Realizability for Peano Arithmetic with Winning Conditions in HON Games

Valentin Blot

Realizability for Peano Arithmetic with Winning Conditions in HON Games

Valentin Blot

Laboratoire de l'Informatique et du Parallélisme
ENS Lyon - Université de Lyon
UMR 5668 CNRS ENS-Lyon UCBL INRIA
46, allée d'Italie
69364 Lyon cedex 07 - FRANCE
valentin.blot@ens-lyon.fr

Abstract. We build a realizability model for Peano arithmetic based on winning conditions for HON games. First we define a notion of winning strategies on arenas equipped with winning conditions. We prove that the interpretation of a classical proof of a formula is a winning strategy on the arena with winning condition corresponding to the formula. Finally we apply this to Peano arithmetic with relativized quantifications and give the example of witness extraction for Π_2^0-formulas.

1 Introduction

Realizability is a technique to extract computational content from formal proofs. It has been widely used to analyze intuitionistic systems (for e.g. higher-order arithmetic or set theory), see [1] for a survey. Following Griffin's computational interpretation of Peirce's law [2], Krivine developed in [3–5] a realizability for second-order classical arithmetic and Zermelo-Fraenkel set theory.

On the other hand, Hyland-Ong game semantics provide precise models of various programming languages such as PCF [6] (a similar model has simultaneously been obtained in [7]), also augmented with control operators [8] and higher-order references [9]. In these games, plays are interactions traces between a program (player P) and an environment (opponent O). A program is interpreted by a strategy for P which represents the interactions it can have with any environment.

In this paper, we devise a notion of realizability for HON general games based on winning conditions on plays. We show that our model is sound for classical Peano arithmetic and allows to perform extraction for Π_2^0-formulas.

HON games with winning conditions on plays have been used in e.g. [10] for intuitionistic propositional logic with fixpoints. Our winning conditions can be seen as a generalization of the ones of [10] in order to handle full first-order classical logic, while [10] only deals with totality. Our witness extraction is based on a version of Friedman's trick inspired from Krivine [4]. Classical logic is handled similarly to the unbracketed game model of PCF of [8].

We start from the cartesian closed category of single-threaded strategies which contains the unbracketed and non-innocent strategies used to model control operators and references. We use a category of continuations in the coproduct completion of [11], so that the usual flat arena of natural numbers in HON games is indeed in the image of a negative translation. Our realizability is then obtained by equipping arenas with winning conditions on plays.

The paper is organized as follows. Section 2 recalls the game semantics framework and how to interpret $\lambda\mu$-calculus in it. Section 3 defines the notion of winning strategies. Section 4 contains the definition of our realizability relation and its adequacy for classical logic. Section 5 applies our realizability model to Peano arithmetic and shows witness extraction for Π^0_2-formulas.

2 HON Games

Our realizability model is based on the Hyland-Ong-Nickau games [6] with no bracketing or innocence constraint, so as to model control operators and references [8, 9]. We consider single-threaded strategies in order to have a cartesian closed category.

2.1 Arenas and Strategies

Definition 1 (Arena). *An* arena *is a countable forest of* moves*. Each move is given a polarity O (for Opponent) or P (for Player or Proponent):*

- *A root is of polarity O.*
- *A move which is not a root has the inverse polarity of that of his parent.*

A root of an arena is also called an initial move. We will often identify an arena with its set of moves.

Definition 2 (Justified sequence). *Given an arena $\mathcal{A}$, we define a* justified sequence *on $\mathcal{A}$ to be a word s (finite or infinite) of $\mathcal{A}$ together with a partial* justifying function *$f : |s| \rightharpoonup |s|$ such that:*

- *If $f(i)$ is undefined, then s_i is an initial move.*
- *If $f(i)$ is defined, then $f(i) < i$ and s_i is a child of $s_{f(i)}$.*

We denote the empty justified sequence by ϵ. Remark here that by definition of the polarity, if $f(i)$ is undefined (s_i is initial), then s_i is of polarity O, and if $f(i)$ is defined, then s_i and $s_{f(i)}$ are of opposite polarities. Also, $f(0)$ is never defined, and so s_0 is always an initial O-move. A justified sequence is represented for example as:

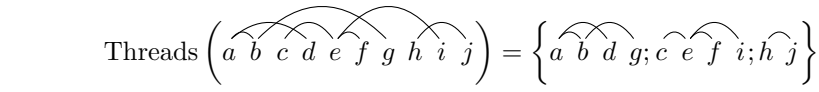
A subsequence of a justified sequence s is a subword of s together with a justifying function defined accordingly. In particular if a move a points to a move b in the original sequence and if a is in the subsequence but b is not, then the pointer

from a is left undefined. For example the following sequence is a subsequence of the one above:

If $\mathcal{A}$ is an arena, X is a subset of $\mathcal{A}$ and s is a justified sequence on $\mathcal{A}$, then $s_{|X}$ is the subsequence of s consisting of the moves of s which are in X.
In a sequence s, a move s_j is hereditarily justified by a move s_i if s_i is initial and for some n, $f^n(j) = i$.

Definition 3 (Thread). *If s is a justified sequence on $\mathcal{A}$ and if s_i is initial, then the* thread associated *to s_i is the subsequence of s consisting of the moves hereditarily justified by s_i. The* set of threads *of s,* Threads(s)*, is the set of threads associated to the initial moves of s.*

For example we have:



Warning. Note that a thread is a justified sequence which may not be alternating, so our definition of thread differs from the usual one.

By extension a justified sequence s will be called a thread if it contains exactly one thread (i.e. Threads(s) = $\{s\}$). Remark that Threads(ϵ) = $\emptyset$ and so ϵ is not a thread.
A P-sequence (resp. O-sequence) is a sequence ending with a P-move (resp. a O-move). Write $t \sqsubseteq s$ if t is a prefix of s, i.e. t is a prefix of s as a word and their justifying functions coincide (this is a particular case of subsequence). Write $t \sqsubseteq_P s$ (resp. $t \sqsubseteq_O s$) if t is a P-prefix (resp. O-prefix) of s, i.e. $t \sqsubseteq s$ and t is a P-sequence (resp. O-sequence).

Definition 4 (Play). *A* play *s on $\mathcal{A}$ is an alternating justified sequence of $\mathcal{A}$, i.e., for any i, s_{2i} is a O-move and s_{2i+1} is a P-move. We denote the set of plays of $\mathcal{A}$ by $\mathcal{P}_{\mathcal{A}}$.*

A play on an arena is the trace of an interaction between a program and a context, each one performing an action alternatively. A P-play (resp. O-play) is a play which is a P-sequence (resp. O-sequence).

Definition 5 (Strategy). *A* strategy *σ on $\mathcal{A}$ is a P-prefix-closed set of finite P-plays on $\mathcal{A}$ such that:*

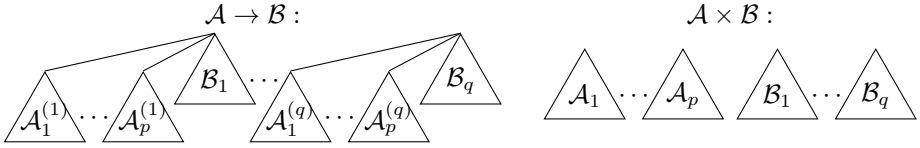
- *σ is deterministic: if sm and sm' are in σ, then $m = m'$.*
- *σ is single-threaded: for any P-play s, $s \in \sigma \Leftrightarrow$ Threads(s) $\subseteq \sigma$.*

Our notion of single-threadedness matches the usual one of thread-independence (see e.g. [9]). Remark also that a strategy always contains the empty play ϵ since $Threads(\epsilon) = \emptyset$.

2.2 Cartesian Closed Structure

The constructions we use will sometimes contain multiple copies of the same arena (for example $\mathcal{A} \to \mathcal{A}$), so we distinguish the instances with superscripts (for example $\mathcal{A}^{(1)} \to \mathcal{A}^{(2)}$).

Let $\mathcal{U}$ be the empty arena and $\mathcal{V}$ be the arena with only one (opponent) move. If $\mathcal{A}$ and $\mathcal{B}$ are arenas consisting of the trees $\mathcal{A}_1 \dots \mathcal{A}_p$ and $\mathcal{B}_1 \dots \mathcal{B}_q$, then the arenas $\mathcal{A} \to \mathcal{B}$ and $\mathcal{A} \times \mathcal{B}$ can be represented as follows:



The constructions described here define a cartesian closed category whose objects are arenas and morphisms are strategies. Details of the construction can be found in [12]. In the following this category will be denoted as $\mathcal{C}$.

These definitions of arenas will be used to associate arenas to the following simple types:

Definition 6 (Simple types). *The* simple types *are defined by the following grammar, where ι ranges over a set of base types:*

$$T, U \;:=\; \iota \mid \mathsf{void} \mid \mathsf{unit} \mid T \times U \mid T \to U$$

We suppose given an object $[\![\iota]\!]$ of $\mathcal{C}$ for each base type ι, and we associate to each simple type T an object $[\![T]\!]$ of $\mathcal{C}$ as follows:

$$[\![\mathsf{void}]\!] = \mathcal{V} \qquad [\![\mathsf{unit}]\!] = \mathcal{U} \qquad [\![T \times U]\!] = [\![T]\!] \times [\![U]\!] \qquad [\![T \to U]\!] = [\![U]\!]^{[\![T]\!]}$$

Since $\mathcal{C}$ is cartesian closed, we use the syntax of λ-calculus to define strategies from other strategies. In order to distinguish this notation from the $\lambda\mu$-terms of Sect. 2.3 we use a bold lambda $\boldsymbol{\lambda}$.

