A Formalization of the Process Algebra CCS in HOL4

Chun Tian
Scuola di Scienze, Università di Bologna
chun.tian@studio.unibo.it
Numero di matricola: 0000735539

Abstract. An old formalization of the Process Algebra CCS (no value passing, with explicit relabeling operator) has been ported from HOL88 theorem prover to HOL4 (Kananaskis-11 and later). Transitions between CCS processes are defined by SOS (Structural Operational Semantics) rules, then algebraic laws for strong equivalence (including the expansion law) were proved upon SOS transition rules.

We used HOL4's new co-inductive relation support to re-define strong and weak bisimulation equivalences, and showed that these new definitions are equivalent with the old ones. There's also a decision procedure for automatic detection of CCS transitions. The aim of this project is to provide an up-to-date sound and effective tool to support verifications and reasoning in CCS, and to provide a formal logic basis for further theoretical developments in CCS.

1 Introduction

Concurrency Theory \[1\] has been successfully applied for explaining many concurrency phenomena in Computer Science. In this theory, reactive systems can be modelled as (possibly infinite) directed graphs of some (atomic) states with labeled edges as transitions between these states. Reactive systems defined in this way are called Labeled Transition Systems (LTSs) \[2\].

But it’s usually inconvenient to describe and use (rooted) LTSs when studying the behaviors of reactive systems, especially when the system has infinite number of states. To overcome such difficulties, different compact representations were invented as languages for describing reactive systems. One notable is Milner’s Calculus of Communicating Systems (CCS) \[3\]. Such a language can be considered as process algebras (or syntactic calculus), with LTSs as its underlying semantic models. The possible transitions of processes can be defined by a group of inference rules called Structural Operational Semantics (SOS), then these rules can be used as a set of axioms for proving all of algebraic laws about the equivalence of CCS processes.

There’re usually two methods to study the behaviors of reactive systems. One is through the behavior equivalence checking between the specification and implementation of the same reactive system. Notable behavior equivalences include the strong and (rooted) weak bisimilarities.

The other method is to do model checking directly on the implementation, in which the target properties were usually expressed in $\mu$-Calculus or Hennessy-Milner Logics (HML) \[4\].

Concurrency Theory is a proof-intense area: the contents of related course and textbooks are full of theorems, definitions and proofs, just like mathematics. On the other side, non-trivial algorithms and their optimizations used in model checking software were usually not considered as necessary part of textbooks. However, most of these theorems were only done in pencil-and-paper, i.e. they have no formal proofs, although their correctness rarely raises doubts. When people was publishing new process algebras like new CCS variants, usually there’s no corresponding software environments to actually play with the new theory, nor the theorems presented in the paper were formally verified. We think the main reason is the lack of the formal basis in which fundamental datatypes and relations and theorems were supplied for further extension.

The CCS formalization done by Monica Nesi in 1992-1995 was a success. The work was ever considered as a major success story \[5\] of HOL theorem prover, not to further mention that both CCS and HOL (derived from Edinburgh LCF) were derived from the initial pioneering work by the same scholar, Robin Milner. After more than 20 years, HOL88 and HOL90 were replaced

---

1 A formalization of HML was part of the original work by Prof. Monica Nesi, but it’s not included in this project, because the related HOL88 scripts were not sent to the author during the porting work. The porting of HML formalization is planed in futher projects.
by HOL4 (latest release is called Kananaskis-11); even the underlying programming language for writing HOL has changed from Classic ML (defined on top of Common Lisp) to Standard ML. But the CCS formalization seems being forgotten and to the best of our knowledge there’s no other CCS formalizations done in HOL\textsuperscript{2} and other theorem provers (e.g. Coq). New variants of concurrency theory and new theorems kept being introduced, but rarely they were formally verified. This is a rather unacceptable situation from the view of the author. As a little contributions to adademic, the author has spent several months porting all the old code (provided by Prof. Nesi) to latest HOL4 with some improvements, new theorems, also with new features (e.g. co-inductive relation) used as alternative ways to define certain important concepts (e.g. bisimulation equivalence) in concurrency theory.

Currently this work contains about 6000 lines of proof scripts in Standard ML\textsuperscript{3}, with examples. About 170 theorems were proved (most of them were part of the old project), including the Expansion Law for strong equivalence. There’s also a ML function for computing CCS transitions from any given CCS process, and the output is a theorem which completely characterizes its transitions. Programs written in this way can be seen as kind of trusted computing, in the sense that, whenever the computation is terminated, the result must be correct, since it’s a proven theorem. This prevented any doubts from the possible bugs existed in the software. For instance, if there’s a hiding bug in Concurrency Workbench and have caused two complicated CCS processes being considered as equivalent but actually they’re not, there’s almost no way to know, except for comparing the results from another different software. Of course, any program including our ML functions could have bugs, thus we’re not sure if the program can always give the result for any valid input, but as long as it does have a result, the result MUST be true (since it’s a theorem) thus can be fully trusted. We think this is a major advantage to use theorem provers in place of usual programming languages (e.g. C, Java or OCaml) for implementing software verification tools, as reliability is more important than other factors.

2 Background

Back to one year ago (May 2016), soon after the author has just attended his 2nd-year course MODELLI E SISTEMI CONCORRENTI (Concurrent Models and Systems) of Computer Science (Informatica) at University of Bologna, he was looking on Internet for connections between CCS and the HOL theorem prover (HOL4) that he just began to learn. At that time, the author didn’t know how to use HOL4 yet, but he liked it and the whole formal methods area very much.

Fortunately, the author found a paper \cite{4} about the history of HOL theorem prover, in which Mike Gordon wrote:

\begin{quote}
I had been impressed by how the Expansion Theorem of Milner’s Calculus of Communicating Systems (CCS) \cite{7} enabled a direct description of the behaviour of a composite agent to be calculated from the parallel composition of its individual components. 

... Incidently, not only was CCS’s Expansion Theorem an inspirational stepping stone from LCF via LSM to HOL, but recently things have come ‘full circle’ and Monica Nesi has used HOL to provide proof support for CCS, including the mechanisation of the Expansion Theorem \cite{8}.
\end{quote}

This is how the author found the paper of Prof. Monica Nesi and some deep connections between LCF (Robin Milner), HOL (Mike Gordon) and CCS (again Robin Milner!). Then on May 24, 2016, the author posted on HOL’s mailing list asking for the proof scripts code mentioned in the paper. Surprisingly Mike Gordon replied that mail with the following contents:

\begin{quote}
“Hi,

I don’t have Monica’s email address, but I do have her husband’s, so I’ve forwarded your email to him.

\textsuperscript{2} Except that Prof. Monica Nesi further published her formalizations of value-passing CCS in 1994 \cite{5} and 1997 \cite{6}.

\textsuperscript{3} Currently it’s stored in GitHub: \url{https://github.com/binghe/informatica-public/tree/master/CCS} and recently these code has entered into HOL official code base in its "examples/CCS" folder.
\end{quote}
In later mails in the same day, Mike Gordon also told the author that, “Monica Nesi is also in Italy: she works at the University of L'Aquila (unless she has moved recently)”.

Just one day later, on May 25, 2016, Professor Nesi sent an email to the author:

“Dear student,
I am Monica Nesi (a "she" :-)) from University of L’Aquila. My HOL scripts on CCS formalization are not available on Internet, but just give me time to find back my files and I will send them to you. I haven’t been working on that after my PhD, already more than 20 years ago, and I am pleased that someone might be interested in having a look and maybe do something similar in HOL4.
I have some deadlines to meet by Friday. I will come back to you asap.
Best regards, Monica Nesi”

And finally on June 7, the author received about 4500 lines of HOL88 proof scripts in 21 disk files. Here is a list of these files:

- syntax.ml
- syntax_aux.ml
- aux_fun.ml
- basic_rule_tac.ml
- opsem.ml
- runM.ml
- StrongEQ/basic_conv_tac.ml
- StrongEQ/basic_fun.ml
- StrongEQ/par_strong_laws.ml
- StrongEQ/parallel_new.ml
- StrongEQ/rec_strong_laws.ml
- StrongEQ/relab_strong_laws.ml
- StrongEQ/restr_strong_laws.ml
- StrongEQ/strong_par_conv_new.ml
- StrongEQ/strong_rec_conv.ml
- StrongEQ/strong_relab_conv.ml
- StrongEQ/strong_restr_conv.ml
- StrongEQ/strong_sem.ml
- StrongEQ/strong_sum_conv.ml
- StrongEQ/strong_tac.ml
- StrongEQ/sum_strong_laws.ml

These include basic CCS definitions, proofs for all algebraic laws (including the expansion law) for strong equivalence, and a complicated ML function (in runM.ml) for automatically computing the transitions from a given CCS process.

The author saved these code and continued learning HOL4. Finally, starting from Jan 2017, the author was able to read proof scripts written in HOL4 and prove some new theorems in it. With several theorem proving projects doing in parallel, and kindly help from people of HOL community (Thomas Tuerk, Michael Norrish, Ramana Kumar, etc.), the author quickly improved his proof skills (in HOL4) and programing skills (in Standard ML). With a Classic ML document found on Internet, porting Classic ML code into Standard ML seems quite straightforward.

The porting process of old HOL88 proof scripts is not very difficult: the underlying HOL logic didn’t change at all, so is the name of almost all tacticals and other ML functions. So basically what the author did is the following:

1. Copy a piece of ML code from old files into current HOL proof script;
2. Change the grammar from Classic ML to Standard ML;
3. Replay the proof in HOL4’s interactive proof manager;

I should have really searched on Internet first...
4. Make necessary changes for those tacticals which has slightly changed their semantics in HOL4;
5. Save the working proof in forms of HOL \texttt{store_thm} function calls and go to next theorem.

Beside those small new inventions and some new ways to define old concepts (e.g. strong equivalence), the major efforts in this project were lots of time spent on carefully replaying each of the proofs: most proofs on strong laws were quite long (usually made of hundreds of tacticals, in four or five levels). In the time of HOL88, there's NO automatic first-order proof searching tools like Mason and Metis, nor the Q method, thus all proofs were done manually including each small steps involving only bool theory and higher order logic (beta-conversion, etc.). And whatever any literal terms are mentioned in the proof, full type info must be given manually, this makes the proof longer, but each step is very clear.

On the other side, Prof. Roberto Gorrieri was informed since the very beginning. He agreed that this project could be used as part of the exam. Thus the current paper (as a project report) is actually the the exam paper for the author’s \textit{MODELLI E SISTEMI CONCORRENTI} (\textit{Concurrent Models and Systems}) course.

\section{A Formalization of CCS in HOL4}

The precise class of CCS we have formalized here, is \textit{CCS}^{rel}, the Finitary CCS with explicit relabeling operator\footnote{The relabeling operator in core CCS syntax is not necessary, because it’s possible to define the \textit{Syntactic relabeling} as a recursive function on top of other CCS operators. But we think having native relabeling facility makes many things easier.}

\subsection{Labels and Actions}

In most literature, the concept \textit{Action} was usually defined as the union of a countable set of input actions $\mathcal{L}$ and output actions (co-actions) $\overline{\mathcal{L}}$ and a special invisible action $\tau \notin \mathcal{L} \cup \overline{\mathcal{L}}$. Actions are also called labels when LTS is considered.

In the formalization of CCS, however, it’s better to have two distinct types: the type \textit{Label} is the union of input and output (visible) actions, and the data type \textit{Action} is the union of all visible and invisible actions. This is better because certain formulae and constructors in CCS doesn’t accept $\tau$ as valid actions, e.g. the restriction operator of CCS. Thus, having two distinct types it’s possible to make sure all CCS terms constructed from all possible values of their parameters are valid. Thus we have defined the following two data types in HOL:

\begin{verbatim}
Datatype 'Label = name string | coname string';
Datatype 'Action = tau | label Label';
\end{verbatim}

Noticed that, the type \textit{Action} contains the type \textit{Label}, but they’re not in sub-type relation (there’s no such support in HOL): for operators accepting \textit{Action}, if a term of \textit{Label} were used, will result into type mismatch.

