



Structural Equivalence in Reversible Calculus of Communicating Systems (Abstract)

Clément Aubert, Ioana Cristescu

► To cite this version:

Clément Aubert, Ioana Cristescu. Structural Equivalence in Reversible Calculus of Communicating Systems (Abstract). 2020. hal-02118036v2

HAL Id: hal-02118036

<https://hal.science/hal-02118036v2>

Preprint submitted on 26 Dec 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Structural Equivalences for Reversible Calculi of Communicating Systems (Oral communication)

Clément Aubert

School of Computer and Cyber Sciences,
Augusta University, USA
caubert@augusta.edu

Ioana Cristescu

Tarides,
Paris, France
ioana@tarides.com

The formalization of process algebras usually starts with a minimal core of operators and rules for its transition system, and then relax the system to improve its usability and ease the proofs. In the calculus of communicating systems (CCS), the structural congruence plays this role by making e.g. parallel composition commutative and associative: without it, the system would be cumbersome to use and reason about, and it can be proven that this change is innocuous in a precise technical sense. For the two reversible calculi extending CCS, the situation is less clear: CCS with Communication Keys (CCSK) was first defined without any structural congruence, and then was endowed with a fragment of CCS's congruence. Reversible CCS (RCCS) made the choice of “backing in” the structural equivalence, that became part of the “minimal core” of the system. In this short oral communication, we would like to re-consider the status and role of the structural congruence in general, to question its role in RCCS in particular, and to ask the more general question of the structural equivalences legitimacy.

1 Introduction

It is often useful to have a look at the fundamentals of your research field. For instance, a classical textbook states that constructing a process algebra often uses a two-stages approach [4, p. V]:

“In a process-algebraic approach to system verification, one typically writes two specifications. One, call it SYS, captures the design of the actual system and the other, call it SPEC, describes the system's desired ‘high-level’ behavior. One may then establish the correctness of SYS with respect to SPEC by showing that SYS behaves the ‘same as’ SPEC.”

This is generally the approach taken to define the calculus of communicating systems (CCS) [9].

Stage 1: SYS_{CCS} CCS processes are defined using simple operators (parallel composition, name prefixing or action, choice or sum, recursion, restriction and renaming), a single empty process denoted 0, and a collection of (co-)names $a, \bar{a}, b, \bar{b}, \dots$ over which λ ranges:

$$P, Q := P \mid Q \parallel \lambda.P \parallel \sum_{i \in I} P_i \parallel A \parallel P \backslash a \parallel P[a \leftarrow b] \parallel 0 \quad (\text{CCS Processes})$$

where A are (recursive) definitions of processes, that is $A \stackrel{\text{def}}{=} P$ and A can occur in P , $P[a \leftarrow b]$ is the capture-avoiding substitution, and we write $P[\vec{a} \leftarrow \vec{b}]$ for $P[a_1 \leftarrow b_1, \dots, a_n \leftarrow b_n]$.

To create SYS_{CCS} , the processes are endowed with an evaluation mechanism given by the labeled transition system (LTS) of Fig. 1. A process P reduces—or evaluates—to P' with label α (which can be a

$$\begin{array}{c}
\frac{P \xrightarrow{\alpha} P'}{P \mid Q \xrightarrow{\alpha} P' \mid Q} \text{ com.}_1 \qquad \frac{Q \xrightarrow{\alpha} Q'}{P \mid Q \xrightarrow{\alpha} P \mid Q'} \text{ com.}_2 \qquad \frac{P \xrightarrow{\lambda} P' \quad Q \xrightarrow{\bar{\lambda}} Q'}{P \mid Q \xrightarrow{\tau} P' \mid Q'} \text{ syn.} \\
\frac{}{\lambda.P \xrightarrow{\lambda} P} \text{ act.} \qquad \frac{P_j \xrightarrow{\alpha} P'_j \quad j \in I}{\sum_{i \in I} P_i \xrightarrow{\alpha} P'_i} \text{ sum.} \qquad \frac{P \xrightarrow{\alpha} P' \quad A \stackrel{\text{def}}{=} P}{A \xrightarrow{\alpha} P'} \text{ rec.} \\
\frac{P \xrightarrow{\alpha} P' \quad a \notin \alpha}{P \backslash a \xrightarrow{\alpha} P' \backslash a} \text{ res.} \qquad \frac{P \xrightarrow{\alpha} P'}{P[\vec{d} \leftarrow \vec{b}] \xrightarrow{\alpha[\vec{d} \leftarrow \vec{b}]} P'[\vec{d} \leftarrow \vec{b}]} \text{ rel.}
\end{array}$$

Figure 1: Rules of the labeled transition system of CCS (LTS_{CCS})

(co-)name, or the special label τ for “silent”, internal, transitions) if a tree whose root is $P \xrightarrow{\alpha} P'$ can be derived using the rules of Fig. 1.

