Computer Assisted Manipulation of Algebraic Process Specifications

Jan Friso Groote and Bert Lisser
J.F.Groote@tue.nl, Bert.Lisser@cwi.nl

CWI
P.O. Box 94079, 1090 GB Amsterdam, The Netherlands

ABSTRACT
Specifications of system behaviour tend to become large. Analysis of such specifications requires automated tools. Most attention hitherto has been invested in fully automatic tools. We however believe that in many cases human intervention is required and we therefore propose a number of computer tools to transform process specifications. The concrete manipulation tools that we describe can eliminate constants, redundant sum variables and parameters, and allow to split variables ranging over complex datatypes. These tools can transform specifications with large finite state spaces to variants with state spaces being a fraction of their original size, and transform specifications with infinite state spaces to those with finite state spaces.

2000 Mathematics Subject Classification: 68M14, 68Q60, 68Q85
Keywords and Phrases: Automated Reasoning, Distributed systems, Linear Process Equations, Model Checking, Verification
Note: Research carried out in SEN2, with financial support of the "Systems Validation Center".

1. Introduction

Tools and techniques for the analysis of system behaviour become increasingly powerful. Currently, we can regularly, automatically and thus efficiently answer questions about systems with a restricted state space, and we can also occasionally obtain insight in the behaviour of more substantial systems. But the results in this last category, often require ingenuity, insight in the problem domain, and often the ad hoc design or adaption of tools.

We believe that this is typical for the study of more complex systems. In the first place, fully automatic analysis tools are generally not able to perform the analysis of complex systems fully on their own. This explains why human ingenuity is required in the process. In the second place, it is out of the question that these systems be analysed by hand only. The size of such descriptions may literally stretch to up to thousands of pages. This is why automation is needed.

We think that it is not desired that for each complex system to be analysed in the future, new transformation programs must be designed, or old analysis programs must be adapted. It is better to provide a set of manipulation tools that can be used to preprocess and transform a given system such that it fits a standard analysis tool.

Note that such a situation is not very uncommon in the field of mathematical analysis. Typical mathematical analysis tools such as *Mathematica* and *Maple* do not attempt to solve a formula on their own, but they operate under strict supervision of a user, who, when sufficiently skilled in the use of such a tool, can lead the system to an answer.

In this paper we describe a number of transformation tools that we have developed. We show how in certain cases we can manipulate descriptions of distributed systems to reduce their state spaces from infinite to finite, or to a fraction of their original size.

We work in the setting of process algebra with data μCRL [10], or more precisely in the setting of linear process equations. The language μCRL is a straightforward process algebra, based on ACP_τ [2],

which means that it comprises operators such as $+, \cdot, \|, \tau_I$ and ∂_H extended with equational abstract datatypes. In order to combine data with processes the then_if_else operator $\_\triangleleft\_\triangleright\_$ and the choice over a possibly infinite datatype $\sum_{d:D}$ have been added, and parametric process variables and actions are allowed. This language is rather compact, but sufficiently complete to describe virtually any distributed system. When investigating systems described in μCRL our current standard approach is to transform these processes to linear process equations (LPEs). In essence this is a vector of data parameters and a list of condition, action and effect triples that describes when an action may happen, and what its effect is on the vector of data parameters. An LPE is a special instance of a μCRL process. In [11, 16] it is described how a large class of μCRL processes can be transformed automatically to LPE format in such a way that the resulting LPE is strongly bisimilar to the original. Our transformation tools work strictly on LPEs.

There are three tools that we describe here:

Elimination of constant process parameters (Subsection 4.1)**.** A parameter of an LPE can be replaced by a constant value, if that parameter remains constant throughout any run of the process.

Elimination of sum variables (Subsection 4.3)**.** It happens that the choice over infinite datatypes is restricted in the condition to a single concrete value. In that case it is more efficient to replace the sum variable by this single value.

Elimination of inert process parameters (Subsection 4.2)**.** A parameter of an LPE can be removed, if that parameter does not influence the behaviour of a process (has neither directly or nor indirectly influence on actions and conditions). We call such a parameter a inert parameter. Whereas the first two reduction techniques only simplify the description of an LPE, this one also allows substantial reduction of the state space underlying an LPE. Actually, if the inert process parameter ranges over an infinite domain, the state space can be changed from infinite to finite by this operation.