Here we have used the string type provided in HOL’s \texttt{stringTheory}, thus the distinction and injectivity of the type \textit{Label} also depends on the distinction and injectivity of type \texttt{string} proved in HOL’s \texttt{stringTheory}. In theory, it’s possible to use type variables instead of the string type and allow arbitrary types being used as labels, however we found no such needs so far.

Thus, an input action $a$ must be represented as “In “a” in HOL, while a output action (co-action) $\overline{a}$ must be represented as “Out “a””. Instead, the invisible action can be written either in ASCII form \texttt{tau} or Greek letter $\tau$ in Unicode. This makes literature actions quite long, and we have defined the following syntactic sugars\footnote{This new solution based overloading was suggested by Michael Norrish.} as compat representations of actions (not part of the original CCS work):

\begin{verbatim}
val _ = overload_on ("In", "\a. label (name a)"');
val _ = overload_on ("Out", "\a. label (coname a)"');
\end{verbatim}

As the results, whenever literal visible actions will appear in above compact forms automatically.
The main operation on the types Label and Action is COMPL which gets their complements: (for convinence we also define the complement of \( \tau \) as itself)

\[
\forall s. \text{COMPL (name } s\text{)} = \text{name } s \land \forall l. \text{COMPL (label } l\text{)} = \text{label (COMPL } l\text{)} \land (\text{COMPL } \tau = \tau)
\]

As we know Label and Action are different types, the COMPL operator on them are actually over-loaded operator of COMPL\_LAB and COMPL\_ACT, the complement operator for Label and Action.

The key theorem about Label says that, doing complements twice for the same label gets the label itself:

\[
\text{COMPL\_COMPL\_LAB:} \quad \forall l. \text{COMPL (COMPL } l\text{)} = l
\]

There’s also a similar theorem for the double-complements of Action.

The following table listed the notation of various actions, with notations from \textit{Currency Workbench} [10] compared:

| Action      | notation | CWB | HOL (ASCII)   | HOL (compact form) |
|-------------|----------|-----|---------------|-------------------|
| internal    | \( \tau \) | tau | tau           | \( \tau \)          |
| input       | \( a \)  | a   | label (name "a") | In “a”             |
| output      | \( \bar{a} \) | \('a\) | label (coname "a") | Out “a”           |

### 3.2 Relabeling

In the literature, Relabeling is usually defined as an unary substitution operator: 
\([b/a] \) takes a unary substitution \( b/a \) (hence, \( a \neq b \)), and a process \( p \) to construct a new process \( p[b/a] \), whose semantics is that of \( p \), where action \( a(\bar{a}) \) is turned into \( b(\bar{b}) \). And multi-label relabeling can be done by appending more unary substitution operators to the new process. The order of multiple relabellings is important, especially when new labels introduced in previous relabeling operation were further relabeled.

In our formalization, instead we support multi-label relabeling in one opearation, and instead of using a list of substitutions, we have defined a new fundamental type in called \texttt{Relabeling}.

\texttt{Relabeling} is a abstract type which is bijected into a subset of function of type \texttt{Label -> Label}, which is called the \textit{representation} of the type \texttt{Relabeling}. Not all functions of type \texttt{Label -> Label} are valid representations of \texttt{Relabeling}, but only functions which satisfy the following property:

\[
\forall s. f (\text{name } s) = \text{COMPL } (f (\text{name } s))
\]

Noticed that, any identify function of type \texttt{Label -> Label} also satisfy above property. Thus, beside specific substitutions that we want, all relabeling functions must be able to handle all other labels too (just return the same label as input). (As we’ll see later, such requirements could reduce the two rules for relabelling into just one).

But usually it’s more convenient to represent relabeling functions as a list of substitutions of type \((\text{Label} \times \text{Label}) \text{ list}\). The operator \texttt{RELAB} can be used to define such a relabeling function. For instance, the term \texttt{RELAB \{(name "b",name "a"); (name "d",name "c")\}} can be used in place of a relabeling operator \([b/a,d/c] \), because its type is \texttt{Relabeling}. And it must be understood that, all relabeling functions are total functions: for all other labels except \( a \) and \( c \), the substitution will be themselves (another way to express “no relabeling”).

Finally, have the relabeling facility defined as a multi-label relabeling function and part of CCS syntax, we can completely avoid the complexity of the Syntactic Substitution (c.f. p.171 of [1]).

---

1 The idea of defining relabeling as type bijections belongs to Prof. Monica Nesi. The author did nothing but the porting work from HOL88 to HOL4. Fortunately the related API didn’t change at all.
which has a quite complicated recursive definition\(^5\) and heavily depends on some other recursive
functions like \(f_n(\cdot)\) (free names) and \(b_n(\cdot)\) (bound names) for CCS processes (in our project, these
functions are not included nor needed).

### 3.3 CCS processes and operators

The type CCS is defined as an inductive data type: (thus it must be finitary)

\[
\text{val } \_ = \text{Datatype } \text{CCS} = \text{nil} \\
\quad \mid \text{var string} \\
\quad \mid \text{prefix Action CCS} \\
\quad \mid \text{sum CCS CCS} \\
\quad \mid \text{par CCS CCS} \\
\quad \mid \text{restr (Label set) CCS} \\
\quad \mid \text{relab CCS Relabeling} \\
\quad \mid \text{rec string CCS}';
\]

In HOL4, we have added some minimal grammar support, to represent CCS processes in
more compact forms (not available in HOL88). The following table listed the notation of typical
CCS processes and major operators supported by above definition, with notations from Currency
Workbench \(^{10}\) compared:

| op name                  | notation | CWB         | HOL (ASCII) | HOL (compact) |
|--------------------------|----------|-------------|-------------|---------------|
| Deadlock (nil)           | 0        | 0           | nil         | nil           |
| Prefix                   | a.0      | a.0         | prefix (label (name "a")) nil | In “a”..nil |
| Sum                      | \(p + q\) | \(p + q\)   | sum \(p q\) | \(p + q\)     |
| Parallel                 | \(p|q\)  | \(p | q\)    | par \(p q\) | \(p || q\)    |
| Restriction of action    | \((\nu a)p\) | \(p \setminus a\) | nu \{"a"\} \(p\) | \(\nu "a"\) \(p\) |
| Restriction of actions   | \((\nu L)p\) | \(p \setminus L\) | restr L \(p\) | \(\nu L\) \(p\) |

For Relabeling, as we described in the last section, to express \(p[b/a]\), it must be written as
\(\text{relab } p\ (\text{RELAB } [(\text{name }"b", \text{name }"a")])\), which is a little long.

For CCS processes defined by one or more constants, in our formalization in HOL4, all constants
must be written into single term. (This is necessary for theorem proving, because otherwise there’s
no way to store all information into single variable in CCS-related theorems) The syntax for
defining new constants is \texttt{rec} and the syntax to actually use a constant is \texttt{var}. To see how these
operators are actually used, consider the following CCS process (the famous coffee machine model
from \cite{1}):

\[
VM \overset{\text{def}}{=} \text{coin.} \ (\text{ask-esp.} VM_1 + \text{ask-am.} VM_2)
\]

\[
VM_1 \overset{\text{def}}{=} \text{esp-coffee.} VM
\]

\[
VM_2 \overset{\text{def}}{=} \text{am-coffee.} VM
\]

In our formalization in HOL4, the above CCS process can be represented as the following single
term:

```
"\text{rec } "VM"

\text{(In } "\text{coin}"

\text{(In } "\text{ask-esp}" \text{} \text{(rec } "VM1" \text{} \text{(Out } "\text{esp-coffee}"\text{} \text{} \text{var } "VM")\text{)}) + \\
\text{(In } "\text{ask-am}" \text{} \text{(rec } "VM2" \text{} \text{(Out } "\text{am-coffee}"\text{} \text{} \text{var } "VM")\text{)})"
```

That is, for the first time a new constant appears, use \texttt{rec} with the name of constants as string
to “declare” it; when any constant appears again, use \texttt{var} to access it.

Finally, although not part of the formal definition, the \texttt{if-then-else} construct from value-
passing CCS is automatically supported by HOL. This is because, for any boolean value \(b\) and two

---

\(^5\) However, syntactic relabeling is still considered as an “economic” way of doing relabeling, because having
one native CCS operator will also introduce the corresponding SOS inference rules and equivalence laws.
terms \( t_1 \) and \( t_2 \) of type \( \alpha \), the term \( \text{if } b \text{ then } t_1 \text{ else } t_2 \) has also the type \( \alpha \). Thus the conditional term can legally appears inside other CCS processes as a sub-process. We’ll see in next section that it’s necessary for handling transitions of CCS processes containing constants.

### 3.4 CCS transitions and SOS inference rules

The transitions of CCS processes were defined by the following Structural Operational Semantics (SOS for short) rules:

1. **(Perf)**
   
   \[
   \mu. p \xrightarrow{\mu} p
   \]

2. **(Rec)**
   
   \[
   \text{rec } x.q \xrightarrow{\mu} r
   \]

3. **(Sum 1)**
   
   \[
   p \xrightarrow{\mu} p' \\
   p + q \xrightarrow{\mu} p'
   \]

4. **(Sum 2)**
   
   \[
   q \xrightarrow{\mu} q' \\
   p + q \xrightarrow{\mu} q'
   \]

5. **(Par 1)**
   
   \[
   p \xrightarrow{\mu} p' \\
   p|q \xrightarrow{\mu} p'|q
   \]

6. **(Par 2)**
   
   \[
   q \xrightarrow{\mu} q' \\
   p|q \xrightarrow{\mu} p|q'
   \]

7. **(Par 3)**
   
   \[
   p \xrightarrow{\mu} p' \\
   (\nu a)p \xrightarrow{\mu} (\nu a)p' \\
   \mu \neq a, \bar{a}
   \]

Besides, we have a rule for relabeling:

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

In [1], the rule Par 3 is called “Com” (rule of communication), and the rule “Rec” (in a different form based on separated agent definitions) is also called “Cons” (rule of constants). (Here we have preserved the rule names in the HOL88 work, because it’s easier to locate for their names in the proof scripts.)

From the view of theorem prover (or just first-order logic), these inference rules are nothing but an inductive definition on 3-ary relation \( \text{TRANS} \) (with compact representation \(-\rightarrow\) of type \( \text{CCS} \rightarrow \text{Action} \rightarrow \text{CCS} \rightarrow \text{bool} \), generated by HOL4’s function \( \text{Hol_reln} \)). Then we break them into separated theorems as primitive inference rules.

