The Undecidability of Contextual Equivalence of PCF_2 – Towards a Mechanisation in Coq

Final Bachelor talks

Fabian Brenner

Advisors: Yannick Forster, Dominik Kirst

Supervisor: Prof. Gert Smolka

August 23, 2024

Programming Systems Lab
Saarland University

Programming Computable Functions and full abstraction

- Programming Computable Functions (PCF): simply typed λ-calculus with $\mathbb{N}$ and recursion

Full abstraction problem for PCF

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

- Such a model would permit to decide contextual equivalence of finitary fragments of PCF.
- Is contextual equivalence of finitary fragments of PCF decidable? (Jung, Stoughton, 1993)

Loader's result

Theorem (Loader, 2000)

Contextual equivalence of PCF_2 is undecidable.

- Negative answer to full abstraction problem
- Surprising result: In related calculi, contextual equivalence decidable
- Proof well-known to be difficult and intransparent:
  "the proof is long and technical, and consists of intricate syntactic arguments"
  (Longley, Normann, 2015)

Synthetic Undecidability in Coq

- Introduced by Forster, Kirst, and Smolka in 2019
- Undecidability defined relative to Halting problem for Turing machines

Lemma

- *Halting problem for Turing machines is undecidable*
- *If $P \leq_m Q$ and P is undecidable, Q is undecidable*

Definition (Many-one reductions)

For predicates $P : X \to \mathbb{P}$, $Q : Y \to \mathbb{P}$:

$P \leq_m Q$ iff $\exists f : X \to Y.\ \forall x.\ P\ x \leftrightarrow Q\ (f\ x)$ ~~$\wedge$ f is computable~~

- Independent of concrete model of computation
- Our work is based on Coq Library of Undecidability Proofs (Forster et al., 2020)

PCF_2 and contextual equivalence

Definition (PCF_2)

Extension of simply typed λ-calculus

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

$$s, t, u \colon \mathrm{tm} ::= \lambda x.s \mid s\ t \mid x \mid \texttt{if}\ s\ \texttt{then}\ t\ \texttt{else}\ u \mid \mathsf{true} \mid \mathsf{false} \mid \bot$$

Operational semantics

$$\texttt{if true then}\ t\ \texttt{else}\ u \quad \succ \quad t \quad \mid$$

$$\texttt{if}\ \bot\ \texttt{then}\ t\ \texttt{else}\ u \quad \succ \quad \bot \quad \mid \quad \ldots$$

Definition (Contextual equivalence)

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

Observational preorder

- For closed boolean terms, $\leq_b$ is defined by

$$s \leq_b t \;:=\; s \Downarrow \bot \;\vee\; (\exists v.\ v \in [\text{true}, \text{false}, \bot] \;\wedge\; s \Downarrow v \;\wedge\; t \Downarrow v).$$

- Inductively lifted to arbitrary closed well-typed terms:

$$\begin{aligned} s \leq_c t \colon \mathbb{B} \;&:=\; s \leq_b t \\ s \leq_c t \colon A \to B \;&:=\; \text{for all } a, b \text{ with } \emptyset \vdash a\colon\ A,\ \emptyset \vdash b\colon\ A \text{ and } a \leq_c b\colon A, \\ &\qquad \text{it holds that } s\ a \leq_c t\ b\colon B. \end{aligned}$$

- Lifted to arbitrarily typed terms:

$$\begin{aligned} \Gamma \vdash s \leq_o t\colon A \;&:=\; \Gamma \vdash s,\ t\colon\ A \text{ and for all substitutions } \sigma \text{ of closed terms for} \\ &\qquad \text{free variables in } s, t,\ \text{it holds that } s[\sigma] \leq_c t[\sigma]\colon A \end{aligned}$$

Observational equivalence

Definition (Observational Equivalence)

$$\Gamma \vdash s \equiv_o t : A \quad := \quad \Gamma \vdash s \leq_o t : A \ \wedge \ \Gamma \vdash t \leq_o s : A$$

- Agrees with contextual equivalence
- Proof involves two unmechanised result about PCF_2:

Lemma

- *Church-Rosser property holds for PCF_2*
- *Boolean normal forms are computable for PCF_2*

Proof of Loader's theorem

Theorem (Loader 2000)

Contextual equivalence (CE) of PCF_2 is undecidable.