The reduction methods have been implemented in the μCRL toolset [18]. We explain all the reduction techniques and show that they are sound in the sense that they maintain strong bisimulation. Furthermore, in some cases we show the strength of the algorithm, by providing a theorem to which extent the transformation can be considered complete. We show how the tools interact restricting the sequences in which they need to be applied and we show the effect of the tools on a number of rather diverse communication protocols.

Currently, we are working on a next generation of these tools. The reasoning engine we use is an extremely fast rewriting engine built according to the ideas in [1]. We found that with an adequate theorem prover [15] , we can on the one hand increase the power of the current tools, and on the other hand build additional tools, for instance those based on confluence reduction [5] [12] of which first prototypes are very promising.

2. Preliminaries

The *Micro Common Representation Language* [10], *μCRL*, has been defined to describe interacting processes that rely on data. This language includes a formalism for algebraic specification of abstract data types (data part) and the Algebra of Communicating Processes with abstraction, *ACP* [6] [2] (process part). An algebraic specification consists of a signature which contains the definitions of abstract data types, constructors, and operators, and a set of equations. In subsections 2.1 and 2.2 we describe the data part. In the subsequent subsections we describe linear process equations and bisimulation.

2.1 Algebraic specifications of abstract data types

In this subsection we describe the basic aspects of abstract data types in a standard way, see e.g. [17]. We make a distinction between 'ordinary' functions, which we call *mappings*, and *constructors*, with the requirement that all terms of a sort that contains constructors can be written using constructors only.

Throughout the text we assume the existence of an infinite set V of variable declarations of the form x: $\mathbf{S}$, where $\mathbf{S}$ is some sort.

Definition 2.1. A *signature* is a triple $\Sigma = (\mathcal{S}, \mathcal{F}, \mathcal{M})$ where

- $\mathcal{S}$ is a set of *sorts*. We assume that **Bool** is an existing sort, i.e. $\mathbf{Bool} \in \mathcal{S}$;
- $\mathcal{F}$ is a set of *constructors*, i.e. functions of the form f: $\mathbf{S}_1 \times \cdots \times \mathbf{S}_n \to \mathbf{S}$ and $\mathbf{S}_i, \mathbf{S} \in \mathcal{S}$. Moreover, we presuppose the existence of the constructors $\mathsf{t}, \mathsf{f} :\to \mathbf{Bool}$ in $\mathcal{F}$; t stands for "true" and f for "false".
- $\mathcal{M}$ is a set of *mappings*, i.e. functions of the form f: $\mathbf{S}_1 \times \cdots \times \mathbf{S}_n \to \mathbf{S}$ and $\mathbf{S}_i, \mathbf{S} \in \mathcal{S}$. The sets $\mathcal{F}$, $\mathcal{M}$ and V are pairwise disjoint.

We call $\mathbf{S} \in \mathcal{S}$ a Σ-*constructor sort* iff there is a function symbol f: $\mathbf{S}_1 \times \cdots \times \mathbf{S}_n \to \mathbf{S}$ in $\mathcal{F}$. A Σ-*term* is a term defined over the signature Σ in the standard way.

We use substitutions mapping variables to terms with the same sort. We typically use either the letter ρ, or $[x{:=}t]$ for substitutions.

Definition 2.2. An *abstract data type* is a tuple $\mathcal{A} = (\Sigma, \mathcal{E})$ where

- $\Sigma = (\mathcal{S}, \mathcal{F}, \mathcal{M})$ is a signature;
- $\mathcal{E}$ is a set of *equations* (generally used as *rewrite rules*), i.e. expressions of the form $t = u$ with both t and u Σ-terms of some sort $\mathbf{S} \in \mathcal{S}$.

We specify data types using the syntax of μCRL [10]. The function symbols that follow the keyword **func** are constructors. The function symbols that follow **map** are mappings. Here follows an example of an algebraic specification of the datatype **Bool**.

Example 2.3. The data type associated with the sort **Bool** consists of the constants t (true) and f (false). Mappings $\neg$ and $\wedge$ are specified.

sort **Bool**
func $\mathsf{t}, \mathsf{f} :\to \mathbf{Bool}$
map $\neg : \mathbf{Bool} \to \mathbf{Bool}$, $\wedge : \mathbf{Bool} \times \mathbf{Bool} \to \mathbf{Bool}$
var $b : \mathbf{Bool}$
rew $\neg\mathsf{t} = \mathsf{f}$, $\neg\mathsf{f} = \mathsf{t}$, $\mathsf{t} \wedge b = b$, $\mathsf{f} \wedge b = \mathsf{f}$

2.2 Interpretation of abstract data types

We interpret an abstract data type using model class semantics, of which we describe only the main ingredients here (see [8] for a detailed account).