**PREFIX**: \( \vdash u_..E \xrightarrow{---u} E \)

**REC**: \( \vdash \text{CCS_Subst } E \xrightarrow{(\text{rec } X E) X \xrightarrow{---u} E_1 \Rightarrow \text{rec } X E \xrightarrow{---u} E_1} \)

**SUM1**: \( \vdash E \xrightarrow{---u} E_1 \Rightarrow E + E' \xrightarrow{---u} E_1 \)

**SUM2**: \( \vdash E \xrightarrow{---u} E_1 \Rightarrow E' + E \xrightarrow{---u} E_1 \)

**PAR1**: \( \vdash E \xrightarrow{---u} E_1 \Rightarrow E | E' \xrightarrow{---u} E_1 | E' \)

**PAR2**: \( \vdash E \xrightarrow{---u} E_1 \Rightarrow E' | E \xrightarrow{---u} E' | E_1 \)

**PAR3**: \( \vdash E \xrightarrow{---label \ l} E_1 \wedge E' \xrightarrow{---label \ (\text{COMPL } l)} E_2 \Rightarrow E | E' \xrightarrow{---\tau} E_1 | E_2 \)

**RESTR**: \( \vdash E \xrightarrow{---u} E' \wedge ((u = \tau) \lor (u = \text{label } l) \wedge l \notin L \wedge \text{COMPL } l \notin L) \Rightarrow \nu L E \xrightarrow{---u} \nu L E' \)

**RELAB**: \( \vdash E \xrightarrow{---u} E' \Rightarrow \text{relab } E \ \text{rf} \xrightarrow{---\text{relabel } \text{rf} \ u} \Rightarrow \text{relab } E' \ \text{rf} \)

---

9 The other similar benefit from HOL is the let-in binding construct, but so far it’s not well supported.

10 They’re considered as the axioms in our logic system, however they’re not defined directly as axioms. HOL makes sure in such cases the logic system is still consistent.
Noted that, in the rule \textsc{rec}, a recursive function \texttt{CCS/Subst} was used. It has the following definition which depends on the conditional clause (if \texttt{if} .. then .. else ..):

\[ \left\{ \begin{array} {l}
E' \rightarrow a_0 \rightarrow a_2 \iff \left( (a_0 = a_1 \rightarrow a_2) \equiv (a_0 \equiv \texttt{label} \ l) \land l \notin L \land \texttt{COMPL} l \notin L \right) \\
\end{array} \right. \]

Here are some results proved using above “cases” theorem (i.e. they cannot be proved with only the SOS inference rules):

\begin{itemize}
  \item \texttt{NIL_NO_TRANS}:
    \[ \vdash \neg (\texttt{nil} \rightarrow \rightarrow E) \]
  \item \texttt{TRANS_IMP_NO_NIL}:
    \[ \vdash E \rightarrow \rightarrow E' \rightarrow \rightarrow E' \neq \texttt{nil} \]
  \item \texttt{TRANS_SUM_EQ}:
    \[ \vdash E + E' \rightarrow \rightarrow E'' \equiv \rightarrow \rightarrow E' \land \rightarrow \rightarrow E'' \land \rightarrow \rightarrow E'' \rightarrow \rightarrow E'' \]
  \item \texttt{TRANS_PAR_EQ}:
    \[ \vdash E \rightarrow \rightarrow E' \rightarrow \rightarrow E'' \equiv \left( \begin{array} {l}
(\exists E_1. \ E'' = \rightarrow \rightarrow E' \rightarrow \rightarrow E_1) \lor \\
(\exists E_1. \ E'' = \rightarrow \rightarrow E' \lor \rightarrow \rightarrow E_1) \lor \\
\end{array} \right) \]
\end{itemize}
Michael Norrish has different opinion with the following argument: “Infinite sums and parallels would not require a coinductive definition. Coinductive definitions give you “infinite depth”. Infinite sums and parallels would only require infinite breadth.” However, a CCS transition which is inside the fixed point but outside of the least fixed point, is yet to be found to support this argument.

\[(u = \tau) \land (E'' = E_1 \parallel E_2) \land E \dashv \text{label } \rightarrow E_1 \land E' \dashv \text{label } (\text{COMPL } l) \rightarrow E_2\]

\[\text{TRANS\\_RESTR\\_EQ}:
\vdash \nu L E \dashv u \rightarrow E' \iff
\exists E'' l.
(E' = \nu L E'') \land E \dashv u \rightarrow E'' \land
((u = \tau) \lor (u = \text{label } l) \land l \notin L \land \text{COMPL } l \notin L)\]

Finally, it’s worth to mention that, the following induction theorem generated by Hol\_reln was never used (nor needed) in this project:

\[\text{TRANS\\_ind}:
\vdash (\forall a. \text{TRANS'} (u.E) \ u E) \land
(\forall E a E_l E_1. \text{TRANS'} E a E_1 \Rightarrow \text{TRANS'} (E + E') \ a E_1) \land
(\forall E a E_1 E_2. \text{TRANS'} E a E_1 \Rightarrow \text{TRANS'} (E' + E) \ a E_1) \land
(\forall E a E_1 E_2. \text{TRANS'} E a E_1 \Rightarrow \text{TRANS'} (E || E') \ u (E_1 || E_2)) \land
(\forall E a E_1 E_2. \text{TRANS'} E a E_1 \Rightarrow \text{TRANS'} (E' || E) \ u (E' || E_1)) \land
(\forall E l E_1 E_2. \text{TRANS'} (\text{label } l) E_1 \land \text{TRANS'} E' \ (\text{label } (\text{COMPL } l)) E_2 \Rightarrow
\text{TRANS'} (E || E') \ (\nu l E) (E_1 || E_2)) \land
(\forall E a E_1. \text{TRANS'} E a E' \land
((u = \tau) \lor (u = \text{label } l) \land l \notin L \land \text{COMPL } l \notin L) \Rightarrow
\text{TRANS'} (\nu L E) u (u = \text{label } E')) \land
(\forall E a E' \ \text{rf}. \text{TRANS'} E a E' \Rightarrow
\text{TRANS'} (\text{relab } E \ \text{rf}) (\text{relabel } \text{rf} \ u) (\text{relab } E' \ \text{rf})) \land
(\forall E a X E_1. \text{TRANS'} (\text{CCS\_Subst } E (\text{rec } X E) X) u E_1 \Rightarrow
\text{TRANS'} (\text{rec } X E) u E_1) \Rightarrow
\forall a_0 a_1 a_2. a_0 \rightarrow a_1 \rightarrow a_2 \Rightarrow \text{TRANS'} a_0 a_1 a_2\]

The purpose of above induction theorem is to assert the transition relation to the least fixed point of the function generated from SOS inference rules. On the other side, if we define a co-inductive relation from the same SOS rules, we get the same rules and “cases” theorems, and the only difference is another co-induction theorem in place of above induction theorem. This seems indicating that, the least fixed point coincides with greatest fixed point for Finitary CCS. This result is never formally proved, but both Prof. Gorrieri and the author believe it’s true. (However, Prof. Gorrieri thinks it’s NOT appropriate to use co-induction in this case, unless infinite sums and parallels were defined as part of CCS syntax)

Also, we have noticed that, to prove certain CCS transition is impossible, it’s enough to use just the above “cases” theorem. Since the CCS datatype itself is inductively defined, therefore already Finitary, all those invalid transitions seems must be outside of the fixed point, in another word, they’re even outside of the greatest fixed point. If one day we had changed the definition of CCS datatype to allow infinite sums and parallels, the SOS inference rules should still work, but the transition relation should be then defined co-inductively, to allow valid transitions for both finitary and infinitary CCS processes.\[^{1}\]

\[^{1}\] Michael Norrish has different opinion with the following argument: “Infinite sums and parallels would not require a coinductive definition. Coinductive definitions give you “infinite depth”. Infinite sums and parallels would only require infinite breadth.” However, a CCS transition which is inside the fixed point but outside of the least fixed point, is yet to be found to support this argument.
3.5 Decision procedure for CCS transitions

It’s possible to use SOS inference rules and theorems derived from them for proving theorems about the transitions between any two CCS processes. However, what’s more useful is the decision procedure which automatically decide all possible transitions and formally prove them.

For any CCS process, there is a decision procedure as a recursive function, which can completely decide all its possible (one-step) transitions. In HOL, this decision procedure can be implemented as a normal Standard ML function $\text{CCS\_TRANS\_CONV}$ of type $\text{term} \rightarrow \text{theorem}$, the returned theorem fully characterize the possible transitions of the input CCS process.

For instance, we know that the process $(a\cdot \bar{a}.0) | (\bar{a}.0)$ have three possible transitions:

1. $(a\cdot \bar{a}.0) | (\bar{a}.0) \rightarrow (0\cdot \bar{a}.0)$;
2. $(a\cdot \bar{a}.0) \rightarrow (a.0)$;
3. $(a\cdot \bar{a}.0) \rightarrow (0\cdot 0)$.

To completely decide all possible transitions, if done manually, the following work should be done:

1. Prove there exists transitions from $(a\cdot \bar{a}.0)$ (optionally);
2. Prove each of above three transitions using SOS inference rules;
3. Prove there’s no other transitions, using the “cases” theorems generated from the $\text{TRANS}$ relation.

Here are the related theorems manually proved:

```
> r1_has_trans:
  ⊢ ∃ l G. In "a"..nil || Out "a"..nil --l-> G
> r1_trans_1:
  ⊢ In "a"..nil || Out "a"..nil --In "a"-> nil || Out "a"..nil
> r1_trans_2:
  ⊢ In "a"..nil || Out "a"..nil --Out "a"-> In "a"..nil || nil
> r1_trans_3:
  ⊢ In "a"..nil || Out "a"..nil --τ-> nil || nil
> r1_has_no_other_trans:
  ⊢ ¬∃ l G. ¬((G = nil || Out "a"..nil) ∧ (l = In "a") ∨ (G = In "a"..nil || nil) ∧ (l = Out "a") ∨ (G = nil || nil) ∧ (l = τ)) ∧ In "a"..nil || Out "a"..nil --l-> G
```

Instead, if we use the function $\text{CCS\_TRANS\_CONV}$ with the root process:

```
> CCS_TRANS_CONV
  "par (prefix (label (name "a")) nil)
  (prefix (label (coname "a")) nil)"
```

As the result, the following theorem is returned:

```
> ex_A: ⊢ In "a"..nil || Out "a"..nil --u-> E ⇐⇒
  ((u = In "a") ∧ (E = nil || Out "a"..nil)) ∨
  (u = Out "a") ∧ (E = In "a"..nil || nil)) ∨
  (u = τ) ∧ (E = nil || nil)
```

From this theorem, we can see there’re only three possible transitions and there’s no others. Therefore it contains all information expressed by previous manually proved 5 theorems (in theory we can also try to manually prove this single theorem, but it’s not easy since the steps required will be at least the sum of all previous proofs).

As a further example, if we put a restriction on label “a” and check the process $(\nu a)(a.0|\bar{a}.0)$ instead, there will be only one possible transition:

```
> ex_B: ⊢ ν "a" (In "a"..nil || Out "a"..nil) --u-> E ⇐⇒
  (u = τ) ∧ (E = ν "a" (nil || nil))
```
It’s possible to extract a list of possible transitions together with the actions, into a list. This work can be done automatically by the function \texttt{strip\_trans}. Finally, if both the theorem and the list of transitions are needed, the function \texttt{CCS\_TRANS} and its compact-form variant \texttt{CCS\_TRANS’} can be used. For the previous example process \((a.0|\bar{a}.0)\), calling \texttt{CCS\_TRANS’} on it in HOL’s interactive environment has the following results:

\[
> \text{CCS\_TRANS ‘‘In “a”..nil || Out “a”..nil’’; val it =}
\]

\[
(|- !u E.
In “a”..nil || Out “a”..nil --u-> E <=>
\((u = \text{In “a”}) \lor (E = \text{nil || Out “a”..nil}) \lor
\((u = \text{Out “a”}) \lor (E = \text{In “a”..nil || nil})) \lor
\((u = \text{tau}) \lor (E = \text{nil || nil}),
\[(\text{‘‘In “a”’’},
\text{‘‘Out “a”’’},
\text{‘‘In “a”..nil || nil’’}),
\text{‘‘Out “a”’’},
\text{‘‘In “a”..nil || nil’’}),
\text{‘‘tau’’},
\text{‘‘nil || nil’’})]:
\text{thm * (term * term) list}
\]

The main function \texttt{CCS\_TRANS\_CONV} is implemented in about 500 lines of Standard ML code, and it depends on many customized tactics, and functions to access the internal structure of CCS related theorem and terms. We have tried our best to make sure the correctness of this function, but certain bugs are still inevitable. However, since it’s implemented in theorem prover, and the return value of this function is a theorem, what we can guarantee is the following fact:

Whenever the function terminates with a theorem returned, as long as the theorem has “correct” forms, the CCS transitions indicated in the returned theorem is indeed all possible transitions from the input process. No matter if there’re bugs in our program.

In another words, any remain bug in the program can only stop the whole function for returning a result, but as long as the result is returned, it cannot be wrong (i.e. a fake theorem). This sounds like a different kind of trusted computing than normal sense. In general, for any algorithm implemented in any normal programming languages, since the output is just a primitive value or data structure which can be arbitrary constructed or changed due to potential bugs in the implementation, the only way to trust these results, is to have the entire program carefully modelled and verified. But in our case, the Standard ML program code is not verified, but the result (once appears) can still be fully trusted, isn’t this amazing?

