$ means that τ is of the form $a_{k+1} R a_k R \ldots R a_1$, that is, that τ is a generic one-step extension of σ. We write $\mu \prec_1 \nu$ for "μ is a child of ν in π", too. We first prove that $\sim$ is a weak simulation, then that $\sim$ is a simulation.

▶ **Lemma 12** (Weak simulation). *Let T be the tree of R-decreasing sequences, $\pi : \vdash \mathtt{WF}(R)$ a normal proof in $\mathtt{PA}^\omega + \omega$-rule, and $\sim$ as in Def. 10. Then $\sim$ is a weak simulation between $(T, \prec_1)$ and $(\pi, \prec\!\!\prec)$.*

Proof. Assume $\sigma = a_k R a_{k-1} R \ldots R a_1$ and $\tau = a_{k+1} R a_k R \ldots R a_1 \prec_1 \sigma$ and $\sigma \sim \nu$. We have to prove that there is some $\mu \prec_1 \nu$ in π such that $\sigma \sim \mu$, or $\tau \sim \mu$. There are 9 classes of formulas $\in \Gamma \vdash \Delta$. We distinguish 9 cases according to the formula inferred in ν.

1. $\mathtt{WF}(R)$. We infer $\mathtt{WF}(R) \in \Delta$ from all $\mathtt{Wf}(p) \in \Delta$ with $p \in \mathtt{Nat}$, using the ω-rule with one premise $\mu_p \prec_1 \nu$ for each p. We choose $p = a_{k+1}$, the node added in τ. The extra formula $\mathtt{Wf}(a_{k+1})$ we have in the right-hand-side of the premise μ_p satisfies the clause 2 of Lemma 11 for τ, therefore $\tau \sim \mu_p$.
2. $\mathtt{Wf}(a_i)$. We infer $\mathtt{Wf}(a_i) \in \Delta$ from some $\mathtt{wf}(a_i, X) \in \Delta$ using the rule $\forall_r$ with a single premise $\mu \prec_1 \nu$. The extra formula $\mathtt{wf}(a_i, X)$ we have in the right-hand-side of the premise satisfies the clause 3 of Lemma 11 for σ, therefore $\sigma \sim \mu$.

3. $\mathtt{wf}(a_i, X)$ for some $a_i \in \sigma$. We infer $\mathtt{wf}(a_i, X) = (\mathtt{IND}(X) \implies X(a_i)) \in \Delta$ from some $\mathtt{IND}(X)$ and some $X(a_i)$ in the left- and right-hand-side using the rule $\implies_r$ with a single premise $\mu \prec_1 \nu$. The extra formulas $\mathtt{IND}(X) \in \Gamma$ and $X(a_i) \in \Delta$ we have in the premise satisfy the clauses 4, 5 of Lemma 11, therefore $\sigma \sim \mu$.
4. $\mathtt{IND}(X)$. We infer $\mathtt{IND}(X) \in \Gamma$ from some $\mathtt{Ind}(m, X) \in \Gamma$ using the rule $\forall_l$ with a single premise $\mu \prec_1 \nu$. The extra formula $\mathtt{Ind}(m, X)$ we have in the left-hand-side of the premise satisfies the clause 5 of Lemma 11, therefore $\sigma \sim \mu$.
5. $\mathtt{Ind}(m, X)$. We infer $\mathtt{Ind}(m, X) = (\mathtt{IH}(m, X) \implies X(m)) \in \Gamma$ using the rule $\implies_l$ from two premises: a left premise μ having $\mathtt{IH}(m, X)$ added to Δ, and a right premise μ' having $X(m)$ added to Γ, for some $\mu \prec_1 \mu' \prec_1 \nu$. The formula $X(m)$ added to Γ satisfies the clause 6a of Lemma 11, therefore $\sigma \sim \mu' \prec_1 \nu$.
6. $X(m)$. Using the Identity rule, we infer the same formula $X(m) \in \Gamma$ and $X(m) \in \Delta$, for some $m \in \mathtt{Nat}$. From $X(m) \in \Delta$ we get $m = a_i$ for some $i = 1, \ldots, k$ by the clause 6b of Lemma 11. $X(a_i)$ does not belong to the left-hand-side of the root of π, therefore we may find the last node $\nu \prec \mu$ in the path from ν to the root of π such that $X(a_i)$ belongs to the left-hand-side of the conclusion of μ. The only formula in π which we may prove from some $X(a_i)$ in the left-hand-side is a left occurrence of $\mathtt{Ind}(a_i, X) = (\mathtt{IH}(a_i, X) \implies X(a_i))$. Therefore there is some node η having μ as right premise, in which we introduce by $\implies_l$ some $\mathtt{Ind}(a_i, X) = (\mathtt{IH}(a_i, X) \implies X(a_i))$. The left premise of η is some node θ in which $\mathtt{IH}(a_i, X)$ occurs in the right-hand-side and it is used by $\implies_l$ to derive $\mathtt{Ind}(a_i, X)$. We sum up the situation in the proof tree below.