2.3 Interpretation of the call-by-name $\lambda\mu$-calculus

We map classical proofs to strategies using the interpretation of call-by-name $\lambda\mu$-calculus in categories of continuations described in [13]. In order to make explicit the double negation translation of the base types, we base the model on the category of continuations $R^{\mathrm{Fam}(\mathcal{C})}$, where the response category $\mathrm{Fam}(\mathcal{C})$ is a variant of the coproduct completion described in [11] applied to the category $\mathcal{C}$ defined in Sect. 2.2:

Definition 7 ($\mathrm{Fam}(\mathcal{C})$). *The objects of $\mathrm{Fam}(\mathcal{C})$ are families of objects of $\mathcal{C}$ indexed by at most countable sets, and a morphism from $\{A_i \mid i \in I\}$ to $\{B_j \mid j \in J\}$ is a function $f : I \to J$ together with a family of morphisms of $\mathcal{C}$ from A_i to $B_{f(i)}$, for $i \in I$.*

Remark here that we differ from [11] because $\mathcal{C}$ doesn't have weak coproducts nor all small products, and the families are countable. Thus $\mathrm{Fam}(\mathcal{C})$ is not bicartesian closed, but since $\mathcal{C}$ is cartesian closed and has countable products, $\mathrm{Fam}(\mathcal{C})$ is still a distributive category with finite products and coproducts, and has exponentials of all singleton families. The empty product and terminal object is the singleton family $\{1\}$, the empty sum and initial object is the empty family $\{\}$, and:

$$\{A_i \mid i \in I\} \times \{B_j \mid j \in J\} = \{A_i \times B_j \mid (i,j) \in I \times J\}$$
$$\{A_i \mid i \in I\} + \{B_j \mid j \in J\} = \{C_k \mid k \in I \uplus J\} \text{ where } C_k = \begin{cases} A_k \text{ if } k \in I \\ B_k \text{ if } k \in J \end{cases}$$
$$\{B_0\}^{\{A_i \mid i \in I\}} = \{\Pi_{i \in I} B_0^{A_i}\}$$

We fix once and for all:

$$R = \{\mathcal{V}\} = \{[\![\mathsf{void}]\!]\}$$

which is an object of $\mathrm{Fam}(\mathcal{C})$ as a singleton family. R has all exponentials as stated above. Note that the canonical morphism $\delta_A : A \to R^{(R^A)}$ is a mono.

The category of continuations $R^{\mathrm{Fam}(\mathcal{C})}$ is the full subcategory of $\mathrm{Fam}(\mathcal{C})$ consisting of the objects of the form R^A. The objects of $R^{\mathrm{Fam}(\mathcal{C})}$ are singleton families, and $R^{\mathrm{Fam}(\mathcal{C})}$ is isomorphic to $\mathcal{C}$. We will consider that objects and morphisms of $R^{\mathrm{Fam}(\mathcal{C})}$ are arenas and strategies and we will use the vocabulary defined at the end of Sect. 2.2 on $R^{\mathrm{Fam}(\mathcal{C})}$ also.

Interpreting the call-by-name $\lambda\mu$-calculus. The types of $\lambda\mu$-calculus are the simple types of Definition 6. Let k^T range over a set of typed constants and x^T (resp. α^T) range over a countable set of variables (resp. names) for each type T. The grammar of $\lambda\mu$-terms is the following:

$$M, N \;:=\; k^T \mid x^T \mid * \mid \langle M, N\rangle \mid \pi_1 M \mid \pi_2 M \mid \lambda x^T.M \mid MN \mid \mu\alpha^T.M \mid [\alpha]M$$

The typing rules can be found in [13], where our unit is their $\top$, our $\times$ is their $\wedge$ and our void is their $\bot$. For instance, the Law of Peirce is the type of the following term (we omit the type annotation of the variables).

$$\lambda x.\mu\alpha.[\alpha]s(\lambda y.\mu\beta.[\alpha]y) : ((T \to U) \to T) \to T \tag{1}$$

This $\lambda\mu$-term will be denoted cc.

We follow [13] to interpret call-by-name $\lambda\mu$-calculus in $R^{\mathrm{Fam}(\mathcal{C})}$. In particular if M is a $\lambda\mu$-term of type T with free variables in $\{x_1^{T_1}, \ldots, x_n^{T_n}\}$, then its interpretation is a morphism $[\![M]\!]$ from $[\![T_1]\!] \times \ldots \times [\![T_n]\!]$ to $[\![T]\!]$. This morphism coincides with the interpretation of the call-by-name CPS translation of M (defined in [13]) in the cartesian closed category $R^{\mathrm{Fam}(\mathcal{C})}$. See [13] for details. As stated in [13], if the call-by-name CPS translations of two terms are $\beta\eta$-equivalent, then their interpretations are the same.

In the following we will drop the double brackets for the interpretation of simple types.

3 Winning Conditions on Arenas

We will now define our notion of realizability. We equip arenas with winning conditions on threads. Realizers are then winning strategies, intuitively strategies which threads are all winning.

It is well-known that preservation of totality by composition of strategies is problematic in game semantics. Luckily we do not need to preserve totality, but only winningness. We thus do not impose any totality condition on strategies, but when it turns to the definition of winning threads, we have to take into account all maximal threads, including both infinite and odd-length threads. This leads to the notion of winning strategy proposed in Definition 12.

In order to define the notion of winning condition on an arena we introduce the notion of P-subthread and O-subthread:

Definition 8 (P-subthread, O-subthread). *If t is a thread and u is a subsequence of t which is a thread, then u is a:*

- *P-subthread of t if when m^O points to n^P in t and $n^P \in u$, then $m^O \in u$,*
- *O-subthread of t if when m^P points to n^O in t and $n^O \in u$, then $m^P \in u$.*

Now we can define the notion of winning condition on an arena:

Definition 9 (Winning condition). *A* winning condition *on $\mathcal{A}$ is a set $\mathcal{W}$ of threads on $\mathcal{A}$ such that:*

- *If t is a thread on $\mathcal{A}$ and if some P-subthread of t is in $\mathcal{W}$, then $t \in \mathcal{W}$.*
- *If $t \in \mathcal{W}$ then all the O-subthreads of t are in $\mathcal{W}$.*

A justified sequence s on the arena $\mathcal{A}$ equipped with the winning condition $\mathcal{W}$ is said to be winning *if* $\mathrm{Threads}(s) \subseteq \mathcal{W}$.

Our notion of winning sequence can be seen as a generalization of the one defined in [10]. In order to obtain a realizability model of first-order logic, the notion of winning sequence is non-trivial and there can be odd-length sequences which are winning and even-length sequences which are losing.
Remark that if t is a thread on $\mathcal{A} \to \mathcal{B}$, then $t_{|\mathcal{B}}$ is a thread on $\mathcal{B}$, so $t_{|\mathcal{B}}$ is winning iff $t_{|\mathcal{B}} \in \mathcal{W}_{\mathcal{B}}$, and if t is a thread on $\mathcal{A} \times \mathcal{B}$, then t is either a thread on $\mathcal{A}$, either a thread on $\mathcal{B}$.

Definition 10 (Arrow and product of winning conditions). *If $W_{\mathcal{A}}$ and $W_{\mathcal{B}}$ are sets of threads on the arenas $\mathcal{A}$ and $\mathcal{B}$, then we define:*

$$W_{\mathcal{A}\to\mathcal{B}} = \{t \text{ thread on } \mathcal{A} \to \mathcal{B} \mid \mathrm{Threads}(t_{|\mathcal{A}}) \subseteq W_{\mathcal{A}} \;\Rightarrow\; t_{|\mathcal{B}} \in W_{\mathcal{B}}\}$$

$$W_{\mathcal{A}\times\mathcal{B}} = \left\{ t \text{ thread on } \mathcal{A}\times\mathcal{B} \;\middle|\; \begin{array}{l} t \text{ thread on } \mathcal{A} \;\Rightarrow\; t \in W_{\mathcal{A}} \\ t \text{ thread on } \mathcal{B} \;\Rightarrow\; t \in W_{\mathcal{B}} \end{array} \right\}$$

Lemma 1. *If $W_{\mathcal{A}}$ and $W_{\mathcal{B}}$ are winning conditions on $\mathcal{A}$ and $\mathcal{B}$, then $W_{\mathcal{A}\to\mathcal{B}}$ is a winning condition on $\mathcal{A} \to \mathcal{B}$ and $W_{\mathcal{A}\times\mathcal{B}}$ is a winning condition on $\mathcal{A} \times \mathcal{B}$.*

Winning Strategies. In order to define what is a winning strategy, we use a notion of augmented plays of a strategy inspired from [14]:

Definition 11 (Augmented play). *If σ is a strategy on $\mathcal{A}$, then s is an* augmented play *of σ if one of the following holds:*

- $s \in \sigma$, *or*
- $s \in \mathcal{P}_{\mathcal{A}}$ *is such that* $\forall t \sqsubset_P s, t \in \sigma$ *and* $\forall t \in \sigma, s \not\sqsubseteq t$.

In particular, in the second case of the above definition, s is either a O-sequence, either an infinite sequence (in which case $s \sqsubseteq t \Leftrightarrow s = t$ and so the second condition, equivalent to $s \notin \sigma$, is always true). Remark that unlike [14], we consider not only odd-length extensions (with an O-move), but also infinite ones.

Definition 12 (Winning strategy). *If σ is a strategy on the arena $\mathcal{A}$ equipped with the winning condition $\mathcal{W}$, then σ is said to be* winning *if all its augmented plays are winning.*

The following lemma will be useful to prove that a strategy σ is winning on $(\mathcal{A}, \mathcal{W})$.

