

# 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 Theorem Proving (ITP), after having learnt  $\lambda$ -calculus and Simple Type Theory;

## Project summary

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

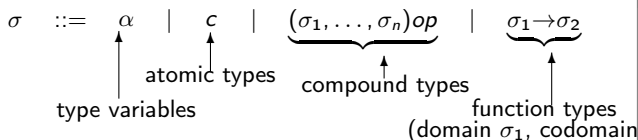
Available in HOL official examples: <https://github.com/HOL-Theorem-Prover/HOL/tree/master/examples/CCS>

# Relationship with the work of Monica Nesi

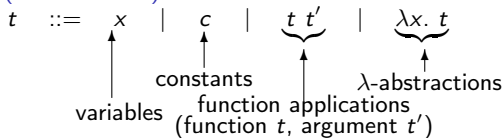
- ① The work of Monica Nesi was ported from HOL88 to HOL4;
- ② The porting work was relative easy: most of proof steps (tactics) have still the same name and (almost the same) behavior;
- ③ Some changes in the work of Nesi:
  - the type of `Action` has been re-defined as `Label option`;
  - redefined 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)



## Definition (Term in HOL)



## Primitive rules

- 1 Assumption introduction [ASSUME],
- 2 Reflexivity [REFL],
- 3  $\beta$ -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

$\vdash T = ((\lambda x_{\text{bool}}. x) = (\lambda x_{\text{bool}}. x))$   
 $\vdash \forall = \lambda P_{\alpha \rightarrow \text{bool}}. P = (\lambda x. T)$   
 $\vdash \exists = \lambda P_{\alpha \rightarrow \text{bool}}. P(\varepsilon P)$   
 $\vdash F = \forall b_{\text{bool}}. b$   
 $\vdash \neg = \lambda b. b \Rightarrow F$   
 $\vdash \wedge = \lambda b_1 b_2. \forall b. (b_1 \Rightarrow (b_2 \Rightarrow b)) \Rightarrow b$   
 $\vdash \vee = \lambda b_1 b_2. \forall b. (b_1 \Rightarrow b) \Rightarrow ((b_2 \Rightarrow b) \Rightarrow b)$

## Axioms

BOOL\_CASES\_AX     $\vdash \forall b. (b = T) \vee (b = F)$   
 ETA\_AX     $\vdash \forall f_{\alpha \rightarrow \beta}. (\lambda x. f \ x) = f$   
 SELECT\_AX     $\vdash \forall P_{\alpha \rightarrow \text{bool}} x. P \ x \Rightarrow P(\varepsilon P)$   
 INFINITY\_AX     $\vdash \exists f_{\text{ind} \rightarrow \text{ind}}. \text{One\_One } f \wedge \neg(\text{Onto } f)$

# Calculus of Communicating Systems (CCS)

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

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

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

Operator	Notation	HOL	HOL (alternative)
nil	<b>0</b>	nil	nil
Rprefix	$a.b.0$	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	$\nu L p$
Constant	$A = a.A$	rec A (prefix a (var A))	rec A (a..var A)

Definition (Guarded sums)

$$\alpha.p + \beta.q \quad \text{or} \quad \sum_i \mu_i.p_i$$

# Structural Operational Semantics (SOS)

## The TRANS relation

defined by 9 *inductive rules*:

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

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

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

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

$$(\text{Prefix}) \frac{}{\mu.p \xrightarrow{\mu} p}$$

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

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

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

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

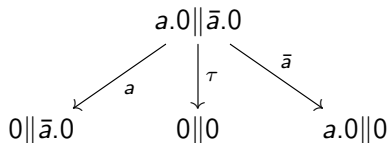
# A decision procedure for CCS transitions

## Decision procedure implemented as ML function

CCS\_TRANS\_CONV : term -> thm

### Example

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



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

$$\begin{aligned}
 \vdash \text{In "a"..nil} \parallel \text{Out "a"..nil} \multimap E &\iff \\
 ((u = \text{In "a"}) \wedge (E = \text{nil} \parallel \text{Out "a"..nil}) \vee & \\
 (u = \text{Out "a"}) \wedge (E = \text{In "a"..nil} \parallel \text{nil})) \vee & \\
 (u = \tau) \wedge (E = \text{nil} \parallel \text{nil}) &
 \end{aligned}$$

