Relational Reasoning
(Relationel ræsonnement)

Mathias Pedersen, 201808137

Bachelor Report (15 ECTS) in Computer Science
Advisor: Amin Timany
Department of Computer Science, Aarhus University
October 2021

AARHUS UNIVERSITY
DEPARTMENT OF COMPUTER SCIENCE

Abstract

►in English. . . ◄

Mathias Pedersen,
Aarhus, October 2021.

Contents

Chapter 1

Introduction

►motivate and explain the problem to be addressed◄

►example of a citation: [1]◄ ►get your bibtex entries from `https://dblp.org/`◄

Chapter 2

Definition of Language

►create draft◄

Syntax

$$
\begin{aligned}
e ::= {} & () \mid && \text{(unit value)}\\
& x \mid && \text{(variables)}\\
& \overline{n} \mid e+e \mid e-e \mid e \leq e \mid e < e \mid e = e \mid && \text{(integers)}\\
& \mathsf{true} \mid \mathsf{false} \mid \mathsf{if}\ e\ \mathsf{then}\ e\ \mathsf{else}\ e \mid && \text{(booleans)}\\
& (e,e) \mid \mathsf{fst}\ e \mid \mathsf{snd}\ e \mid && \text{(products)}\\
& \mathsf{inj}_1\ e \mid \mathsf{inj}_2\ e \mid \mathsf{match}\ e\ \mathsf{with}\ \mathsf{inj}_1\ x \Rightarrow e \mid \mathsf{inj}_2\ x \Rightarrow e\ \mathsf{end} \mid && \text{(sums)}\\
& \mathsf{rec}\ f(x) := e \mid e\ e && \text{(recursive functions)}\\
& \Lambda\, e \mid e\ \_ && \text{(polymorphism)}
\end{aligned}
$$

$$
v ::= () \mid \overline{n} \mid \mathsf{true} \mid \mathsf{false} \mid (v,v) \mid \mathsf{inj}_1\ v \mid \mathsf{inj}_2\ v \mid \mathsf{rec}\ f(x) := e \mid \Lambda\, e \qquad \text{(values)}
$$

$$
\tau ::= \mathsf{Unit} \mid \mathbb{Z} \mid \mathbb{B} \mid \tau \times \tau \mid \tau + \tau \mid \tau \to \tau \mid \forall X.\ \tau \qquad \text{(types)}
$$

$$
\begin{aligned}
K ::= {} & [] \mid K+e \mid v+K \mid K-e \mid v-K \mid K \leq e \mid v \leq K \mid K < e \mid v < K \mid && \text{(evaluation context)}\\
& K = e \mid v = K \mid \mathsf{if}\ K\ \mathsf{then}\ e\ \mathsf{else}\ e \mid (K,e) \mid (v,K) \mid \mathsf{fst}\ K \mid \mathsf{snd}\ K \mid\\
& \mathsf{inj}_1\ K \mid \mathsf{inj}_2\ K \mid \mathsf{match}\ K\ \mathsf{with}\ \mathsf{inj}_1\ x \Rightarrow e \mid \mathsf{inj}_2\ x \Rightarrow e\ \mathsf{end} \mid K\ e \mid v\ K \mid K\ \_
\end{aligned}
$$

Typing rules

$$\textsc{T-Var}\ \frac{(x:\tau)\in\Gamma}{\Xi \mid \Gamma \vdash x:\tau} \qquad \textsc{T-Unit}\ \frac{}{\Xi \mid \Gamma \vdash ():\mathsf{Unit}} \qquad \textsc{T-Int}\ \frac{}{\Xi \mid \Gamma \vdash \overline{n}:\mathbb{Z}}$$

$$\textsc{T-Add}\ \frac{\Xi \mid \Gamma \vdash e_1:\mathbb{Z} \qquad \Xi \mid \Gamma \vdash e_2:\mathbb{Z}}{\Xi \mid \Gamma \vdash e_1+e_2:\mathbb{Z}} \qquad \textsc{T-Sub}\ \frac{\Xi \mid \Gamma \vdash e_1:\mathbb{Z} \qquad \Xi \mid \Gamma \vdash e_2:\mathbb{Z}}{\Xi \mid \Gamma \vdash e_1-e_2:\mathbb{Z}}$$