Lemma 2. *If σ is a strategy on $\mathcal{A}$ and if s is an augmented play of σ, then every $t \in Threads(s)$ is an augmented play of σ.*

Using this lemma it is sufficient to prove that every augmented play of σ which is a thread (let us call it an augmented thread of σ) is in $\mathcal{W}_{\mathcal{A}}$ in order to prove that σ is winning on $(\mathcal{A}, \mathcal{W}_{\mathcal{A}})$.

We now prove that the winning conditions on the arrow and product are compatible with application and pairing of strategies.

Lemma 3. *If σ is a winning strategy on $(\mathcal{A} \to \mathcal{B}, \mathcal{W}_{\mathcal{A}\to\mathcal{B}})$ and τ is a winning strategy on $(\mathcal{A}, \mathcal{W}_{\mathcal{A}})$, then $\sigma(\tau)$ is a winning strategy on $(\mathcal{B}, \mathcal{W}_{\mathcal{B}})$.*

Proof. Let t be an augmented thread of $\sigma(\tau)$. By definition of composition of strategies, there is some augmented play u of σ such that $u_{|\mathcal{A}}$ is an augmented play of τ and $u_{|\mathcal{B}} = t$. Since t is a thread, u is also a thread, so since σ is winning on $\mathcal{A} \to \mathcal{B}$, $u \in \mathcal{W}_{\mathcal{A}\to\mathcal{B}}$. $u_{|\mathcal{A}}$ is an augmented play of τ which is winning on $\mathcal{A}$, so $u_{|\mathcal{B}}$ is winning, and so $t = u_{|\mathcal{B}}$ is a winning thread: $t \in \mathcal{W}_{\mathcal{B}}$. Therefore $\sigma(\tau)$ is winning. □

Lemma 4. *If σ is a winning strategy on $(\mathcal{A}, \mathcal{W}_{\mathcal{A}})$ and τ is a winning strategy on $(\mathcal{B}, \mathcal{W}_{\mathcal{B}})$, then $\langle \sigma, \tau \rangle$ is a winning strategy on $(\mathcal{A} \times \mathcal{B}, \mathcal{W}_{\mathcal{A}\times\mathcal{B}})$.*

Proof. Let t be an augmented thread of $\sigma(\tau)$. By definition of product of strategies, $t_{|\mathcal{A}}$ is an augmented play of σ and $t_{|\mathcal{B}}$ is an augmented play of τ, so since σ and τ are winning, $t_{|\mathcal{A}}$ and $t_{|\mathcal{B}}$ are winning, and so $t \in \mathcal{W}_{\mathcal{A}\times\mathcal{B}}$. Therefore $\langle \sigma, \tau \rangle$ is winning. □

The following technical lemma on the interpretation of cc will be useful.

Lemma 5. *If t is an augmented thread of $[\![\mathsf{cc}]\!]$ on the arena $((T \to U) \to T) \to T$ (written $((T^{(1)} \to U) \to T^{(2)}) \to T^{(3)}$), then the threads of $t_{|T^{(1)}}$ and $t_{|T^{(2)}}$ are P-subthreads of $t_{|T^{(3)}}$.*

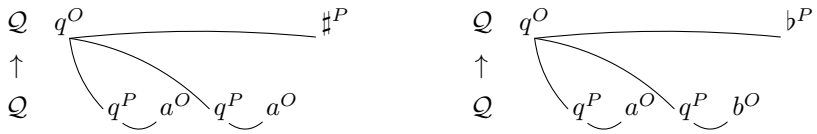
It follows easily from this lemma and Lemma 1 that for any winning conditions W_T and W_U, $[\![\mathsf{cc}]\!]$ is winning on the arena

$$\Big(((T \to U) \to T) \to T, W_{((T\to U)\to T)\to T)}\Big)$$

Remark on the arrow on winning conditions. Let $\mathcal{A}, \mathcal{B}$ be arenas equipped with winning conditions $W_\mathcal{A}$, $W_\mathcal{B}$. We define here a strategy σ on $\mathcal{A} \to \mathcal{B}$ such that for any winning strategy τ on $\mathcal{A}$, $\sigma(\tau)$ is winning on $\mathcal{B}$, but σ is not winning on $\mathcal{A} \to \mathcal{B}$. Hence the arrow on winning conditions differs from the usual Kleene realizability arrow (see [1]).
We choose $\mathcal{A}$ and $\mathcal{B}$ to be the same arena $\mathcal{Q}$ consisting of one root with three children $\sharp$, $\flat$ and $\natural$, equipped with the winning condition

$$\mathcal{W}_\mathcal{Q} = \{q^O a_1^P a_2^P \dots \mid \exists i, a_i \in \{\sharp, \natural\}\}$$

where the threads may be finite or infinite. We define a strategy σ on $\mathcal{Q} \to \mathcal{Q}$ such that for any τ winning on $(\mathcal{Q}, \mathcal{W}_\mathcal{Q})$, $\sigma(\tau)$ is winning on $(\mathcal{Q}, \mathcal{W}_\mathcal{Q})$, but σ is not winning on $(\mathcal{Q} \to \mathcal{Q}, \mathcal{W}_{\mathcal{Q}\to\mathcal{Q}})$. σ is the innocent strategy defined by the views:



where a and b are distinct moves. The interaction with any single threaded strategy will produce the left view, and so the projection $q^O\sharp^P$ will be winning, but the right view (which will never happen in an interaction with a single-threaded strategy) with $a = \sharp$ and $b = \natural$ is losing, so σ is losing.

4 First-order Logic

We define a realizability model for first-order classical logic with possibilities of witness extraction. For that the proposition $\bot$ will be mapped to an arena ι in general different from $\mathcal{V}$. Its associated winning condition will be a parameter of the model, in the spirit of [4].

Let x range over a countable set of variables, f range over a set of function symbols with fixed finite arity and P range over a set of predicate symbols with fixed finite arity. First-order terms and formulas are defined by the following grammar:

$$a, b \;:=\; x \mid f(a_1, \dots, a_n)$$
$$A, B \;:=\; P(a_1, \dots, a_n) \mid \top \mid A \wedge B \mid A \Rightarrow B \mid \forall x A \mid \bot$$

In the following we use syntactic sugar for the negation of formulas: $\neg A \equiv A \Rightarrow \bot$ and for the existential: $\exists x A \equiv \neg\forall x \neg A$. We fix a countable first-order structure interpreting the terms of our logic, that is a countable set E together with an interpretation $f^E : E^n \to E$ for each function symbol. The interpretation is extended to every closed term: if a is a closed term of the logic, then a^E denotes its interpretation in the first-order structure, so a^E is an element of E.

4.1 Realizability

We let $\perp\!\!\!\perp$ be an arbitrary subset of E. We consider simple types with a type constant P^* for each predicate P and a type constant ι to interpret $\bot$. We can map any first-order formula A to such a simple type A^* as follows:

$$(P(a_1,\dots,a_n))^* = P^* \qquad \top^* = \mathsf{unit} \qquad (A \wedge B)^* = A^* \times B^*$$

$$(A \Rightarrow B)^* = A^* \to B^* \qquad (\forall x A)^* = A^* \qquad \bot^* = \iota$$

Remark that the type $\bot^*$ is not the type void because the associated arena would be too small to hold informational content.

Recall that we omit the double bracket notation for the arenas, so a type T also denotes the associated arena. We suppose that for each atomic predicate P, the type P^* comes with its associated arena. We fix the arena associated to ι to be $R^{(R^{\mathbf{E}})}$, where $\mathbf{E} = \{\mathcal{U}_e \mid e \in E\}$ is the countable family of empty arenas (and $R = \{\mathcal{V}\}$). Hence ι is the usual flat arena for the set E.

Let us suppose we associate to each predicate $P(a_1,\dots,a_n)$ with $a_1,\dots,a_n$ closed first-order terms a winning condition $\mathcal{W}_{P(a_1,\dots,a_n)}$ on the arena P^*. We can then define for each closed first-order formula A a winning condition $\mathcal{W}_A$ on the arena A^*. The winning conditions $\mathcal{W}_{A\wedge B}$ and $\mathcal{W}_{A\Rightarrow B}$ are as in Definition 10, and we let:

$$\mathcal{W}_\top = \emptyset \qquad \mathcal{W}_{\forall x A} = \bigcap_{a \text{ closed}} \mathcal{W}_{A[a/x]} \qquad \mathcal{W}_\bot = \{q^O m_1^P m_2^P \dots \mid \exists i, m_i \in \perp\!\!\!\perp\}$$

Note that these are indeed winning conditions. For $\mathcal{W}_\top$, the empty set is a winning condition on $\mathcal{U}$ which is the empty arena with no thread. For $\mathcal{W}_{\forall x A}$, it is easy to see that an intersection of winning conditions is a winning condition. For $\mathcal{W}_\bot$, the thread $q^O m_1^P m_2^P \dots$ (that may be finite or infinite) has only itself as O-subthread and $q^O m_{i_1}^P m_{i_2}^P \dots$ for $1 \le i_1 < i_2 \le \dots$ as P-subthreads so $\mathcal{W}_\bot$ is a winning condition on ι.

We can now define our notion of realizability:

Definition 13 (Realizability relation). *If A is a closed first-order formula and if σ is a strategy on A^*, then σ realizes A (denoted $\sigma \Vdash A$) if σ is a winning strategy on $(A^*, \mathcal{W}_A)$.*

The following lemma shows that the identity formulas are realized by the corresponding identity strategies.

