A Curry-Style Realizability Interpretation for Monotone Inductive Definitions ⋆ (Extended Version ⋆⋆)

Favio E. Miranda-Perea

Institut für Informatik der Ludwig-Maximilians-Universität München
Oettingenstr. 67, D-80538 München, Germany
miranda@informatik.uni-muenchen.de

Version 13.06.2002

Abstract. The logical system AF2μ, an extension of second-order predicate calculus with monotone inductive definitions, is presented. Some properties of this system are shown including that it is a good system for extracting programs from proofs by means of a realizability interpretation in the style of Krivine-Parigot, where the realizers are terms of the Curry-system of $\lambda^{\rightarrow}$-calculus and the realizability formulas belong to second-order logic.

1 Introduction

Realizability interpretations have been used extensively in proof theory and recently also as a tool in computer science to extract programs from proofs. However, the class of programs obtained with this so-called *proofs as programs* paradigm is still quite restricted. On the other hand the use of inductive definitions, polymorphic and inductively defined datatypes in modern programming languages is indispensable. This motivates us to investigate logical systems of inductive definitions and realizability interpretations, which allow to extract programs from proofs in these systems.

2 A Logical System for Monotone Inductive Definitions

2.1 A Language for Inductive Definitions

The system is second-order and is based on a term language which is a subset of the untyped lambda calculus with function symbols.

⋆ This Research is being supported by grant 154186 of the CONACyT-DAAD treaty.
⋆⋆ Extended version of a paper accepted for oral presentation at the 7th. ESSLLI Student Session, Trento, Italy, August 2002 and to be published in the Proceedings of the 7th. ESSLLI Student Session, edited by Malvina Nissim.

The formulas are defined by the following grammar:

$$A, B, C ::= X^{(n)}t_1 \dots t_n \mid P^{(n)}t_1 \dots t_n \mid A \to B \mid \forall x.A \mid \forall X.B,$$

where $X^{(n)}$ is a predicate variable of arity n and $P^{(n)}$ is either a predicate symbol or a *defined predicate* of arity n.A *defined predicate* is either a comprehension predicate or an inductive predicate. More precisely we have a simultaneous definition of defined predicates and formulas.

Definition 1. *Let F be a formula. The expression $\lambda \boldsymbol{y}.F$ is called a comprehension predicate.* Intuitively, the expression $\lambda \boldsymbol{y}.F$ represents the set $\{\boldsymbol{t} \mid F[\boldsymbol{y} := \boldsymbol{t}]\}$, so the expression $(\lambda \boldsymbol{y}.F)\boldsymbol{t}$ must be understood as $F[\boldsymbol{y} := \boldsymbol{t}]$. From now on, we denote a comprehension predicate defined by a formula F with the respective calligraphic letter $\mathcal{F}$.

Definition 2. *Let $\mathcal{F}$ be a comprehension predicate. The expression $\mu X.\mathcal{F}$ is called an inductive predicate.*

Intuitively $\mu X.\mathcal{F}$ represents the least fixed point of the operator defined by $\mathcal{F}$, and in a model $\mathcal{M}$ it will be interpreted as the least predicate $\mathcal{K}$ such that $\mathcal{M}[X/\mathcal{K}] \models \forall \boldsymbol{y}.X\boldsymbol{y} \leftrightarrow F$ holds. The existence of such predicate $\mathcal{K}$ will be guaranteed by the monotonicity of $\mathcal{F}$, ensured by the rule (μI). If $\mathcal{F}$ is not monotone $\mu X.\mathcal{F}$ would be interpreted by the empty set.

Let $0, s$ be function symbols and set $\mathcal{F} := \lambda y.\forall Y.Y0, (\forall z.Xz \to Ysz) \to Yy$,[1] the defining formula $F[X, y]$ may be seen as a function associating to every predicate X the least predicate containing 0 and all successors of an element of X. So $\mathbb{N} := \mu X.\mathcal{F}$ is the least predicate which contains 0 and is closed under the function s, which is the intended set of (recursive) natural numbers. Similarly we can define lists of natural numbers as

$$\mathsf{List}(\mathbb{N}) := \mu X.\lambda z.\forall Y.\, Y\mathsf{nil}, (\forall n \forall y.\, \mathbb{N}n, Xy \to Y\mathsf{cons}(n, y)) \to Yz.$$

As syntactical sugar we have Leibniz equality and inclusion between predicates:

$$x = y := \forall X.Xx \to Xy \qquad P \subseteq Q := \forall \boldsymbol{z}.P\boldsymbol{z} \to Q\boldsymbol{z}.$$

The symbol $\therefore$ found in some proofs must be read as "therefore".

2.2 System Rules

The logical rules are the usual natural deduction rules for $\to$, $\forall, \forall^2$, the rule for Leibniz Equality, and rules for inductive predicates, annotated

[1] $A_1, \dots, A_k \to B$ means $A_1 \to (A_2 \to \dots \to B)$

by proof-terms, it is important to remark that we make no syntactic distinction between object variables and proof-term variables. Let $\Gamma = \{x_1 : A_1, \ldots, x_n : A_n\}$. The relation $\Gamma \vdash t : A$ is defined inductively, from

$$\{x_1 : A_1, \ldots, x_n : A_n\} \vdash x_i : A_i \ (Var),$$

as follows:

$$\frac{\Gamma, x : A \vdash t : B}{\Gamma \vdash \lambda x.t : A \to B} \ (\to I) \quad \frac{\Gamma \vdash r : A \to B \quad \Gamma \vdash s : A}{\Gamma \vdash rs : B} \ (\to E)$$

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash t : \forall x.A} \ (\forall I) \quad \frac{\Gamma \vdash t : \forall x.A}{\Gamma \vdash t : A[x := s]} \ (\forall E)$$

$$\frac{\Gamma \vdash t : A}{\Gamma \vdash t : \forall X.A} \ (\forall^2 I) \quad \frac{\Gamma \vdash t : \forall X.A}{\Gamma \vdash t : A[X := \mathcal{F}]} \ (\forall^2 E)$$

$$\frac{\Gamma \vdash u = v \qquad \Gamma \vdash r : A[x := u]}{\Gamma \vdash r : A[x := v]} \ (Eq)^2$$

$$\frac{\Gamma \vdash t : \mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s} \qquad \Gamma \vdash m : \mathcal{F}\mathsf{mon}X}{\Gamma \vdash Cmt : (\mu X.\mathcal{F})\boldsymbol{s}} \ (\mu I)$$

where $\mathcal{F}\mathsf{mon}X \ := \ \forall X \forall Y.X \subseteq Y \to \mathcal{F} \subseteq \mathcal{F}[X := Y]$.

$$\frac{\Gamma \vdash r : (\mu X.\mathcal{F})\boldsymbol{s} \qquad \Gamma \vdash s : \mathcal{F}[X := \mathcal{K}] \subseteq \mathcal{K}}{\Gamma \vdash rE_\mu s : \mathcal{K}\boldsymbol{s}} \ (\mu E)$$

where the rules $(\forall I), (\forall^2 I)$ have the usual variable conditions.
The rule (Eq) for Leibniz Equality is trivial if we do not have some equalities a priori, because we can prove $t = r$ if and only if $t \equiv r$, so the relation $\vdash$ really depends in some set of equalities $\mathbb{E}$ that we only make explicit if necessary. The starting system of equalities is

$$\mathbb{E} := \{t = r \mid t \to_\beta r \text{ or } r \to_\beta t\},$$

So we have β-equality but only for one-step reduction.
The annotated terms for the rules involving a universal quantifier are equal for the premiss and for the conclusion, thus yielding a Curry-style system of proof-terms generated by the following grammar:

$$r, s, t, m ::= x \mid \lambda x.r \mid rs \mid Cmt \mid rE_\mu s.$$

[2] The proof-term for $u = v$ is irrelevant.

The reduction relation $\rightarrow_\beta$ between proofs is defined as the term-closure of the following β-reduction relation $\mapsto_\beta$ for proof-terms:

$$(\lambda x.t)r \mapsto_\beta t[x := r]$$
$$(Cmr)E_\mu s \mapsto_\beta s(m(\lambda x.xE_\mu s)r)$$

The second reduction rule corresponds to iteration on inductive types (see [Mat99]).

The underlying untyped calculus is a Curry-style version of the iterative fragment of the system EMIT of monotone inductive types, studied in [Mat98].

As we can see the introduction rule (μI) allows the introduction of an inductive definition $(\mu X.\mathcal{F})\boldsymbol{s}$ only when it has been proved that the comprehension predicate $\mathcal{F}$ is monotone in X. The proof of $\mathcal{F}\mathsf{mon}X$ is called a *monotonicity proof* and the proof-term m is called a *monotonicity witness*. The term m must not be closed, in that case we speak of conditional monotonicity. Moreover m can even be a variable, in which case we have hypothetical monotonicity.
These kind of definitions are therefore called monotone inductive definitions. Hence our system is an extension of the system AF2 (see [Kri93]) with monotone inductive definitions and we call it AF2μ. It is well-known that if X has only positive occurrences in $\mathcal{F}$,[3] then $\mathcal{F}\mathsf{mon}X$ holds. Hence our system includes all positive inductive definitions and is therefore more general that Parigot's TTR (see [Par92]).

For our definition of natural numbers we can derive the expected properties, zero is a natural number: $\vdash Cm(\lambda u\lambda f.u) : \mathbb{N}0$ and the successor of a natural number is again a natural number: $\vdash \lambda n.Cm(\lambda u\lambda f.fn) : \forall x.\mathbb{N}x \rightarrow \mathbb{N}sx$, where m is a canonical monotonicity witness.

2.3 Embedding AF2μ into AF2

In this section we provide an embedding of AF2μ into AF2 which allows, knowing that AF2 strong normalizes, to show the strong normalization of AF2μ.

[3] i.e. X does not occur in F to the left of an odd number of implications

Definition 3. *The embedding* $(\cdot)' : \mathsf{AF2}\mu \to \mathsf{AF2}$ *is defined as follows:*

$$\begin{array}{rlrl} x' & := x & (rs)' & := r's' \\ (\lambda x.r)' & := \lambda x.r' & (Cmr)' & := \lambda x.x(m'(\lambda z.zx)r') \\ (rE_\mu s)' & := r's' & & \\ (X\boldsymbol{t}\,)' & := X\boldsymbol{t} & (P\boldsymbol{t})' & := P\boldsymbol{t} \\ (A \to B)' & := A' \to B' & (\forall\gamma.A)' & := \forall\gamma.A' \\ \mathcal{F}' & := \lambda\boldsymbol{y}.F' & (\mu X.\mathcal{F})' & := \lambda\boldsymbol{z}.\forall X.\mathcal{F}' \subseteq X \to X\boldsymbol{z} \end{array}$$

where P *is a predicate symbol and* γ *is a first or second order variable.*

This lemma says that the embedding preserves substitutions.

Lemma 1 (Embedding Properties). *The embedding* $'$ *has the following properties:*

1. *For object or proof-terms:* $r[\boldsymbol{x} := \boldsymbol{s}]' = r'[\boldsymbol{x} := \boldsymbol{s}\,']$
2. *For object-terms:* $A[\boldsymbol{x} := \boldsymbol{r}]' = A'[\boldsymbol{x} := \boldsymbol{r}]$
3. $A[X := \mathcal{K}]' = A'[X := \mathcal{K}']$
4. $(\mathcal{F}[X := \mathcal{K}]\boldsymbol{s})' = \mathcal{F}'[X := \mathcal{K}']\boldsymbol{s}$
5. $(\mathcal{F} \subseteq X)' = \mathcal{F}' \subseteq X$
6. $(\mathcal{F}\mathsf{mon}X)' = \mathcal{F}'\mathsf{mon}X$

Proof. Part 1 is proved by induction on r; parts 2 and 3 are proved by induction on A; part 4 is a consequence of parts 2 and 3; parts 5 and 6 are straightforward. Qed

The following proposition shows that the embedding has a good reduction behaviour.