Let $\mathcal{A} = (\Sigma, \mathcal{E})$ be an abstract data type with $\Sigma = (\mathcal{S}, \mathcal{F}, \mathcal{M})$ a signature. For each $\mathbf{S} \in \mathcal{S}$ there is a non empty domain $\mathbf{D_S}$ and a valuation σ that maps variables of sort $\mathbf{S}$ to elements of $\mathbf{D_S}$. $\mathbb{M} = \{\mathbf{D_S} | \mathbf{S} \in \mathcal{S}\}$ is a model of $\mathcal{A}$ iff for every sort $\mathbf{S}$ of the abstract data type there is some interpretation $[\![\cdot]\!]^\sigma$ that maps each term of sort $\mathbf{S}$ to an element of $\mathbf{D_S}$, coincides with σ on the variables, and respects the equations $\mathcal{E}$. An interpretation $[\![\cdot]\!]^\sigma$ respects the equations $\mathcal{E}$ iff the following applies: if $t = u \in \mathcal{E}$ then $[\![t]\!]^\sigma = [\![u]\!]^\sigma$.

If $\mathbf{S}$ is a constructor sort, then each element of $\mathbf{D_S}$ must be equal to a term consisting of constructors only, possibly applied to elements of non constructor domains. We say two terms are equal, notation $t = u$ when for every model of $\mathcal{A}$ and interpretation function t and u are interpreted as the same element in the domain. We can reason about equality using standard equational logic enhanced with induction principles for constructors.

For the sort **Bool** with elements t and f we assume that $\mathbf{D_{Bool}}$ is a domain with exactly two elements representing t and f. We also assume that for each sort $\mathbf{S}$ there is a mapping $\doteq: \mathbf{S} \times \mathbf{S} \to \mathbf{Bool}$ that represents equality between terms of sort $\mathbf{S}$. I.e., $t \doteq u = \mathsf{t}$ iff $t = u$.

2.3 Linear Process Equations

We specify processes in μCRL, which is ACP [6] [2], comprising in essence actions and the operators $+$, $\cdot$, $\|$, ∂_H, τ_I, δ, extended with abstract data types. Furthermore, actions and processes can be parameterised with data, and there are two new operators, namely $\sum_{d:D}$, the sum over possibly infinite data types, and $\_ \lhd \_ \rhd \_$ which is the then-if-else operator. Despite the fact that μCRL is a straightforward language, we want an even more straightforward form to facilitate analysis. This basic form is called a linear process equation (LPE) and it consists essentially of a state vector of typed variables and a list of condition-action-effect triples. The LPE basic format is particularly powerful, because it allows parallel processes to be combined without the *state space explosion* effect that occurs in automata. There are effective algorithms to transform process specifications to LPEs [11]. Recently specifications with 250 parallel components and over thousand pages of description have been transformed to LPE format [4].

We want an LPE to be a μCRL process itself, explaining the process algebraic formulation of the condition-action-effect rules below:

Definition 2.4. Let $\Sigma = (\mathcal{S}, \mathcal{F}, \mathcal{M})$ be the signature defined in the data part. A *linear process equation (LPE)* over Σ is an expression of the form:

$$X(d_1{:}D_1, \ldots, d_n{:}D_n) = \sum_{i \in I} \sum_{e_1^i : E_1^i} \cdots \sum_{e_{n_i}^i : E_{n_i}^i} a_i(f_i)\, X(g_1^i, \ldots, g_n^i) \lhd c_i \rhd \delta$$

where I is a finite index set, and for each $i \in I$:

- $d_1, \ldots, d_n, e_1^i, \ldots, e_{n_i}^i$ are pairwise different variables;
- $D_1, \ldots, D_n, E_1^i, \ldots, E_{n_i}^i \in \mathcal{S}$;
- f_i is a Σ-term in which variables $d_1, \ldots, d_n$ and $e_1^i, \ldots, e_{n_i}^i$ may occur;
- for $1 \leq j \leq n$, g_j^i is a Σ-term of sort D_j in which variables $d_1, \ldots, d_n$ and $e_1^i, \ldots, e_{n_i}^i$ may occur;
- c_i is a Σ-term of sort **Bool** in which variables $d_1, \ldots, d_n$ and $e_1^i, \ldots, e_{n_i}^i$ may occur.