# EPS, Weak Transition and Trace

EPS:  $E \xRightarrow{\epsilon} E'$  as Reflexive Transitive Closure (RTC) of " $\xrightarrow{\tau}$ "

$$\text{EPS} = (\lambda E E'. E \xrightarrow{\tau} E')^*$$

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

$$E \xRightarrow{u} E' \iff \exists E_1 E_2. E \xRightarrow{\epsilon} E_1 \wedge E_1 \xrightarrow{u} E_2 \wedge E_2 \xRightarrow{\epsilon} E'$$

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

TRACE = LRTC TRANS

$$\vdash E \xRightarrow{\epsilon} E' \iff \exists xs. \text{TRACE } E \text{ } xs \text{ } E' \wedge \text{NO\_LABEL } xs$$

$$\vdash E \xRightarrow{u} E' \iff$$

$$\exists us.$$

$$\text{TRACE } E \text{ } us \text{ } E' \wedge \neg \text{NULL } us \wedge$$

$$\text{if } u = \tau \text{ then NO\_LABEL } us \text{ else UNIQUE\_LABEL } u \text{ } us$$

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

$$\vdash \text{UNIQUE\_LABEL } u \text{ } L \iff$$

$$\exists L_1 L_2.$$

$$(L_1 \# [u] \# L_2 = L) \wedge$$

$$\neg \exists l. \text{MEM (label } l) \text{ } L_1 \vee \text{MEM (label } l) \text{ } L_2$$



# Bisimulation and bisimulation equivalences

Definition (Strong/weak bisimulations; observational congruence)

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

Definition (Strong/weak equivalence (bisimilarity))

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

Theorem (Property (\*)) (PROPERTY\_STAR))

$$\begin{array}{ccccc}
 P & \sim / \approx & Q & \text{old proof: } P & \sim' & Q \\
 \downarrow \mu & & \downarrow \mu & \downarrow \mu & & \downarrow \mu \\
 \forall P' & \sim / \approx & \exists Q' & \forall P' & \sim & \exists Q'
 \end{array}$$