$$\textsc{T-Le}\ \frac{\Xi \mid \Gamma \vdash e_1:\mathbb{Z} \qquad \Xi \mid \Gamma \vdash e_2:\mathbb{Z}}{\Xi \mid \Gamma \vdash e_1\leq e_2:\mathbb{B}} \qquad \textsc{T-Lt}\ \frac{\Xi \mid \Gamma \vdash e_1:\mathbb{Z} \qquad \Xi \mid \Gamma \vdash e_2:\mathbb{Z}}{\Xi \mid \Gamma \vdash e_1< e_2:\mathbb{B}}$$

$$\textsc{T-Eq}\ \frac{\Xi \mid \Gamma \vdash e_1:\mathbb{Z} \qquad \Xi \mid \Gamma \vdash e_2:\mathbb{Z}}{\Xi \mid \Gamma \vdash e_1= e_2:\mathbb{B}} \qquad \textsc{T-True}\ \frac{}{\Xi \mid \Gamma \vdash \mathsf{true}:\mathbb{B}} \qquad \textsc{T-False}\ \frac{}{\Xi \mid \Gamma \vdash \mathsf{false}:\mathbb{B}}$$

$$\textsc{T-If}\ \frac{\Xi \mid \Gamma \vdash e_1:\mathbb{B} \qquad \Xi \mid \Gamma \vdash e_2:\tau \qquad \Xi \mid \Gamma \vdash e_3:\tau}{\Xi \mid \Gamma \vdash \mathsf{if}\ e_1\ \mathsf{then}\ e_2\ \mathsf{else}\ e_3:\tau}$$

$$\textsc{T-Pair}\ \frac{\Xi \mid \Gamma \vdash e_1:\tau_1 \qquad \Xi \mid \Gamma \vdash e_2:\tau_2}{\Xi \mid \Gamma \vdash (e_1,e_2):\tau_1\times\tau_1} \qquad \textsc{T-Fst}\ \frac{\Xi \mid \Gamma \vdash e:\tau_1\times\tau_2}{\Xi \mid \Gamma \vdash \mathsf{fst}\ e:\tau_1} \qquad \textsc{T-Snd}\ \frac{\Xi \mid \Gamma \vdash e:\tau_1\times\tau_2}{\Xi \mid \Gamma \vdash \mathsf{snd}\ e:\tau_2}$$

$$\textsc{T-Inj1}\ \frac{\Xi \mid \Gamma \vdash e:\tau_1}{\Xi \mid \Gamma \vdash \mathsf{inj}_1\ e:\tau_1+\tau_2} \qquad \textsc{T-Inj2}\ \frac{\Xi \mid \Gamma \vdash e:\tau_2}{\Xi \mid \Gamma \vdash \mathsf{inj}_2\ e:\tau_1+\tau_2}$$

$$\textsc{T-Match}\ \frac{\Xi \mid \Gamma \vdash e_1:\tau_1+\tau_2 \qquad \Xi \mid \Gamma,x:\tau_1 \vdash e_2:\tau \qquad \Xi \mid \Gamma,x:\tau_2 \vdash e_3:\tau}{\Xi \mid \Gamma \vdash \mathsf{match}\ e_1\ \mathsf{with}\ \mathsf{inj}_1\ x\Rightarrow e_2 \mid \mathsf{inj}_2\ x\Rightarrow e_3\ \mathsf{end}:\tau}$$

$$\textsc{T-Rec}\ \frac{\Xi \mid \Gamma, f:\tau_1\to\tau_2, x:\tau_1 \vdash e:\tau_2}{\Xi \mid \Gamma \vdash \mathsf{rec}\ f(x):=e:\tau_1\to\tau_2} \qquad \textsc{T-App}\ \frac{\Xi \mid \Gamma \vdash e_1:\tau_1\to\tau_2 \qquad \Xi \mid \Gamma \vdash e_2:\tau_1}{\Xi \mid \Gamma \vdash e_1\ e_2:\tau_2}$$

$$\textsc{T-TLam}\ \frac{\Xi,X \mid \Gamma \vdash e:\tau}{\Xi \mid \Gamma \vdash \Lambda\, e:\forall X.\ \tau} \qquad \textsc{T-TApp}\ \frac{\Xi \mid \Gamma \vdash e:\forall X.\ \tau}{\Xi \mid \Gamma \vdash e\ \_:\tau[\tau'/X]}$$