Proposition 1. *The embedding* $'$ *translates a reduction step* $r \to_\beta s$ *in at least one reduction step* $r' \to_\beta^+ s'$.

Proof. Induction on $\to_\beta$.
Case $(\lambda x.t)r \to_\beta t[x := r]$.

$$\begin{array}{rcl} ((\lambda x.t)r)' & = & (\lambda x.t')r' \\ & \to_\beta^+ & t'[x := r'] \\ & \underset{\mathsf{lemma}1,1}{=} & t[x := r]' \end{array}$$

Case $(Cmr)E_\mu s \to_\beta s(m(\lambda x.xE_\mu s)r)$ (w.l.o.g. $x \notin FV(m', r')$).

$$\begin{array}{rcl} (CmrE_\mu s)' & = & (\lambda x.x(m'(\lambda z.zx)r'))s' \\ & \to_\beta^+ & s'(m'(\lambda z.zs')r') \\ & =_\alpha & s'(m'(\lambda x.xs')r') \\ & = & (s(m(\lambda x.xE_\mu s)r))' \end{array}$$

The remaining cases are immediate from the induction hypothesis. ℚed

The next proposition shows that the embedding also preserves derivations.

Proposition 2. *If* $\Gamma \vdash_{\mathsf{AF2}\mu} t : A$ *then* $\Gamma' \vdash_{\mathsf{AF2}} t' : A'$.

Proof. Induction on $\vdash_{\mathsf{AF2}\mu}$. We only consider the cases $(\mu I), (\mu E)$. For the case (μI), we have $t \equiv Cmr$ and $A \equiv (\mu X.\mathcal{F})\boldsymbol{s}, \Gamma \vdash m : \mathcal{F}\mathsf{mon}X$ and $\Gamma \vdash r : \mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s}$. By Induction Hypothesis we have $\Gamma' \vdash r' : (\mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s})', \Gamma' \vdash m' : (\mathcal{F}\mathsf{mon}X)'$. Now using parts 4 and 6 of lemma 1 we obtain $\Gamma' \vdash r' : \mathcal{F}'[X := (\mu X.\mathcal{F})']\boldsymbol{s}$ $(*)$ and $\Gamma' \vdash m' : \mathcal{F}'monX$ $(**)$. On the other hand we have $x : \mathcal{F}' \subseteq X \vdash \lambda z.zx : (\lambda \boldsymbol{z}.\forall X.\mathcal{F}' \subseteq X \to X\boldsymbol{z}) \subseteq X$, and from this and $(**)$ applying $(\forall^2 E), (\forall^2 E), (\to E), (\forall E)$ we get $\Gamma', x : \mathcal{F}' \subseteq X \vdash m'(\lambda z.zx) : \mathcal{F}'[X := \lambda \boldsymbol{z}.\forall X.\mathcal{F}' \subseteq X \to X\boldsymbol{z}]\boldsymbol{s} \to \mathcal{F}'\boldsymbol{s}$, i.e., $\Gamma', x : \mathcal{F}' \subseteq X \vdash m'(\lambda z.zx) : \mathcal{F}'[X := (\mu X.\mathcal{F})']\boldsymbol{s} \to \mathcal{F}'\boldsymbol{s}$, now using $(*), (\to E)$ and the obvious $x : \mathcal{F}' \subseteq X \vdash x : \mathcal{F}'\boldsymbol{s} \to X\boldsymbol{s}$, we get, by $(\to E)$, $\Gamma', x : \mathcal{F}' \subseteq X \vdash x(m'(\lambda z.zx)r') : X\boldsymbol{s}$, finally by $(\to I), (\forall I)$ we get $\Gamma' \vdash \lambda x.x(m'(\lambda z.zx)r') : \forall X.\mathcal{F}' \subseteq X \to X\boldsymbol{s}$, that is $\Gamma' \vdash (Cmr)' : ((\mu X.\mathcal{F})\boldsymbol{s})'$.
For the case (μE) we have $t \equiv rE\mu s, A \equiv \mathcal{K}\boldsymbol{s}$ and $\Gamma \vdash r : (\mu X.\mathcal{F})\boldsymbol{s}, \Gamma \vdash s : \mathcal{F}[X := \mathcal{K}] \subseteq K$. By IH and parts 4 and 5 of lemma 1 we have $\Gamma' \vdash r' : \forall X.\mathcal{F}' \subseteq X \to X\boldsymbol{s}$ and $\Gamma' \vdash s' : \mathcal{F}'[X := \mathcal{K}'] \subseteq \mathcal{K}'$. Now, by $(\forall^2 E)$ and $(\to E)$ we get $\Gamma' \vdash r's' : \mathcal{K}'\boldsymbol{s}$, i.e. $\Gamma' \vdash (rE_\mu s)' : (\mathcal{K}\boldsymbol{s})'$. ℚed

Now, if we consider $\mathsf{AF2}\mu$ as a system of proof transformation rules, we obtain that

Proposition 3. $\mathsf{AF2}\mu$ *is strongly normalizing.*

Proof. From propositions 1,2, knowing that $\mathsf{AF2}$ is strongly normalizing (see [Kri93]). ℚed

2.4 Subject Reduction

In this section we prove subject reduction for $\mathsf{AF2}\mu$, Recall that this property is not trivial for Curry-systems because of the rules for $\forall, \forall^2$ and Eq, which are not reflected in the proof-term system. Instead of Barendregt's Method, we prefer to follow the more easily extensible Krivine's Method ([Kri93]).

Lemma 2 (Substitution Properties).

1. *If* $\Gamma \vdash t : A$ *then* $\Gamma[x := u] \vdash t : A[x := u]$.

2. *If* $\Gamma \vdash t : A$ *then* $\Gamma[X := \mathcal{F}] \vdash t : A[X := \mathcal{F}]$.
3. *If* $u = v$ *and* $\Gamma[x := u] \vdash t : A[x := u]$ *then* $\Gamma[x := v] \vdash t : A[x := v]$.
4. $A[\boldsymbol{\gamma} := \boldsymbol{\chi}][\boldsymbol{x} := \boldsymbol{s}] = A[\boldsymbol{x} := \boldsymbol{s}][\boldsymbol{\gamma} := \boldsymbol{\chi}[\boldsymbol{x} := \boldsymbol{s}]]$. *Where* $\boldsymbol{\gamma}$ *are 1st. (2nd.) order variables and* $\boldsymbol{\chi}$ *are terms (comprehension predicates).*
5. *If* $\Gamma, x_1 : A_1, \ldots, x_k : A_k \vdash r : B$ *and* $\Gamma \vdash t_i : A_i$ *then* $\Gamma \vdash r[\boldsymbol{x} := \boldsymbol{t}] : B$.

Proof. Parts 1,2,5 are proved by induction on $\vdash_{\mathsf{AF2}\mu}$; part 3 is proved using (Eq) and part 5; part 4 is proved by induction on A. Qed

Definition 4. *Given a formula* A *and a context* Γ*, we define the set* $\mathcal{C}_{\Gamma,A}$ *of* Γ*-instances of* A *as the least class of formulas which contains* A *and such that:*

- *If* $B \in \mathcal{C}_{\Gamma,A}$ *and* $x \notin FV(\Gamma)$ *then* $B[x := t] \in \mathcal{C}_{\Gamma,A}$.
- *If* $B \in \mathcal{C}_{\Gamma,A}$ *and* $X \notin FV(\Gamma)$ *then* $B[X := \mathcal{F}] \in \mathcal{C}_{\Gamma,A}$.
- *If* $B[x := u] \in \mathcal{C}_{\Gamma,A}$ *and* $u = v$ *then* $B[x := v] \in \mathcal{C}_{\Gamma,A}$.

Definition 5. *A formula* A *is an open formula if it does not start with* $\forall$*. In the formula* $G := \forall \boldsymbol{\gamma}.F$*, where* F *is an open formula,* F *is called the interior of* G *and is denoted* G°.

Lemma 3. *Let* $\widetilde{A}$ *be an open formula. If* $\Gamma \vdash t : \widetilde{A}$ *can be derived from* $\Gamma \vdash t : A$ *using only the rules* $(\forall I), (\forall E), (\forall^2 I), (\forall^2 E), (Eq)$ *then* $\widetilde{A} \in \mathcal{C}_{\Gamma,A^\circ}$.

Proof. Induction on the number of steps in the derivation of $\Gamma \vdash t : \widetilde{A}$ from $\Gamma \vdash t : A$. Case Analysis on the first rule used in that derivation.
$(\forall^2 E)$. We have $A \equiv \forall X.\forall \boldsymbol{\gamma}.A^\circ$ and after $(\forall^2 E)$,$\Gamma \vdash (\forall \boldsymbol{\gamma}.A^\circ)[X := \mathcal{F}]$. By IH we have $\widetilde{A} \in \mathcal{C}_{\Gamma,(\forall \boldsymbol{\gamma}.A^\circ[X:=\mathcal{F}])^\circ}$, i.e., $\widetilde{A} \in \mathcal{C}_{\Gamma,(A^\circ[X:=\mathcal{F}])^\circ}$. We have two subcases:
A° is atomic not beginning with X or an implication. This implies that $A^\circ[X := \mathcal{F}]$ is of the same form, i.e., $A^\circ[X := \mathcal{F}]$ is open. Therefore we have $\widetilde{A} \in \mathcal{C}_{\Gamma,A^\circ[X:=\mathcal{F}]}$, which implies $\widetilde{A} \in \mathcal{C}_{\Gamma,A^\circ}$.
$A^\circ \equiv X\boldsymbol{r}$. We have $A^\circ[X := \mathcal{F}] = \mathcal{F}\boldsymbol{r}$, therefore $\widetilde{A} \in \mathcal{C}_{\Gamma,(\mathcal{F}\boldsymbol{r})^\circ}$, that is $\widetilde{A} \in \mathcal{C}_{\Gamma,F^\circ[\boldsymbol{y}:=\boldsymbol{r}]}$. Finally we have $F^\circ[\boldsymbol{y} := \boldsymbol{r}] = (A^\circ[X := \mathcal{F}])^\circ = A^\circ[X := \mathcal{F}]$. Hence $\widetilde{A} \in \mathcal{C}_{\Gamma,A^\circ[X:=\mathcal{F}]}$ which leads to $\widetilde{A} \in \mathcal{C}_{\Gamma,A^\circ}$.
The remaining cases are easier. Qed

Lemma 4 (Generation Lemma). *Let* $\Gamma \vdash t : A$*, where* A *is an open formula. Then*

- *If* $t = x$ *then there exists* $(x : B) \in \Gamma$ *such that* $A \in \mathcal{C}_{\Gamma,B^\circ}$.

