Realizability with Stateful Computations for Nonstandard Analysis

Bruno Dinis
Faculdade de Ciências, University of Lisbon, Portugal
bmdinis@fc.ul.pt

Étienne Miquey
ÉNS de Lyon, Université de Lyon, LIP, France
etienne.miquey@ens-lyon.fr

Abstract

In this paper we propose a new approach to realizability interpretations for nonstandard arithmetic. We deal with nonstandard analysis in the context of intuitionistic realizability, focusing on the Lightstone-Robinson construction of a model for nonstandard analysis through an ultrapower. In particular, we consider an extension of the λ-calculus with a memory cell, that contains an integer (the state), in order to indicate in which slice of the ultrapower $\mathcal{M}^{\mathbb{N}}$ the computation is being done. We shall pay attention to the nonstandard principles (and their computational content) obtainable in this setting. We then discuss how this product could be quotiented to mimic the Lightstone-Robinson construction.

2012 ACM Subject Classification Theory of computation → Proof theory; Theory of computation → Constructive mathematics

Keywords and phrases realizability, nonstandard analysis, states, glueing, ultrafilters, Łoś' theorem

Digital Object Identifier 10.4230/LIPIcs.CSL.2021.19

Funding *Bruno Dinis*: The author acknowledges the support of FCT - Fundação para a Ciência e Tecnologia under the projects UIDB/04561/2020 and UIDP/04561/2020, and the research center Centro de Matemática, Aplicações Fundamentais e Investigação Operacional, Universidade de Lisboa.
Étienne Miquey: The author was supported by the Paris Ile-de-France Region and the Inria research team Deducteam (LSV, ÉNS Paris-Saclay).

Acknowledgements The authors would like to thank Alexandre Miquel for suggesting several ideas at the root of this work and Valentin Blot and Mikhail Katz, as well as the anonymous reviewers, for their accurate remarks and suggestions.

1 Introduction

In this paper we propose a new approach to realizability interpretations for nonstandard arithmetic. On the one hand, we deal with nonstandard analysis in the context of intuitionistic realizability. On the other hand, we focus on Lightstone and Robinson's construction of a model for nonstandard analysis through an ultrapower [23].

Throughout the history of mathematics, infinitesimals were crucial for the intuitive development of mathematical knowledge by authors such as Archimedes, Stevin, Fermat, Leibniz, Euler and Cauchy, to name but a few (see e.g. [15, 4, 3]). In particular, in Leibniz's Calculus one may recognize calculation rules – sometimes called the *Leibniz rules* [24, 7, 10] – which correspond to heuristic intuitions for how the infinitesimals should operate under calculations: the sum and product of infinitesimals is infinitesimal, the product of a limited number (i.e. not infinitely large) with an infinitesimal is infinitesimal, ...

© Bruno Dinis and Étienne Miquey;
licensed under Creative Commons License CC-BY

In [35, 36] Robinson showed that, in the setting of model theory, it is possible to extend usual mathematical sets ($\mathbb{N}$, $\mathbb{R}$, etc.) witnessing the existence of new elements, the so-called *nonstandard* individuals. In this way, it is possible to deal consistently with infinitesimal and infinitely large numbers via ultraproducts and ultrapowers, in a way that is consistent with the Leibniz rules. Since the extended structures are nonstandard models of the original structures, this new setting was dubbed *nonstandard analysis*.

These constructions are meant to simplify doing mathematics: notions like limits or continuity can for instance be given a simpler form in nonstandard analysis. Later in the 70s, Nelson developed a syntactical approach to nonstandard analysis, introducing in particular three key principles: idealization, standardization and transfer [31]. The validity of these principles for constructive mathematics has been studied in many different settings, in particular, following some pioneer work by Moerdijk, Palmgren and Avigad [29, 30, 2] in nonstandard intuitionistic arithmetic, several recent works, inspired by Nelson's approach, lead to interpretations of nonstandard theories in intuitionistic realizability models [6, 8, 13, 9].

The very first ideas of *realizability* are to be found in the Brouwer-Heyting-Kolmogorov interpretation [14, 17], which identifies evidences and computing proofs (the realizers). Realizability was designed by Kleene to interpret the computational content of the proofs of Heyting arithmetic [16], and was later extended to more expressive frameworks [11, 18, 20]. While the Curry-Howard isomorphism focuses on a syntactical correspondence between proofs and programs, realizability rather deals with the (operational) semantics of programs: a *realizer* of a formula A is a program which *computes* adequately with the specification that A provides. As such, realizability constitutes a technique to develop new models of a wide class of theories (from Heyting arithmetic to Zermelo-Fraenkel set theory), whose algebraic structures has been studied in [38, 22, 27].

With the development of his classical realizability, Krivine evidences the fact that extending the λ-calculus with new programming instructions may result in getting new reasoning principles: `call/cc` to get classical logic [12, 20], `quote` for dependent choice [19], etc. In this paper, we follow this path to show how the addition of a monotonic reference allows us to get a realizability interpretation for nonstandard analysis. The realizability interpretation proposed here can be understood as a computational interpretation of the ultraproduct construction in [23], where the value of the reference indicates the slice of the product in which the computation takes place. In particular, we obtain a realizer for the idealization principle whose computational behaviour increases the reference in the manner of a diagonalization process.

Outline

We start this paper by recalling the main ideas of the ultraproduct construction (Section 2) and the definition of a standard realizability interpretation for second-order Heyting arithmetic (Section 3). We then introduce stateful computations and our notion of realizability with slices in Section 4. As shown in Section 5, this interpretation provides us with realizers for several nonstandard reasoning principles. Finally, we discuss the possibility of taking a quotient for this interpretation in Section 6.1 and we conclude the paper in Section 6.2 with a comparison to related works and questions left for future work.

N.B.: due to the page limit, proofs sketches are given in the appendices.

2 The ultrapower construction

The main contribution of this paper consists in defining a realizability interpretation to give a computational content to the ultrapower construction of Robinson and Lightstone in [23]. We shall begin by briefly explaining how this construction works in the realm of model theory.

First, recall that an *ultrafilter* over a set I is a filter $\mathcal{U} \subseteq \mathcal{P}(I)$ such that for any $F \in \mathcal{P}(I)$, either F or its complement $\overline{F}$ are in $\mathcal{U}$. For instance, the set of cofinite subsets of $\mathbb{N}$ defines the so-called *Fréchet filter*, which is not an ultrafilter since it contains neither the set of even natural numbers nor the set of odd natural numbers. Nonetheless, it is well-known that any filter $\mathcal{F}$ over an infinite set I is contained in an ultrafilter $\mathcal{U}$ over I: this is the so-called *ultrafilter principle*. An ultrafilter that contains the Fréchet filter is called a *free ultrafilter*. The existence of free ultrafilters was proved by Tarski in 1930 [37] and is in fact a consequence of the axiom of choice.

Given two sets V and I and an ultrafilter $\mathcal{U}$ over I, we can define an equivalence relation $\cong_{\mathcal{U}}$ over V^I by $u \cong_{\mathcal{U}} v \triangleq \{i \in I : u_i = v_i\} \in \mathcal{U}$. We write $V^I/\mathcal{U}$ for the set obtained by performing a quotient on the set V^I by this equivalence relation, which is called an *ultrapower*.

Consider a theory $\mathcal{T}$ (say ZFC) and its language $\mathcal{L}$, for which we assume the existence of a model $\mathcal{M}$. The goal is to build a nonstandard model $\mathcal{M}^*$ of the theory $\mathcal{T}$ that validates new principles. Let us denote by $\mathcal{V}$ the set which interprets individuals in $\mathcal{M}$, and let us fix a free ultrafilter $\mathcal{U}$ over $\mathbb{N}$. Roughly speaking, the new model $\mathcal{M}^*$ is defined as the ultrapower $\mathcal{M}^{\mathbb{N}}/\mathcal{U}$. Individuals are interpreted by functions in $\mathcal{V}^{\mathbb{N}}$ while the validity of a relation $R(x_1, ..., x_k)$ (where the x_i are interpreted by f_i, for $i \in \{1, ..., k\}$) is defined by

$$\mathcal{M}^* \vDash R(f_1, ..., f_k) \qquad \text{iff} \qquad \{n \in \mathbb{N} : \mathcal{M} \vDash R(f_1(n), ..., f_k(n))\} \in \mathcal{U}.$$

We can now extend the language with a new predicate $\mathrm{st}(x)$ to express that x is *standard*. Standard elements are defined as the ones that, with respect to $\cong_{\mathcal{U}}$, are equivalent to constant functions, i.e. $\mathcal{M}^* \vDash \mathrm{st}(f)$ if and only if there exists $p \in \mathbb{N}$ such that $\{n \in \mathbb{N} : f(n) = p\} \in \mathcal{U}$. Formulas that involve this new predicate are called *external*, while formulas of the original language $\mathcal{L}$ are called *internal*.

Lightstone and Robinson's construction relies on the well-known Łoś' theorem [33] which states that if φ is an internal formula (with parameters in $\mathcal{V}^{\mathbb{N}}$), then $\mathcal{M}^* \vDash \varphi$ if and only $\{n \in \mathbb{N} : \mathcal{M} \vDash \overline{\varphi}^n\} \in \mathcal{U}$, where $\overline{\varphi}^n$ refers to the formula φ whose parameters have been replaced by their values in n. This construction indeed defines a model of $\mathcal{T}$ which satisfies other relevant properties, namely transfer, idealization and standardization. As a consequence of Łoś' theorem, to see that an internal formula $\varphi(x)$ holds for all elements, it is enough to see that it holds for all standard elements: this is the *transfer* principle. In our setting, *idealization* amounts to a diagonalization process: it is for instance easy to see that if one defines $\delta : n \mapsto n$ (where we, with abuse of notation, write n for both the natural number n and its interpretation in $\mathcal{V}$), then $\mathcal{M}^* \vDash \forall x.(\mathrm{st}(x) \to x < \delta)$. Finally, *standardization* is a sort of "comprehension scheme" which states that we can specify subsets of standard sets by giving a membership criterion for standard elements (by means of an internal formula).

3 Realizability in a nutshell

3.1 Heyting second-order arithmetic

We start by introducing the terms and formulas of Heyting second-order arithmetic (HA2), for which we follow Miquel's presentation [25]. Second-order formulas are build on top of first-order arithmetical expressions, by means of logical connectives, first- and second-order quantifications and primitive predicates. We use upper case letters for second-order variables and lower case for first-order ones. We use a primitive predicate $\mathrm{Nat}(e)$ to denote that e is a natural number (0 then has type $\mathrm{Nat}(0)$ and the term $\mathsf{s}\,t$ has type $\mathrm{Nat}(S(e))$ provided that t has type $\mathrm{Nat}(e)$). We consider the usual λ-calculus terms extended with pairs, projections (written π_i), injections (written ι_i), case analysis, natural numbers and a recursion operator:

$$\begin{array}{lrcl}
\textbf{1st-order expressions} & e & ::= & x \mid 0 \mid S(e) \mid f(e_1,\dots,e_n) \\
\textbf{Formulas} & A, B & ::= & \mathrm{Nat}(e) \mid X(e_1,\dots,e_n) \mid A \to B \mid A \wedge B \mid A \vee B \\
 & & & \mid \forall x.A \mid \exists x.A \mid \forall X.A \mid \exists X.A \\
\textbf{Terms} & t, u & ::= & x \mid 0 \mid \mathsf{s} \mid \mathsf{rec} \mid \lambda x.t \mid t\,u \mid (t,u) \mid \pi_1(t) \mid \pi_2(t) \\
 & & & \mid \iota_1(t) \mid \iota_2(t) \mid \mathsf{case}\; t\,\{\iota_1(x_1) \mapsto t_1 | \iota_2(x_2) \mapsto t_2\}
\end{array}$$

where $f : \mathbb{N}^n \to \mathbb{N}$ is any arithmetical function. We write Λ for the set of all closed λ-terms.

As in Miquel's presentation, we consider formulas up to the following congruences:

$$(\exists x.A) \to B \cong \forall x.(A \to B) \qquad\qquad (\exists X.A) \to B \cong \forall X.(A \to B) \tag{1}$$

These congruences allow us to avoid having elimination rules for the existential quantifiers, thus simplifying the resulting type system. The type system, which is given in Figure 1, corresponds to the usual rules of natural deduction. The reader may observe that we do not give computational content to quantifications.

In the sequel, we make use of the following usual abbreviations:

$$\begin{array}{rcl|rcl|rcl}
\mathsf{s}^{n+1}0 & \triangleq & \mathsf{s}\,(\mathsf{s}^n 0) & \top & \triangleq & \exists X.X & e = e' & \triangleq & \forall Z.(Z(e) \to Z(e')) \\
\overline{n} & \triangleq & \mathsf{s}^n 0 & \bot & \triangleq & \forall X.X & \forall^{\mathbb{N}} x.A & \triangleq & \forall x.(\mathrm{Nat}(x) \to A) \\
 & & & \neg A & \triangleq & A \to \bot & \exists^{\mathbb{N}} x.A & \triangleq & \exists x.(\mathrm{Nat}(x) \wedge A)
\end{array}$$

It is well-known that the above definition of equality (often called *Leibniz law*) enjoys the usual expected properties (reflexivity, symmetry, transitivity) and allows to perform substitution of equal terms. The quantifications $\forall^{\mathbb{N}} x.A$ and $\exists^{\mathbb{N}} x.A$ are often said to be *relativized* to natural numbers.

