Intuitionistic Fixed Point Logic and Program Extraction (with Prawf)

Prifysgol Abertawe
Swansea University

Olga Petrovska
(joint work with Ulrich Berger (SU) and Hideki Tsuiki (Kyoto University))

6-8 April, BCTCS 2020 (Coronavirus Edition )

This work was supported by the Marie Curie International Research Staff Exchange Schemes *Computable Analysis* (PIRSES-GA-2011-294962) and *Correctness by Construction* (FP7-PEOPLE-2013-IRSES-612638) as well as the Marie Curie RISE project *Computing with Infinite Data* (H2020-MSCA-RISE-2016-731143) and the EPSRC Doctoral Training Grant No. 1818640.

Motivation

Creating a formal system exploiting Curry-Howard isomorphism to extract useful and ‘correct-by-construction’ programs from proofs about abstract mathematics.

Motivation

Creating a formal system exploiting Curry-Howard isomorphism to extract useful and ‘correct-by-construction’ programs from proofs about abstract mathematics.

Existing systems:

Motivation

Creating a formal system exploiting Curry-Howard isomorphism to extract useful and ‘correct-by-construction’ programs from proofs about abstract mathematics.

Existing systems:

- Minlog (H. Schwichtenberg): *http://www.mathematik.uni-muenchen.de/~logik/minlog/index.php*

Motivation

Creating a formal system exploiting Curry-Howard isomorphism to extract useful and ‘correct-by-construction’ programs from proofs about abstract mathematics.

Existing systems:

- Minlog (H. Schwichtenberg): *http://www.mathematik.uni-muenchen.de/~logik/minlog/index.php*

- Nuprl, Isabelle, Coq etc.

Motivation

Creating a formal system exploiting Curry-Howard isomorphism to extract useful and ‘correct-by-construction’ programs from proofs about abstract mathematics.

Existing systems:

- Minlog (H. Schwichtenberg): *http://www.mathematik.uni-muenchen.de/~logik/minlog/index.php*
- Nuprl, Isabelle, Coq etc.
-  Prawf *NEW*

Agenda

- Intuitionistic Fixed Point Logic
- Realizability
- Soundness
- Demo

Intuitionistic Fixed Point Logic (IFP) as a schema

First-order logic with lambda abstractions and fixed point operators

IFP is a schema

(1) *Sorts* $\iota, \iota_1, \ldots$ as names for spaces of abstract mathematical objects.

(2) *Terms* $(\vec{t})$ that include *variables*, *constants* of fixed sorts ι and *function symbols* types $\vec{\iota} \to \iota$.

(3) *Predicate constants* of fixed arities $(\vec{\iota})$.

$$
\begin{array}{lll}
\textit{Formulas} \ni A, B & ::= & P(\vec{t}) \\
& \mid & A \wedge B \mid A \vee B \mid A \to B \mid \forall x\, A \mid \exists x\, A \\
\textit{Predicates} \ni P, Q & ::= & X \mid P \mid \lambda \vec{x}\, A \mid \mu\, \Phi \mid \nu\, \Phi \\
\textit{Operators} \ni \Phi, \Psi & ::= & \lambda X\, P \ (P \text{ is strictly positive in } X)
\end{array}
$$

Intuitionistic Fixed Point Logic (IFP)

- Intuitionistic Predicate Logic

  Natural deduction with equality

- Inductions and Coinduction

$$\frac{}{\Phi(\mu\,\Phi) \subseteq \mu\,\Phi}\ \mathrm{cl} \qquad \frac{\Phi(P) \subseteq P}{\mu\,\Phi \subseteq P}\ \mathrm{ind}$$

$$\frac{}{\nu\,\Phi \subseteq \Phi(\nu\,\Phi)}\ \mathrm{cocl} \qquad \frac{P \subseteq \Phi(P)}{P \subseteq \nu\,\Phi}\ \mathrm{coind}$$

- Axioms consisting of closed disjunction-free formulas

  e.g., $\forall x\,, y(x + y = y + x)$

Realizability and RIFP

A *realizer* is an object that "realizes" a formula from a formal theory, i.e. serves as a confirmation of its truth.