- *If* $t = \lambda x.r$ *then* $A \equiv B \to C$ *and* $\Gamma, x : B \vdash r : C$ *for some* B, C.
- *If* $t = rs$ *then there exist* B, C *such that* $\Gamma \vdash r : C \to B, \Gamma \vdash s : C$ *and* $A \in \mathcal{C}_{\Gamma,B^\circ}$.
- *If* $t = Cmr$ *then there is a formula* F *and terms* $\boldsymbol{s}$ *such that* $A \equiv (\mu X.\mathcal{F})\boldsymbol{s}$, $\Gamma \vdash m : \mathcal{F}\mathsf{mon}X$ *and* $\Gamma \vdash r : \mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s}$.
- *If* $t = rE_\mu s$ *then there are formulas* F, K *and terms* $\boldsymbol{s}$ *such that* $\Gamma \vdash r : (\mu X.\mathcal{F})\boldsymbol{s}$, $\Gamma \vdash s : \mathcal{F}[X := \mathcal{K}] \subseteq \mathcal{K}$ *and* $A \in \mathcal{C}_{\Gamma,(\mathcal{K}\boldsymbol{s})^\circ}$.

Proof. Consider in the derivation $\Gamma \vdash t : A$ the last step where a rule $\mathcal{R} \in \{(Var), (\to I), (\to E), (\mu I), (\mu E)\}$ occur. Suppose that the conclusion of $\mathcal{R}$ is $\Gamma \vdash t : B$. The previous lemma implies that $A \in \mathcal{C}_{\Gamma,B^\circ}$. Case Analysis on t.
The cases $t \equiv x, t \equiv rs, t \equiv rE_\mu s$ are immediate. We concentrate on $t \equiv Cmr$. We have $\mathcal{R} = (\mu I), B \equiv (\mu X.\mathcal{G})\boldsymbol{s}, \Gamma \vdash r : \mathcal{G}[X := \mu X.\mathcal{G}]\boldsymbol{s}$ and $\Gamma \vdash m : \mathcal{G}\mathsf{mon}X$. Clearly $B = B^\circ$, therefore $A \in \mathcal{C}_{\Gamma,B}$. Let $\mathcal{C} = \{(\mu X.\mathcal{F})\boldsymbol{s} \mid \Gamma \vdash r : \mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s}, \quad \Gamma \vdash m : \mathcal{F}\mathsf{mon}X\}$, we need to show that $A \in \mathcal{C}$. We claim that $\mathcal{C}_{\Gamma,B} \subseteq \mathcal{C}$. Obviously $B \in \mathcal{C}$. Suppose that $R \in \mathcal{C}$ and $x \notin FV(\Gamma)$. We have $R[x := u] \equiv ((\mu X.\mathcal{F})\boldsymbol{s})[x := u] = (\mu X.\mathcal{F}[x := u])\boldsymbol{s}[x := u]$. $R \in \mathcal{C}$ implies $\Gamma \vdash r : \mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s}, \quad \Gamma \vdash m : \mathcal{F}\mathsf{mon}X \underset{(x \notin FV(\Gamma))}{\Rightarrow} \Gamma \vdash r : (\mathcal{F}[X := \mu X.F]\boldsymbol{s})[x := u]$ and $\Gamma \vdash m : (\mathcal{F}\mathsf{mon}X)[x := u]$. Using lemma 2, parts 1,4, we obtain that $\Gamma \vdash r : \mathcal{F}[x := u][X := \mu X.\mathcal{F}[x := u]]\boldsymbol{s}[x := u]$ and $\Gamma \vdash m : \mathcal{F}[x := u]\mathsf{mon}X$. Therefore $R[x := u] \in \mathcal{C}$. Suppose $R \in \mathcal{C}$ and $Y \notin FV(\Gamma)$. We have $R[Y := \mathcal{K}] \equiv ((\mu X.\mathcal{F})\boldsymbol{s})[Y := \mathcal{K}] = (\mu X.\mathcal{F}[Y := \mathcal{K}])\boldsymbol{s}$. $R \in \mathcal{C}$ implies $\Gamma \vdash r : \mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s}, \quad \Gamma \vdash m : \mathcal{F}\mathsf{mon}X \underset{(Y \notin FV(\Gamma))}{\Rightarrow} \Gamma \vdash r : (\mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s})[Y := \mathcal{K}]$ and $\Gamma \vdash m : (\mathcal{F}\mathsf{mon}X)[Y := K]$. Using lemma 2 parts 2,4 we obtain $\Gamma \vdash: r : (\mathcal{F}[Y := \mathcal{K}][X := \mu X.\mathcal{F}[Y := \mathcal{K}]\boldsymbol{s}$ and $\Gamma \vdash \mathcal{F}[Y := \mathcal{K}]\mathsf{mon}X$. Therefore $R[Y := \mathcal{K}] \in \mathcal{C}$. Suppose $R[x := u] \in \mathcal{C}$ and $u = v$. We have $R[x := u] \equiv ((\mu X.\mathcal{F})\boldsymbol{s})[x := u]$ with $\Gamma \vdash r : (\mathcal{F}[X := \mu X.F]\boldsymbol{s})[x := u]$ and $\Gamma \vdash m : (\mathcal{F}\mathsf{mon}X)[x := u]$ Now using (Eq) we obtain $\Gamma \vdash r : (\mathcal{F}[X := \mu X.F]\boldsymbol{s})[x := v]$ and $\Gamma \vdash m : (\mathcal{F}\mathsf{mon}X)[x := v]$, i.e., $\Gamma \vdash r : \mathcal{F}[x := v][X := \mu X.\mathcal{F}[x := v]]\boldsymbol{s}[x := v]$ and $\Gamma \vdash m : \mathcal{F}[x := v]\mathsf{mon}X$. Therefore $R[x := v] \in \mathcal{C}$, which concludes the proof of $\mathcal{C}_{\Gamma,B} \subseteq \mathcal{C}$. This implies that $A \in \mathcal{C}$.
The case for $t \equiv \lambda x.r$ is proved analogously with $\mathcal{C} = \{P \to Q \mid \Gamma, x : P \vdash r : Q\}$. Qed

Lemma 5. *$\Gamma \vdash t : A$ if and only if $\Gamma \vdash t : A^\circ$.*

Proof. If A is open then $A^\circ = A$ and there is nothing to prove. Otherwise $A = \forall\gamma_1 \ldots \forall\gamma_n.A^\circ$. The direction $(\leftarrow)$ follows immediately from $\forall I, \forall^2 I$.

For $(\to)$, $\Gamma \vdash t : \forall\gamma_1 \ldots \forall\gamma_n.A^\circ$ and by using $\forall E, \forall^2 E$ we obtain $\Gamma \vdash t : A^\circ$. ℚed

Lemma 6. *If $\Gamma \vdash t : A$ and $\widetilde{A} \in \mathcal{C}_{\Gamma,A}$ then $\Gamma \vdash t : \widetilde{A}$.*

Proof. Let $\mathcal{C} = \{B | \Gamma \vdash t : B\}$. We claim that $\mathcal{C}_{\Gamma,A} \subseteq \mathcal{C}$. By Hypothesis $A \in \mathcal{C}$. Now if $B \in \mathcal{C}$ and $x \notin FV(\Gamma)$ then $\Gamma \vdash t : \forall x.B$, by $(\forall I)$, and applying $(\forall E)$ we obtain $\Gamma \vdash t : B[x := r]$. $\therefore B[x := r] \in \mathcal{C}$, analogously we conclude that $B[X := \mathcal{F}] \in \mathcal{C}$. Finally if $B[x := u]$ and $u = v$ using (Eq) we obtain $B[x := v] \in \mathcal{C}$. The lemma follows immediately. ℚed

Lemma 7 (Subject Reduction for Open Formulas). *Let A be an open formula. If $\Gamma \vdash t : A$ and $t \to_\beta \hat{t}$ then $\Gamma \vdash \hat{t} : A$.*

Proof. Induction on t. If $t \equiv x$, there is no redex, and the claim is trivial.
$t \equiv \lambda x.r$, which implies $\hat{t} \equiv \lambda x.\hat{r}$ with $r \to_\beta \hat{r}$. By lemma 4 we have $A \equiv C \to B$ and $\Gamma, x : C \vdash r : B \underset{\text{lemma 5}}{\Rightarrow} \Gamma, x : C \vdash r : B^\circ \underset{IH}{\Rightarrow} \Gamma, x : C \vdash \hat{r} : B^\circ \underset{\text{lemma 5}}{\Rightarrow} \Gamma, x : C \vdash \hat{r} : B \Rightarrow \Gamma \vdash \lambda x.\hat{r} : C \to B$.
$t \equiv rs$. We have two subcases: $\hat{t} \equiv \hat{r}\hat{s}$ with $r \to_\beta \hat{r}, s \to_\beta \hat{s}$. By lemma 4 we have $\Gamma \vdash r : C \to B, \Gamma \vdash s : C$ and $A \in \mathcal{C}_{\Gamma,B^\circ}$. Lemma 5 implies $\Gamma \vdash s : C^\circ$. By IH we have $\Gamma \vdash \hat{r} : C \to B, \Gamma \vdash \hat{s} : C^\circ$, applying again lemma 5 yields $\Gamma \vdash \hat{s} : C$. Therefore $\Gamma \vdash \hat{r}\hat{s} : B \Rightarrow \Gamma \vdash \hat{r}\hat{s} : B^\circ$. Finally by lemma 6 we have $\Gamma \vdash \hat{r}\hat{s} : A$.
$t \equiv (\lambda x.r)s$ and $\hat{t} \equiv r[x := s]$. The Generation lemma implies $\Gamma \vdash \lambda x.r : C \to B, \Gamma \vdash s : C$ and $A \in \mathcal{C}_{\Gamma,B^\circ}$. Generation implies also $\Gamma, x : C \vdash r : B$. Lemma 2,part 5 yields $\Gamma \vdash r[x := s] : B \Rightarrow \Gamma \vdash r[x := s] : B^\circ \underset{\text{lemma 6}}{\Rightarrow} \Gamma \vdash r[x := s] : A$.
$t \equiv Cmr$, which implies $\hat{t} \equiv C\hat{m}\hat{r}$ with $m \to_\beta \hat{m}, r \to_\beta \hat{r}$. By Generation lemma we have $A \equiv (\mu X.\mathcal{F})\boldsymbol{s}$, $\Gamma \vdash m : \mathcal{F}\mathsf{mon}X$ and $\Gamma \vdash r : \mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s}$. Lemma 5 implies $\Gamma \vdash m : (\mathcal{F}\mathsf{mon}X)^\circ$ and $\Gamma \vdash r : (\mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s})^\circ \underset{IH}{\Rightarrow} \Gamma \vdash \hat{m} : (\mathcal{F}\mathsf{mon}X)^\circ$ and $\Gamma \vdash \hat{r} : (\mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s})^\circ \underset{\text{lemma 5}}{\Rightarrow} \Gamma \vdash \hat{m} : \mathcal{F}\mathsf{mon}X$ and $\Gamma \vdash \hat{r} : \mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s}$. Finally (μI) implies $\Gamma \vdash C\hat{m}\hat{r} : (\mu X.\mathcal{F})\boldsymbol{s}$.
$t \equiv rE_\mu s$. We have two subcases: $t \equiv \hat{r}E_\mu\hat{s}$ with $r \to_\beta \hat{r}, s \to_\beta \hat{s}$. This case is analogous to the first subcase for application.
$t \equiv (Cmr)E_\mu s$ and $\hat{t} \equiv s(m(\lambda x.xE_\mu s)r)$. The generation lemma yields $\Gamma \vdash m : \mathcal{F}\mathsf{mon}X, \Gamma \vdash r : \mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s}, \Gamma \vdash s : \mathcal{F}[X := \mathcal{K}] \subseteq \mathcal{K}$ and $A \in \mathcal{C}_{\Gamma,(\mathcal{K}\boldsymbol{s})^\circ}$. It is easy to see that $\Gamma \vdash \lambda x.xE_\mu s : \mu X.\mathcal{F} \subseteq \mathcal{K}$. Now by $(\forall^2 E), (\to E)$ we have $\Gamma \vdash m(\lambda x.xE_\mu s) : \mathcal{F}[X := \mu X.\mathcal{F}] \subseteq \mathcal{F}[X := \mathcal{K}] \Rightarrow \Gamma \vdash m(\lambda x.xE_\mu s)r : \mathcal{F}[X := \mathcal{K}]\boldsymbol{s} \Rightarrow \Gamma \vdash s(m(\lambda x.xE_\mu s)r) : \mathcal{K}\boldsymbol{s} \Rightarrow \Gamma \vdash s(m(\lambda x.xE_\mu s)r) : (\mathcal{K}\boldsymbol{s})^\circ$. Finally, by lemma 6 we conclude $\Gamma \vdash s(m(\lambda x.xE_\mu s)r) : A$. ℚed

Proposition 4 (Subject Reduction). $\mathsf{AF2}\mu$ *has subject reduction.*

Proof. Immediately from lemmas 5,7. Qed

3 Realizability

Realizability interpretations are given by saying what it means for computational objects of some kind to *realize* logical formulas. In our case the computational objects (programs) are modelled by simply lambda terms in Curry-style. The concept "the program t realizes the specification A" is formalized by means of a new formula $t\ \mathtt{r}\ A$, which generally belongs to an extended language.

