A Formalization of Unique Solutions of Equations in Process Algebra

Chun Tian

<chun.tian@studio.unibo.it>

Supervised by: Prof. Davide Sangiorgi

December 20, 2017

Project Motivation

- Concurrency Theory is interesting, beautiful, self-consistent, and important for understanding concurrent and reactive systems;
- Milner's Calculus of Communicating Systems (CCS) is simple/elegant process algebra widely adopted in Concurrency Theory courses, yet textbooks cannot provide all proof details;
- The author was seeking formalization projects for learning Interactive Theorm Proving (ITP), after having learnt λ-calculus and Simple Type Theory;

Project summary

- 19,247 lines of Standard ML code;
- 463 manually proved lemmas/theorems (150+ were new).

Availabile in HOL official examples: https://github.com/HOL-Theorem-Prover/HOL/tree/master/examples/CCS

Relationship with the work of Monica Nesi

1. The work of Monica Nesi was ported from HOL88 to HOL4;
2. The porting work was relative easy: most of proof steps (tactics) have still the same name and (almost the same) behavior;
3. Some changes in the work of Nesi:
   - the type of `Action` has been re-defined as `Label option`;
   - redefined strong and weak equivalence using HOL's co-inductive relation package.
   - previously unfinished proof (transitivity of observational congruence) is finished.
4. Properties and algebraic laws for strong/weak equivalence and observational congruence; decision procedure for CCS transitions.
5. (Internship project) Hennessy Lemma, Deng Lemma, Coarsest congruence contained in weak equivalence.
6. (Thesis project) Bisimulation up-to; unique solution of equations; expansion/contraction; trace; unique solution of contractions.

Higher Order Logic and HOL Theorem Prover (HOL4)

Definition (Type in HOL)

$$\sigma \quad ::= \quad \alpha \quad | \quad c \quad | \quad \underbrace{(\sigma_1, \ldots, \sigma_n) op} \quad | \quad \underbrace{\sigma_1 \to \sigma_2}$$

atomic types

compound types

type variables

function types
(domain σ_1, codomain

Definition (Term in HOL)

$$t \quad ::= \quad x \quad | \quad c \quad | \quad \underbrace{t\ t'} \quad | \quad \underbrace{\lambda x.\ t}$$

constants

λ-abstractions

function applications
(function t, argument t')

variables

Primitive rules

1. Assumption introduction [ASSUME],
2. Reflexivity [REFL],
3. β-conversion [BETA_CONV],
4. Substitution [SUBST],
5. Abstraction [ABS],
6. Type instantiation [INST_TYPE],
7. Discharging an assumption [DISCH],
8. Modus Ponens [MP]

Logical constants

$$\begin{array}{l}
\vdash \ \mathrm{T} = ((\lambda x_{\mathbf{bool}}.\ x) = (\lambda x_{\mathbf{bool}}.\ x)) \\
\vdash \ \forall = \lambda P_{\alpha \to \mathbf{bool}}.\ \ P = (\lambda x.\ \mathrm{T}) \\
\vdash \ \exists = \lambda P_{\alpha \to \mathbf{bool}}.\ \ P(\varepsilon\ P) \\
\vdash \ \mathrm{F} = \forall b_{\mathbf{bool}}.\ \ b \\
\vdash \ \neg = \lambda b.\ \ b \Rightarrow \mathrm{F} \\
\vdash \ \wedge = \lambda b_1\ b_2.\ \forall b.\ (b_1 \Rightarrow (b_2 \Rightarrow b)) \Rightarrow b \\
\vdash \ \vee = \lambda b_1\ b_2.\ \forall b.\ (b_1 \Rightarrow b) \Rightarrow ((b_2 \Rightarrow b) \Rightarrow b)
\end{array}$$

Axioms

BOOL_CASES_AX	$\vdash \forall b.\ (b = \mathrm{T}) \vee (b = \mathrm{F})$
ETA_AX	$\vdash \forall f_{\alpha \to \beta}.\ (\lambda x.\ f\ x) = f$
SELECT_AX	$\vdash \forall P_{\alpha \to \mathbf{bool}}\ x.\ P\ x \Rightarrow P(\varepsilon\ P)$
INFINITY_AX	$\vdash \exists f_{\mathit{ind} \to \mathit{ind}}.\ \mathrm{One\_One}\ f\ \wedge\ \neg(\mathrm{Onto}\ f)$