### 3.6 Strong bisimulation, strong equivalence and co-induction

The concept of \textit{Bisimulation} (and \textit{Bisimulation Equivalence} with variants) stands at the central position of Concurrency Theory, as one major approach of model checking is to check the bisimulation equivalence between the specification and implementation of the same reactive system. Besides, it’s well known that, Strong Equivalence as a relation, must be defined \textit{co-inductively}. (And in fact, strong equivalence is one of the most well-studied co-inductive relation in computer science. \cite{12}) In this section, we study the definition of strong and weak bisimulation and (bisimulation) equivalences, and their possible formalizations in HOL.

Recall the standard definition of strong bisimulation and strong equivalence (c.f. p.43 of \cite{11}):

**Definition 1.** ((Strong) bisimulation and (strong) bisimulation equivalence) Let \(TS = (Q,A,\rightarrow)\) be a transition system. A bisimulation is a relation \(R \subseteq Q \times Q\) such that \(R\) and its inverse \(R^{-1}\) are both simulation relations. More explicitly, a bisimulation is a relation \(R\) such that if \((q_1,q_2) \in R\) then for all \(\mu \in A\).

\cite{11} If the internal proof constructed in the function is wrong, then the function won’t return a theorem. But if the function successfully returns a theorem, the proof for this theorem must be correct, because there’s no other way to return a theorem except for correctly proving it in HOL theorem prover.
Whenever ASCII-based HOL proof scripts were directly pasted, please understand the letter “∀” as ∀, and “∃” as ∃. They’re part of HOL’s term syntax. [13]

Two states \( q \) and \( q' \) are bisimilar (or bisimulation equivalent), denoted \( q \sim q' \), if there exists a bisimulation \( R \) such that \( (q, q') \in R \).

Noticed that, although above definition is expressed in LTS, it’s also applicable to CCS in which each process has the semantic model as a rooted LTS. Given the fact that, all states involved in above definition are target states of direct or indirect transition of the initial pair of states, above definition can be directly used for CCS.

In HOL88, there’s no way to define co-inductive relation directly. However, it’s possible to follow above definition literally and define bisimulation first, then define the bisimulation equivalence on top of bisimulation. Here are the definitions translated from HOL88 to HOL4:

\[
\vdash \text{STRONG_BISIM } \neg \Rightarrow
\]

\[
\forall E \ E'.
\]

\[
\text{Bsm } E \ E' \Rightarrow
\]

\[
\forall u.
\]

\[
(\forall E_1. \ E \ --u-> E_1 \Rightarrow \exists E_2. \ E' \ --u-> E_2 \land \text{Bsm } E_1 \ E_2) \land
\]

\[
(\forall E_2. \ E' \ --u-> E_2 \Rightarrow \exists E_1. \ E \ --u-> E_1 \land \text{Bsm } E_1 \ E_2
\]

\[
\vdash E \sim E' \iff \exists \text{Bsm}. \ \text{Bsm } E \ E' \land \text{STRONG_BISIM } \text{Bsm}
\]

From the second definition, we can see that, \( q \sim q' \) if there exists a bisimulation containing the pair \( (q, q') \). This means that \( \sim \) is the union of all bisimulations, i.e.,

\[
\sim \ = \bigcup \{ R \subset Q \times Q : R \text{ is a bisimulation} \}.
\]

In HOL4, the last formula can be proved with the notion “bigunion” in HOL’s pred_setTheory used. The only thing needed from CCS is above definition of strong equivalence (the definition of strong bisimulation is not needed at all):

\[
\vdash \text{STRONG_EQIV } = \text{CURRY } (\text{BIGUNION } \{ \text{UNCURRY } R \ | \ \text{STRONG_BISIM } R \})
\]

However, this theorem is not very useful for proving other results. And the use of CURRY and UNCURRY is to transform the relation from types between CCS -> CCS -> bool and CCS × CCS -> bool, since relations in HOL cannot be treated directly as mathematical sets.

The other way to define strong bisimulation equivalence is through the fixed point of the following function \( F \): (c.f. p.72 of [1])

**Definition 2.** Given an LTS \((Q, A, \rightarrow)\), the function \( F \) : \( \wp(Q \times Q) \rightarrow \wp(Q \times Q) \) (i.e., a transformer of binary relations over \( Q \)) is defined as follows. If \( R \subset Q \times Q \), then \( (q_1, q_2) \in F(R) \) if and only if for all \( \mu \in A \)

\[
- \forall q'_1 \text{ such that } q_1 \xrightarrow{\mu} q'_1, \exists q'_2 \text{ such that } q_2 \xrightarrow{\mu} q'_2 \text{ and } (q'_1, q'_2) \in R,
\]

\[
- \forall q''_1 \text{ such that } q_1 \xrightarrow{\mu} q''_1, \exists q''_2 \text{ such that } q_2 \xrightarrow{\mu} q''_2 \text{ and } (q''_1, q''_2) \in R.
\]

And we can see by comparing the definition of above function and the definition of bisimulation that (no formal proofs):

1. The function \( F \) is monotone, i.e. if \( R_1 \subset R_2 \) then \( F(R_1) \subset F(R_2) \).
2. A relation \( R \subset Q \times Q \) is a bisimulation if and only if \( R \subseteq F(R) \).

Then according to Knaster-Tarski Fixed Point theorem, strong bisimilarity \( \sim \) is the greatest fixed point of \( F \). And this is also the definition of co-inductive relation defined by the same rules.

In HOL4, since the release Kananaskis-11, there’s a new facility for defining co-inductive relation. The entry command is Hol_coreln, which has the same syntax as Hol_reln for defining inductive relations. Using Hol_coreln, it’s possible to define the bisimulation equivalence directly in this way: (here we have chosen a new relation name STRONG_EQ [14]
any information about the size of such a fixed point. In general, if the greatest fixed point and
least fixed point doesn’t coincide, without the restriction by co-induction theorem, the rest two
theorems will not give a precise definition for that relation. For strong equivalence, we already
know that, the least fixed point is the maximal relation containing all others.

The first theorem is the original rules appearing in the definition. Roughly speaking, it’s kind of
rules for building a bisimulation relation in forward way, however this is impossible because of the
lack of base rules (which exists in most inductive relation). And it’s not original in this case, since
it can be derived from the last theorem \(\text{STRONG\_EQ\_cases} \). (c.f. p. 49 of [1])

The second theorem is the co-induction principle, it says, for whatever relation which satisfy
the rules, that relation must be contained in strong equivalence. In another word, it make sure
the target relation is the maximal relation containing all others.

The purpose of the last theorem (also called “cases” theorem), is to make sure the target
relation is indeed a fixed point of the function \( F \) built by the given rules. However, it doesn’t give
any information about the size of such a fixed point. In general, if the greatest fixed point and
least fixed point doesn’t coincide, without the restriction by co-induction theorem, the rest two
theorems will not give a precise definition for that relation. For strong equivalence, we already
know that, the least fixed point of \( F \) is empty relation \( \emptyset \), and the great fixed point is the strong
equivalence \( \sim \). And in fact, the “cases” theorem has “defined” a relation which lies in the middle
of the greatest and least fixed point. To see why this argument is true, we found this theorem as
an equation could be used as a possible definition of strong equivalence: (c.f. p. 49 of [1])

**Definition 3.** Define recursively a new behavioral relation \( \sim' \in Q \times Q \) as follows: \( q_1 \sim' q_2 \) if and
only if for all \( \mu \in A \)

\[
- \forall q'_1 \text{ such that } q_1 \xrightarrow{\mu} q'_1, \exists q'_2 \text{ such that } q_2 \xrightarrow{\mu} q'_2 \text{ and } q'_1 \sim' q'_2, \\
- \forall q'_1 \text{ such that } q_2 \xrightarrow{\mu} q'_2, \exists q'_1 \text{ such that } q_1 \xrightarrow{\mu} q'_1 \text{ and } q'_1 \sim' q'_2.
\]

This is exactly the same as above “cases” theorem if the theorem were used as a definition of
strong equivalence. Robin Milner calls this theorem the “property (*)” of strong equivalence. (c.f.
p.88 of [7]) But as Prof. Gorrieri’s book [1] already told with examples: “this does not identify a
unique relation, as many different relations satisfy this recursive definition.”, and the fact that any
mathematical (or logic) definitions must precisely specify the targeting object (unless the possible
covered range itself is a targeting object).
But why the recursive definition failed to define a largest bisimulation (i.e. strong equivalence)? The textbooks didn’t give a clear answer, but in the view of theorem proving, now it’s quite clear: such a recursive definition can only restrict the target relation into the range of all fixed points, while it’s the co-induction thereom who finally restricts the target relation to the greatest solution. Without any of them, the solution will not be unique (thus not a valid mathematical definition).

Now we prove the old (STRONG_EQUIV, ~) and new definition (STRONG_EQ) of strong equivalence are equivalent, i.e.

\[ \text{STR_EQUIV_TO_STR_EQ:} \]
\[ \vdash E \sim E' \iff \text{STRONG_EQ } E E' \]

The proof of above theorem is the result when combining the proof for each directions:

\[ \text{STR_EQ_IMP_STR_EQUIV:} \]
\[ \vdash \text{STRONG_EQ } E E' \Rightarrow E \sim E' \]

\[ \text{STR_EQUIV_IMP_STR_EQ:} \]
\[ \vdash E \sim E' \Rightarrow \text{STRONG_EQ } E E' \]

The direction from the co-inductively defined STRONG_EQ to traditionally defined STRONG_EQUIV is relatively easy, the proof only depends on the definition of STRONG_EQUIV and the fact that STRONG_EQ is also a STRONG_BISIM relation:

\[ \text{STR_EQ_IS_STR_BISIM:} \]
\[ \vdash \text{STRONG_BISIM STRONG_EQ} \]

which can be easily proved by comparing the definition of STRONG_BISIM and the “cases” theorem generated from the co-inductively defined STRONG_EQ. Thus the maximality of strong equivalence is not needed.

The proof of the other direction, instead, must use the co-induction theorem STRONG_EQ_coind and the “property (*)” of STRONG_EQUIV mentioned once previously:

\[ \text{PROPERTY_STAR:} \]
\[ \vdash E \sim E' \iff \forall u. \]
\[ (\forall E_1. E \dashv u \rightarrow E_1 \Rightarrow \exists E_2. E' \dashv u \rightarrow E_2 \wedge E_1 \sim E_2) \wedge \]
\[ \forall E_2. E' \dashv u \rightarrow E_2 \Rightarrow \exists E_1. E \dashv u \rightarrow E_1 \wedge E_1 \sim E_2 \]

The proof of above “property (*)” is similar with previous steps, but it’s not trivial. Here we omit the details (the reader can always check the proof scripts for all details). For just one time we show how co-induction theorem is used to prove STR_EQUIV_IMP_STR_EQ and we replay this proof by HOL’s interactive proof manager:\[14\]

\[ \text{Proof manager status: 1 proof.} \]
1. Incomplete goalstack:
   \[ \begin{align*}
   & \text{Initial goal:} \\
   & \vdash E \sim E' \Rightarrow \text{STRONG_EQ } E E'
   \end{align*} \]

\[ \text{Proofs} \]

Now we’re going to apply the co-induction theorem:

\[ \vdash (\forall a_0 a_1. \]
\[ \begin{align*}
   & \text{STRONG_EQ'} a_0 a_1 \Rightarrow \\
   & \forall u. \]
\[ \begin{align*}
   & (\forall E_1. \]

\[14\] in the following quote text, the leading > is the prompt of HOL running in PolyML, the function g puts an initial goal into the proof manager, and the function e applies tacticals to current goal.
\[ a_0 \dashv u E_1 \Rightarrow \exists E_2. a_1 \dashv u E_2 \land STRONG_EQ E_1 E_2 \land \\
\forall E_2, \\
a_1 \dashv u E_2 \Rightarrow \exists E_1. a_0 \dashv u E_1 \land STRONG_EQ E_1 E_2 \Rightarrow \\
\forall a_0 a_1, STRONG_EQ E_0 a_0 a_1 \Rightarrow STRONG_EQ a_0 a_1 \]

The tactical for applying such (co)induction theorems in HOL is to reduces the goal using a supplied implication, with higher-order matching, this tactical is called \texttt{HO\_MATCH\_MP\_TAC}:

> e (HO\_MATCH\_MP\_TAC STRONG\_EQ\_coind);
OK..
1 subgoal:
val it =

\[ !E E'. E ~ E' ==> \]
\[ !u. (\{E1. E \dashv u E1 \Rightarrow ?E2. E' \dashv u E2 \land E1 ~ E2\} \land \\
\{E2. E' \dashv u E2 \Rightarrow ?E1. E \dashv u E1 \land E1 ~ E2\} : \\
?.proof \]

The rest steps is to use the “property (*)” to rewrite the right side of the implication:

> e (PURE\_ONCE\_REWRITE\_TAC [GSYM PROPERTY\_STAR]);
OK..
1 subgoal:
val it =

\[ !E E'. E ~ E' ==> E ~ E' \]
\[ : \\
?.proof \]

Now things get very clear, a simple rewrite with boolean theorems will solve the goal easily:

> e (RW\_TAC bool\_ss []);
OK..