Let $\mathcal{L}^+$ be the extension of $\mathcal{L}_{\mathsf{AF2}}$ given by extending the object-term system with pure λ-terms and adding a new predicate variable (symbol) X^+ (P^+) for every predicate variable (symbol) X (P) where the arity of X^+ (P^+) equals the arity of X (P) plus 1.

Definition 6. *Given a $\lambda^{\to}$-term t and a $\mathcal{L}_{\mathsf{AF2}}$-formula A, we define the $\mathcal{L}^+$-formula $t\ \mathtt{r}\ A$ as follows:*

$$t\ \mathtt{r}\ X\boldsymbol{s} := X^+\boldsymbol{s}t \qquad t\ \mathtt{r}\ P\boldsymbol{s} := P^+\boldsymbol{s}t$$
$$t\ \mathtt{r}\ A \to B := \forall z.z\ \mathtt{r}\ A \to tz\ \mathtt{r}\ B$$
$$t\ \mathtt{r}\ \forall x.A := \forall x.t\ \mathtt{r}\ A \qquad t\ \mathtt{r}\ \forall X.A := \forall X^+.t\ \mathtt{r}\ A$$
$$t\ \mathtt{r}\ (\mu X.\mathcal{F})\boldsymbol{s} := t\ \mathtt{r}\ \forall X.\mathcal{F} \subseteq X \to X\boldsymbol{s}$$

The following notation will be useful: $\mathcal{F}^{\mathtt{r}} := \lambda \boldsymbol{y}, z.z\ \mathtt{r}\ F$ where $z \notin FV(F)$. Given a context $\Gamma = \{x_1 : A_1, \dots x_k : A_k\}$ and arbitrary but fixed realizers t_i of A_i we set $\Gamma^{\mathtt{r}} := \{x_1 : t_1\ \mathtt{r}\ A_1, \dots x_k : t_k\ \mathtt{r}\ A_k\}$.

Proposition 5 (Substitution Properties).

1. $(t\ \mathtt{r}\ A)[\boldsymbol{x} := \boldsymbol{r}] = t[\boldsymbol{x} := \boldsymbol{r}]\ \mathtt{r}\ A[\boldsymbol{x} := \boldsymbol{r}]$.
2. $t\ \mathtt{r}\ A[X := \mathcal{F}] = (t\ \mathtt{r}\ A)[X^+ := \mathcal{F}^{\mathtt{r}}]$.

Proof. Induction on A in both cases. Qed

Theorem 1 (Soundness of Realizability). *Let $'$ be the embedding of definition 3 and t_i an arbitrary realizer of A_i. If $\Gamma \vdash_{\mathsf{AF2}\mu} t : A$, then $\Gamma^{\mathtt{r}} \vdash_{\mathsf{AF2}} t' : t'[\boldsymbol{x} := \boldsymbol{t}]\ \mathtt{r}\ A$*

Proof. Induction on $\vdash_{\mathsf{AF2}\mu}$. We concentrate on the cases for μ:
Case (μE). We have $A \equiv \mathcal{K}\boldsymbol{s}$, $t \equiv rE_\mu s$, $\Gamma \vdash r : (\mu X.\mathcal{F})\boldsymbol{s}$ and $\Gamma \vdash s : \mathcal{F}[X := \mathcal{K}] \subseteq \mathcal{K}$. By IH we have $\Gamma^{\mathtt{r}} \vdash r' : r'[\boldsymbol{x} := \boldsymbol{t}]\ \mathtt{r}\ (\mu X.\mathcal{F})\boldsymbol{s}$, that is

$$\Gamma^{\mathtt{r}} \vdash r' : \forall X^+.\forall z.z\ \mathtt{r}\ \mathcal{F} \subseteq X \to r'[\boldsymbol{x} := \boldsymbol{t}]z\ \mathtt{r}\ X\boldsymbol{s},$$

from this, instantiating X^+ with $\mathcal{K}^{\mathtt{r}}$ and using proposition 5, part 2 we get

$$\Gamma^{\mathtt{r}} \vdash r' : \forall z.z\ \mathtt{r}\ (\mathcal{F} \subseteq X)[X := \mathcal{K}] \to r'[\boldsymbol{x} := \boldsymbol{t}]z\ \mathtt{r}\ (X\boldsymbol{s})[X := \mathcal{K}].$$

Next we instantiate z with $s'[\boldsymbol{x} := \boldsymbol{t}]$ to get

$$\Gamma^{\mathtt{r}} \vdash r' : s'[\boldsymbol{x} := \boldsymbol{t}]\ \mathtt{r}\ \mathcal{F}[X := \mathcal{K}] \subseteq \mathcal{K} \to r'[\boldsymbol{x} := \boldsymbol{t}]s'[\boldsymbol{x} := \boldsymbol{t}]\ \mathtt{r}\ \mathcal{K}\boldsymbol{s},$$

but by IH we have $\Gamma^{\mathtt{r}} \vdash s' : s'[\boldsymbol{x} := \boldsymbol{t}]\ \mathtt{r}\ \mathcal{F}[X := \mathcal{K}] \subseteq \mathcal{K}$. Therefore by $(\to E)$ we finally obtain

$$\Gamma^{\mathtt{r}} \vdash r's' : r'[\boldsymbol{x} := \boldsymbol{t}]s'[\boldsymbol{x} := \boldsymbol{t}]\ \mathtt{r}\ \mathcal{K}\boldsymbol{s},$$

which is the same as

$$\Gamma^{\mathtt{r}} \vdash (rE_\mu s)' : (rE_\mu s)'[\boldsymbol{x} := \boldsymbol{t}]\ \mathtt{r}\ \mathcal{K}\boldsymbol{s}.$$

Case (μI). We have $A \equiv (\mu X.\mathcal{F})\boldsymbol{s}, t \equiv Cmr$ and $\Gamma \vdash m : \mathcal{F}\mathsf{mon}X,\ \Gamma \vdash r : \mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s}$.
We want to show that $\Gamma^r \vdash (Cmr)' : (Cmr)'[\boldsymbol{x} := \boldsymbol{t}]\ \mathtt{r}\ (\mu X.\mathcal{F})\boldsymbol{s}$.

It suffices to show

$$\Gamma^r \vdash \lambda y.y(m'(\lambda u.uy)r') : z\ \mathtt{r}\ \mathcal{F} \subseteq X \to (Cmr)'[\boldsymbol{x} := \boldsymbol{t}]z\ \mathtt{r}\ X\boldsymbol{s}$$

and to show this is enough to show:

$$\Gamma^r, y : z\ \mathtt{r}\ \mathcal{F} \subseteq X \vdash y(m'(\lambda u.uy)r') : (Cmr)'[\boldsymbol{x} := \boldsymbol{t}]z\ \mathtt{r}\ X\boldsymbol{s} \qquad (1)$$

and then apply $(\to I)$.

Let $\widehat{m} := m'[\boldsymbol{x} := \boldsymbol{t}], \widehat{r} := r'[\boldsymbol{x} := \boldsymbol{t}], \Delta := \Gamma^{\mathtt{r}}, y : z\ \mathtt{r}\ \mathcal{F} \subseteq X$, we show first the following two derivations:

$$\Delta \vdash \lambda u.uy : \lambda w.wz\ \mathtt{r}\ \mu X.\mathcal{F} \subseteq X \qquad (2)$$

$$\Delta \vdash m'(\lambda u.uy)r' : \widehat{m}(\lambda w.wz)\widehat{r}\ \mathtt{r}\ \mathcal{F}\boldsymbol{s} \qquad (3)$$

Proof (of derivation 2). By rule (Var) and definition of realizability we have:

$$\Delta, u : w\ \mathtt{r}\ (\mu X.\mathcal{F})\boldsymbol{y} \vdash u : \forall X^+ \forall z.z\ \mathtt{r}\ \mathcal{F} \subseteq X \to wz\ \mathtt{r}\ X\boldsymbol{y}$$

By $\forall^2 E, \forall E, \to E$ we obtain

$$\Delta, u : w\ \mathtt{r}\ (\mu X.\mathcal{F})\boldsymbol{y} \vdash uy : wz\ \mathtt{r}\ X\boldsymbol{y}$$

and by $\to I$,

$$\Delta \vdash \lambda u.uy : w \ \mathtt{r} \ (\mu X.\mathcal{F})\boldsymbol{y} \to wz \ \mathtt{r} \ X\boldsymbol{y}$$

Using Eq with $(\lambda w.wz)w = wz \in \mathbb{E}$ we get

$$\Delta \vdash \lambda u.uy : w \ \mathtt{r} \ (\mu X.\mathcal{F})\boldsymbol{y} \to (\lambda w.wz)w \ \mathtt{r} \ X\boldsymbol{y}$$

Finally by $\forall I, \forall I$ and definition of realizability

$$\Delta \vdash \lambda u.uy : \lambda w.wz \ \mathtt{r} \ \forall \boldsymbol{y}.(\mu X.\mathcal{F})\boldsymbol{y} \to X\boldsymbol{y}$$

and derivation (2) is proved. ℚed

Proof (of derivation 3). By IH we have $\Gamma^r \vdash m' : \widehat{m} \ \mathtt{r} \ \mathcal{F}\mathsf{mon}X$, which implies

$$\Delta \vdash m' : \forall X^+ \forall Y^+ \forall w.w \ \mathtt{r} \ X \subseteq Y \to \widehat{m}w \ \mathtt{r} \ \mathcal{F} \subseteq \mathcal{F}[X := Y]$$

Instantiating $X^+, Y^+ := (\mu X.\mathcal{F})^{\mathtt{r}}, X^+$ and using proposition 5 we get

$$\Delta \vdash m' : \forall w.w \ \mathtt{r} \ \mu X.\mathcal{F} \subseteq X \to \widehat{m}w \ \mathtt{r} \ \mathcal{F}[X := \mu X.\mathcal{F}] \subseteq \mathcal{F}$$

Instantiating $w := \lambda w.wz$ and using $(\to E)$ with derivation (2) we obtain

$$\Delta \vdash m'(\lambda u.uy) : \widehat{m}(\lambda w.wz) \ \mathtt{r} \ \mathcal{F}[X := \mu X.\mathcal{F}] \subseteq \mathcal{F}$$

