

A Cyclic Proof System for HFL_N

Mayuko Kori (SOKENDAI & NII, Tokyo, Japan),
Takeshi Tsukada (Chiba University, Chiba, Japan),
Naoki Kobayashi (The University of Tokyo, Tokyo, Japan)

Jan 27, 2021 in Computer Science Logic

Overview

A cyclic proof system for $\text{HFL}_{\mathbb{N}}$ (Higher-order logic with fixed-points and $\mathbb{N}$ [Kobayashi+ ESOP18])

- Convenient for semi-automated verification of higher-order programs

What is a Cyclic Proof?

- Finite derivation tree with back edges (pre-proof)
+ soundness condition (global trace condition)

[Sprenger&Dam FoSSaCS03; Brotherston&Simpson IJLP11]

$$\begin{array}{c}
 \frac{\frac{\frac{}{\vdash \mathbf{Z} = \mathbf{Z} \wedge \mathbf{Z} = \mathbf{Z}}{(\wedge R, = R)}}{\vdash P(\mathbf{Z}, \mathbf{Z}, \mathbf{Z})} (\mu R)}{x = \mathbf{Z} \vdash P(x, \mathbf{Z}, x)} (= L) \\
 \frac{\frac{\frac{Nx' \vdash P(x', \mathbf{Z}, x')}{Nx' \vdash P(\mathbf{S}x', \mathbf{Z}, \mathbf{S}x')} (\mu R)}{x = \mathbf{S}x', Nx' \vdash P(x, \mathbf{Z}, x)} (= L)}{\exists x'. x = \mathbf{S}x' \wedge Nx' \vdash P(x, \mathbf{Z}, x)} (\exists L, \wedge L) \\
 \frac{(x = \mathbf{Z}) \vee (\exists x'. x = \mathbf{S}x' \wedge Nx' \vdash P(x, \mathbf{Z}, x))}{Nx \vdash P(x, \mathbf{Z}, x)} (\vee L) \quad \leftarrow (\mu L)
 \end{array}$$

- Convenient for automated proof search
[Brotherston+ CADE11; Brotherston+ APLAS12]

Contributions

First cyclic proof system for a higher-order logic

- Definition of the global trace condition (soundness criterion for cyclic proofs)
- Soundness
- Decidability of the global trace condition
- Completeness of an infinitary variant

Outline

- Background: $\text{HFL}_{\mathbb{N}}$ syntax & semantics
- Definition of our cyclic proof system
 - Example of cyclic proofs (from program verif.)
- Some properties
 - Soundness
 - Decidability of g.t.c.
 - Completeness of the infinitary system
- Related work
- Conclusion & Future work

Outline

- Background: $\text{HFL}_{\mathbb{N}}$ syntax & semantics
- Definition of our cyclic proof system
 - Example of cyclic proofs (from program verif.)
- Some properties
 - Soundness
 - Decidability of g.t.c.
 - Completeness of the infinitary system
- Related work
- Conclusion & Future work

HFL_N syntax

for propositions

- Type $A ::= \mathbf{N} \mid T \quad T ::= \mathbf{\Omega} \mid A \rightarrow T$

- Term $s, t ::= x \mid \mathbf{Z} \mid St$

- Formula

$$\varphi, \psi ::= x \mid s^{\mathbf{N}} = t^{\mathbf{N}} \mid \varphi \vee \psi \mid \varphi \wedge \psi \mid$$
$$\lambda x^A . \varphi \mid \varphi \psi \mid \varphi t \mid \mu x^T . \varphi \mid \nu x^T . \varphi$$

least fixed-point
of $\lambda x . \varphi$

greatest fixed-point
of $\lambda x . \varphi$

Examples of $\text{HFL}_{\mathbb{N}}$ formulas

$$\begin{aligned}
 & (\mu Y^{\mathbb{N} \rightarrow \Omega} . \lambda x^{\mathbb{N}} . \varphi \vee Y(\mathbf{S}x)) \mathbf{Z} \\
 & \equiv \varphi[\mathbf{Z}/x] \vee (\mu Y . \lambda x . \varphi \vee Y(\mathbf{S}x)) \mathbf{SZ} \\
 & \equiv \dots \equiv \varphi[\mathbf{Z}/x] \vee \varphi[\mathbf{SZ}/x] \vee \dots \equiv \exists x^{\mathbb{N}} . \varphi
 \end{aligned}$$