$$\dfrac{\theta : \Gamma'', \mathtt{Ind}(a_i, X) \vdash \mathtt{IH}(a_i, X), \Delta'' \qquad \dfrac{\dfrac{}{\nu : \Gamma', X(a_i) \vdash X(a_i), \Delta'}\ \mathtt{id}}{\mu : \Gamma'', \mathtt{Ind}(a_i, X), X(a_i) \vdash \Delta''}\,\vdots}{\eta : \Gamma'', \mathtt{Ind}(a_i, X) \vdash \Delta''}\ \implies_l$$

We have $\sigma \sim \eta$ because η is an ancestor of ν. $\mathtt{IH}(a_i, X)$ satisfies the clause 7 of Lemma 11, therefore $\sigma \sim \theta$. We have $\theta \lll \nu$ because θ is the left premise and μ the right premise of η, and μ is an ancestor of ν.
7. $\mathtt{IH}(a_i, X)$. For some $i = 0, \ldots, k$, we infer $\mathtt{IH}(a_i, X) \in \Delta$ using the recursive ω-rule. For every $p \in \mathtt{Nat}$, there is some assumption μ_p of ν adding to Δ the formula $F_p = (pRa_i \implies X(p))$. In post-order we have $\mu_0 \lll \mu_1 \lll \mu_2 \lll \ldots \lll \nu$. We distinguish two sub-cases according to $i < k$ or $i = k$.

   a. Let $i < k$. Then $i + 1 \leq k$, therefore $(a_{i+1} R a_i \implies X(a_{i+1}))$ has the form required by clause 8 of Lemma 11 for σ. If we choose $p = a_{i+1}$, we conclude $\sigma \sim \mu_p$, for some $\mu_p \prec_1 \nu$.
   b. Let $i = k$. Then a_{k+1} is the last element of τ. The formula $(a_{k+1} R a_k) \implies X(a_{k+1})$ has the form required by clause 8 of Lemma 11 for τ. If we choose $p = a_{i+1}$, we conclude $\tau \sim \mu_p$ for some $\mu_p \prec_1 \nu$.

8. $(a_{i+1} R a_i \implies X(a_i), \implies_r)$. We infer some formula $a_{i+1} R a_i \implies X(a_{i+1}) \in \Delta$ using the rule $\implies_r$, from one premise μ having $(a_{i+1} R a_i)$ in the left-hand-side and $X(a_i)$ in the right-hand-side. The first formula satisfies the clause 9 of Lemma 11, the second one the clause 6b of the same Lemma. We conclude $\sigma \sim \mu \prec_1 \nu$.
9. *One or more formulas aRb.* We infer some atomic formulas using the rule $\mathtt{axiom}$ and one basic arithmetical axiom $\alpha_1, \ldots, \alpha_n \vdash \alpha$ or $\beta_1, \ldots, \beta_n \vdash$, with all α_i, α of the form $p(t_1, \ldots, t_m)$ for some $p, t_1, \ldots, t_m$. All atomic formulas $p(t_1, \ldots, t_m)$ in π have the form

$a_{i+1}Ra_i$, are closed, are true by assumption on σ, and are in the left-hand side. Thus, the basic arithmetical axiom has the form $\alpha_1, \ldots, \alpha_n \vdash$, with all α_i closed and true. *This case cannot happen*, because `axiom` may infer a closed sequence $\alpha_1, \ldots, \alpha_n \vdash$ only if it is true, hence if some α_i is false. ◀

We have now all the ingredients we need to intuitionistically derive our conservativity result.

▶ **Lemma 13** (well-foundedness of R). *Assume R is any primitive recursive binary relation on* `Nat`*, and $(T, \prec_1)$ is the tree of R-decreasing sequences with the child/father relation. Let $\pi : \mathtt{WF}(R)$ be any proof of $\mathtt{WF}(R)$ in $\mathtt{PA}^\omega$, and $\Pi = gf(\pi) : \mathtt{WF}(R)$ be the normal proof of $\mathtt{WF}(R)$ in $\mathtt{PA}^\omega +$ recursive ω-rule, obtained by 8.1, 2. Let $\sim$ be the simulation relation defined above, and $\lll$ the post-order ordering on Π.*

1. *Π with $\lll$ is well-founded.*
2. *$\sim$ is a simulation relation of $(T, \prec_1)$ in Π, $\lll$.*
3. *$(T, \prec_1)$ is well founded*
4. *R is well founded.*

Proof.