The one-step (weak) reduction over terms is defined by the following rules:

$$\frac{}{(\lambda x.t)u \rhd_\beta t[u/x]} \qquad \frac{}{\mathsf{rec}\; u_0\, u_1\, 0 \rhd_\beta u_0} \qquad \frac{}{\mathsf{rec}\; u_0\, u_1\, (\mathsf{s}\, t) \rhd_\beta u_1\, t\, (\mathsf{rec}\; u_0\, u_1\, t)}$$

$$\frac{}{\pi_1(t,u) \rhd_\beta t} \qquad \frac{}{\pi_2(t,u) \rhd_\beta u} \qquad \frac{}{\mathsf{case}\; \iota_i(t)\, \{\iota_1(x_1) \mapsto t_1 | \iota_2(x_2) \mapsto t_2\} \rhd_\beta t_i[t/x_i]}$$

We write $\to_\beta$ for the congruent reflexive-transitive closure of $\rhd_\beta$. The reduction $\to_\beta$ is known to be confluent, type-preserving and normalizing on typed terms [5].

3.2 Realizability interpretation of HA2

In this subsection we define the realizability interpretation of the type system defined in Figure 1, in which formulas are interpreted as *saturated sets* of terms, i.e. as sets of closed terms $S \subseteq \Lambda$ such that $t \to_\beta t'$ and $t' \in S$ imply that $t \in S$. We write $\mathbf{SAT}$ to denote the set of all saturated sets and, given a formula A, we call *truth value* its realizability interpretation.

▶ **Definition 1** (Valuation). A valuation *is a function ρ that associates a natural number $\rho(x)$ to every first-order variable x and a* truth value function *$\rho(X)$, i.e. a function in $\mathbb{N}^k \to \mathbf{SAT}$ to every second-order variable X of arity k.*

1. *Given a valuation ρ, a first-order variable x and a natural number n, we denote by $\rho, x \mapsto n$ the valuation defined by $(\rho, x \mapsto n) \triangleq \rho_{|\,\mathrm{dom}(\rho)\setminus\{x\}} \cup \{x \mapsto n\}$.*

$$\frac{}{\Gamma \vdash 0 : \mathrm{Nat}(0)}\ (0) \qquad \frac{}{\Gamma \vdash \mathsf{s} : \forall^{\mathbb{N}} x.\mathrm{Nat}(S(x))}\ (S)$$

$$\frac{}{\Gamma \vdash \mathsf{rec} : \forall Z.Z(0) \to (\forall^{\mathbb{N}} y.(Z(y) \to Z(S(y)))) \to \forall^{\mathbb{N}} x.Z(x)}\ (\mathrm{rec}) \qquad \frac{(x : A) \in \Gamma}{\Gamma \vdash x : A}\ (\mathrm{Ax})$$

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x\,.\,t : A \to B}\ (\to_I) \qquad \frac{\Gamma \vdash t : A \to B \qquad \Gamma \vdash u : A}{\Gamma \vdash t\,u : B}\ (\to_E) \qquad \frac{\Gamma \vdash t : A \quad \Gamma \vdash u : B}{\Gamma \vdash (t, u) : A \wedge B}\ (\wedge_I)$$

$$\frac{\Gamma \vdash t : A \wedge B}{\Gamma \vdash \pi_1(t) : A}\ (\wedge_E^1) \qquad \frac{\Gamma \vdash t : A \wedge B}{\Gamma \vdash \pi_2(t) : B}\ (\wedge_E^2) \qquad \frac{\Gamma \vdash t : A}{\Gamma \vdash \iota_1(t) : A \vee B}\ (\vee_I^1) \qquad \frac{\Gamma \vdash t : B}{\Gamma \vdash \iota_2(t) : A \vee B}\ (\vee_I^2)$$

$$\frac{\Gamma \vdash t : A_1 \vee A_2 \quad \Gamma, x_i : A_i \vdash t_i : C}{\Gamma \vdash \mathsf{case}\ t\, \{\iota_1(x_1) \mapsto t_1 | \iota_2(x_2) \mapsto t_2\} : C}\ (\vee_E) \qquad \frac{\Gamma \vdash t : A[x := n]}{\Gamma \vdash t : \exists x.A}\ (\exists_I^1) \qquad \frac{\Gamma \vdash t : \forall x.A}{\Gamma \vdash t : A[x := n]}\ (\forall_E^1)$$

$$\frac{\Gamma \vdash t : A \quad x \notin FV(\Gamma)}{\Gamma \vdash t : \forall x.A}\ (\forall_I^1) \qquad \frac{\Gamma \vdash t : A[X(x_1, \ldots, x_n) := B]}{\Gamma \vdash t : \exists X.A}\ (\exists_I^2)$$

$$\frac{\Gamma \vdash t : \forall X.A}{\Gamma \vdash t : A[X(x_1, \ldots, x_n) := B]}\ (\forall_E^2) \qquad \frac{\Gamma \vdash t : A \quad X \notin FV(\Gamma)}{\Gamma \vdash t : \forall X.A}\ (\forall_I^2) \qquad \frac{\Gamma \vdash t : A' \quad A \cong A'}{\Gamma \vdash t : A}\ (\cong)$$

Figure 1 Type system.

2. *Given a valuation ρ, a second-order variable X of arity k and a truth value function $F : \mathbb{N}^k \to \mathbf{SAT}$, the valuation defined by $(\rho, X \mapsto F) \triangleq \rho_{|\,\mathrm{dom}(\rho) \setminus \{X\}} \cup \{X \mapsto F\}$ will be denoted by $\rho, X \mapsto F$.*

We say that a valuation ρ is closing *the formula A if $FV(A) \subseteq \mathrm{dom}(\rho)$.*

▶ **Definition 2** (Realizability interpretation). *We interpret closed arithmetical expressions e in the standard model of first-order Peano arithmetic $\mathbb{N}$. Given a valuation ρ and a first-order expression e (whose variables are in the domain of ρ) we denote its interpretation by $[\![e]\!]_\rho$. The interpretation of a formula A together with a valuation ρ closing A is the set $|A|_\rho$ defined inductively according to the following clauses:*

$$\begin{array}{rcl}
|\mathrm{Nat}(e)|_\rho & \triangleq & \{t \in \Lambda : t \to_\beta \mathsf{s}^n 0,\ \textit{where}\ n = [\![e]\!]_\rho\} \\
|X(e_1, \ldots, e_n)|_\rho & \triangleq & \rho(X)([\![e_1]\!]_\rho, \ldots, [\![e_n]\!]_\rho) \\
|A \to B|_\rho & \triangleq & \{t \in \Lambda : \forall u \in |A|_\rho.(t\,u \in |B|_\rho)\} \\
|A_1 \wedge A_2|_\rho & \triangleq & \{t \in \Lambda : \pi_1(t) \in |A_1|_\rho \wedge \pi_2(t) \in |A_2|_\rho\} \\
|A_1 \vee A_2|_\rho & \triangleq & \{t \in \Lambda : \exists i \in \{1, 2\}.\, \mathsf{case}\ t\, \{\iota_1(x_1) \mapsto x_1 | \iota_2(x_2) \mapsto x_2\} \in |A_i|_\rho\} \\
|\forall x.A|_\rho & \triangleq & \bigcap_{n \in \mathbb{N}} |A|_{\rho, x \mapsto n} \qquad\qquad |\forall X.A|_\rho \ \triangleq\ \bigcap_{F : \mathbb{N}^k \to \mathbf{SAT}} |A|_{\rho, X \mapsto F} \\
|\exists x.A|_\rho & \triangleq & \bigcup_{n \in \mathbb{N}} |A|_{\rho, x \mapsto n} \qquad\qquad |\exists X.A|_\rho \ \triangleq\ \bigcup_{F : \mathbb{N}^k \to \mathbf{SAT}} |A|_{\rho, X \mapsto F}
\end{array}$$

Observe that in the previous definition, the universal quantifications cannot be seen as generalized conjunctions. Indeed, the conjunction is given computational content through pairs, while the universal quantifications are defined as intersections of truth values.

It is easy to see that for any formula A and any valuation ρ closing A, one has $|A|_\rho \in \mathbf{SAT}$. As it turns out, the congruences defined by Equation (1) are sound w.r.t. the interpretation.

▶ **Proposition 3** ([25]). *If A and A' are two formulas of HA2 such that $A \cong A'$, then for all valuations ρ closing both A and A' we have $|A|_\rho = |A'|_\rho$.*

In order to show that the realizability interpretation is adequate with respect to the type system we need the following preliminary notions.

▶ **Definition 4** (Substitution). *A* substitution *is a finite function σ from λ-variables to closed λ-terms. Given a substitution σ, a λ-variable x and a closed λ-term u, we denote by $(\sigma, x := u)$ the substitution defined by $(\sigma, x := u) \triangleq \sigma_{|\operatorname{dom}(\sigma)\setminus\{x\}} \cup \{x := u\}$.*

▶ **Definition 5.** *Given a context Γ and a valuation ρ closing the formulas in Γ, we say that a substitution σ* realizes *$\rho(\Gamma)$ and write $\sigma \Vdash \rho(\Gamma)$ if $\operatorname{dom}(\Gamma) \subseteq \operatorname{dom}(\sigma)$ and $\sigma(x) \in |A|_\rho$ for every declaration $(x : A) \in \Gamma$.*

▶ **Definition 6.** *A typing judgement $\Gamma \vdash t : A$ is* adequate *if for all valuations ρ closing A and Γ and for all substitutions $\sigma \Vdash \rho(\Gamma)$ we have $\sigma(t) \in |A|_\rho$. More generally, we say that an inference rule $\dfrac{J_1 \quad \cdots \quad J_n}{J_0}$ is adequate if the adequacy of all typing judgements $J_1, \ldots, J_n$ implies the adequacy of the typing judgement J_0.*

▶ **Theorem 7** (Adequacy [25]). *The typing rules of Figure 1 are adequate.*

▶ **Corollary 8.** *If $\Gamma \vdash t : A$ is derivable, then it is adequate.*

The adequacy theorem is the key result when defining realizability interpretations in that fundamental properties stem from it. For example, we have the following corollary.

▶ **Corollary 9** (Consistency). *There is no proof term t such that $\vdash t : \bot$.*

We would like to point out that the proof of adequacy is very flexible. Indeed, if one wants to add a new instruction to the language of terms via its typing rule, it is enough to check that this typing rule is adequate while the remainder of the proof is exactly the same.

3.3 Introducing value restrictions

The realizability interpretation of Definition 2 is also flexible regarding the set of formulas that are interpreted. We illustrate this point here by introducing a new construction extending formulas. For these formulas we shall not give any typing rule, instead we will see how this construction allows us to enforce value restrictions, which will turn out to be crucial afterwards in a setting where stateful computations occur. We start by defining the subset $\mathcal{V} \subseteq \Lambda$ of *values* by the following grammar:

$$\textbf{Values} \qquad V \quad ::= \quad 0 \mid \mathsf{s}\, V \mid \lambda x.t \mid (V_1, V_2) \mid \iota_i(V)$$

Observe that variables are not values, otherwise the system would not be stable by substitution. In the remainder of this paper, we adopt the convention that λ-terms are denoted by lowercase letters $t, u, \ldots$ while uppercase letters $V, W, \ldots$ refer to values.

Distinguishing the set of values allows for instance to restrict the β-reduction rule to applications of functions to values:

$$\frac{}{(\lambda x.t)V \rhd_{\mathrm{v}} t[V/x]} \qquad \frac{t \rhd_{\mathrm{v}} t'}{t\, u \rhd_{\mathrm{v}} t'\, u} \qquad \frac{u \rhd_{\mathrm{v}} u'}{V\, u \rhd_{\mathrm{v}} V\, u'}$$

The reflexive transitive closure $\to_{\mathrm{v}}$ of the one-step reduction $\rhd_{\mathrm{v}}$ is known as the (left-to-right) *call-by-value* evaluation strategy. While it is well-known that the reduction system of the λ-calculus is confluent, so that the choice of a particular evaluation strategy does not have any consequence in terms of expressiveness, this is no longer the case when side effects (such as stateful computations in the next sections) come into play.

To enforce value restrictions, let us now extend the language of formulas with a new construction $\{A\} \mapsto B$ and the realizability interpretation accordingly by

$$|\{A\} \mapsto B|_\rho \quad \triangleq \quad \{t \in \Lambda : \forall V \in |A|_\rho.(t\,V \in |B|_\rho)\}$$

In particular, we have $|\{\mathrm{Nat}(e)\} \mapsto B|_\rho \;=\; \{t \in \Lambda : t\,\overline{n} \in |B|_\rho,$ where $n = [\![e]\!]_\rho\}$. It is easy to check that for any formulas A and B, $|\{A\} \mapsto B|_\rho$ is a saturated set, and the adequacy of the $(\forall^2_E)$-rule is thus preserved.

While there is currently no rule to type a term t with a formula of the shape $\{A\} \mapsto B$, we can nonetheless extend the type system with any rule as long as it is adequate (see Proposition 45). We can also extend, maintaining the adequacy of the interpretation of $\{A\} \mapsto B$ (see Proposition 46), the congruence relation with the following rules:

$$\{\exists x.A\} \mapsto B \cong \forall x.\{A\} \mapsto B \qquad\qquad \{\exists X.A\} \mapsto B \cong \forall X.\{A\} \mapsto B$$

We will make use of the following abbreviations:

$$\forall^{\{\mathbb{N}\}}x.A \triangleq \forall x.(\{\mathrm{Nat}(x)\} \mapsto A) \qquad\qquad \exists^{\{\mathbb{N}\}}x.A \triangleq \forall X.(\forall^{\{\mathbb{N}\}}x.(A \to X)) \to X$$

While the first definition is natural, the second one may be a bit more puzzling at first sight. As we saw, the truth value of any formula has to be a saturated set. However, given a formula $A(x)$, the set $\{(\overline{n}, t) : t \in |A(n)|_\rho\}$ is not saturated, and so we cannot define a formula $\exists x.\{\mathrm{Nat}(x)\} \wedge A(x)$ whose realizers would be this set. Nonetheless, the definition of $\exists^{\{\mathbb{N}\}}x.A$ is somehow doing the trick in continuation-passing style, in the sense that we have:

▶ **Proposition 10.** *For any formula A, any valuation ρ and any term t, if $t \in |\exists^{\{\mathbb{N}\}}x.A|_\rho$ then there exists a natural number $n \in \mathbb{N}$ and a term $u \in |A[x := n]|_\rho$ s.t.: $t\,(\lambda xy.(x, y)) \to_\beta (\overline{n}, u)$.*

▶ **Definition 11.** *We define $T \triangleq \lambda zx.(\mathsf{rec}\,(\lambda y.y\,0)\,(\lambda xyz.y\,(\lambda x.z\,(\mathsf{s}\,x)))\,x)\,z$.*

The next proposition relates these new quantifications with the relativized quantifications $\forall^{\mathbb{N}}x.A$ and $\exists^{\mathbb{N}}x.A$ using the term T.