Lemma 6. *If A is a closed formula, then the identity strategy id_{A^*} on A^* is a realizer for the formula $A \Rightarrow A$.*

Proof. Let $\mathcal{A}^{(1)} \to \mathcal{A}^{(2)}$ denote the arena $A^* \to A^*$. If t is an augmented thread of id_{A^*}, then $t_{|\mathcal{A}^{(1)}} = t_{\mathcal{A}^{(2)}}$, so if $t_{|\mathcal{A}^{(1)}}$ is winning, then $t_{|\mathcal{A}^{(2)}} = t_{\mathcal{A}^{(1)}}$ is also winning, and so $t \in \mathcal{W}_{A^*}$. □

The following result is a consequence of the remark following Lemma 5.

Lemma 7. *If A and B are closed formulas, then* $\mathsf{cc} \Vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A$.

4.2 Adequacy for Minimal Classical Logic

We now show that realizability is compatible with deduction in minimal classical logic. Full classical logic is discussed in Sect. 4.3.

Deduction system. Let $\boldsymbol{Ax}$ be a set of closed formulas. We use the following deduction system based on natural deduction with a rule for the law of Peirce, where Γ is a sequence of formulas $A_1, \ldots, A_n$.

$$\frac{}{\Gamma \vdash A}\ {\scriptstyle A \in \Phi} \qquad \frac{}{\Gamma \vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A} \qquad \frac{}{\Gamma \vdash A}\ {\scriptstyle A \in \boldsymbol{Ax}}$$

$$\frac{}{\Gamma \vdash \top} \qquad \frac{\Gamma \vdash A \qquad \Gamma \vdash B}{\Gamma \vdash A \wedge B} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash A} \qquad \frac{\Gamma \vdash A \wedge B}{\Gamma \vdash B}$$

$$\frac{\Gamma, A \vdash B}{\Gamma \vdash A \Rightarrow B} \qquad \frac{\Gamma \vdash A \Rightarrow B \qquad \Gamma \vdash A}{\Gamma \vdash B}$$

$$\frac{\Gamma \vdash A}{\Gamma \vdash \forall x A}\ {\scriptstyle x \notin FV(\Gamma)} \qquad \frac{\Gamma \vdash \forall x A}{\Gamma \vdash A[a/x]}$$

Remark that $\bot$ has no associated rule, since the ex-falso rule has a particular status, given the interpretation of $\bot$. This will be discussed in Sect. 4.3.

Translation of proofs to strategies. We use $\lambda\mu$-calculus and its interpretation in $R^{\mathrm{Fam}(\mathcal{C})}$ to map a first-order proof to a typed $\lambda\mu$-term which is then interpreted in $R^{\mathrm{Fam}(\mathcal{C})}$ as a strategy.

Assume given a constant k^A of type A^* for each $A \in \boldsymbol{Ax}$. We map a derivation ν of $A_1, \ldots, A_n \vdash A$ to a typed $\lambda\mu$-term ν^* of type A with free variables among $x^{A_1^*}, \ldots, x^{A_n^*}$ as follows:

$$\frac{}{A_1, \ldots, A_n \vdash A_i} \rightsquigarrow x^{A_i^*} \qquad \frac{}{\Gamma \vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A} \rightsquigarrow \mathsf{cc}\ \text{(see (1))}$$

$$\frac{\dfrac{\nu}{\Gamma \vdash A} \qquad \dfrac{\nu'}{\Gamma \vdash B}}{\Gamma \vdash A \wedge B} \rightsquigarrow \langle \nu^*, \nu'^* \rangle \qquad \frac{}{\Gamma \vdash \top} \rightsquigarrow * \qquad \frac{}{\Gamma \vdash A}\ {\scriptstyle A \in \boldsymbol{Ax}} \rightsquigarrow k^A$$

$$\frac{\dfrac{\nu}{\Gamma \vdash A \wedge B}}{\Gamma \vdash A} \rightsquigarrow \pi_1 \nu^* \qquad \frac{\dfrac{\nu}{\Gamma \vdash A}}{\Gamma \vdash \forall x A}\ {\scriptstyle x \notin FV(\Gamma)} \rightsquigarrow \nu^* \qquad \frac{\dfrac{\nu}{\Gamma, A \vdash B}}{\Gamma \vdash A \Rightarrow B} \rightsquigarrow \lambda x^{A^*}.\nu^*$$

$$\frac{\dfrac{\nu}{\Gamma \vdash A \wedge B}}{\Gamma \vdash B} \rightsquigarrow \pi_2 \nu^* \qquad \frac{\dfrac{\nu}{\Gamma \vdash \forall x A}}{\Gamma \vdash A[a/x]} \rightsquigarrow \nu^* \qquad \frac{\dfrac{\nu}{\Gamma \vdash A \Rightarrow B} \quad \dfrac{\nu'}{\Gamma \vdash A}}{\Gamma \vdash B} \rightsquigarrow \nu^*(\nu'^*)$$

Adequacy. We now prove that the strategies interpreting the proofs are realizers of the proved formula. If A is a formula and θ an assignment of terms to variables, then $\theta(A)$ denotes A where all the free variables are replaced with their image by θ.

Lemma 8. *Let $\perp\!\!\!\perp \subseteq E$. Suppose that we have a realizer for each formula of $\boldsymbol{Ax}$. If ν is a derivation of the sequent $\Gamma \vdash A$ and if θ is an assignment of closed first-order terms to variables, then $[\![\nu^*]\!]$ is a winning strategy on $\Gamma^* \to A^*$ equipped with $\mathcal{W}_{\theta(\Gamma \Rightarrow A)}$.*

Proof (sketch). The case of the variable follows from Lemma 6. That of cc comes from Lemma 5. Product introduction is dealt with using Lemma 4, and arrow elimination using Lemma 3. The other cases are straightforward. □

4.3 Full Classical Logic

In order to get full classical logic we need to add an ex-falso rule. However since the arena $\perp^*$ is not empty (see Sect. 4.1), we restrict ex-falso to a certain class of formulas. We have to ensure that $(\iota, \mathcal{W}_\perp)$ is included in $(A^*, \mathcal{W}_A)$. This means that ι is a subtree of A^*, so a play on ι is in particular a play on A^*, and that $\mathcal{W}_\perp \subseteq \mathcal{W}_A$. We will call these formulas explodable since they satisfy the principle of explosion. We add to our deduction system the following rule:

$$\frac{\Gamma \vdash \perp}{\Gamma \vdash A}\ A \text{ explodable}$$

In particular any formula ending with $\perp$ is explodable, where a formula ending with $\perp$ is a formula generated by the grammar:

$$C, D \ := \ C \wedge D \mid A \Rightarrow C \mid \forall x C \mid \perp$$

where A is any first-order formula (defined in Sect. 4). The corresponding adequacy lemma is immediate from Lemma 8.

4.4 First-order Logic with Equality

We now show how to handle equality. We suppose that our first-order language contains an inequality predicate $\neq$ of arity 2 interpreted by the simple type ι (see Sect. 4.1). The associated winning condition is:

$$\mathcal{W}_{a \neq b} = \begin{cases} \mathcal{W}_\perp & \text{if } a^E = b^E \\ \text{the set of all threads on } \iota & \text{otherwise} \end{cases}$$

(recall that E is the first-order structure chosen at the beginning of Sect. 4). It is easy then to verify that any formula ending with the predicate $a \neq b$ is

explodable. In the following we use the notation $(a = b) \equiv \neg(a \neq b)$. The axioms for equality are:

$$\textbf{(refl)} \quad \forall x(x = x) \qquad\qquad \textbf{(Leib)} \quad \forall x \forall y(\neg A[x] \Rightarrow A[y] \Rightarrow x \neq y)$$

Recall that $\forall x(x = x)$ is only syntactic sugar for $\forall x(x \neq x \Rightarrow \bot)$, and that $\forall x \forall y(\neg A[x] \Rightarrow A[y] \Rightarrow x \neq y)$ is also syntactic sugar for $\forall x \forall y((A[x] \Rightarrow \bot) \Rightarrow A[y] \Rightarrow x \neq y)$.

Lemma 9. *Let $\perp\!\!\!\perp \subseteq E$.*

1. *The identity strategy on ι, is a realizer of* **(refl)**.
2. *The identity strategy on $A^* \to \iota$, is a realizer of* **(Leib)**.

Proof (sketch). For the first point, we always have $a^E = a^E$, so $\mathcal{W}_{a \neq a} = \mathcal{W}_\bot$. Concerning the second point,if a and b are closed first-order terms, if $a^E \neq b^E$ then any thread is winning on $a \neq b$, otherwise if we win on $A[b]$ then we win on $A[a]$, so if we win on $\neg A[a]$ then we win on $\bot$ and therefore on $a \neq b$. □

5 Peano Arithmetic

We now proceed to the realizability interpretation of full Peano arithmetic.

5.1 Definitions

Our first-order language is built from the function symbols 0 of arity 0, S of arity 1 and $+$ and $\times$ of arity 2. The predicate symbols are $\neq$ of arity 2 and nat of arity 1. This choice of function symbols is only for simplicity, and we could choose to have all the symbols of primitive recursive functions.

We also fix the structure interpreting the terms of the logic to be the set of natural numbers $\mathbb{N}$. The symbols 0, S, $+$ and $\times$ are interpreted the standard way. The typed $\lambda\mu$-calculus in which we interpret the proofs has ι as unique base type. All the predicate symbols and $\bot$ are interpreted as ι, and the associated arena in $R^{\mathrm{Fam}(\mathcal{C})}$ is $[\![\iota]\!] = R^{\left(R^{\mathbf{N}}\right)}$ where $\mathbf{N} = \{\mathcal{U}_n \mid n \in \mathbb{N}\}$ (see Sect. 4.1). Hence the type of natural numbers is interpreted as the negative translation of $\mathbf{N}$. Note that this is the usual flat arena of natural numbers:

This differs from Laird's interpretation of PCF with control [15], where the base type of natural numbers is interpreted by the arena $(\iota \to \iota) \to \iota$.