Calculus of Communicating Systems (CCS)

Definition (Syntactically-finite CCS; no value-passing; with relabeling operator)

$$p ::= \mathrm{nil} \mid \alpha.p \mid p+q \mid p \parallel q \mid (\nu a)p \mid p[b/a] \mid \mathrm{var}\, X \mid \mathrm{rec}\, X\, p$$

$$\alpha ::= \tau \mid l \quad \text{(action)}; \qquad l ::= b \mid \overline{b} \quad \text{(label)}$$

Operator	Notation	HOL	HOL (alternative)
nil	$\mathbf{0}$	`nil`	`nil`
Rrefix	$a.b.0$	`prefix a (prefix b nil)`	a`..`b`..nil`
Sum	$p+q$	`sum p q`	p `+` q
Parallel	$p \mid q$	`par p q`	$p \parallel q$
Restriction	$(\nu L)p$	`restr L p`	ν L p
Constant	$A = a.A$	`rec A (prefix a (var A))`	`rec` A `(`a`..var` A`)`

Definition (Guarded sums)

$$\alpha.p + \beta.q \qquad \text{or} \qquad \Sigma_i \mu_i.p_i$$

Structural Operational Semantics (SOS)

The $\mathtt{TRANS}$ relation

defined by 9 *inductive rules:*

$$(\mathrm{Sum}_1)\ \frac{p \xrightarrow{\mu} p'}{p + q \xrightarrow{\mu} p'}$$

$$(\mathrm{Sum}_2)\ \frac{q \xrightarrow{\mu} q'}{p + q \xrightarrow{\mu} q'}$$

$$(\mathrm{Par}_1)\ \frac{p \xrightarrow{\mu} p'}{p|q \xrightarrow{\mu} p'|q}$$

$$(\mathrm{Par}_2)\ \frac{q \xrightarrow{\mu} q'}{p|q \xrightarrow{\mu} p|q'}$$

$$(\mathrm{Perfix})\ \frac{}{\mu.p \xrightarrow{\mu} p}$$

$$(\mathrm{Rec})\ \frac{q[\mathtt{rec}\ x.q\ /\ x] \xrightarrow{\mu} r}{\mathtt{rec}\ x.q \xrightarrow{\mu} r}$$

$$(\mathrm{Restr})\ \frac{p \xrightarrow{\mu} p'}{(\nu a)p \xrightarrow{\mu} (\nu a)p'}\ \mu \neq a, \bar{a}$$

$$(\mathrm{Par}_3)\ \frac{p \xrightarrow{\alpha} p' \qquad q \xrightarrow{\bar{\alpha}} q'}{p|q \xrightarrow{\tau} p'|q'}$$

$$(\mathrm{Relabeling})\ \frac{p \xrightarrow{\mu} p'}{p[f] \xrightarrow{f(\mu)} p'[f]}$$

A decision procedure for CCS transitions

Decision procedure implemented as ML function

```
CCS_TRANS_CONV : term -> thm
```

Example

The CCS process $a.0|\bar{a}.0$ have three possible transitions:

$$\begin{tikzcd} & a.0\|\bar{a}.0 \arrow[dl, "a"] \arrow[d, "\tau"] \arrow[dr, "\bar{a}"] & \\ 0\|\bar{a}.0 & 0\|0 & a.0\|0 \end{tikzcd}$$

Theorem (Transitions coming from $a.0|\bar{a}.0$)

$$\begin{aligned} \vdash\ & \mathtt{In}\ \text{“a”}..\mathtt{nil} \parallel \mathtt{Out}\ \text{“a”}..\mathtt{nil}\ -u\rightarrow\ E \iff \\ & ((u = \mathtt{In}\ \text{“a”}) \land (E = \mathtt{nil} \parallel \mathtt{Out}\ \text{“a”}..\mathtt{nil}) \lor \\ & \ (u = \mathtt{Out}\ \text{“a”}) \land (E = \mathtt{In}\ \text{“a”}..\mathtt{nil} \parallel \mathtt{nil})) \lor \\ & (u = \tau) \land (E = \mathtt{nil} \parallel \mathtt{nil}) \end{aligned}$$

