Alternative quantification vs. input prefixing

Jan Friso Groote[1,2] Bas Luttik[1,3,*†]

JanFriso.Groote@cwi.nl Bas.Luttik@cwi.nl

[1] *CWI, P.O. Box 94079, NL-1090 GB Amsterdam, The Netherlands*

[2] *Computing Science Department, Eindhoven University of Technology P.O. Box 513, NL-5600 MB Eindhoven, The Netherlands*

[3] *Department of Computer Science University of Amsterdam Kruislaan 403, NL-1098 SJ Amsterdam, The Netherlands*

Abstract

This is a summary of our paper "Process algebras with alternative quantification over data" (Groote and Luttik (1998)). In this paper, we define a class of process algebras with a generalised operation $\sum$ that allows explicit treatment of *alternative quantification* over data, and investigate the specific subclass formed by the algebras of finite processes modulo strong bisimulation. We have shown that, in such algebras, equality between finite processes is definable by means of a first-order data formula, and that, if the data is computable and has a built-in equality predicate, any Π^0_4 data formula is definable by means of an equation between ground process terms. Hence, equality in strong bisimulation algebras with a computable data part is Π^0_4-hard.

We have also investigated a restricted version of alternative quantification: the input prefix mechanism of Parrow and Sangiorgi (1995) and Hennessy and Lin (1996). This restriction, for computable data with a built-in equality predicate, yields a less expressive formalism, namely equality in the strong bisimulation algebra coincides with the universal fragment of first-order logic for the data; so the input prefix mechanism gives rise to strong bisimulation algebras for which equality is complete in Π^0_1.

1 Process algebras with alternative quantification

A *process algebra* is an algebra that contains a universe P and binary operations $+$ and $\cdot$ on P such that $\langle \mathrm{P}, + \rangle$ is a semilattice, $\langle \mathrm{P}, \cdot \rangle$ is a semigroup, and $\cdot$ distributes from the right over $+$. The operation $+$ is used to model *alternative composition*, a nondeterministic choice between its arguments, and $\cdot$ stands for *sequential composition*, performing its second argument upon completion of its first. A many-sorted process algebra that does not contain operations that take the sort of processes into some other sort, is often called a *process algebra with data*; the

* Corresponding author.

† Research supported by the Netherlands Organization for Scientific Research (NWO) under contract SION 612-33-008.

data being the reduct one obtains by removing the universe of processes and all operations involving this universe.

The algebras that we have considered consist of a many-sorted algebra $\mathfrak{D}$ of data that contains a two-element boolean algebra, and have besides the usual process algebraic operations $+$ and $\cdot$:

1. a constant $\boldsymbol{\delta}$ modelling unsuccesful termination (it is a unit for $\langle \mathrm{P}, + \rangle$ and additionally satisfies $\boldsymbol{\delta} \cdot \mathbf{p} = \boldsymbol{\delta}$ for all $\mathbf{p} \in \mathrm{P}$);

2. operations $\mathsf{a} : \mathrm{D}_1 \times \cdots \times \mathrm{D}_n \to \mathrm{A}$ that map an n-tuple of data elements injectively onto a special set $\mathrm{A} \subseteq \mathrm{P}$, the elements of which will be called *atomic actions*;

3. a ternary operation

$$\mathbf{p} \lhd \mathbf{b} \rhd \mathbf{q} \mapsto \begin{cases} \mathbf{p} & \text{if } \mathbf{b} = \top \\ \mathbf{q} & \text{if } \mathbf{b} = \bot \end{cases}$$

   that receives a boolean $\mathbf{b}$ and processes $\mathbf{p}$ and $\mathbf{q}$ and yields the process that performs a choice between $\mathbf{p}$ and $\mathbf{q}$, but one that depends on the evaluation of $\mathbf{b}$; the construction should be read "$\mathbf{p}$ if $\mathbf{b}$, else $\mathbf{q}$".