The winning conditions for $\bot$ and $a \neq b$ are as in Sects. 4.1 and 4.4, and the winning condition for $\mathsf{nat}(a)$ is:

$$\mathcal{W}_{\mathsf{nat}(a)} = \{q^O n_1^P n_2^P \ldots \mid \exists i, n_i = a^{\mathbb{N}}\}$$

which is a winning condition, using the same arguments as for $\mathcal{W}_\perp$. From this we can check that every formula which contains no $\mathsf{nat}(a)$ predicate at rightmost position is explodable. We use the following syntactic sugar:

$$\forall^{\mathsf{n}} x A \;\equiv\; \forall x\ (\mathsf{nat}(x) \Rightarrow A) \qquad \exists^{\mathsf{n}} x A \;\equiv\; \neg\forall^{\mathsf{n}} x \neg A \;\equiv\; \neg\forall x\ (\mathsf{nat}(x) \Rightarrow \neg A)$$

The relativization A^{n} of a formula is defined as the identity on all constructions except for the quantification: $(\forall x A)^{\mathsf{n}} \;\equiv\; \forall^{\mathsf{n}} x A^{\mathsf{n}}$. Note that if a formula does not contain any $\mathsf{nat}(a)$ predicate, then its relativization has no $\mathsf{nat}(a)$ predicate at rightmost position, so it is explodable.

The axioms are the ones for equality (defined in Sect. 4.4) and the universal closures of:

$(\boldsymbol{Snz})$	$S(x) \neq 0$	$(\boldsymbol{Sinj})$	$x \neq y \Rightarrow S(x) \neq S(y)$
$(\boldsymbol{+0})$	$x + 0 = x$	$(\boldsymbol{nat0})$	$\mathsf{nat}(0)$
$(\boldsymbol{+S})$	$x + S(y) = S(x + y)$	$(\boldsymbol{natS})$	$\mathsf{nat}(x) \Rightarrow \mathsf{nat}(S(x))$
$(\boldsymbol{\times 0})$	$x \times 0 = 0$	$(\boldsymbol{nat+})$	$\mathsf{nat}(x) \Rightarrow \mathsf{nat}(y) \Rightarrow \mathsf{nat}(x + y)$
$(\boldsymbol{\times S})$	$x \times S(y) = x \times y + x$	$(\boldsymbol{nat\times})$	$\mathsf{nat}(x) \Rightarrow \mathsf{nat}(y) \Rightarrow \mathsf{nat}(x \times y)$

$$(\boldsymbol{ind}) \quad A[0] \Rightarrow \forall^{\mathsf{n}} x (A[x] \Rightarrow A[S(x)]) \Rightarrow \forall^{\mathsf{n}} x A[x]$$

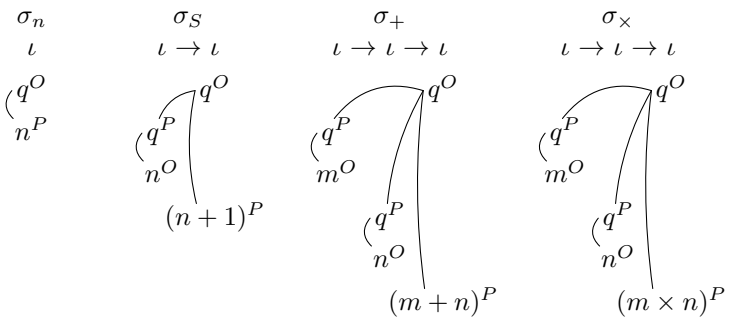
We will now define the realizers for these axioms. We first define the strategies computing basic operations and recursion on natural numbers.

In $\mathrm{Fam}(\mathcal{C})$ a morphism from $\top^* = \{\mathcal{U}\}$ to $\mathbf{N} = \{\mathcal{U}_n \mid n \in \mathbb{N}\}$ is given by a function from the singleton set to $\mathbb{N}$ together with a strategy from $\mathcal{U}$ to $\mathcal{U}$. Since there is only one such strategy, such a morphism is given by a natural number. We will call this morphism τ_n. Similarly a morphism from $\mathbf{N}^k$ to $\mathbf{N}$ is given by a function from $\mathbb{N}^k$ to $\mathbb{N}$. This leads to morphisms τ_S, τ_+ and $\tau_\times$ respectively on $\mathbf{N} \to \mathbf{N}$, $\mathbf{N} \to \mathbf{N} \to \mathbf{N}$ and $\mathbf{N} \to \mathbf{N} \to \mathbf{N}$. From these we define the following morphisms of $R^{\mathrm{Fam}(\mathcal{C})}$:

$$\begin{aligned}
\sigma_n &= \boldsymbol{\lambda} k.k\tau_n \;:\; \iota \\
\sigma_S &= \boldsymbol{\lambda} n.\boldsymbol{\lambda} k.n(\boldsymbol{\lambda} n'.k(\tau_S n')) \;:\; \iota \to \iota \\
\sigma_+ &= \boldsymbol{\lambda} m\boldsymbol{\lambda} n.\boldsymbol{\lambda} k.m(\boldsymbol{\lambda} m'.n(\boldsymbol{\lambda} n'.k(\tau_+ m' n'))) \;:\; \iota \to \iota \to \iota \\
\sigma_\times &= \boldsymbol{\lambda} m\boldsymbol{\lambda} n.\boldsymbol{\lambda} k.m(\boldsymbol{\lambda} m'.n(\boldsymbol{\lambda} n'.k(\tau_\times m' n'))) \;:\; \iota \to \iota \to \iota
\end{aligned}$$

The above morphisms correspond to the expected strategies:

Lemma 10. *The strategies σ_n, σ_S, σ_+ and $\sigma_\times$ are the innocent strategies defined by the views:*

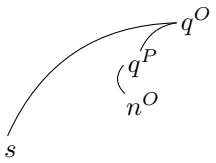


We now move to the definition of ρ^T, the recursor on type T, which is the usual recursor of Gödel's system T. For that we define for each $n \in \mathbb{N}$ and simple type T a strategy ρ_n^T by:

$$\begin{aligned}
&\rho_0^T = [\![\lambda x.\lambda y.x]\!] : T \to (\iota \to T \to T) \to T\\
&\xi^T = [\![\lambda n.\lambda r.\lambda x.\lambda y.y(n)(rxy)]\!]\\
&\qquad\qquad : \iota \to (T \to (\iota \to T \to T) \to T) \to T \to (\iota \to T \to T) \to T\\
&\rho_{n+1}^T = \xi^T(\sigma_n)(\rho_n^T) : T \to (\iota \to T \to T) \to T
\end{aligned}$$

and we finally define the strategy ρ^T as the innocent strategy which views are:

$$T \to (\iota \to T \to T) \to \iota \to T$$



where $q^{\frown O} s$ is a view of ρ_n^T on the subarena $T \to (\iota \to T \to T) \to T$.

We use the following lemma in order to prove the validity of **(*ind*)**:

Lemma 11. *1. ρ_0^T is a realizer of $A[0] \Rightarrow \forall^{\mathsf{n}} x(A[x] \Rightarrow A[S(x)]) \Rightarrow A[0]$*
2. ξ^T is a realizer of:

$$\forall^{\mathsf{n}} y\Big(\Big(A[0] \Rightarrow \forall^{\mathsf{n}} x(A[x] \Rightarrow A[S(x)]) \Rightarrow A[y]\Big) \Rightarrow A[0] \Rightarrow \forall^{\mathsf{n}} x(A[x] \Rightarrow A[S(x)]) \Rightarrow A[S(y)]\Big)$$

Proof. This is an immediate consequence of Lemma 8, since the strategies ρ_0^T and ξ^T are the interpretations of proofs of the formulas.

5.2 Validity of Axioms

We prove that all the axioms are realized:

Lemma 12. *Let $\perp\!\!\!\perp \subseteq \mathbb{N}$.*

1. *The empty strategy on ι is a realizer of* **(*Snz*)**
2. *The identity strategy on ι is a realizer of* **(*Sinj*)**, **(+0)**, **(+*S*)**, **(×0)** *and* **(×*S*)**
3. *σ_0 is a realizer of* **(*nat*0)**
4. *σ_S is a realizer of* **(*natS*)**
5. *σ_+ is a realizer of* **(*nat*+)**
6. *$\sigma_\times$ is a realizer of* **(*nat*×)**
7. *ρ^{A^*} is a realizer of* **(*ind*)**

Proof (sketch). The cases 1 and 2 are straightforward. We prove cases 3, 4, 5 and 6 using Lemma 10. For 7 we prove by induction on n that:

$$\rho_n^{A^*} \Vdash A[0] \Rightarrow \forall^{\mathsf{n}} x(A[x] \Rightarrow A[S(x)]) \Rightarrow A[\overline{n}]$$

using Lemma 11. We finally prove that ρ^{A^*} is a realizer of the (***ind***) axiom for formula A. Let t be an augmented thread of ρ^{A^*} on the arena

$$A^{(1)} \to \left(\iota^{(1)} \to A^{(2)} \to A^{(3)}\right) \to \iota^{(2)} \to A^{(4)}$$