EPS, Weak Transition and Trace

EPS: $E \stackrel{\epsilon}{\Rightarrow} E'$ as Reflexive Transitive Closure (RTC) of "$\stackrel{\tau}{\rightarrow}$"

$$\texttt{EPS} = (\lambda E\ E'.\ E \ {-\tau\rightarrow}\ E')^*$$

Weak Transition: $E \stackrel{\mu}{\Rightarrow} E'$ (and $E \stackrel{\hat{\mu}}{\Rightarrow} E' ::= E \stackrel{\epsilon}{\Rightarrow} E'$ if $\mu = \tau$)

$$E \ {=u\Rightarrow}\ E' \iff \exists E_1\ E_2.\ E \stackrel{\epsilon}{\Rightarrow} E_1 \land E_1 \ {-u\rightarrow}\ E_2 \land E_2 \stackrel{\epsilon}{\Rightarrow} E'$$

Trace: $E \xrightarrow{h::t} E'$ as List-accumulated RTC of "$\rightarrow$"

$$\texttt{TRACE} = \texttt{LRTC TRANS}$$

$\vdash E \stackrel{\epsilon}{\Rightarrow} E' \iff \exists xs.\ \texttt{TRACE}\ E\ xs\ E' \land \texttt{NO\_LABEL}\ xs$

$\vdash E \ {=u\Rightarrow}\ E' \iff$
$\quad \exists us.$
$\quad\quad \texttt{TRACE}\ E\ us\ E' \land \neg\texttt{NULL}\ us \land$
$\quad\quad \textbf{if}\ u = \tau\ \textbf{then}\ \texttt{NO\_LABEL}\ us\ \textbf{else}\ \texttt{UNIQUE\_LABEL}\ u\ us$

$\vdash \texttt{NO\_LABEL}\ L \iff \neg\exists l.\ \texttt{MEM (label}\ l\texttt{)}\ L$

$\vdash \texttt{UNIQUE\_LABEL}\ u\ L \iff$
$\quad \exists L_1\ L_2.$
$\quad\quad (L_1 +\!\!+ [u] +\!\!+ L_2 = L) \land$
$\quad\quad \neg\exists l.\ \texttt{MEM (label}\ l\texttt{)}\ L_1 \lor \texttt{MEM (label}\ l\texttt{)}\ L_2$

Bisimulation and bisimulation equivalences

Definition (Strong/weak bisimulations; observational congruence)

$$
\begin{array}{ccc}
P & \mathcal{R} & Q \\
\downarrow{\scriptstyle\mu} & & \downarrow{\scriptstyle\mu} \\
\forall P' & \mathcal{R} & \exists Q'
\end{array}
,\quad
\begin{array}{ccc}
P & \mathcal{R} & Q \\
\downarrow{\scriptstyle\mu} & & \Downarrow{\scriptstyle\hat{\mu}} \\
\forall P' & \mathcal{R} & \exists Q'
\end{array}
,\quad
\begin{array}{ccc}
P & \approx^c & Q \\
\downarrow{\scriptstyle\mu} & & \Downarrow{\scriptstyle\mu} \\
\forall P' & \approx & \exists Q'
\end{array}
$$

Definition (Strong/weak equivalence (bisimilarity))

$$\sim / \approx = \bigcup \{\mathcal{R} \subseteq Q \times Q \colon \mathcal{R} \text{ is a strong/weak bisimulation}\}$$

Theorem (Property (*) (`PROPERTY_STAR`))

$$
\begin{array}{ccc}
P & \sim / \approx & Q \\
\downarrow{\scriptstyle\mu} & & \downarrow{\scriptstyle\mu} \\
\forall P' & \sim / \approx & \exists Q'
\end{array}
\qquad
\textit{old proof:}\quad
\begin{array}{ccc}
P & \sim' & Q \\
\downarrow{\scriptstyle\mu} & & \downarrow{\scriptstyle\mu} \\
\forall P' & \sim & \exists Q'
\end{array}
$$

