Adapting the partial model checking technique for use in the mCRL2 toolkit

Kevin van der Pol

Eindhoven University of Technology
March 12, 2012

Abstract

We explore the quotienting procedure, a part of the partial model checking technique by Andersen [2], in the setting of mCRL2-style models. We prove the procedure to be correct, i.e. that quotienting out a system from a parallel composition and then model checking the obtained new property on the remainder, yields the same answer as model checking the original property on the combined system. We extend the procedure to include modal operators on sets of actions rather than individual actions, and to quotient out the mCRL2-specific communication and allow operators working on the combined system.

Contents

Introduction

The model checking problem is to determine whether a given system satisfies a given property. Usually the system is an abstracted software system. This can be an important step in validating the safety of a variety of systems, such as railroad switches and signals, or critical medical equipment. This becomes increasingly hard as systems become very large, which they typically are. Fortunately, such a large system usually consists of multiple simpler components working in parallel.

The partial model checking technique by Andersen [2] exploits this modularity by operating on each of the components separately instead of calculating the more complex behavior of the entire system. The partial model checking technique consists of two alternating steps: quotienting and reduction. Quotienting is moving part of the behavior from the system to the property to be checked on the remainder. This makes the system smaller, but the property larger. The next step is to reduce the property again. These steps make the model checking problem smaller and thus faster to solve. We will explore the quotienting procedure to the models used in the model checking tool set mCRL2.

In Section 1, we introduce the formalism used to describe systems in the model checker mCRL2 and in Section 2 we introduce a formalism to describe the properties to be checked. In Section 3 we introduce the quotienting procedure and prove that it is sound in the setting of mCRL2. Finally, in Section 4 we extend the quotienting procedure with modal operators working on sets of actions and with two mCRL2-specific operators working on the combined system: the communication operator and the allow operator.

1 Models

We reason about a set of *labeled transition systems* working in parallel.

1.1 Labeled transition systems

A labeled transition system is a transition system with labels on the transitions. We assume the action labels come from a set of actions Act.

Definition 1 (labeled transition system)**.**
A labeled transition system t is a triple $(S_t, \rightarrow_t, i_t)$, where S_t is a finite set of states, $\rightarrow_t \subseteq S_t \times Act \times S_t$ is a transition relation and $i_t \in S_t$ is the initial state. We often drop the subscript t if it is clear from the context.

1.2 Multi-actions

In our model we do allow actions to occur simultaneously, as a multi-action. A multi-action is a collection of actions that occur at the same time instant. Multi-actions are either τ, a regular action $a \in Act$, or the composition of two multi-actions $\alpha|\beta$. The multi-action τ is the empty multi-action. It contains no actions and thus cannot be observed. It is called the *internal* or *hidden* action. The composition $\alpha|\beta$ is the multi-action of α and β occurring simultaneously. The axioms on equality of multi-actions are given in Definition 2.

Furthermore, we define the operators $\setminus$ and $\sqsubseteq$ on multi-actions to be the removal and inclusion of multi-actions.

Definition 2 (multi-action equality ($=$), removal ($\setminus$) and inclusion ($\sqsubseteq$))**.**

$$\begin{array}{ccc} & \tau \setminus \alpha = \tau & \\ \alpha|\beta = \beta|\alpha & \alpha \setminus \tau = \alpha & \tau \sqsubseteq \alpha = \mathsf{true} \\ (\alpha|\beta)|\gamma = \alpha|(\beta|\gamma) & \alpha \setminus (\beta|\gamma) = (\alpha \setminus \beta) \setminus \gamma & a \sqsubseteq \tau = \mathsf{false} \\ \alpha|\tau = \alpha & (a|\alpha) \setminus a = \alpha & a|\alpha \sqsubseteq a|\beta = \alpha \sqsubseteq \beta \\ & (a|\alpha) \setminus b = a|(\alpha \setminus b), \text{ if } a \not\equiv b & a|\alpha \sqsubseteq b|\beta = a|(\alpha \setminus b) \sqsubseteq \beta, \text{ if } a \not\equiv b \end{array}$$

Here $\equiv$ denotes syntactic equality.