Goal proved.
\[ |- !E E'. E ~ E' ==> E ~ E' \]

Goal proved.
\[ |- !E E'. \\
E ~ E' ==> \\
!u. \\
(\{E1. E \dashv u E1 \Rightarrow ?E2. E' \dashv u E2 \land E1 ~ E2\} \land \\
\{E2. E' \dashv u E2 \Rightarrow ?E1. E \dashv u E1 \land E1 ~ E2\} \\
val it = \\
Initial goal proved.
\[ |- !E E'. E ~ E' ==> STRONG\_EQ E E' \]
\[ : \\
?.proof \]

Combining all the step together, a single Standard ML function in the proof script can be written to finish the proof and store the theorem with a name:

val STR\_EQUIV\_IMP\_STR\_EQ = store_thm (  "STR\_EQUIV\_IMP\_STR\_EQ",  '"\{E E'. STRONG\_EQUIV E E' ==> STRONG\_EQ E E'\}";  \texttt{HO\_MATCH\_MP\_TAC STRONG\_EQ\_coind (* co-induction principle used here! *)}  \texttt{REPEAT GEN\_TAC}  \texttt{PURE\_ONCE\_REWRITE\_TAC [GSYM PROPERTY\_STAR]}  \texttt{RW\_TAC bool\_ss []});
3.7 Weak transition and weak equivalence

The formalization of weak bisimulation, together with weak (and rooted) equivalence (also called “observation equivalence” and “observation congruence” in old books) is minimal in this project. In this part, the main purpose is to define the weak equivalence co-inductively first and then prove the traditional definition (like _STRONG_EQUIV_) as a theorem. We wants to convince the reader that, by using HOL’s coinduction facility, it’s much easier to get the same set of theorems like those for strong equivalence. These works are not part of the old CCS formalization in HOL88, it belongs to the author.[15]

There’re multiple ways to define the concept of weak transitions used in the definition of weak bisimulation. In early approach like Milner’s book, the first step is to define a weak bisimulation. In HOL, this can be defined through a non-recursive inductive relation and the RTC (reflexive transitive closure) on top of it:

\[ \vdash \text{EPS}_1 \quad a_0 \quad a_1 \iff a_0 \xrightarrow{-\tau} a_1 \]
\[ \vdash \text{EPS} = \text{EPS}_1 \]  

Once we have the EPS relation, the weak transition can be defined but a normal transition wrapped with two EPS transitions:

\[ \vdash a_0 ==_{a_1} >>= a_2 \iff \exists E_1, E_2. \text{EPS} \ a_0 \ E_1 \mid \ a_1 \ E_2 \mid \ EPS \ E_1 \ E_2 \ a_2 \]

Modern textbooks like [1] directly uses “weak trace” transition for defining weak bisimulation, in which there’s only one action in the trace. Here are the definition of weak trace:

**Definition 4.** (Weak trace) For any LTS \( TS = (Q, A \cup \tau, \rightarrow) \), where \( \tau \notin A \), define relation \( \rightarrow \subset Q \times A^* \times Q \) as the weak reflexive and transitive closure of \( \rightarrow \), i.e., as the least relation induced by the following axiom and rules, where \( \epsilon \) is the empty trace:

\[
\frac{q_1 \xrightarrow{\alpha} q_2}{q_1 \rightarrow q_2} \quad \frac{q_1 \xrightarrow{\tau} q_2}{q_1 \rightarrow q_2} \quad \frac{q \rightarrow q}{q_1 \sigma_1 \rightarrow q_2 \quad q_2 \sigma_2 \rightarrow q_3}{q_1 \sigma_1 \sigma_2 \rightarrow q_3}
\]

In HOL, we can use a list of _Label_ to represent the trace (thus there’s naturally no \( \tau \) in the list, as \( \tau \) is not part of the type _Label_ but _Action_) and empty list can be seen as the \( \epsilon \). As the result, the relation WEAK_TRACE has type _CCS \rightarrow Label_ list \rightarrow _CCS_ \rightarrow bool. Below is the “rules” theorem generated by Hol_reln command:

\[ \vdash (\forall E. \ \text{WEAK_TRACE} \ E \in E) \land \\
(\forall E \ E'. \ E \rightarrow_{\tau} E' \Rightarrow \text{WEAK_TRACE} \ E \in E') \land \\
(\forall E \ E'. \ l. \ E \rightarrow_{\text{label}} l \rightarrow E' \Rightarrow \text{WEAK_TRACE} \ E [l] E') \land \\
\forall E_1 \ E_2 \ E_3 \ l_1 \ l_2. \\
\text{WEAK_TRACE} \ E_1 \ l_1 \ E_2 \land \text{WEAK_TRACE} \ E_2 \ l_2 \ E_3 \Rightarrow \\
\text{WEAK_TRACE} \ E_1 \ (l_1 ++ l_2) \ E_3
\]

Now we take a look at the definition of weak bisimulation:

**Definition 5.** (Weak bisimulation and weak equivalence) For any LTS \( TS = (Q, A \cup \tau, \rightarrow) \), where \( \tau \notin A \), a weak bisimulation is a relation \( R \subset Q \times Q \) such that both \( R \) and its inverse \( R^{-1} \) are weak simulations. More explicitly, a weak bisimulation is a relation \( R \) such that if \( (q_1, q_2) \in R \) then for all \( \alpha \in A \)

---

[15] Of course, we can also rewrite the proof scripts for strong equivalence and fully benefit from HOL’s coinductive relation facility, but this is not very useful. The central idea of theorem proving is, once a theorem is successfully proved, its statement can be saved into disk for later use without the need to run the proof again everytime when it’s used. And the proof steps are not saved at all. Thus, the same theorem proved by different methods, when they were saved into disk, there’s absolutely no difference except for their names. On the other side, we want to keep the old definition for at least strong equivalence, because it’s a literature formalization of the definitions in standard textbooks.
And the relation \( \text{WEAK_EQUIV} \) part of \( \text{definition} \) coincides with \( \text{WEAK_TRANS} \) the list of labels. To simplify things, in all these weak bisimulation variants, we only use \( \text{WEAK_TRACE}' \) another relation then invalid traces like \( \sigma \) illegal with the existing definition of \( \text{WEAK_TRACE} \) and, symmetrically, \( \text{WEAK_TRACE} \) will cause theorems from HOL’s \( \text{listTheory} \) be handled.

States \( q \) and \( q' \) are weakly bisimilar (or weak bisimulation equivalent), denoted with \( q \approx q' \), if there exists a weak bisimulation \( R \) such that \( (q,q') \in R \).

There’s no big problem to use all weak traces in above definition, as long as we limit the number of labels in the trace to just one. The real difficulty happens when we try to further define the rooted weak bisimilarity on top of weak equivalence, in which an auxiliary relation \( q \overset{\tau}{\rightarrow} q' \) must be defined as

\[
q \overset{\tau}{\rightarrow} q' \quad \text{if and only if} \quad \exists q_1, q_2, \; q \overset{\tau}{\rightarrow} q_1 \Rightarrow q_2 \overset{\tau}{\rightarrow} q'.
\]

(1)

And the definition of rooted weak bisimilarity (in Milner’s book it’s also called “observation congruence”), noticed that it’s not recursive:

**Definition 6.** (Rooted weak bisimilarity) Given an LTS \((Q, \Delta \cup \tau, \rightarrow)\), two states \( q_1 \) and \( q_2 \) are rooted weak bisimilar, denoted \( q_1 \approx \mu q_2 \), for all \( \mu \in \Delta \cup \{\tau\} \)

\[
- \forall q_1' \; \text{such that} \; q_1 \overset{\sigma}{\rightarrow} q_1', \exists q_2' \; \text{such that} \; q_2 \overset{\sigma}{\rightarrow} q_2' \; \text{and} \; (q_1', q_2') \in R,
\]

\[
- \forall q_1' \; \text{such that} \; q_1 \overset{\tau}{\rightarrow} q_1', \exists q_2' \; \text{such that} \; q_2 \overset{\tau}{\rightarrow} q_2' \; \text{and} \; (q_1', q_2') \in R,
\]

and, symmetrically,

\[
- \forall q_2' \; \text{such that} \; q_2 \overset{\sigma}{\rightarrow} q_2', \exists q_1' \; \text{such that} \; q_1 \overset{\sigma}{\rightarrow} q_1' \; \text{and} \; (q_1', q_2') \in R,
\]

\[
- \forall q_2' \; \text{such that} \; q_2 \overset{\tau}{\rightarrow} q_2', \exists q_1' \; \text{such that} \; q_1 \overset{\tau}{\rightarrow} q_1' \; \text{and} \; (q_1', q_2') \in R.
\]

But there’s a type error here: \( \tau \) is not a legal trace, thus a term like \( \text{WEAK_TRACE} \ E \ [\tau] \ E' \) is illegal with the existing definition of \( \text{WEAK_TRACE} \). If we enlarge the type of traces to \( \text{Action list} \), then invalid traces like \( \sigma_1 \tau \sigma_2 \) will become legal in HOL terms. One dirty solution is to define another relation \( \text{WEAK_TRACE}' \) which takes single \( \text{Action} \) having the above auxiliary relation as part of is definition. But this actually coincides with \( \text{WEAK_TRANS} \).