IFP for Realisers (RIFP)

The Scott domain of realizers is defined by the recursive domain equation

$$D = \mathbf{Nil} + \mathbf{Lt}(D) + \mathbf{Rt}(D) + \mathbf{Pair}(D \times D) + \mathbf{F}(D \to D)$$

where $+$ denotes the separated sum, $\times$ the Cartesian product and $D \to D$ is the continuous function space.

Non-Computational and Harrop Expressions

A *Harrop* expression contains no disjunction or free predicate variable at a strictly positive position [1].

A *non-computational* expression contains neither disjunctions nor free predicate variable.

[1] predicate variable is not free in the premise of an implication

Realizability and Simplified Realizability

We assing to every

- non-Harrop formula A a predicate $\mathsf{R}(A)$ with one argument for realizers
- non-Harrop predicate P a predicate $\mathsf{R}(P)$ with an extra argument for realizers
- non-Harrop operator Φ an operator $\mathsf{R}(\Phi)$ with an extra argument for realizers

- Harrop formula A a formula $\mathsf{H}(A)$
- Harrop predicate P a predicate $\mathsf{H}(P)$ of the same arity
- Harrop operator Φ an operator $\mathsf{H}(\Phi)$ of the same arity

Realizability interpretation

$$
\begin{aligned}
a \,\mathbf{r}\, A &= \mathbf{H}(A) \wedge a = \mathbf{Nil} \ (A \text{ Harrop}) \\
\mathbf{R}(P) &= \lambda(\vec{x}, a)\,(\mathbf{H}(P) \wedge a = \mathbf{Nil}) \ (P \text{ Harrop}) \\
&\text{Otherwise} \\
a \,\mathbf{r}\, P(\vec{t}) &= \mathbf{R}(P)(\vec{t}, a) \qquad\qquad \mathbf{H}(P(\vec{t})) = \mathbf{H}(P)(\vec{t}) \\
c \,\mathbf{r}\, (A \wedge B) &= ((\pi_l c) \,\mathbf{r}\, A \wedge (\pi_r c) \,\mathbf{r}\, B) \qquad \mathbf{H}(A \wedge B) = \mathbf{H}(A) \wedge \mathbf{H}(B) \\
&\quad (\text{neither } A \text{ nor } B \text{ Harrop}) \\
a \,\mathbf{r}\, (A \wedge B) &= a \,\mathbf{r}\, A \wedge \mathbf{H}(B) \quad (B \text{ Harrop}) \\
b \,\mathbf{r}\, (A \wedge B) &= \mathbf{H}(A) \wedge b \,\mathbf{r}\, B \quad (A \text{ Harrop}) \\
c \,\mathbf{r}\, (A \vee B) &= \exists a\,(c = \mathbf{Lt}(a) \wedge a \,\mathbf{r}\, A \vee c = \mathbf{Rt}(a) \wedge a \,\mathbf{r}\, B) \\
f \,\mathbf{r}\, (A \to B) &= \forall a\,(a \,\mathbf{r}\, A \to (f\, a) \,\mathbf{r}\, B)) \qquad \mathbf{H}(A \to B) = \mathbf{r}\, A \to \mathbf{H}(B) \\
&\quad (\text{neither } A \text{ nor } B \text{ Harrop}) \\
b \,\mathbf{r}\, (A \to B) &= \mathbf{H}(A) \to b \,\mathbf{r}\, B \quad (A \text{ Harrop}) \\
a \,\mathbf{r}\, \Diamond x\, A &= \Diamond x\, (a \,\mathbf{r}\, A) \quad (\Diamond \in \{\forall, \exists\}) \qquad \mathbf{H}(\Diamond x\, A) = \Diamond x\, \mathbf{H}(A) \\
\mathbf{R}(X) &= \tilde{X} \qquad\qquad \mathbf{H}(P) = P \\
\mathbf{R}(\Diamond\, \Phi) &= \Diamond\, \mathbf{R}(\Phi) \quad (\Diamond \in \{\nu, \mu\}) \qquad \mathbf{H}(\Diamond\, \Phi) = \Diamond\, \mathbf{H}(\Phi) \\
\mathbf{R}(\lambda \vec{x}\, A) &= \lambda \vec{x}\, \mathbf{R}(A) \quad (= \lambda(\vec{x}, a)\, a \,\mathbf{r}\, A) \qquad \mathbf{H}(\lambda \vec{x}\, A) = \lambda \vec{x}\, \mathbf{H}(A) \\
\mathbf{R}(\lambda X\, P) &= \lambda \tilde{X}\, \mathbf{R}(P) \qquad\qquad \mathbf{H}(\lambda X\, P) = \lambda X\, \mathbf{H}_X(P)
\end{aligned}
$$