Example 3 (multi-actions; equality, removal and inclusion)**.** Let $a, b, c, \ldots$ be actions. Examples of multi-actions are a, $a|a$ and $a|b|b|c$. Multi-actions are similar to bags of actions. Ordering is not relevant, so $a|b$ and $b|a$ are equivalent. The following are examples of the removal operator:

- $a|b|b|c \setminus a|b = b|c$
- $a|b|b|c \setminus a|a = b|b|c$
- $a|b|b|c \setminus d = a|b|b|c$

Examples of the inclusion operator are:

- $a|b|b|c \sqsubseteq a|b = \mathsf{true}$
- $a|b|b|c \sqsubseteq a|a = \mathsf{false}$
- $a|b|b|c \sqsubseteq d = \mathsf{false}$

1.3 Parallel composition

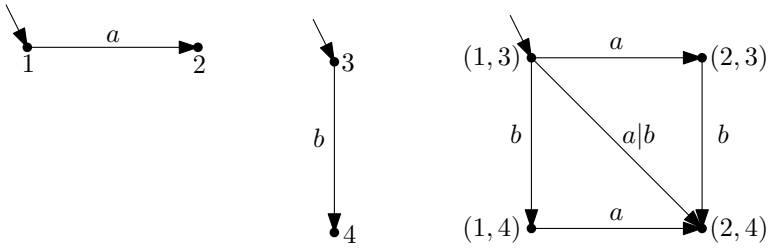
The parallel composition of systems t_1 and t_2 is denoted $t_1 \,||\, t_2$. Informally, if t_1 can do an a action from state s_1 and t_2 can do a b action from state s_2, then the parallel system $t_1 \,||\, t_2$ in state (s_1, s_2) can do the a-step, b-step or the multi-action $a|b$. The formal definition of $t_1 \,||\, t_2$, given in Definition 4, is a formalization of the informal descriptions of parallel composition given in the System Validation reader by Groote [4].

Definition 4 (parallel composition)**.**

$$\begin{array}{l} (S_{t_1}, \rightarrow_{t_1}, i_{t_1}) \,||\, (S_{t_2}, \rightarrow_{t_2}, i_{t_2}) = (S_{t_1} \times S_{t_2}, \rightarrow_{t_1 \,||\, t_2}, (i_{t_1}, i_{t_2})), \\ \text{where } (s_1, s_2) \xrightarrow{a}_{t_1 \,||\, t_2} (s_1', s_2') \Leftrightarrow s_1 = s_1' \text{ and } s_2 \xrightarrow{a}_{t_2} s_2', \text{ or} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad s_1 \xrightarrow{a}_{t_1} s_1' \text{ and } s_2 = s_2', \text{ or} \\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (\exists a_1 \sqsubset a \;:\; s_1 \xrightarrow{a_1}_{t_1} s_1' \text{ and } s_2 \xrightarrow{a \setminus a_1}_{t_2} s_2') \end{array}$$

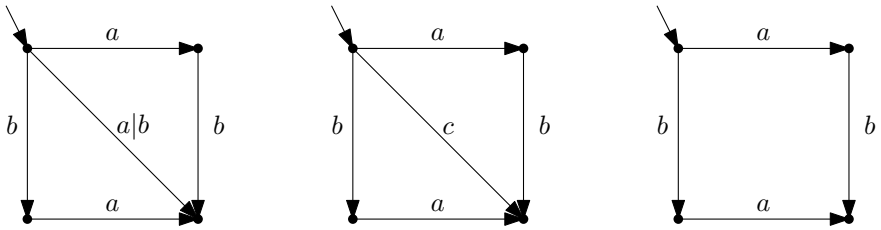
Note that the deadlock system $t_\delta = (\{s\}, \emptyset, \{s\})$ is the unity element of the parallel composition, up to renaming of states.