$\mathrm{CE}(s, t, A) \quad := \quad \emptyset \vdash s \equiv_c t : A$

SR: String rewriting

$$\overline{\mathrm{SR}} \leq_m \overline{\mathrm{SATIS}} \leq_m \overline{\mathrm{PS}} \leq_m \overline{\mathrm{RPS}} \leq_m \mathrm{CE}$$

Actual reductions proven:

$$\mathrm{SR} \leq_m \mathrm{SATIS} \leq_m \mathrm{PS} \leq_m \mathrm{RPS} \qquad \overline{\mathrm{RPS}} \leq_m \mathrm{CE}$$

- Main difficulty lies in first reduction

String Rewriting (SR)

- Decision problem going back to Thue
- Mechanised in Coq by Forster, Heiter, and Smolka
- Finite alphabet of symbols Σ, finitely many rewriting rules $R\colon \mathcal{L}(\mathcal{L}(\Sigma) \times \mathcal{L}(\Sigma))$

$$\frac{(e,\ f) \in R}{d_1 e d_2 \ \Rightarrow_R \ d_1 f d_2}\ , \qquad \frac{}{a \ \Rightarrow_R^* \ a}\ , \qquad \frac{a \ \Rightarrow_R^* \ b \quad b \ \Rightarrow_R \ c}{a \ \Rightarrow_R^* \ c}\ .$$

Reachability problem: $\mathrm{SR}_R(a\colon \mathcal{L}(\Sigma), b\colon \mathcal{L}(\Sigma)) \ := \ a \ \Rightarrow_R^* \ b$

Lemma (Davis)

There exist rewriting rules R such that the following problem is undecidable:

$$\mathrm{SR}(a\colon \mathcal{L}(\mathcal{B}), b\colon \mathcal{L}(\mathcal{B})) \ := \ \mathrm{SR}_R(a, b).$$

Encoding of words

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

Definition (Word encoding)

Let $v \in [\text{true}, \text{false}]$. $Enc\colon \mathcal{L}(\mathcal{B}) \to \text{tm}$ is a v-encoding iff for all words a, it holds that $\emptyset \vdash Enc(a)\colon\ T(a)$ and $Enc(a)$ only returns $\perp$ or v.

Example

- $\texttt{Const}_v(a)\ s_1 \ldots s_{2|a|}\ i\ j = v$
- Let $a = a_1 \ldots a_n$.

  $$\texttt{Word}_v(a)\ s_1\ s_1' \ldots s_{|a|}\ s_{2|a|}'\ i\ j = \begin{cases} v & \forall k.\ s_k \Downarrow a_k \ \wedge\ s_k' \Downarrow a_k \\ \perp & \text{otherwise} \end{cases}$$

Encoding of rules

Term F encodes rule (e, f) with respect to v-encoding Enc:

- $\emptyset \vdash F: \ T(e) \to T(f)$
- For all words d_1, d_2, F simulates behavior of $Enc(d_1 f d_2)$ with only knowing arguments representing f and behaviour of $Enc(d_1 e d_2)$

Example

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

$$F \ g \ s_1 \ s'_1 \ldots s_{|f|} \ s'_{2|f|} i \ j = \begin{cases} v & \forall k. \ s_k \Downarrow f_k \ \wedge \ s'_k \Downarrow f_k \ \wedge \ g \ e_1 e_1 \ldots e_{|e|} e_{|e|} \bot \bot \Downarrow v \\ \bot & \text{otherwise} \end{cases}$$

Equivalence between SR and SATIS

Recap (SR)

$$\mathrm{SR}(a, b) \;:=\; a \;\Rightarrow^*_R\; b$$

- Choose $\mathcal{E}$ as set of Loader's 32 mostly technical word enodings.

Definition (SATIS)

$$\begin{aligned}\mathrm{SATIS}(a, b) \;:=\; & \exists t.\; w_0, r_1, \ldots, r_{|R|}, x_1, \ldots, x_{2|b|+2} \vdash t : \mathbb{B} \quad \wedge \\ & \forall Enc \in \mathcal{E}.\; t \text{ satisfies } b \text{ w.r.t. } Enc,\; a,\; \text{and } R\end{aligned}$$

Theorem (Equivalence between SR and SATIS)

$$\forall a\; b.\; \mathrm{SR}(a, b) \;\leftrightarrow\; \mathrm{SATIS}(a, b)$$

- Induces a reduction SR $\leq_m$ SATIS

Satisfiability of words

Recap (SATIS)

$$\begin{aligned}\mathrm{SATIS}(a, b) \;:=\; & \exists t.\; w_0, r_1, \ldots, r_{|R|}, x_1, \ldots, x_{2|b|+2} \vdash t : \mathbb{B} \quad \wedge \\ & \forall Enc \in \mathcal{E}.\; t \text{ satisfies } b \text{ w.r.t. } Enc,\; a,\; \text{and } R\end{aligned}$$

Let $R = [(e_1,\ f_1), \ldots, (e_N,\ f_N)]$.

