On Decidability and Small Model Property of Process Equations*

Xinxin Liu

School of Cognitive and Computing Sciences

University of Sussex

Brighton BN1 9QH

England

October 1993

Abstract

This paper studies the *decidability* and *small model property* of process equations of the form

$$(P|\prod_{i=1}^{n} C_i(X_i))\backslash L \equiv (Q|\prod_{j=1}^{m} D_j(Y_j))\backslash K$$

where P, Q are finite state processes, X_i, Y_j are process variables, and $C_i(X_i)$, $D_j(Y_j)$ are process expressions *linear* in X_i and Y_j respectively. It shows that, when $n + m > 1$, the equation problem is not decidable and does not have small model property for any equivalence relation $\equiv$ which is at least as strong as complete trace equivalence but not stronger than strong bisimulation equivalence.

1 Introduction

This paper examines *small model property* and *decidability* of equations in process algebras [Mil80, Mil89, Hoa85, BK85, Bou85, Hen88]. In general, process equations have the following form

$$C(X_1, \ldots, X_n) \equiv D(Y_1, \ldots, Y_m) \tag{1}$$

where C, D are arbitrary process contexts, $X_1, \ldots, X_n$ and $Y_1, \ldots, Y_m$ are process variables, $\equiv$ is some equivalence relation on processes. Some well studied equivalence relations on processes are strong and weak bisimulation equivalences $\sim$ and $\approx$

*This work has been supported by the SERC grant GR/H16537

[Mil80, Mil89], branching bisimulation equivalence $\approx_b$ [vGW89], testing equivalence [dNH8], failure equivalence [BHR84], GSOS trace congruence or $\frac{2}{3}$–bisimulation equivalence [BIM88, LS89], and 2–nested simulation equivalence [GV89]. Equation (1) is said to be solved by processes $P_1, \ldots, P_n$ and $Q_1, \ldots, Q_m$ if the following equivalence holds

$$C(P_1, \ldots, P_n) \equiv D(Q_1, \ldots, Q_m)$$

In this case we say that (1) is *solvable*. A type of equation is said to be *decidable* if the where Q is a finite state process and $C(X)$ is linear in X:

$$C(X) \equiv Q \qquad (\ )$$

Results in [ZIG87, SI91, Liu92] show that, for many equivalence relations $\equiv$ (including $\sim$, $\approx$, and $\approx_b$), Q has a *characteristic formula* $F_Q^{\equiv}$ of the modal μ–calculus such that, for any process

Now, the blank tape in its initial state is just a row of cells in state $S_l(b)$. The following recursive definition gives the blank tape T

$$T \stackrel{d}{=} (S_l(b)[link/sr]|T[link/sl])\backslash link$$

The construction is pictured in Figure 1, where A and $\overline{A}$ are in fact two sets of ports named by the letters and barred letters in the alphabet of the Turing machine.

A Turing machine tape can also be described by the following infinite set of equations about $B(s_1, s_2)$, where $s_1 \in (A \cup \{b\})^*$ is the contents of the tape between the end of the tape and the currentS

Lemma 2.2 *When $\equiv$ is $\approx_t$, equation (4) has unique solution modulo $\approx_t$.*

Proof For any process P, lets write $D^n(P)$ for $D(D^{n-1}(P))$ when $n > 0$ and $D^0(P)$ for P. Notice that if $D^n(P) \stackrel{s}{\Longrightarrow} R$ and still give a better idea how R actually works. However, these τ's are necessary in order to satisfy the equation in the first part of Lemma 2.4 which enables us to derive more general conclusions. Otherwise, using the simpler definition, we can only show a weaker version of that equation with $\approx$ in place of $\sim$. From now on we will write $C(X, Y)$ for $(X[f_1]|R|Y[f_2])\backslash L_1 \cup L_2$. It is not difficult to see that a necessary condition for $C(P, Q)$ to be always capable of doing *syn* and nothing else (no *err*) is that whatever 24(rom)]TJ 1.4 980Td[(no)999.959(w)]TJ24.71990Td(on)Tj-408.4814.64

3 Main Results

With the preparation in the last section, we are now ready to show the main results of the paper, namely that many equation problems are undecidable and do not have small model property.