Example 5 (parallel composition)**.** An example of the parallel composition of two systems is given in Figure 1. The system $t_1 \,||\, t_2$ is the parallel composition of systems t_1 and t_2. It can take transitions from either system, or a multi-action transition of one transition from the one system and one from the other.



(a) System t_1 (b) System t_2 (c) System $t_1 \,||\, t_2$

Figure 1: parallel composition. The labels of the states are for illustrative purpose only.



(a) System t (b) System $\Gamma_{\{a|b\to c\}}(t)$ (c) System $\nabla_{\{a,b\}}(t)$

Figure 2: Example of the communication and allow operators. The system $\Gamma_{\{a|b\to c\}}(t)$ is equal to t where all occurrences of $a|b$ in a transition label are replaced with c. The system $\nabla_{\{a,b\}}(t)$ is equal to t where all transitions from t with a label other than a or b are removed. Note that $a|b$ is also removed, even though its constituents are in the set $\{a, b\}$.

1.4 Communication

The *communication* operator $\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}}(t)$ is the system obtained from t by replacing all occurrences of all multi-actions α_i by the corresponding a_i. It is pronounced as that the multi-action α *communicates* or *synchronizes* to an a-action. This a need not be a fresh action, i.e. it can be an action already occurring in t. It is even allowed to have actions occurring on both sides of the arrow, such as $a|b \to a$. However, for the communication operator to be well-defined, it must hold that for $\Gamma_{C_1\cup C_2}(t)$, the systems $\Gamma_{C_1}(\Gamma_{C_2}(t))$ and $\Gamma_{C_2}(\Gamma_{C_1}(t))$ are equal. The formal definition of the communication operator is given in Definition 6.

Definition 6 (communication operator)**.**

$$\begin{aligned}\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}}(t) &= (S_t, \to'_t, i_t), \text{ where}\\ s \xrightarrow{a}{}'_t s' \Leftrightarrow (s \xrightarrow{a} s' \wedge (\forall\ 1 \le i \le n\ &:\ \alpha_i \not\sqsubseteq a))\\ \vee (\exists\ 1 \le i \le n\ &:\ s \xrightarrow{\alpha_i|(a\setminus a_i)} s')\end{aligned}$$

Any $\Gamma_{C_1\cup C_2}(t)$ *where* $\Gamma_{C_1}(\Gamma_{C_2}(t)) \neq \Gamma_{C_2}(\Gamma_{C_1}(t))$ *is disallowed.*

Example 7 (communication operator)**.** An example of the communication operator on a system is given in Figure 2. The system $\Gamma_{\{a|b\to c\}}(t)$ is equal to t where all occurrences of $a|b$ in a transition label are replaced with c.

1.5 Allow

The *allow* operator $\nabla_H(t)$ is the system obtained from t by removing all transitions $s \xrightarrow{a} s'$, where $a \notin H$. The formal definition of the allow operator is given in Definition 8.

Definition 8 (allow operator)**.**

$$\nabla_H(t) = (S_t, \rightarrow'_t, i_t),$$
$$\text{where } s \xrightarrow{\alpha}{}'_t s' \Leftrightarrow s \xrightarrow{\alpha}_t s' \text{ and } \alpha \in H$$

Example 9 (allow operator)**.** Consider Figure 2. The system $\nabla_{\{a,b\}}(t)$ is equal to t where all transitions from t with a label other than a or b are removed. Note that the transition with label $a|b$ is also removed, even though its constituents are in the set $\{a, b\}$.