The Theory of Congruence for CCS

Semantic Context (multi-hole or no-hole) as an inductive set of λ-functions

$\texttt{CONTEXT}\ (\lambda t.\ t)$
$\texttt{CONTEXT}\ (\lambda t.\ p)$
$\texttt{CONTEXT}\ e \Rightarrow \texttt{CONTEXT}\ (\lambda t.\ a..e\ t)$
$\texttt{CONTEXT}\ e_1 \wedge \texttt{CONTEXT}\ e_2 \Rightarrow \texttt{CONTEXT}\ (\lambda t.\ e_1\ t + e_2\ t)$
$\texttt{CONTEXT}\ e_1 \wedge \texttt{CONTEXT}\ e_2 \Rightarrow \texttt{CONTEXT}\ (\lambda t.\ e_1\ t \parallel e_2\ t)$
$\texttt{CONTEXT}\ e \Rightarrow \texttt{CONTEXT}\ (\lambda t.\ \nu\ L\ (e\ t))$
$\texttt{CONTEXT}\ e \Rightarrow \texttt{CONTEXT}\ (\lambda t.\ \texttt{relab}\ (e\ t)\ rf)$

The combination of two contexts is still a context:
$\vdash \texttt{CONTEXT}\ c_1 \wedge \texttt{CONTEXT}\ c_2 \Rightarrow \texttt{CONTEXT}\ (c_1 \circ c_2)$

Definition (Precongruence and Congruence)

- $\texttt{precongruence}\ R \iff$
  $\forall x\ y\ ctx.\ \texttt{CONTEXT}\ ctx \Rightarrow R\ x\ y \Rightarrow R\ (ctx\ x)\ (ctx\ y)$
- $\texttt{congruence}\ R \iff \texttt{equivalence}\ R \wedge \texttt{precongruence}\ R$
  $\texttt{equivalence}\ R \iff \texttt{reflexive}\ R \wedge \texttt{symmetric}\ R \wedge \texttt{transitive}\ R$
- $\sim$, $\approx^c$ are congruence. (so is $\approx$ if guarded sums are required)

Unique Solutions of Equations

Definition (Process Equations)

An equation of CCS has the form $\tilde{X} \asymp E[\tilde{X}]$ in which E is a semantic context, $\asymp$ is an equivalence relation.

Definition (Guardedness)

- X is *weakly guarded* in E if each occurrence of X is within some subexpression $\alpha.F$ of E.
- X is (strongly) guarded in E if each occurrence of X is within some subexpression $l.F$ of E (l is a visible action).
- X is *sequential* in E if every subexpression of E which contains X, apart from X itself, is of the form $\alpha.F$ or ΣF.

Theorem (Milner's three "Unique solutions of equations" theorems)

$\vdash \texttt{WG}\ E \Rightarrow \forall P\ Q.\ P \sim E\ P \land Q \sim E\ Q \Rightarrow P \sim Q$
$\vdash \texttt{SG}\ E \land \texttt{GSEQ}\ E \Rightarrow \forall P\ Q.\ P \approx E\ P \land Q \approx E\ Q \Rightarrow P \approx Q$
$\vdash \texttt{SG}\ E \land \texttt{SEQ}\ E \Rightarrow \forall P\ Q.\ P \approx^c E\ P \land Q \approx^c E\ Q \Rightarrow P \approx^c Q$

Bisimulation Up-to Techniques

Definition (Bisimulation up to $\sim$)

$$\begin{tikzcd} & P \arrow[dl, "\alpha"] & \mathcal{S} & Q \arrow[dr, "\alpha"] & \\ \forall P' \arrow[r, dotted, no head, "\sim"] & P'' & \mathcal{S} & Q'' \arrow[r, dotted, no head, "\sim"] & \exists Q' \end{tikzcd}$$

Definition (Bisimulation up to $\approx$, two versions)

$$\begin{tikzcd} & P \arrow[dl, "\alpha"] & \mathcal{S} & Q \arrow[dr, Rightarrow, "\hat{\alpha}"] & \\ \forall P' \arrow[r, dotted, no head, "\sim"] & P'' & \mathcal{S} & Q'' \arrow[r, dotted, no head, "\approx"] & \exists Q' \end{tikzcd}
\qquad
\begin{tikzcd} & P \arrow[dl, Rightarrow, "\alpha"] & \mathcal{S} & Q \arrow[dr, Rightarrow, "\hat{\alpha}"] & \\ \forall P' \arrow[r, dotted, no head, "\approx"] & P'' & \mathcal{S} & Q'' \arrow[r, dotted, no head, "\approx"] & \exists Q' \end{tikzcd}$$