Sometimes we provide an initial state $s_1, \ldots, s_n$ for an LPE. It is convenient to use the vector notation $\vec{s}$ for $s_1, \ldots, s_n$. Consequently, we speak about the initial vector. The process $X(\vec{s})$ represents the behaviour of X from initial state $\vec{s}$. In μCRL a process definition, and hence an LPE, is preceded with the keyword `proc` and an initial state with the keyword `init`. See e.g. the example in Section 4.4.

2.4 Bisimulation

All the reduction methods that we present preserve strong bisimulation. Therefore, we define the notion of strong bisimulation on LPEs directly.

Definition 2.5. Let $\mathcal{A} = (\Sigma, \mathcal{E})$ be a datatype. Let

$$X(d_1{:}D_1, \ldots, d_n{:}D_n) = \sum_{i \in I} \sum_{e^i_1 : E^i_1} \cdots \sum_{e^i_{n_i} : E^i_{n_i}} a_i(f_i)\, X(g^i_1, \ldots, g^i_n) \lhd c_i \rhd \delta$$

and

$$Y(d'_1{:}D'_1, \ldots, d'_{n'}{:}D'_{n'}) = \sum_{i \in I'} \sum_{e'^i_1 : E'^i_1} \cdots \sum_{e'^i_{n'_i} : E'^i_{n'_i}} a'_i(f'_i)\, Y(g'^i_1, \ldots, g'^i_{n'}) \lhd c'_i \rhd \delta$$

be LPEs. Assume $\mathbb{M}$ is a model for $\mathcal{A}$. Let $\mathbf{D}_1, \ldots, \mathbf{D}_n$, $\mathbf{D}'_1, \ldots, \mathbf{D}'_{n'}$, $\mathbf{E}^i_1, \ldots, \mathbf{E}^i_{n_i}$ for all $i \in I$ and $\mathbf{E}'^i_1, \ldots, \mathbf{E}'^i_{n'_i}$ for all $i \in I'$ be the domains belonging to $D_1, \ldots, D_n$, $D'_1, \ldots, D'_{n'}$, $E^i_1, \ldots, E^i_{n_i}$ for all $i \in I$ and $E'^i_1, \ldots, E'^i_{n'_i}$ for all $i \in I'$. We write $\mathbf{d}$ for elements from $\mathbf{D}_1 \times \cdots \times \mathbf{D}_n$ and the jth element of $\mathbf{d}$ is written as $\mathbf{d}_j$. Similarly, we write $\mathbf{d}'$ for elements from $\mathbf{D}'_1 \times \cdots \times \mathbf{D}'_{n'}$, $\mathbf{e}^i$ for elements from $\mathbf{E}^i_1 \times \cdots \times \mathbf{E}^i_{n_i}$ and $\mathbf{e}'^{i'}$ for elements from $\mathbf{E}'^{i'}_1 \times \cdots \times \mathbf{E}'^{i'}_{n'_{i'}}$. Below σ is a valuation mapping variable d_j to $\mathbf{d}_j$ and variable e^i_j to value $\mathbf{e}^i_j$, and σ' is a valuation that maps variable d'_j to $\mathbf{d}'_j$ and variable $e'^{i'}_j$ to value $\mathbf{e}'^{i'}_j$. A relation $R \subseteq (\mathbf{D}_1 \times \cdots \times \mathbf{D}_n) \times (\mathbf{D}'_1 \times \cdots \times \mathbf{D}'_{n'})$ is called a bisimulation relation w.r.t. $\mathcal{A}$ and $\mathbb{M}$ iff for all $\mathbf{d}$ and $\mathbf{d}'$ such that $\mathbf{d} R \mathbf{d}'$

- if for all $i \in I$ and $\mathbf{e}^i$ such that $[\![c_i]\!]^\sigma$, there is some $i' \in I'$ and $\mathbf{e}'^{i'}$ such that $[\![c'_{i'}]\!]^{\sigma'}$, $a_i = a'_{i'}$, $[\![f_i]\!]^\sigma = [\![f'_{i'}]\!]^{\sigma'}$ and $[\![g^i_1, \ldots, g^i_n]\!]^\sigma R [\![g'^{i'}_1, \ldots, g'^{i'}_{n'}]\!]^{\sigma'}$.
- Vice versa.