Unfolding the definition of realizability we get

$$\Delta \vdash m'(\lambda u.uy) : \forall \boldsymbol{y} \forall x.x \ \mathtt{r} \ \mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{y} \to \widehat{m}(\lambda w.wz)x \ \mathtt{r} \ \mathcal{F}\boldsymbol{y}$$

By IH we have $\Gamma^{\mathtt{r}} \vdash r' : \widehat{r} \ \mathtt{r} \ \mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s}$ from this, by instantiating in the previous derivation $\boldsymbol{y}, x := \boldsymbol{s}, \widehat{r}$, and applying $(\to E)$ we conclude

$$\Delta \vdash m'(\lambda u.uy)r' : \widehat{m}(\lambda w.wz)\widehat{r} \ \mathtt{r} \ \mathcal{F}\boldsymbol{s}$$

and derivation (3) is proved ℚed

Now we proceed to derive (1):

From rule (Var) and definition of realizability we obtain

$$\Delta \vdash y : \forall \boldsymbol{y} \forall x.x \ \mathtt{r} \ \mathcal{F}\boldsymbol{y} \to zx \ \mathtt{r} \ X\boldsymbol{y}$$

Instantiating $\boldsymbol{y}, x := \boldsymbol{s}, \widehat{m}(\lambda w.wz)\widehat{r}$ and applying $(\to E)$ by derivation (3) we get

$$\Delta \vdash y(m'(\lambda u.uy)r') : z(\widehat{m}(\lambda w.wz)\widehat{r}) \ \mathtt{r} \ X\boldsymbol{s}$$

Now using that $z(\widehat{m}(\lambda w.wz)\widehat{r}) = (\lambda z.z(\widehat{m}(\lambda w.wz)\widehat{r}))z \in \mathbb{E}$ by rule (Eq) we have

$$\Delta \vdash y(m'(\lambda u.uy)r') : (\lambda z.z(\widehat{m}(\lambda w.wz)\widehat{r}))z \; \mathtt{r} \; X\boldsymbol{s}$$

Finally from $(\lambda z.z(\widehat{m}(\lambda w.wz)\widehat{r}))z \equiv (\lambda z.z(m'(\lambda w.wz)r'))[\boldsymbol{x} := \boldsymbol{t}]z \equiv (Cmr)'[\boldsymbol{x} := \boldsymbol{t}]z$, we conclude (1).

Qed

The soundness theorem guarantees the correctness of program extraction. If we have a proof t of a specification A from some assumptions A_i then if we assume that every hypothesis A_i is realized by some program t_i, we obtain a proof t' of the fact that the program $t'[\boldsymbol{x} := \boldsymbol{t}\,]$ realizes the specification A. Moreover the proof of $t'[\boldsymbol{x} := \boldsymbol{t}\,]\ \mathtt{r}\ A$ is in some sense the same proof of A because is just the image of the original proof under the embedding $'$.

4 Semantics

In this section we define a classical semantics for $\mathsf{AF2}\mu$ and present the important concept of datatype in a model, which allows to establish a relation between modified realizability and our realizability concept.

Definition 7. *A standard model of $\mathcal{L}^+$ is a full model for second order logic such that $|\mathcal{M}| = \Lambda/\!\sim_\beta$, i.e, the universe is the set of λ-terms modulo β-equivalence.*

Definition 8. *The interpretation of a term t under a valuation ν in $\mathcal{M}$, denoted $t^{\mathcal{M}}[\nu]$ is defined as usual. The notion of satisfaction $\mathcal{M} \models A[\nu]$ is the usual one for formulas of second order logic and for inductive predicates is defined as:*

$$\mathcal{M} \models (\mu X.\mathcal{F})\boldsymbol{s}[\nu] := \mathcal{I}_F(\boldsymbol{s}^{\mathcal{M}}[\nu]),$$

where $\mathcal{I}_F := \bigcap\{\mathcal{R} \subseteq |\mathcal{M}|^n \mid Sat_{\mathcal{M}[X/\mathcal{R}],\nu}(\mathcal{F}) \subseteq \mathcal{R}\}$ and $Sat_{\mathcal{M},\nu}(\lambda \boldsymbol{z}.A) := \{\boldsymbol{t} \mid \mathcal{M}[\boldsymbol{z}/\boldsymbol{t}] \models A[\nu]\}$.

Fortunately we have a useful equivalence to avoid this difficult definition.

Proposition 6. $\mathcal{M} \models (\mu X.\mathcal{F})\boldsymbol{s}[\nu] \Leftrightarrow \mathcal{M} \models (\forall X.\mathcal{F} \subseteq X \to X\boldsymbol{s})[\nu]$

Proof. Straightforward. Qed

Corollary 1 (Semantical Soundness).
Let $\Gamma = \{x_1 : A_1, \ldots, x_k : A_k\}$, $\Gamma \vdash_{\mathsf{AF2}\mu} t : A$ *and* t_i *a realizer of* A_i. *If* $\mathcal{M} \models t_i \mathtt{r}\ A_i$ *then* $\mathcal{M} \models t'[\boldsymbol{x} := \boldsymbol{t}]\ \mathtt{r}\ A$.

Proof. By theorem 1 and soundness of second-order predicate logic or alternatively by induction on $\vdash_{\mathsf{AF2}\mu}$ Qed

Definition 9. *Let* $\mathcal{M}$ *be a standard model and* $D[x]$ *a formula with* $FV(D) = \{x\}$. *We say that* D *is a data type in* $\mathcal{M}$ *if*

$$\mathcal{M} \models \forall x \forall y. y\ \mathtt{r}\ D[x] \leftrightarrow y = x \wedge D[x]$$

With this concept we can represent typed terms in our untyped setting. The direction ($\leftarrow$) of this definition can be simplified to $D[x] \rightarrow x\ \mathtt{r}\ D[x]$ which means that every inhabitant of the type D realizes its own inhabitation. The direction ($\rightarrow$) says that every realizer y of the inhabitation of D by x is already that inhabitant x.

As a consequence of realizability soundness and semantical soundness we have the following

Corollary 2 (Correctness Lemma). *Let* $\mathcal{M}$ *be a standard model,* f *a function symbol,* $D_i[x_i], E[y]$ *datatypes in* $\mathcal{M}$ *and* s_i *an inhabitant of* D_i *(i.e.* $\mathcal{M} \models D_i[s_i]$*).*
If $\vdash_{\mathsf{AF2}\mu} t : \forall x_1 \ldots \forall x_n . D_1[x_1], \ldots, D_n[x_n] \rightarrow E[f x_1 \ldots x_n]$ *then* $t'^{\mathcal{M}} s_1 \ldots s_n = f^{\mathcal{M}} s_1 \ldots s_n$. *Therefore the* λ*-term* $t'^{\mathcal{M}}$ *is a program to compute the function* $f^{\mathcal{M}}$.

This corollary provides a method of programming: to obtain a program for a function f we just have to derive $D_1[x_1], \ldots, D_n[x_n] \vdash_{\mathsf{AF2}\mu} E[f x_1 \ldots x_n]$.

5 Modified Realizability

We have shown that our realizability interpretation is good to extract program from proofs. However, the methods of program extraction via realizability are often developed with Kreisel's modified realizability (see [Ber93,BBS02]). Therefore I want to finish this paper by showing a relation between both concepts of realizability.
Modified realizability ($\mathtt{mr}$) is usually defined in a typed setting, the definition of $t\ \mathtt{mr}\ A$ for first order formulas is the same as for $t\ \mathtt{r}\ A$ except for the case of a universal quantifier. For this case we have

$$t^{\rho \rightarrow \tau(A)}\ \mathtt{mr}\ \forall x^{\rho}.A := \forall x^{\rho}.(tx)^{\tau(A)}\ \mathtt{mr}\ A$$

where $\tau(A)$ is a type assigned to A. The essential point is that the realizer is a function with domain ρ.
The quantification over typed variables can be represented in our untyped setting with a universal quantifier relativized to a datatype D: $\forall_D x.A := \forall x.D[x] \to A$. For the universal formula $\forall_D x.A$ we define $t\ \mathtt{mr}\ \forall_D x.A := \forall_D x.tx\ \mathtt{r}\ A$, note that here the realizer t also behaves as a function with domain D. The relation between both concepts of realizability for relativized quantifiers is expressed in the following

Proposition 7. *Let D be a datatype in $\mathcal{M}$. Then*

$$\mathcal{M} \models t\ \mathtt{mr}\ \forall_D x.A \ \leftrightarrow\ t\ \mathtt{r}\ \forall_D x.A$$

Proof. $\to$). Assume that $\mathcal{M} \models \forall x.D[x] \to tx\ \mathtt{r}\ A$. It suffices to show $\mathcal{M}[x, y/r, s] \models y\ \mathtt{r}\ D[x] \to ty\ \mathtt{r}\ A$ for every $r, s \in |\mathcal{M}|$. Suppose $\mathcal{M}[x, y/r, s] \models y\ \mathtt{r}\ D[x]$, D being a datatype implies that $\mathcal{M}[x, y/r, s] \models y = x \wedge D[x]$. Hence $\mathcal{M}[x, y/r, s] \models D[x]$, which by the main assumption yields $\mathcal{M}[x, y/r, s] \models tx\ \mathtt{r}\ A$ and as $\mathcal{M}[x, y/r, s] \models y = x$ we conclude $\mathcal{M}[x, y/r, s] \models ty\ \mathtt{r}\ A$, $\therefore \mathcal{M} \models t\ \mathtt{r}\ \forall_D x.A$.

$\leftarrow$). Suppose $\mathcal{M} \models t\ \mathtt{r}\ \forall x.D[x] \to A$. It suffices to show that $\mathcal{M}[x/s] \models D[x] \to tx\ \mathtt{r}\ A$ for $s \in |\mathcal{M}|$. Suppose $\mathcal{M}[x/s] \models D[x]$, this implies that $\mathcal{M}[x/s] \models x\ \mathtt{r}\ D[x]$, because D is a datatype also in $\mathcal{M}[x/s]$. Our main assumption implies that $\mathcal{M}[x/s] \models x\ \mathtt{r}\ D[x] \to tx\ \mathtt{r}\ A$. Thus $\mathcal{M}[x/s] \models tx\ \mathtt{r}\ A$, $\therefore \mathcal{M} \models t\ \mathtt{mr}\ \forall_D x.A$. ℚed

6 Final Remarks and Future Work

Systems like AF2μ have been developed in [Par92,Raf94], indeed the concept of datatype is taken from [KrPa90,Par92]. The essential difference is that our system works on monotone and not just positive inductive definitions and is, in contrast with those of [Par92,Raf94], strongly normalizing. The definition of realizability for inductive definitions, contrary to that of [Par92], has been inspired by the embedding of least fixed points in second order logic, as seen, for instance, in [Raf94,UuVe02].

