The undecidability of PCF_2 in synthetic computability

Second Bachelor seminar talk

Fabian Brenner
Advisors: Yannick Forster, Dominik Kirst
Supervisor: Prof. Gert Smolka

June 6, 2024

Programming Systems Lab
Saarland University

A long-standing open problem

Recap: PCF, PCF_2

- PCF: simply typed λ-calculus with $\mathbb{N}$ and recursion
- PCF_2: simply typed λ-calculus with $\mathbb{B}$ and `if`

Full abstraction problem of PCF

Is there a fully abstract model of PCF that is concrete and independent of syntax?

Necessary criterion

If a fully abstract model exists, then contextual equivalence of PCF_2 is decidable.

Theorem (Loader 2000)

Contextual equivalence of PCF_2 *is undecidable.*

PCF_2 and contextual equivalence

Definition (PCF_2)

Extension of simply typed λ-calculus

$$T_1, T_2 := \mathbb{B} \mid T_1 \to T_2$$

$$s, t, u := \lambda x.\ s \mid s\ t \mid x \mid \mathtt{true} \mid \mathtt{false} \mid \bot \mid \mathtt{if}\ s\ \mathtt{then}\ t\ \mathtt{else}\ u$$

Operational semantics

$$\mathtt{if}\ \mathtt{true}\ \mathtt{then}\ t\ \mathtt{else}\ u \quad \succ \quad t,$$

$$\mathtt{if}\ \bot\ \mathtt{then}\ t\ \mathtt{else}\ u \quad \succ \quad \bot \quad \mid \quad \dots$$

Definition (Contextual equivalence)

Two terms $\Gamma \vdash s, t \colon A$ are **contextually equivalent** $\Gamma \vdash s \equiv_c t : A$ iff for all contexts $C \colon (\Gamma, A) \rightsquigarrow (\emptyset, \mathtt{Bool})$ and values v we have that $C[s] \Downarrow v \longleftrightarrow C[t] \Downarrow v$

Proof of Loader's theorem

Theorem (Loader 2000)

Contextual equivalence of PCF_2 *is undecidable.*

$\leq_m$: many-one reducible

SR: Word problem for string rewriting systems

CE: Contextual equivalence on PCF_2

$$\mathrm{SR} \leq_m \mathrm{SATIS} \leq_m \mathrm{CIE\text{-}SYS} \leq_m \mathrm{CE\text{-}RES\text{-}SYS} \leq_m \mathrm{CE}$$

For finite alphabet Σ, finite set of rewriting rules R, define:

$$\frac{(C,\ C') \in R}{D_1 C D_2 \Rightarrow_R D_1 C' D_2} \qquad \frac{}{W \Rightarrow_R^* W} \qquad \frac{X \Rightarrow_R^* Y \quad Y \Rightarrow_R Z}{X \Rightarrow_R^* Z}$$

Observational preorder

$$\begin{tikzcd} \texttt{true} & & \texttt{false} \\ & \bot \arrow[ul] \arrow[ur] & \end{tikzcd}$$

Obervational preorder (on $\mathbb{B}$)

- $s \leq t$ iff $s = \bot$ or $s = t$ for $s, t \in \{\texttt{true}, \texttt{false}\}$
- $\Gamma \vdash s \leq t$ iff $\Gamma \vdash s, t \colon \mathbb{B}$ and for all substitutions σ of closed terms for free variables in s, t the normal forms of $\sigma\ s$ and $\sigma\ t$ are in relation

Encoding of words

$$T\ W := \underbrace{\mathbb{B} \to \cdots \to \mathbb{B}}_{2|W|+2} \to \mathbb{B}$$

Definition (Word encoding)

Let $v \in \{\texttt{true},\ \texttt{false}\}$. Enc is a v-encoding iff for all words W: $\emptyset \vdash Enc\ W : T\ W$ and $Enc\ W$ only returns $\perp$ or v.