2 Properties

2.1 Modal equation systems

Properties to check the systems against are expressed in a *modal equation system* with a *top variable*. The property expressed by such a sequence is the value of the top variable in the simultaneous solution to the equations. The left-hand sides of the equations are variables, ranged over by $X, Y, Z, \ldots$. The right-hand sides are called assertions. They are given by the following grammar, where a is an action in Act:

$$A ::= \mathsf{true} \mid \mathsf{false} \mid X \mid A \vee A \mid A \wedge A \mid \langle a \rangle A \mid [a]A$$

Let Var be a set of variables and S be a set of states. An *environment* $\rho : \mathsf{Var} \to 2^S$ is a function that assigns values to the variables. We often use an explicit assignment of a value to a variable. This is called an *assignment*. The assignment of value v to variable X in environment ρ is denoted $\rho[X := v]$. An assignment to an environment is again an environment, defined as follows:

Definition 10 (assignment)**.**

$$\rho[X := v](Y) = \begin{cases} v & \text{if } Y = X \\ \rho(Y) & \text{if } Y \neq X \end{cases}$$

An assertion, in which variables may occur, only has a value with respect to the values of those variables. Put otherwise, the semantics of an assertion are a function from an environment to a set of states.

Definition 11 (assertion semantics)**.**
The semantics of an assertion A in an environment ρ and system t, denoted $[\![A]\!]_t\rho$, are defined as follows:

$$[\![\mathsf{true}]\!]_t\rho = S_t$$
$$[\![X]\!]\rho_t = \rho(X)$$
$$[\![A_1 \vee A_2]\!]_t\rho = [\![A_1]\!]_t\rho \cup [\![A_2]\!]_t\rho$$
$$[\![\langle a \rangle A]\!]_t\rho = \{s \in S_t \mid \exists s' \ : \ s \xrightarrow{a}_t s' \text{ and } s' \in [\![A]\!]_t\rho\}$$

The cases for $[a]A$, $\wedge$ and false are immediate duals of $\langle a \rangle A$, $\vee$ and true. We often drop the subscript t if it is clear from the context.

The assertions true and false denote the boolean constants true and false. The binary operators $\wedge$ and $\vee$ are the usual conjunction and disjunction of properties. The modal operators $\langle a \rangle$ and $[a]$ characterize states by their ability to perform actions.

A modal equation system is constructed from assertions as follows. We denote by ϵ the empty modal equation system, containing no assertions. The syntax of modal equation systems is then given by the following grammar:

$$\mathcal{E} ::= (\mu X = A)\ \mathcal{E} \mid (\nu X = A)\ \mathcal{E} \mid \epsilon$$

We often use the symbol σ to denote a fixed point of either modality, i.e. if it is not important whether it is the least or greatest fixed point.

A variable X is *bound* in $\mathcal{E}$ if and only if there is an equation in $\mathcal{E}$ with X on its left hand side. Similarly, a variable X is *occurring* in $\mathcal{E}$ if and only if there is an equation in $\mathcal{E}$ with X on its right hand side.

Definition 12 (bound and occurring variables)**.**

$$\begin{aligned}
\mathsf{bnd}(\epsilon) &= \emptyset \\
\mathsf{bnd}((\sigma X = A)\ \mathcal{E}) &= \{X\} \cup \mathsf{bnd}(\mathcal{E}) \\
\\
\mathsf{occ}(\epsilon) &= \emptyset \\
\mathsf{occ}((\sigma X = A)\ \mathcal{E}) &= \mathsf{occ}(A) \cup \mathsf{occ}(\mathcal{E}) \\
\mathsf{occ}(\mathsf{true}) &= \emptyset \\
\mathsf{occ}(X) &= \{X\} \\
\mathsf{occ}(A_1 \vee A_2) &= \mathsf{occ}(A_1) \cup \mathsf{occ}(A_2) \\
\mathsf{occ}(\langle a \rangle A) &= \mathsf{occ}(A)
\end{aligned}$$

The cases for $[a]A$, $\wedge$ and false are immediate duals of $\langle a \rangle A$, $\vee$ and true.

A modal equation system $\mathcal{E}$ is called *closed* if and only if all occurring variables are also bound, i.e. $\mathsf{occ}(\mathcal{E}) \subseteq \mathsf{bnd}(\mathcal{E})$. Otherwise, it is called *open*.