1. By the Kleene-Brouwer Theorem (Lemma 7.4) and the hypothesis that Π, $\prec_1$ is well-founded.
2. By Lemma 7.6, the fact that $\sim$ is a weak simulation (Lemma 12), and that $(\Pi, \lll)$ is well-founded (point 1).
3. By point 2 above, $\sim$ is a simulation. By point 1, the root of Π is $\lll$-well-founded. Any node of T is related to the root of Π by $\sim$, hence by Lemma 7.3, any node of T is $\prec_1$-well-founded. We conclude that $(T, \prec_1)$ is well-founded.
4. R is well founded by Lemma 7.5, because $(T, \prec_1)$ is well-founded by point 3. ◀

Eventually, we conclude:

▶ **Theorem 14** (Conservativity). *Assume $R, R_1, \ldots, R_n$ are any binary primitive recursive relation over* `Nat` *and $n > 0$.*

1. *If $\mathtt{PA}^n \vdash \mathtt{WF}(R_1), \ldots, \mathtt{WF}(R_n) \implies \mathtt{WF}(R)$, then using Comprehension of order $n + 1$we may intuitionistically derive $\mathtt{WF}(R_1), \ldots, \mathtt{WF}(R_n) \implies \mathtt{WF}(R)$.*
2. *If $\mathtt{PA}^\omega \vdash \mathtt{WF}(R_1), \ldots, \mathtt{WF}(R_n) \implies \mathtt{WF}(R)$, then using Comprehension of order ω we may intuitionistically derive $\mathtt{WF}(R_1), \ldots, \mathtt{WF}(R_n) \implies \mathtt{WF}(R)$.*

Proof.

1. Assume $\mathtt{WF}(R_1)$, $\ldots$, $\mathtt{WF}(R_n)$ and $\mathtt{PA}^n \vdash \mathtt{WF}(R_1), \ldots, \mathtt{WF}(R_n) \implies \mathtt{WF}(R)$, in order to deduce $\mathtt{WF}(R)$. By Lemma 5 we have $\mathtt{PA}^n \vdash \mathtt{WF}(R_1)$ and … and $\mathtt{PA}^n \vdash \mathtt{WF}(R_n)$. By cut rule we deduce $\mathtt{PA}^n \vdash \mathtt{WF}(R)$. By Lemma 13.4 we conclude $\mathtt{WF}(R)$. The proof is intuitionistic because all proofs in this paper are intuitionistic. The proof may be obtained using comprehension of order $n + 1$ because this is the case for normalization for $\mathtt{PA}^n + \omega$-rule.
2. By the previous point. ◀

6 Conclusions

The aim of this work is to isolate classes $\mathcal{C}$ of formulas such that all proofs of formulas in $\mathcal{C}$ may be turned into intuitionistic proofs, at least in principle. The idea is that, if we care about proving a mathematical result having a concrete meaning, and we have a theorem which is classically but not intuitionistically provable, then we should reformulate our goal in order to obtain one formula in one of these classes. Then we may prove our result freely using classical logic, knowing that, afterward, our proof may always be made intuitionistic. The advantage is that it is much easier to restrict ourselves to a goal in a class $\mathcal{C}$ of formulas, instead than to the use of intuitionistic logic in the proof of the goal. Intuitionistic proofs provide extra information, but if we choose to prove a statement in $\mathcal{C}$, then we know that the intuitionistic proof may always be done as a second step. As a first step we check whether the statement is classically true, a much easier task.

The very first example for $\mathcal{C}$ was provided by K. Gödel. In this case, $\mathcal{C}$ is the set of formulas obtained inserting a double negation ($\neg\neg$) everywhere. However, this class $\mathcal{C}$ has mainly an interest from a foundational viewpoint, because in intuitionistic logic the proof of a negation provides no concrete information.

A second example for $\mathcal{C}$ is the set of formulas provided by the Dialectica interpretation. In this case we have formulas whose intuitionistic proofs are rich of concrete consequences. Indeed, these formulas are successfully used by U. Kohlenbach [11] and others to analyze, say, proofs of fixed point results for non-expansive maps. A drawback of this class, however, lies in the complexity of these formulas, which are long, involved, and use functionals of higher types. Often, formulas in $\mathcal{C}$ require a real effort to be understood.

