Realizability and Parametricty in Pure Type Systems

Jean-Philippe Bernardy[1] and Marc Lasson[2]

[1] Chalmers University of Technology and University of Gothenburg
[2] ENS Lyon, Université de Lyon, LIP (UMR 5668 CNRS ENS Lyon UCBL INRIA)

Abstract. We describe a systematic method to build a logic from any programming language described as a Pure Type System (PTS). The formulas of this logic express properties about programs. We define a parametricity theory about programs and a realizability theory for the logic. The logic is expressive enough to internalize both theories. Thanks to the PTS setting, we abstract most idiosyncrasies specific to particular type theories. This confers generality to the results, and reveals parallels between parametricity and realizability.

1 Introduction

During the past decades, a recurring goal among logicians was to give a computational interpretation of the reasoning behind mathematical proofs. In this paper we adopt the converse approach: we give a systematical way to build a logic from a programming language. The structure of the programming language is replicated at the level of the logic: the expressive power of the logic (e.g. the ability of expressing conjunctions) is directly conditioned by the constructions available in the programming language (e.g. presence of products).

We use the framework of Pure Type Systems (PTS) to represent both the starting programming language and the logic obtained by our construction. A PTS [2, 3] is a generalized λ-calculus where the syntax for terms and types are unified. Many systems can be expressed as PTSs, including the simply typed λ-calculus, Girard and Reynolds polymorphic λ-calculus (System F) and its extension system Fω, Coquand's Calculus of Constructions, as well as some exotic, and even inconsistent systems such as λU [8]. PTSs can model the functional core of many modern programming languages (Haskell, Objective Caml) and proof assistants (Coq [25], Agda [19], Epigram [17]). This unified framework provides meta-theoretical such as substitution lemmas, subject reduction and uniqueness of types.

In the Sec. 3, we describe a transformation which maps any PTS P to a PTS P^2. The starting PTS P will be viewed as a programming language in which live *types* and *programs* and P^2 will be viewed as a proof system in which live *proofs* and *formulas*. The logic P^2 is expressive enough to state properties about the programs. It is therefore a setting of choice to develop a parametricity and a realizability theory.

Parametricity. Reynolds [23] originally developed the theory of parametricity to capture the meaning of types of his polymorphic λ-calculus (equivalent to Girard's System F). Each closed type can be interpreted as a predicate that all its inhabitants satisfy. Reynolds' approach to parametricity has proven to be a successful tool: applications range from program transformations to speeding up program testing [28, 7, 4].

Parametricity theory can be adapted to other λ-calculi, and for each calculus, parametricity predicates are expressed in a corresponding logic. For example, Abadi et al. [1] remark that the simply-typed corresponds to LCF [18]. For System F, predicates can be expressed in second order predicate logic, in one or another variant [1, 16, 29]. More recently, Bernardy et al. [5] have shown that parametricity conditions for a reflective PTS can be expressed in the PTS itself.

Realizability. The notion of realizability was first introduced by Kleene [10] in his seminal paper. The idea of relating programs and formulas, in order to study their constructive content, was then widely used in proof theory. For example, it provides tools for proving that an axiom is not derivable in a system (excluded middle in [11, 26]) or that intuitionistic systems satisfy the *existence property*[3] [9, 26]; see Van Oosten [27] for an historical account of realizability.

Originally, Kleene represented programs as integers in a theory of recursive functions. Later, this technique has been extended to other notions of programs like combinator algebra [24, 26] or terms of Gödel's system T [12, 26] in Kreisel's modified realizability. In this article, we generalize the latter approach by using an arbitrary pure type system as the language of programs.

Krivine [13] and Leivant [15] have used realizability to prove Girard's representation theorem[4] [8] and to build a general framework for extracting programs from proofs in second-order logic [14]. In this paper, we extend Krivine's methodology to languages with dependent types, like Paulin-Mohring [20, 21] did with the realizability theory behind the program extraction in the Coq proof assistant [25].

Contributions. Viewed as syntactical notions, realizability and parametricity bear a lot of similarities. Our aim was to understand trough the generality of PTSs how they are related. Our main contributions are:

- The general construction of a logic from the programming language of its realizers with syntactic definitions of parametricity and realizability (Sec. 3).
- The proof that this construction is strongly normalizing if the starting programming language is (Thm. 2).
- A characterization of both realizability in terms of parametricity (Thm. 6) and parametricity in terms of realizability (Thm. 5).

[3] If $\forall x \exists y, \varphi(x, y)$ is a theorem, then there exists a program f such that $\forall x, \varphi(x, f(x))$.
[4] Functions definable in system F are exactly those provably total in second-order arithmetic.

2 The First Level

In this section, we recall basic definitions and theorems about pure types systems (PTSs). We refer the reader to [2] for a comprehensive introduction to PTSs. PTSs are defined by a specification $(\mathcal{S}, \mathcal{A}, \mathcal{R})$ where $\mathcal{S}$ is a set of *sorts*, $\mathcal{A} \subseteq \mathcal{S} \times \mathcal{S}$ a set of *axioms* and $\mathcal{R} \subseteq \mathcal{S} \times \mathcal{S} \times \mathcal{S}$ a set of *rules*. This specification parametrizes both the syntax of term and the rules of the type system.

A PTS is defined by a specification $(\mathcal{S}, \mathcal{A}, \mathcal{R})$ where $\mathcal{S}$ is a set of *sorts*, $\mathcal{A} \subseteq \mathcal{S} \times \mathcal{S}$ a set of *axioms* and $\mathcal{R} \subseteq \mathcal{S} \times \mathcal{S} \times \mathcal{S}$ a set of *rules*, with determines the typing of product types. The typing judgement is written $\Gamma \vdash A : B$. The notation $\Gamma \vdash A : B : C$ is a shorthand for having both $\Gamma \vdash A : B$ and $\Gamma \vdash B : C$ simultaneously.

Example 1 (System F*).* The PTS F has the following specification:

$$\mathcal{S}_{\mathrm{F}} = \{\star, \Box\} \qquad \mathcal{A}_{\mathrm{F}} = \{(\star, \Box)\} \qquad \mathcal{R}_{\mathrm{F}} = \{(\star, \star, \star), (\Box, \star, \star)\}.$$

It defines the λ-calculus with polymorphic types known as system F [8] and is our running example. The rule $(\star, \star, \star)$ corresponds to the formation of arrow types (usually written $\sigma \to \tau$) and the rule $(\Box, \star, \star)$ corresponds to quantification over types $(\forall \alpha, \tau)$.

Even though we use F as a running example throughout the article to illustrate our general definitions our results apply to any PTS.

Sort annotations. We sometimes decorate terms with *sort annotations*. They function as a syntactic reminder of the first component of the rule used to type a product. We divide the set of variables into disjoint infinite subsets $\mathcal{V} = \bigsqcup\{\mathcal{V}_s | s \in \mathcal{S}\}$ and we write x^s to indicate that a variable x belongs to $\mathcal{V}_s$. We also annotate applications $F\,a$ with the sort of the variable of the product type of F. Using this notation, the product rule and the application rule are written

$$\frac{\Gamma \vdash A : s_1 \qquad \Gamma, x^{s_1} : A \vdash B : s_2}{\Gamma \vdash (\Pi x^{s_1} : A.\, B) : s_3}\ (s_1, s_2, s_3) \in \mathcal{R}\ \textsc{Product} \qquad \frac{\Gamma \vdash F : (\Pi x^s : A.\, B) \qquad \Gamma \vdash a : A}{\Gamma \vdash (F\,a)_s : B[x \mapsto a]}\ \textsc{Application}.$$

Since sort annotations can always be recovered by using the type derivation, we do not write them in our examples.

Example 2 (System F *terms).* In system F, we adopt the following convention: the letters x, y, z, ... range over $\mathcal{V}_\star$, and α, β, γ, ... over $\mathcal{V}_\Box$. Here are some examples using that notation:

- The identity program $\mathrm{Id} \equiv \lambda(\alpha : \star)(x : \alpha).x$ of type $\mathrm{Unit} \equiv \Pi\alpha : \star.\alpha \to \alpha$.
- The Church numeral $0 \equiv \lambda(\alpha : \star)(f : \alpha \to \alpha)(x : \alpha).x$ is a program of type $\mathrm{Nat} \equiv \Pi\alpha : \star.(\alpha \to \alpha) \to (\alpha \to \alpha)$.
- The successor function on Church numerals $\mathrm{Succ} \equiv \lambda(n : \mathrm{Nat})(\alpha : \star)(f : \alpha \to \alpha)(x : \alpha).f\,(n\,\alpha\,f\,x)$ is a program of type $\mathrm{Nat} \to \mathrm{Nat}$.

3 The Second Level

In this section we describe the logic to reason about the programs and types written in an arbitrary PTS P, as well as basic results concerning the consistency of the logic. This logic is also a PTS, which we name P^2. Because we carry out most of our development in P^2, judgments refer to that system unless the symbol $\vdash$ is subscripted with the name of a specific system.