▶ **Proposition 12.** *We have*

1. $T \Vdash \forall^{\{\mathbb{N}\}}x.A \to \forall^{\mathbb{N}}x.A$
2. $\lambda x.x \Vdash \forall^{\mathbb{N}}x.A \to \forall^{\{\mathbb{N}\}}x.A$
3. $\lambda z.z\,\lambda xy.(x, y) \Vdash \exists^{\{\mathbb{N}\}}x.A \to \exists^{\mathbb{N}}x.A$
4. $\lambda xy.T\,y\,\pi_1(x)\,\pi_2(x) \Vdash \exists^{\mathbb{N}}x.A \to \exists^{\{\mathbb{N}\}}x.A$

The term T, which forces the evaluation of an argument of type $\mathrm{Nat}(n)$ to get the underlying value $\overline{n}$ to make it compatible with a function $\forall^{\{\mathbb{N}\}}x.A$, is somehow simulating a call-by-value evaluation (for natural numbers). Such a term is usually called a *storage operator* [20].

While Proposition 12 indicates that the different ways of relativizing the quantifiers are equivalent (in the sense that one admits a realizer if and only if the other does), it is important to keep in mind that this result is peculiar to the current effect-free settings. In particular, this result no longer holds once stateful computations are allowed.

4 Realizability with slices

4.1 Stateful computations

The first step in the Lightstone-Robinson construction aims at getting a product $\mathcal{M}^{\mathbb{N}}$ of the (initial) model $\mathcal{M}$. In order to achieve this goal in our setting, we add a memory cell to our calculus that contains an integer, which we call the *state*. The purpose of the state is to keep track of which "slice" of the product is the interpretation being done. This product allows us to interpret first-order individuals as functions in $\mathbb{N}^{\mathbb{N}}$, so that the interpretation accounts for new elements – the so-called nonstandard elements – for instance the diagonal function (see Proposition 30).

In our extended calculus, the first-order expressions are the same, while second-order formulas now use a value restriction for natural numbers and include a predicate $\mathrm{st}(e)$, as per usual in nonstandard analysis, denoting that the expression e is standard. This means that in our framework we will also have two types of nonstandard quantifications: the usual $\forall^{\mathrm{st}}$, $\exists^{\mathrm{st}}$ and the relativised $\forall^{\{\mathrm{st}\}}$,$\exists^{\{\mathrm{st}\}}x$. We say that a formula is *internal* if it does not contain the predicate $\mathrm{st}(\cdot)$, and *external* otherwise. Terms are extended with two new instructions get and set. The former allows to obtain the content of the current state while the latter allows to increase its content. Formally, we extend the different grammars as follows:

$$\begin{array}{llcl}
\textbf{Formulas} & A, B & ::= & \mathrm{st}(e) \mid X(e_1, \dots, e_n) \mid \{\mathrm{Nat}(e)\} \mapsto A \mid A \to B \\
 & & \mid & A \wedge B \mid A \vee B \mid \forall x.A \mid \exists x.A \mid \forall X.A \mid \exists X.A \\
\textbf{Terms} & t, u & ::= & \dots \mid \mathsf{get} \mid \mathsf{set} \\
\textbf{States} & \mathfrak{S} & \triangleq & \mathbb{N}
\end{array}$$

Since the formulas no longer include an unrestricted constructor $\mathrm{Nat}(e)$, the typing rules for 0, s and rec are no longer required[1]. Other than that, the type system is unchanged. In particular, the get and set instructions are not given any typing rule. We will make use of the following abbreviations:

$$\begin{array}{rcl|rcl}
\forall^{\mathrm{st}}x.A & \triangleq & \forall x.(\mathrm{st}(x) \to A) & \exists^{\mathrm{st}}x.A & \triangleq & \exists x.(\mathrm{st}(x) \wedge A) \\
\forall^{\{\mathrm{st}\}}x.A & \triangleq & \forall x.(\mathrm{st}(x) \to (\{\mathrm{Nat}(x)\} \mapsto A)) & \exists^{\{\mathrm{st}\}}x.A & \triangleq & \forall X.((\forall^{\{\mathrm{st}\}}x.(A \to X)) \to X)
\end{array}$$

With the exception of the get / set instructions, the syntax of terms does not account for states. In fact, only the reduction rule for the set instruction allows to change the state. Nonetheless, states play a crucial role in the reduction system. In particular, one-step reductions are now defined for terms together with a state. We write $t \triangleright^{\mathfrak{s}}_{\mathfrak{s}'} t'$ to denote that the term t in state $\mathfrak{s}$ reduces to the term t' in state $\mathfrak{s}'$. The one-step reduction over terms is defined by the following rules:

$$\frac{t \triangleright_\beta t'}{t \triangleright^{\mathfrak{s}}_{\mathfrak{s}} t'} \qquad \frac{}{\mathsf{get} \triangleright^{\mathfrak{s}}_{\mathfrak{s}} \mathfrak{s}} \qquad \frac{\mathfrak{s}'' = \max(\mathfrak{s}, \mathfrak{s}')}{\mathsf{set}\,\bar{\mathfrak{s}}\,t \triangleright^{\mathfrak{s}'}_{\mathfrak{s}''} t} \qquad \frac{t \triangleright^{\mathfrak{s}}_{\mathfrak{s}'} t'}{C[t] \triangleright^{\mathfrak{s}}_{\mathfrak{s}'} C[t']}$$

where $C[\,] ::= \mathsf{rec}\; u_0\, u_1\, [\,] \;\mid\; [\,]\, u \;\mid\; \pi_i([\,]) \;\mid\; \mathsf{case}\, [\,]\, \{\iota_1(x_1) \mapsto t_1 | \iota_2(x_2) \mapsto t_2\} \;\mid\; \mathsf{s}\, [\,] \;\mid\; \mathsf{set}\, [\,]\, u$.

We write $t \;{}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}'}\; t'$ for the reflexive-transitive closure of this relation.

Since we now consider effectful computations, we have to fix an evaluation strategy in order to ensure the confluence of the reduction system[2]. Here we follow a call-by-name evaluation strategy (we substitute unevaluated arguments), while for rec and set one of their arguments must be reduced.

[1] In Proposition 29, we show how these terms define realizers for the value restricted natural numbers.

[2] Observe that our definition for $C[\,]$ ensures that our reduction system has no critical pair. We refer the reader unfamiliar with side effects to Example 47, given in the appendices.

4.2 Stateful realizability interpretation

The fact that our syntax now includes states allows us to interpret formulas as terms-with-states[3]. Truth values are then defined as saturated sets in $\mathcal{P}(\Lambda \times \mathfrak{S})$. Individuals are now individuals with states, so elements of $\mathbb{N}^{\mathfrak{S}}$, and similarly predicates of arity k are elements of the set of functions from $\mathbb{N}^k$ to $\mathcal{P}(\Lambda \times \mathfrak{S})$. This creates a mismatch in the sense that predicates are no longer shaped to be applied to individuals[4]. In order to define our interpretation, we need to deal with this mismatch between the structure of individuals and the one of predicates, by defining a suitable notion of application.

▶ **Definition 13.** *Let $F : \mathbb{N}^k \to \mathcal{P}(\Lambda \times \mathfrak{S})$ be a predicate. We define the application of F to individuals $f_1, \ldots, f_k \in \mathbb{N}^{\mathfrak{S}}$ by $F@(f_1, \ldots, f_k) \triangleq \{(t; \mathfrak{s}) : (t; \mathfrak{s}) \in F(f_1(\mathfrak{s}), \ldots, f_k(\mathfrak{s}))\}$.*

▶ **Definition 14.** *An individual $f \in \mathbb{N}^{\mathfrak{S}}$ is said to be* standard *if it is a constant function, i.e. if there exists $n \in \mathbb{N}$ such that $\forall \mathfrak{s} \in \mathfrak{S}.(f(\mathfrak{s}) = n)$. We then write $f = n^*$.*

▶ **Definition 15.** *We define* saturated sets with respect to the stateful reduction *to be sets $S \in \Lambda \times \mathfrak{S}$ s.t. for any terms $t, t' \in \Lambda$ and any states $\mathfrak{s}, \mathfrak{s}' \in \mathfrak{S}$, if $(t'; \mathfrak{s}') \in S$ and $t\,{}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}'}\, t'$ then $(t; \mathfrak{s}) \in S$. With abuse of notation we denote the set of these saturated sets by* **SAT***.*

In the realizability interpretation with slices below, truth values are defined as saturated sets. This allows us to reason by *anti-reduction* (sometimes also called *expansion*) in any fixed state. By anti-reduction, we mean that to show that a term t with a state $\mathfrak{s}$ belongs to such a saturated set S, it is enough to find $\mathfrak{s}'$ and t' such that $t\,{}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}'}\, t'$ and $(t'; \mathfrak{s}') \in S$.

We now consider valuations which are functions that associate a function in $\mathbb{N}^{\mathfrak{S}}$ to every first-order variable x and a truth value function from $\mathbb{N}^k$ to **SAT** to every second-order variable X of arity k. Again, with abuse of notation we denote such valuation by ρ.

We also extend the usual interpretation of first-order expressions to range over $\mathbb{N}^{\mathfrak{S}}$. To that end, we simply define arithmetical functions pointwise on the domain. For instance, if $f \in \mathbb{N}^{\mathfrak{S}}$, we write $S^*(f)$ for the function $\mathfrak{s} \mapsto (S(f(\mathfrak{s})))$. When it is clear from the context, we abuse the notation by writing 0, S, $[\![\cdot]\!]_\rho$, etc. instead of 0^*, S^*, $[\![\cdot]\!]_\rho^*$.

▶ **Definition 16** (Realizability with slices)**.** *The interpretation of a formula A together with a valuation ρ is the set $|A|_\rho^{\mathfrak{S}}$ defined inductively according to the following clauses:*

$$\begin{array}{rcl}
|\mathrm{st}(e)|_\rho^{\mathfrak{S}} & \triangleq & \begin{cases} \Lambda \times \mathfrak{S} & \textit{if } [\![e]\!]_\rho \textit{ is standard} \\ \emptyset & \textit{otherwise} \end{cases} \\
|X(e_1, \ldots, e_n)|_\rho^{\mathfrak{S}} & \triangleq & \rho(X)@([\![e_1]\!]_\rho, \ldots, [\![e_n]\!]_\rho) \\
|\{\mathrm{Nat}(e)\} \mapsto A|_\rho^{\mathfrak{S}} & \triangleq & \{(t; \mathfrak{s}) \in \Lambda \times \mathfrak{S} : (t\,\overline{n}; \mathfrak{s}) \in |A|_\rho^{\mathfrak{S}},\ \textit{where } n = [\![e]\!]_\rho(\mathfrak{s})\} \\
|A \to B|_\rho^{\mathfrak{S}} & \triangleq & \{(t; \mathfrak{s}) \in \Lambda \times \mathfrak{S} : \forall u.\big((u; \mathfrak{s}) \in |A|_\rho^{\mathfrak{S}} \Rightarrow (t\,u; \mathfrak{s}) \in |B|_\rho^{\mathfrak{S}}\big)\} \\
|A_1 \wedge A_2|_\rho^{\mathfrak{S}} & \triangleq & \{(t; \mathfrak{s}) \in \Lambda \times \mathfrak{S} : (\pi_1(t); \mathfrak{s}) \in |A_1|_\rho^{\mathfrak{S}} \wedge (\pi_2(t); \mathfrak{s}) \in |A_2|_\rho^{\mathfrak{S}})\}
\end{array}$$

$$|A_1 \vee A_2|_\rho^{\mathfrak{S}} \triangleq \{(t; \mathfrak{s}) \in \Lambda \times \mathfrak{S} : \exists i \in \{1, 2\}.(\mathsf{case}\ t\,\{\iota_1(x_1) \mapsto x_1 | \iota_2(x_2) \mapsto x_2\}; \mathfrak{s}) \in |A_i|_\rho^{\mathfrak{S}}\}$$

$$\begin{array}{rclcrcl}
|\forall x.A|_\rho^{\mathfrak{S}} & \triangleq & \bigcap_{f \in \mathbb{N}^{\mathfrak{S}}} |A|_{\rho, x \mapsto f}^{\mathfrak{S}} & & |\forall X.A|_\rho^{\mathfrak{S}} & \triangleq & \bigcap_{F : \mathbb{N}^k \to \mathbf{SAT}} |A|_{\rho, X \mapsto F}^{\mathfrak{S}} \\
|\exists x.A|_\rho^{\mathfrak{S}} & \triangleq & \bigcup_{f \in \mathbb{N}^{\mathfrak{S}}} |A|_{\rho, x \mapsto f}^{\mathfrak{S}} & & |\exists X.A|_\rho^{\mathfrak{S}} & \triangleq & \bigcup_{F : \mathbb{N}^k \to \mathbf{SAT}} |A|_{\rho, X \mapsto F}^{\mathfrak{S}}
\end{array}$$

We write $(t; s) \Vdash A$ (resp. $t \Vvdash A$) to denote that $(t; s) \in |A|^{\mathfrak{S}}$ (resp. $\forall \mathfrak{s} \in \mathfrak{S}.(t; \mathfrak{s}) \in |A|^{\mathfrak{S}}$). Realizers of the type $t \Vvdash A$ are called universal.