4. a generalised (or: infinitary) operation $\sum : (\mathsf{Pow}(\mathrm{P}) - \emptyset) \to \mathrm{P}$ ($\mathsf{Pow}(\mathrm{P})$ refers to the set of all subsets of P), defined by

$$\mathrm{P}' \mapsto \textstyle\sum \mathrm{P}' \qquad \text{(we shall view } + \text{ as a special case of } \textstyle\sum).$$

Our major concern is with this latter operation: *alternative quantification* over data. We have given it a universal algebraic definition in the same way as Rasiowa and Sikorski (1963) generalise the binary joins ($\vee$) and meets ($\wedge$) of boolean algebras to obtain existential ($\exists$) and universal ($\forall$) quantification. In our signatures alternative quantification is present as an operation symbol that binds a data variable. That is, we shall write $\sum_{x:s} p$ (p some process term and x a variable of data sort s) to denote the (possibly infinite) expression

$$p[x := d_0] + p[x := d_1] + p[x := d_2] + \ldots,$$

where $d_0, d_1, d_2, \ldots$ is an enumeration of the universe associated with data sort s.

Alternative quantification is a very useful feature, since it can be used to model the notion of *input*: if $\mathbf{r}(n)$ refers to the atomic action of reading the natural number n, then $\sum_{x:\mathbb{N}} \mathbf{r}(x)$ can be used to refer to the process that can read any natural number; it is a choice between reading 0, or 1, or 2, ...

Let $\mathfrak{P}$ denote the algebra containing $\mathfrak{D}$ and a universe of processes P consisting of the expressions generated by A and operations $\boldsymbol{\delta}$, $\cdot$ and $\sum$ as defined above. The transition relation $\longrightarrow \subseteq \mathrm{P} \times \mathrm{A} \times (\mathrm{P} \cup \{\epsilon\})$ is defined in Table 1. A binary relation $\mathcal{R} \subseteq \mathrm{P} \times \mathrm{P}$ is a *bisimulation* if it is symmetric and satisfies

> if $\langle \mathbf{p}, \mathbf{q} \rangle \in \mathcal{R}$ and $\mathbf{p} \xrightarrow{\mathbf{a}} \mathbf{p}'$, then there exists $\mathbf{q}' \in \mathrm{P} \cup \{\epsilon\}$ such that $\mathbf{q} \xrightarrow{\mathbf{a}} \mathbf{q}'$ and $\langle \mathbf{p}', \mathbf{q}' \rangle \in \mathcal{R} \cup \{\langle \epsilon, \epsilon \rangle\}$.

$$\mathbf{a} \xrightarrow{\mathbf{a}} \epsilon \qquad \text{for all } \mathbf{a} \in \mathrm{A}$$

$$\frac{\mathbf{p} \xrightarrow{\mathbf{a}} \mathbf{p}'}{\mathbf{p} \cdot \mathbf{q} \xrightarrow{\mathbf{a}} \mathbf{p}' \cdot \mathbf{q}} \qquad \frac{\mathbf{p} \xrightarrow{\mathbf{a}} \epsilon}{\mathbf{p} \cdot \mathbf{q} \xrightarrow{\mathbf{a}} \mathbf{q}} \qquad \mathbf{a} \in \mathrm{A} \text{ and } \mathbf{p}, \mathbf{p}', \mathbf{q} \in \mathrm{P}$$

$$\frac{\mathbf{p} \xrightarrow{\mathbf{a}} \mathbf{q}}{\sum \mathrm{P}' \xrightarrow{\mathbf{a}} \mathbf{q}} \qquad \mathbf{a} \in \mathrm{A},\ \mathbf{p} \in \mathrm{P}' \subseteq \mathrm{P} \text{ and } \mathbf{q} \in (\mathrm{P} \cup \{\epsilon\})$$

Table 1: The transition system specification for $\mathfrak{P}$.

We write $\mathbf{p} \leftrightarroweq \mathbf{q}$ if there exists a bisimulation that contains the pair $\langle \mathbf{p}, \mathbf{q} \rangle$. The union of $\leftrightarroweq$ with the diagonals on the data universes defines a congruence (that we also denote by $\leftrightarroweq$) on $\mathfrak{P}$ and it turns out that $\mathfrak{P}/\leftrightarroweq$ is a process algebra with data, conditionals and alternative quantification.