Let suppose that $t_{|A^{(1)}}$ is winning on $A[0]$ and $t_{|\iota^{(1)} \to A^{(2)} \to A^{(3)}}$ is winning on $\forall^{\mathsf{n}} x(A[x] \Rightarrow A[S(x)])$. We want to prove that $t_{|\iota^{(2)} \to A^{(4)}}$ is winning on $\forall x^{\mathsf{n}} A[x]$, so let a be a closed first-order term, let $n = a^{\mathbb{N}}$ and let suppose that $t_{|\iota^{(2)}}$ is winning on $\mathsf{nat}(a)$. Then there must be some n^O in $t_{|\iota^{(2)}}$. Let u be the subsequence of t consisting of the initial q^O, the following q^P, this n^O and all the moves m of t such that the view obtained immediately after m contains n^O. Then u is a play of $\rho_n^{A^*}$. Since a P-move does not change the current view, the threads of $u_{|A^{(1)}}$ are O-subthreads of $t_{|A^{(1)}}$ (the projection induces an inversion of polarities), so they are winning on $A[0]$, and the threads of $u_{|\iota^{(1)} \to A^{(2)} \to A^{(3)}}$ are O-subthreads of $t_{|\iota^{(1)} \to A^{(2)} \to A^{(3)}}$, so they are winning on $\forall^{\mathsf{n}} x(A[x] \Rightarrow A[S(x)])$. Then by the property on $\rho_n^{A^*}$, $u_{|A^{(4)}}$ is winning on $A[a]$. But $u_{|A^{(4)}}$ is a P-subthread of $t_{|A^{(4)}}$ (no inversion here), so $t_{|A^{(4)}}$ is winning on $A[a]$. □

Theorem 1. *If A is provable in Peano arithmetic then there is a computable strategy σ such that $\sigma \Vdash A^{\mathsf{n}}$.*

5.3 Extraction

We now show that from any provable Π_2^0-formula we can extract a computable witnessing function.

Suppose that we have a proof of $\vdash \forall^{\mathsf{n}} x \exists^{\mathsf{n}} y(a = b)$. We obtain by double-negation elimination a proof of $\vdash \forall^{\mathsf{n}} x(\neg\forall^{\mathsf{n}} y(a \neq b))$, and we map it to a strategy σ such that:

$$\sigma \quad \Vdash \quad \forall^{\mathsf{n}} x(\neg\forall^{\mathsf{n}} y(a \neq b)) \;\equiv\; \forall x(\mathsf{nat}(x) \Rightarrow (\forall y(\mathsf{nat}(y) \Rightarrow a \neq b) \Rightarrow \bot)$$

Then if $n \in \mathbb{N}$, $\sigma_n \Vdash \mathsf{nat}(\overline{n})$, so $\sigma(\sigma_n) \Vdash \forall y(\mathsf{nat}(y) \Rightarrow a[\overline{n}/x] \neq b[\overline{n}/x]) \Rightarrow \bot$. Let now fix $\perp\!\!\!\perp = \{m \in \mathbb{N} \mid (a[\overline{n}/x, \overline{m}/y])^{\mathbb{N}} = (b[\overline{n}/x, \overline{m}/y])^{\mathbb{N}}\}$. By a simple disjunction of cases we get

$$id_\iota \Vdash \forall y(\mathsf{nat}(y) \Rightarrow a[\overline{n}/x] \neq b[\overline{n}/x])$$

and therefore $\sigma(\sigma_n)(id_\iota) \Vdash \bot$. Then we can prove that $\sigma(\sigma_n)(id_\iota)$ is some σ_m such that $m \in \perp\!\!\!\perp$. Indeed, if $\sigma(\sigma_n)(id_\iota)$ is the empty strategy then its only augmented play is q^O, which is losing on $\bot$.

6 Conclusion & Future Work

We have built a realizability model for Peano arithmetic using winning conditions on arenas, and have used it in the context of witness extraction for Π^0_2-formulas. Future work will be the comparison of the present model with the game interpretation of classical arithmetic of [16], and with the winning conditions on sequential games of [17] and [18]. Our main goal is to compare two different versions of realizers for the axiom of dependent choices: the modified bar recursion of [19] and the clock of [3].

References

1. Troelstra, A.: Chapter VI Realizability. Studies in Logic and the Foundations of Mathematics **137** (1998) 407–473
2. Griffin, T.: A Formulae-as-Types Notion of Control. In: POPL, ACM Press (1990) 47–58
3. Krivine, J.L.: Dependent choice, 'quote' and the clock. Theor. Comput. Sci. **308**(1-3) (2003) 259–276
4. Krivine, J.L.: Realizability in classical logic. Panoramas et synthèses **27** (2009) 197–229
5. Krivine, J.L.: Typed lambda-calculus in classical Zermelo-Frænkel set theory. Arch. Math. Log. **40**(3) (2001) 189–205
6. Hyland, J.M.E., Ong, C.H.L.: On Full Abstraction for PCF: I, II, and III. Inf. Comput. **163**(2) (2000) 285–408
7. Nickau, H.: Hereditarily Sequential Functionals. In: LFCS, Springer (1994) 253–264
8. Laird, J.: Full Abstraction for Functional Languages with Control. In: LICS, IEEE (1997) 58–67
9. Abramsky, S., Honda, K., McCusker, G.: A Fully Abstract Game Semantics for General References. In: LICS, IEEE (1998) 334–344
10. Clairambault, P.: Least and Greatest Fixpoints in Game Semantics. In: FOSSACS, Springer (2009) 16–31
11. Abramsky, S., McCusker, G.: Call-by-Value Games. In: CSL, Springer (1997) 1–17
12. Harmer, R.: Games and full abstraction for non-deterministic languages. PhD thesis, Imperial College London (University of London) (1999)
13. Selinger, P.: Control categories and duality: on the categorical semantics of the lambda-mu calculus. Mathematical Structures in Computer Science **11**(2) (2001) 207–260
14. Melliès, P.A.: Sequential algorithms and strongly stable functions. Theor. Comput. Sci. **343**(1-2) (2005) 237–281
15. Laird, J.: A semantic analysis of control. PhD thesis, University of Edinburgh. (1999)
16. Coquand, T.: A Semantics of Evidence for Classical Arithmetic. J. Symb. Log. **60**(1) (1995) 325–337
17. Hyland, J.M.E.: Game semantics. In Pitts, A.M., Dybjer, P., eds.: Semantics and logics of computation. Volume 14. Cambridge University Press (1997)
18. Melliès, P.A., Tabareau, N.: Resource modalities in game semantics. In: LICS, IEEE (2007) 389–398
19. Berardi, S., Bezem, M., Coquand, T.: On the Computational Content of the Axiom of Choice. J. Symb. Log. **63**(2) (1998) 600–622

7 Appendix

Lemma 13. *If $W_{\mathcal{A}}$ and $W_{\mathcal{B}}$ are winning conditions on $\mathcal{A}$ and $\mathcal{B}$, then $W_{\mathcal{A}\to\mathcal{B}}$ is a winning condition on $\mathcal{A}\to\mathcal{B}$ and $W_{\mathcal{A}\times\mathcal{B}}$ is a winning condition on $\mathcal{A}\times\mathcal{B}$.*

Proof. – Let t be a thread on $\mathcal{A}\to\mathcal{B}$ and let u be a P-subthread of t such that $u\in W_{\mathcal{A}\to\mathcal{B}}$. Suppose that $Threads(t_{|\mathcal{A}})\subseteq W_{\mathcal{A}}$. If $v\in Threads(u|\mathcal{A})$ then v is a O-subthread of some $w\in Threads(t_{|\mathcal{A}}\subseteq W_{\mathcal{A}}$, so $v\in W_{\mathcal{A}}$. Then since u is winning, $u_{|\mathcal{B}}$ is winning and is a P-subthread of $t_{|\mathcal{B}}$ which is therefore also winning. Finally t is winning.

– Let t be a thread on $\mathcal{A}\to\mathcal{B}$ such that $t\in W_{\mathcal{A}\to\mathcal{B}}$ and let u be a O-subthread of t. Let suppose that $Threads(u_{|\mathcal{A}})\subseteq W_{\mathcal{A}}$. If $v\in Threads(t|\mathcal{A})$ and if m is the initial move of v, then m points to the initial move of t which is a O-move, and since u is a O-subthread of t, we get $m\in u$. Now the thread of $u_{|\mathcal{A}}$ which initial move is m is in $W_{\mathcal{A}}$ and is a P-subthread of v, so $v\in W_{\mathcal{A}}$. Therefore $Threads(t|\mathcal{A})\subseteq W_{\mathcal{A}}$, and since $t\in W_{\mathcal{A}\to\mathcal{B}}$ we have $t_{|\mathcal{B}}\in W_{\mathcal{B}}$, and since $u_{|\mathcal{B}}$ is a O-subthread of $t_{|\mathcal{B}}$, we get $u_{|\mathcal{B}}\in W_{\mathcal{B}}$. Finally $u\in W_{\mathcal{A}\to\mathcal{B}}$.

– Let t be a thread on $\mathcal{A}\times\mathcal{B}$. t is either a thread on $\mathcal{A}$, either a thread on $\mathcal{B}$, so if u is a winning P-subthread of t, then either $u\in W_{\mathcal{A}}$, either $u\in W_{\mathcal{B}}$. Therefore $t\in W_{\mathcal{A}}$ or $t\in W_{\mathcal{B}}$, and so $t\in W_{\mathcal{A}\times\mathcal{B}}$.

– Let t be a thread on $\mathcal{A}\times\mathcal{B}$ such that $t\in W_{\mathcal{A}\times\mathcal{B}}$. Either $t\in W_{\mathcal{A}}$, either $t\in W_{\mathcal{B}}$, so any O-subthread of t is in $W_{\mathcal{A}}$ or $W_{\mathcal{B}}$, so in $W_{\mathcal{A}\times\mathcal{B}}$. □

Lemma 14. *If σ is a strategy on $\mathcal{A}$ and if s is an augmented play of σ, then every $t\in Threads(s)$ is an augmented play of σ.*

Proof. – If $s\in\sigma$, then by single-threadedness of σ, $Threads(s)\subseteq\sigma$.