We say that two terms $X(t_1, \ldots, t_n)$ and $Y(t'_1, \ldots, t'_{n'})$ are strongly bisimilar w.r.t. $\mathcal{A}$, notation $X(t_1, \ldots, t_n) \underline{\leftrightarrow} Y(t'_1, \ldots, t'_{n'})$, iff for all models $\mathbb{M}$ of $\mathcal{A}$ and valuations σ there exists a bisimulation relation R w.r.t. $\mathcal{A}$ and $\mathbb{M}$ such that $[\![t_1, \ldots, t_n]\!]^\sigma R [\![t'_1, \ldots, t'_{n'}]\!]^\sigma$.

3. The μCRL Toolset

The μCRL toolset is a collection of tools manipulating data and process descriptions written in μCRL. The toolset contains four groups of tools (see [18] for a detailed overview of all tools).

Linearizing tools. This group contains one tool, called `mcrl`.The tool `mcrl` transforms μCRL process definitions to linear process equations (LPEs). See [11, 16] for linearisation algorithms and [18] for a detailed description of `mcrl`. All the other tools of the toolset work on LPEs. Thus, before doing any analysis, `mcrl` must be invoked with a μCRL specification as input.

State space explorators. This group contains two tools. The `instantiator` which generates from an LPE a concrete transition system and the simulator, `msim`, which can single-step a process. The instantiator is highly optimized by using a very fast compiling rewriter. The output of the instantiator can be read, manipulated and, visualized by the CADP (Caesar/Aldebaran) toolset [7].

Reduction tools. This group contains four reduction tools (each of them reads an LPE and writes an LPE). These reduction tools are `constelm`, constant elimination, `parelm`, parameter elimination, and `sumelm`, sum elimination. `structelm`, structure elimination. These reduction tools are the implementations of the reduction methods described in this paper. The tool `structelm` will not be treated in this paper (see [13] for a description of this tool).

Rewrite tools. This group contains the tool `rewr`, rewrite, which normalizes the LPE, with respect to the rewrite rules a given abstract data type. If a condition belonging to a summand is equal to false then that summand will be removed.

4. Reduction Methods

4.1 Elimination of Constant Process Parameters

Some data parameters are constant throughout any run of the process. These parameters can be eliminated. All occurrences of these parameters throughout the LPE are replaced by their initial value. This does not reduce the state space of a process, but it may considerably shorten the time to generate a state space from a linear process operator, and can make other reduction tools much more effective.

4.1.1 Algorithm to Detect Constant Parameters

1. Mark all process parameters.
2. Define a substitution ρ that replaces all marked process parameters with its initial value, and that leaves other variables unchanged.
3. If a process parameter d_j with initial value v exists such that $g_j^i \rho \doteq v$ does not rewrite to true, where g_j^i is a process argument that occurs in a summand i with condition c_i, and $c_i \rho$ does not rewrite to false, then d_j must be unmarked and this algorithm must be continued at step 2.
4. Repeat step 2-3 until no additional process parameter becomes unmarked.
5. Remove all marked process parameters from the LPE. Substitute the initial value for all occurrences of marked process parameters in conditions and action arguments.

In the sequel we call this algorithm `constelm`.

Example 4.1. Let Nat be the natural numbers, and r and s be actions.

$$\begin{array}{lcl} \texttt{proc}\ X(a{:}Nat, b{:}Nat, c{:}Nat, d{:}Nat) & = & r(b)\,X(b,a,d,c) \lhd c \doteq 0 \rhd \delta + \\ & & s(c)\,X(1,b,0,c+d) \\ \texttt{proc}\ Y(a{:}Nat, b{:}Nat) & = & r(b)\,Y(b,a) + s(0)\,Y(1,b) \end{array}$$

`Constelm` finds that $X(0,0,0,0) \underline{\leftrightarrow} Y(0,0)$.

Note that the complexity of the algorithm is $O(m^2 N)$ with m the number of process parameters, and N the size of the input LPE.

4.2 Elimination of Inert Process Parameters

Some process parameters do not influence the behaviour of a system, as they do not occur directly or indirectly in conditions and actions. By removing these parameters, the state space of an LPE can be reduced considerably.

4.2.1 Algorithm to Mark Parameters as Influential Parameters.

We mark parameters if they can have an influence on the behaviour of the LPE. The remaining parameters can be removed. Here follows the algorithm, which we call `parelm`.

1. Mark the process parameters which occur in the conditions and in the action arguments of the LPE. These are not removed, as they clearly have influence on the behaviour of the process.
2. If a process parameter d_j is marked then mark also all process parameters occurring in g_j^i for all $i \in I$, as these parameters can indirectly influence the process behaviour. Repeat this step until no more parameters are marked.