Definition 1 (second-level system). *Given a PTS $P = (\mathcal{S}, \mathcal{A}, \mathcal{R})$, we define $P^2 = (\mathcal{S}^2, \mathcal{A}^2, \mathcal{R}^2)$ by*

$$\begin{aligned}
\mathcal{S}^2 &= \mathcal{S} \cup \{\lceil s \rceil \mid s \in \mathcal{S}\} \\
\mathcal{A}^2 &= \mathcal{A} \cup \{(\lceil s_1 \rceil, \lceil s_2 \rceil) \mid (s_1, s_2) \in \mathcal{A}\} \\
\mathcal{R}^2 &= \mathcal{R} \cup \{(\lceil s_1 \rceil, \lceil s_2 \rceil, \lceil s_3 \rceil), (s_1, \lceil s_3 \rceil, \lceil s_3 \rceil) \mid (s_1, s_2, s_3) \in \mathcal{R}\} \\
&\quad \cup \{(s_1, \lceil s_2 \rceil, \lceil s_2 \rceil) \mid (s_1, s_2) \in \mathcal{A}\}
\end{aligned}$$

Because we see P as a programming language and P^2 as a logic for reasoning about programs in P, we adopt the following terminology and conventions. We use the metasyntactic variables $s, s_1, s_2, \ldots$ to range over sorts in $\mathcal{S}$ and $t, t_1, t_2, \ldots$ to range over sorts in $\mathcal{S}^2$. We say that a term is

- a *type* if it inhabits a first-level sort (s),
- a *formula* if it inhabits a second-level sort ($\lceil s \rceil$),
- a *program* if it inhabits a type,
- a *proof* if it inhabits a formula.

We also say that types and programs are *first-level* terms, and formulas and proofs are *second-level* terms.

If s is a sort of P, then $\lceil s \rceil$ is the sort of formulas expressing properties of types of sort s. For each rule (s_1, s_2, s_3) in $\mathcal{R}$,

- $(\lceil s_1 \rceil, \lceil s_2 \rceil, \lceil s_3 \rceil)$ maps constructs of the programming language at the level of the logic,
- $(s_1, \lceil s_3 \rceil, \lceil s_3 \rceil)$ allows to build the quantification of programs of sort s_1 in formulas of sort $\lceil s_3 \rceil$.

For each axiom (s_1, s_2) in $\mathcal{A}$, we add the rule $(s_1, \lceil s_2 \rceil, \lceil s_2 \rceil)$ in order to build the type of predicates of sort $\lceil s_2 \rceil$ parametrized by programs of sort s_1.

Example 3. The PTS F^2 has the following specification:

$$\begin{aligned}
\mathcal{S}^2_{\mathrm{F}} &= \{ \quad \star, \Box, \lceil\star\rceil, \lceil\Box\rceil \quad \} \\
\mathcal{A}^2_{\mathrm{F}} &= \{ \quad (\star, \Box), (\lceil\star\rceil, \lceil\Box\rceil) \quad \} \\
\mathcal{R}^2_{\mathrm{F}} &= \{ \ (\star,\star,\star), (\Box,\star,\star), (\lceil\star\rceil, \lceil\star\rceil, \lceil\star\rceil), (\lceil\Box\rceil, \lceil\star\rceil, \lceil\star\rceil) \\
&\qquad (\star, \lceil\Box\rceil, \lceil\Box\rceil), (\star, \lceil\star\rceil, \lceil\star\rceil), (\Box, \lceil\star\rceil, \lceil\star\rceil) \quad \}.
\end{aligned}$$

We extend our variable-naming convention to $\mathcal{V}_{\lceil\star\rceil}$ and $\mathcal{V}_{\lceil\Box\rceil}$ as follows:

- the variables h, h_1, h_2, ... range over $\mathcal{V}_{\lceil\star\rceil}$,

– and the variables X, Y, Z, ... range over $\mathcal{V}_{\lceil\Box\rceil}$.

The logic F^2 is a second-order logic with typed individuals (Wadler [29] gives another presentation of the same system).

– The rule $(\lceil\star\rceil, \lceil\star\rceil, \lceil\star\rceil)$ allows to build implication between formulas, written $P \to Q$.
– The rule $(\lceil\star\rceil, \lceil\star\rceil, \lceil\star\rceil)$ allows to quantify over individuals (as in $\Pi x : \tau.P$).
– The rule $(\Box, \lceil\star\rceil, \lceil\star\rceil)$ allows to quantify over types (as in $\Pi\alpha : \star.P$).
– The rule $(\star, \lceil\Box\rceil, \lceil\Box\rceil)$ is used to build types of predicates depending on programs, which are of the form $\tau_1 \to \cdots \to \tau_n \to \lceil\star\rceil$.
– The rule $(\lceil\Box\rceil, \lceil\star\rceil, \lceil\star\rceil)$ allows to quantify over predicates (as in $\Pi X : \tau_1 \to \cdots \to \tau_n \to \lceil\star\rceil.P$).

Here are some examples in F^2.

– Truth can be encoded by $\top \equiv \Pi X : \lceil\star\rceil.X \to X$ and is proved by $\mathrm{Obvious} \equiv \lambda(X : \lceil\star\rceil)(h : X).h$.
– The Leibniz equality $x =_\tau y \equiv \Pi X : \tau \to \lceil\star\rceil.X\,x \to X\,y$ is a formula (where τ is the type of x and y).
– The term $\mathrm{Refl} \equiv \lambda(\alpha : \star)(x : \alpha)(X : \alpha \to \lceil\star\rceil)(h : X\,x).h$ is a proof of the reflexivity of equality $\Pi(\alpha : \star)(x : \alpha).x =_\alpha x$.
– The induction principle over Church numerals is a formula

$$N \equiv \lambda x : \mathrm{Nat}\,.\Pi X : \mathrm{Nat} \to \lceil\star\rceil.(\Pi y : \mathrm{Nat}\,.X\,y \to X\,(\mathrm{Succ}\ y)) \to X\,0 \to X\,x.$$

3.1 Structure of P^2

Programs (or types) can never refer to proofs (nor formulas). In other words, a first-level term never contains a second-level term: it is typable in P. Formally:

Theorem 1 (level separation). *if $\Gamma \vdash A : B : s$ (resp. $\Gamma \vdash B : s$), then there exists a sub-context Γ' of Γ such that $\Gamma' \vdash_P A : B : s$ (resp. $\Gamma' \vdash_P B : s$).*

Proof. By induction on the structure of terms, and relying on the generation lemma [2, 5.2.13] and on the form of the rules in $\mathcal{R}^2$: assuming $(t_1, t_2, t_3) \in \mathcal{R}^2$ then $t_3 \in \mathcal{S} \Rightarrow (t_1 \in \mathcal{S} \wedge t_2 \in \mathcal{S})$ and $t_2 \in \mathcal{S} \Rightarrow (t_1 \in \mathcal{S} \wedge t_3 \in \mathcal{S})$.

Lifting. The major part of the paper is about transformations and relations between the first and the second level. The first and simplest transformation lifts terms from the first level to the second level, by substituting occurrences of a sort s by $\lceil s\rceil$ everywhere (see Fig. 1). The function is defined only on first-level terms, and is extended to contexts in the obvious way. In addition to substituting sorts, lifting performs renaming of a variable x in $\mathcal{V}_s$ to $\mathring{x}$ in $\mathcal{V}_{\lceil s\rceil}$.

Example 4. In F^2, we have $\lceil\mathrm{Unit}\rceil = \lceil\Pi\alpha : \star.\alpha \to \alpha\rceil = \Pi X : \lceil\star\rceil.X \to X = \top$, and $\lceil\mathrm{Nat}\rceil = \Pi X : \lceil\star\rceil.(X \to X) \to (X \to X)$.

$$
\begin{array}{ll}
\ulcorner x \urcorner & = \mathring{x} \\
\ulcorner s \urcorner & = \ulcorner s \urcorner \\
\ulcorner \Pi x : A.\, B \urcorner & = \Pi \mathring{x} : \ulcorner A \urcorner .\, \ulcorner B \urcorner \\
\ulcorner \lambda x : A.\, b \urcorner & = \lambda \mathring{x} : \ulcorner A \urcorner .\, \ulcorner b \urcorner \\
\ulcorner A\, B \urcorner & = \ulcorner A \urcorner\, \ulcorner B \urcorner \\
\hline
\ulcorner <> \urcorner & = <> \\
\ulcorner \Gamma, x : A \urcorner & = \ulcorner \Gamma \urcorner, \mathring{x} : \ulcorner A \urcorner
\end{array}
$$

$$
\begin{array}{ll}
\lfloor x^{\ulcorner s \urcorner} \rfloor & = \dot{x}^s \\
\lfloor \ulcorner s \urcorner \rfloor & = s \\
\lfloor \Pi x^s : A.B \rfloor & = \lfloor B \rfloor \\
\lfloor \Pi x^{\ulcorner s \urcorner} : A.B \rfloor & = \Pi \dot{x}^s : \lfloor A \rfloor . \lfloor B \rfloor \\
\lfloor \lambda x^s : A.B \rfloor & = \lfloor B \rfloor \\
\lfloor \lambda x^{\ulcorner s \urcorner} : A.B \rfloor & = \lambda \dot{x}^s : \lfloor A \rfloor . \lfloor B \rfloor \\
\lfloor (A\, B)_s \rfloor & = \lfloor A \rfloor \\
\lfloor (A\, B)_{\ulcorner s \urcorner} \rfloor & = \lfloor A \rfloor\, \lfloor B \rfloor \\
\hline
\lfloor <> \rfloor & = <> \\
\lfloor \Gamma, x^s : A \rfloor & = \lfloor \Gamma \rfloor \\
\lfloor \Gamma, x^{\ulcorner s \urcorner} : A \rfloor & = \lfloor \Gamma \rfloor, \dot{x}^s : \lfloor A \rfloor .
\end{array}
$$

Fig. 1. lifting (left) and projection (right)

Lemma 1 (lifting preserves typing).
$\Gamma \vdash A : B : s \Rightarrow \ulcorner \Gamma \urcorner \vdash \ulcorner A \urcorner : \ulcorner B \urcorner : \ulcorner s \urcorner$

Proof. A consequence of P^2 containing a copy of P with s mapped to $\ulcorner s \urcorner$.