Likewise, $\top$, $\perp$, $\forall$, $\exists$, $\neq$ can be represented by

$$\begin{aligned}
 \top & \equiv \nu x^{\Omega} . x, \quad \perp \equiv \mu x^{\Omega} . x, \\
 \forall x^{\mathbb{N}} . \varphi & \equiv (\nu Y^{\mathbb{N} \rightarrow \Omega} . \lambda x^{\mathbb{N}} . \varphi \wedge Y(\mathbf{S}x)) \mathbf{Z}, \text{ etc.}
 \end{aligned}$$

Syntax

- Type $A ::= \mathbb{N} \mid T \quad T ::= \Omega \mid A \rightarrow T$
- Term $s, t ::= x \mid \mathbf{Z} \mid \mathbf{S}t$
- Formula

$$\begin{aligned}
 \varphi, \psi & ::= x \mid s^{\mathbb{N}} = t^{\mathbb{N}} \mid \varphi \vee \psi \mid \varphi \wedge \psi \\
 & \mid \lambda x^A . \varphi \mid \varphi \psi \mid \varphi t \mid \mu x^T . \varphi \mid \nu x^T . \varphi
 \end{aligned}$$

HFL_N semantics

- Type

$$\llbracket \mathbf{N} \rrbracket := (\mathbb{N}, \sqsubseteq_{\mathbf{N}}), \llbracket \mathbf{\Omega} \rrbracket := (\{\top, \perp\}, \sqsubseteq_{\Omega})$$

complete lattice

$$\llbracket A \rightarrow T \rrbracket := (\{f : \llbracket A \rrbracket \rightarrow \llbracket T \rrbracket \mid f \text{ is monotone}\}, \sqsubseteq_{A \rightarrow T})$$

$$\text{where } x \sqsubseteq_{\mathbf{N}} y :\Leftrightarrow x = y$$

$$x \sqsubseteq_{\Omega} y :\Leftrightarrow x = \perp \text{ or } y = \top$$

$$f \sqsubseteq_{A \rightarrow T} g :\Leftrightarrow \forall x \in \llbracket A \rrbracket. f(x) \sqsubseteq_T g(x).$$

- Formulas $\llbracket \mathcal{H} \vdash \varphi : A \rrbracket : \llbracket \mathcal{H} \rrbracket \rightarrow \llbracket A \rrbracket$ ($\mathcal{H}$: type environment)

$$\llbracket \mathcal{H} \vdash \mu x^T. \varphi : T \rrbracket(\rho) = \text{lfp}(\llbracket \mathcal{H} \vdash \lambda x^T. \varphi : T \rightarrow T \rrbracket(\rho))$$

$$\llbracket \mathcal{H} \vdash \nu x^T. \varphi : T \rrbracket(\rho) = \text{gfp}(\llbracket \mathcal{H} \vdash \lambda x^T. \varphi : T \rightarrow T \rrbracket(\rho))$$

Outline

- Background: $\text{HFL}_{\mathbb{N}}$ syntax & semantics
- Definition of our cyclic proof system
 - Example of cyclic proofs (from program verif.)
- Some properties
 - Soundness
 - Decidability of g.t.c.
 - Completeness of the infinitary system
- Related work
- Conclusion & Future work