Now for the semantics of a modal equation system. The definition of the semantics of modal equation systems in Definition 13 is taken from Mader [5]. This definition is similar to the definition of Andersen [2], only with the environment variable ρ *accumulating* values, removing the need for the explicit union $\star$.

Definition 13 (modal equation system semantics)**.**
The semantics of a modal equation system $\mathcal{E}$ in an environment ρ and system t, denoted $[\![\mathcal{E}]\!]_t \rho$, are defined as follows:

$$\begin{aligned}
[\![\epsilon]\!]_t \rho &= \rho \\
[\![(\sigma X = A)\ \mathcal{E}]\!]_t \rho &= [\![\mathcal{E}]\!]_t \rho[X := \sigma U.[\![A]\!]_t([\![\mathcal{E}]\!]_t \rho[X := U])]
\end{aligned}$$

Note that $[\![\mathcal{E}]\!]_t \rho(X) = \rho(X)$ for variables $X \notin \mathsf{bnd}(\mathcal{E})$.

A top assertion is used to encode what is the relevant variable in the modal equation system.

Definition 14 (top assertion)**.**
The semantics of a modal equation system $\mathcal{E}$ with a top variable $X \in \mathsf{bnd}(\mathcal{E})$ is the value of X in the semantics of $\mathcal{E}$ in the empty environment $[]$:

$$\mathcal{E} \downarrow X = ([\![\mathcal{E}]\!]_t [])(X)$$

Lastly, we formalize whether a system satisfies a property expressed by a modal equation system:

Definition 15 (satisfaction)**.**
Let t be a labeled transition system and let $\mathcal{E} = \mathcal{E}' \downarrow X$ be a modal equation system with a top assertion. System t satisfies $\mathcal{E}$, denoted $t \models \mathcal{E}$, if and only if, $i_t \in \mathcal{E}$.

Example 16 (modal equation system)**.** Examples of modal equation systems are:

- ϵ, the empty modal equation system, which is closed.
- $(\mu X = \mathsf{true})$, a closed modal equation system with no top assertion.
- $(\mu X = \langle a|b\rangle(Y \wedge [a|c]\mathsf{false}))$, an open modal equation system with no top assertion.
- $(\mu X = Y \vee [a]\mathsf{true})\ (\nu Y = \mathsf{false})\ \downarrow X$, a closed modal equation system with a top assertion.

2.2 Applicability of Knaster-Tarski's Theorem

Knaster-Tarski's Theorem states that the fixed points of a monotone function over a complete lattice also form a complete lattice. The related Kleene chain iteration states that the least (or greatest) fixed point can be found by transfinite iteration of that monotone function starting from the bottom (or top) element in the complete lattice. In order to use these theorems later, we show the two assumptions are met: sets of states form a complete lattice, and the assertions are monotone functions with respect to the environment.

Lemma 17 ($(2^S, \subseteq)$ is a complete lattice)**.**
Let S be the set of states. The structure $(2^S, \subseteq)$ is a complete lattice.

Proof. Any power set of a given set, ordered by inclusion, is a complete lattice. This means $(2^S, \subseteq)$ is a complete lattice. □

Lemma 18 (assertions are monotone)**.**
Let ρ_1, ρ_2 be arbitrary environments and A an arbitrary assertion. If $\rho_1(X) \subseteq \rho_2(X)$ holds for all $X \in \mathsf{occ}(A)$, then it holds that $([\![A]\!]_t\rho_1) \subseteq ([\![A]\!]_t\rho_2)$ for any system t.