[3] A realizability interpretation with a similar structure, although with a different notion of state, can be found in [28]. The perspective of the latter is also different in that it aims at proving the normalization of a classical call-by-need calculus.

[4] This phenomenon also occurs in the Lightstone-Robinson construction of an ultrapower [23].

Observe that this stateful interpretation has the structure of a product of the interpretation given by Definition 2. The interpretation corresponding to a given state can thus be seen as a *slice* of this product. However, it is important to keep in mind that the set instruction still allows terms to change the value of the state, therefore the slices are not completely independent. We write $|A|_\rho^{\mathfrak{s}}$ to denote the truth value $\{(t;\mathfrak{s}) \in |A|_\rho^{\mathfrak{S}}\}$ in the slice induced by $\mathfrak{s}$. We first verify that truth values are indeed saturated sets and that the interpretation validates the congruence rules.

▶ **Proposition 17**. *Let A be a formula and ρ a valuation closing A. Then $|A|_\rho^{\mathfrak{S}} \in \mathbf{SAT}$.*

▶ **Proposition 18**. *If A and A' are two formulas of HA2 such that $A \cong A'$, then for all valuations ρ closing both A and A' we have $|A|_\rho^{\mathfrak{S}} = |A'|_\rho^{\mathfrak{S}}$.*

We need to adapt a few definitions to prove the adequacy theorem in this setting.

▶ **Definition 19.** *Given a context Γ, a state $\mathfrak{s}$ and a valuation ρ closing the formulas in Γ, we say that a substitution σ* realizes $\rho(\Gamma)$ *in the state $\mathfrak{s}$ and write $(\sigma;\mathfrak{s}) \Vdash \rho(\Gamma)$ if* $\mathrm{dom}(\rho(\Gamma)) \subseteq \mathrm{dom}(\sigma)$ *and $(\sigma(x);\mathfrak{s}) \in |A|_\rho^{\mathfrak{S}}$, for every declaration $(x : A) \in \Gamma$.*

▶ **Definition 20.** *We say that a typing judgement $\Gamma \vdash t : A$ is* adequate *w.r.t. a state $\mathfrak{s}$ in the stateful system if for any valuation ρ and any substitution $(\sigma;\mathfrak{s}) \Vdash \rho(\Gamma)$ we have $(\sigma(t);\mathfrak{s}) \in |\rho(A)|$. An inference rule is adequate w.r.t. a state $\mathfrak{s}$ if the adequacy (w.r.t. $\mathfrak{s}$) of all its premises implies the adequacy (w.r.t. $\mathfrak{s}$) of its conclusion.*

We are now able to show that, with the exception of the $(\forall_E^2)/(\exists_I^2)$-rules, our rules are adequate. The $(\forall_E^2)/(\exists_I^2)$-rules are shown to be adequate, for internal formulas only, in Proposition 27.

▶ **Theorem 21** (Adequacy). *The typing rules of Figure 1, except the $(\forall_E^2)/(\exists_I^2)$-rules, are adequate.*

▶ Remark 22. Let us explain why the $(\forall_E^2)$-rule is not adequate in general (the same argument applies to the $(\exists_I^2)$-rule). As emphasized at the beginning of this section, we interpret predicates by functions from $\mathbb{N}^k$ to $\mathbf{SAT}$, while the truth values of formulas may vary in the set of functions from $(\mathbb{N}^{\mathfrak{S}})^k$ to $\mathbf{SAT}$. Theorem 26 will make this more precise: internal formulas correspond to functions from $\mathbb{N}^k$ to $\mathbf{SAT}$ while external formulas correspond to functions from $(\mathbb{N}^{\mathfrak{S}})^k$ to $\mathbf{SAT}$. Therefore, in general we cannot substitute a second-order variable by any formula. Indeed, in the second-order elimination rule (for universal quantifiers) variables can only be instantiated by internal formulas. Moreover, if the formula B that we want to substitute is a proposition (i.e. if its arity k is equal to 0), then the substitution is valid since the interpretations of internal and external formulas coincide. This means that we could have chosen to work with impredicative encodings of the conjunction (or other connectives) as in the Russell-Prawitz translation [34]. Indeed, such an encoding relies on the use of propositions, which are thus compatible with the elimination rule:

$$A \wedge B \triangleq \forall X.(A \to B \to X) \to X \qquad\qquad A \vee B \triangleq \forall X.(A \to X) \to (B \to X) \to X$$

We show that rec realizes a formula that emulates its former typing rule by using quantifiers relativized with a value restriction.

▶ **Proposition 23**. *We have* rec $\Vdash \forall X.X(0) \to \forall^{\{\mathbb{N}\}}x.(X(x) \to X(S(x))) \to \forall^{\{\mathbb{N}\}}x.X(x)$.

▶ Remark 24. Regarding the necessity of restricting the relativization of quantifiers to values, the proof of Proposition 23 is enlightening. Indeed, given a state $\mathfrak{s}$, two terms $(u_S;\mathfrak{s}) \Vdash \forall^{\{\mathbb{N}\}}y.(X(y) \to X(S(y)))$ and $(u_0;\mathfrak{s}) \Vdash X(0)$ and an individual $f \in \mathbb{N}^{\mathfrak{S}}$ to instantiate x, if instead of a value we were only given a term reducing to a value witnessing $\mathrm{Nat}(f)$, this term may change the value of the state, say to some $\mathfrak{s}'$, before reducing to the value of $f(\mathfrak{s}')$. This would break the proof since nothing is assumed on u_0 and u_S in this new state $\mathfrak{s}'$.

4.3 Glueing

An important property of our interpretation (which also reflects a similar property in the Lightstone-Robinson construction) is that the interpretation of internal formulas can be decomposed as the product of its slices. In other words, internal formulas can only access information in the current state. In particular, and as expected, this means that it is impossible to express standardness by means of internal formulas. To state this formally, we first define the restriction of formulas and truth values with respect to a slice.

▶ **Definition 25.** *Given an internal formula A, we define $\overline{A}^{\mathfrak{s}}$ as the formula whose individuals are all applied in $\mathfrak{s}$. Formally, it amounts to replacing each individual by the standard individual with which it coincides in the state $\mathfrak{s}$:*

$$\begin{array}{rcl|rcl|rcl}
\overline{F(e_1,...,e_k)}^{\mathfrak{s}} & \triangleq & F((e_1(\mathfrak{s}))^*,\dots,(e_k(\mathfrak{s}))^*) & \overline{A\wedge B}^{\mathfrak{s}} & \triangleq & \overline{A}^{\mathfrak{s}}\wedge\overline{B}^{\mathfrak{s}} & \overline{\exists x.A}^{\mathfrak{s}} & \triangleq & \exists x.\overline{A}^{\mathfrak{s}} \\
\overline{A\to B}^{\mathfrak{s}} & \triangleq & \overline{A}^{\mathfrak{s}}\to\overline{B}^{\mathfrak{s}} & \overline{A\vee B}^{\mathfrak{s}} & \triangleq & \overline{A}^{\mathfrak{s}}\vee\overline{B}^{\mathfrak{s}} & \overline{\forall X.A}^{\mathfrak{s}} & \triangleq & \forall X.\overline{A}^{\mathfrak{s}} \\
\overline{\{\mathrm{Nat}(e)\}\mapsto B}^{\mathfrak{s}} & \triangleq & \{\mathrm{Nat}((e(\mathfrak{s}))^*)\}\mapsto\overline{B}^{\mathfrak{s}} & \overline{\forall x.A}^{\mathfrak{s}} & \triangleq & \forall x.\overline{A}^{\mathfrak{s}} & \overline{\exists X.A}^{\mathfrak{s}} & \triangleq & \exists X.\overline{A}^{\mathfrak{s}}
\end{array}$$

The next result ensures that truth values of internal formulas can be split into slices.

▶ **Theorem 26** (Glueing). *For any internal formula A and valuation ρ closing A, we have that $(t;\mathfrak{s}) \in |A|_\rho^{\mathfrak{S}} \Leftrightarrow t \in |\overline{A}^{\mathfrak{s}}|_\rho^{\mathfrak{s}}$.*

Let $B(x)$ be a formula whose only free variable is x, and ρ a valuation. In general, the function $\mathcal{F}_B$ that associates to any individual f the truth value $|B(f)|_\rho^{\mathfrak{S}}$ is a function from $\mathbb{N}^{\mathfrak{S}}$ to $\mathbf{SAT}$. If B is internal, by the glueing theorem, to determine $\mathcal{F}_B$ it is enough to know its value for standard individuals. This means that we only need to know a function from $\mathbb{N}$ to $\mathbf{SAT}$. As such, we can now formally state the intuition developed in Remark 22.

▶ **Proposition 27.** *The elimination rule $(\forall_E^2)$ for the 2nd-order universal quantification and the introduction rule $(\exists_I^2)$ for the 2nd-order existential quantification are adequate for any internal formula B whose only free variables are $(x_1,...,x_k)$.*

▶ Remark 28. Observe that external formulas such as $\mathrm{st}(x) \to \bot$ cannot be defined by glueing. Consider for instance a nonstandard element τ. Then $|\mathrm{st}(\tau) \to \bot|^{\mathfrak{S}} = \Lambda \times \mathfrak{S}$, while for any state $\mathfrak{s} \in \mathfrak{S}$ we have $|\overline{\mathrm{st}(\tau) \to \bot}^{\mathfrak{s}}|_{\mathfrak{s}} = |\mathrm{st}(\tau(\mathfrak{s})^*) \to \bot|_{\mathfrak{s}} = |\top \to \bot|_{\mathfrak{s}} = \emptyset$.

It is well-known that the comprehension scheme $\mathrm{CA}_B \triangleq \exists X.\forall x.(X(x) \Leftrightarrow B)$ is a logical consequence of the elimination principle $\mathrm{Elim}_A^B \triangleq (\forall X.A) \Rightarrow A[X(x) := B]$ (by taking $A = \exists Y.\forall x.(Y(x) \Leftrightarrow X(x))$). Since we have the $(\forall_E^2)$-rule restricted to internal formulas B, the comprehension scheme is also valid for these formulas. In particular, this implies standardization for internal formulas, i.e. $\forall^{\mathrm{st}}X.\exists^{\mathrm{st}}Y.\forall^{\mathrm{st}}z.(Y(z) \Leftrightarrow X(z) \wedge B(z))$ holds for B an internal formula. The usual standardization scheme, formulated for all formulas, requires further investigation and is left for future work. Of course, the comprehension scheme does not hold for external formulas, so the relativization on the quantifiers in standardization is in this sense necessary.

5 Nonstandard principles in realizability with slices

5.1 Natural numbers

Observe that the language of HA2 does not express the existence of specific nonstandard elements, e.g. δ is not in the language. However, to refer to some nonstandard element τ, we can always consider a valuation that maps a variable x to τ. With abuse of notation, in the remainder of this paper, we will write nonstandard elements directly in formulas as if they were in the language. Also, we will use the notation † to refer to an arbitrary λ-term with no further assumption.

In the stateful interpretation (Definition 16), we considered a value restriction to natural numbers. Nonetheless, we can assert that an expression is a natural number through the formula $\mathrm{Nat}'(e) \quad \triangleq \quad \forall X.(\{\mathrm{Nat}(e)\} \mapsto X) \to X$. It is easy to see, by an argument similar to Proposition 10, that for any individual $f \in \mathbb{N}^{\mathfrak{S}}$, if t is a term such that $(t;\mathfrak{s}) \in |\mathrm{Nat}'(f)|^{\mathfrak{S}}$, then $t\,\lambda x.x\,{}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}}\,\overline{n}$ where $n = f(\mathfrak{s})$. In other words, t is an effect-free term producing $\overline{n}$. This is to be compared with $\mathrm{Nat}(f)$, for which the requirement for its truth value to be saturated, would have entailed its interpretation to reduce to a natural number $f(\mathfrak{s}')$ in a possibly different state. We show that (by-value) natural numbers, i.e. Nat', contain 0, and are closed under the successor and recursion for internal formulas.

▶ **Proposition 29**. *Let A be an internal formula. We have*

1. $\lambda x.x\,0 \Vdash \mathrm{Nat}'(0)$
2. $\lambda xy.y\,(\mathsf{s}\,x) \Vdash \forall^{\{\mathbb{N}\}}x.\mathrm{Nat}'(S(x))$
3. $\mathsf{rec} \Vdash A(0) \to \big(\forall^{\{\mathbb{N}\}}y.(A(y) \to A(S\,y))\big) \to \forall^{\{\mathbb{N}\}}x.A(x))$

The interpretation now witnesses the existence of new elements. The canonical example is the *diagonal*, i.e. the function $\delta : n \mapsto n$. Indeed, the diagonal is a nonstandard natural number which is realized by the get instruction.