Stage 2: SPEC_{CCS} The SYS_{CCS} specification, although capturing the intended calculus, is cumbersome because of its syntactical rigidity: everything has to be spelled out rigorously, and basics properties like the commutativity of the product (i.e., writing $P_1 \mid P_2$ or $P_2 \mid P_1$ should not make a difference) are cumbersome to prove. The solution is to define an equivalence relation on processes, define another specification using it— SPEC_{CCS} —, and then to prove that they coincide.

Definition 1 (CCS Structural equivalence) *Structural equivalence on processes is the smallest equivalence relation—sometimes “closed under context”—generated by the following rules:*

$$\begin{array}{lll}
P \mid Q \equiv Q \mid P & (P \mid Q) \mid V \equiv P \mid (Q \mid V) & P \mid 0 \equiv P \\
P + Q \equiv Q + P & (P + Q) + V \equiv P + (Q + V) & P + 0 \equiv P \\
(P \backslash a) \mid Q \equiv (P \mid Q) \backslash a \text{ with } a \notin \text{fn}(Q) & (P \backslash a) \backslash b \equiv (P \backslash b) \backslash a & \\
A \stackrel{\text{def}}{=} P \Rightarrow A \equiv P & P =_{\alpha} Q \Rightarrow P \equiv Q &
\end{array}$$

Where $\text{fn}(Q)$ is the set of free names in Q , and $=_{\alpha}$ is the α -equivalence given by capture-free substitution.

SPEC_{CCS} is then defined by adding the rule $\frac{P'_1 \equiv P_1 \quad P_1 \xrightarrow{\alpha} P_2 \quad P_2 \equiv P'_2}{P'_1 \xrightarrow{\alpha} P'_2} \text{ con.}$ to LTS_{CCS} , and removing com._1 (or com._2), rec. and rel. from it. Finally, the correctness of SPEC_{CCS} is proven by showing that it is a “conservative extension of SYS_{CCS} ”, in the following sense:

Lemma 1 *If $P \xrightarrow{\alpha} P'$ with SYS_{CCS} and $P \equiv Q$ then $Q \xrightarrow{\alpha} Q'$ with SPEC_{CCS} and $P' \equiv Q'$.*

This lemma guarantees that reasoning modulo the structural congruence does not alter the correctness of the system, and that we don’t have to track small and innocuous modifications in the terms under study—it just cuts the red tape.

2 What About Reversible Calculii?

There are two ways of extending CCS to reversible calculus: the “static” approach “marks” each occurrence of an action, and gave birth to CCS with Communication Keys (CCSK) [11]. The “dynamic” approach uses *memories* attached to the threads of a process, and gave Reversible CCS (RCCS) [5, 6]. Both calculii evolved over the time, notably regarding structural equivalence.

CCSK Some versions of CCSK “does not exploit any structural congruence”¹ [11], while some other [7] uses a structural congruence that contains a significant subset of the one from CCS, plus a rule to deal with keys [7, p. 105].

To our knowledge, the innocuity of this latter congruence has not been proven, but it was shown that a model based on reversible bundle structure was “stable” [7, Proposition 4.9] under it.

RCCS RCCS’ congruence evolved as well, from containing additive structural congruence but not the α -equivalence [5, Section 2.3] to being pretty much only the α -equivalence [2]. But in any case, RCCS does not benefit from the clear distinction we discussed at the beginning of this paper. To understand why, let us explain how this system was designed.

In RCCS, reversibility is implemented thanks to memories that are *complete*—so that every forward step can be backtracked—, *minimal*—so that only the relevant information is saved—, but also *distributed*—to avoid centralization. Technically, *memories* are attached to the threads of a process.

$$\begin{aligned} T &:= m \triangleright P && \text{(Reversible Thread)} \\ R, S &:= T \parallel R \mid S \parallel R \backslash a && \text{(RCCS Processes)} \end{aligned}$$

for m a memory stack (whose definition [2] is not included here), and P a CCS process.

A forward *and* backward LTS is then defined, but it is extremely limited: any transition leading to $m \triangleright (P_1 \mid P_2)$ is blocked. Indeed, to fulfill our requirement to distribute as much as possible the memories, the system needs to block this execution, and to be given an equivalence rule

$$m \triangleright (P_1 \mid P_2) \equiv (\gamma.m \triangleright P_1) \mid (\gamma.m \triangleright P_2) \quad \text{(Distribution of memory)}$$

that distributes the computation (and the memory, prepended with a special “fork” symbol γ) over two units of computation.

There are two perspectives on this: 1. We can consider that the equivalence relation now becomes part of the definition of SYS_{RCCS} , and that there are no $\text{SPEC}_{\text{RCCS}}$, 2. We can consider that $\text{SPEC}_{\text{RCCS}}$ is strictly more expressive than SYS_{RCCS} .