Since the use of \( \text{WEAK_TRACE} \) will cause theorems from HOL’s \( \text{listTheory} \) being used to handle the list of labels. To simplify things, in all these weak bisimulation variants, we only use \( \text{WEAK_TRANS} \) and \( \text{EPS} \). Here is the definition of \( \text{WEAK_BISIM} \) (not recursive) in HOL:

\[
\vdash \text{WEAK_BISIM} \; \text{Wbsm} \iff \forall E, E'. \; \text{Wbsm} \ E \ E' \Rightarrow \forall l, \; \forall E_1, \; E \longrightarrow \text{label} \ l \rightarrow E_1 \Rightarrow \exists E_2. \; E' \longrightarrow \text{label} \ l \rightarrow E_2 \wedge \text{Wbsm} \; E_1 \ E_2 \wedge \forall E_2, \; E' \longrightarrow \text{label} \ l \rightarrow E_2 \Rightarrow \exists E_1. \; E \longrightarrow \text{label} \ l \rightarrow E_1 \wedge \text{Wbsm} \; E_1 \ E_2 \wedge \forall E_1, \; E \longrightarrow \tau \rightarrow E_1 \Rightarrow \exists E_2. \; \text{EPS} \; E' \ E_2 \wedge \text{Wbsm} \; E_1 \ E_2 \wedge \forall E_2, \; E' \longrightarrow \tau \rightarrow E_2 \Rightarrow \exists E_1. \; \text{EPS} \; E \ E_1 \wedge \text{Wbsm} \; E_1 \ E_2.
\]

And the relation \( \text{WEAK_EQUIV} \) is co-inductively defined by HOL’s \( \text{Hol_coreln} \) command:

\[
\text{val} \; (\text{WEAK_EQUIV_rules}, \text{WEAK_EQUIV_coind}, \text{WEAK_EQUIV_cases}) = \text{Hol_coreln} ' (\text{WEAK_BISIM} E').
\]

\[
(\forall E_1. \; \text{TRANS} \; E \; (\text{label} \; 1) \ E_1 \Rightarrow \exists E_2. \; \text{WEAK_TRANS} \; E' \; (\text{label} \; 1) \ E_2 \wedge \text{WEAK_EQUIV} \; E_1 \ E_2) \quad /\quad (\forall E_2. \; \text{TRANS} \; E' \; (\text{label} \; 1) \ E_2 \Rightarrow \exists E_1. \; \text{WEAK_TRANS} \; E \; (\text{label} \; 1) \ E_1 \wedge \text{WEAK_EQUIV} \; E_1 \ E_2)\quad /\quad (\forall E_1. \; \text{TRANS} \; \tau \ E_1 \Rightarrow \exists E_2. \; \text{EPS} \; E' \ E_2 \wedge \text{WEAK_EQUIV} \; E_1 \ E_2) \quad /\quad (\forall E_2. \; \text{TRANS} \; E' \; \tau \ E_2 \Rightarrow \exists E_1. \; \text{EPS} \; E \ E_1 \wedge \text{WEAK_EQUIV} \; E_1 \ E_2) \Rightarrow \text{WEAK_EQUIV} \; E \ E'.
\]
Like for the strong equivalence, the above command generates three theorems which fully characterizes the weak equivalence relation:

1. The (forward) rules for weak equivalence:

   \[ \forall l. (\forall E_1. E' \rightarrow \text{label} \; l \rightarrow E_1 \Rightarrow \exists E_2. E' \approx \text{label} \; l \Rightarrow E_2 \land E_1 \approx E_2) \land \forall E_2. E' \rightarrow \text{label} \; l \rightarrow E_2 \Rightarrow \exists E_1. E \approx \text{label} \; l \Rightarrow E_1 \land E_1 \approx E_2) \land (\forall E_1. E \rightarrow \tau \rightarrow E_1 \Rightarrow \exists E_2. \text{EPS} E' \land E_1 \approx E_2) \land (\forall E_2. E' \rightarrow \tau \rightarrow E_2 \Rightarrow \exists E_1. \text{EPS} E \land E_1 \approx E_2) \Rightarrow E \approx E' \] 

2. The co-induction theorem which assert the maximality of the relation:

   \[ \forall a_0 a_1. \text{WEAK\_EQUIV}' a_0 a_1 \Rightarrow \forall l. (\forall E_1. a_0 \rightarrow \text{label} \; l \rightarrow E_1 \Rightarrow \exists E_2. a_1 \approx \text{label} \; l \Rightarrow E_2 \land \text{WEAK\_EQUIV}' E_1 E_2) \land \forall E_2. a_1 \rightarrow \text{label} \; l \rightarrow E_2 \Rightarrow \exists E_1. a_0 \approx \text{label} \; l \Rightarrow E_1 \land \text{WEAK\_EQUIV}' E_1 E_2) \land (\forall E_1. a_0 \rightarrow \tau \rightarrow E_1 \Rightarrow \exists E_2. \text{EPS} a_1 E_2 \land \text{WEAK\_EQUIV}' E_1 E_2) \land \forall E_2. a_1 \rightarrow \tau \rightarrow E_2 \Rightarrow \exists E_1. \text{EPS} a_0 E_1 \land \text{WEAK\_EQUIV}' E_1 E_2) \Rightarrow \forall a_0 a_1. \text{WEAK\_EQUIV}' a_0 a_1 \Rightarrow a_0 \approx a_1 \]

3. The “cases” theorem (or “property (*)”) for weak equivalence:

   \[ \forall l. (\forall E_1. a_0 \rightarrow \text{label} \; l \rightarrow E_1 \Rightarrow \exists E_2. a_1 \approx \text{label} \; l \Rightarrow E_2 \land E_1 \approx E_2) \land \forall E_2. a_1 \rightarrow \text{label} \; l \rightarrow E_2 \Rightarrow \exists E_1. a_0 \approx \text{label} \; l \Rightarrow E_1 \land E_1 \approx E_2) \land (\forall E_1. a_0 \rightarrow \tau \rightarrow E_1 \Rightarrow \exists E_2. \text{EPS} a_1 E_2 \land \text{WEAK\_EQUIV}' E_1 E_2) \land \forall E_2. a_1 \rightarrow \tau \rightarrow E_2 \Rightarrow \exists E_1. \text{EPS} a_0 E_1 \land \text{WEAK\_EQUIV}' E_1 E_2) \Rightarrow \forall a_0 a_1. \text{WEAK\_EQUIV}' a_0 a_1 \Rightarrow a_0 \approx a_1 \]

Unlike in the definition of strong equivalence, our definition of WEAK\_EQUIV is unrelated to the definition of WEAK\_BISIM. But we want to show that, the textbook definition for weak equivalence which is similar with the definition of strong equivalence

\[ \forall l. (\forall E_1. a_0 \rightarrow \text{label} \; l \rightarrow E_1 \Rightarrow \exists E_2. a_1 \approx \text{label} \; l \Rightarrow E_2 \land E_1 \approx E_2) \land \forall E_2. a_1 \rightarrow \text{label} \; l \rightarrow E_2 \Rightarrow \exists E_1. a_0 \approx \text{label} \; l \Rightarrow E_1 \land E_1 \approx E_2) \land (\forall E_1. a_0 \rightarrow \tau \rightarrow E_1 \Rightarrow \exists E_2. \text{EPS} a_1 E_2 \land \text{WEAK\_EQUIV}' E_1 E_2) \land \forall E_2. a_1 \rightarrow \tau \rightarrow E_2 \Rightarrow \exists E_1. \text{EPS} a_0 E_1 \land \text{WEAK\_EQUIV}' E_1 E_2) \Rightarrow \forall a_0 a_1. \text{WEAK\_EQUIV}' a_0 a_1 \Rightarrow a_0 \approx a_1 \]

can now be proved as a theorem:

\[ \forall l. (\forall E_1. a_0 \rightarrow \text{label} \; l \rightarrow E_1 \Rightarrow \exists E_2. a_1 \approx \text{label} \; l \Rightarrow E_2 \land E_1 \approx E_2) \land \forall E_2. a_1 \rightarrow \text{label} \; l \rightarrow E_2 \Rightarrow \exists E_1. a_0 \approx \text{label} \; l \Rightarrow E_1 \land E_1 \approx E_2) \land (\forall E_1. a_0 \rightarrow \tau \rightarrow E_1 \Rightarrow \exists E_2. \text{EPS} a_1 E_2 \land \text{WEAK\_EQUIV}' E_1 E_2) \land \forall E_2. a_1 \rightarrow \tau \rightarrow E_2 \Rightarrow \exists E_1. \text{EPS} a_0 E_1 \land \text{WEAK\_EQUIV}' E_1 E_2) \Rightarrow \forall a_0 a_1. \text{WEAK\_EQUIV}' a_0 a_1 \Rightarrow a_0 \approx a_1 \]

The proof is very simple, because now we have the “property (*)” for free. The first step is to prove that the weak equivalence is also a weak bisimulation relation:

\[ \forall l. (\forall E_1. a_0 \rightarrow \text{label} \; l \rightarrow E_1 \Rightarrow \exists E_2. a_1 \approx \text{label} \; l \Rightarrow E_2 \land E_1 \approx E_2) \land \forall E_2. a_1 \rightarrow \text{label} \; l \rightarrow E_2 \Rightarrow \exists E_1. a_0 \approx \text{label} \; l \Rightarrow E_1 \land E_1 \approx E_2) \land (\forall E_1. a_0 \rightarrow \tau \rightarrow E_1 \Rightarrow \exists E_2. \text{EPS} a_1 E_2 \land \text{WEAK\_EQUIV}' E_1 E_2) \land \forall E_2. a_1 \rightarrow \tau \rightarrow E_2 \Rightarrow \exists E_1. \text{EPS} a_0 E_1 \land \text{WEAK\_EQUIV}' E_1 E_2) \Rightarrow \forall a_0 a_1. \text{WEAK\_EQUIV}' a_0 a_1 \Rightarrow a_0 \approx a_1 \]

Then in the proof of WEAK\_EQUIV, one direction can be easily proved by above theorem, and other direction can also be proved easily by co-induction theorem and first-order proof searching (using HOL’s METIS\_TAC [14]):
As mentioned in the literature \cite{12}, bisimulation equivalence is one of the most well-studied co-inductive relation. But since HOL (and other theorem provers like Coq and Isabelle) started to support the co-inductive relation features (in very recent years), the correctness of these features were never confirmed on the (strong and weak) bisimulation equivalence defined on CCS-like graph structures. Now in this project, we have finally done this experiment.

Finally the rooted weak equivalence is defined in HOL as follows: (again, not recursive)

\[ E \approx c E' \iff \forall u. \(\forall E_1. E \xrightarrow{-u} E_1 \Rightarrow \exists E_2. E' = u \Rightarrow E_2 \wedge E_1 \approx E_2\) \land \forall E_2. E' \xrightarrow{-u} E_2 \Rightarrow \exists E_1. E = u \Rightarrow E_1 \wedge E_1 \approx E_2 \]

However, there’s no theorems proven for rooted weak equivalences in this project.

### 3.8 Laws for strong equivalence

Based on the definition of \texttt{STRONG_EQUIV} and SOS inference rules for the \texttt{TRANS} relation, we have proved a large set of theorems concerning the strong equivalence of CCS processes. Below is a list of fundamental congruence theorems for strong equivalence:

**STRONG_EQUIV_SUBST_PREFIX:**

\[ \vdash E \sim E' \Rightarrow \forall u. u..E \sim u..E' \]

**STRONG_EQUIV_PRESD_BY_SUM:**

\[ \vdash E_1 \sim E_1' \wedge E_2 \sim E_2' \Rightarrow E_1 + E_2 \sim E_1' + E_2' \]

**STRONG_EQUIV_PRESD_BY_PAR:**

\[ \vdash E_1 \sim E_1' \wedge E_2 \sim E_2' \Rightarrow E_1 || E_2 \sim E_1' || E_2' \]

**STRONG_EQUIV_SUBST_RESTR:**

\[ \vdash E \sim E' \Rightarrow \forall L. \nu L E \sim \nu L E' \]

**STRONG_EQUIV_SUBST_RELAB:**

\[ \vdash E \sim E' \Rightarrow \forall rf. \text{relab} E rf \sim \text{relab} E' rf \]

Noticed that, the strong bisimulation equivalence is co-inductively defined, and two processes are strong equivalent if there’s a bisimulation containing them. Thus, to prove two processes are strong equivalent, it’s enough to find a bisimulation containing them. To prove the they’re not strong equivalent, it’s enough to try to construct a bisimulation starting from them and the proof is finished whenever the attempt fails. In any case, there’s no need to do induction on the data type of involved CCS processes.