▶ **Proposition 30**. *We have that*

1. $† \Vdash \neg\mathrm{st}(\delta)$
2. $† \Vdash \exists x.\neg\mathrm{st}(x)$
3. $\lambda x.T\,x\,\mathsf{get} \Vdash \mathrm{Nat}'(\delta)$
4. $\lambda x.T\,x\,\mathsf{get}\,† \Vdash \exists^{\{\mathbb{N}\}}x.\neg\mathrm{st}(x)$

Part 2 in Proposition 30 is sometimes referred to as the ENS_0 (existence of nonstandard elements) principle [6]. As a consequence of Proposition 27, Leibniz equality is only compatible with the $(\forall^2_E)$-rule restricted to internal formulas. In our setting, this encoding only reflects equality in the current state, i.e. a local knowledge of individuals (slice by slice), while the usual notion of equality (for $\mathbb{N}^{\mathfrak{S}}$) requires a global knowledge (on all the slices). If $A(x)$ is an external formula, we cannot hope to have an internal definition of equality such that its elimination principle $x = y \to A(x) \to A(y)$ is valid.

▶ **Example 31.** Consider an individual f, equal to 1 everywhere except for some state $\mathfrak{s}_0$ where it is equal to 0. Then by considering the formula $A(x) \triangleq (\mathrm{st}(x) \to \bot) \to \bot$, it is easy to get a realizer of $\bot$ out of any realizer of $(\forall Z.(Z(1^*) \to Z(f))) \to A(1^*) \to A(f)$.

Nonetheless, the elimination of Leibniz equality is realizable for standard individuals or for internal formulas.

▶ **Proposition 32**. *Let f and g be individuals in $\mathbb{N}^{\mathfrak{S}}$, then*

1. *For any formula $A(x)$, $\lambda x.x \Vdash \mathrm{st}(f) \to \mathrm{st}(g) \to (\forall Z.(Z(f) \to Z(g))) \to A(f) \to A(g)$*
2. *If $A(x)$ is an internal formula, then $\lambda x.x \Vdash (\forall Z.(Z(f) \to Z(g))) \to A(f) \to A(g)$*

5.2 Nonstandard reasoning principles

In this section, we prove some properties which are usual in frameworks that use nonstandard analysis: transfer, overspill, external induction, idealization, etc.

Theorem 33 below indicates that the transfer property (for internal formulas) is devoid of computational content. This is a somewhat reassuring fact: properties that are true for standard individuals are automatically true for all individuals.

▶ **Theorem 33** (Transfer). *For any internal formula A we have:*

1. $\bigcap_{f\in\mathbb{N}^{\mathfrak{S}}} |A|^{\mathfrak{S}}_{x\mapsto f} = \bigcap_{n\in\mathbb{N}} |A|^{\mathfrak{S}}_{x\mapsto n^*}$
2. $\lambda xy.x \Vdash\!\!\vdash \forall x.A(x) \to \forall^{\mathrm{st}} x.A(x)$
3. $\lambda x.x\,\dagger \Vdash\!\!\vdash \forall^{\mathrm{st}} x.A(x) \to \forall x.A(x)$
4. $\bigcup_{f\in\mathbb{N}^{\mathfrak{S}}} |A|^{\mathfrak{S}}_{x\mapsto f} = \bigcup_{n\in\mathbb{N}} |A|^{\mathfrak{S}}_{x\mapsto n^*}$
5. $\lambda x.(\dagger, x) \Vdash\!\!\vdash \exists x.A(x) \to \exists^{\mathrm{st}} x.A(x)$
6. $\lambda x.\pi_2(x) \Vdash\!\!\vdash \exists^{\mathrm{st}} x.A(x) \to \exists x.A(x)$

As expected, transfer does not hold for all formulas. A counter-example is given in the next proposition by the external formula stating that all individuals are (not not) standard.

▶ **Proposition 34.** *Let $A(x)$ be the formula $\neg\mathrm{st}(x)$. The formulas $\forall^{\mathrm{st}} x.\neg A(x) \to \forall x.\neg A(x)$ and $\exists x.A(x) \to \exists^{\mathrm{st}} x.A(x)$ have no realizer.*

The principle of external induction [32] allows to prove that a certain property is valid for all standard natural numbers, for instance, that every nonstandard element is larger than all standard natural numbers[5]. We show that in our context, this principle can be realized using the rec instruction.

▶ **Proposition 35** (External induction). *For any formula $A(x)$ whose only free variable is x*

$$\mathsf{rec} \Vdash\!\!\vdash A(0^*) \to \forall^{\{\mathrm{st}\}} x.(A(x) \to A(S(x))) \to \forall^{\{\mathrm{st}\}} x.A(x).$$

The next two propositions, show that one cannot separate standard natural numbers from nonstandard natural numbers using an internal formula [36]. We first show that overspill can be *realized* by combining the realizers for ENS_0 and for the transfer principle.

▶ **Proposition 36** (Overspill). *For any internal formula A, we have*

$$\lambda x.(x\,\dagger, \dagger) \Vdash\!\!\vdash \forall^{\mathrm{st}} x.A(x) \to \exists x.(\neg\mathrm{st}(x) \wedge A(x)).$$

The usual proof of underspill is by contradiction, hence using classical logic, which we do not have here. Nevertheless, we can obtain the following version in which a double-negation occurs.

▶ **Proposition 37** (Underspill). *For any internal formula A, we have*

$$\lambda xy.(\lambda z.y\,(\dagger, z))(x\,\dagger) \Vdash\!\!\vdash (\forall x.\neg\mathrm{st}(x) \to A(x)) \to \neg\neg\exists^{\mathrm{st}} x.A(x).$$

[5] Actually, this requires to consider a quotiented definition of the standardness predicate, see Proposition 42.

5.3 Idealization

We first extend the realizability interpretation to take into account relations $R : \mathbb{N}^2 \to \mathbb{N}$ on the natural numbers:

$$|R(e_1, e_2)|^{\mathfrak{S}}_{\rho} \quad \triangleq \quad \{(t; \mathfrak{s}) : R(\llbracket e_1 \rrbracket_{\rho}(\mathfrak{s}), \llbracket e_2 \rrbracket_{\rho}(\mathfrak{s})) \text{ holds}\}$$

This coincides with the interpretation of the relation R through a second-order variable and the corresponding semantic relation from $\mathbb{N}^2$ to **SAT** in the interpretation.

Let us now briefly illustrate the main idea behind the proof of idealization by showing that there exists a (nonstandard) natural number greater than or equal to any standard number. The usual proof relies on the fact that δ is such a number, since for any standard number n, in any slice greater than or equal to n, the relation $n \le \delta$ holds. In our setting, we use the set instruction to reach such a state.

▶ **Proposition 38** (Diagonalization). *We have* $\lambda z.T\,z\,\mathsf{get}\,(\lambda xy.\,\mathsf{set}\,y\,\dagger) \Vvdash \exists^{\{\mathbb{N}\}}x.\forall^{\{\mathrm{st}\}}y.y \le x$.

▶ Remark 39. Consider a term loop^+ such that for any state $\mathfrak{s} \in \mathfrak{S}$, $\mathsf{loop}^+\ {}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}}\ \mathsf{incr}\ \mathsf{loop}^+$ where $\mathsf{incr} \triangleq \lambda x.\,\mathsf{set}\,(\mathsf{s}\ \mathsf{get})\,x$. Observe that $\mathsf{loop}^+ \Vvdash \forall^{\mathrm{st}}x.x < \delta$ where the quantifier does not need to be relativized since the value of x is not required. Yet, the computation never terminates and we do not even know when the computation reaches a correct state.

As mentioned above, the idea to prove the general case of idealization is very similar. If for any $n \in \mathbb{N}$ there exists $\tau_n \in \mathbb{N}$ such that for any $m \le n$, $R(\tau_n, m)$ holds, we can consider the nonstandard natural number $\tau \triangleq (\tau_{\mathfrak{s}})_{\mathfrak{s}\in\mathfrak{S}} \in \mathbb{N}^{\mathfrak{S}}$. As shown by the following lemma, we can compute τ from any realizer of $\forall^{\{\mathrm{st}\}}n.\exists^{\{\mathrm{st}\}}x.\forall^{\{\mathrm{st}\}}y.(y \le n \to R(x, y))$.

▶ **Lemma 40.** *For any formula A, any valuation ρ, any state $\mathfrak{s}$ and any term t such that $(t; \mathfrak{s}) \in |\exists^{\{\mathrm{st}\}}x.A|^{\mathfrak{S}}_{\rho}$, there exists a natural number $n \in \mathbb{N}$ and a term u such that $(u; \mathfrak{s}) \in |A|^{\mathfrak{S}}_{\rho,x\mapsto n}$ and $t\,(\lambda xyz.(y, z))\ {}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}}\ (\overline{n}, u)$.*

The term $\mathsf{ideal} \triangleq \lambda x.\lambda y.T\,y\,(\pi_1(T\,(x\,\dagger)\,\mathsf{get}\,(\lambda wyz.(y, z))))\,(\lambda yz.\,\mathsf{set}\,z\,y)$ is a realizer for the idealization principle. Indeed, in any state $\mathfrak{s}$ the first component of ideal computes $\tau(\mathfrak{s})$, using Lemma 40, while the second component increases the state to ensure the validity of the relation (as in Proposition 38).

▶ **Theorem 41** (Idealization). $\mathsf{ideal} \Vvdash \forall^{\{\mathrm{st}\}}n.\exists^{\{\mathrm{st}\}}x.\forall^{\{\mathrm{st}\}}y.(y \le n \to R(x, y)) \to \exists^{\{\mathbb{N}\}}x.\forall^{\{\mathrm{st}\}}y.R(x, y)$

6 Conclusion and future work

6.1 Towards a quotient

In order to fully mimic Lightstone and Robinson's construction, an extra step would be required where one would take a quotient of the interpretation with slices. The study of such an interpretation is outside the scope of this paper[6]. Let us nevertheless comment on a possibility. Fix a free ultrafilter $\mathcal{U}$ over the set of states. Given any set V, let us denote by $\cong$ the equivalence relation over $V^{\mathfrak{S}}$ defined by $f \cong g \triangleq \{\mathfrak{s} \in \mathfrak{S} : f(\mathfrak{s}) = g(\mathfrak{s})\} \in \mathcal{U}$.

First, we can, within the realizability with slices, change the way $\mathrm{st}(f)$ is interpreted to consider standardness up to the ultrafilter. In this way, $f \in \mathbb{N}^{\mathfrak{S}}$ is said to be standard if and only if there exists $n \in \mathbb{N}$ s.t. $f \cong n^*$. As a consequence, we for instance get that:

[6] We leave it for future work, but more details sketching this construction are given in Appendix C.

▶ **Proposition 42.** $\lambda xy.\mathsf{loop}^+ \Vdash \forall x, y.\neg\mathrm{st}(x) \to \mathrm{st}(y) \to y < x$

We then need to define a new notion of realizability in which realizers are also considered up to the equivalence relations induced by $\mathcal{U}$. To that end, a natural attempt consists in considering Łoś' theorem as a guideline. For the sake of clarity, let us denote by $|A|^*$ the truth values in this interpretation, which we shall call *realizability up to* $\mathcal{U}$.

▶ **Definition 43.** *We say that a formula A is* Łoś-reducible *if for any valuation ρ closing A, $t \in |A|^*$ if and only if $\{\mathfrak{s} \in \mathfrak{S} : (t;\mathfrak{s}) \in |A|^{\mathfrak{S}}_\rho\} \in \mathcal{U}$.*

We actually define the interpretation of connectives by this equivalence (*e.g.*, we define $|A \to B|^*_\rho \triangleq \{t \in \Lambda : \{\mathfrak{s} \in \mathfrak{S} : (t;\mathfrak{s}) \in |A \to B|^{\mathfrak{S}}_\rho\} \in \mathcal{U},\})$ while the interpretation of the quantifiers is still defined via intersections (resp. unions) over the same domain as in the interpretation with slices (*e.g.*, $|\forall x.A|^*_\rho \triangleq \bigcap_{f\in\mathbb{N}^{\mathfrak{S}}} |A|^*_{\rho,x\mapsto f}$). As shown in the following theorem, first-order quantifiers behave well with respect to the ultrafilter.

▶ **Theorem 44** (Łoś' theorem). *First-order internal formulas as well as arbitrary disjunctions, conjunctions and implications are Łoś-reducible.*

Theorem 44 implies that if a term t is a realizer of a first-order internal formula A "often enough" in the interpretation with slices, then t is still a realizer in the interpretation up to $\mathcal{U}$. Since all the realizers in Section 5 were universal, they are still realizers in this new setting, meaning that all the results from that section remain valid in the interpretation up to $\mathcal{U}$. In particular, Theorem 44 applies to transfer, idealization, overspill or underspill.

A simple example illustrating this new interpretation is the formula $\forall^{\mathrm{st}} x.x < \delta$, which was realized by loop^+ in the interpretation with slices and is now realized by any term (because for any $n \in \mathbb{N}$, the set of states such that $n < \delta$ is equal to $[n; +\infty[$ which belongs to $\mathcal{U}$). Similarly, loop^+ can be replaced by † in Proposition 42.

However, this construction is still prospective and it raises several questions. On the one hand, such a definition is not as compositional as one usually expects in realizability. Indeed, while we have that $|A \to B|^*_\rho \subseteq \{t : \forall u \in |A|^*_\rho.t\,u \in |B|^*_\rho\}$ for any internal formulas A and B and any valuation ρ, this inclusion is strict in general (see Remark 52) . In other words, we can compose a realizer $t \in |A \to B|^*_\rho$ with a realizer in $u \in |A|^*_\rho$ to get $t\,u \in |B|^*_\rho$, but the $(\to_I)$-rule is not adequate when considering substitutions of variables by realizers in the quotiented truth values. More generally, such a definition does not exactly match the intuition of the quotient in the Lightstone-Robinson construction, just like the interpretation with slices does not exactly define a product due to the ability to change the state via set.