2 Undecidability of strong bisimulation

Let us refer by the term *finite process* to those elements of P that are denoted by a ground process term (i.e. one that does not contain free variables). We have shown that bisimulation is definable by means of a first-order formula in the language of the data. We have also found that if the data algebra has a built-in equality predicate, then we can translate any closed first-order data formula φ in prenex form that starts with a universal quantifier and has a prefix consisting of three alternations, to a pair of finite processes $\langle \mathbf{p}_\varphi, \mathbf{q}_\varphi \rangle$ such that $\mathbf{p}_\varphi \leftrightarroweq \mathbf{q}_\varphi$ iff $\mathfrak{D} \models \varphi$. Taking for $\mathfrak{D}$ the field of integers with built-in equality, and using the result of Matijasevič (1970) that any r.e. set is definable by means of a formula $\exists x_1{:}\mathbb{Z} \ldots \exists x_{13}{:}\mathbb{Z}(P \approx 0)$, we conclude that strong bisimulation on finite processes is Π^0_4-hard (any problem in Π^0_4 can be reduced effectively to the problem of whether two processes are bisimilar).

We have also considered the expressivity of the input prefix mechanism, a restricted version of alternative quantification, used by Hennessy and Lin (1995) and Parrow and Sangiorgi (1995) to model input. Let us refer by the term *input prefix process* to those elements of P that are denoted by a process term in which alternative quantification only occurs in the form $\sum_{\bar{x}:\bar{s}} \mathsf{a}(\bar{x})p \lhd b \rhd \delta$.[1] It turns out that bisimulation on the set of input prefix processes is definable by a *universal* data formula. This also follows from the work of Hennessy and Lin (1995), but we give an alternative proof of this fact. Moreover, we have shown that for any universal data formula φ one can find a pair of input prefix processes $\langle \mathbf{p}_\varphi, \mathbf{q}_\varphi \rangle$ such that $\mathbf{p}_\varphi \leftrightarroweq \mathbf{q}_\varphi$ iff $\mathfrak{D} \models \varphi$. Thus we conclude that strong bisimulation on input prefix processes is complete in Π^0_1, and hence, in bisimulation semantics alternative quantification is

[1]this is, in fact, a somewhat more liberal definition than used by aforementioned authors: they excluded the part $\_ \lhd b \rhd \delta$.

strictly more expressive than input prefixing.

3 Complete axiomatisations

It follows from these results, that there is no general complete axiomatisation of strong bisimulation, not even if we restrict alternative quantification to input prefixing. Hennessy and Lin (1996) devise a complete proof system for a language with input prefixing that is based on a presumed complete proof system for a data algebra (with a built-in equality predicate) that allows the derivation of propositions of the form $b \triangleright s = t$, meaning that the identity $s \approx t$ holds in $\mathfrak{D}$ for every valuation that assigns $\top$ to b. Evidently, such a proof system does not always exist (e.g., it does not exist for the field of integers with built-in equality). We have given a complete axiomatisation of strong bisimulation for the language with alternative quantification under the assumption that the data has built-in equality and built-in Skolem functions (i.e., the first-order theory of the data algebra should be decidable).

We have found a data algebra that has an (infinite) ω-complete axiomatisation and built-in equality for which strong bisimulation is Π^0_2-hard. Thus we were able to motivate the requirement that the data should have built-in Skolem functions: the restriction to algebras that have built-in equality and an ω-complete axiomatisation of Hennessy and Lin (1996) does not enforce the existence of a complete axiomatisation of strong bisimulation for the language with alternative quantification.

References

Groote, J. F. and Luttik, S. P. (1998). Undecidability and completeness results for process algebras with alternative quantification over data. Report SEN-R9806, CWI, The Netherlands. Available from `http://www.cwi.nl/~luttik/`.

Hennessy, M. and Lin, H. (1995). Symbolic bisimulations. *Theoretical Computer Science*, **138**(2), 353–389.

Hennessy, M. and Lin, H. (1996). Proof systems for message-passing process algebras. *Formal Aspects of Computing*, **8**(4), 379–407.

Matijasevič, Y. (1970). Enumerable sets are diophantine. *Soviet Math. Dokl.*, **11**, 345–358.

Parrow, J. and Sangiorgi, D. (1995). Algebraic theories for name-passing calculi. *Information and Computation*, **120**(2), 174–197.

Rasiowa, H. and Sikorski, R. (1963). *The mathematics of metamathematics*. Pańs̈towe wydawnictwo naukowe, Warszawa, Poland.