– If s is an O-sequence, then we write $s=s'm$ with $s'\in\sigma$. Let $t\in Threads(s)$. If m is not a move in t, then $t\in Threads(s')\subseteq\sigma$. If m is a move in t, then we write $t=t'm$, so $t'\in Threads(s')\subseteq\sigma$. If there is some n such that $tn=t'mn\in\sigma$, then $Threads(s'mn)=(Threads(s')\setminus\{t'\})\cup\{t'mn\}\subseteq\sigma$, so by single-threadedness of σ, $sn=s'mn\in\sigma$, contradicting the fact that s is an augmented play of σ.

– If s is infinite, let $t\in Threads(s)$. If t is finite, then there is some $s'\sqsubseteq_P s$ such that $t\in Threads(s')$, but $s'\in\sigma$, so by single-threadedness of σ $t\in\sigma$. If t is infinite, then for all $t'\sqsubseteq_P t$ there is some $s'\sqsubseteq_P s$ such that $t'\in Threads(s')$, but $s'\in\sigma$, so by single-threadedness of σ $t\in\sigma$. □

Fam($\mathcal{C}$) satisfies the mono requirement and therefore Fam($\mathcal{C}$) is a response category(see [13]):

Lemma 15 (mono requirement). *If $\mathcal{C}$ is the category defined in Sect. 2.2, then the canonical morphism $\partial_A : A\to R^{(R^A)}$ in* Fam($\mathcal{C}$) *is monic.*

Proof. Let $\varphi : B\to A$. If we write $A=\{A_i \mid i\in I\}$ and $B=\{B_j \mid j\in J\}$ in Fam($\mathcal{C}$), then φ consists of a function $f_\varphi : J\to I$ together with a family of strategies $\varphi_j : B_j\to A_{f_\varphi(j)}$.

∂_A consists of a family of strategies ∂_{Ai_0} on $A_{i_0} \to (\Pi_{i\in I}(A_i \to R)) \to R$ which plays are copycat plays on the subarena $A_{i_0} \to (A_{i_0} \to R) \to R$.
Therefore, the plays of the jth fiber of $\varphi;\partial_A$ are in the subarena $B_j \to (A_{f_\varphi(j)} \to R) \to R$ and their projections on $B_j \to A_{f_\varphi(j)}$ are exactly the plays of φ_j. In other words:

$$\varphi_j = \{s_{|B_j \to A_{f_\varphi(j)}} \mid s \in (\varphi;\partial_A)_j\}$$

therefore, if $\varphi;\partial_A = \psi;\partial_A$, then $\varphi = \psi$, so ∂_A is monic. □

Lemma 16. *Let $\perp\!\!\!\perp \subseteq E$. Suppose that we have a realizer for each formula of $\boldsymbol{Ax}$. If ν is a derivation of the sequent $\Gamma \vdash A$ and if θ is an assignment of closed first-order terms to variables, then $[\![\nu^*]\!]$ is a winning strategy on $\Gamma^* \to A^*$ equipped with $\mathcal{W}_{\theta(\Gamma \Rightarrow A)}$*

Proof. We prove the property by induction on the proof tree:

- $\dfrac{}{\Gamma \vdash A}\ {\scriptstyle A \in \Gamma}$: this is a consequence of Lemma 6
- $\dfrac{}{\Gamma \vdash A}\ {\scriptstyle A \in \boldsymbol{Ax}}$: this is an assumption of the lemma
- $\dfrac{}{\Gamma \vdash ((A \Rightarrow B) \Rightarrow A) \Rightarrow A}$: this is a consequence of Lemma 5
- $\dfrac{}{\Gamma \vdash \top}$: $Threads(*) = \emptyset$ so the result is immediate
- $\dfrac{\begin{matrix}\nu \\ \Gamma \vdash A\end{matrix} \qquad \begin{matrix}\nu' \\ \Gamma \vdash B\end{matrix}}{\Gamma \vdash A \wedge B}$: this follows from Lemma 4
- $\dfrac{\begin{matrix}\nu \\ \Gamma \vdash A \wedge B\end{matrix}}{\Gamma \vdash A}$: An augmented thread of $[\![\pi_1\nu^*]\!]$ is an augmented thread of $[\![\nu^*]\!]$ which is a thread on $\Gamma^* \to A^*$, so by Definition 10 it is winning on $\big(\Gamma^* \to A^* \times B^*, \mathcal{W}_{\theta(\Gamma \Rightarrow A \wedge B)}\big)$
- $\dfrac{\begin{matrix}\nu \\ \Gamma \vdash A \wedge B\end{matrix}}{\Gamma \vdash B}$: idem
- $\dfrac{\begin{matrix}\nu \\ \Gamma, A \vdash B\end{matrix}}{\Gamma \vdash A \Rightarrow B}$: the induction property is unchanged
- $\dfrac{\begin{matrix}\nu \\ \Gamma \vdash A \Rightarrow B\end{matrix} \qquad \begin{matrix}\nu' \\ \Gamma \vdash A\end{matrix}}{\Gamma \vdash B}$: this follows from Lemma 3
- $\dfrac{\begin{matrix}\nu \\ \Gamma \vdash A\end{matrix}}{\Gamma \vdash \forall x A}\ {\scriptstyle x \notin FV(\Gamma)}$: If t is an augmented thread of $[\![\nu^*]\!]$ such that:

  $$Threads(t_{|\Gamma^*}) \subseteq \mathcal{W}_{\theta(\Gamma)}$$

  Let a be a closed term and let $\theta' = \theta[x \mapsto a]$. Since $x \notin FV(\Gamma)$, $\theta'(\Gamma) = \theta(\Gamma)$ so:

  $$Threads(t_{|\Gamma^*}) \subseteq \mathcal{W}_{\theta'(\Gamma)}$$

  And then by induction hypothesis $t_{|A^*} \in \mathcal{W}_{\theta'(A)}$. Since $\theta'(A) = \theta(A[a/x])$, we get that for all closed term a, $t_{|A^*} \in \mathcal{W}_{\theta(A[a/x])}$, and so $t_{|A^*} \in \mathcal{W}_{\theta(\forall x A)}$

– $\dfrac{\dfrac{\nu}{\Gamma \vdash \forall x A}}{\Gamma \vdash A[a/x]}$: If t is an augmented thread of $[\![\nu^*]\!]$ such that:

$$Threads(t_{|\Gamma^*}) \subseteq \mathcal{W}_{\theta(\Gamma)}$$

Then by induction hypothesis, since $\theta(a)$ is a closed term we get $t_{|A^*} \in \mathcal{W}_{\theta(A[\theta(a)/x])}$, which terminates the proof since $\theta(A[\theta(a)/x]) = \theta(A[a/x])$.

□

Lemma 17. *Let $\perp\!\!\!\perp \subseteq E$.*

1. *The identity strategy on ι, is a realizer of* (**refl**)
2. *The identity strategy on $A^* \to \iota$, is a realizer of* (**Leib**)

Proof. 1. If t is an augmented thread of id_ι on the arena $\iota^{(1)} \to \iota^{(2)}$, then t is even or infinite (since id_ι is total) and verifies $t_{|\iota^{(1)}} = t_{|\iota^{(2)}}$. Let a be a closed first-order term. We must prove that $t \in \mathcal{W}_{a\neq a\to\perp}$. Suppose that

$$Threads(t_{|\iota^{(1)}}) \subseteq \mathcal{W}_{a\neq a}$$

First, t is a thread so $t_{|\iota^{(2)}}$ is a thread and $t_{|\iota^{(1)}} = t_{|\iota^{(2)}}$ is also a thread. Therefore we have $t_{|\iota^{(1)}} \in \mathcal{W}_{a\neq a}$. On the other hand, we have of course $a^E = a^E$, so $\mathcal{W}_{a\neq a} = \mathcal{W}_\perp$. Finally we obtain $t_{|\iota^{(2)}} \in \mathcal{W}_\perp$, so $t \in \mathcal{W}_{a\neq a\to\perp}$.

2. If t is an augmented thread of $id_{A^*\to\iota}$ on the arena

$$(A^{(1)} \to \iota^{(1)}) \to A^{(2)} \to \iota^{(2)}$$

then t is even or infinite (since $id_{A^*\to\iota}$ is total) and verifies $t_{|A^{(1)}\to\iota^{(1)}} = t_{|A^{(2)}\to\iota^{(2)}}$. Let a and b be closed first-order terms. We must prove that $t \in \mathcal{W}_{(A[a]\to\perp)\to A[b]\to a\neq b}$. We distinguish two cases:
   – $a^E \neq b^E$: any thread is in $\mathcal{W}_{a\neq b}$ so in particular $t \in \mathcal{W}_{a\neq b}$ and therefore $t \in \mathcal{W}_{(A[a]\to\perp)\to A[b]\to a\neq b}$
   – $a^E = b^E$: Suppose that

$$Threads(t_{|A^{(1)}\to\iota^{(1)}}) \subseteq \mathcal{W}_{|A[a]\to\perp} \text{ and } Threads(t_{|A^{(2)}}) \subseteq \mathcal{W}_{A[b]}$$

Since $a^E = b^E$, $\mathcal{W}_{|A[a]} = \mathcal{W}_{|A[b]}$, and since $t_{|A^{(1)}\to\iota^{(1)}} = t_{|A^{(2)}\to\iota^{(2)}}$,

$$Threads(t_{|A^{(1)}}) = Threads(t_{|A^{(2)}})$$

$$\text{so } Threads(t_{|A^{(1)}}) \subseteq \mathcal{W}_{A[a]}$$

$$\text{If } u \in Threads(t_{|A^{(1)}\to\iota^{(1)}}) \subseteq \mathcal{W}_{|A[a]\to\perp}$$

$$\text{then } Threads(u_{|A^{(1)}}) \subseteq Threads(t_{|A^{(1)}}) \subseteq \mathcal{W}_{A[a]}$$

and so $u_{|\iota^{(1)}} \in \mathcal{W}_\perp$. Therefore

$$Threads(t_{|\iota^{(1)}}) \subseteq \mathcal{W}_\perp$$

$$\text{but } Threads(t_{|\iota^{(1)}}) = Threads(t_{|\iota^{(2)}}) = \{t_{|\iota^{(2)}}\}$$

so $t_{|\iota^{(2)}} \in \mathcal{W}_\perp = \mathcal{W}_{a\neq b}$. Finally we obtain $t \in \mathcal{W}_{(A[a]\to\perp)\to A[b]\to a\neq b}$. □

Lemma 18. *Let* $\perp\!\!\!\perp \subseteq \mathbb{N}$.