On the other hand, the interpretation up to $\mathcal{U}$ is indeed a new and more flexible interpretation in that it allows us to get realizers for principles that were inaccessible in the interpretation with slices (e.g., $\forall x, y.\neg\mathrm{st}(x) \to \mathrm{st}(y) \to y < x$). We would like to determine whether it allows us to realize other, more involved, nonstandard reasoning principles such as standardization but *prima facie* this principle does not seem to be realizable with the current definitions.

6.2 Related and future work

Some related works concern notions of realizability for nonstandard arithmetic which are variants of Kreisel's modified realizability [6, 9]. These notions of realizability are more inspired by Nelson's syntactical approach to nonstandard analysis. In particular, they rely on translations of formulas inducing conservative extensions of Heyting arithmetic. An important difference with our work is that we are able to give non-trivial computational content to idealization. It could be interesting to better understand the relation between this approach and the approaches based on Kreisel's realizability. In particular, we would like to know whether we can obtain a preservation result for some class of formulas (*e.g.* internal, quantifier-free, ∃-free formulas).

It seems that our interpretation with slices can be adapted without difficulty to Krivine's classical realizability. In particular, a similar interpretation (but with a very different purpose) for a classical calculus with a global environment is given in [28]. This setting could possibly allow to validate new principles by taking advantage of the computational power brought by control operators.

Finally, similar ideas have been adressed by Aschieri. In [1] the author uses a notion of state which allows to construct a forcing model. In particular, natural numbers are interpreted as functions from states to $\mathbb{N}$. Yet, his work does not pay attention to the nonstandard principles that can be obtained in his setting but rather to forcing. It would be natural to investigate whether our setting also allows for forcing techniques. This connection with forcing is reinforced by the fact that in the realm of Krivine's realizability, which generalizes Cohen's forcing, the latter is given a computational content via the addition of a monotone memory cell to the abstract machine in order to store forcing conditions [21, 26].

References

1 Federico Aschieri. Constructive forcing, CPS translations and witness extraction in interactive realizability. *Mathematical Structures in Computer Science*, 27(6):993–1031, 2017. doi:10.1017/S0960129515000468.

2 Jeremy Avigad. Weak theories of nonstandard arithmetic and analysis. In *Reverse mathematics 2001*, volume 21 of *Lect. Notes Log.*, pages 19–46. Assoc. Symbol. Logic, La Jolla, CA, 2005.

3 Jacques Bair, Piotr Błaszczyk, Elías Guillén, Peter Heinig, Vladimir Kanovei, and Mikhail G. Katz. Continuity between Cauchy and Bolzano: issues of antecedents and priority. *British Journal for the History of Mathematics*, pages 1–18, 2020. doi:10.1080/26375451.2020.1770015.

4 Jacques Bair, Piotr Błaszczyk, Robert Ely, Peter Heinig, and Mikhail Katz. Leibniz's well-founded fictions and their interpetations. *Mat. Stud.*, 49(2):186–224, 2018.

5 Henk Barendregt. Lambda calculi with types. In S. Abramsky, Dov M. Gabbay, and S. E. Maibaum, editors, *Handbook of Logic in Computer Science (Vol. 2)*, pages 117–309. Oxford University Press, Inc., New York, NY, USA, 1992.

6 Benno van den Berg, Eyvind Briseid, and Pavol Safarik. A functional interpretation for nonstandard arithmetic. *Ann. Pure Appl. Logic*, 163(12):1962–1994, 2012.

7 Jean-Louis Callot. Trois leçons d'analyse infinitésimale. In J.M. Salanskis and H. Sinaceur, editors, *Le labyrinthe du continu*, pages 369–381. Springer-Verlag, Paris, 1992.

8 Bruno Dinis and Fernando Ferreira. Interpreting weak Kőnig's lemma in theories of nonstandard arithmetic. *Mathematical Logic Quarterly*, 63(1-2):114–123, 2017. doi:10.1002/malq.201600066.

9 Bruno Dinis and Jaime Gaspar. Intuitionistic nonstandard bounded modified realisability and functional interpretation. *Ann. Pure Appl. Logic*, 169(5):392–412, 2018. doi:10.1016/j.apal.2017.12.004.

10 Bruno Dinis and Imme van den Berg. *Neutrices and external numbers: A flexible number system.* Monographs and Research Notes in Mathematics. CRC Press, Boca Raton, FL, 2019. With a foreword by Claude Lobry. doi:10.1201/9780429291456.

11 Kurt Gödel. Über eine bisher noch nicht benützte Erweiterung des finiten Standpunktes. *Dialectica*, 12(3-4):280–287, 1958. doi:10.1111/j.1746-8361.1958.tb01464.x.

12 Timothy Griffin. A formulae-as-type notion of control. In *Proceedings of the 17th ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages*, POPL '90, pages 47–58, New York, NY, USA, 1990. ACM. doi:10.1145/96709.96714.

13 Amar Hadzihasanovic and Benno van den Berg. Nonstandard functional interpretations and categorical models. *ND Journal of Formal Logic*, 58(3), 2017.

14 Arend Heyting. *Mathematische Grundlagenforschung. Intuitionismus. Beweistheorie.* Springer-Verlag, Berlin, 1934. doi:10.1007/978-3-642-65617-0.

15 Mikhail Katz and David Sherry. Leibniz's infinitesimals: their fictionality, their modern implementations, and their foes from Berkeley to Russell and beyond. *Erkenntnis*, 78(3):571–625, 2013. doi:10.1007/s10670-012-9370-y.

16 Stephen Kleene. On the interpretation of intuitionistic number theory. *Journal of Symbolic Logic*, 10:109–124, 1945.

17 Andrey Kolmogorov. Zur Deutung der intuitionistischen Logik. *Mathematische Zeitschrift*, 35(1):58–65, 1932. doi:10.1007/BF01186549.

18 Georg Kreisel. On the interpretation of non-finitist proofs, I. *J. Symb. Log.*, 16:241–267, 1951.

19 Jean-Louis Krivine. Typed lambda-calculus in classical Zermelo-Fraenkel set theory. *Arch. Math. Log.*, 40(3):189–205, 2001.

20 Jean-Louis Krivine. Realizability in classical logic. In Interactive models of computation and program behaviour. *Panoramas et synthèses*, 27, 2009.

21 Jean-Louis Krivine. Realizability algebras: a program to well order $\mathbb{R}$. *Logical Methods in Computer Science*, 7(3), 2011. doi:10.2168/LMCS-7(3:2)2011.

22 Jean-Louis Krivine. Bar Recursion in Classical Realisability: Dependent Choice and Continuum Hypothesis. In Jean-Marc Talbot and Laurent Regnier, editors, *25th EACSL Annual Conference on Computer Science Logic (CSL 2016)*, volume 62 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 25:1–25:11, Dagstuhl, Germany, 2016. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik. doi:10.4230/LIPIcs.CSL.2016.25.

23 Albert Lightstone and Abraham Robinson. *Nonarchimedean Fields and Asymptotic Expansions*. North-Holland mathematical library. North-Holland, 1975.

24 Robert Lutz. Rêveries infinitésimales. *Gazette des mathématiciens*, 34:79–87, 1987.

25 Alexandre Miquel. Existential witness extraction in classical realizability and via a negative translation. *Logical Methods in Computer Science*, 7(2):188–202, 2011. doi:10.2168/LMCS-7(2:2)2011.

26 Alexandre Miquel. Forcing as a program transformation. In *Proceedings of the 2011 IEEE 26th Annual Symposium on Logic in Computer Science*, LICS '11, page 197–206, USA, 2011. IEEE Computer Society. doi:10.1109/LICS.2011.47.

27 Alexandre Miquel. Implicative algebras: A new foundation for realizability and forcing. *ArXiv e-prints*, 2020. arXiv:1802.00528.

28 Étienne Miquey and Hugo Herbelin. Realizability interpretation and normalization of typed call-by-need λ-calculus with control. In *Foundations of software science and computation structures*, volume 10803 of *Lecture Notes in Comput. Sci.*, pages 276–292. Springer, Cham, 2018. doi:10.1007/978-3-319-89366-2_1.

29 Ieke Moerdijk. A model for intuitionistic non-standard arithmetic. *Ann. Pure Appl. Logic*, 73(1):37–51, 1995. A tribute to Dirk van Dalen. doi:10.1016/0168-0072(93)E0071-U.

30 Ieke Moerdijk and Erik Palmgren. Minimal models of Heyting arithmetic. *J. Symbolic Logic*, 62(4):1448–1460, 1997. doi:10.2307/2275651.

31 Edward Nelson. Internal set theory: A new approach to nonstandard analysis. *Bull. Amer. Math. Soc*, 1977.

32 Edward Nelson. *Radically Elementary Probability Theory*. Annals of Mathematical Studies, vol. 117. Princeton University Press, Princeton, N. J., 1987.

33 Jerzy Łoś. Quelques remarques, théorèmes et problèmes sur les classes définissables d'algèbres. *Journal of Symbolic Logic*, 25(2):168–168, 1960. doi:10.2307/2964232.

34 Dag Prawitz. *Natural deduction. A proof-theoretical study.* Acta Universitatis Stockholmiensis. Stockholm Studies in Philosophy, No. 3. Almqvist & Wiksell, Stockholm, 1965.

35 Abraham Robinson. Non-standard analysis. *Proc. Roy. Acad. Sci.*, 1961.

36 Abraham Robinson. *Non-standard analysis.* North-Holland Publishing Co., Amsterdam, 1966.

37 Alfred Tarski. Une contribution à la théorie de la mesure. *Fundamenta Mathematicae*, 15(1):42–50, 1930. URL: http://eudml.org/doc/212372.

38 Jaap van Oosten. *Realizability: an introduction to its categorical side*, volume 152 of *Studies in Logic and the Foundations of Mathematics.* Elsevier B. V., Amsterdam, 2008.

A Proofs of Section 3

A.1 Realizability interpretation

Proof of Proposition 3. By induction on $A \cong A'$. The interesting case is for proving the equality $|(\exists x.A) \to B|^{\mathfrak{S}}_{\rho} = |\forall x.(A \to B)|^{\mathfrak{S}}_{\rho}$. ◀

Proof of Theorem 7 (Adequacy). The proof is standard, by case analysis. ◀

Proof of Corollary 9 (Consistency). If $\vdash t : \bot$, then by Theorem 7 one has $t \in |\bot| = |\forall X.X| = \bigcap_{S \in \mathbf{SAT}} S = \emptyset$. To see that this intersection is indeed empty, one may take for example $S_0 = \{t \in \Lambda : t \to 0\} \in \mathbf{SAT}$ and $S_1 = \{t \in \Lambda : t \to \mathsf{s}0\} \in \mathbf{SAT}$, and clearly $S_0 \cap S_1 = \emptyset$. ◀

A.2 Introducing value restrictions

▶ **Proposition 45.** *The following typing rules are adequate:*

$$\frac{\Gamma \vdash t : A \to B}{\Gamma \vdash t : \{A\} \mapsto B}\ (\mapsto_I) \qquad\qquad \frac{\Gamma \vdash t : \{A\} \mapsto B \quad \Gamma \vdash V : A}{\Gamma \vdash t\,V : B}\ (\mapsto_E)$$

Proof. For the first rule it suffices to see that for any valuation ρ, we have:

$$\{t \in \Lambda : \forall u \in |A|^{\mathfrak{S}}_{\rho}.(t\,u \in |B|^{\mathfrak{S}}_{\rho})\} \subseteq \{t \in \Lambda : \forall V \in |A|^{\mathfrak{S}}_{\rho}.(t\,V \in |B|^{\mathfrak{S}}_{\rho})\}$$

For the second one, the proof is analogous to the adequacy of the $(\to_E)$-rule. ◀

▶ **Proposition 46.** *For any formulas A and B, we have*

1. $|\{\exists x.A\} \mapsto B|^{\mathfrak{S}}_{\rho} = |\forall x.\{A\} \mapsto B|^{\mathfrak{S}}_{\rho}$
2. $|\{\exists X.A\} \mapsto B|^{\mathfrak{S}}_{\rho} = |\forall X.\{A\} \mapsto B|^{\mathfrak{S}}_{\rho}$

Proof. The proof is analogous to the proof of Proposition 3. ◀

Proof of Proposition 10. Let t be a term in $|\exists^{\{\mathbb{N}\}}x.A|^{\mathfrak{S}}_{\rho}$. For any $\mathbb{X} \in \mathbf{SAT}$ and any $v \in |\forall^{\{\mathbb{N}\}}x.(A \to X)|_{\rho, X \mapsto \mathbb{X}}$, we have that $t\,v \in \mathbb{X}$. Let us define the set $\mathbb{X} = \{w \in \Lambda : \exists n, u.w \to_{\beta} (\overline{n}, u) \wedge u \in |A[x := n]|^{\mathfrak{S}}_{\rho}\}$, which is obviously saturated. It is clear that $\lambda xy.(x,y) \in |\forall^{\{\mathbb{N}\}}x.(A \to X)|_{\rho, X \mapsto \mathbb{X}}$ since for any $n \in \mathbb{N}$ and any $u \in |A[x := n]|^{\mathfrak{S}}_{\rho}\}$, it holds that $(\lambda xy.(x,y))\,\overline{n}\,u \to_{\beta} (\overline{n}, u) \in \mathbb{X}$. We conclude that $t\,(\lambda xy.(x,y)) \to_{\beta} (\overline{n}, u)$. ◀

Proof of Proposition 12. Easy realizability proofs by anti-reduction. ◀

B Proofs of Section 4

B.1 Stateful computations

We illustrate the need for an evaluation strategy to ensure confluence in the presence of states by giving a simple example of stateful computation whose result is not the same using call-by-name and call-by-value strategies.