The ultimate goal is to work out realizability interpretations for several logical systems of monotone inductive definitions, using as realizers not only $\lambda^{\to}$-terms but term systems of monotone inductive types, in particular Curry-versions (when possible) of the systems developed in [Mat98], this also implies to define realizability of inductive definitions again as an inductive definition, like the definitions of modified realizability in [Ber95,Ben98] or q-realizability in [Tat93]. See the appendix B for

first steps in this direction.A parallel goal is to extend the Curry-Howard Isomorphism to logical systems of inductive definitions, using the type systems of [Mat98], a reason why we use full second-order logic and not only first-order logic plus inductive predicates.
Unfortunately, for the time being, we do not have a specific example of program extraction, we need either to consider realizability interpretations like that of [Par92], which allows to prove that formulas like $\mathbb{N}[x]$ are datatypes or to formulate an adequate concept of datatype for our purposes. A concept of datatype which seems to be related with our research is a type that is both parametric and extensive in the sense of [Wad01].
To simplify the syntactic machinery and to provide a connection with category theory, which would be useful to consider later coinductive definitions I want to define logical systems of inductive definitions using the categorical point of view, where inductive predicates represent (weak) initial algebras of functors, and the existence of the algebra is used as an inductive definition principle (see [Geu92,JaRu97]). In this way the complicated inductive definitions in $\mathsf{AF2}\mu$, like that of $\mathbb{N}$ would be simplified to $\mathbb{N} := \mu X.1 + X$, which represents the initial algebra of the functor $T(X) = 1 + X$, where $+$ means coproduct. This is clearly related to algebraic types as presented in [Wad01].

A Defining Inductive Predicates with Sums and Products

We add to the language $\mathcal{L}$, the function symbols inl,inr, pair,$\mathsf{in1}$ and define the unit predicate $\mathbb{1} := \lambda z.\forall Y.Y\mathsf{in1} \to Yz$ and the empty predicate $\mathbb{0} := \lambda z.\forall Z.Zz$.

Definition 10. *Let $\mathcal{F}, \mathcal{G}$ be comprehension predicates. We define two new comprehension predicates, the sum and product of $\mathcal{F}$ and $\mathcal{G}$, as follows*

$$\mathcal{F} + \mathcal{G} := \lambda z.\forall Y.\ (\forall x.\mathcal{F}x \to Y\mathsf{inl}x),\ (\forall y.\mathcal{G}y \to Y\mathsf{inr}y) \to Yz$$
$$\mathcal{F} \times \mathcal{G} := \lambda z.\forall Y.\ (\forall x \forall y.\mathcal{F}x, \mathcal{G}y \to Y\mathsf{pair}xy) \to Yz$$

Proposition 8. *We have the following derivations:*

1. $\vdash \mathsf{id} : \mathbb{1}\mathsf{in1}$
2. $z : \mathcal{F}x \vdash \underline{\mathsf{inl}}z : (\mathcal{F} + \mathcal{G})\mathsf{inl}x.$
3. $z : \mathcal{G}y \vdash \underline{\mathsf{inr}}z : (\mathcal{F} + \mathcal{G})\mathsf{inr}y.$
4. $u : \mathcal{F}x, v : \mathcal{G}y \vdash \underline{\mathsf{pair}}uv : (\mathcal{F} \times \mathcal{G})\mathsf{pair}xy$

where $\mathsf{id} := \lambda x.x$, $\underline{\mathsf{inl}} := \lambda x.\lambda y.\lambda z.yx$, $\underline{\mathsf{inr}} := \lambda x.\lambda y.\lambda z.zx$, $\underline{\mathsf{pair}} := \lambda x.\lambda y\lambda z.zxy$

Proof. Straightforward ℚed

From this proposition we obtain the following derived rules:

$$\frac{\Gamma \vdash t : \mathcal{F}s}{\Gamma \vdash \underline{\mathsf{inl}}t : (\mathcal{F}+\mathcal{G})\mathsf{inl}s}\ (+Il) \qquad \frac{\Gamma \vdash t : \mathcal{G}s}{\Gamma \vdash \underline{\mathsf{inr}}t : (\mathcal{F}+\mathcal{G})\mathsf{inr}s}\ (+Ir)$$

$$\frac{\Gamma \vdash t : \mathcal{F}s_1 \qquad \Gamma \vdash r : \mathcal{G}s_2}{\Gamma \vdash \underline{\mathsf{pair}}\ tr : (\mathcal{F}\times\mathcal{G})\mathsf{pair}s_1s_2}\ (\times I)$$

Define the natural numbers as: $\mathbb{N} := \mu X.\mathbb{1} + X$, now using the previous rules and (μI) we have:

$$\vdash Cm(\underline{\mathsf{inl}}(\mathsf{id})) : \mathbb{N}\mathsf{inl}\,\mathsf{in1}$$

$$z : \mathbb{N}y \vdash Cm(\underline{\mathsf{inr}}z) : \mathbb{N}\mathsf{inr}y$$

where m is the monotonicity witness for $\mathbb{1}+X$. Note that $\mathsf{inl}\,\mathsf{in1}$ is working as 0 and inr as the successor function.

B Inductive definition of Realizability for Inductive Predicates

Definition 11. *Let* $\mathcal{F} := \lambda\boldsymbol{y}.F$ *and* $\mathcal{F}^{\mathtt{r}} := \lambda\boldsymbol{y}, z.z\ \mathtt{r}\ F$. *We define the realizability for an inductive predicate as:*

$$t\ \mathtt{r}\ (\mu X.\mathcal{F})\boldsymbol{s} := (\mu X^{+}.\mathcal{F}^{\mathtt{r}})\boldsymbol{s}t$$

Observe that

$$(\mu X.\mathcal{F})^{\mathtt{r}} \equiv \lambda\boldsymbol{y}, z.z\ \mathtt{r}\ (\mu X.\mathcal{F})\boldsymbol{y} \equiv \lambda\boldsymbol{y}, z.(\mu X^{+}.\mathcal{F}^{\mathtt{r}})\boldsymbol{y}z = \mu X^{+}.\mathcal{F}^{\mathtt{r}}$$

Lemma 8. *If* $\Gamma \vdash \mathcal{G}\mathsf{mon}X$ *then* $\Gamma \vdash (\mu X.\mathcal{G})\boldsymbol{s} \leftrightarrow \mathcal{G}[X := \mu X.\mathcal{G}]\boldsymbol{s}$.

Proof. The direction $(\leftarrow)$ is consequence of (μI). To prove $(\rightarrow)$, use (μE) with $\mathcal{K} := \mathcal{G}[X := \mu X.\mathcal{G}]$. $\mathcal{G}[X := \mathcal{K}] \subseteq \mathcal{K}$ is provable from $\mathcal{G}\mathsf{mon}X$ by instantiating $X, Y := \mathcal{K}, \mu X.\mathcal{G}$, and using $(\rightarrow E)$ with $\mathcal{K} \subseteq \mu X.\mathcal{G}$, which is consequence of part $(\leftarrow)$.

ℚed

Proposition 9. *If* $\Gamma \vdash \mathcal{F}^{\mathtt{r}}\mathsf{mon}X^{+}$ *then*

$$\Gamma \vdash t\ \mathtt{r}\ (\mu X.\mathcal{F})\boldsymbol{s} \ \leftrightarrow\ t\ \mathtt{r}\ \mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s}.$$

Proof.

$$\begin{array}{rcl} t\ \mathtt{r}\ (\mu X.\mathcal{F})\boldsymbol{s} & = & (\mu X^{+}.\mathcal{F}^{\mathtt{r}})\boldsymbol{s}t \\ & \underset{\text{lemma } 8}{\Leftrightarrow} & \mathcal{F}^{\mathtt{r}}[X^{+} := \mu X^{+}.\mathcal{F}^{\mathtt{r}}]\boldsymbol{s}t \\ & = & \mathcal{F}^{\mathtt{r}}[X^{+} := (\mu X.\mathcal{F})^{\mathtt{r}}]\boldsymbol{s}t \\ & = & (t\ \mathtt{r}\ \mathcal{F}\boldsymbol{s}\,)[X^{+} := (\mu X.\mathcal{F})^{\mathtt{r}}] \\ & \underset{\text{prop. } 5}{=} & t\ \mathtt{r}\ (\mathcal{F}\boldsymbol{s}\,)[X := \mu X.\mathcal{F}] \\ & = & t\ \mathtt{r}\ \mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s} \end{array}$$

$\mathbb{Q}\mathbb{e}\mathbb{d}$

Corollary 3. *If* $\Gamma \vdash \mathcal{F}^{\mathtt{r}}\mathsf{mon}X^{+}$ *then*

$$\Gamma \vdash (\lambda x.x)\ \ \mathtt{r}\ \ \mathcal{F}[X := \mu X.\mathcal{F}]\boldsymbol{s} \to (\mu X.\mathcal{F})\boldsymbol{s}$$

Proof. Straightforward $\mathbb{Q}\mathbb{e}\mathbb{d}$

Proposition 10. *If* $\Gamma \vdash m : \mathcal{F}\mathsf{mon}X$ *then*

$$\Gamma \vdash \lambda x.Cmx : \mathcal{F}[X := \mu X.\mathcal{F}] \subseteq \mu X.\mathcal{F}.$$

Proof. Immediate from (μI). $\mathbb{Q}\mathbb{e}\mathbb{d}$

Proposition 11. *If* $\Gamma \vdash m : \mathcal{F}\mathsf{mon}X$ *then*

$$\Gamma \vdash \forall \boldsymbol{y}.(\mu X.\mathcal{F})\boldsymbol{y} \leftrightarrow (\forall X.\mathcal{F} \subseteq X \to X\boldsymbol{y}).$$

Proof. Let $\mathcal{K} := \lambda \boldsymbol{y}.\forall X.\mathcal{F} \subseteq X \to X\boldsymbol{y}$
$\leftarrow$) Claim. $\Gamma \vdash \lambda u.u(\lambda x.Cmx) : \mathcal{K}\boldsymbol{y} \to (\mu X.\mathcal{F})\boldsymbol{y}$. By $(\forall^2 E)$ with $X := \mu X.\mathcal{F}$ we get $\Gamma, u : \mathcal{K}\boldsymbol{y} \vdash u : \mathcal{F}[X := \mu X.\mathcal{F}] \subseteq \mu X.\mathcal{F} \to (\mu X.\mathcal{F})\boldsymbol{y}$. Using proposition 10 we obtain $\Gamma, u : \mathcal{K}\boldsymbol{y} \vdash u(\lambda x.Cmx) : (\mu X.\mathcal{F})\boldsymbol{y}$ and the claim follows by $(\to I)$.
$\to$) We prove $\Gamma, x : (\mu X.\mathcal{F})\boldsymbol{y} \vdash \mathcal{K}\boldsymbol{y}$ with the rule (μE).
Let $\Delta := \Gamma, x : (\mu X.\mathcal{F})\boldsymbol{y}, z : \mathcal{F} \subseteq X$. By (Var) We have $\Delta \vdash x : (\mu X.\mathcal{F})\boldsymbol{y}$ and $\Delta \vdash z : \mathcal{F}[X := X] \subseteq X$, therefore by (μE) we get $\Delta \vdash xE_{\mu}z : X\boldsymbol{y}$ which leads to $\Gamma, x : (\mu X.\mathcal{F})\boldsymbol{y} \vdash \lambda z.xE_{\mu}z : \mathcal{F} \subseteq X \to X\boldsymbol{y}$, the claim follows by $(\forall^2 I)$.

$\mathbb{Q}\mathbb{e}\mathbb{d}$

Corollary 4 (Parigot's Definition). *If $\Gamma \vdash \mathcal{F}^{\mathtt{r}}\mathsf{mon}X^{+}$ then, under the assumptions Γ, Parigot's definition of realizability for inductive definitions given in [Par92] coincides with our definition.*

Proof. Parigot's definition is, in our notation:

$$t\ \mathtt{r}\ (\mu X.\mathcal{F})\boldsymbol{s} := \forall X^{+}.\mathcal{F}^{\mathtt{r}} \subseteq X^{+} \to X^{+}\boldsymbol{s}t$$

By proposition 11 this is equivalent with $(\mu X^{+}.\mathcal{F}^{\mathtt{r}})\boldsymbol{s}t$, which is our definition of realizability for inductive definitions. ℚed

C System MID2

We propose a system MID2 which includes monotonicity witnesses also in the elimination rule for inductive definitions. We obtain a realizability soundness theorem, with respect to Parigot's definition,[4] into system AF2. This proof depends on the existence of a particular term.