1. *The empty strategy on* ι*, is a realizer of* $(\boldsymbol{Snz})$
2. *The identity strategy on* ι*, is a realizer of* $(\boldsymbol{Sinj})$*,* $(\boldsymbol{+0})$*,* $(\boldsymbol{+S})$*,* $(\boldsymbol{\times 0})$ *and* $(\boldsymbol{\times S})$
3. σ_0 *is a realizer of* $(\boldsymbol{nat0})$
4. σ_S *is a realizer of* $(\boldsymbol{natS})$
5. σ_+ *is a realizer of* $(\boldsymbol{nat+})$
6. $\sigma_\times$ *is a realizer of* $(\boldsymbol{nat\times})$
7. ρ^{A^*} *is a realizer of* $(\boldsymbol{ind})$

Proof. 1. Let a be a closed first-order term. Then $a^{\mathbb{N}}$ is some $n \in \mathbb{N}$, so we have $(S(a))^{\mathbb{N}} = n+1 \neq 0 = 0^{\mathbb{N}}$ and $\mathcal{W}_{S(a)\neq 0}$ is the set of all threads on ι.

2. – Let a and b be closed terms, then $a^{\mathbb{N}} = b^{\mathbb{N}} \Leftrightarrow (S(a))^{\mathbb{N}} = (S(b))^{\mathbb{N}}$ so $\mathcal{W}_{a\neq b} = \mathcal{W}_{S(a)\neq S(b)}$, and the identity strategy on ι realizes $(\boldsymbol{Sinj})$.
   – Let a be a closed term, then $(a+0)^{\mathbb{N}} = a^{\mathbb{N}}$, so $\mathcal{W}_{a+0\neq a} = \mathcal{W}_\perp$, and the identity strategy on ι realizes $(\boldsymbol{+0})$.
   – Let a and b be closed terms, then $(a+S(b))^{\mathbb{N}} = (S(a+b))^{\mathbb{N}}$, so
   $$\mathcal{W}_{a+S(b)\neq S(a+b)} = \mathcal{W}_\perp$$
   and the identity strategy on ι realizes $(\boldsymbol{+S})$.
   – The cases for $(\boldsymbol{\times 0})$ and $(\boldsymbol{\times S})$ are the same as for $(\boldsymbol{+0})$ and $(\boldsymbol{+S})$

3. If t is an augmented thread of σ_0, then $t = q^O 0^P$, so
$$t \in \mathcal{W}_{\mathsf{nat}(0)} = \{q^O n_1^P \dots n_k^P \mid \exists 1 \leq i \leq k, n_i = 0^{\mathbb{N}} = 0\}$$

4. If t is an augmented thread of σ_S on $\iota^{(1)} \to \iota^{(2)}$, let a be a closed first-order term and let $n = a^{\mathbb{N}}$. By definition of σ_S, $t_{|\iota^{(1)}}$ is a thread. If $t_{|\iota^{(1)}} \in \mathcal{W}_{\mathsf{nat}(a)}$, there is a move n^O in $t_{|\iota^{(1)}}$, so the next move in t is $(n+1)^P$ in $t_{|\iota^{(2)}}$, so
$$t_{|\iota^{(2)}} \in \mathcal{W}_{\mathsf{nat}(S(a))} = \{q^O n_1^P \dots n_k^P \mid \exists 1 \leq i \leq k, n_i = (S(a))^{\mathbb{N}} = n+1\}$$
and therefore $t \in \mathcal{W}_{\mathsf{nat}(a)\to\mathsf{nat}(S(a))}$.

5. If t is an augmented thread of σ_+ on $\iota^{(1)} \to \iota^{(2)} \to \iota^{(3)}$, let a and b be closed first-order terms and let $m = a^{\mathbb{N}}$ and $n = b^{\mathbb{N}}$. By definition of σ_+, $t_{|\iota^{(1)}}$ is a thread. If $t_{|\iota^{(1)}} \in \mathcal{W}_{\mathsf{nat}(a)}$, there is a move n^O in $t_{|\iota^{(1)}}$, so the next move in t is q^P in $t_{|\iota^{(2)}}$. Let u be the thread associated to this q^P. u is a thread on $\iota^{(2)}$ and $u \in \mathit{Threads}(t_{|\iota^{(2)}})$, so if $\mathit{Threads}(t_{|\iota^{(2)}}) \subseteq \mathcal{W}_{\mathsf{nat}(b)}$, there is a move n^O in $t_{|\iota^{(2)}}$, so the next move in t is $(m+n)^P$ in $t_{|\iota^{(3)}}$, so
$$t_{|\iota^{(3)}} \in \mathcal{W}_{\mathsf{nat}(a+b} = \{q^O n_1^P \dots n_k^P \mid \exists 1 \leq i \leq k, n_i = (a+b)^{\mathbb{N}} = m+n\}$$
and therefore $t \in \mathcal{W}_{\mathsf{nat}(a)\to\mathsf{nat}(b)\to\mathsf{nat}(a+b)}$.

6. This is the same proof as the preceding case

7. We first prove by induction on $n \in \mathbb{N}$ that $\rho_n^{A^*}$ is a realizer of the formula
$$A[0] \Rightarrow \forall^{\mathsf{n}} x(A[x] \Rightarrow A[S(x)]) \Rightarrow A[\overline{n}]$$
where $\overline{n}$ is the closed term $S(S(\dots S(0)))$, so we have $\overline{n}^{\mathbb{N}} = n$

– The case for 0 is the first part of Lemma 11
– By induction hypothesis we have:

$$\rho_n^{A^*} \Vdash A[0] \Rightarrow \forall^{\mathsf{n}} x(A[x] \Rightarrow A[S(x)]) \Rightarrow A[\overline{n}]$$

and by Lemma 11 we have:

$$\xi^T \Vdash \forall^{\mathsf{n}} y\Big(\Big(A[0] \Rightarrow \forall^{\mathsf{n}} x(A[x] \Rightarrow A[S(x)]) \Rightarrow A[y]\Big) \Rightarrow A[0] \Rightarrow \forall^{\mathsf{n}} x(A[x] \Rightarrow A[S(x)]) \Rightarrow A[S(y)]\Big)$$

so since $\sigma_n \Vdash \mathsf{nat}(\overline{n})$ and $\rho_{n+1}^T = \xi^T(\sigma_n)(\rho_n^T)$, we get by Lemma 3:

$$\rho_{n+1}^{A^*} \Vdash A[0] \Rightarrow \forall^{\mathsf{n}} x(A[x] \Rightarrow A[S(x)]) \Rightarrow A[S(\overline{n})]$$

which terminates the induction case since $\overline{n+1} = S(\overline{n})$.

Let now t be an augmented thread of ρ^{A^*} on the arena

$$A^{(1)} \to \Big(\iota^{(1)} \to A^{(2)} \to A^{(3)}\Big) \to \iota^{(2)} \to A^{(4)}$$

Let suppose that $t_{|A^{(1)}}$ is winning on $A[0]$ and $t_{|\iota^{(1)} \to A^{(2)} \to A^{(3)}}$ is winning on $\forall^{\mathsf{n}} x(A[x] \Rightarrow A[S(x)])$. We want to prove that $t_{|\iota^{(2)} \to A^{(4)}}$ is winning on $\forall x^{\mathsf{n}} A[x]$, so let a be a closed first-order term, let $n = a^{\mathbb{N}}$ and let suppose that $t_{|\iota^{(2)}}$ is winning on $\mathsf{nat}(a)$. Then there must be some n^O in $t_{|\iota^{(2)}}$. Let u be the subsequence of t consisting of the initial q^O, the following q^P, this n^O and all the moves of t such that the view obtained immediately after having been played contains n^O. Then u is a play of $\rho_n^{A^*}$. Since a P-move does not change the current view, the threads of $u_{|A^{(1)}}$ are O-subthreads of $t_{|A^{(1)}}$ (the projection induces an inversion of polarities), so they are winning on $A[0]$, and the threads of $u_{|\iota^{(1)} \to A^{(2)} \to A^{(3)}}$ are O-subthreads of $t_{|\iota^{(1)} \to A^{(2)} \to A^{(3)}}$, so they are winning on $\forall^{\mathsf{n}} x(A[x] \Rightarrow A[S(x)])$. Then by the property on $\rho_n^{A^*}$, $u_{|A^{(4)}}$ is winning on $A[a]$. But $u_{|A^{(4)}}$ is a P-subthread of $t_{|A^{(4)}}$ (no inversion here), so $t_{|A^{(4)}}$ is winning on $A[a]$. □