# The Theory of Congruence for CCS

Semantic Context (multi-hole or no-hole) as an inductive set of  $\lambda$ -functions

```

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

The combination of two contexts is still a context:

$\vdash \text{CONTEXT } c_1 \wedge \text{CONTEXT } c_2 \Rightarrow \text{CONTEXT } (c_1 \circ c_2)$

## Definition (Precongruence and Congruence)

- precongruence  $R \iff \forall x y \text{ ctx}. \text{CONTEXT } \text{ctx} \Rightarrow R x y \Rightarrow R (\text{ctx } x) (\text{ctx } y)$
- congruence  $R \iff \text{equivalence } R \wedge \text{precongruence } R$   
 $\text{equivalence } R \iff \text{reflexive } R \wedge \text{symmetric } R \wedge \text{transitive } R$
- $\sim, \approx^c$  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)

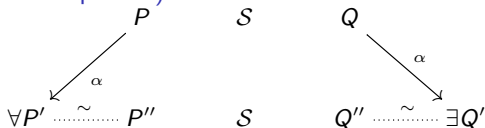
- $X$  is *weakly guarded* in  $E$  if each occurrence of  $X$  is within some subexpression  $\alpha.F$  of  $E$ .
- $X$  is (strongly) *guarded* in  $E$  if each occurrence of  $X$  is within some subexpression  $l.F$  of  $E$  ( $l$  is a visible action).
- $X$  is *sequential* in  $E$  if every subexpression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

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

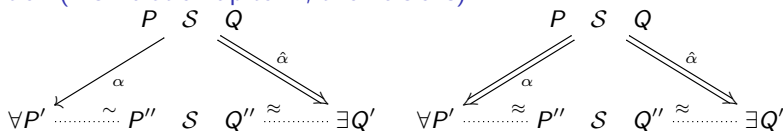
$$\begin{aligned} \vdash \text{WG } E &\Rightarrow \forall P Q. P \sim E P \wedge Q \sim E Q \Rightarrow P \sim Q \\ \vdash \text{SG } E \wedge \text{GSEQ } E &\Rightarrow \forall P Q. P \approx E P \wedge Q \approx E Q \Rightarrow P \approx Q \\ \vdash \text{SG } E \wedge \text{SEQ } E &\Rightarrow \forall P Q. P \approx^c E P \wedge Q \approx^c E Q \Rightarrow P \approx^c Q \end{aligned}$$

# Bisimulation Up-to Techniques

## Definition (Bisimulation up to $\sim$ )



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



## Theorem (Proof techniques using “Bisimulation up to”)

If  $S$  is a “bisimulation up to  $\sim$  (or  $\approx$ )”, then  $S \subseteq \sim$  (or  $\approx$ ):

$\vdash \text{STRONG\_BISIM\_UPTO } Bsm \Rightarrow Bsm \subseteq_r \text{STRONG\_EQUIV}$

$\vdash \text{WEAK\_BISIM\_UPTO } Wbsm \Rightarrow Wbsm \subseteq_r \text{WEAK\_EQUIV}$

# Expansion and Contraction

Definition (Expansion (preorder; 'precongruence'))

$$\begin{array}{ccccc}
 P & \mathcal{R} & Q, & P & Q \\
 \downarrow \mu & & \downarrow \hat{\mu} & \Downarrow \mu & \downarrow \mu \\
 \forall P' & \mathcal{R} & \exists Q' & \exists P' & \mathcal{R} & \forall Q'
 \end{array}$$

$P$  expands  $Q$ , written  $P \succeq_e Q$ , if  $P \mathcal{R} Q$ , for some expansion  $\mathcal{R}$ .

Definition (Contraction (preorder; 'precongruence'))

$$\begin{array}{ccccc}
 P & \mathcal{R} & Q, & P & Q \\
 \downarrow \mu & & \downarrow \hat{\mu} & \Downarrow \hat{\mu} & \downarrow \mu \\
 \forall P' & \mathcal{R} & \exists Q' & \exists P' & \approx & \forall Q'
 \end{array}$$

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

Definition (Preorder and 'precongruence')

`PreOrder`  $R \iff$  reflexive  $R \wedge$  transitive  $R$

`precongruence1`  $R \iff$

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

# Unique Solution of Expansions/Contractions

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

$$\succeq_e \subset \succeq_{\text{bis}} \subset \approx$$

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

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

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

$$\vdash \text{WGS } E \Rightarrow \forall P Q. P \succeq_e E \wedge Q \succeq_e E \Rightarrow P \approx Q$$

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  $\succeq_{\text{bis}}$ .)

# Observational Contractions

## Definition (Observational contraction)

$$\begin{aligned}
 E \succeq_{bis}^c E' &\iff \\
 \forall u. & \\
 (\forall E_1. E -u \rightarrow E_1 \Rightarrow \exists E_2. E' -u \rightarrow E_2 \wedge E_1 \succeq_{bis} E_2) \wedge & \\
 \forall E_2. E' -u \rightarrow E_2 \Rightarrow \exists E_1. E =u \Rightarrow E_1 \wedge E_1 \approx E_2 &
 \end{aligned}$$

## Theorem (Relationships of $\succeq_{bis}^c$ with others)

$$\begin{aligned}
 \succeq_{bis}^c &\subset \succeq_{bis} \subset \approx \\
 \succeq_{bis}^c &\subset \approx^c \subset \approx
 \end{aligned}$$

## Theorem (Properties of $\succeq_{bis}^c$ )

$$\begin{aligned}
 &\vdash \text{PreOrder OBS\_contracts} \\
 &\vdash \text{precongruence OBS\_contracts}
 \end{aligned}$$

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

$$\vdash \text{WG } E \Rightarrow \forall P \ Q. P \succeq_{bis}^c E \wedge Q \succeq_{bis}^c E \Rightarrow P \approx Q$$

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

$$\vdash \text{free\_action } p \wedge \text{free\_action } q \Rightarrow (p \succeq_{bis}^c q \iff \forall r. p + r \succeq_{bis} q + r)$$

# Conclusions

- ① An old formalization of Finitary 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

- ❶ Nesi, M.: *A formalization of the process algebra CCS in high order logic*. University of Cambridge, Computer Laboratory (1992).
- ❷ Sangiorgi, D.: *Equations, contractions, and unique solutions*. ACM SIGPLAN Notices. (2015).
- ❸ Gorrieri, R., Versari, C.: *Introduction to Concurrency Theory*. Springer, Cham (2015).
- ❹ Sangiorgi, D.: *Introduction to Bisimulation and Coinduction*. Cambridge University Press (2011).
- ❺ Milner, R.: *Communication and Concurrency*. Prentice Hall International Series in Computer Science (1989).
- ❻ 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).
- ❼ Sangiorgi, D., Milner, R.: *The problem of “Weak Bisimulation up to”*. CONCUR’92. (1992).
- ❽ 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.