Theorem 3.1 *For any $\equiv$ such that $\sim\subseteq\equiv\subseteq\approx_t$, both the unary $1 \equiv 1$ equation problem and the binary $1 \equiv 1$ equation problem are not decidable and do not have the small model property.*

Proof It is sufficient to construct some effective reductions from the divergence problem of Turing machines, which is well known to be not semi–decidable. There is a systematic way of constructing a finite state process M_i which simulates the finite–state control mechanism of the i–th Turing machine for each i. Thus $(M_i|T)\backslash L$ will simulate the i–th Turing machine such that $(M_i|T)\backslash L \sim \tau^\omega$ if and only if the i–th Turing machine does not halt on a blank tape, and also that $(M_i|T)\backslash L$ outputs something if and only if the i–th Turing machine halts, where τ^ω is the process which only performs internal actions for ever. Now we can show that the i–th Turing machine diverges if and only if the following unary $1 \equiv 1$ equation is solvable when $\sim\subseteq\equiv\subseteq\approx_t$ and $a \neq b$

$$a.(M_i|X)\backslash L + b.X \equiv a.\tau^\omega + b.D(X) \tag{5}$$

For one direction, suppose the i–th Turing machine diverges, that is to say $(M_i|T)\backslash L \sim \tau^\omega$. Since $T \sim D(T)$, and $\sim\subseteq\equiv$, T solves equation (6).

For the converse direction, suppose T' solves equation (6). Because $\equiv\subseteq\approx_t$ and $a \neq b$, in this case $(M_i|T')\backslash L \approx_t \tau^\omega$ and $T' \approx_t D(T')$. By Lemma 2.2 $T' \approx_t T$, thus $(M_i|T)\backslash L \approx_t (M_i|T')\backslash L \approx_t \tau^\omega$, and the i–th Turing machine diverges on a blank tape (otherwise $(M_i|T)\backslash L$ should be able to output something).

Similarly, it is easy to work out that the i–th Turing machine diverges if and only if the following binary $1 \equiv 1$ equation is solvable when $\sim\subseteq\equiv\subseteq\approx_t$ and a, b, c are three different actions

$$a.(M_i|X)\backslash L + b.X + c.D(X) \equiv a.\tau^\omega + b.Y + c.Y \tag{6}$$

Thus we showed effective reductions from the divergence problem of Turing machines to the unary and binary $1 \equiv 1$ equation problems. So the unary $1 \equiv 1$ equation problem and the binary $1 \equiv 1$ equation problem are not semi-decidable and thus not decidable.

In order to prove that a type of equation does not have the small model property, we only need to find a solvable equation of that type and show that any solution to the equation has infinite states. It is easy to see from Lemma 2.2 and Lemma 2. that, when $\equiv\subseteq\approx_t$, equation (4) is a solvable unary $1 \equiv 1$ equation which only has infinite state solutions. Also for the same reason, when $\equiv\subseteq\approx_t$ and $a \neq b$, the following is a solvable binary $1 \equiv 1$ equation which only has infinite state solutions.

$$a.X + b.D(X) \equiv a.Y + b.Y$$

but only have infinite state solutions

$$((a.(D(X)[f_1])|R) + b.(X[f_1]|R))|(\bar{a}.X[f_2] + \bar{b}.D(X)[f_2]))\backslash L_1 \cup L_2 \quad \equiv \tau.C(T_0, T_0)$$

$$((a.X[f_1] + a.D(X)[f_1] + b.X[f_2] + \bar{b}.D(X)[f_2]) \\ |(\bar{a}.(R|Y[f_2]) + \bar{b}.(Y[f_1]|R))\backslash L_1 \cup L_2 \quad \equiv \tau.C(T_0, T_0)$$

Thus both unary and binary $2 \equiv 0$ equation problems do not have small model property. □

4 Conclusion and Related Works

In the last section we showed that four types of $n \equiv m$ equation problems are not decidable and do not have small model property for any equivalence relation which is as least as strong as complete trace equivalence (this can be relaxed to trace equivalence in the case of $1 \equiv 1$) but not stronger than strong bisimulation equivalence. These four types of equation problems are the unary and binary $1 \equiv 1$ equation problems and the unary and binary $2 \equiv 0$ equation problems. Undecidability of $1 \equiv 1$ equation problems is somewhat expected because recursion can be coded into such an equation problem, but undecidability of $2 \equiv 0$ equation problems is rather unexpected. This shows the computation power of communication.