Proof. Proof by structural induction on A:

- true:

$$
\begin{aligned}
& [\![\mathsf{true}]\!]_t\rho_1 \\
= & \{\text{def. } 11\} \\
& S_t \\
= & \{\text{def. } 11\} \\
& [\![\mathsf{true}]\!]_t\rho_2
\end{aligned}
$$

- X:

$$\begin{aligned}
&[\![X]\!]_t\rho_1 \\
=\ &\{\text{def. 11}\} \\
&\rho_1(X) \\
\subseteq\ &\{\text{assumption}\} \\
&\rho_2(X) \\
=\ &\{\text{def. 11}\} \\
&[\![X]\!]_t\rho_2
\end{aligned}$$

- $A_1 \vee A_2$:

Induction Hypothesis: $[\![A_1]\!]_t\rho_1 \subseteq [\![A_1]\!]_t\rho_2$ and similarly for A_2

$$\begin{aligned}
&[\![A_1 \vee A_2]\!]_t\rho_1 \\
=\ &\{\text{def. 11}\} \\
&[\![A_1]\!]_t\rho_1 \cup [\![A_2]\!]_t\rho_1 \\
\subseteq\ &\{\text{Induction Hypothesis}\} \\
&[\![A_1]\!]_t\rho_2 \cup [\![A_2]\!]_t\rho_2 \\
=\ &\{\text{def. 11}\} \\
&[\![A_1 \vee A_2]\!]_t\rho_2
\end{aligned}$$

- $\langle a \rangle A_1$:

$$\begin{aligned}
&[\![\langle a \rangle A_1]\!]_t\rho_1 \\
=\ &\{\text{def. 11}\} \\
&\{s \in S_t \mid (\exists s' \ :\ s \xrightarrow{a} s' \wedge s' \in [\![A_1]\!]_t\rho_1)\} \\
=\ &\{\text{Induction Hypothesis}\} \\
&\{s \in S_t \mid (\exists s' \ :\ s \xrightarrow{a} s' \wedge s' \in [\![A_1]\!]_t\rho_2)\} \\
=\ &\{\text{def. 11}\} \\
&[\![\langle a \rangle A_2]\!]_t\rho_2
\end{aligned}$$

□

3 Quotienting

3.1 Existing work

The quotienting procedure aims to move part of the model checking problem from the system to the property to be checked on the remainder. We will introduce the quotienting procedure by Andersen [2], which finds a new property $\mathcal{E}/t'$ such that $t \models \mathcal{E}/t'$ if and only if $t \,||\, t' \models \mathcal{E}$. This bi-implication indicates we are indeed moving part of the system's behavior into the property. If the new property is not much larger than the original, or if we can easily reduce it to be so, we have simplified the task of model checking.

The formal definition of quotienting is given in Definition 19. This definition is inspired by Andersen [2] and adapted slightly to match the definition of models used in this paper.

Definition 19 (quotienting)**.**

$$(\mathcal{E} \downarrow X)/t = (\mathcal{E}/t) \downarrow X_{i_t}$$

$$\epsilon/t = \epsilon$$

$$(\sigma X = A\ \mathcal{E})/t = \begin{cases} \sigma X_{s_1} = A/s_1 \\ \cdots \\ \sigma X_{s_n} = A/s_n \\ \mathcal{E}/t \end{cases}$$

$$X/s = X_s$$

$$\langle a \rangle A/s = \langle a \rangle (A/s) \vee \bigvee_{s \xrightarrow{a} s'} A/s' \vee \bigvee_{\substack{a_1 \sqsubset a \\ s \xrightarrow{a_1} s'}} \langle a \setminus a_1 \rangle A/s'$$

$$(A_1 \vee A_2)/s = (A_1/s) \vee (A_2/s)$$

$$\mathsf{false}/s = \mathsf{false}$$

The quotienting rules for $[a]$, $\wedge$ *and* true *are immediate duals of the cases* $\langle a \rangle$, $\vee$ *and* false.

Example 20 (quotienting)**.** Consider the system $t_1 \,||\, t_2$ from Figure 1.