Another choice for $\mathcal{C}$ is the set of Π^0_2-sentences, those of the form $\forall x \in \mathtt{Nat}.\exists y \in \mathtt{Nat}.R(x, y)$, for any primitive recursive binary relation R on $\mathtt{Nat}$. The conservativity result for this class was proved by G. Kreisel [12]. Later, H. Friedman provided A-translation, the first realistic and purely mechanical method for turning a classical proof of a Π^0_2-formula into an intuitionistic one of the same formula [8]. An intuitionistic proof of a Π^0_2-formula is not a mere existence result, but it outlines a method for computing y given x. The only limitation is that this class is very narrow: in a proof of a Π^0_2-formula we often use as lemmas some statements which are much more complex in the arithmetical hierarchy. We would like intuitionistically provable versions for lemmas, too.

One way to overcome this limitation is to generalize A-translation to a larger class of first order formulas. Berger, Buchholz and Schwichtenberg [4] proved, for instance, that we may take as $\mathcal{C}$ the set of all sequents $\Gamma \vdash A$ with A some Π^0_2-formula and Γ containing only formulas $\forall x_1, \ldots, x_n.(\alpha_1, \ldots, \alpha_m \implies \alpha)$, with α and all α_i atomic and different from the constant $\perp$ (false). There are more results along this line [4] .

However, there are Π^0_2-theorems requiring more than first order formulas. For instance, Paris-Harrington theorem, the Theorem about Goodstein sequences, Higman Lemma and Kruskal Lemma are Π^0_2-theorems whose proof requires second order formulas. Therefore it makes sense to look for a choice of $\mathcal{C}$ including some second order formulas.

In this paper we considered a choice of this kind, all statements of the form: "if $\mathtt{WF}(R_1)$, $\ldots$, $\mathtt{WF}(R_n)$ then $\mathtt{WF}(R)$", where $\mathtt{WF}(S)$ means: "S is inductively well-founded", again for any primitive recursive binary relations S on $\mathtt{Nat}$.

6.1 Some corollaries of the conservativity result

The conservativity results holds for statements of the form: "$\mathtt{WF}(R_1), \ldots, \mathtt{WF}(R_n) \implies \mathtt{WF}(R)$". The relevance of this class relies on the empirical evidence that many mathematical results, if expressed in this form, are rich of concrete and interesting intuitionistic consequences.

For instance, *Higman's Lemma* may be expressed in the form $\mathtt{WF}(R)$ for some primitive recursive R, as follows. Let us denote with $\mathtt{List}(I)$ the set of finite lists over some set I. For any $L, M \in \mathtt{List}(I)$, we write $L \sqsubseteq M$ if L may be obtained from M by possibly skipping some elements of M. Let T be the set of $\langle L_1, \ldots, L_n \rangle \in \mathtt{List}(\mathtt{List}(\mathtt{Nat}))$ such that for all $0 < i < j < n$ we have $L_i \not\sqsubseteq L_j$. Then Higman Lemma may be expressed by saying that the set T is well-founded by one-step extension (see [5], [7]). A similar remark applies to Kruskal's Lemma. More in general, the theory of Almost Full Relations, the intuitionistic version of Quasi-Well-Orders, may be developed using theorems of the form $\mathtt{WF}(R_1), \ldots, \mathtt{WF}(R_n) \implies \mathtt{WF}(R)$ ([20]).

Another example is *Ramsey's Theorem*. Let $G \subseteq \mathtt{Nat}$ be any primitive recursive complete graph and $c : G \times G \to \{1, \ldots, n\}$ be any primitive recursive n-color assignment . Define, for $i = 1, \ldots, n$, T_i as the set of all finite increasing lists $\langle x_1, \ldots, x_n \rangle$ over $\mathtt{Nat}$, such that for all $0 < j < k < n$ we have $x_j, x_k \in G$ and $c(x_j, x_k) = i$. Define T as the set of all finite increasing lists $\langle x_1, \ldots, x_n \rangle$ over $\mathtt{Nat}$, such that for all $0 < j < k < n$ we have $x_j, x_k \in G$. Then we may express Ramsey theorem by saying: if $T_1, \ldots, T_n$ are well-founded then T is well-founded. Indeed, by definition unfolding, this implication means: if, for $i = 1, \ldots, n$, the tree of finite i-colored sub-graph of G is well-founded by one-point extension, then the tree of all finite sub-graphs of G is well-founded by one-step extension. This latter is just a way of saying: G itself is finite. We recognize this statement as a variant of the contrapositive of Ramsey. By Theorem 14 this statement has an intuitionistic proof, whenever G, c are primitive recursive. In fact, this variant of Ramsey theorem has an intuitionistic proof for *any* G, c ([3]), but Theorem 14 cannot prove it.