Lemma 2 (lifting preserves β-reduction).
$A \longrightarrow_\beta B \Rightarrow \ulcorner A \urcorner \longrightarrow_\beta \ulcorner B \urcorner$

Proof. $\ulcorner A \urcorner$ has the same structure as A.

Projection. We define a projection from second-level terms into first-level terms, which maps second-level constructs into first-level constructs. The first-level subterms are removed, as well as the interactions between the first and second levels. The reader may worry that some variable bindings are removed, potentially leaving some occurrences unbound in the body of the transformed term. However, these variables are first level, and hence their occurrences are removed too (by the application case).

The function is defined only on second-level terms, and behaves differently when facing pure second level or interaction terms. In order to distinguish these cases, the projection takes sort-annotated terms as input. Like the lifting, the projection performs renaming of each variable x in $\mathcal{V}_{\ulcorner s \urcorner}$ to $\dot{x}$ in $\mathcal{V}_s$. We postulate that this renaming cancels that of the lifting: we have $\dot{\mathring{x}} = x$.

Example 5 (projections in F^2).

$$
\begin{array}{cc}
\lfloor \top \rfloor = \mathrm{Unit} & \lfloor \mathrm{Obvious} \rfloor = \mathrm{Id} \\
\lfloor \Pi(\alpha : \star)(x : \alpha).x =_\alpha x \rfloor = \mathrm{Unit} & \lfloor N\, t \rfloor = \mathrm{Nat}
\end{array}
$$

Lemma 3 (projection is the left inverse of lifting). $\lfloor \ulcorner A \urcorner \rfloor = A$

Proof. By induction on the structure of A.

Lemma 4 (projection preserves typing).
$\Gamma \vdash A : B : \lceil s \rceil \Rightarrow \lfloor \Gamma \rfloor \vdash \lfloor A \rfloor : \lfloor B \rfloor : s$

Proof. By induction on the derivation $\Gamma \vdash A : B$.

In contrast to lifting, which keeps a term intact, projection may remove parts of a term, in particular abstractions at the interaction level. Therefore, β-reduction steps may be removed by projection.

Lemma 5 (projection preserves or removes β-reduction).
If $A \longrightarrow_\beta B$, then either $\lfloor A \rfloor \longrightarrow_\beta \lfloor B \rfloor$ or $\lfloor A \rfloor = \lfloor B \rfloor$.

3.2 Strong normalization

Theorem 2 (normalization). *If P is strongly normalizing, so is P^2.*

Proof. The proof is based on the observation that, if a term A is typable in P^2 and not normalizable, then at least either:

- one of the first-level subterms of A is not normalizable, or
- the first-level term $\lfloor A \rfloor$ is not normalizable.

Then, by separation (Thm. 1), the first-level subterms are typable in P, so they must be normalizable. We conclude that A must be normalizable. (Details in appendix.)

3.3 Parametricity

In this section we develop Reynolds-style [23] parametricity for P, in P^2. While parametricity theory is often defined for binary relations, we abstract from the arity and develop the theory for an arbitrary arity n, even though we omit the index n when the arity of relations plays no role or is obvious from the context.

The definition of parametricity is done in two parts: first we define what it means for a n-tuple of programs $\overline{z}$ to satisfy the relation generated by a type T ($\overline{z} \in [\![T]\!]_n$); then we define the translation from a program z of type T to a proof $[\![z]\!]_n$ that a tuple $\overline{z}$ satisfies the relation.

The definition below uses $n+1$ renamings: one of them ($^\circ$) coincides with that of lifting, and the others map x respectively to $x_1, \ldots, x_n$. The tuple $\overline{A}$ denotes n terms A_i, where A_i is the term A where each free variable x is replaced by a fresh variable x_i.

Definition 2 (parametricity).

$$
\begin{array}{ll}
\overline{C} \in [\![s]\!] & = \overline{C} \to \lceil s \rceil \\
\overline{C} \in [\![\Pi x : A.\, B]\!] & = \Pi \overline{x : A}.\, \Pi \mathring{x} : \overline{x} \in [\![A]\!].\, \overline{C\, x} \in [\![B]\!] \\
\overline{C} \in [\![T]\!] & = [\![T]\!]\, \overline{C} \text{ otherwise} \\
\hline
[\![x]\!] & = \mathring{x} \\
[\![\lambda x : A.\, B]\!] & = \lambda \overline{x : A}.\, \lambda \mathring{x} : \overline{x} \in [\![A]\!].\, [\![B]\!] \\
[\![A\, B]\!] & = [\![A]\!]\, \overline{B}\, [\![B]\!] \\
[\![T]\!] & = \lambda z : T.\, \overline{C} \in [\![T]\!] \text{ otherwise} \\
\hline
[\![<>]\!] & = <> \\
[\![\Gamma, x : A]\!] & = [\![\Gamma]\!], \overline{x : A}, \mathring{x} : \overline{x} \in [\![A]\!]
\end{array}
$$

Because the syntax of values and types are unified in a PTS, each of the definitions $\cdot \in [\![\cdot]\!]$ and $[\![\cdot]\!]$ must handle all constructions. In both cases, this is done by using a catch-all case (the last line) that refers to the other part of the definition.

Remark 1 *For arity* 0*, parametricity specializes to lifting* ($[\![A]\!]_0 = \lceil A \rceil$).

Theorem 3 (abstraction). *If* $\Gamma \vdash A : B : s$*, then* $[\![\Gamma]\!] \vdash [\![A]\!] : \overline{A} \in [\![B]\!] : \lceil s \rceil$

Proof. The result is a consequence of the following lemmas:

- $A \longrightarrow_\beta B \Rightarrow [\![A]\!] \longrightarrow_\beta^* [\![B]\!]$
- $\Gamma \vdash A : B \Rightarrow [\![\Gamma]\!] \vdash \overline{A : B}$
- $\Gamma \vdash B : s \Rightarrow [\![\Gamma]\!], \overline{z : B} \vdash \overline{z} \in [\![B]\!] : \lceil s \rceil$
- $\Gamma \vdash A : B : s \Rightarrow [\![\Gamma]\!] \vdash [\![A]\!] : \overline{A} \in [\![B]\!]$

The proof of the last three lemmas is done by simultaneous induction on the length of the derivations. (Details in appendix.)

A direct reading of the above result is as a typing judgement about translated terms (as for lemmas 1 and 4): if A has type B, then $[\![A]\!]$ has type $\overline{A} \in [\![B]\!]$. However, it can also be understood as an abstraction theorem for system P: if a program A has type B in Γ, then various interpretations of A ($\overline{A}$) in related environments ($[\![\Gamma]\!]$) are related, by the formula $\overline{A} \in [\![B]\!]$.

The system P^2 is a natural setting to express parametricity conditions for P. Indeed, the interaction rules of the form $(s, \lceil s' \rceil, \lceil s' \rceil)$ coming from axioms in P are needed to make the sort case valid; and the interaction rules $(s_1, \lceil s_3 \rceil, \lceil s_3 \rceil)$ are needed for the quantification over individuals in the product case.

3.4 Realizability

We develop here a Krivine-style [13] internalized realizability theory. Realizability bears similarities both to the projection and the parametricity transformations defined above.

Like the projection, the realizability transformation is applied on second-level constructs, and behaves differently depending on whether it treats interaction constructs or pure second-level ones. It is also similar to parametricity, as it is defined in two parts. In the first part we define what it means for a program C to realize a formula F ($C \Vdash F$); then we define the translation from a proof p to a proof $\langle p \rangle$ that a program $\lfloor p \rfloor$ satisfies the realizability predicate.

Definition 3 (realizability).

$$
\begin{array}{ll}
C \Vdash \lceil s \rceil & = C \to \lceil s \rceil \\
C \Vdash \Pi x^s : A.B & = \Pi x^s : A.C \Vdash B \\
C \Vdash \Pi x^{\lceil s \rceil} : A.B & = \Pi(\dot{x}^s : \lfloor A \rfloor)(x^{\lceil s \rceil} : \dot{x} \Vdash A).(C\,\dot{x}) \Vdash B \\
C \Vdash F & = \langle F \rangle\, C \text{ otherwise} \\
\hline
\langle x^{\lceil s \rceil} \rangle & = x^{\lceil s \rceil} \\
\langle \lambda x^s : A.B \rangle & = \lambda x^s : A.\langle B \rangle \\
\langle \lambda x^{\lceil s \rceil} : A.B \rangle & = \lambda(\dot{x}^s : \lfloor A \rfloor)(x^{\lceil s \rceil} : \dot{x} \Vdash A).\langle B \rangle \\
\langle (A\,B)_s \rangle & = (\langle A \rangle\, B)_s \\
\langle (A\,B)_{\lceil s \rceil} \rangle & = ((\langle A \rangle\, \lfloor B \rfloor)_s\, \langle B \rangle)_{\lceil s \rceil} \\
\langle T \rangle & = \lambda z^s : \lfloor T \rfloor.\, z \Vdash T \text{ otherwise} \\
\hline
\langle \Gamma, x^s : A \rangle & = \langle \Gamma \rangle, x^s : A \\
\langle \Gamma, x^{\lceil s \rceil} : A \rangle & = \langle \Gamma \rangle, \dot{x}^s : \lfloor A \rfloor, x^{\lceil s \rceil} : \dot{x} \Vdash A
\end{array}
$$

Theorem 4 (adequacy). *If* $\Gamma \vdash A : B : \lceil s \rceil$, *then* $\langle \Gamma \rangle \vdash \langle A \rangle : \lfloor A \rfloor \Vdash B : \lceil s \rceil$

Proof (idea). Similar in structure to the proof of the abstraction theorem.