Here are the strong laws proved for the sum operator: (noticed that, the lack of some parentheses is because we have defined the sum and parallel operators as left-associative)

**STRONG_SUM_IDENT_R:**

\[ \vdash E + \text{nil} \sim E \]

**STRONG_SUM_IDEMP:**

\[ \vdash E + E \sim E \]
STRONG_SUM_COMM: ⊢ E + E' ∼ E' + E
STRONG_SUM_IDENT_L: ⊢ nil + E ∼ E
STRONG_SUM_ASSOC_R: ⊢ E + E' + E'' ∼ E + (E' + E'')
STRONG_SUM_ASSOC_L: ⊢ E + (E' + E'') ∼ E + E' + E''
STRONG_SUM_MID_IDEMP: ⊢ E + E' + E'' ∼ E' + E
STRONG_LEFT_SUM_MID_IDEMP: ⊢ E + E' + E'' + E ∼ E + E'' + E'

Not all proven theorems are fundamental (in the sense of providing a minimal axiomatization set for proving all other algebraic laws). The first several theorems must be proved by constructing bisimulation relations and then verifying the definitions of strong bisimulation and strong equivalence, and their formal proofs were written in goal-directed ways. Instead, the last three ones were all constructed in forward way by applications of previous proven algebraic laws, without directly using any SOS inference rules and the definition of strong equivalence. Such constructions were based on two useful ML functions S_SYM and S_TRANS which builds new strong laws from the symmetry and transitivity of strong equivalence:

(* Define S_SYM such that, when given a theorem A |- STRONG_EQUIV t1 t2, returns the theorem A |- STRONG_EQUIV t2 t1. *)
fun S_SYM thm = MATCH_MP STRONG_EQUIV_SYM thm;

(* Define S_TRANS such that, when given the theorems thm1 and thm2, applies STRONG_EQUIV_TRANS on them, if possible. *)
fun S_TRANS thm1 thm2 =
  if rhs_tm thm1 = lhs_tm thm2 then
    MATCH_MP STRONG_EQUIV_TRANS (CONJ thm1 thm2)
  else
    failwith "transitivity of strong equivalence not applicable";

For instance, to construct the proof of STRONG_SUM_MID_IDEMP, the following code was written:

(* STRONG_SUM_MID_IDEMP:  
|> !E E'. STRONG_EQUIV (sum (sum E E')) E) (sum E' E) 
*)
val STRONG_SUM_MID_IDEMP = save_thm (  
"STRONG_SUM_MID_IDEMP",  
GEN "E: CCS"  
(S_TRANS  
(SPEC "E: CCS"  
(MATCH_MP STRONG_EQUIV_SUBST_SUM_R  
(SPECL ["E: CCS", "E': CCS'" ] STRONG_SUM_COMM)))  
(S_TRANS  
(SPECL ["E': CCS", "E: CCS", "E': CCS'" ] STRONG_SUM_ASSOC_R)  
(SPEC "E: CCS"  
(MATCH_MP STRONG_EQUIV_SUBST_SUM_L  
(SPEC "E: CCS'" STRONG_SUM_MID_IDEMP))))));

Here are the strong laws we have proved for the par operator:

STRONG_PAR_IDENT_R: ⊢ E || nil ∼ E
STRONG_PAR_COMM: ⊢ E || E' ∼ E' || E
STRONG_PAR_IDENT_L: ⊢ nil || E ∼ E
STRONG_PAR_ASSOC: ⊢ E || E' || E'' ∼ E || (E' || E'')
STRONG_PAR_PREF_TAU: ⊢ u..E || τ..E' ∼ u..(E || τ..E') + τ..(u..E || E')
STRONG_PAR_TAU_PREF: ⊢ τ..E || u..E' ∼ τ..(E || u..E') + u..(τ..E || E')
STRONG_PAR_TAU_TAU: ⊢ τ..E || τ..E' ∼ τ..(E || τ..E') + τ..(τ..E || E')
STRONG_PAR_PREF_NO_SYNCR:
|> l ≠ COMPL l' ⇒
  ∀E E'.
  label l..E || label l'.E' ∼
  label l.(E || label l'..E') +
\begin{align*}
\text{ STRONG_PAR_PREF_SYNCR:} & \vdash (l = \text{COMPL} l') \Rightarrow \\
& \forall E E'. \\
& \text{label } l..E || \text{label } l'..E' \sim \\
& \text{label } l.(E || \text{label } l'..E') + \\
& \text{label } l'..(\text{label } l..E || E') + \tau..(E || E')
\end{align*}

And the strong laws for the restriction operator:

\begin{align*}
\text{ STRONG_RESTR_NIL:} & \vdash \nu L \text{nil} \sim \text{nil} \\
\text{ STRONG_RESTR_SUM:} & \vdash \nu L (E + E') \sim \nu L E + \nu L E' \\
\text{ STRONG_RESTR_PREFIX_TAU:} & \vdash l \in L \lor \text{COMPL } l \notin L \Rightarrow \forall E. \nu L (\text{label } l..E) \sim \text{nil} \\
\text{ STRONG_RESTR_PREFIX_LABEL:} & \vdash l \notin L \land \text{COMPL } l \notin L \Rightarrow \\
& \forall E. \nu L (\text{label } l..E) \sim \text{label } l..\nu L E
\end{align*}

The strong laws for the relabeling operator:

\begin{align*}
\text{ STRONG_RELAB_NIL:} & \vdash \text{relab nil } rf \sim \text{nil} \\
\text{ STRONG_RELAB_SUM:} & \vdash \text{relab } (E + E') rf \sim \text{relab } E rf + \text{relab } E' rf \\
\text{ STRONG_RELAB_PREFIX:} & \vdash \text{relab } (u..E) (\text{RELAB } labl) \sim \\
& \text{relabel } \text{RELAB } labl \ u..\text{relab } E \text{RELAB } labl
\end{align*}

The strong laws for the recursion operator (for constants):

\begin{align*}
\text{ STRONG_UNFOLDING:} & \vdash \text{rec } X E \sim \text{CCS}_{\text{Subst}} E (\text{rec } X E) X \\
\text{ STRONG_PREF_REC_Equiv:} & \vdash u..\text{rec } s (v..u..\text{var } s) \sim \text{rec } s (u..v..\text{var } s) \\
\text{ STRONG_REC_ACT2:} & \vdash \text{rec } s (u..u..\text{var } s) \sim \text{rec } s (u..\text{var } s)
\end{align*}

All above three theorems for recursion operator were fundamental (in the sense that, they cannot be proved by just using other strong laws).

Finally, all above strong laws could be used either manually or as part of the decision procedure for automatically deciding strong equivalences between two CCS process. However such a decision procedure is not done in the current project.

### 3.9 Expansion Law for strong equivalence

The final big piece of proof work in this project is the representation and proof of the following \textit{expansion law} (sometimes also called the \textit{interleaving law}):

\textbf{Proposition 1.} \textit{(Expansion Law)} Let $p = \sum_{i=1}^{n} \mu_i p_i$ and $q = \sum_{j=1}^{m} \mu'_j q_j$. Then

$$p|q \sim \sum_{i=1}^{n} \mu_i (p_i|q) + \sum_{j=1}^{m} \mu'_j (p|q_j) + \sum_{i,j: \mu_i = \mu'_j} \tau. \ (p_i|q_j) \quad (2)$$

Some characteristics made the formal proof very special and different from all other theorems that we have proved so far. First of all, arithmetic numbers (of type \texttt{num}) were involved for the first time, and now our CCS theory depends on elementary mathematical theories provided by HOL, namely the \texttt{prim_recTheory} and \texttt{arithmeticTheory}. Although arithmetic operations like $+, -, \ldots$ were not involved (yet), but we do need to compare number values and use some related theorems.

Also two CCS accessors were defined and used to access the internal structure of CCS processes, namely \texttt{PREF_ACT} for getting the initial action and \texttt{PREF_PROC} for getting the rest of process without the first action. Together there’s predicate \texttt{Is_Prefix} for testing if a CCS is a prefixed process:
⊢ PREF_ACT (u..E) = u
⊢ PREF_PROC (u..E) = E
⊢ Is_Prefix E ⇐⇒ ∃ u E'. E = u..E'

They are needed because we’re going to represent \( \mu_i.p_i \) as the value of a function: \( f(i) \) in which \( f \) has the type \( \text{num} \rightarrow \text{CCS} \). And in this way, to get \( \mu_i \) and \( p_i \) we have to use accessor: “PREF_ACT (f i)” and “PREF_PROC (f i)”.

The next job is to represent a finite sum of CCS processes. This is done by the following recursive function SIGMA:

\[
\forall f \cdot \text{SIGMA} f \ 0 = f \ 0 \\
\forall f \ n. \text{SIGMA} f \ (\text{SUC} \ n) = \text{SIGMA} f \ n + f \ (\text{SUC} \ n)
\]

Thus if there’s a function \( f \) of type \( \text{num} \rightarrow \text{CCS} \), we should be able to represent \( \sum_{i=1}^{n} f(i) \) by HOL term “SIGMA f n”.

Now if we took a deeper look at the last summation of the right side of the expansion law, i.e. \( \sum_{i,j} \tau.(p_i|q_j) \), we found that such a “sum” cannot be represented directly, because there’re two index \( i, j \) and their possible value pairs used in the sum depends on the synchronization of corresponding actions from each \( p_i \) and \( q_j \). What we actually need is a recursively defined function taking all the \( p_i \) and \( q_j \) and return the synchronized process in forms like \( \tau.(p_i|q_j) \).

But this is still too complicated, instead we first define functions to synchronize just one process with another group of processes. This work is achieved by the function SYNC of type \( \text{Action} \rightarrow \text{CCS} \rightarrow (\text{num} \rightarrow \text{CCS}) \rightarrow \text{num} \rightarrow \text{CCS} \):

\[
\forall u \ P \ f. \\
\text{SYNC} u \ P \ f \ 0 = \\
\quad \text{if} \ (u = \tau) \lor (\text{PREF_ACT} (f \ 0) = \tau) \ \text{then} \ \text{nil} \\
\quad \text{else if} \ \text{LABEL} u = \text{COMPL} (\text{LABEL} (\text{PREF_ACT} (f \ 0))) \ \text{then} \\
\quad \quad \tau..(P \ || \ \text{PREF_PROC} (f \ 0)) \\
\quad \text{else} \ \text{nil}) \ \\
\forall u \ P \ f \ n. \\
\text{SYNC} u \ P \ f \ (\text{SUC} \ n) = \\
\quad \text{if} \ (u = \tau) \lor (\text{PREF_ACT} (f \ (\text{SUC} \ n)) = \tau) \ \text{then} \\
\quad \quad \text{SYNC} u \ P \ f \ n \\
\quad \text{else if} \\
\quad \quad \text{LABEL} u = \text{COMPL} (\text{LABEL} (\text{PREF_ACT} (f \ (\text{SUC} \ n)))) \\
\quad \quad \text{then} \\
\quad \quad \quad \tau..(P \ || \ \text{PREF_PROC} (f \ (\text{SUC} \ n))) + \text{SYNC} u \ P \ f \ n \\
\quad \text{else} \ \text{SYNC} u \ P \ f \ n
\]

Then the synchronization of two group of processes can be further defined by another recursive function ALL_SYNC of type \( \text{num} \rightarrow \text{CCS} \rightarrow \text{num} \rightarrow \text{CS} \rightarrow \text{num} \rightarrow \text{CCS} \):

\[
\forall f \ f' \ m. \\
\text{ALL_SYNC} f \ 0 \ f' \ m = \\
\text{SYNC} \ (\text{PREF_ACT} (f \ 0)) \ (\text{PREF_PROC} (f \ 0)) \ f' \ m \ \\
\forall f \ n \ f' \ m. \\
\text{ALL_SYNC} f \ (\text{SUC} \ n) \ f' \ m = \\
\text{ALL_SYNC} f \ n \ f' \ m + \\
\text{SYNC} \ (\text{PREF_ACT} (f \ (\text{SUC} \ n))) \ (\text{PREF_PROC} (f \ (\text{SUC} \ n))) \ f' \ m
\]

Some lemmas about SIGMA and the two synchronization functions were proved first:

SIGMA_TRANS_THM_EQ:
\[
\vdash \text{SIGMA} f \ n \rightarrow u \rightarrow E \iff \exists k. k \leq n \land f \ k \rightarrow \rightarrow u \rightarrow E
\]

SYNC_TRANS_THM_EQ:
\[
\vdash \text{SYNC} u \ P \ f \ n \rightarrow v \rightarrow Q \iff \exists j \ l. \\
\quad j \leq m \land (u = \text{label} \ l) \land
\]
(PREF_ACT (f j) = label (COMPL l)) \land (v = \tau) \land 
(Q = P' \parallel PREF_PROC (f j))

ALL_SYNC_TRANS_THM_EQ:
\[ \vdash ALL_SYNC f n f' m \rightarrow u \rightarrow E \iff \exists k k' l. 
   k \leq n \land k' \leq m \land (PREF_ACT (f k) = label l) \land 
   (PREF_ACT (f' k') = label (COMPL l)) \land (u = \tau) \land 
   (E = PREF_PROC (f k) \parallel PREF_PROC (f' k')) \]

Finally, we have proved the Expansion Law in the following form:

STRONG_PAR_LAW:
\[ \vdash (\forall i. i \leq n \Rightarrow Is_Prefix (f i)) \land 
   (\forall j. j \leq m \Rightarrow Is_Prefix (f' j)) \Rightarrow 
   SIGMA f n \parallel SIGMA f' m \sim 
   SIGMA (\lambda i. PREF_ACT (f i) \ldots (PREF_PROC (f i) \parallel SIGMA f' m)) 
   n + 
   SIGMA (\lambda j. PREF_ACT (f' j) \ldots (SIGMA f n \parallel PREF_PROC (f' j))) 
   m + ALL_SYNC f n f' m \]

4 Missing pieces and Future directions

The old proof scripts provided by Prof. Nesi do not contain anything related to weak bisimulation, while these things were talked as major work in the original paper. We think those proof scripts must have been unfortunately lost. In our project, due to time limits we only re-defined the concepts of weak transitions, weak bisimulation, weak bisimulation equivalence (observation equivalence) and rooted weak equivalence (observation congruence), but almost didn’t prove any useful results, except for the experiments to show the correctness of HOL’s co-inductive relation defining facility (Hol_coreln) for weak bisimulation equivalences. Given the fact that, more practical model checking were done by comparing (rooted) weak bisimulation equivalences between two CCS processes, our current work is far from complete.