Besides, an intuitionistic proof of "R is inductively well-founded" is not just a proof of: "there is some bound to the ordinal height of R", it effectively provides such a bound. This extra information about ordinals has been used, for instance, to characterize the programs proved terminating by the Termination algorithm [2].

It is worth to quote that the statements of the form $\mathtt{WF}(R)$ are used to develop formal topology ([6]).

Acknowledgments. We thank F. Aschieri, U. Berger, T. Coquand, P. Martin-Löf and P. Oliva for the fruitful suggestions about an earlier version of this paper.

References

1. T. Altenkirch. *Constructions, Inductive Types and Strong Normalization.* PhD thesis, University of Edinburgh, 1993.
2. Stefano Berardi, Paulo Oliva, and Silvia Steila. Proving termination of programs having transition invariants of height ω. In *Proceedings of the 15th Italian Conference on Theoretical Computer Science, Perugia, Italy, September 17-19, 2014.*, pages 237–240, 2014.
3. Stefano Berardi and Silvia Steila. Ramsey theorem as an intuitionistic property of well founded relations. In *Rewriting and Typed Lambda Calculi – Joint International Conference, RTA-TLCA 2014, Held as Part of the Vienna Summer of Logic, VSL 2014, Vienna, Austria, July 14-17, 2014. Proceedings*, pages 93–107, 2014.
4. Ulrich Berger, Wilfried Buchholz, and Helmut Schwichtenberg. Refined program extraction form classical proofs. *Ann. Pure Appl. Logic*, 114(1-3):3–25, 2002.
5. T. Coquand and D. Fridlender. A proof of higman's lemma by structural induction. unpublished draft.
6. Thierry Coquand, Giovanni Sambin, Jan M. Smith, and Silvio Valentini. Inductively generated formal topologies. *Ann. Pure Appl. Logic*, 124(1-3):71–106, 2003.
7. D. Fridlender. *Higman's lemma in Type Theory.* PhD thesis, Chalmers University, 1997.
8. H. Friedman. Classically and intuitionistically provably recursive functions. *Lecture Notes in Mathematics*, 669:21–27, 1978.
9. J.-Y. Girard. *Proof theory and logical complexity.* Studies in Proof Theory. Monographs, 1. Bibliopolis, 1987.

10 William A. Howard and Georg Kreisel. Transfinite induction and bar induction of types zero and one, and the role of continuity in intuitionistic analysis. *J. Symb. Log.*, 31(3):325–358, 1966.

11 U. Kohlenbach. *Applied Proof Theory: Proof Interpretation and their Use in Mathematics*. Springer-Verlag Berlin Heidelberg, 2008.

12 Georg Kreisel. On the interpretation of non-finitist proofs: Part II. interpretation of number theory. applications. *J. Symb. Log.*, 17(1):43–58, 1952.

13 P. Martin-Lof. Hauptsatz for the intuitionistic theory of iterated inductive definitions. In *Proceedings of the Second Scandinavian Logic Symposium, Oslo*, pages 179–216, 1971.

14 P. Martin-Lof. Hauptsatz for the theory of species. In *Proceedings of the Second Scandinavian Logic Symposium, Oslo*, pages 217–233, 1971.

15 David Michael Ritchie Park. Concurrency and automata on infinite sequences. In *Theoretical Computer Science, 5th GI-Conference, Karlsruhe, Germany, March 23-25, 1981, Proceedings*, pages 167–183, 1981.

16 D. Prawitz. Ideas and results in proof theory. In *Proceedings of the Second Scandinavian Logic Symposium, Oslo*, pages 235–307, 1971.

17 K. Schutte. *Proof Theory.* Springer-Verlag, Berlin Heildelberg New York, 1977.

18 W. Sieg, W. Buchholz, S. Feferman, and W. Pohlers. *Iterated Inductive Definitions and Subsystems of Analysis – Recent Proof Theoretical Studies*, volume 897. Springer Lecture Notes in Mathematics (LNM) Berlin-Heidelberg-New York, 1981.

19 Jean van Heijenoort. *From Frege to Gödel, A Source Book in Mathematical Logic, 1879-1931.* Harward University Press, 2002.

20 Dimitrios Vytiniotis, Thierry Coquand, and David Wahlstedt. Stop when you are almost-full – adventures in constructive termination. In *Interactive Theorem Proving – Third International Conference, ITP 2012, Princeton, NJ, USA, August 13-15, 2012. Proceedings*, pages 250–265, 2012.