4 The Third Level

By casting both parametricity and realizability in the mold of PTSs, we are able to discern the connections between them. The connections already surface in the previous sections: the definitions of parametricity and realizability bear some resemblance, and the adequacy and abstraction theorems appear suspiciously similar. In this section we precisely spell out the connection: realizability and parametricity can be defined in terms of each other.

Theorem 5 (realisability increases arity of parametricity).
$\big(B, \overline{C}\big) \in [\![A]\!]_{n+1} = B \Vdash \big(\overline{C} \in [\![A]\!]_n\big)$ *and* $[\![A]\!]_{n+1} = \langle [\![A]\!]_n \rangle$

Proof. By induction on the structure of A.

As a corollary, parametricity is the composition of lifting and realizability:

Corollary 1 (from realizability to parametricity).
$\overline{z} \in [\![A]\!]_n = z_1 \Vdash z_2 \Vdash \cdots \Vdash z_n \Vdash \lceil A \rceil$ *and* $[\![A]\!]_n = \langle \cdots \langle \lceil A \rceil \rangle \cdots \rangle$

Proof. By induction on n. The base case uses $[\![A]\!]_0 = \lceil A \rceil$.

One may also wonder about the converse: is it possible to define realizability in terms of parametricity? We can answer by the affirmative, but we need a bigger system to do so. Indeed, we need to extend $[\![\cdot]\!]$ to work on second-level terms, and that is possible only if a third level is present in the system. To do so, we can iterate the construction used in Sec. 3 to build a logic for an arbitrary PTS.

Definition 4 (third-level system). *Given a PTS $P = (\mathcal{S}, \mathcal{A}, \mathcal{R})$, we define $P^3 = (P^2)^2$, where the sort-lifting $\lceil\cdot\rceil$ used by both instances of the $\cdot^2$ transformation are the same.*

Remark 2 *Because the sort-lifting used by both instances of the $\cdot^2$ transformation are the same, P^3 contains only three copies of P (not four). In fact $P^3 = (\mathcal{S}^3, \mathcal{A}^3, \mathcal{R}^3)$, where*

$$\begin{aligned}
\mathcal{S}^3 &= \mathcal{S} \ \cup \lceil\mathcal{S}\rceil \cup \lceil\lceil\mathcal{S}\rceil\rceil \\
\mathcal{A}^3 &= \mathcal{A} \ \cup \lceil\mathcal{A}\rceil \cup \lceil\lceil\mathcal{A}\rceil\rceil \\
\mathcal{R}^3 &= \mathcal{R} \ \cup \lceil\mathcal{R}\rceil \cup \lceil\lceil\mathcal{R}\rceil\rceil \\
&\qquad \cup \{(s_1, \lceil s_3\rceil, \lceil s_3\rceil), (\lceil s_1\rceil, \lceil\lceil s_3\rceil\rceil, \lceil\lceil s_3\rceil\rceil) \mid (s_1, s_2, s_3) \in \mathcal{R}\} \\
&\qquad \cup \{(s_1, \lceil s_2\rceil, \lceil s_2\rceil), (\lceil s_1\rceil, \lceil\lceil s_2\rceil\rceil, \lceil\lceil s_2\rceil\rceil) \mid (s_1, s_2) \in \mathcal{A}\}
\end{aligned}$$

The $[\![\cdot]\!]$ transformation is extended second-level constructs in P^2, mapping them to third-level ones in P^3. The $\lfloor\cdot\rfloor$ transformation is be similarly extended, to map the third level constructs to the second level, in addition of mapping the second to the first one (only the first level is removed).

Given these extensions, we obtain that realizability is the composition of parametricity and projection.

Lemma 6. *If A is a first-level term, then*
$A = \lfloor z \in [\![A]\!]_1 \rfloor$ *and* $A = \lfloor [\![A]\!]_1 \rfloor$

Proof. By induction on the structure of A, using separation.

Theorem 6 (from parametricity to realizability). *If A is a second-level term, then*
$z \Vdash A = \lfloor z \in [\![A]\!]_1 \rfloor$ *and* $\langle A \rangle = \lfloor [\![A]\!]_1 \rfloor$

Proof. By induction on the structure of A, using the above lemma.

5 Extensions

5.1 Inductive definitions

Even though our development assumes pure type systems, with only axioms of the form (s_1, s_2), the theory easily accommodates the addition of inductive definitions.

For parametricity, the way to extend the theory is exposed by Bernardy et al. [5]. In brief: if for every inductive definition in the programming language there

is a corresponding inductive definition in the logic, then the abstraction theorem holds.

For example, to the indexed inductive definition I corresponds $[\![I]\!]$, as defined below. (We write only one constructor c_p for concision, but the result applies to any number of constructors.)

$$\begin{array}{l}\textsf{data}\ I : \Pi(x_1 : A_1) \cdots (x_n : A_n).s\ \textsf{where} \\ \quad c_p : \Pi(x_1 : B_{p,1}) \cdots (x_{n_1} : B_{p,n_1}).I\ a_{p,1} \cdots a_{p,n}\end{array}$$

$$\begin{array}{l}\textsf{data}\ [\![I]\!] : \overline{I} \in [\![\Pi(x_1 : A_1) \cdots (x_n : A_n).s]\!]\ \textsf{where} \\ \quad [\![c_p]\!] : \overline{c_p} \in [\![\Pi(x_1 : B_{p,1}) \cdots (x_{n_1} : B_{p,n_1}).I\ a_{p,1} \cdots a_{p,n}]\!]\end{array}$$

The result can be transported to realizability by following the correspondence developed in the previous section. By taking the composition of $[\![\cdot]\!]$ and $\lfloor\cdot\rfloor$ for the definition of realizability, and knowing how to extend $[\![\cdot]\!]$ to inductive types, it suffices to extend $\lfloor\cdot\rfloor$ as well (respecting typing: Lem. 4). The corresponding extension to realizability is compatible with the definition for a pure system (by Thm. 6). Adequacy is proved by the composition of abstraction and Lem. 4. The definition of $\lfloor\cdot\rfloor$ is straightforward: each component of the definition must be transformed by $\lfloor\cdot\rfloor$. That is, for any inductive definition in the logic, there must be another inductive definition in the programming language that realizes it.

For instance, given the definition I given below, one must also have $\lfloor I\rfloor$. $\langle I\rangle$ is then given by $\langle I\rangle = \lfloor[\![I]\!]\rfloor$, but can also be expanded as below.

$$\begin{array}{l}\textsf{data}\ I : \Pi(x_1 : A_1) \cdots (x_n : A_n).\lceil s\rceil\ \textsf{where} \\ \quad c_p : \Pi(x_1 : B_{p,1}) \cdots (x_{n_1} : B_{p,n_1}).I\ a_{p,1} \cdots a_{p,n}\end{array}$$

$$\begin{array}{l}\textsf{data}\ \lfloor I\rfloor : \lfloor\Pi(x_1 : A_1) \cdots (x_n : A_n).\lceil s\rceil\rfloor\ \textsf{where} \\ \quad \lfloor c_p\rfloor : \lfloor\Pi(x_1 : B_{p,1}) \cdots (x_{n_1} : B_{p,n_1}).I\ a_{p,1} \cdots a_{p,n}\rfloor\end{array}$$

$$\begin{array}{l}\textsf{data}\ \langle I\rangle : \lfloor I\rfloor \Vdash (\Pi(x_1 : A_1) \cdots (x_n : A_n).\lceil s\rceil)\ \textsf{where} \\ \quad \langle c_p\rangle : \lfloor c_p\rfloor \Vdash (\Pi(x_1 : B_{p,1}) \cdots (x_{n_1} : B_{p,n_1}).I\ a_{p,1} \cdots a_{p,n})\end{array}$$

We can use inductive types to encode usual logical connectives, and derive realizability for them.

Example 6 (conjunction). The encoding of conjunction in a sort $\lceil s\rceil$ is as follows:

$$\begin{array}{l}\textsf{data}\ \_\wedge\_ : \lceil s\rceil \to \lceil s\rceil \to \lceil s\rceil\ \textsf{where} \\ \quad \mathsf{conj} : \Pi\, P\, Q : \lceil s\rceil.P \to Q \to P \wedge Q\end{array}$$

If we apply the projection operator to the conjunction we obtain the type of its realizers: the cartesian product in s.

$$\begin{array}{l}\textsf{data}\ \_\times\_ : s \to s \to s\ \textsf{where} \\ \quad (\_,\_) : \Pi\, \alpha\, \beta : s.\alpha \to \beta \to \alpha \times \beta\end{array}$$

Now we can apply our realizability construction to obtain a predicate telling what it means to realize a conjunction.

$$\begin{aligned}\textbf{data}\ \langle\wedge\rangle : \mathit{\Pi}(\alpha : s).(\alpha \to \lceil s\rceil) \to \\ \mathit{\Pi}(\beta : s).(\beta \to \lceil s\rceil) \to \\ \alpha \times \beta \to s\ \textbf{where} \\ \langle\mathsf{conj}\rangle : \mathit{\Pi}(\alpha : s)(P : \alpha \to \lceil s\rceil) \\ (\beta : s)(Q : \beta \to \lceil s\rceil)(x : \alpha)(y : \beta). \\ P\,x \to Q\,y \to \langle\wedge\rangle\,\alpha\,P\,\beta\,Q\,(x, y)\end{aligned}$$

By definition, $t \Vdash P \wedge Q$ means $\langle\wedge\rangle\,\lfloor P\rfloor\,\langle P\rangle\,\lfloor Q\rfloor\,\langle Q\rangle\,t$. We have

$$t \Vdash P \wedge Q \Leftrightarrow (\pi_1\,t) \Vdash P \wedge (\pi_2\,t) \Vdash Q$$

where π_1 and π_2 are projections upon cartesian product.