Theorem (Proof techniques using "Bisimulation up to")

If $\mathcal{S}$ is a "bisimulation up to $\sim$ (or $\approx$)", then $\mathcal{S} \subseteq \sim$ (or $\approx$):

$\vdash$ `STRONG_BISIM_UPTO` $Bsm \Rightarrow Bsm \subseteq_r$ `STRONG_EQUIV`

$\vdash$ `WEAK_BISIM_UPTO` $Wbsm \Rightarrow Wbsm \subseteq_r$ `WEAK_EQUIV`

Expansion and Contraction

Definition (Expansion (preorder; 'precongruence'))

$$
\begin{tikzcd}
P \arrow[d, "\mu"] & \mathcal{R} & Q \arrow[d, "\hat{\mu}"] \\
\forall P' & \mathcal{R} & \exists Q'
\end{tikzcd}
,\quad
\begin{tikzcd}
P \arrow[d, Rightarrow, "\mu"] & \mathcal{R} & Q \arrow[d, "\mu"] \\
\exists P' & \mathcal{R} & \forall Q'
\end{tikzcd}
$$

P *expands* Q, written $P \succeq_{\mathrm{e}} Q$, if $P \mathcal{R} Q$, for some expansion $\mathcal{R}$.

Definition (Contraction (preorder; 'precongruence'))

$$
\begin{tikzcd}
P \arrow[d, "\mu"] & \mathcal{R} & Q \arrow[d, "\hat{\mu}"] \\
\forall P' & \mathcal{R} & \exists Q'
\end{tikzcd}
,\quad
\begin{tikzcd}
P \arrow[d, Rightarrow, "\hat{\mu}"] & \mathcal{R} & Q \arrow[d, "\mu"] \\
\exists P' & \approx & \forall Q'
\end{tikzcd}
$$

P *contracts* (to) Q, written $P \succeq_{\mathrm{bis}} Q$, if $P \mathcal{R} Q$, for some contraction $\mathcal{R}$.

Definition (Preorder and 'precongruence')

$\texttt{PreOrder}\ R \iff \texttt{reflexive}\ R \land \texttt{transitive}\ R$

$\texttt{precongruence1}\ R \iff$

$\forall x\ y\ ctx.\ \texttt{GCONTEXT}\ ctx \Rightarrow R\ x\ y \Rightarrow R\ (ctx\ x)\ (ctx\ y)$

Unique Solution of Expansions/Contractions

Theorem (Relationships between expands, contracts and $\approx$)

$$\succeq_{\mathrm{e}} \subset \succeq_{\mathrm{bis}} \subset \approx$$

Theorem (Unique solution of contraction (Davide Sangiorgi, 2015))

$\vdash \texttt{WGS}\ E \Rightarrow \forall P\ Q.\ P \succeq_{bis} E\ P \wedge Q \succeq_{bis} E\ Q \Rightarrow P \approx Q$

Theorem (Unique solution of expansion, easily derivable from $\succeq_{\mathrm{e}} \subset \succeq_{\mathrm{bis}}$)

$\vdash \texttt{WGS}\ E \Rightarrow \forall P\ Q.\ P \succeq_{e} E\ P \wedge Q \succeq_{e} E\ Q \Rightarrow P \approx Q$

Why contraction?

Completeness holds only for contraction. (Completeness: suppose $\mathcal{R}$ is a bisimulation, then there is a system of weakly-guarded pure contractions of which $\mathcal{R}_1$ and $\mathcal{R}_2$ are solutions for $\succeq_{\mathrm{bis}}$.