3. Remove all unmarked parameters from the process.

Note that the complexity of the algorithm is $O(mN)$ with m the number of process parameters, and N the size of the input LPE.

Example 4.2. Assume X and Y are defined by:

$$\begin{aligned}\texttt{proc}\ X(a{:}D, b{:}D, c{:}D) &= s\,X(a,c,b) + \sum_{d:D} r(c)\,X(d,b,c)\\ \texttt{proc}\ Y(b{:}D, c{:}D) &= s\,Y(c,b) + r(c)\,Y(b,c)\end{aligned}$$

As parameter a has no influence on the behaviour of process X, `parelm` finds for all a, b and c that $X(a,b,c) \underline{\leftrightarrow} Y(b,c)$.

4.3 Elimination of Sum Variables

There are cases in which a condition forces a sum variable to be equal to one particular value (data term). A transformation step towards simpler LPEs can be made by eliminating these sum variables and replacing their occurrences by that value. We call this transformation sum elimination, or `sumelm`.

4.3.1 Computing the set of variables which are candidate for elimination

The function $\mathit{Values}(x,c)$, in which x is a sum variable and c a condition, computes a set of values for which it is possible to assign one value from this set to sum variable x. The resulting LPE is bisimilar to the original LPE. The function *Values* is defined by induction.

$$\begin{aligned}\mathit{Values}(x, s \doteq t) &= \begin{cases}\text{if } x \equiv s \wedge x \notin \mathit{Vars}(t) & \text{then } \{t\}\\ \text{if } x \equiv t \wedge x \notin \mathit{Vars}(s) & \text{then } \{s\}\\ \emptyset, \text{ otherwise}\end{cases}\\ \mathit{Values}(x, (c_1 \wedge c_2)) &= \mathit{Values}(x,c_1) \cup \mathit{Values}(x,c_2)\\ \mathit{Values}(x, (c_1 \vee c_2)) &= \mathit{Values}(x,c_1) \cap \mathit{Values}(x,c_2)\\ \mathit{Values}(x,c) &= \emptyset, \text{ otherwise}\end{aligned}$$

where x stands for variables, s and t stand for data terms and c, c_1 and c_2 stand for conditions. The expression $x \in \mathit{Vars}(s)$ stands for variable x occurs in s. Note that in order to calculate the intersection of two sets, it must be determined that values are equal, which requires the use of $\doteq$ and rewriting.

4.3.2 Substitution and Elimination.

For all $i \in I$, $j \in 1 \ldots n_i$, at which the set $\mathit{Values}(e^i_j, c_i)$ is not empty (choose a value v from this set):

1. Substitute v in all occurrences of e^i_j in the ith summand of the LPE, and
2. Eliminate e^i_j from the list of sum variables of the ith summand.

Example 4.3. Consider

$$\begin{aligned}\texttt{proc}\ X(d{:}\mathbf{Bool}) &= \sum_{b:\mathbf{Bool}} a(b).X(b) \lhd b \doteq \mathsf{f} \rhd \delta\\ \texttt{proc}\ Y(d{:}\mathbf{Bool}) &= a(\mathsf{f}).Y(\mathsf{f}) \lhd \mathsf{f} \doteq \mathsf{f} \rhd \delta\end{aligned}$$

`Sumelm` yields $X(d) \underline{\leftrightarrow} Y(d)$. Rewriting the condition in Y makes it equal to `t` (true).

4.4 An application of the reduction tools to an example

To demonstrate the cooperation of the three reduction algorithms, we take a slightly more substantial example. The patterns which are found in this example occur often in bigger specifications after linearization.