We could build the realizers of other logical constructs in the same way: we would obtain a sum-type for the disjunction, an empty type for falsity, and a box type for the existential quantifier. All the following properties (corresponding to the usual definition of the realizability predicate) would then be satisfied:

- $t \Vdash P \vee Q \Leftrightarrow \textbf{case}\,t\,\textbf{with}\,\iota_1\,x \to x \Vdash P \,|\, \iota_2\,x \to x \Vdash Q$.
- $t \Vdash \bot \Leftrightarrow \bot$ and $t \Vdash \neg P \Leftrightarrow \mathit{\Pi}(x : \lfloor P\rfloor).\neg(x \Vdash P)$
- $t \Vdash \exists x : A.P \Leftrightarrow \exists x : A.(\mathit{unbox}\,t) \Vdash P$

where $\textbf{case}\ldots\textbf{with}\ldots$ is the destruction of the sum type, and *unbox* is the destructor of the box type.

5.2 Program extraction and computational irrelevance

An application of the theory developed so far is the extraction of programs from proofs. Indeed, an implication of the adequacy theorem is that the program $\lfloor A\rfloor$, obtained by projection of a proof A of a formula B, corresponds to an implementation of B, viewed as a specification. One says that $\lfloor\cdot\rfloor$ implements program extraction.

For example, applying extraction to an expression involving vectors ($Vec : (A : \lceil\star\rceil) \to Nat \to \lceil\star\rceil$) yields a program over lists. This means that programs can be justified in the rich system P^2, and realized in the simple system P. Practical benefits include a reduction in memory usage: Brady et al. [6] measure an 80% reduction using a technique with similar goals.

While P^2 is already much more expressive than P, it is possible to further increase the expressive power of the system, while retaining the adequacy theorem, by allowing quantification of first-level terms by second-level terms.

Definition 5 ($P^{2'}$). *Let $P = (\mathcal{S}, \mathcal{A}, \mathcal{R})$, we define $P^{2'} = (\mathcal{S}^{2'}, \mathcal{A}^{2'}, \mathcal{R}^{2'})$*

$$\begin{aligned}\mathcal{S}^{2'} &= \mathcal{S} \cup \{\lceil s\rceil \mid s \in \mathcal{S}\} \\ \mathcal{A}^{2'} &= \mathcal{A} \cup \{(\lceil s_1\rceil, \lceil s_2\rceil) \mid (s_1, s_2) \in \mathcal{A}\} \\ \mathcal{R}^{2'} &= \mathcal{R} \cup \{(\lceil s_1\rceil, \lceil s_2\rceil, \lceil s_3\rceil), (s_1, \lceil s_3\rceil, \lceil s_3\rceil), (\lceil s_1\rceil, s_3, s_3) \mid (s_1, s_2, s_3) \in \mathcal{R}\} \\ &\quad \cup \{(s_1, \lceil s_2\rceil, \lceil s_2\rceil), (\lceil s_1\rceil, s_2, s_2) \mid (s_1, s_2) \in \mathcal{A}\}\end{aligned}$$

The result is a symmetric system, with two copies of P. Within either side of the system, one can reason about terms belonging to the other side. Furthermore, either side has a computational interpretation where the terms of the other side are irrelevant. For the second level, this interpretation is given by $\lfloor \cdot \rfloor$.

Even though there is no separation between first and second level in $P^{2'}$, adequacy is preserved: the addition of rules of the form $(\lceil s_1 \rceil, s_2, s_3)$ only adds first level terms, which are removed by projection.

6 Related work and Conclusion

Our work is based on Krivine-style realizability [13] and Reynolds-style parametricity [23], which have both spawned large bodies of work.

Logics for parametricity. Study of parametricity is typically semantic, including the seminal work of Reynolds [23]. There, the concern is to capture the polymorphic character of λ-calculi (typically system F) in a model.

Mairson [16] pioneered a different angle of study, where the expressions of the programming language are (syntactically) translated to formulas describing the program. That style has then been picked by various authors before us, including Abadi et al. [1], Plotkin and Abadi [22], Bernardy et al. [5].

Plotkin and Abadi [22] introduce a logic for parametricity, similar to F^2, but with several additions. The most important addition is that of a parametricity axiom. This addition allows to prove the initiality of Church-style encoding of types.

Wadler [29] defines essentially the same concepts as us, but in the special case of system F. He points out that realizability transforms unary parametricity into binary parametricity, but does not generalize to arbitrary arity. We find the $n = 0$ case particularly interesting, as it shows that parametricity can be constructed purely in terms of realizability and a trivial lifting to the second level. We additionally show that realizability can be obtained by composing realizability and projection, while Wadler only defines the realizability transformation as a separate construct.

The parametricity transformation and the abstraction theorem that we expose here are a modified version of [5]. The added benefits of the present version is that we handle finite PTSs, and we allow the target system to be different from the source. The possible separation of source and targets is already implicit in that paper though. The way we handle finite PTSs is by separating the treatment of types and programs.

Realizability. Our realizability construction can be understood as an extension of the work of Paulin-Mohring [20], providing a realizability interpretation for a variant of the Calculus of Construction. Paulin-Mohring [20] splits CC in two levels; one where $\star$ becomes *Prop* and one where it becomes *Spec*. Perhaps counter-intuitively, *Prop* lies in what we call the first level; and *Spec* lies in the second level. Indeed, *Prop* is removed from the realizers. The system is

symmetric, as the one we expose in Sec. 5.2, in the sense that there is both a rule $(\mathit{Spec}, \mathit{Prop}, \mathit{Prop})$ and $(\mathit{Prop}, \mathit{Spec}, \mathit{Spec})$.

In order to see that Paulin-Mohring's construction as a special case of ours, it is necessary to recognize a number of small differences:

1. The sort *Spec* is transformed into *Prop* in the realizability transformation, whereas we would keep *Spec*.
2. The sorts of the original system use a different set of names (*Data* and *Order*). Therefore the sort *Spec* is transformed into *Data* in the projection, whereas we would use *Prop*.
3. The types of *Spec* and *Prop* inhabit the same sort, namely *Type*.
4. There is elimination from *Spec* to *Prop*, breaking the computational irrelevance in that direction.

The first two differences are essentially renamings, and thus unimportant.

Connections. We are unaware of previous work showing the connection between realizability and parametricity, at least as clearly as we do. Wadler [29] comes close, giving a version of Thm. 5 specialized to system F, but not its converse, Thm. 6. Mairson [16] mentions that his work on parametricity is directly inspired by that of Leivant [15] on realizability, but does not formalize the parallels.

Conclusion. We have given an account of parametricity and realizability in the framework of PTSs. The result is very concise: the definitions occupy only a dozen of lines. By recognizing the parallels between the two, we are able to further shrink the number of primitive concepts.

Our work points the way towards the transportation of every parametricity theory into a corresponding realizability theory, and *vice versa*.

Acknowledgments. Thanks to Thorsten Altenkirch, Thierry Coquand, Peter Dybjer and Guilhem Moulin for helpful comments and discussions.

Bibliography

[1] M. Abadi, L. Cardelli, and P. Curien. Formal parametric polymorphism. In *Proc. of POPL'93*, pages 157–170. ACM, 1993.

[2] H. P. Barendregt. Lambda calculi with types. *Handbook of logic in computer science*, 2:117–309, 1992.

[3] S. Berardi. *Type Dependence and Constructive Mathematics.* PhD thesis, Dipartimento di Informatica, Torino, 1989.

[4] J.-P. Bernardy, P. Jansson, and K. Claessen. Testing polymorphic properties. In A. Gordon, editor, *Proc. of ESOP 2010*, volume 6012 of *LNCS*, pages 125–144. Springer, 2010.

[5] J.-P. Bernardy, P. Jansson, and R. Paterson. Parametricity and dependent types. In *Proc. of ICFP 2010*, pages 345–356. ACM, 2010.