The system MID2 is defined as $\mathsf{AF2} + (\mu I)$ plus the following rule for elimination of inductive definitions.

$$\frac{\Gamma \vdash r : (\mu X.\mathcal{F})\boldsymbol{s} \qquad \Gamma \vdash m : \mathcal{F}\mathsf{mon}X \quad \Gamma \vdash s : \mathcal{F}[X := \mathcal{K}] \subseteq \mathcal{K}}{\Gamma \vdash rE_{\mu}ms : \mathcal{K}\boldsymbol{s}}\ (\mu E^{\dagger})$$

Proposition 12. *If $\Gamma \vdash_{\mathsf{MID2}} m : \mathcal{F}\mathsf{mon}X$ then*

$$\Gamma \vdash_{\mathsf{MID2}} \lambda y.\lambda x.xE_{\mu}my : \mathcal{F}[X := \mathcal{K}] \subseteq \mathcal{K} \to \mu X.\mathcal{F} \subseteq \mathcal{K}.$$

Proof. Straightforward from $(\mu E^{\dagger})$. ℚed

Definition 12. *The formula $\mathcal{F}[X := \mathcal{K}] \subseteq \mathcal{K} \to \mu X.\mathcal{F} \subseteq \mathcal{K}$ is called an induction axiom and is denoted $\mathsf{Ind}_{\mu X.\mathcal{F},\mathcal{K}}$.*

Definition 13. *Let $\widehat{m}, f, w$ be realizers of $\mathcal{F}\mathsf{mon}X$, $\mathcal{F}[X := \mathcal{K}] \subseteq K$ and $(\mu X.\mathcal{F})\boldsymbol{y}$ respectively. The term $\mathbb{R}_{\mu X.\mathcal{F},\mathcal{K}}$ is defined as a solution of the equation*

$$\mathbb{R}_{\mu X.\mathcal{F},\mathcal{K}} f w = f(\widehat{m}(\mathbb{R}_{\mu X.\mathcal{F},\mathcal{K}} f)w),$$

Moreover we add this equation to $\mathbb{E}$.

Proposition 13. *If $\mathbb{O} \vdash m' : \widehat{m}\ \mathtt{r}\ \mathcal{F}\mathsf{mon}X$ then*

$$\mathbb{O} \vdash \lambda x.\lambda y.y(\lambda z.x(m'(\lambda v.v)z)) : \mathbb{R}_{\mu X.\mathcal{F},\mathcal{K}}\ \mathtt{r}\ \mathsf{Ind}_{\mu \mathsf{X}.\mathcal{F},\mathcal{K}}$$

[4] With Parigot's definition we understand definition 6,where the clause for inductive definitions is replaced by $t\ \mathtt{r}\ (\mu X.\mathcal{F})\boldsymbol{s} := \forall X^{+}.\mathcal{F}^{\mathtt{r}} \subseteq X^{+} \to X^{+}\boldsymbol{s}t$

Proof. Let $\mathbb{R} := \mathbb{R}_{\mu X.\mathcal{F},\mathcal{K}}$.
$\mathbb{R}\ \mathtt{r}\ \mathsf{Ind}_{\mu \mathsf{X}.\mathcal{F},\mathcal{K}}$ unfolds to

$$\begin{array}{c}\forall f.(\forall \boldsymbol{y}\forall u.u\ \mathtt{r}\ \mathcal{F}[X := \mathcal{K}]\boldsymbol{y} \to fu\ \mathtt{r}\ \mathcal{K}\boldsymbol{y}) \to \\ (\forall \boldsymbol{y}\forall w.w\ \mathtt{r}\ (\mu X.\mathcal{F})\boldsymbol{y} \to \mathbb{R}fw\ \mathtt{r}\ \mathcal{K}\boldsymbol{y})\end{array}$$

Let $\mathcal{Q} := \lambda \boldsymbol{y}, w.\mathbb{R}fw\ \mathtt{r}\ \mathcal{K}\boldsymbol{y}$ and

$$\Delta := \Theta, x : \forall \boldsymbol{y}\forall u.\mathcal{F}^{\mathtt{r}}[X^+ := \mathcal{K}^{\mathtt{r}}]\boldsymbol{y}u \to \mathcal{K}^{\mathtt{r}}\boldsymbol{y}(fu),$$

we have to prove

$$\Theta \vdash (\forall \boldsymbol{y}\forall u.\mathcal{F}^{\mathtt{r}}[X^+ := \mathcal{K}^{\mathtt{r}}]\boldsymbol{y}u \to \mathcal{K}^{\mathtt{r}}\boldsymbol{y}(fu)) \to (\mu X.\mathcal{F})^{\mathtt{r}} \subseteq \mathcal{Q} \tag{4}$$

We will show first

$$\Delta \vdash (\mu X.\mathcal{F})^{\mathtt{r}} \subseteq \mathcal{Q} \tag{5}$$

Set $\Delta^* := \Delta, y : \forall X^+.\mathcal{F}^{\mathtt{r}} \subseteq X^+ \to X^+\boldsymbol{y}x$, obviously $\Delta^* \vdash y : \mathcal{F}^{\mathtt{r}}[X^+ := \mathcal{Q}] \subseteq \mathcal{Q} \to \mathcal{Q}\boldsymbol{y}x$, therefore, it suffices to show

$$\Delta^* \vdash \mathcal{F}^{\mathtt{r}}[X^+ := \mathcal{Q}] \subseteq \mathcal{Q} \tag{6}$$

Which is a consequence of

$$\Delta^*, z : \mathcal{F}^{\mathtt{r}}[X^+ := \mathcal{Q}]\boldsymbol{u}w \vdash \mathcal{Q}\boldsymbol{u}w \tag{7}$$

Unfolding $\Theta \vdash m' : \widehat{m}\ \mathtt{r}\ \mathcal{F}\mathsf{mon}X$ and instantiating $X^+, Y^+, z := \mathcal{Q}, \mathcal{K}^{\mathtt{r}}, \mathbb{R}f$ we have

$$\begin{array}{l}\Theta \vdash m' : \forall \boldsymbol{y}\forall x.\mathbb{R}fx\ \mathtt{r}\ \mathcal{K}\boldsymbol{y} \to \mathcal{K}^{\mathtt{r}}\boldsymbol{y}(\mathbb{R}fx) \to \\ \quad \forall \boldsymbol{y}\forall x.\mathcal{F}^{\mathtt{r}}[X^+ := \mathcal{Q}]\boldsymbol{y}x \to \mathcal{F}^{\mathtt{r}}[X^+ := \mathcal{K}^{\mathtt{r}}]\boldsymbol{y}(\widehat{m}(\mathbb{R}f)x)\end{array}$$

and from $\vdash \lambda v.v : \forall \boldsymbol{y}\forall x.\mathbb{R}fx\ \mathtt{r}\ \mathcal{K}\boldsymbol{y} \to \mathcal{K}^{\mathtt{r}}\boldsymbol{y}(\mathbb{R}fx)$ we conclude

$$\Delta^* \vdash m'(\lambda v.v) : \mathcal{F}^{\mathtt{r}}[X^+ := \mathcal{Q}]\boldsymbol{u}w \to \mathcal{F}^{\mathtt{r}}[X^+ := \mathcal{K}^{\mathtt{r}}]\boldsymbol{u}(\widehat{m}(\mathbb{R}f)w)$$

which implies

$$\Delta^*, z : \mathcal{F}^{\mathtt{r}}[X^+ := \mathcal{Q}]\boldsymbol{u}w \vdash m'(\lambda v.v)z : \mathcal{F}^{\mathtt{r}}[X^+ := \mathcal{K}^{\mathtt{r}}]\boldsymbol{u}(\widehat{m}(\mathbb{R}f)w) \tag{8}$$

On the other hand we have

$$\Delta \vdash x : \mathcal{F}^{\mathtt{r}}[X^+ := \mathcal{K}^{\mathtt{r}}]\boldsymbol{u}(\widehat{m}(\mathbb{R}f)w) \to \mathcal{K}^{\mathtt{r}}\boldsymbol{u}(f(\widehat{m}(\mathbb{R}f)w))$$

Therefore from (8) we obtain

$$\Delta^*, z : \mathcal{F}^{\mathtt{r}}[X^+ := \mathcal{Q}]\boldsymbol{u}w \vdash x(m'(\lambda v.v)z) : \mathcal{K}^{\mathtt{r}}\boldsymbol{u}(f(\widehat{m}(\mathbb{R}f)w))$$

and from this, by (Eq) with $f(\widehat{m}(\mathbb{R}f)w) = \mathbb{R}fw \in \mathbb{E}$

$$\Delta^*, z : \mathcal{F}^{\mathtt{r}}[X^+ := \mathcal{Q}]\boldsymbol{u}w \vdash x(m'(\lambda v.v)z) : \mathcal{K}^{\mathtt{r}}\boldsymbol{u}(\mathbb{R}fw)$$

and derivation (7) and therefore (6) is proved.

From this we have

$$\Delta^* \vdash \lambda z.x(m'(\lambda v.v)z) : \mathcal{F}^{\mathtt{r}}[X^+ := \mathcal{Q}] \subseteq \mathcal{Q}$$

We have $\Delta^* \vdash y : \mathcal{F}^{\mathtt{r}}[X^+ := \mathcal{Q}] \subseteq \mathcal{Q} \to \mathcal{Q}\boldsymbol{y}x$, therefore

$$\Delta^* \vdash y(\lambda z.x(m'(\lambda v.v)z)) : \mathcal{Q}\boldsymbol{y}x$$

this implies

$$\Delta \vdash \lambda y.y(\lambda z.x(m'(\lambda v.v)z)) : (\mu X.\mathcal{F})^{\mathtt{r}} \subseteq \mathcal{Q}$$

and derivation (5) is proved.

Finally we have

$$\begin{array}{l}\mathbb{\Theta} \vdash \lambda x.\lambda y.y(\lambda z.x(m'(\lambda v.v)z)) : \\ (\forall \boldsymbol{y}\forall u.\mathcal{F}^{\mathtt{r}}[X^+ := \mathcal{K}^{\mathtt{r}}]\boldsymbol{y}u \to \mathcal{K}^{\mathtt{r}}\boldsymbol{y}(fu)) \to (\mu X.\mathcal{F})^{\mathtt{r}} \subseteq \mathcal{Q}\end{array}$$

which is derivation (4).