Both approaches are somehow problematic since we are losing a way of syntactically assessing that the equivalence relation (which generally contains more than just Distribution of memory) is “the right one”, and have to assume that it is reasonable. The reduction semantics of CCS can also be considered to be SPEC_{CCS} , so we loose the clear distinction between the two (reduction semantics and LTS) in RCCS. Furthermore, to prove that RCCS and CCSK are equi-expressive [8], the authors had to remove from the rest of the LTS the possibility to use Distribution of memory between two transitions [8, Lemma 4], making their proof actually *harder*. All in all, the questions we are asking are,

1. Can we on one hand enrich this congruence (with e.g. some form of commutativity of parallel composition), and on the other extract from it the Distribution of memory rule?
2. What criteria should we use to determine that our newly defined SYS_{RCCS} and $\text{SPEC}_{\text{RCCS}}$ are correct?

Our first question aims at restoring the conceptual purity of our system and of the structural congruence, but also to provide tools to improve this latter (which is very limited, as of now). Regarding our second question, and similarly to what has been done with CCSK, a model of the memories based on configuration structures has been show to be stable under structural congruence [3, Lemma 43]. However, the congruence considered was very small, and the result applied only to memories, and not to processes as a whole.

¹As noted in a paper [8] that furthermore note that α -equivalence can and should be added in any case [8, Remark 2].

3 Conclusion

One of the true puzzle raised by this small introspection is the second question asked previously: while “making up” SYS_{RCCS} and $\text{SPEC}_{\text{RCCS}}$ is “easy”, gaining evidence that they are the correct systems, and that they are equi-expressive, is harder. The equivalence between CCSK and RCCS, as well as the numerous denotational models for those calculi and their simulation results, are good safe-guards that those models are relevant, and capture reversibility in a satisfactory way. But how can we endow them with “the right” structural congruence?

This investigation actually raises another question, less expected: looking back, the way CCS assesses that its equivalence relation is “the right one” is somehow circular, since our Lemma 1 uses the equivalence “on the outside” and “on the inside”. One of our current investigation is to precisely pinpoint why is this equivalence in CCS acceptable, and to see if the criteria we identify can be imported to RCCS and CCSK. Mechanized methods are likely to be of little help in this domain² as e.g. formalization of CCS in Coq [1] or of the π -calculus in Agda [10] either discard syntactical congruences, or pose them as axioms.

References

- [1] Reynald Affeldt & Naoki Kobayashi (2008): *A Coq Library for Verification of Concurrent Programs*. ENTCS 199, pp. 17 – 32, doi:10.1016/j.entcs.2007.11.010.
- [2] Clément Aubert & Ioana Cristescu (2017): *Contextual equivalences in configuration structures and reversibility*. J. Log. Algebr. Methods Program. 86(1), pp. 77–106, doi:10.1016/j.jlamp.2016.08.004.
- [3] Clément and Aubert (2020): *How Reversibility Can Solve Traditional Questions: The Example of Hereditary History-Preserving Bisimulation*. Available at <https://hal.archives-ouvertes.fr/hal-02568250>.
- [4] J.A. Bergstra, A. Ponse & S.A. Smolka, editors (2001): *Handbook of Process Algebra*. Elsevier Science, Amsterdam, doi:10.1016/B978-044482830-9/50017-5.
- [5] Vincent Danos & Jean Krivine (2004): *Reversible Communicating Systems*. In Philippa Gardner & Nobuko Yoshida, editors: CONCUR, LNCS 3170, Springer, pp. 292–307, doi:10.1007/978-3-540-28644-8_19.
- [6] Vincent Danos & Jean Krivine (2005): *Transactions in RCCS*. In Martín Abadi & Luca de Alfaro, editors: CONCUR, LNCS 3653, Springer, pp. 398–412, doi:10.1007/11539452_31.
- [7] Eva Graversen, Iain Phillips & Nobuko Yoshida (2018): *Event Structure Semantics of (controlled) Reversible CCS*. In Jarkko Kari & Irek Ulidowski, editors: *Reversible Computation - 10th International Conference, RC 2018, Leicester, UK, September 12-14, 2018, Proceedings*, LNCS 11106, Springer, pp. 102–122, doi:10.1007/978-3-319-99498-7_7.
- [8] Ivan Lanese, Dorian Medić & Claudio Antares Mezzina (2019): *Static versus dynamic reversibility in CCS*. Acta Inform., doi:10.1007/s00236-019-00346-6.
- [9] Robin Milner (1980): *A Calculus of Communicating Systems*. LNCS, Springer-Verlag, doi:10.1007/3-540-10235-3.
- [10] Roly Perera & James Cheney (2018): *Proof-relevant π -calculus: a constructive account of concurrency and causality*. MSCS 28(9), pp. 1541–1577, doi:10.1017/S096012951700010X.
- [11] Iain Phillips & Irek Ulidowski (2007): *Reversing algebraic process calculi*. J. Log. Algebr. Program. 73(1-2), pp. 70–96, doi:10.1016/j.jlap.2006.11.002.

²An impressive list of the “mechanized formalizations of the π -calculus (and friends)” can be found at <http://why-lambda.blogspot.com/2015/04/mechanized-formalizations-of-pi.html>.