The other big missing piece is the decision procedure for automatic checking of strong (and weak) bisimulation equivalence. There exists some fast algorithms for bisimulation equivalence checking, they were mostly based on reductions of the equivalence checking to the so-called “coarsest relational partitioning” problem. (c.f. [15] and [16]), some variants (e.g. [17]) are suitable for compact representations like CCS, in which the whole graph is not visible. On the other side, we know Concurrency Workbench didn’t use the most efficient algorithm (c.f. p.13 of [18]), and this leaves us a room to create a faster equivalence checking tool, and it runs even inside a theorem prover!

Thus, the author hopes to continue this project with the following possible direction:

1. Complete the theory for (rooted) weak equivalence and prove the related weak laws.
2. Create decision procedures for bisimulation equivalence checking which take two CCS processes and give a theorem about their equivalence.
3. Formally prove some deep theorems for bisimulation equivalences, e.g. the Hennessy Lemma (c.f. p.176 of [1])

Finally, any tool is only useful when it’s proven to be useful for resolving practical problems. But so far we haven’t shown anything for its applications. Indeed, maybe we can never show more useful results than those already have with software like Concurrency Workbench. So our main hope here, is to provide experiences and good basis for building more complicated process algebras (e.g. CCS variants with more operators). And when future researchers published new theorems in this area, maybe they could provide also formal proofs using the framework provided in this project.

---

This is not true any more. Prof. Monica Nesi still have all these proof scripts, and the author is now waiting for these code to continue the rests of the porting work.
5 On the choice of HOL

On the initial choice of using HOL for the CCS formalization, we believe this was partially influenced by the theorem proving environment in Britain in 1990s, and the fact that, the creator of HOL (Mike J. C. Gordon) was also working in Cambridge University since 1981. Students and researchers usually choose to use software developed and taught by scholars in their own university, or country. The latter case is particularly true for researchers of formal methods in France: they almost always use Coq and OCaml to build everything.

Beside environment reasons, and the fact that the work in this project is not original (porting old code), the author still thinks that HOL4 is a better choice than other popular theorem provers like Coq and Isabelle. This is because, only in HOL4, it’s possible to write proof scripts, new tacticals and ordinary functions (which generates new theorems) in the same underlying programming language (Standard ML). And the powerful source-level debugging support in Poly/ML was essential to us for fixing the bugs found in the big function `CCS_TRANS_CONV`.

There’s one extra benefit to use theorem prover built on top of Standard ML: it’s a smaller language than OCaml, and currently there’s an ongoing project called CakeML with the aim to formally verify the compiler for the substantial subset of Standard ML. When this project finally succeeds to build HOL on top of it, we’ll have a fully trusted computing environment including the underlying programming language, the theorem prover and the formal theories. With other programming languages and theorem provers written in them, there’s little hope in short future to achieve the same level of confidence.

On the other side, Matita was written in OCaml, a programming language more complex than Standard ML. Matita is a pure graphics program, and there’s no interactive interface. It lacks of a rich theorem library (there’s even no RTC support in its relation theory) that users could benefit. And there’s no interface to develop new tacticals and other proof tools directly at OCaml level. Due to these limitations, Matita can’t be used in projects like the current one. Not to mention that, Matita is not actively developed any more, and its user group can be almost ignored.

From the view of the author, HOL4 has been designed in an unique way that no other theorem prover can provide the same feature sets.

6 Conclusions

In this exam paper (and project report), we have successfully ported the old formalization of process algebra CCS (no value passing, with explicit relabeling operator) from HOL88 to latest HOL4 (Kananaskis-11 and later). We started from the definition and syntax of CCS processes defined as inductive datatypes in Higher Order Logic, and then defined all the SOS (Structured Operational Semantics) inference rules as an relation `TRANS`. Then all the algebraic laws including the Expansion Theorem were proved on top of CCS datatype and SOS rules.

The other big work in this project is a single ML function (part of the old work, but we have fixed and enhanced the code) which could automatically compute the possible transitions for a given CCS process. Different from the similar facility in softwares like Concurrency Workbench, the output of our function is a theorem. This is kind of trusting computing, as the only way to build theorems is to construct it from other theorems. Although the correctness of such a program is not formally verified, but as long as it terminates with a theorem as output, the output MUST be correct. We have future plans to create a similar tool for equivalence checking, in which equivalence results are theorems constructed from existing manually proved theorems.

This work is based on old CCS formalization in HOL88, done by Prof. Monica Nesi (of University of L’Aquila, Italy) in 1992-1995 when he was studying at University of Cambridge. Thanks to Prof. Nesi for finding and sending the old HOL88 proof scripts to the author.

---

17 Both Matita and Coq were written in OCaml, however Coq (and maybe also Matita) didn’t use any OO feature provided by OCaml.

18 [https://cakeml.org](https://cakeml.org)

19 [http://matita.cs.unibo.it/](http://matita.cs.unibo.it/)
Thanks to Prof. Roberto Gorrieri, who taught CCS and LTS theory to the author, and his supports on continuing this HOL-CCS project as exam project of his course.

Thanks to Prof. Andrea Asperti, who taught the interactive theorem proving techniques to the author, although it’s in another different theorem prover (Matita).

Thanks to people from HOL community (Thomas Tuerk, Michael Norrish, Ramana Kumar and many others) for resolving issues and doubts the author met when using HOL theorem prover.

The paper is written in \LaTeX and LNCS template, with theorems generated automatically by HOL’s $\text{EmitTex}$ exporting module from the proof scripts.

References

1. Gorrieri, R., Versari, C.: Introduction to Concurrency Theory. Transition Systems and CCS. Springer, Cham (September 2015)
2. Keller, R.M.: Formal verification of parallel programs. Communications of the Association for Computing Machinery 19(7) (1976) 371–384
3. Milner, R.: A Calculus of Communicating Systems. Volume 92 of Lecture Notes in Computer Science. Springer Berlin Heidelberg, Berlin, Heidelberg (1980)
4. Gordon, M.: From LCF to HOL: a short history. Proof, language, and interaction (July 2000)
5. Nesi, M.: Value-passing ces in hol. In: Higher Order Logic Theorem Proving and Its Applications. Springer (1994) 352–365
6. Nesi, M.: Mechanising a modal logic for value-passing agents in HOL. Electronic Notes in Theoretical Computer Science (1997)
7. Milner, R.: Communication and concurrency. Prentice Hall (1989)
8. Nesi, M.: A formalization of the process algebra CCS in high order logic. Technical report, University of Cambridge, Computer Laboratory (1992)
9. Kreitz, C., Rahli, V.: Introduction to Classic ML. (August 2011) 1–18
10. Moller, F.: The Edinburgh Concurrency Workbench user manual (Version 7.1). (April 2017)
11. Melham, T.F.: A Package For Inductive Relation Definitions In HOL. In: 1991., International Workshop on the HOL Theorem Proving System and Its Applications, IEEE (1991) 350–357
12. Sangiorgi, D.: Introduction to Bisimulation and Coinduction. Cambridge University Press (October 2011)
13. : The HOL System DESCRIPTION. (March 2017) 1–349
14. Hurd, J.: First-order proof tactics in higher-order logic theorem provers. Design and Application of Strategies/Tactics in Higher ... (2003)
15. Kanellakis, P.C., Smolka, S.A.: CCS expressions, finite state processes, and three problems of equivalence. Information and Computation 86(1) (1990) 43–68
16. Paige, R., Tarjan, R.E.: Three partition refinement algorithms. SIAM Journal on Computing 16(6) (1987) 973–989
17. Lee, D., Yannakakis, M.: Online minimization of transition systems (extended abstract). ACM, New York, New York, USA (July 1992)
18. CLEAVELAND, R., PARROW, J., STEFFEN, B.: The Concurrency Workbench - a Semantics-Based Tool for the Verification of Concurrent Systems. Acm Transactions on Programming Languages and Systems 15(1) (January 1993) 36–72

Appendix A: running the proof scripts in HOL4

Suppose HOL (Kananaskis-11) has been installed and the two entry commands hol and Holmake have been made available in current Shell environment (e.g. their containing directory is in \texttt{PATH} environment variable). Copying all above 4 files into a empty directory and execute Holmake, they should be compiled correctly with some extra files generated.

Then after executing hol, enter the following commands to load all CCS related scripts:

\begin{verbatim}
HOL-4 [Kananaskis 11 (logknl, built Sat Apr 29 12:55:33 2017)]

For introductory HOL help, type: help "hol";
\end{verbatim}

\footnote{For installation instructions of HOL4, see \url{https://hol-theorem-prover.org/#get}. To run the scripts mentioned in this paper correctly, please use kananaskis-11 (latest released version).}
> load "ExampleTheory";
val it = (): unit
> open ExampleTheory;
...
>
Then we can either access already proved theorems storing in ML variables:

> STRONG_PAR_LAW;
val it =
|- !f n f' m.
  (!i. i <= n ==> Is_Prefix (f i)) \&\& (!j. j <= m ==> Is_Prefix (f' j)) ==> 
  SIGMA f n || SIGMA f' m
~
SIGMA (\i. PREF_ACT (f i)...(PREF_PROC (f i) \| SIGMA f' m)) n +
SIGMA (\j. PREF_ACT (f' j)...(SIGMA f n || PREF_PROC (f' j))) m +
ALL_SYNC f n f' m:
thm

or compute CCS transitions from any given process:

> CCS_TRANS "(nu "a") (In "a"..nil || Out "a"..nil)";
val it =
( |- !u E.
  'm "a" (In "a"..nil || Out "a"..nil) --u-> E <=>
  (u = tau) \&\& (E = 'm "a" (nil || nil)),
  ["tau",
  "m "a" (nil || nil)"]):
thm * (term * term) list

> CCS_TRANS "(In "a"..nil || Out "a"..nil)";
val it =
( |- !u E.
  In "a"..nil || Out "a"..nil --u-> E <=>
  ((u = In "a") \&\& (E = nil || Out "a"..nil) \&\&
  (u = Out "a") \&\& (E = In "a"..nil || nil)) \&\&
  (u = tau) \&\& (E = nil || nil),
  ["In "a",
  "nil || Out "a"..nil"],
  ["Out "a"",
  "In "a"..nil || nil"],
  ["tau",
  "nil || nil"]):
thm * (term * term) list

The generated files *.sig contain lists of all proved theorems, the HTML versions were also generated as *.html files.