$\mathbb{Q}\mathrm{ed}$

Definition 14. *Given a term r we define the terms $\widetilde{r}$ and $[\![r]\!]$ as follows:*

$$\begin{array}{rl}\widetilde{x} := x & [\![x]\!] := x \\ \widetilde{\lambda x.r} := \lambda x.\widetilde{r} & [\![\lambda x.r]\!] := \lambda x.[\![r]\!] \\ \widetilde{rs} := \widetilde{r}\,\widetilde{s} & [\![rs]\!] := [\![r]\!][\![s]\!] \\ \widetilde{Cmt} := \lambda x.x(\widetilde{m}(\lambda w.wx)\widetilde{t}) & [\![Cmt]\!] := [\![m]\!](\lambda u.u)[\![t]\!] \\ \widetilde{rE_\mu ms} := \widetilde{r}(\lambda z.\widetilde{s}(\widetilde{m}(\lambda v.v)z)) & [\![rE_\mu ms]\!] := \mathbb{R}_{\mu X.\mathcal{F},\mathcal{K}}[\![s]\!][\![r]\!]\end{array}$$

Theorem 2 (Soundness of Realizability for MID2).
If $\Gamma \vdash_{\mathsf{MID2}} s : A$ then $\Gamma^{\mathtt{r}} \vdash_{\mathsf{AF2}} \widetilde{s} : [\![s]\!][\boldsymbol{x} := \boldsymbol{t}]\ \mathtt{r}\ A$

Proof. Induction on $\vdash_{\mathsf{MID2}}$. We concentrate on the cases for inductive definitions. For a term r let $\widehat{r} := [\![r]\!][\boldsymbol{x} := \boldsymbol{t}]$.
Case $(\mu E^\dagger)$. By IH we have $\Gamma^{\mathtt{r}} \vdash \widetilde{m} : \widehat{m}\ \mathtt{r}\ \mathcal{F}\mathsf{mon}X$, therefore by proposition 13 we have

$$\Gamma^{\mathtt{r}} \vdash \lambda x.\lambda y.y(\lambda z.x(\widetilde{m}(\lambda v.v)z)) : \forall x.x\ \mathtt{r}\ \mathcal{F}[X := \mathcal{K}] \subseteq \mathcal{K} \to \mathbb{R}x\ \mathtt{r}\ \mu X.\mathcal{F} \subseteq \mathcal{K}$$

Again by IH we have $\Gamma^{\mathtt{r}} \vdash \widetilde{s} : \widehat{s}\ \mathtt{r}\ \mathcal{F}[X := \mathcal{K}] \subseteq \mathcal{K}$, hence by $(\to E)$ and subject reduction:

$$\Gamma^{\mathtt{r}} \vdash \lambda y.y(\lambda z.\widetilde{s}(\widetilde{m}(\lambda v.v)z)) : \mathbb{R}\widehat{s}\ \mathtt{r}\ \mu X.\mathcal{F} \subseteq \mathcal{K}$$

which is identical with

$$\Gamma^{\mathtt{r}} \vdash \lambda y.y(\lambda z.\widetilde{s}(\widetilde{m}(\lambda v.v)z)) : \forall \boldsymbol{y} \forall z.z\ \mathtt{r}\ (\mu X.\mathcal{F})\boldsymbol{y} \to \mathbb{R}\widehat{s}z\ \mathtt{r}\ \mathcal{K}\boldsymbol{y}$$

By IH we have $\Gamma^{\mathtt{r}} \vdash \widetilde{r} : \widehat{r}\ \mathtt{r}\ (\mu X.\mathcal{F})\boldsymbol{s}$, and we conclude, again by $(\to E)$ and subject reduction:

$$\Gamma^{\mathtt{r}} \vdash \widetilde{r}(\lambda z.\widetilde{s}(\widetilde{m}(\lambda v.v)z)) : \mathbb{R}\widehat{s}\widehat{r}\ \mathtt{r}\ \mathcal{K}\boldsymbol{s},$$

i.e.,

$$\Gamma^{\mathtt{r}} \vdash \widetilde{rE_\mu ms} : [\![rE_\mu ms]\!][\boldsymbol{x} := \boldsymbol{t}]\ \mathtt{r}\ \mathcal{K}\boldsymbol{s}$$

Case (μI). By IH we have $\Gamma^{\mathtt{r}} \vdash_{\mathsf{AF2}\mu} \widetilde{m} : \widehat{m}\ \mathtt{r}\ \mathcal{F}\mathsf{mon}X$, which is the same as

$$\begin{aligned}\Gamma^{\mathtt{r}} \vdash_{\mathsf{AF2}\mu} \widetilde{m} : \forall X^+ \forall Y^+ \forall z.(\forall \boldsymbol{y} \forall x.X^+\boldsymbol{y}x \to Y^+\boldsymbol{y}(zx)) \quad \to \\ (\forall \boldsymbol{y} \forall x.\mathcal{F}^{\mathtt{r}}\boldsymbol{y}x \to \mathcal{F}^{\mathtt{r}}[X^+ := Y^+]\boldsymbol{y}(\widehat{m}zx))\end{aligned} \tag{9}$$

First we prove

$$\Gamma^{\mathtt{r}}, x : \mathcal{F}^{\mathtt{r}} \subseteq X^+ \vdash_{\mathsf{AF2}\mu} \lambda w.wx : \mu X^+.\mathcal{F}^{\mathtt{r}} \subseteq X^+ \tag{10}$$

From

$$\Gamma^{\mathtt{r}}, x : \mathcal{F}^{\mathtt{r}} \subseteq X^+, w : (\mu X^+.\mathcal{F}^{\mathtt{r}})\boldsymbol{y}z \vdash_{\mathsf{AF2}\mu} w : \forall X^+.\mathcal{F}^{\mathtt{r}} \subseteq X^+ \to X^+\boldsymbol{y}z$$

we have

$$\Gamma^{\mathtt{r}}, x : \mathcal{F}^{\mathtt{r}} \subseteq X^+, w : (\mu X^+.\mathcal{F}^{\mathtt{r}})\boldsymbol{y}z \vdash_{\mathsf{AF2}\mu} wx : X^+\boldsymbol{y}z$$

and from $(\to I)$ we conclude

$$\Gamma^{\mathtt{r}}, x : \mathcal{F}^{\mathtt{r}} \subseteq X^+ \vdash_{\mathsf{AF2}\mu} \lambda w.wx : \forall \boldsymbol{y}z : (\mu X^+.\mathcal{F}^{\mathtt{r}})\boldsymbol{y}z \to X^+\boldsymbol{y}z$$

and derivation (10) is proved.
Instantiating $X^+, Y^+, z := \mu X^+.\mathcal{F}^{\mathtt{r}}, X^+, \lambda u.u$ in derivation (9), and using (Eq) with $(\lambda u.u)x = x\ \in \mathbb{E}$, we get

$$\begin{aligned}&\Gamma^{\mathtt{r}} \vdash_{\mathsf{AF2}\mu} \widetilde{m} : \mu X^+.\mathcal{F}^{\mathtt{r}} \subseteq X^+ \\ &\quad \to \quad \forall \boldsymbol{y} \forall x.\mathcal{F}^{\mathtt{r}}[X^+ := \mu X^+.\mathcal{F}^{\mathtt{r}}]\boldsymbol{y}x \to \mathcal{F}^{\mathtt{r}}\boldsymbol{y}(\widehat{m}(\lambda u.u)x)\end{aligned}$$

By derivation (10) and $(\to E)$ we have

$$\begin{aligned}\Gamma^{\mathbf{r}}, x : \mathcal{F}^{\mathbf{r}} \subseteq X^+ \vdash_{\mathsf{AF2}\mu} \widetilde{m}(\lambda w.wx) : \forall \boldsymbol{y} \forall x.\mathcal{F}^{\mathbf{r}}[X^+ := \mu X^+.\mathcal{F}^{\mathbf{r}}]\boldsymbol{y}x \\ \to \quad \mathcal{F}^{\mathbf{r}}\boldsymbol{y}(\widehat{m}(\lambda u.u)x)\end{aligned}$$

By IH we have $\Gamma^{\mathbf{r}} \vdash_{\mathsf{AF2}\mu} \widetilde{r} : \mathcal{F}^{\mathbf{r}}[X^+ := \mu X^+.\mathcal{F}^{\mathbf{r}}]\boldsymbol{s}\widehat{r}$, therefore applying $\forall E, \forall E, \to E$ we obtain

$$\Gamma^{\mathbf{r}}, x : \mathcal{F}^{\mathbf{r}} \subseteq X^+ \vdash_{\mathsf{AF2}\mu} \widetilde{m}(\lambda w.wx)\widetilde{r} : \mathcal{F}^{\mathbf{r}}\boldsymbol{s}(\widehat{m}(\lambda u.u)\widehat{r})$$

Finally by $\to I, \forall^2 I$ we get

$$\Gamma^{\mathbf{r}} \vdash_{\mathsf{AF2}\mu} \lambda x.x(\widetilde{m}(\lambda w.wx)\widetilde{r}) : \forall X^+.\mathcal{F}^r \subseteq X^+ \to X^+\boldsymbol{s}(\widehat{m}(\lambda u.u)\widehat{r})$$

That is, $\Gamma^{\mathbf{r}} \vdash_{\mathsf{AF2}\mu} \widetilde{Cmr} : \widehat{Cmr}\ \mathtt{r}\ (\mu X.\mathcal{F})\boldsymbol{s}$

Qed

References

[Ben98] Holger Benl. Konstruktive Interpretation induktiver Definitionen. (Constructive Interpretation of Inductive Definitions) (In German). Diplomarbeit, Mathematisches Institut der LMU München. June 1996.

[Ber93] Ulrich Berger. Program Extraction from normalization proofs. In *Typed Lambda Calculus and Applications*, edited by, M. Bezem and J.F. Groote. LNCS 664, Springer Verlag. 1993.

[Ber95] Ulrich Berger. A constructive interpretation of positive inductive definitions. Unpublished Draft. March 1995.

[BBS02] U. Berger, W. Buchholz, H. Schwichtenberg. Refined Program Extraction from Classical Proofs. In *Annals of Pure and Applied Logic* 114(1-3), pp. 3-25. Elsevier Science B.V. April 2002.

[Geu92] H. Geuvers. Inductive and coinductive types with iteration and recursion. In B. Nordström, K. Petterson, G. Plotkin, Eds. *Proceedings of the 1992 Workshop on Types for Proofs and Programs* Båstad, Sweden, June 1992, pp. 193-217, 1992.

[JaRu97] B. Jacobs, J. Rutten. A Tutorial on (Co)Algebras and (Co)Induction. EATCS Bulletin 62. p. 222-259. 1997.

[KrPa90] J.L. Krivine, M. Parigot. Programming with Proofs. In *Journal of Information Processing and Cybernetics EIK (Formerly Elektronische Informationsverarbeitung und Kybernetik)* 26(3) pp. 149-167. 1990.

[Kri93] J.L. Krivine. Lambda-Calculus, Types and Models. Ellis Horwood Series in Computers and their Applications. Ellis Horwood, Masson 1993.

[Mat98] Ralph Matthes, Extensions of System F by Iteration and Primitive Recursion on Monotone Inductive Types, Dissertation Universität München, 1999.

[Mat99] Ralph Matthes. Monotone (co)inductive types and positive fixed-point types. In *Theoretical Informatics and Applications* 33(4-5) pp. 309-328. EDP Sciences. 1999.

[Par92] M. Parigot, Recursive programming with proofs. In *Theoretical Computer Science* 94, pp 335-356. Elsevier. 1992.

[Raf94] C. Raffalli. L' Arithmétique Fonctionnelle du Second Ordre avec Points Fixes, Thése de l'Université Paris VII. 1994.

[Tat93] M. Tatsuta, Realizability of Inductive Definitions for Constructive Programming. PhD Thesis, University of Tokyo, 1993.

[UuVe02] T. Uustalu, V. Vene. Least and greatest fixed points in intuitionistic natural deduction. In *Theoretical Computer Science*, 272(1-2),pp. 315-339. Elsevier Science B.V. February 2002.

[Wad01] P. Wadler. The Girard-Reynolds Isomorphism. In TACS2001, *Theoretical Aspects of Computer Software*, edited by N. Kobayashi, B.C. Pierce. LNCS 2215. Springer Verlag. 2001