▶ **Example 47.** Let us write $x+y$ for a term that computes the addition of x and y (such term is easily definable via rec). Let us define $\mathsf{incr}_0 \triangleq \mathsf{set}\,(\mathsf{s}\ \mathsf{get})\,0$ (which increases the state and reduces to 0) and $t \triangleq (\lambda x.(\mathsf{get}+x)+x)\ \mathsf{incr}_0$. If we reduce the argument of the functions first (call-by-value) we obtain $t\ {}^0{\downarrow}^1\ (\lambda x.(\mathsf{get}+x)+x))\,0\ {}^1{\downarrow}^1\ (\mathsf{get}+0)+0\ {}^1{\downarrow}^1\ 1$. In turn, if we perform the β-reduction without reducing the argument (call-by-name), we get $t\ {}^0{\downarrow}^0\ (\mathsf{get}+\mathsf{incr}_0)+\mathsf{incr}_0\ {}^0{\downarrow}^1\ (\mathsf{get}+\mathsf{incr}_0)+0\ {}^1{\downarrow}^2\ \mathsf{get}+0\ {}^2{\downarrow}^2\ 2$. In the absence of an evaluation strategy, the system would thus have admitted unsolvable critical pairs.

B.2 Realizability interpretation

Proof of Proposition 17. By a straighforward induction on the structure of A. Observe for instance that the case $\mathrm{st}(f)$ follows from the definition and that the case $X(e_1,\ldots,e_n)$ follows from the fact that, by definition, $\rho(X)$ takes values in $\mathbf{SAT}$. ◀

Proof of Proposition 18. The proof, by induction on $A \cong A'$, is similar to the proof of Proposition 3. ◀

Proof of Theorem 21 (Adequacy). The proof, by case analysis, is essentially the same as the usual adequacy proof for HA2, since none of the instructions involved in the typing rules allows to change the value of the state. Let us prove the case $(\to_I)$. Writing Γ for the typing context, ρ for a valuation closing all the considered formulas, $\mathfrak{s}$ for the considered state and σ for a substitution such that $(\sigma;\mathfrak{s}) \Vdash \rho(\Gamma)$, by assumption, for any substitution σ' such that $(\sigma';\mathfrak{s}) \Vdash \rho(\Gamma), x:\rho(A)$, we have that $(\sigma(t);\mathfrak{s}) \in |B|_\rho^{\mathfrak{S}}$. We have to prove that $(\lambda x.\sigma(t);\mathfrak{s}) \in |A\to B|_\rho^{\mathfrak{S}}$. Let then u be a term such that $(u;\mathfrak{s}) \in |A|_\rho^{\mathfrak{S}}$. By definition, we have $\lambda x.\sigma(t)\,u\ {}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}}\ \sigma(t)[u/x]$. Since $\sigma(t)[u/x] = (\sigma, x:=u)(t)$ and $(\sigma, x:=u;\mathfrak{s}) \Vdash \rho(\Gamma, x:A)$, we obtain $(\sigma(t)[u/x];\mathfrak{s}) \in |B|_\rho^{\mathfrak{S}}$. We conclude that $(\lambda x.\sigma(t)\,u;\mathfrak{s}) \in |B|_\rho^{\mathfrak{S}}$ by anti-reduction. ◀

Proof of Proposition 23. Let $\mathbb{X}:\mathbb{N}\to\mathbf{SAT}$ be a predicate, $\mathfrak{s}\in\mathfrak{S}$, $f\in\mathbb{N}^{\mathfrak{S}}$, u_0 and u_S be terms, and V be a value such that $(u_0;\mathfrak{s}) \in \mathbb{X}(0)$, $(u_S;\mathfrak{s}) \in |\forall^{\mathbb{N}}y.(X(y)\to X(S(y)))|_{X\mapsto\mathbb{X}}^{\mathfrak{S}}$ and $(\overline{n};\mathfrak{s}) \in |\mathrm{Nat}(f)|^{\mathfrak{S}}$. The latter implies that $n = f(\mathfrak{s})$. The result follows from the fact that $\mathsf{rec}\ u_0\,u_S\,\overline{n} \in \mathbb{X}(n)$, which is proved by induction on n. ◀

B.3 Glueing

Proof of Theorem 26 (Glueing). The proof is by induction on the structure of A. ◀

Proof of Proposition 27. We consider $\mathcal{F}:(n_1,\ldots,n_k)\mapsto |B[x_1:=n_1^*,\ldots,x_k:=n_k^*]|_\rho^{\mathfrak{S}}$ which defines a function from $\mathbb{N}^k$ to $\mathbf{SAT}$. By an easy induction on A, we show using the glueing theorem and Definition 13 that $|A|_{\rho,X\mapsto\mathcal{F}}^{\mathfrak{S}} = |A[X(x_1,\ldots,x_k):=B]|_\rho^{\mathfrak{S}}$. ◀

B.4 Natural numbers

▶ **Proposition 48**. *Let $f \in \mathbb{N}^{\mathfrak{S}}$ and $\mathfrak{s} \in \mathfrak{S}$. If t is a term such that $(t; \mathfrak{s}) \in |\mathrm{Nat}'(f)|^{\mathfrak{S}}$, then $t\,\lambda x.x\,{}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}}\,\overline{n}$, where $n = f(\mathfrak{s})$.*

Proof. Let us define $\mathbb{X} \triangleq \{(t; \mathfrak{s}') : t\,{}^{\mathfrak{s}}{\downarrow}'\ \mathfrak{s}\overline{n}\}$. This set is clearly saturated, and it is easy to see that $(\lambda x.x; \mathfrak{s}) \in |\{\mathrm{Nat}(f)\} \mapsto \mathbb{X}|^{\mathfrak{S}}$ (since $\lambda x.x\,\overline{n}\,{}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}}\,\overline{n}$). Therefore, we have that $t \in |(\{\mathrm{Nat}(f)\} \mapsto \mathbb{X}) \to \mathbb{X}|^{\mathfrak{S}}$ and then $(t\,\lambda x.x; \mathfrak{s}) \in \mathbb{X}$, that is $t\,\lambda x.x\,{}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}}\,\overline{n}$. ◀

Proof of Proposition 29. Easy realizability proofs by anti-reduction. ◀

▶ **Lemma 49.** *Let $\mathfrak{s} \in \mathfrak{S}$ and t, u be terms.*

1. *For any $n \in \mathbb{N}$, if $u\,{}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}}\,\overline{n}$, then $T\,t\,u\,{}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}}\,t\,\overline{n}$.*
2. *For any $f \in \mathbb{N}^{\mathfrak{S}}$, if $u\,{}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}}\,\overline{f(\mathfrak{s})}$ and $(t; \mathfrak{s}) \in |\forall^{\{\mathbb{N}\}}x.A(x)|^{\mathfrak{S}}$, then $T\,t\,u \in |A(f)|^{\mathfrak{S}}$.*

Proof. The first part is an easy induction on n, and the second part follows from the first by anti-reduction. ◀

Proof of Proposition 30. The first three parts are easy, and the fourth one is similar to Proposition 12 using Lemma 49. ◀

Proof of Proposition 32. 1. If either f or g is not standard, the result is trivial. Assume that f and g are standard. If $f \neq g$, we have $|(\forall Z.(Z(f) \mapsto Z(g))|^{\mathfrak{S}} = |\top \mapsto \bot|^{\mathfrak{S}}$, while the case $f = g$ is trivial.

2. The result easily follows from Proposition 27. ◀

B.5 Nonstandard reasoning principles

Proof of Theorem 33 (Transfer). Parts 1 and 4 follow from the glueing theorem, while parts 2 and 3 (resp. 5, 6) are direct consequences of the first (resp. fourth) part. ◀

Proof of Proposition 34. Both statements follow by unfolding the definitions. ◀

Proof of Proposition 35. Let $\mathfrak{s}$ be a state, $n \in \mathbb{N}$ and u_0, u_S be terms and V be a value such that $(u_0; \mathfrak{s}) \in |A(0^*)|^{\mathfrak{S}}$, $(u_S; \mathfrak{s}) \in |\forall^{\mathrm{st}}y.(A(y) \to A(S(y))|^{\mathfrak{S}}$ and $(V; \mathfrak{s}) \in |\mathrm{Nat}(n^*)|^{\mathfrak{S}}$. The latter implies that $V = \overline{n}$. The result follows from the fact that $\mathsf{rec}\ u_0\,u_S\,\overline{n} \in |A(n^*)|^{\mathfrak{S}}$, which is proved by induction on n. ◀

Proof of Proposition 36 (Overspill). We show that $((\lambda x.(x\,t, t))u; \mathfrak{s}) \Vdash \exists x.(\neg\mathrm{st}(x) \wedge A(x))$ where $(u; \mathfrak{s}) \Vdash \forall^{\mathrm{st}}x.A(x)$. Following the proof of part 3 in Theorem 33, we obtain that $(u\,t; \mathfrak{s}) \Vdash \forall x.A(x)$ and consequently $(u\,t; \mathfrak{s}) \Vdash A(\delta)$. By ENS_0 (Proposition 30), we have $(t; \mathfrak{s}) \Vdash \neg\mathrm{st}(\delta)$. Then $((u\,t, t); \mathfrak{s}) \Vdash \exists x.(\neg\mathrm{st}(x) \wedge A(x))$ and we conclude by anti-reduction. ◀

Proof of Proposition 37 (Underspill). Let u and v be terms s.t. $(u; \mathfrak{s}) \Vdash \forall x.\neg\mathrm{st}(x) \to A(x)$ and $(v; \mathfrak{s}) \Vdash \neg\exists^{\mathrm{st}}x.A(x)$. Using Proposition 18, we get that $(v; \mathfrak{s}) \Vdash \forall x.((\mathrm{st}(x) \wedge A(x)) \to \bot)$, and by currying $(\lambda wz.v\,(w, z); \mathfrak{s}) \Vdash \forall^{\mathrm{st}}x.A(x) \to \bot$.

Since A is internal, by transfer, we obtain that$(\lambda z.v\,(t, z); \mathfrak{s}) \Vdash \forall x.A(x) \to \bot$. By the hypothesis on u and ENS_0, we have $(u\,t; \mathfrak{s}) \Vdash A(\delta)$, hence $(\lambda z.v\,(t, z))(u\,t); \mathfrak{s}) \Vdash \bot$, and we can conclude by anti-reduction. ◀

B.6 Idealization

Proof of Proposition 38 (Diagonalization). Let $\mathfrak{s}$ be an arbitrary state. Following the proof of part 2 of Lemma 49, it is clearly enough to prove that $(\lambda xy.\,\mathsf{set}\ y\,\dagger;\mathfrak{s}) \Vdash \forall^{\{\mathrm{st}\}}y.y \leq \delta$ (the rest of the proof is exactly the same replacing $\neg\mathrm{st}(\delta)$ by $\forall^{\{\mathrm{st}\}}y.y \leq \delta$). Let $n \in \mathbb{N}$ and t an arbitrary term. Then

$$(\lambda xy.\,\mathsf{set}\ y\,t)\,t\,\overline{n}\ \ {}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}}\ \ \mathsf{set}\ \overline{n}\,t\ \ {}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}'}\ \ t$$

where $\mathfrak{s}' = \max(n,\mathfrak{s})$. In particular, $n \leq \delta(\mathfrak{s}')$ holds, hence $(t;\mathfrak{s}') \in |n \leq \delta|^{\mathfrak{S}}$ and we can conclude by anti-reduction. ◀

Proof of Lemma 40. The proof is analogous to the proof of Proposition 10. ◀

Recall that we define $\mathsf{ideal} \triangleq \lambda x.\lambda y.T\,y\,(\pi_1(T\,(x\,\dagger)\ \mathsf{get}\,(\lambda wyz.(y,z)))\,(\lambda yz.\,\mathsf{set}\ z\,y)$.

Proof of Theorem 41 (Idealization). Let $\mathfrak{s}$ be any state and let u be a term such that $(u;\mathfrak{s}) \in |\forall^{\{\mathrm{st}\}}n.\exists^{\{\mathrm{st}\}}x.\forall^{\{\mathrm{st}\}}y.(y \leq n \to R(x,y))|^{\mathfrak{S}}$. By part 2 of Lemma 49, this entails that

$$(T\,(u\,\dagger)\ \mathsf{get};\mathfrak{s}) \in |\exists^{\{\mathrm{st}\}}x.\forall^{\{\mathrm{st}\}}y.(y \leq \mathfrak{s} \to R(x,y))|^{\mathfrak{S}}_{\rho}.$$

By Lemma 40, we know that there exists a natural number $p_{\mathfrak{s}} \in \mathbb{N}$ and a term $v_{\mathfrak{s}} \in \Lambda$ such that $T\,(u\,\dagger)\ \mathsf{get}\,(\lambda zxy.(x,y))\ {}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}}\ (\overline{p_{\mathfrak{s}}},v_{\mathfrak{s}})$ and $(v_{\mathfrak{s}};\mathfrak{s}) \in |\forall^{\{\mathrm{st}\}}y.(y \leq \mathfrak{s} \to R(p_{\mathfrak{s}},y))|^{\mathfrak{S}}$. The latter implies that for any $m \in \mathbb{N}$ such that $m \leq \mathfrak{s}$ and any term t, it holds that $(v_{\mathfrak{s}}\,t\,\overline{m}\,t;\mathfrak{s}) \in |R(p_{\mathfrak{s}},m)|^{\mathfrak{S}}$ and hence $R(p_{\mathfrak{s}},m)$ holds (otherwise $|R(p_{\mathfrak{s}},m)|_{\mathfrak{s}} = \emptyset$).