sort $\mathbf{Bool}, \mathbf{Bit}, \mathbf{D}$
func $\mathsf{t}, \mathsf{f}: \to \mathbf{Bool}$, $d_1, d_2 :\to \mathbf{D}$, $0, 1: \to \mathbf{Bit}$
map $\neg : \mathbf{Bool} \to \mathbf{Bool}$, $\vee : \mathbf{Bool} \times \mathbf{Bool} \to \mathbf{Bool}$
$\doteq$:$\mathbf{D} \times \mathbf{D} \to \mathbf{Bool}$, $\doteq$:$\mathbf{Bit} \times \mathbf{Bit} \to \mathbf{Bool}$
var $b : \mathbf{Bool}$
rew $\neg\mathsf{t} = \mathsf{f}$, $\neg\mathsf{f} = \mathsf{t}$, $\mathsf{t} \vee b = \mathsf{t}$, $\mathsf{f} \vee b = b$
var $d : \mathbf{D}$
rew $d_1 \doteq d_2 = \mathsf{f}$, $d_2 \doteq d_1 = \mathsf{f}$, $d \doteq d = \mathsf{t}$
var $b : \mathbf{Bit}$
rew $0 \doteq 1 = \mathsf{f}$, $1 \doteq 0 = \mathsf{f}$, $b \doteq b = \mathsf{t}$
proc $X(d{:}\mathbf{D}, b{:}\mathbf{Bit}) = \sum_{d_0:\mathbf{D}} \tau\, X(d_0, b) \lhd d \doteq d_2 \vee b \doteq 0 \rhd \delta + \sum_{b_0:\mathbf{Bit}} \tau\, X(d, b_0) \lhd b_0 \doteq 0 \rhd \delta$
init $X(d_1, 0)$

- Algorithm `parelm` does not change the LPE, because the process parameters d and b occur in one of the conditions.
- Algorithm `constelm` does not change the LPE, because the sum variables d_0 or b_0 occur in both process argument vectors.
- Algorithm `sumelm` changes the LPE. It substitutes 0 in each occurrence of sum variable b_0 and removes that sum variable. The equation becomes

  proc $X(d{:}\mathbf{D}, b{:}\mathbf{Bit}) = \sum_{d_0:\mathbf{D}} \tau\, X(d_0, b) \lhd d \doteq d_2 \vee b \doteq 0 \rhd \delta + \tau\, X(d, 0) \lhd 0 \doteq 0 \rhd \delta$
  init $X(d_1, 0)$

- Algorithm `parelm` still cannot change the modified LPE.
- Algorithm `constelm` changes the LPE. It substitutes 0 in each occurrence of b and removes that parameter. The equation becomes

  proc $X(d{:}\mathbf{D}) = \sum_{d_0:\mathbf{D}} \tau\, X(d_0) \lhd d \doteq d_2 \vee 0 \doteq 0 \rhd \delta + \tau\, X(d) \lhd 0 \doteq 0 \rhd \delta$
  init $X(d_1)$

- After rewriting the equation becomes

  proc $X(d{:}\mathbf{D}) = \sum_{d_0:\mathbf{D}} \tau\, X(d_0) \lhd \mathsf{t} \rhd \delta + \tau\, X(d) \lhd \mathsf{t} \rhd \delta$
  init $X(d_1)$

- Algorithm `parelm` changes the LPE. Process parameter d does not occur in the condition. Process parameter d will be removed. Sum variable d_0 does not occur in the equation. Sum variable d_0 will be removed.

  proc $X() = \tau\, X() \lhd \mathsf{t} \rhd \delta + \tau\, X() \lhd \mathsf{t} \rhd \delta$
  init $X()$

The state space is reduced from two states to one state, a reduction of 50 per cent.

5. Experimental results

Bounded retransmission protocol						
	before reduction			after reduction		
l	# states	# transitions	time	# states	# transitions	time
1	454	518	1.34s	454	518	1.45s
2	1856	2134	2.02s	834	954	1.65s
3	10550	12170	6.28s	1202	1378	1.89s
4	86968	100406	44.09s	2224	2558	2.49s
5	968538	1118498	8m27.13s	8642	9970	6.45s
Onebit sliding window protocol						
	before reduction			after reduction		
n	# states	# transitions	time	# states	# transitions	time
1	39577	229650	21.19s	39577	229650	20.42s
2	319912	1937388	3m44.29s	39577	229650	19.37s
3	1208737	7484714	29m56.95s	39577	229650	18.79s
Firewire link layer protocol						
	before reduction			after reduction		
n	# states	# transitions	time	# states	# transitions	time
1	95160	158017	17m15.58s	74271	123370	59m31.00s
2	371804	641565	1h9m15.30s	74271	145456	1h0m1.79s
3	872224	1548401	2h22m18.41s	74271	167542	59m56.56s

Table 1: The effect of the elimination tools on the size of state spaces

We applied our reduction techniques to a number of data transfer protocols that have been described in μCRL. These are the bounded retransmission protocol [9], the one bit sliding window protocol [3] and the Firewire link layer protocol [14]. These protocols are quite different in nature. For all protocols we hid the delivery of data, in order to investigate the control structure. By applying the different elimination algorithms we were able to remove most or even all occurrences of variables refering to data reducing the state space substantially. If all variables refering to data are removed, results on the control structure hold for any data domain, in particular for those of infinite size.