Cyclic Proof

pre-proof + global trace condition

finite derivation tree
+ back-edges

soundness condition

$$\begin{array}{c}
 \frac{\frac{\frac{}{\vdash \mathbf{Z} = \mathbf{Z} \wedge \mathbf{Z} = \mathbf{Z}}{(\wedge R, = R)}}{\vdash P(\mathbf{Z}, \mathbf{Z}, \mathbf{Z})} (\mu R)}{x = \mathbf{Z} \vdash P(x, \mathbf{Z}, x)} (= L) \\
 \frac{\frac{\frac{Nx' \vdash P(x', \mathbf{Z}, x')}{Nx' \vdash P(\mathbf{S}x', \mathbf{Z}, \mathbf{S}x')} (\mu R)}{x = \mathbf{S}x', Nx' \vdash P(x, \mathbf{Z}, x)} (= L)}{\exists x'. x = \mathbf{S}x' \wedge Nx' \vdash P(x, \mathbf{Z}, x)} (\exists L, \wedge L) \\
 \frac{(x = \mathbf{Z}) \vee (\exists x'. x = \mathbf{S}x' \wedge Nx') \vdash P(x, \mathbf{Z}, x)}{Nx \vdash P(x, \mathbf{Z}, x)} (\vee L, \mu L)
 \end{array}$$

Deduction rules

Rules of LK (including the cut rule) plus...

- $$\frac{\Gamma, \varphi[\sigma x.\varphi/x] \vec{\psi} \vdash \Delta}{\Gamma, (\sigma x.\varphi) \vec{\psi} \vdash \Delta} (\sigma L) \quad \frac{\Gamma \vdash \varphi[\sigma x.\varphi/x] \vec{\psi}, \Delta}{\Gamma \vdash (\sigma x.\varphi) \vec{\psi}, \Delta} (\sigma R)$$

where $\sigma \equiv \mu, \nu$
- $$\frac{\Gamma \vdash \Delta}{\Gamma[\varphi/x] \vdash \Delta[\varphi/x]} (\text{Subst})$$
- $$\frac{\Gamma, \psi \vec{y} \vdash \chi \vec{y}, \Delta}{\Gamma, \varphi[\psi/x^T] \vdash \varphi[\chi/x^T], \Delta} \vec{y} \cap FV(\Gamma, \psi, \chi, \Delta) = \emptyset, (\text{Mono})$$
- $$\frac{\Gamma, N x^{\mathbf{N}} \vdash \Delta}{\Gamma \vdash \Delta} (\text{Nat}) \quad \frac{}{\mathbf{S}s = \mathbf{Z} \vdash} (\text{P1}) \quad \frac{\Gamma, s = t \vdash \Delta}{\Gamma, \mathbf{S}s = \mathbf{S}t \vdash \Delta} (\text{P2})$$

where $N \equiv \mu X. \lambda x. (x = \mathbf{Z}) \vee (\exists x'. x = \mathbf{S}x' \wedge X x')$

Cyclic Proof

pre-proof + **global trace condition**

$$\begin{array}{c}
 \frac{\frac{\frac{}{\vdash \mathbf{Z} = \mathbf{Z} \wedge \mathbf{Z} = \mathbf{Z}}{(\wedge R, = R)}}{\vdash P(\mathbf{Z}, \mathbf{Z}, \mathbf{Z})} (\mu R)}{x = \mathbf{Z} \vdash P(x, \mathbf{Z}, x)} (= L) \\
 \frac{\frac{\frac{Nx' \vdash P(x', \mathbf{Z}, x')}{Nx' \vdash P(\mathbf{S}x', \mathbf{Z}, \mathbf{S}x')} (\mu R)}{x = \mathbf{S}x', Nx' \vdash P(x, \mathbf{Z}, x)} (= L)}{\exists x'. x = \mathbf{S}x' \wedge Nx' \vdash P(x, \mathbf{Z}, x)} (\exists L, \wedge L) \\
 \frac{(x = \mathbf{Z}) \vee (\exists x'. x = \mathbf{S}x' \wedge Nx' \vdash P(x, \mathbf{Z}, x))}{Nx \vdash P(x, \mathbf{Z}, x)} (\vee L, \mu L)
 \end{array}$$

Global trace condition

Def. Global trace condition:

For all infinite paths in the pre-proof,
there exists some left μ or right ν
which is unfolded infinitely.