Example

- $\texttt{Const}_v W\ x_1 \ldots x_{2|W|}\ i\ j = v$
- Let $W = w_1 \ldots w_n$.

  $$\texttt{Word}_v W\ x_1\ x_2 \ldots x_{2|W|-1}\ x_{2|W|}\ i\ j = \begin{cases} v & \forall n.\ x_{2n-1} = x_{2n} = w_n \\ \perp & \text{otherwise} \end{cases}$$

Encoding of rules

Definition (Rule encoding)

F encodes rule $(C,\ C')$ w.r.t. Enc iff $\emptyset \vdash F\colon T\ C\ \rightarrow\ T\ C'$, it is $\leq$-minimal s.t. for all $W = D_1 C D_2,\ W' = D_1 C' D_2$ and $\Gamma := x_n, y'_n, z_n, i', j' \colon \mathbb{B}$ we have

$$\Gamma \vdash F(\lambda y_1 \ldots y_{2|C|} ij.Enc\ W\ x_1 \ldots x_{2|D_1|} y_1 \ldots y_{2|C|} z_1 \ldots z_{2|D_2|} ij) y'_1 \ldots y'_{2|C'|} i'j'$$
$$\geq Enc\ W' x_1 \ldots x_{2|D_1|} y'_1 \ldots y'_{2|C'|} z_1 \ldots z_{2|D_2|} i'j'$$

- F simulates behavior of $Enc\ W'$ with less information provided by arguments

Example

For the rule $(C,\ C')$ and the $\texttt{Word}_v$ encoding, we have

$$F\ f\ y'_1 \ldots y'_{2|C'|} i'j' = \begin{cases} v & \forall n\colon y'_{2n-1} = y'_{2n} = c'_n \quad \wedge \quad f\ c_1 c_1 \ldots c_{|C|} c_{|C|} \bot\bot = v \\ \bot & \text{otherwise} \end{cases}$$

Reduction from string rewriting

- $\mathsf{SR}(R, W_0, W) := W_0 \Rightarrow_R^* W$
- Choose $\mathcal{E}$ as set of Loader's 32 mostly technical word enodings.
- $\mathsf{SATIS}(R, W_0, W) := \exists t.\ w_0, r_1, \ldots, r_{|R|}, x_1, \ldots, x_{2|W|+2} \vdash t : \mathbb{B} \quad \wedge$
  $\forall Enc \in \mathcal{E}.\ t$ satisfies W w.r.t. Enc, W_0, R

$$\mathsf{SR} \leq_m \mathsf{SATIS}$$

Reduction function is identity function.

Satisfiability of words

Recap (SATIS)

$$\mathrm{SATIS}(R, W_0, W) := \exists t.\ w_0, r_1, \ldots, r_{|R|}, x_1, \ldots, x_{2|W|+2} \vdash t : \mathbb{B} \quad \wedge$$
$$\forall Enc \in \mathcal{E}.\ t \text{ satisfies } W \text{ w.r.t. } Enc, W_0, R$$

We write $R = R_1, \ldots, R_N = (C_1,\ C_1'), \ldots, (C_N,\ C_N')$

Definition

We say t **satisfies** W with respect to Enc, W_0, R iff
t is a normal term with $w_0 : T\ W_0,\quad r_i : T\ C_i \to\ T\ C_i',\quad x_i : \mathbb{B} \vdash t : \mathbb{B}$ such that

$$t[Enc\ W_0,\ F_{R_1}, \ldots, F_{R_N},\ x_1, \ldots, x_{2|W|+2}] \geq Enc\ W\ x_1 \ldots x_{2|W|+2}$$

Construction of satisfying terms - example

Recap (Satisfiability)

t satisfies W: $t[Enc\ W_0,\ F_{R_1}, \ldots, F_{R_N},\ x_1, \ldots, x_{2|W|+2}] \geq Enc\ W\ x_1 \ldots x_{2|W|+2}$

Consider $W_0 = AA,\ A \Rightarrow_{R_1} BB,\ B \Rightarrow_{R_2} A$.

$$
\begin{array}{ll}
AA: & Enc\ W_0 x_1 x_2 x_3 x_4 ij \ \geq\ Enc\ W_0 x_1 x_2 x_3 x_4 ij \\
\Downarrow_{R_1} & \\
ABB: & F_{R_1}(\lambda y_1 y_2 ij.\color{blue}{Enc\ W_0 x_1 x_2 y_1 y_2 ij})y'_1 y'_2 y'_3 y'_4 i' j' \ \geq\ Enc\ ABB\ x_1 x_2 y'_1 y'_2 y'_3 y'_4 i' j' \\
\Downarrow_{R_2} & \\
AAB: & F_{R_2}(\lambda y_1 y_2 ij.\color{blue}{F(R_1)(\lambda \tilde{y}_1 \tilde{y}_2 kl.Enc\ W_0 x_1 x_2 \tilde{y}_1 \tilde{y}_2 kl) y_1 y_2 z_1 z_2 ij})y'_1 y'_2 i' j' \\
 & \geq\ Enc\ AAB\ x_1 x_2 x_1 x_2 y'_1 y'_2 z_1 z_2 i' j'
\end{array}
$$

Correctness proof of reduction - Forward direction

Theorem (Forward direction)

If $W_0 \Rightarrow_R^* W$, *then* $\mathrm{SATIS}(R, W_0, W)$.