In the tables we list the sizes of the state spaces for different sizes of the data domain. For the bounded retransmission protocol the length of the data packages and the number of data elements is given by l and the number of retransmissions has been set to 3. For the two other protocols the number of data elements is given by n. The one bit sliding window protocol is a unidirectional sliding window protocol with buffer size 1 at both the sending and receiving sides. The Firewire link layer protocol consists of a bus and two link processes. The results have been obtained on a SGI Powerchallenge with R12000 processors on 300Mhz. The version of the toolset that has been used is 2.8.3.

5.0.1 Acknowledgments.

We thank Jaco van de Pol for his comments on this paper.

References

1. M.G.J. van den Brand, P. Klint, and P.A. Olivier. Compilation and Memory Management for ASF+SDF. In: Proceedings in Compiler Construction (CC'99) (ed. S. Jähnichen), LNCS 1575,

198–213, Springer-Verlag, 1999.

2. J.A. Bergstra and J.W. Klop. Process algebra for synchronous communication. *Information and Communication*, 60(1/3):109-137,1984.
3. M.A. Bezem and J.F. Groote. A correctness proof of a one bit sliding window protocol in μCRL. *The Computer Journal*, 37(4): 289-307, 1994.
4. S.C.C. Blom. Verification of the Euris railway control specification of Woerden-Harmelen. Work in progress. Centrum voor Wiskunde en Informatica, Amsterdam, 2000
5. S.C.C. Blom. Partial τ-confluence for efficient state space generation. Technical report R0123, CWI, Amsterdam, 2001. Available at `http://www.cwi.nl`
6. W.J. Fokkink. Introduction to Process Algebra, In Texts in Theoretical Computer Science, An EATCS Series. Springer-Verlag, 2000.
7. H. Garavel. `OPEN/CAESAR`: An Open Software Architecture for Verification, Simulation, and Testing". In G. Goos, J. Hartmanis, and J. van Leeuwen, Editors, *Proceedings of TACAS'98*, volume 1384 of *Lecture Notes in Computer Science*, Springer Verlag, pages 68-84, 1998. Available from `http://www.inrialpes.fr/vasy/Publications.`
8. J.F. Groote. The syntax and semantics of timed μCRL. Report SEN-R9709. CWI, The Netherlands, 1997.
9. J.F. Groote and J.C. van de Pol. A bounded retransmission protocol for large data packets. A case study in computer checked verification. In M. Wirsing and M. Nivat, Editors, *Proceedings of AMAST'96*, Munich, volume 1101 of *Lecture Notes in Computer Science*, Springer Verlag, pages 536-550, 1996.
10. J.F. Groote and A. Ponse. The Syntax and Semantics of μCRL. In A. Ponse and C. Verhoef and S.F.M. van Vlijmen,editors, *Workshops in Computing*, pages 26–62. Springer-Verlag, 1994.
11. J.F. Groote, A. Ponse and Y.S. Usenko. Linearization in parallel pCRL. *Journal of Logic and Algebraic Programming*, 48(1-2):39-72, 2001.
12. J.F. Groote and M.P.A. Sellink. Confluence for Process Verification. In *Theoretical Computer Science B (Logic, semantics and theory of programming)*, 170(1-2):47-81, 1996.
13. J.F. Groote and B Lisser Computer assisted manipulation of algebraic process specifications Technical report SEN-R0117, CWI, Amsterdam, 2001. Available at `http://www.cwi.nl`.
14. S.P. Luttik. Description and formal specification of the link layer of P1394. Technical Report SEN-R9706, CWI, Amsterdam, 1997. Available at `http://www.cwi.nl`.
15. J.C. van de Pol. A Prover for the μCRL Toolset with Applications – version 0.1. Technical report SEN-R0106, CWI, Amsterdam, 2001.
16. Y.S. Usenko. Linearization of μCRL specifications. Technical report SEN-R0209, CWI, Amsterdam, 2002. Available at `http://www.cwi.nl`.
17. M. Wirsing. Algebraic specification. In J. van Leeuwen, editor, *Handbook of Theoretical Computer Science*, volume II, pages 677–788. Elsevier Science Publishers B.V., 1990.
18. A.G. Wouters Manual for the μCRL toolset. Technical report SEN-R0130, CWI, Amsterdam, 2001. Available at `http://www.cwi.nl`.