Definition (Satisfies)

It is said t **satisfies** b with respect to $Enc, a,$ and R iff
t is a normal term with $w_0 : T(a),\ r_k : T(e_k) \to\ T(f_k),\ \ x_l : \mathbb{B} \vdash t : \mathbb{B}$ such that

$$x_1, \ldots, x_{2|b|+2} \vdash t[Enc(a),\ F_1, \ldots, F_N,\ x_1, \ldots, x_{2|b|+2}] \geq_o Enc(b)\, x_1 \ldots x_{2|b|+2} : \mathbb{B}$$

where F_k is any rule encoding of of $(e_k,\ f_k)$.

Correctness proof of reduction - Forward direction

Theorem (Forward direction)

If SR(a, b)*, then* SATIS(a, b)*.*

- Around half a page in Loader's paper
- Construct t by induction on derivation of b
- No properties of $\mathcal{E}$ needed, any set of encodings would work

Correctness proof of reduction - Backward direction

Theorem (Backward direction)

If $\mathrm{SATIS}(a, b)$, *then* $\mathrm{SR}(a, b)$.

- Around 13 pages in Loader's paper
- A priori, one does not know which form t has
- If t is in the form of terms constructed in the forward direction, proof is fairly straightforward
- Intricate technical arguments necessary to manipulate the structure of t (5 structural simplifications)
- Makes use of specifc enodings in $\mathcal{E}$

Contributions

$$\overline{\mathsf{SR}} \leq_m \overline{\mathsf{SATIS}} \leq_m \overline{\mathsf{PS}} \leq_m \overline{\mathsf{RPS}} \leq_m \mathsf{CE}$$

- Turned Loader's proof into a reduction chain
- Mechanised PCF_2 as well as observational and contextual equivalence in Coq
- Mechanised all but first reduction in Coq
- Presented remaning reduction on paper, with several nontrivial details Loader left out, serving as basis for future mechanisations
- Provided insightful examples and technical observations

Remark: Attempted to mechanise forward direction of equivalence between SR and SATIS in Coq (unfinished due to lack of time)

Future Work

Fill gaps in mechanisation:

- Show remaning results about PCF_2 (Church-Rosser property, computability of boolean normal forms)
- Show existence of rule encodings
- Complete mechanisation of equivalence between SR and SATIS

Connect this work to Coq Library of Undecidability Proofs: Mechanise undecidability of SR for some fixed rewriting rules

References i

Coq Mechanisation

- Preliminaries: $\sim$ 150 loc
- Results about PCF_2: $\sim$ 700 loc
- Observational and contextual equivalence: $\sim$ 700 loc
- Definition of decision problems: $\sim$ 100 loc
- Undecidability result: $\sim$ 50 loc

$$\text{SR} \leq_m \text{SATIS} \leq_m \text{RPS} \leq_m \text{RPS} \leq_m \text{CE}$$

- Orange reduction: $\sim$ 700 loc
- Blue reduction: $\sim$ 100 loc
- Green reduction: $\sim$ 200 loc

Overall: $\sim$ 500 loc specification, $\sim$ 2200 loc proofs

(Unfinished forward direction of remaing reduction: additional $\sim$ 300 loc)

Encoding of rules

Definition (Rule encoding)

Term F encodes rule (e, f) w.r.t. Enc iff $\emptyset \vdash F : \ T(e) \to T(f)$, it is $\leq_o$-minimal s.t. for all $a = d_1 e d_2$, and $b = d_1 f d_2$, it holds that

$$\Gamma \vdash F(\lambda y_1 \ldots y_{2|e|} i\ j. Enc(a)\ x_1 \ldots x_{2|d_1|} y_1 \ldots y_{2|e|} z_1 \ldots z_{2|d_2|} i\ j) y'_1 \ldots y'_{2|f|} i'\ j'$$
$$\geq_o Enc(b) x_1 \ldots x_{2|d_1|} y'_1 \ldots y'_{2|f|} z_1 \ldots z_{2|d_2|} i'\ j'$$

with $\Gamma \ := \ x_1, \ldots, x_{2|d_1|},\ y'_1, \ldots, y'_{2|f|},\ z_1, \ldots, z_{2|d_2|},\ i',\ j'$

- F simulates behavior of $Enc(b)$ with less information provided by arguments

Example

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

$$F\ g\ s_1\ s'_1 \ldots s_{|f|}\ s'_{2|f|} i\ j = \begin{cases} v & \forall k.\ s_k \Downarrow f_k \ \wedge \ s'_k \Downarrow f_k \ \wedge \ g\ e_1 e_1 \ldots e_{|e|} e_{|e|} \bot \bot \Downarrow v \\ \bot & \text{otherwise} \end{cases}$$