- Construct t by induction on derivation of W as in previous example
- No properties of $\mathcal{E}$ needed, any set of encodings would work

Correctness proof of reduction - Backwards direction

Theorem (Backwards direction)

If SATIS (R, W_0, W), *then* $W_0 \Rightarrow_R^* W$.

- A priori, we do not know which form t has
- We need to derive a term t' satisfying W of useful form
- Intricate technical arguments necessary
- Makes use of specifc enodings in $\mathcal{E}$

Current state and outlook

Reduction chain in Loader's proof

$$\text{SR} \leq_m \text{SATIS} \leq_m \text{CIE-RES-SYS} \leq_m \text{CE-SYS} \leq_m \text{CE}$$

- Formalised PCF_2, observational and contextual equivalence in Coq
- Understood orange, blue and green reductions, formalised green reduction in Coq
- Understood forward direction and high-level reasoning in backwards direction of violet reduction
- Formalising forward direction of violet reduction
- Formalise remaining reductions in Coq
- Deepen understanding of syntactical arguments in backwards direction of violet reduction
- Formalising definitions necessary for backwards direction

Goals and key take-aways

Recap of Loader's result

- Solved important problem
- Technical and intricate proof
- Original paper known to be intransparent, provides no examples and barely any intuition

Goals of this project

- Clarification of reduction from string rewriting
- Formalising parts of a synthetic version of Loader's result and possibly contributing to Coq Library of Undecidable Problems [CLUP]
- Developing presentation of Loader's proof containing insightful examples and providing better intuition than original paper as base for future projects

References 1

- [Plotkin 1977] G.D. Plotkin, LCF considered as a programming language, Theoretical Computer Science, Volume 5, Issue 3, 1977, Pages 223-255, ISSN 0304-3975, https://doi.org/10.1016/0304-3975(77)90044-5.
- [Scott 1993] Dana S. Scott, A type-theoretical alternative to ISWIM, CUCH, OWHY, Theoretical Computer Science, Volume 121, Issues 1–2, 1993, Pages 411-440, ISSN 0304-3975, https://doi.org/10.1016/0304-3975(93)90095-B.
- [Higher-Order Computability: Longley, Normann] John Longlay, Dag Normann, Higher-Order-Computability, Chapter 7, Theorem 7.5.22, 2015, Page 342, ISSN 2190-619X

References 2

- [Loader 2000] Ralph Loader, Finitary PCF is not decidable, Theoretical Computer Science, Volume 266, Issues 1–2, 2001, Pages 341-364, ISSN 0304-3975, https://doi.org/10.1016/S0304-3975(00)00194-8.
- [CLUP] Yannick Forster, Dominique Larchey-Wendling, Andrej Dudenhefner, Edith Heiter, Dominik Kirst, et al..
  A Coq Library of Undecidable Problems, CoqPL 2020 The Sixth International Workshop on Coq for Programming Languages, Jan 2020, New Orleans, United States. ⟨10.1017/S0960129597002302⟩. ⟨hal-02944217⟩

Decidability problems in Loader's proof

Definition

- $\mathrm{SR}(R, W_0, W) := W_0 \Rightarrow_R^* W$
- $\mathrm{SATIS}(R, W_0, W) := \exists t.\ w_0,\ r_1, \ldots, r_{|R|},\ x_1, \ldots, x_{2|W|+2} \vdash t : \mathbb{B} \quad \wedge$
  $\forall Enc \in \mathcal{E}.\ t$ satisfies W w.r.t. Enc, W_0, R
- CIE-SYS: Contains lists of pairs of PCF terms, such that $s_i, t_i : \mathcal{B}$ and $s_i \leq t_i$.
- CE-SYS: Contains lists of pairs of PCF terms, such that $s_i : \mathcal{B}$, $b_i \in \{\mathtt{true}, \mathtt{false}\}$ and $s_i \simeq b_i$.
- CE: Contains pairs of PCF terms s, t, such that they are contextually equivalent.