Dynamics

$$\frac{e \to_h e'}{K[e] \to K[e']}\ \text{HEAD-STEP-STEP}$$

$$\text{E-ADD}\quad \overline{n_1} + \overline{n_2} \to_h \overline{n_1 + n_2}$$

$$\text{E-SUB}\quad \overline{n_1} - \overline{n_2} \to_h \overline{n_1 - n_2}$$

$$\frac{n_1 = n_2}{\overline{n_1} = \overline{n_2} \to_h \mathsf{true}}\ \text{E-EQ}$$

$$\frac{n_1 \neq n_2}{\overline{n_1} = \overline{n_2} \to_h \mathsf{false}}\ \text{E-NOT-EQ}$$

$$\frac{n_1 \leq n_2}{\overline{n_1} \leq \overline{n_2} \to_h \mathsf{true}}\ \text{E-LE}$$

$$\frac{n_1 \nleq n_2}{\overline{n_1} \leq \overline{n_2} \to_h \mathsf{false}}\ \text{E-NOT-LE}$$

$$\frac{n_1 < n_2}{\overline{n_1} < \overline{n_2} \to_h \mathsf{true}}\ \text{E-LT}$$

$$\frac{n_1 \nless n_2}{\overline{n_1} < \overline{n_2} \to_h \mathsf{false}}\ \text{E-NOT-LT}$$

$$\text{E-IF-TRUE}\quad \mathsf{if\ true\ then}\ e_2\ \mathsf{else}\ e_3 \to_h e_2$$

$$\text{E-IF-FALSE}\quad \mathsf{if\ false\ then}\ e_2\ \mathsf{else}\ e_3 \to_h e_3$$

$$\text{E-FST}\quad \mathsf{fst}\ (v_1, v_2) \to_h v_1$$

$$\text{E-SND}\quad \mathsf{snd}\ (v_1, v_2) \to_h v_2$$

$$\text{E-MATCH-INJ1}\quad \mathsf{match}\ (\mathsf{inj}_1\ v)\ \mathsf{with\ inj}_1\ x \Rightarrow e_2 \mid \mathsf{inj}_2\ x \Rightarrow e_3\ \mathsf{end} \to_h e_2[v/x]$$

$$\text{E-MATCH-INJ2}\quad \mathsf{match}\ (\mathsf{inj}_2\ v)\ \mathsf{with\ inj}_1\ x \Rightarrow e_2 \mid \mathsf{inj}_2\ x \Rightarrow e_3\ \mathsf{end} \to_h e_3[v/x]$$

$$\text{E-REC-APP}\quad (\mathsf{rec}\ f(x) := e) v \to_h e[\mathsf{rec}\ f(x) := e / f][v/x]$$

$$\text{E-TAPP-TLAM}\quad (\Lambda\, e)\ \_ \to_h e$$

Lemma 1. $K[e] \to_h e' \wedge \neg(K = []) \implies \mathrm{Val}(e)$

Proof. This can be shown by doing case distinction on the head-step $K[e] \to_h e'$. We show it here only for case E-ADD, as all the other cases are similar.

So assume $K[e] = \overline{n_1} + \overline{n_2}$, and $e' = \overline{n_1 + n_2}$. Then there are three cases: $K = []$ and $e = \overline{n_1} + \overline{n_2}$, $K = [] + \overline{n_2}$ and $e = \overline{n_1}$, or $K = \overline{n_1} + []$ and $e = \overline{n_2}$. The first case raises a contradiction as we have assumed $\neg(K = [])$. In the remaining two cases, we may conclude $\mathrm{Val}(e)$, as wanted. □

Lemma 2 (Evaluation under Context)**.** $K[e] \to^* e' \implies \exists e''.(e \to^* e'') \wedge ((\mathrm{Val}(e'') \wedge K[e''] \to^* e') \vee (\neg\mathrm{Val}(e'') \wedge K[e''] = e'))$

Proof. So assuming $K[e] \to^* e'$, we must show

$$\exists e''.(e \to^* e'') \wedge \big((\mathrm{Val}(e'') \wedge K[e''] \to^* e') \vee (\neg\mathrm{Val}(e'') \wedge K[e''] = e')\big) \tag{2.1}$$

We proceed by induction on the number of steps in the evaluation $K[e] \to^* e'$. Let n denote the number of steps taken, so that $K[e] \to^n e'$.