Soundness

$$\Gamma, \Delta \vdash_{IFP} A^* \Rightarrow \mathsf{H}(\Gamma), \vec{a}\,\mathsf{r}\,\Delta \vdash_{RIFP} p\,\mathsf{r}\,A, \text{ where } \mathrm{FV}(p) \subseteq \vec{a}.$$

*The admissibility condition is that either Φ and P are both Harrop or both non-Harrop or Φ is Harrop and *simple* and P is non-Harrop. Simple means that no sub-expression (of an expression in question) of a form $\mu\Phi$ or $\nu\Phi$ contains a predicate variable X free.

IFP' and the Soundness Theorem

Hideki Tsuiki suggested creating IFP' to get rid of the admissibility restriction. This also proved to be useful for simplifying program extraction implementation.

Monotonicity of the operator Φ:

$$\mathrm{Mon}(\Phi) \stackrel{\mathrm{Def}}{=} X \subseteq Y \to \Phi(X) \subseteq \Phi(Y)$$

where X and Y are fresh variables.

$$\frac{\Phi(P) \subseteq P \quad \mathrm{Mon}(\Phi)}{\mu(\Phi) \subseteq P}\ \mathrm{IND'}(\Phi, P) \quad (*)$$

$$\frac{P \subseteq \Phi(P) \quad \mathrm{Mon}(\Phi)}{P \subseteq \nu(\Phi)}\ \mathrm{COIND'}(\Phi, P) \quad (*)$$

$(*)$ free assumptions in the proof of $\mathrm{Mon}(\Phi)$ must not contain X or Y free.

Soundness proof i

$\Gamma, \Delta \vdash_{IFP'} A \Rightarrow \mathsf{H}(\Gamma), \vec{a}\,\mathbf{r}\,\Delta \vdash_{RIFP} p\,\mathbf{r}\,A$, where $\mathrm{FV}(p) \subseteq \vec{a}$.
Proof by induction on the length of IFP' derivations.

Soundness proof ii

Ind′. Assume $\vdash_{IFP'} (\Phi(P) \subseteq P)$, where $\Phi(P) = Q[P/X]$ and $\vdash_{IFP'} Mon(\Phi)$, i.e. $X \subseteq Y \to Q \subseteq Q[Y/X]$.

- I.h.$_{1nH} \vdash_{RIFP} s\,\mathbf{r}\,(\Phi(P) \subseteq P)$;
- I.h.$_{mon_{nH}} \vdash_{RIFP} m\,\mathbf{r}\,(Mon(\Phi))$;

If Φ and P are non-Harrop show:

$$
\begin{array}{lll}
 & f\,\mathbf{r}\,(\mu(\Phi) \subseteq P) & \\
\equiv & \mathbf{R}(\mu\Phi) \subseteq f^{-1} \circ \mathbf{R}(P) & f\,\mathbf{r}\,(Q \subseteq P) \equiv \mathbf{R}(Q) \subseteq f^{-1} \circ \mathbf{R}(P)* \\
= & \mathbf{R}(\mu(\lambda X\, Q)) \subseteq f^{-1} \circ \mathbf{R}(P) & \text{since } \Phi = \lambda X\, Q \\
= & (\mu(\lambda \tilde{X} \mathbf{R}(Q))) \subseteq f^{-1} \circ \mathbf{R}(P) & \text{since } \mathbf{R}(\mu\Phi) = \mu(\mathbf{R}(\Phi)) \\
 & & \text{and } \mathbf{R}(\lambda X\, Q) = \lambda \tilde{X}(\mathbf{R}(Q))
\end{array}
$$

* Proven by a separate lemma, which includes a number of equivalences like above

Soundness proof iii

By s.p. induction, it is enough to show

$$\mathbf{R}(Q)[f^{-1} \circ \mathbf{R}(P)/\tilde{X}] \subseteq f^{-1} \circ \mathbf{R}(P) \tag{1}$$