$$\begin{array}{c}
 \frac{\frac{\frac{\vdash \underline{\nu}x.(x \vee \perp)}{\vdash \underline{\nu}x.(x \vee \perp), \perp} (\text{Wk})}{\vdash (\underline{\nu}x.(x \vee \perp)) \vee \perp} (\vee\text{R})}{\vdash \underline{\nu}x.(x \vee \perp)} (\nu\text{R})
 \end{array}$$

satisfies the g.t.c.

$$\begin{array}{c}
 \frac{\frac{\frac{\vdash \underline{\mu}x.(x \vee \perp)}{\vdash \underline{\mu}x.(x \vee \perp), \perp} (\text{Wk})}{\vdash (\underline{\mu}x.(x \vee \perp)) \vee \perp} (\vee\text{R})}{\vdash \underline{\mu}x.(x \vee \perp)} (\mu\text{R})
 \end{array}$$

does not satisfy the g.t.c.

Comparison to other g.t.c.

- [Brotherston&Simpson IJLP11]:
track μ, ν by tracking formulas
- [Doumane 17]:
track μ, ν by tracking formulas with priorities
derived from subformula ordering
- Ours: track μ, ν by tracking precise μ, ν .

$$\begin{array}{c}
 \boxed{
 \begin{array}{c}
 \frac{\vdash \Psi_G \Phi_F}{\vdash \Phi_F (\Psi_G \Phi_F)} (\mu R) \quad \frac{\vdash \Psi_G \Phi_F}{\vdash \Phi_F (\Psi_G \Phi_F)} (\mu R) \\
 \hline
 \vdash \Phi_F (\Psi_G \Phi_F) \wedge \Phi_F (\Psi_G \Phi_F) \\
 \hline
 \vdash (\nu G. \lambda F. FG \Phi_F \wedge FGF) \Phi_F (\nu R)
 \end{array}
 }
 \end{array}$$

where

$$\Phi_F = (\mu F. \lambda a. a)$$

$$\Psi_G = (\nu G. \lambda F. FG \Phi_F \wedge FGF)$$

Outline

- Background: $\text{HFL}_{\mathbb{N}}$ syntax & semantics
- Definition of our cyclic proof system
 - Example of cyclic proofs (from program verif.)
- Some properties
 - Soundness
 - Decidability of g.t.c.
 - Completeness of the infinitary system
- Related work
- Conclusion & Future work

Example of $\text{HFL}_{\mathbb{N}}$ formula

Higher-order program

Is f called infinitely?

```
let rec g n = if n=0 then () and g (n-1) in
let rec f h m = h m; f h (m+1) in f g 0
```

↓ [Kobayashi+ ESOP18]

$\text{HFL}_{\mathbb{N}}$ formula

$$(\nu F . \lambda h . \lambda m . h \ m \wedge F \ h \ (m + 1)) (\mu G . \lambda n . (n = 0 \vee (n \neq 0 \wedge G \ (n - 1)))) \ 0$$

Example of $\text{HFL}_{\mathbb{N}}$ formula

Higher-order program

Is f called infinitely?

```
let rec  $g\ n = \text{if } n=0 \text{ then } () \text{ and } g\ (n-1)$  in  
let rec  $f\ h\ m = h\ m; f\ h\ (m+1)$  in  $f\ g\ 0$ 
```

↓ [Kobayashi+ ESOP18]

$\text{HFL}_{\mathbb{N}}$ formula

$$(\nu F . \lambda h . \lambda m . h\ m \wedge F\ h\ (m + 1)) (\mu G . \lambda n . (n = 0 \vee (n \neq 0 \wedge G\ (n - 1)))) 0$$