- Base Case $n = 0$. In this case, we have that $K[e] \to^0 e'$, which means that $K[e] = e'$. Now use e for e'' in 2.1. We must show

$$(e \to^* e) \wedge \big((\mathrm{Val}(e) \wedge K[e] \to^* e') \vee (\neg\mathrm{Val}(e) \wedge K[e] = e')\big)$$

  Trivially, $e \to^* e$. For the second part, we proceed by case distinction on $\mathrm{Val}(e)$.

  - $\mathrm{Val}(e)$. We have that $K[e] \to^0 e'$, so $K[e] \to^* e'$. Thus, we have $\mathrm{Val}(e) \wedge K[e] \to^* e'$, which matches the left part of the "$\vee$".
  - $\neg\mathrm{Val}(e)$. We know that $K[e] = e'$, so we have $\neg\mathrm{Val}(e) \wedge K[e] = e'$, which matches the right part of the "$\vee$".

- Inductive Step $n = m+1$. Now we have $K[e] \to^{m+1} e'$. By the Induction Hypothesis, we have:

$$\begin{aligned}\forall F, f, f'. F[f] \to^m f' \implies \exists f''.(f \to^* f'')\wedge \\ \big((\mathrm{Val}(f'') \wedge F[f''] \to^* f') \vee (\neg\mathrm{Val}(f'') \wedge K[f''] = f')\big)\end{aligned} \quad (2.2)$$

  Split the evaluation, $K[e] \to^{m+1} e'$, up, so that $K[e] \to g \wedge g \to^m e'$. Looking at our dynamics, we must have that $K[e] = H[h]$, and $g = H[h']$, for some evaluation context H, and expressions h, h', and $h \to_h h'$. There are now three possible cases. Either $e = h$, e is a superexpression of h, or e is a subexpression of h. We will consider each in turn.

  - $K = H$ and $e = h$.
    Then $g = H[h'] = K[h']$, and $e \to_h h'$. Furthermore, $K[h'] \to^m e'$. Instantiate I.H. with this to get

$$\begin{aligned}\exists f''.(h' \to^* f'')\wedge \\ \big((\mathrm{Val}(f'') \wedge K[f''] \to^* e') \vee (\neg\mathrm{Val}(f'') \wedge K[f''] = e')\big)\end{aligned} \quad (2.3)$$

    Call this quantified expression for f'', and use it for e'' in 2.1. We must then show

$$(e \to^* f'') \wedge \big((\mathrm{Val}(f'') \wedge K[f''] \to^* e') \vee (\neg\mathrm{Val}(f'') \wedge K[f''] = e')\big)$$

    We know that $e \to h'$, as $e \to_h h'$, and by 2.3, we know that $h' \to^* f''$, so that $e \to^* f''$. The second part follows directly from 2.3.

  - $K[E[]] = H$ and $e = E[h]$.
    Then $g = H[h'] = K[E[]][h'] = K[E[h']]$, thus $K[E[h']] \to^m e'$. Instantiate I.H. with this to get

$$\begin{aligned}\exists f''.(E[h'] \to^* f'')\wedge \\ \big((\mathrm{Val}(f'') \wedge K[f''] \to^* e') \vee (\neg\mathrm{Val}(f'') \wedge K[f''] = e')\big)\end{aligned} \quad (2.4)$$

Call this quantified expression for f'', and use it for e'' in 2.1. We must then show

$$(e \to^* f'') \wedge \big((\mathrm{Val}(f'') \wedge K[f''] \to^* e') \vee (\neg\mathrm{Val}(f'') \wedge K[f''] = e')\big)$$

We know that $E[h] \to E[h']$, as $h \to_h h'$, and since $e = E[h]$, then $e \to E[h']$. By 2.4, we know that $E[h'] \to^* f''$, so that $e \to^* f''$. The second part follows directly from 2.4.