[6] E. Brady, C. McBride, and J. McKinna. Inductive families need not store their indices. In S. Berardi, M. Coppo, and F. Damiani, editors, *Types for Proofs and Programs*, volume 3085 of *LNCS*, pages 115–129. Springer Berlin / Heidelberg, 2004.
[7] A. Gill, J. Launchbury, and S. Peyton Jones. A short cut to deforestation. In *Proc. of FPCA*, pages 223–232. ACM, 1993.
[8] J. Y. Girard. *Interprétation fonctionnelle et elimination des coupures de l'arithmétique d'ordre supérieur*. Thèse d'état, Université de Paris 7, 1972.
[9] R. Harrop. On disjunctions and existential statements in intuitionistic systems of logic. *Mathematische Annalen*, 132(4):347–361, 1956.
[10] S. C. Kleene. On the interpretation of intuitionistic number theory. *J. of Symbolic Logic*, 10(4):109–124, 1945.
[11] S. C. Kleene. *Introduction to metamathematics*. Wolters-Noordhoff, 1971.
[12] G. Kreisel. Interpretation of analysis by means of constructive functionals of finite types. In A. Heyting, editor, *Constructivity in mathematics*, pages 101–128, 1959.
[13] J.-L. Krivine. *Lambda-calcul types et modèles*. Masson, 1990.
[14] J.-L. Krivine and M. Parigot. Programming with proofs. *J. Inf. Process. Cybern.*, 26(3):149–167, 1990.
[15] D. Leivant. Contracting proofs to programs. In *Logic and Comp. Sci.*, pages 279–327, 1990.
[16] H. Mairson. Outline of a proof theory of parametricity. In *Proc. of FPCA 1991*, volume 523 of *LNCS*, pages 313–327. Springer-Verlag, 1991.
[17] C. McBride and J. McKinna. The view from the left. *J. Funct. Program.*, 14(01):69–111, 2004.
[18] R. Milner. Logic for Computable Functions: description of a machine implementation. *Artificial Intelligence*, 1972.
[19] U. Norell. *Towards a practical programming language based on dependent type theory*. PhD thesis, Chalmers Tekniska Högskola, 2007.
[20] C. Paulin-Mohring. Extracting Fω's programs from proofs in the calculus of constructions. In *POPL'89*, pages 89–104. ACM, 1989.
[21] C. Paulin-Mohring. *Extraction de programmes dans le Calcul des Constructions*. PhD thesis, Université Paris 7, 1989.
[22] G. Plotkin and M. Abadi. A logic for parametric polymorphism. In *LNCS*, volume 664, page 361–375. Springer-Verlag, 1993.
[23] J. C. Reynolds. Types, abstraction and parametric polymorphism. *Information processing*, 83(1):513–523, 1983.
[24] J. Staples. Combinator realizability of constructive finite type analysis. *Cambridge Summer School in Mathematical Logic*, pages 253–273, 1973.
[25] The Coq development team. The Coq proof assistant, 2010.
[26] A. Troelstra. *Handbook of proof theory*, chapter Realizability. Elsevier, 1998.
[27] J. Van Oosten. Realizability: a historical essay. *Mathematical Structures in Comp. Sci.*, 12(03):239–263, 2002.
[28] P. Wadler. Theorems for free! In *Proc. of FPCA 1989*, pages 347–359. ACM, 1989.
[29] P. Wadler. The Girard–Reynolds isomorphism. *Theor. Comp. Sci.*, 375 (1–3):201–226, 2007.

Appendix

This appendix contains the details of the proofs of normalization and abstraction theorems.

6.1 Normalization

Theorem 7 (normalization). *If P is strongly normalizing, so is P^2.*

Proof. The proof is based on the observation $(*)$ that, if a term A is typable in P^2 and not normalizable, then at least either:

- one of the first-level subterms of A is not normalizable, or
- the first-level term $\lfloor A \rfloor$ is not normalizable.

Then, by separation (Thm. 1), the first-level subterms are typable in P, so they must be normalizable. We conclude that A must be normalizable.

To prove $(*)$ we first decompose the reduction relation $\longrightarrow_\beta$ into three disjoint relations $\longrightarrow_\beta = \longrightarrow_1 \cup \longrightarrow_2 \cup \longrightarrow_i$:

1. The relation $\longrightarrow_1$ reduces abstractions typable with the rules already in $\mathcal{R}$.
2. The relation $\longrightarrow_2$ reduces abstractions typable with rules of the form $(\lceil s_1 \rceil, \lceil s_2 \rceil, \lceil s_3 \rceil)$ for $(s_1, s_2, s_3) \in \mathcal{R}$.
3. The relation $\longrightarrow_i$ reduces abstractions typable with the other rules (corresponding to interaction reductions).

We then remark the following facts:

1. If $A \longrightarrow_2 A'$, then A is a second-level term and $\lfloor A \rfloor \longrightarrow_\beta \lfloor A' \rfloor$; because the projection does not erase redexes reduced by $\longrightarrow_2$.
2. If A is a second-level term, then
$$A(\longrightarrow_1 \cup \longrightarrow_i)A' \text{ implies } \lfloor A \rfloor = \lfloor A' \rfloor$$
because the projection erases all redexes reduced by $\longrightarrow_1$ and by $\longrightarrow_i$.
3. If $A \longrightarrow_i A'$, then the number of interaction redexes in A has been decreased by one in A'.
Indeed, an interaction redex is always a second-level term and it always involves an abstraction whose argument is a first-level term. Therefore, the argument does not contain any interaction redex and cannot be an abstraction that would create an interaction redex. This is why $\longrightarrow_i$ does not create nor duplicate interaction redexes.
4. The number of interaction redexes is invariant by $\longrightarrow_1$ because interaction redexes are second-level terms.

Let $A \longrightarrow_\beta A_1 \longrightarrow_\beta A_2 \longrightarrow_\beta ... \longrightarrow_\beta A_n \longrightarrow_\beta ...$ be an infinite sequence of terms. [5] Then we are in one of these situations:

[5] The proof may also be carried out constructively: the idea is to reuse the normalization procedure of terms in P to normalize terms in P^2. More precisely, given a well-typed A, one can use the normalization procedure of $\lfloor A \rfloor$ to normalize the 2nd level structure, and normalize the 1st level sub-terms independently. The separation properties guarantee that the interactions between first and second level structure only adds a finite number of β-reductions.

– either we can extract a sub-sequence $(A_{n_i})_{i\in\mathbb{N}}$ such that $A_{n_i}(\longrightarrow_1 \cup \longrightarrow_i)^* \cdot \longrightarrow_2 A_{n_{i+1}}$ for all $i \in \mathbb{N}$;
– or there exists a N such that for all $n \geqslant N$, $A_n(\longrightarrow_1 \cup \longrightarrow_i)A_{n+1}$ or more prosaically $\longrightarrow_2$ is not used in the chain starting from N.

In the former case, because $A(\longrightarrow_1 \cup \longrightarrow_i)^* \cdot \longrightarrow_2 A'$ implies $\lfloor A \rfloor \longrightarrow_\beta \lfloor A' \rfloor$, we can build an infinite sequence $(\lfloor A_{n_i} \rfloor)_{i\in\mathbb{N}}$ decreasing for $\longrightarrow_1$.

In the latter case, because $\longrightarrow_i$ strictly decreases the number of insignificant redexes and the reduction $\longrightarrow_1$ does not change this number, there exists an integer $M \geqslant N$, such that for all $n \geqslant M$, $A_n \longrightarrow_1 A_{n+1}$. We can write A_M as $B[x_1 \mapsto t_1, ..., x_k \mapsto t_k]$ where all sub-terms of B that are types or programs are variables among $\{x_1, ..., x_k\}$. Now, if $B[x_1 \mapsto t_1, ..., x_k \mapsto t_k] \longrightarrow_\beta A_{N+1}$ it means there exists t'_i such that $A_{N+1} = B[x_1 \mapsto t_1, ..., x_i \mapsto t'_i, ..., x_k \mapsto t^k]$ and $t_i \longrightarrow_\beta t'_i$. By iterating this, we can build an infinite decreasing sequence starting from t_i for some $1 \leqslant i \leqslant k$.

6.2 Abstraction

Lemma 7 ($[\![\cdot]\!]$ and substitution).

$$[\![t[x \mapsto e]]\!] = [\![t]\!][\overline{x} \mapsto \overline{e}][\mathring{x} \mapsto [\![e]\!]]$$

Proof. Recall that if x is free in t, then x_i and $\mathring{x}$ are free in $[\![t]\!]$. The free variable $\mathring{x}$ is introduced by the rule $[\![x]\!] = \mathring{x}$, therefore if x is substituted by e, $\mathring{x}$ must be substituted by $[\![e]\!]$. Similarly, each of the x_i must be substituted by e_i (renaming must be applied to the substituted expression).

Lemma 8. $A \longrightarrow_\beta B \implies [\![A]\!] \longrightarrow_\beta^* [\![B]\!]$

Proof. By induction on the derivation. All cases are congruences, except for the interesting base case, where β-reduction happens.

In that case, we want to show that if $(\lambda x : T.\, t)\, e \longrightarrow_\beta t[x \mapsto e]$ then $[\![(\lambda x : T.\, t)\, e]\!] \longrightarrow_\beta^* [\![t[x \mapsto e]]\!]$.

By definition:

$$\begin{aligned}[\![(\lambda x : T.\, t)\, e]\!] &= [\![\lambda x : T.\, t]\!]\, \overline{e}\, [\![e]\!] \\ &= (\lambda \overline{x : T}.\, \lambda \mathring{x} : [\![T]\!]\, \overline{x}.\, [\![t]\!])\, \overline{e}\, [\![e]\!]\end{aligned}$$

And by Lem. 7, we are left with showing that $(\lambda \overline{x : T}.\, \lambda \mathring{x} : [\![T]\!]\, \overline{x}.\, [\![t]\!])\, \overline{e}\, [\![e]\!] \longrightarrow_\beta^* [\![t]\!][\overline{x} \mapsto \overline{e}][\mathring{x} \mapsto [\![e]\!]]$, which one can easily identify as $n + 1$ instances of β-reduction.

Corollary 2 ($[\![\cdot]\!]$ preserves reduction).

$$A \longrightarrow_\beta^* B \implies [\![A]\!] \longrightarrow_\beta^* [\![B]\!]$$

Furthermore, the number of reductions in the target is $n + 1$ times the number of reductions in the source.