Observational preorder - formal definition

Definition (Observational preorder)

- $s \leq t$ iff $s = \bot$ or $s = t$ for $s, t \in \{\texttt{true}, \texttt{false}\}$
- $\leq$ is extended to closed terms of type $\mathbb{B}$ by comparing normal forms
- For $\emptyset \vdash s, t \colon A \to B$: $f \leq g$ iff for all closed s, t of type A we have $f\ s \leq g\ t$
- For $\Gamma \vdash s, t \colon A$: $s \leq t$ iff this is the case for all substitutions of closed terms for the free variables in s, t

Proof sketch of forward direction

Proof.

Induction on derivation of W.

- $W = W_0$
  - $t := Enc\ W_0\ w_1 \dots w_{2|W_0|} ij$
  - Satisfies W_0 by reflexivity
- Assume $W = D_1 C D_2$ derivable, $D_1 C D_2 \Rightarrow_R D_1 C' D_2$
  - By IH, exists t satisfying W, define t' as:

$$t' := F_{(C,C'),Enc}$$
$$(\lambda y_1 \dots y_{2|C|} ij.t[x_1, \dots, x_{2|D_1|}, y_1, \dots, y_{2|C|}, z_1, \dots, z_{2|D_2|}, i, j]) y'_1 \dots y'_{2|C'|} i' j'$$

  - As t satisfies W:
    $t[x_1, \dots, x_{2|D_1|}, y_1, \dots, y_{2|C|}, z_1, \dots, z_{2|D_2|}, i, j] \geq$
    $Enc\ W\ x_1 \dots x_{2|D_1|} y_1 \dots y_{2|C|} z_1 \dots z_{2|D_2|} ij$
  - Claim follows now by definition of rule encodings

Preliminaries for backwards direction

Lemma

If t satisfies W, then there exists t' with all the following reductions applied satisfying W.

- Spine reduction
- Rib reduction
- Chain reduction

Proof sketch of backwards direction

Assume that t satisfies word with all the previous reductions applied.

- t has either the form $\mathit{Enc}\ W_0\ a_1 \dots a_{2|W_0|} ij$ or $F_{(C,C')}(\lambda y_1 \dots y_{2|C|} ij.s) a_1 \dots a_2 |C'| i'j'$ (because of the reductions and technical lemmas)
- $t = \mathit{Enc}\ W_0\ a_1 \dots a_{2|W_0|} ij$:
  Implies that $W = W_0$ (clearly derivable)
- $t = F_{(C,C')}(\lambda y_1 \dots y_{2|C|} ij.s) a_1 \dots a_{2|C'|} i'j'$ we can deduce that rule (C, C') has been applied and s satisfies $W = D_1 C D_2$, then claim follows by IH

Spine reduction

Definition (Spinal sub-terms)

- s is spinal sub-term of itself
- Spinal sub-terms of s are also spinal sub-terms of $R_i(\lambda\bar{y}.s)\bar{a}$

Definition

- The **coccyx** is the unique spinal sub-term not of the form $R_i(\lambda\bar{y}.s)\bar{a}$
- A term has reduced spine if its coccyx has form $W_0\bar{a}$

Rib reduction

Let t have reduced spine.

Definition (Rib sub-terms)

- If $t = W_0\ a_1 \ldots a_k$, its rib sub-terms are $\{a_1, \ldots, a_k\}$
- If $t = R_i\ (\lambda \bar{y}.s)a_1 \ldots a_k$, then the set of its rib sub-terms is then union of $\{a_1, \ldots, a_k\}$ with the set of rib sub-terms of s

Definition (Reduced ribs)

A term t with reduced spine has reduced ribs if W_0, R_i have no occurences in the rib sub-terms of t.

Rib sanity

Definition (Classification)

Consider terms of the form $W_0 \; a_1 \ldots a_{2l+2}$ and $R_i(\lambda y_1 \ldots y_{2k+2}.b)a_1 \ldots a_{2k+2}$

- a_{2i-1} are odd sub-terms
- a_{2i} are even sub-terms
- $a_1 \ldots a_{2l}$ are positional sub-terms
- a_{2i+1}, a_{2i+2} are control sub-terms

Variables are classified in the same way.

Chain reduction and Linearity

Definition (Chain reduction)

A term t is chain reduced iff for each spinal sub-term in the form $R_i(\lambda \bar{y} ij.f\,\bar{b}\alpha\beta)\bar{a}$, we have that $\beta = j$.

Lemma (Linearity)

If $t[W_0, \bar{R}, x_1, \ldots, x_{2n+2}]$ satisfies W and has all the previous reductions applied, then each x_i occurs exactly once in t.