Consider the (nonstandard) individual $\tau \in \mathbb{N}^{\mathfrak{S}}$ defined by $\tau(\mathfrak{s}) = p_{\mathfrak{s}}$. We have

$$\mathsf{ideal}\ u\ \ {}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}}\ \ \lambda y.T\,y\,(\pi_1(T\,(u\,\dagger)\ \mathsf{get}\,(\lambda wyz.(y,z))))\,(\lambda yz.\,\mathsf{set}\ z\,y)$$

hence, by part 2 of Lemma 49, to conclude by anti-reduction it suffices to prove that

1. $\underline{\pi_1(T\,(u\,\dagger)\ \mathsf{get}\,(\lambda wyz.(y,z)))\ {}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}}\ \overline{\tau(\mathfrak{s})}}$. Indeed, we know that this term reduces as follows:

   $$\pi_1(T\,(u\,\dagger)\ \mathsf{get}\,(\lambda wyz.(y,z)))\ {}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}}\ \pi_1(\overline{p_{\mathfrak{s}}},v_{\mathfrak{s}})\ {}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}}\ \overline{p_{\mathfrak{s}}}$$

   and by definition $\tau(\mathfrak{s}) = p_{\mathfrak{s}}$.
2. $\underline{(\lambda yz.\,\mathsf{set}\ z\,y;\mathfrak{s}) \Vdash \forall^{\{\mathrm{st}\}}y.R(\tau,y)}$. To prove this, it suffices to show that for any $m \in \mathbb{N}$ and any $t \in \Lambda$, we have $((\lambda yz.\,\mathsf{set}\ z\,y)\,t\,\overline{m};\mathfrak{s}) \Vdash R(\tau,m^*)$. With $\mathfrak{s}' \triangleq \max(\mathfrak{s},m)$, we have that $(\lambda yz.\,\mathsf{set}\ z\,y)\,t\,\overline{m}\ {}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}}\ \mathsf{set}\ \overline{m}\,t\ {}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}'}\ t$. By construction, since $m \leq \mathfrak{s}'$, we know that $R(\tau(\mathfrak{s}'),m)$ holds, hence $(t;\mathfrak{s}') \in |R(\tau(\mathfrak{s}'),m)|^{\mathfrak{S}}_{\rho}$ and we conclude by anti-reduction. ◀

C Realizability up to $\mathcal{U}$

Proof of Proposition 42. Follows from the fact that for any nonstandard $f \in \mathbb{N}^{\mathfrak{S}}$, any $n \in \mathbb{N}$ and any $\mathfrak{s} \in \mathfrak{S}$, there exists $\mathfrak{s}' \in \mathfrak{S}$ such that $\mathfrak{s}' > \mathfrak{s}$ and $n < f(\mathfrak{s}')$. The result then follows by anti-reduction from the fact that $\mathsf{loop}^{+}\ {}^{\mathfrak{s}}{\downarrow}^{\mathfrak{s}'}\ \mathsf{loop}^{+}$. ◀

We give here the quotiented interpretation referred to in Section 6.1.

▶ **Definition 50** (Realizability up to $\mathcal{U}$). *The interpretation of a formula A together with a valuation ρ is the set $|A|^{*}_{\rho}$ defined inductively according to the following clauses:*

$$\begin{array}{rcl}
|\mathrm{st}(f)|^*_\rho & \triangleq & \begin{cases} \Lambda & \textit{if } f \cong n^*, \textit{ for some } n \in \mathbb{N} \\ \emptyset & \textit{otherwise} \end{cases} \\
|X(e_1,\dots,e_n)|^*_\rho & \triangleq & \{t \in \Lambda : \{\mathfrak{s} \in \mathfrak{S} : (t;\mathfrak{s}) \in \rho(X)@(\llbracket e_1 \rrbracket_\rho,\dots,\llbracket e_n \rrbracket_\rho)\} \in \mathcal{U}\} \\
|\{\mathrm{Nat}(e)\} \mapsto A|^*_\rho & \triangleq & \{t \in \Lambda : \{\mathfrak{s} \in \mathfrak{S} : (t;\mathfrak{s}) \in |\{\mathrm{Nat}(e)\} \mapsto A|^{\mathfrak{S}}_\rho\} \in \mathcal{U}\}\} \\
|A \to B|^*_\rho & \triangleq & \{t \in \Lambda : \{\mathfrak{s} \in \mathfrak{S} : (t;\mathfrak{s}) \in |A \to B|^{\mathfrak{S}}_\rho\} \in \mathcal{U}\} \\
|A_1 \wedge A_2|^*_\rho & \triangleq & \{t \in \Lambda : \{\mathfrak{s} \in \mathfrak{S} : (\pi_1(t);\mathfrak{s}) \in |A_1|^{\mathfrak{S}}_\rho \wedge (\pi_2(t);\mathfrak{s}) \in |A_2|^{\mathfrak{S}}_\rho\} \in \mathcal{U}\}
\end{array}$$

$$|A_1 \vee A_2|^*_\rho \triangleq \{t \in \Lambda : \{\mathfrak{s} \in \mathfrak{S} : \exists i \in \{1,2\}.\, \mathsf{case}\ t\,\{\iota_1(x_1) \mapsto x_1 | \iota_2(x_2) \mapsto x_2\} \in |A_i|^{\mathfrak{S}}_\rho\} \in \mathcal{U}\}$$

$$\begin{array}{rclr}
|\forall x.A|^*_\rho & \triangleq & \bigcap_{f \in \mathbb{N}^{\mathfrak{S}}} |A|^*_{\rho,x\mapsto f} & |\forall X.A|^*_\rho \triangleq \bigcap_{F:\mathbb{N}^k \to \mathbf{SAT}} |A|^*_{\rho,X\mapsto F} \\
|\exists x.A|^*_\rho & \triangleq & \bigcup_{f \in \mathbb{N}^{\mathfrak{S}}} |A|^*_{\rho,x\mapsto f} & |\exists X.A|^*_\rho \triangleq \bigcup_{F:\mathbb{N}^k \to \mathbf{SAT}} |A|^*_{\rho,X\mapsto F}
\end{array}$$

We write $t \Vdash^* A$ if $t \in |A|^*$.

As explained in Section 6.1, this definition is meant to satisfy a counterpart of Łoś' theorem in our setting.

Proof of Theorem 44 (Łoś' theorem). The proof goes by induction on the structure of A. In the cases $\{\mathrm{Nat}(e)\} \mapsto A$, $X(e_1,\dots,e_n)$, $A \to B$, $A \vee B$ and $A \wedge B$, the result follows directly from the definitions. The proof for quantifiers is similar to the usual proof of Łoś' theorem, we only give here the case of the existential quantifier.

Case $\exists x.A$ By the induction hypothesis, we have that for any $f \in \mathbb{N}^{\mathfrak{S}}$,

$$|A|^*_{\rho,x\mapsto f} = \{t : \{\mathfrak{s} \in \mathfrak{S} : t;\mathfrak{s} \in |A|^{\mathfrak{S}}_{\rho,x\mapsto f}\} \in \mathcal{U}\}$$

By glueing, we have that $|A|^{\mathfrak{S}}_{\rho,x\mapsto f} = |\overline{A}^{\mathfrak{s}}|^{\mathfrak{s}}_{\rho,x\mapsto f} = |\overline{A}^{\mathfrak{s}}|^{\mathfrak{s}}_{\rho,x\mapsto (f(\mathfrak{s}))^*}$. We want to prove that for any $t \in \Lambda$

$$\exists f \in \mathbb{N}^{\mathfrak{S}}.t \in |A|^*_{\rho,x\mapsto f} \text{ iff } \{\mathfrak{s} \in \mathfrak{S} : t;\mathfrak{s} \in |\exists x.A|^{\mathfrak{S}}_\rho\} \in \mathcal{U}$$

Observe that, by glueing, the right-hand side is equivalent to $\{\mathfrak{s} \in \mathfrak{S} : \exists n \in \mathbb{N}.t \in |A|^{\mathfrak{s}}_{\rho,x\mapsto n^*}\} \in \mathcal{U}$.

$\underline{\Rightarrow|}$ If there exists $f \in \mathbb{N}^{\mathfrak{S}}$ such that $t \in |A|^*_{\rho,x\mapsto f}$. We easily see that

$$\{\mathfrak{s} \in \mathfrak{S} : t \in |A|^{\mathfrak{s}}_{\rho,x\mapsto (f(\mathfrak{s}))^*}\} \subseteq \{\mathfrak{s} \in \mathfrak{S} : \exists n \in \mathbb{N}.t \in |A|^{\mathfrak{s}}_{\rho,x\mapsto n^*}\}$$

hence we can conclude by upwards closure of the ultrafilter.

$\underline{\Leftarrow|}$ Assume that $E \triangleq \{\mathfrak{s} \in \mathfrak{S} : \exists n \in \mathbb{N}.t \in |A|^{\mathfrak{s}}_{\rho,x\mapsto n^*}\} \in \mathcal{U}$

For any $\mathfrak{s} \in E$, using countable choice we can pick an integer $n_{\mathfrak{s}}$ such that $t \in |A|^{\mathfrak{s}}_{\rho,x\mapsto n^*_{\mathfrak{s}}}$. We may then define the function $g \in \mathbb{N}^{\mathfrak{S}}$ by $g(\mathfrak{s}) \triangleq n_{\mathfrak{s}}$ if $\mathfrak{s} \in E$, 0 otherwise. By definition, $E \subseteq \{\mathfrak{s} \in \mathfrak{S} : t \in |A|^{\mathfrak{s}}_{\rho,x\mapsto (g(\mathfrak{s}))^*}\}$, hence this set belongs to $\mathcal{U}$ by upwards closure. Therefore we can conclude by induction hypothesis that $t \in |A|^*_{\rho,x\mapsto f}$. ◀

▶ **Proposition 51.** *For any internal formulas A and B, and any valuation ρ closing both A and B, we have $|A \to B|^*_\rho \subseteq \{t : \forall u \in |A|^*_\rho.t\,u \in |B|^*_\rho\}$.*

Proof. For any term t and any formula A, let us denote by S^A_t the set $\{\mathfrak{s} \in \mathfrak{S} : (t;\mathfrak{s}) \in |A|^{\mathfrak{S}}_\rho\}$. Let $t \in \Lambda$ be such that $S^{A\to B}_t \in \mathcal{U}$ and $u \in |A|^*_\rho$. By hypothesis, $S^A_u \in \mathcal{U}$. We need to show that $tu \in |B|^*_\rho$. Again, for any $\mathfrak{s} \in S^{A\to B}_t \cap S^A_u \in \mathcal{U}$, we have $tu;\mathfrak{s} \in |B|^{\mathfrak{S}}_\rho$. By upwards closure, we deduce that $\{\mathfrak{s} : (tu;\mathfrak{s}) \in |B|^{\mathfrak{S}}_\rho\} \in \mathcal{U}$, hence $tu \in |B|^*_\rho$, and the result follows from Theorem 44. ◀

▶ Remark 52. One could have been tempted to define the truth value $|A \to B|_\rho^*$ as the set of terms t such that for any $u \in |A|_\rho^*$, $t\,u \in |B|_\rho^*$, as is usual in realizability. Unfortunately, such a definition is incompatible with Theorem 44, as the other inclusion in Proposition 51 does not hold. To see this, let $A \triangleq \mathrm{Nat}'(\tau)$ and $B \triangleq \bot$ where τ is a non-computable function[7] $\tau : \mathfrak{S} \to \mathbb{N}$ for which there is no term u such that $\forall \mathfrak{s}. u\ {}^{\mathfrak{s}}\!\!\downarrow^{\mathfrak{s}} \tau(\mathfrak{s})$. By construction, we have that $|A|^* = \emptyset$, so that obviously for any $u \in |\mathrm{Nat}'(\tau)|^*$, the function $(\lambda x.x)\,u \in |\bot|^*$. Yet, for each state $\mathfrak{s}$ the truth value $|\mathrm{Nat}'(\tau)|_\rho^{\mathfrak{S}}$ is not empty (it contains at least $(\overline{n}, \mathfrak{s})$, for $n = \tau(\mathfrak{s})$) and therefore $(\lambda x.x; \mathfrak{s}) \notin |\mathrm{Nat}'(\tau) \to \bot|_\rho^{\mathfrak{S}}$ (since for any $(u; \mathfrak{s}) \in |\mathrm{Nat}'(\tau)|^{\mathfrak{S}}$, $(\lambda x.x\,u; \mathfrak{s}) \notin |\bot|^*$).

We want to point out that Remark 52 highlights the "counter-intuitive" peculiarities of the interpretation up to $\mathcal{U}$ with respect to the quotient in the Lightstone-Robinson construction. The latter indeed appears to be more regular, seemingly for two main reasons. First, as we highlight in Section 4, in the stateful interpretation the set instruction allows terms to change the value of the states during computations, and thus of the slices. This phenomenon does not occur in the Lightstone-Robinson construction where slices of the product are complety isolated between them. Second, while the Lightstone-Robinson construction is based on Boolean-valued models, realizability interpretations associate to each formula a set of realizers (instead of one unique Boolean). Besides, the use of relativized quantifiers (for instance in the statement for idealization) forces us to use only computable functions[8].

[7] To that end, one can for instance consider the function τ which to each $\mathfrak{s} \in \mathfrak{S}$ associates the smallest natural number $n \in \mathbb{N}$ such that there is no term of size smaller than or equal to $\mathfrak{s}$ that computes n the state $\mathfrak{s}$: $\tau(\mathfrak{s}) \triangleq \inf\{n \in \mathbb{N} : \neg\exists t. |t| \leq \mathfrak{s} \wedge t\ {}^{\mathfrak{s}}\!\!\downarrow^{\mathfrak{s}} \overline{n}\}$.

[8] This is the reason why, for instance, the premise of idealization needs to be restricted to the existence of a *standard* natural number x, instead of any natural number as is usually the case.