- $K = H[E[]]$ and $E[e] = h$. Here we have $h = E[e]$, so $E[e] \to_h h'$. Note that E is not the empty evaluation context, as otherwise, we would be in case 1. So by lemma 1, we know that $\mathrm{Val}(e)$. Now, pick e for e'' in 2.1. We must show

  $$(e \to^* e) \wedge \big((\mathrm{Val}(e) \wedge K[e] \to^* e') \vee (\neg\mathrm{Val}(e) \wedge K[e] = e')\big)$$

  Trivially, $e \to^* e$. We also have that $\mathrm{Val}(e)$, and since $K[e] \to^{m+1} e'$, then $K[e] \to^* e'$.

$\square$

Chapter 3

Contextual Equivalence

►draft◄

Context

$$
\begin{aligned}
C ::= {} & [] \mid C+e \mid e+C \mid C-e \mid e-C \mid C \leq e \mid e \leq C \mid C < e \mid e < C \mid C = e \mid e = C \mid \\
& \textsf{if } C \textsf{ then } e \textsf{ else } e \mid \textsf{if } e \textsf{ then } C \textsf{ else } e \mid \textsf{if } e \textsf{ then } e \textsf{ else } C \mid (C,e) \mid (e,C) \mid \\
& \textsf{fst } C \mid \textsf{snd } C \mid \textsf{inj}_1\, C \mid \textsf{inj}_2\, C \mid \textsf{match } C \textsf{ with inj}_1\, x \Rightarrow e \mid \textsf{inj}_2\, x \Rightarrow e \textsf{ end} \mid \\
& \textsf{match } e \textsf{ with inj}_1\, x \Rightarrow C \mid \textsf{inj}_2\, x \Rightarrow e \textsf{ end} \mid \\
& \textsf{match } e \textsf{ with inj}_1\, x \Rightarrow e \mid \textsf{inj}_2\, x \Rightarrow C \textsf{ end} \mid \textsf{rec } f(x) := C \mid C\, e \mid e\, C \mid C\, \_
\end{aligned}
$$

►fix unfinished text passage - start◄

We define CE so that two programs are CE iff under all Contexts, one program terminates iff the other does. One may ponder whether this definition is really strong enough. If both terminate, we really want the result of the two programs to have values that are behaviourally the same, otherwise, we can certainly put them in a context, where they have different behaviour. For integer values, for example, this means that the two values must be the same number, and for product types, this means that the first value in each pair should be behaviourally the same, and likewise with the second value in each pair. To give an intuition as to why this definition is strong enough, consider two CE programs e1 and e2, where $\cdot \mid \cdot \vdash e_1 : \tau$ and $\cdot \mid \cdot \vdash e_2 : \tau$. Note first that if both e1 and e2 don't terminate, then they will be behaviourally the same. If we plug them into any context, and the context makes us evaluate the expressions, both will not terminate. And if the context doesn't make us evaluate the expressions, then they have no influence in the run of the programs, so they will behave the same.

Now consider what happens if e1 terminates with some value v1. Can we then guarantee that e2 also terminates with some value v2, and v1 and v2 behave the same? Since e1 and e2 are CE, then we can put them into any context, C, and one will terminate iff the other one does. Let's assume that tau = Z. Then consider when C has the form $\textsf{if } [] = v_1 \textsf{ then } () \textsf{ else } \omega$. Here $C[e_1] \downarrow ()$. But what about $C[e_2]$? If v2 != v1, then our evaluation rules tell us that we will take the else branch, and hence not terminate. However, since e1 and e2 are CE, and C[e1] terminates then we know that C[e2] must also terminate. Hence it is not the case that v2 != v1, and thus v2 = v1. So if our two programs of type integer are CE, and they both don't run forever, then they must both evaluate to the same value.

Now if tau was bool instead, the context if [] then () else ω would suffice in showing that v2 = v1.

►fix unfinished text passage - end◄

Chapter 4

Logical Relations for Contextual Equivalence

►draft◄

Chapter 5

Examples of Application of Contextual Equivalence

►draft◄

Chapter 6

Comparison to Other Work and Ideas for Future Work

▸draft◂

Chapter 7

Conclusion

►conclude on the problem statement from the introduction◄

Acknowledgments

►...◄

Bibliography

[1] Aske Simon Christensen, Anders Møller, and Michael I. Schwartzbach. Precise analysis of string expressions. In Radhia Cousot, editor, *Static Analysis, 10th International Symposium, SAS 2003, San Diego, CA, USA, June 11-13, 2003, Proceedings*, volume 2694 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2003.

Appendix A

The Technical Details

►...◄