Corollary 3 ($[\![\cdot]\!]$ preserves β-equivalence). $A =_\beta B \implies [\![A]\!] =_\beta [\![B]\!]$

The following lemmas (9, 10 and 11) are proved by construction of a derivation tree in P^2 from a derivation tree in P. The three corresponding functions are denoted as follows:

1. $|\cdot|$ for $\Gamma \vdash A : B \Rightarrow [\![\Gamma]\!] \vdash \overline{A : B}$
2. $\{\cdot\}$ for $\Gamma \vdash B : s \Rightarrow [\![\Gamma]\!], \overline{z : B} \vdash \overline{z} \in [\![B]\!] : \lceil s \rceil$
3. $[\![\cdot]\!]$ for $\Gamma \vdash A : B : s \Rightarrow [\![\Gamma]\!] \vdash [\![A]\!] : \overline{A} \in [\![B]\!]$

Even though the constructions are interdependent, it is not difficult to see that recursive calls are made only on strictly smaller trees.

Lemma 9 ($|\cdot|$). $\Gamma \vdash A : B \Rightarrow [\![\Gamma]\!] \vdash \overline{A : B}$

Proof. By the thinning lemma. For each A_i, erase from the context $[\![\Gamma]\!]$ the relational variables and j-indexed variables such that $j \neq i$. The legality of the context is ensured by Lem. 10 and Lem. 11.

The following two lemmas proceed by case analysis on the derivation tree. The presentation uses the following conventions:

- Each case is presented separately: first the input tree is recalled, then the transformed tree is shown.
- The constructions may make use of the other lemmas, and usages are marked by $|\cdot|$, $\{\cdot\}$ or $[\![\cdot]\!]$.
- Usage of the generation lemma is indicated in the input tree.
- For the sake of concision, some usage of the weakening rule are omitted.
- Again, for concision, mundane parts of the construction are omitted (squiggly lines indicate missing parts).

Lemma 10 ($\{\cdot\}$). $\Gamma \vdash B : s \Rightarrow [\![\Gamma]\!], \overline{z : B} \vdash \overline{z} \in [\![B]\!] : \lceil s \rceil$

Proof.

Axiom

$$\frac{}{\vdash s : s'}\,\mathrm{ax} \;\Rightarrow\; \frac{\dfrac{\dfrac{\dfrac{}{\vdash s : s'}\,\mathrm{ax}}{\overline{z : s} \vdash \overline{z : s}}\,\mathrm{st} \quad \dfrac{}{\vdash \lceil s \rceil : \lceil s' \rceil}\,\mathrm{ax}}{\overline{z : s} \vdash \overline{z} \to \lceil s \rceil : \lceil s' \rceil}\,(s, \lceil s' \rceil, \lceil s' \rceil)}{\overline{z : s} \vdash \overline{z} \in [\![s]\!] : \lceil s' \rceil}\,\mathrm{def}$$

Start

$$\frac{\Gamma \vdash s : s'}{\Gamma, x : s \vdash x : s}\,\mathrm{st} \;\Rightarrow\; \frac{\dfrac{\dfrac{\vdots}{[\![\Gamma]\!], \overline{x : s}, \mathring{x} : \overline{x} \in [\![s]\!], \overline{z : x} \vdash \mathring{x} : \overline{x} \to \lceil s \rceil} \quad \dfrac{\dfrac{\vdots}{[\![\Gamma]\!], \overline{x : s} \vdash \overline{x : s}}\,\mathrm{st}}{[\![\Gamma]\!], \overline{x : s}, \mathring{x} : \overline{x} \in [\![s]\!], \overline{z : x} \vdash \overline{z : x}}\,\mathrm{app}}{[\![\Gamma]\!], \overline{x : s}, \mathring{x} : \overline{x} \in [\![s]\!], \overline{z : x} \vdash \mathring{x}\,\overline{z} : \lceil s \rceil}\,\mathrm{def}}{[\![\Gamma]\!], \overline{x : s}, \mathring{x} : \overline{x} \in [\![s]\!], \overline{z : x} \vdash \overline{z} \in [\![x]\!] : \lceil s \rceil}\,\mathrm{def}$$

Weakening

$$\frac{\Gamma \vdash A : s \quad \Gamma \vdash C : s'}{\Gamma, x : C \vdash A : s}\,\mathrm{wk}$$

$\Rightarrow$

$$\frac{\dfrac{\dfrac{\vdots\ \{\Gamma \vdash A : s\}}{[\![\Gamma]\!], \overline{z : A} \vdash \overline{z} \in [\![A]\!] : \lceil s \rceil} \quad \dfrac{\vdots\ |\Gamma \vdash C : s'|}{[\![\Gamma]\!] \vdash \overline{C : s'}}\,\mathrm{wk}}{[\![\Gamma]\!], \overline{x : C}, \overline{z : A} \vdash \overline{z} \in [\![A]\!] : \lceil s \rceil} \quad \dfrac{\vdots\ \{\Gamma \vdash C : s'\}}{[\![\Gamma]\!], \overline{x : C} \vdash \overline{x} \in [\![C]\!] : \lceil s' \rceil}\,\mathrm{wk}}{[\![\Gamma]\!], \overline{x : C}, \mathring{x} : \overline{x} \in [\![C]\!], \overline{z : A} \vdash \overline{z} \in [\![A]\!] : \lceil s \rceil}\,\mathrm{wk}$$

Abstraction impossible: no type is a lambda abstraction.

Application

$$\frac{\Gamma \vdash A : s_1 \quad \Gamma \vdash A \to s : s_3}{\dfrac{\dfrac{\textit{generation}}{\Gamma \vdash F : A \to s} \quad \Gamma \vdash a : A}{\Gamma \vdash F\, a : s}\,\mathrm{app}}$$

$\Rightarrow$

$$\frac{\dfrac{\dfrac{\dfrac{\vdots\ [\![\Gamma \vdash F : A \to s : s_3]\!]}{[\![\Gamma]\!] \vdash [\![F]\!] : \overline{F} \in [\![A \to s]\!]}\,\mathrm{def} \quad \dfrac{\vdots\ |\Gamma \vdash a : A|}{[\![\Gamma]\!] \vdash \overline{a : A}}\,\mathrm{app}}{[\![\Gamma]\!] \vdash [\![F]\!] : \Pi x : A.\, \overline{a} \in [\![A]\!] \to \overline{F\, a} \in [\![s]\!]} \quad \dfrac{\vdots\ [\![\Gamma \vdash a : A : s_1]\!]}{[\![\Gamma]\!] \vdash [\![a]\!] : \overline{a} \in [\![A]\!]}\,\mathrm{app}}{[\![\Gamma]\!] \vdash [\![F]\!]\, \overline{a}\, [\![a]\!] : \overline{F\, a} \in [\![s]\!]}\,\mathrm{def}}{[\![\Gamma]\!] \vdash [\![F]\!]\, \overline{a}\, [\![a]\!] : \overline{F\, a} \to \lceil s \rceil}\,\mathrm{def}$$

$$\frac{\dfrac{\dfrac{\vdots\ |\Gamma \vdash F\, a : s|}{[\![\Gamma]\!] \vdash \overline{F\, a : s}}\,\mathrm{st}}{[\![\Gamma]\!], \overline{z : F\, a} \vdash \overline{z : F\, a}}\,\mathrm{app}}{[\![\Gamma]\!], \overline{z : F\, a} \vdash [\![F]\!]\, \overline{a}\, [\![a]\!]\, \overline{z} : \lceil s \rceil}\,\mathrm{def}}{[\![\Gamma]\!], \overline{z : F\, a} \vdash \overline{z} \in [\![F\, a]\!] : \lceil s \rceil}$$

Product

$$\frac{\Gamma \vdash A : s_1 \quad \Gamma, x : A \vdash B : s_2}{\Gamma \vdash \Pi x : A.\, B : s}\,(s_1, s_2, s)$$

$\Rightarrow$

$$\frac{\dfrac{\vdots\ |\Gamma \vdash A : s_1|}{[\![\Gamma]\!] \vdash \overline{A : s_1}} \quad \dfrac{\dfrac{\dfrac{\vdots}{[\![\Gamma]\!], \overline{z : (\Pi x : A.\, B)}, \overline{x : A} \vdash \overline{z\, x : B}}\,\mathrm{app} \quad \dfrac{\vdots\ \{\Gamma, x : A \vdash B : s_2\}}{[\![\Gamma]\!], \overline{x : A}, \mathring{x} : \overline{x} \in [\![A]\!], \overline{y : B} \vdash \overline{y} \in [\![B]\!] : \lceil s_2 \rceil}}{[\![\Gamma]\!], \overline{z : (\Pi x : A.\, B)}, \overline{x : A}, \mathring{x} : \overline{x} \in [\![A]\!] \vdash \overline{z\, x} \in [\![B]\!] : \lceil s_2 \rceil}\,\mathrm{substitutio}}{\dfrac{\dfrac{\vdots\ \{\Gamma \vdash A : s_1\}}{[\![\Gamma]\!], \overline{x : A} \vdash \overline{x} \in [\![A]\!] : \lceil s_1 \rceil}}{[\![\Gamma]\!], \overline{z : (\Pi x : A.\, B : s_3)}, \overline{x : A} \vdash \Pi \mathring{x} : \overline{x} \in [\![A]\!].\, \overline{z\, x} \in [\![B]\!] : \lceil s \rceil}\,(\lceil s_1 \rceil, \lceil s_2 \rceil, \lceil s \rceil)}}{[\![\Gamma]\!], \overline{z : (\Pi x : A.\, B : s_3)} \vdash \Pi \overline{x : A}.\, \Pi \mathring{x} : \overline{x} \in [\![A]\!].\, \overline{z\, x} \in [\![B]\!] : \lceil s \rceil}\,(s_1, \lceil s \rceil, \lceil s \rceil)}{[\![\Gamma]\!], \overline{z : (\Pi x : A.\, B : s_3)} \vdash \overline{z} \in [\![\Pi x : A.\, B]\!] : \lceil s \rceil}\,\mathrm{def}$$