By i.h.$_{1nH}$ we have: $s\,\mathbf{r}\,(\Phi(P) \subseteq (P))$, which is equivalent to

$$\mathbf{R}(Q[P/X]) \subseteq s^{-1} \circ \mathbf{R}(P) \tag{2}$$

By i.h.$_{mon_{nH}}$ we have $m\,\mathbf{r}\,Mon(\Phi)$ and by Lemma (a) this implies

$$m\,\mathbf{r}\,(Mon(\Phi)[P/Y]) \tag{3}$$

Writing out $Mon(\Phi)[P/Y]$ we obtain $X \subseteq P \to Q \subseteq Q[P/X]$. Hence, 3 can be rewritten as

$$\begin{aligned}
& \forall g(g\,\mathbf{r}\,(X \subseteq P) \to (m\ g)\,\mathbf{r}\,(Q \subseteq Q[P/X])) \\
\equiv\ & \forall g(\mathbf{R}(X) \subseteq g^{-1} \circ \mathbf{R}(P) \to \mathbf{R}(Q) \subseteq (m\ g)^{-1} \circ \mathbf{R}(Q[P/X])) && \text{by the equivalences lemma} \\
=\ & \forall g(\tilde{X} \subseteq g^{-1} \circ \mathbf{R}(P) \to \mathbf{R}(Q) \subseteq (m\ g)^{-1} \circ \mathbf{R}(Q[P/X])) && \text{by def. of } \mathbf{R}(X)
\end{aligned}$$

(a) If RIFP proves $a\,\mathbf{r}\,A$ from assumptions that do not contain the predicate variable X and if P is a non-Harrop predicate of the same arity as X, then RIFP proves $a\,\mathbf{r}\,(A[P/X])$ from the same assumptions.

Soundness proof iv

$\forall g(\tilde{X} \subseteq g^{-1} \circ \mathbf{R}(P) \to \mathbf{R}(Q) \subseteq (m\ g)^{-1} \circ \mathbf{R}(Q[P/X]))$

If we define g as f and $\tilde{X} = f^{-1} \circ \mathbf{R}(P)$ and use Lemma (b), we get

$$\begin{aligned} \mathbf{R}(Q)[f^{-1} \circ \mathbf{R}(P)/\tilde{X}] &\subseteq (m\ f)^{-1} \circ \mathbf{R}(Q[P/X])) \\ &\subseteq (m\ f)^{-1} \circ (s^{-1} \circ \mathbf{R}(P)) && \text{by 2} \\ &= (s\ \circ\ m\ f)^{-1} \circ \mathbf{R}(P) && \text{by the equivalences lemma} \end{aligned}$$

Hence, the realiser is recursively defined as $f = s\ \circ\ m\ f$

(b) If IFP, IFP', or RIFP proves $\mathbf{\Gamma} \vdash A$, then the same system proves $\mathbf{\Gamma}[P/X] \vdash A[P/X]$, $\mathbf{\Gamma}[P/X] \vdash A[P/X]$, where A, P, X are arbitrary formulas, predicates, predicate variables, respectively, and $\hat{X}$ is an arbitrary predicate constant that does not appear in any axiom.

Key points before the demo

- IFP is a scheme

  more flexibility, abstraction (e.g., list reversal, translation between representations)
- Use of classical logic as long as it is disjunction-free
- Prawf is build specifically for the purpose of program extraction

Demo

Future work

- Extensions for sequent calculus proofs (Yvett Szilagyi)
- Extension for CFP (Concurrent Fixed Point Logic)
- Developing theorems database in Prawf

References

U. Berger, P. O., and H. Tsuiki.
Prawf: An interactive proof system for program extraction.
To be published in proceedings of 16th Conference on Computability in Europe, CiE, 2020.

U. Berger and O. Petrovska.
Optimised program extraction for induction and coinduction.
In *Sailing Routes in the World of Computation: 14th Conference on Computability in Europe, CiE 2018, Kiel, Germany, July 30 – August 3*, pages 70–80, 2018.

U. Berger and H. Tsuiki.
Intuitionistic fixed point logic.
Unpublished manuscript available on ArXiv, 2019.

Prawf: *https://prawftree.wordpress.com/*

Thank you