Example of cyclic proof

$$\begin{array}{c}
\frac{}{\vdash 0 = 0} (=R) \quad \frac{}{n = 0 \vdash \psi_G n} (=L) \quad \frac{\frac{\frac{\mathbf{N} n' \vdash \mathbf{S} n' \neq 0}{\mathbf{N} n' \vdash \mathbf{S} n' \neq 0 \wedge \psi_G n'} (\wedge R) \quad \frac{\mathbf{N} n' \vdash \psi_G \mathbf{S} n'}{\mathbf{N} n', n = \mathbf{S} n' \vdash \psi_G n} (=L)}{\mathbf{N} n' \vdash \psi_G \mathbf{S} n'} (\mu R)}{\mathbf{N} n \vdash \psi_G n} (\text{Nat}) \quad \frac{}{\vdash \varphi_F \psi_G n} (\text{Subst}) \\
\frac{}{\vdash \psi_G n} (\wedge R) \quad \frac{\vdash \psi_G n \wedge \varphi_F \psi_G \mathbf{S} n}{\vdash \varphi_F \psi_G n} (\nu R) \quad \frac{}{\vdash \varphi_F \psi_G 0} (\text{Subst})
\end{array}$$

where $N \equiv \mu X. \lambda x. (x = \mathbf{Z}) \vee (\exists x'. x = \mathbf{S}x' \wedge X x')$

$$\varphi_F \equiv \nu F . \lambda h . \lambda m . h \ m \wedge F \ h \ (m + 1)$$
$$\psi_G \equiv \mu G . \lambda n . (n = 0 \vee (n \neq 0 \wedge G (n - 1)))$$

Outline

- Background: $\text{HFL}_{\mathbb{N}}$ syntax & semantics
- Definition of our cyclic proof system
 - Example of cyclic proofs (from program verif.)
- Some properties
 - Soundness
 - Decidability of g.t.c.
 - Completeness of the infinitary system
- Related work
- Conclusion & Future work

Soundness

Thm. If $\Gamma \vdash \Delta$ is provable then $\Gamma \models \Delta$.

Decidability of global trace condition

Thm. “Does a pre-proof satisfy g.t.c.?” is decidable.

Proof. reduction to inclusion problem of Büchi automata
(cf. [Dax+ FSTTCS06], [Brotherston&Simpson IJLP11])

- Construct:
 - Büchi automaton $\mathcal{B}$
that accepts all infinite paths
 - Büchi automaton $\mathcal{A}$
that accepts paths satisfying g.t.c. by
nondeterministically tracking left μ or right ν
- Decide $\mathcal{L}(\mathcal{B}) \subseteq \mathcal{L}(\mathcal{A})$.

Incompleteness of cyclic proof system

Prop. Our cyclic proof system is incomplete.

Proof.

- Cyclic proofs are computably enumerable
- But valid sequents of $\text{HFL}_{\mathbb{N}}$ are not.

Completeness of the infinitary system

Infinitary proof: infinite tree + g.t.c.

- Ordinary proof: finite tree
- Cyclic proof: regular infinite tree + g.t.c.

Thm. $\Gamma \vdash \Delta$: all types of free vars are $\mathbf{N}$ or $\mathbf{N}^k \rightarrow \Omega$.

If $\Gamma \models \Delta$ then $\Gamma \vdash \Delta$ is (cut-free) provable in infinitary system.

- This type restriction is enough for program verif.
- This is an extension of a theorem in [Tsukada LICS20]

Outline

- Background: $\text{HFL}_{\mathbb{N}}$ syntax & semantics
- Definition of our cyclic proof system
 - Example of cyclic proofs (from program verif.)
- Some properties
 - Soundness
 - Decidability of g.t.c.
 - Completeness of the infinitary system
- Related work
- Conclusion & Future work

Related work

- Cyclic proofs for mu-calculus with ordinals
[Sprenger&Dam, FoSSaCS03]
 - Ordinal annotations should be checked
- Cyclic proofs for first-order logic with inductive def.
[Brotherston&Simpson, IJLP11]
 - Include restricted alternation of fixed-points
- Cyclic proofs for linear-time mu-calculus
[Doumane, 17]
 - Include alternation of fixed-points

Conclusion & Future work

- Proposed a cyclic proof system for $\text{HFL}_{\mathbb{N}}$.
- Proved soundness, decidability of g.t.c., and certain completeness for infinitary system.

Future work

- develop a semi-automated tool
- prove Henkin completeness
- (dis)prove cut elimination