Conversion

$$\frac{\Gamma \vdash B : s' \quad s =_\beta s' \quad \Gamma \vdash s : s''}{\Gamma \vdash B : s}\,\text{conv}$$

$\Rightarrow$

$$\frac{\vdots\ \{\Gamma \vdash B : s'\} \qquad \vdots\ |\Gamma \vdash s : s''|}{[\![\Gamma]\!], \overline{z : B} \vdash \overline{z} \in [\![B]\!] : \lceil s' \rceil \quad \lceil s \rceil =_\beta \lceil s' \rceil \quad [\![\Gamma]\!] \vdash s : s''}\,\text{conv}$$
$$[\![\Gamma]\!], \overline{z : B} \vdash \overline{z} \in [\![B]\!] : \lceil s \rceil$$

Lemma 11 ($[\![\cdot]\!]$). *$\Gamma \vdash A : B : s \Rightarrow [\![\Gamma]\!] \vdash [\![A]\!] : \overline{A} \in [\![B]\!]$*

Proof. Case analysis proceeds on the derivation of $\Gamma \vdash A : B$.

$$\Gamma \vdash T : s : s' \Rightarrow \frac{\dfrac{\vdots\ \{\Gamma \vdash T : s\}}{[\![\Gamma]\!], \overline{z : T} \vdash \overline{z} \in [\![T]\!] : \lceil s \rceil}\quad \dfrac{\dfrac{\vdots\ |\Gamma \vdash T : s| \qquad \vdots\ \{\Gamma \vdash s : s'\}}{[\![\Gamma]\!] \vdash \overline{T : s} \qquad [\![\Gamma]\!], \overline{z : s} \vdash \overline{z} \in [\![s]\!] : \lceil s' \rceil}\,\text{substitution}}{[\![\Gamma]\!] \vdash \overline{T} \in [\![s]\!] : \lceil s' \rceil}\,\text{def}}{[\![\Gamma]\!] \vdash \overline{T} \to \lceil s \rceil : \lceil s' \rceil}\,\text{abs}$$
$$\frac{[\![\Gamma]\!] \vdash \lambda \overline{z : T}.\, \overline{z} \in [\![T]\!] : \overline{T} \to \lceil s \rceil}{[\![\Gamma]\!] \vdash [\![T]\!] : \overline{T} \in [\![s]\!]}\,\text{def}$$

Start

$$\frac{\Gamma \vdash A : s}{\Gamma, x : A \vdash x : A}\,\text{st} \Rightarrow \frac{\vdots\ \{\Gamma \vdash A : s\}}{[\![\Gamma]\!], \overline{x : A} \vdash \overline{x} \in [\![A]\!] : \lceil s \rceil}\,\text{st}$$
$$[\![\Gamma]\!], \overline{x : A}, \mathring{x} : \overline{x} \in [\![A]\!] \vdash \mathring{x} : \overline{x} \in [\![A]\!]$$

Weakening

$$\frac{\Gamma \vdash A : B \quad \Gamma \vdash C : s}{\Gamma, x : C \vdash A : B}\,\text{wk}$$

$\Rightarrow$

$$\frac{\dfrac{\vdots\ [\![\Gamma \vdash A : B : s]\!] \qquad \vdots\ |\Gamma \vdash C : s|}{[\![\Gamma]\!] \vdash [\![A]\!] : \overline{A} \in [\![B]\!] \qquad [\![\Gamma]\!] \vdash \overline{C : s}}\,\text{wk} \qquad \vdots\ \{\Gamma \vdash C : s\}}{[\![\Gamma]\!], \overline{x : C} \vdash [\![A]\!] : \overline{A} \in [\![B]\!] \qquad [\![\Gamma]\!], \overline{x : C} \vdash \overline{x} \in [\![C]\!] : \lceil s \rceil}\,\text{wk}$$
$$[\![\Gamma]\!], \overline{x : C}, \mathring{x} : \overline{x} \in [\![C]\!] \vdash [\![A]\!] : \overline{A} \in [\![B]\!]$$

The construction also uses that $\Gamma \vdash A : B \& \Gamma, x : C \vdash B : s \Rightarrow \Gamma \vdash B : s$

Abstraction

$$\frac{\Gamma \vdash A : B \quad \Gamma \vdash C : s}{\Gamma, x : C \vdash A : B}\,\text{wk}$$

$\Rightarrow$

$$\frac{\dfrac{\vdots\ [\![\Gamma \vdash A : B : s]\!] \qquad \vdots\ |\Gamma \vdash C : s|}{[\![\Gamma]\!] \vdash [\![A]\!] : \overline{A} \in [\![B]\!] \qquad [\![\Gamma]\!] \vdash \overline{C : s}}\,\text{wk} \qquad \vdots\ \{\Gamma \vdash C : s\}}{[\![\Gamma]\!], \overline{x : C} \vdash [\![A]\!] : \overline{A} \in [\![B]\!] \qquad [\![\Gamma]\!], \overline{x : C} \vdash \overline{x} \in [\![C]\!] : \lceil s \rceil}\,\text{wk}$$
$$[\![\Gamma]\!], \overline{x : C}, \mathring{x} : \overline{x} \in [\![C]\!] \vdash [\![A]\!] : \overline{A} \in [\![B]\!]$$

Continuations of the tree (squiggly lines) are similar to derivations found in $\{\Gamma \vdash (\Pi x : A.B) : s\}$.

Application

$$\dfrac{\dfrac{\dfrac{\Gamma \vdash A : s_1}{\Gamma \vdash (\Pi x : A.\, B) : s_3}\,(s_1,s_2,s_3)}{\dfrac{\textit{generation}}{\Gamma \vdash F : (\Pi x : A.\, B)}} \quad \Gamma \vdash a : A}{\Gamma \vdash F\, a : B[x \mapsto a]}\,\mathrm{app}$$

$\Rightarrow$

$$\dfrac{\dfrac{\dfrac{\vdots\ [\![\Gamma \vdash F : (\Pi x : A.\, B) : s_3]\!]}{[\![\Gamma]\!] \vdash [\![F]\!] : \overline{F} \in [\![\Pi x : A.\, B]\!] : s_3}\,\mathrm{def}}{[\![\Gamma]\!] \vdash [\![F]\!] : \Pi \overline{x : A}.\, \Pi \mathring{x} : \overline{x} \in [\![A]\!].\, \overline{F\, x} \in [\![B]\!]} \quad \dfrac{\vdots\ |\Gamma \vdash a : A|}{[\![\Gamma]\!] \vdash \overline{a : A}}\,\mathrm{app}}{[\![\Gamma]\!] \vdash [\![F]\!]\, \overline{a} : \Pi \mathring{x} : \overline{a} \in [\![A]\!].\, (\overline{F\, a} \in [\![B]\!])[\overline{x \mapsto a}]} \quad \dfrac{\vdots\ [\![\Gamma \vdash a : A : s_1]\!]}{[\![\Gamma]\!] \vdash [\![a]\!] : \overline{a} \in [\![A]\!]}\,\mathrm{app}}{\dfrac{[\![\Gamma]\!] \vdash [\![F]\!]\, \overline{a}\, [\![a]\!] : (\overline{F\, a} \in [\![B]\!])[\overline{x \mapsto a}][\mathring{x} \mapsto [\![a]\!]]}{[\![\Gamma]\!] \vdash [\![F\, a]\!] : \overline{F\, a} \in [\![B[x \mapsto a]]\!]}\,\mathrm{def}}$$

Conversion

$$\dfrac{\Gamma \vdash A : B' \quad B =_\beta B' \quad \Gamma \vdash B : s}{\Gamma \vdash A : B}\,\mathrm{conv}$$

$\Rightarrow$

$$\dfrac{\dfrac{\vdots\ [\![\Gamma \vdash A : B' : s']\!]}{[\![\Gamma]\!] \vdash [\![A]\!] : \overline{A} \in [\![B']\!]} \quad \overline{A} \in [\![B]\!] =_\beta \overline{A} \in [\![B']\!] \qquad \dfrac{\dfrac{\vdots\ |\Gamma \vdash A : B|}{[\![\Gamma]\!] \vdash \overline{A : B}} \quad \dfrac{\vdots\ \{\Gamma \vdash B : s\}}{[\![\Gamma]\!], \overline{z : B} \vdash \overline{z} \in [\![B]\!] : \lceil s \rceil}\,\mathrm{subs}}{[\![\Gamma]\!] \vdash \overline{A} \in [\![B]\!] : \lceil s \rceil}\,\mathrm{conv}}{[\![\Gamma]\!] \vdash [\![A]\!] : \overline{A} \in [\![B]\!]}$$

$\Gamma \vdash B' : s'$ is a consequence of $\Gamma \vdash B : s$ and $B =_\beta B'$ (Corollary 3).

Theorem 8 (abstraction). *If $\Gamma \vdash A : B : s$, then $[\![\Gamma]\!] \vdash [\![A]\!] : \overline{A} \in [\![B]\!] : \lceil s \rceil$*

Proof. Combine Lem. 10 and Lem. 11.