The negative results about these four basic types of equation problems have very general implications. Because any k–ary $n \equiv m$ equation problem with $m + n > 1$ would have one of these basic problems as special case, such k–ary $n \equiv m$ equation problem is surely undecidable and does not have the small model property if $\equiv$ is and 00.64(am)Tj/1R.78(f.)1000. 7(yp)-1000.67f

m

Another interesting line of research is to identify some decidable subclass of k–ary $n \equiv m$ equation problems. Here the results of [MM90, Mol89, CHM9 b] about unique decomposition of processes may provide some clue. To be somewhat more precise, results in [MM90, Mol89, CHM9 b] show that for certain processes P, there exists a unique decomposition $P_1 \| \ldots \| P_m$ where $\|$ is the merge operator which is like $|$ but without communication. Thus for such process P, we can decompose this kind of k–ary $n \sim 0$ equation

$$C_1(X_1) \| \ldots \| C_n(X_n) \sim P$$

into a set of $1 \sim 0$ equations. It is easy to see that the possibility of such decompositions are

[CHM9 b] S. Christensen, Y. Hirshfeld, and F. Moller. Decomposbility, decidability, and axiomatisability for bisimulation equivalence. In *Proceedings on Logic in Computer Science*, 199 .

[CHS92] S. Christensen, H. Hüttel, and C. Stirling. Bimimulation equivalence is decidable for all context–free processes. *Lecture Notes In Computer Science, Springer Verlag*, 6 0, 1992.

[dNH8] R. de Nicola and M. Hennessy. Testing equivalence for processes. *Theoretical Computer Science*, 4:205–228, 198 .

[Dro92] N. J. Drost. Unification in the algebra of sets with union and empty set. Technical Report Report P921 , University of Amsterdam, July 1992.

[GV89] J.F. Groote and F.W. Vaandrager. Structured operational semantics and bisimulation as a congruence. *Lecture Notes In Computer Science, Springer Verlag*, 72, 1989. Proceedings of ICALP89.

[Hen88] M. Hennessy. *An Algebraic Theory of Processes.* MIT Press, 1988.

[Hoa85] C.A.R. Hoare. *Communicating Sequential Processes.* Prentice–Hall, 1985.

[HS91] H.

[LS89] K.G. Larsen and A. Skou. Bisimulation through probabilistic testing. *Proceedings of Principles of Programming Languages*, 1989.

[Mil80] R. Milner. *Calculus of Communicating Systems*, volume 92 of *Lecture Notes In Computer Science, Springer Verlag*. Springer Verlag, 1980.

[Mil89] R. Milner. *Communication and Concurrency*. Prentice–Hall, 1989.

[MM90] R. Milner and F. Moller. Unique decomposition of processes. *Bulletin of the European Association for Theoretical Computer Science*, 41:226–2 2, 1990.

[Mol89] F. Moller. *Axioms for Concurrency*. PhD thesis, University of Edinburgh, Mayfield Road, Edinburgh, Scotland, 1989.

[Par89] J. Parrow. Submodule construction as equation solving in CCS. *Theoretical Computer Science*, 1989.

[QL90] H. Qin and P. Lewis. Factorization of finite state machines under observational equivalence. *Lecture Notes In Computer Science, Springer Verlag*, 458, 1990.

[SE89] Robert S. Streett and E. Allen Emerson. An automata theoretic decision procedure for the propositional mu-calculus. *Information and Computation*, 81:249–264, 1989.

[Shi89] M.W. Shields. A note on the simple interface equation. *The Computer Journal*, 2(5), 1989.

[SI91] B. Steffen and A. Ingolfsdottir. Characteristic formulae for processes with divergence. Technical Report Technical Report 1/91, School of Congnitive and Computing Sciences, University of Sussex, 1991.

[vGW89] R. J. van Glabbeek and W.P. Weijland. Branching time and abstraction in bisimulation semantics (extended abstract). *Information Processing 89*, pages 61 –618, 1989.

[ZIG87] Michael Zeeberg, Anna Ingolfsdottir, and Jens Christian Godskesen. Fra hennessy–milner