Observational Contractions

Definition (Observational contraction)

$$E \succeq^c_{bis} E' \iff$$
$$\forall u.$$
$$(\forall E_1.\ E \ {-u\rightarrow}\ E_1 \Rightarrow \exists E_2.\ E' \ {-u\rightarrow}\ E_2 \land E_1 \succeq_{bis} E_2) \land$$
$$\forall E_2.\ E' \ {-u\rightarrow}\ E_2 \Rightarrow \exists E_1.\ E \ {=u\Rightarrow}\ E_1 \land E_1 \approx E_2$$

Theorem (Relationships of $\succeq^c_{\text{bis}}$ with others)

$$\succeq^c_{\text{bis}} \subset \succeq_{\text{bis}} \subset \approx$$
$$\succeq^c_{\text{bis}} \subset \approx^c \subset \approx$$

Theorem (Properties of $\succeq^c_{\text{bis}}$)

$\vdash$ `PreOrder OBS_contracts`

$\vdash$ `precongruence OBS_contracts`

Theorem (Unique solution of observational contraction (Chun Tian))

$\vdash \texttt{WG}\ E \Rightarrow \forall P\ Q.\ P \succeq^c_{bis} E\ P \land Q \succeq^c_{bis} E\ Q \Rightarrow P \approx Q$

Theorem (Coarsest precongruence contained in $\succeq_{\text{bis}}$ (Chun Tian))

$\vdash \texttt{free\_action}\ p \land \texttt{free\_action}\ q \Rightarrow (p \succeq^c_{bis} q \iff \forall r.\ p + r \succeq_{bis} q + r)$

Conclusions

1. An old formalization of Finitrary CCS has been ported to currently latest HOL Theorem Prover (HOL4) and merged into official examples;
2. It's the first formalization of Milner's "unique solution of equations" and Sangiorgi's "unique solution of contractions" theorems, although limited into single-variable cases.
3. Modern features (e.g. co-inductive relation) and built-in theories (number, relation, list, ...) in HOL theorem prover were used for minimizing the efforts.
4. The 2015 paper [2] of Prof. Davide Sangiorgi is (partially) formally verified.

Bibliography

1. Nesi, M.: *A formalization of the process algebra CCS in high order logic.* University of Cambridge, Computer Laboratory (1992).
2. Sangiorgi, D.: *Equations, contractions, and unique solutions.* ACM SIGPLAN Notices. (2015).
3. Gorrieri, R., Versari, C.: *Introduction to Concurrency Theory*. Springer, Cham (2015).
4. Sangiorgi, D.: *Introduction to Bisimulation and Coinduction.* Cambridge University Press (2011).
5. Milner, R.: *Communication and Concurrency.* Prentice Hall International Series in Computer Science (1989).
6. Milner, R.: *Operational and Algebraic Semantics of Concurrent Processes.* In: Handbook of Theoretical Computer Science, Volume B: Formal Models and Semantics. pp. 1202–1242. Elsevier (2014).
7. Sangiorgi, D., Milner, R.: *The problem of "Weak Bisimulation up to".* CONCUR'92. (1992).
8. van Glabbeek, R.J.: *A characterisation of weak bisimulation congruence*. Lecture notes in computer science. 3838, 26–39 (2005).

Project History

1. (Feb 2016) First attending of *Concurrent Models and Systems* (MSC) course (Prof. Roberto Gorrieri); (not well understood)
2. (Jun 2016) The author found the CCS formalization [1] of Monica Nesi; Nesi sent an partial copy of proof scripts to the author;
3. (Jan 2017) The author finally learnt to use HOL theorem prover (HOL4) and started porting the old proof code.
4. (Feb 2017) Second attending of MSC course; (fully understood this time)
5. (May 2017) Finished porting all proof scripts from Nesi (resulting work was merged as HOL4 official example); Nesi sent the rest proof scripts to the author;
6. (Jun 2017) MSC exam passed by project + oral exam; Gorrieri agreed to supervise another Internship project (*tirocinio*) for the newly receiving code.
7. (Jul 2017) Finished *tirocinio* project. (Half of proved theorems were new) Gorrieri suggested Prof. Davide Sangiorgi for thesis supervision; Sangiorgi proposed the formalization of his "unique solution of contractions" theorem.
8. (Aug 2017) Formalized "bisimulation upto" and Milner's "unique solution of equation". Sangiorgi agreed the continue of this work as a thesis project.
9. (Oct 2017) Formalized Sangiorgi's "unique solution of contraction" theorem.