We would like to model check the property "after every a-action it is possible to perform a b-action". This property can be expressed by the modal equation system

$$\mathcal{E} = \begin{pmatrix} \nu X = [a]Y \\ \mu Y = \langle b \rangle \mathsf{true} \end{pmatrix} \downarrow X$$

This is the property we want the system $t_1 \,||\, t_2$ to satisfy. We now see what property the system t_1 must satisfy for the entire system to satisfy this property, by quotienting out the system t_2. Applying the quotienting rules given in Definition 19, we obtain the modal equation system

$$\mathcal{E}/t_2 = \begin{pmatrix} \nu X_3 = [a]Y_3 \\ \nu X_4 = [a]Y_4 \\ \mu Y_3 = \mathsf{true} \\ \mu Y_4 = \langle b \rangle \mathsf{true} \end{pmatrix} \downarrow X_1$$

Furthermore, we can quotient out the remaining system t_1 itself. Applying the quotienting rules again, we obtain

$$(\mathcal{E}/t_2)/t_1 = \begin{pmatrix} \nu X_{3_1} = [a]Y_{3_1} \wedge Y_{3_2} \\ \nu X_{3_2} = [a]Y_{3_2} \\ \nu X_{4_1} = [a]Y_{4_1} \wedge Y_{4_2} \\ \nu X_{4_2} = [a]Y_{4_2} \\ \mu Y_{3_1} = \mathsf{true} \\ \mu Y_{3_2} = \mathsf{true} \\ \mu Y_{4_1} = \langle b \rangle \mathsf{true} \\ \mu Y_{4_2} = \langle b \rangle \mathsf{true} \end{pmatrix} \downarrow X_{3_1}$$

We check this property against the deadlock system t_δ. The deadlock system has no transitions, so all $[\cdot]$-expressions are equal to true and all $\langle\cdot\rangle$-expressions are false. This means the entire modal equation system is now rid of all modal operators and thus has become a boolean equation system:

$$\begin{pmatrix} \nu X_{3_1} = Y_{3_2} \\ \nu X_{3_2} = \mathsf{true} \\ \nu X_{4_1} = Y_{4_2} \\ \nu X_{4_2} = \mathsf{true} \\ \mu Y_{3_1} = \mathsf{true} \\ \mu Y_{3_2} = \mathsf{true} \\ \mu Y_{4_1} = \mathsf{false} \\ \mu Y_{4_2} = \mathsf{false} \end{pmatrix} \downarrow X_{3_1}$$

This solves to true, proving the original property holds on the system $t_1 \,||\, t_2$.

3.2 Soundness

We show the soundness of the quotienting procedure. To do this, we first introduce projection of tuples and Bekić Theorem.

Definition 21 (projection)**.**
For any $1 \leq i \leq n$, the projection function π is defined as follows:

$$\pi_i((x_1, \ldots, x_n)) = x_i$$

In the quotienting procedure, equations are replaced by a consecutive series of equations with equal fixed points, called a *block*: $(\sigma X_1 = A_1)\ \ldots\ (\sigma X_n = A_n)$. Bekić Theorem states that a block may be viewed as a *simultaneous* fixed point over all variables X_i:

Theorem 22 (Bekić Theorem)**.**
For any modal equation system $\mathcal{E}$, block $(\sigma X_1 = A_1)\ \ldots\ (\sigma X_n = A_n)$, and environment ρ, the following equality holds:

$$[\![(\sigma X_1 = A_1)\ \ldots\ (\sigma X_n = A_n)\ \mathcal{E}]\!]\rho = [\![(\sigma(X_1, \ldots, X_n) = (A_1, \ldots, A_n))\ \mathcal{E}]\!]\rho$$

This is proven for two simultaneous fixed points by Bekić [3] and generalized to n simultaneous fixed points by Andersen [1].

We show soundness of the quotienting procedure in three steps. First, we prove soundness of quotienting inside a single equation. Second, we relate variables in the original and quotiented modal equation systems. Thirdly, we show that the quotienting procedure is sound with respect to satisfaction, which follows straightforwardly from the more general second step.

3.2.1 Quotienting on assertions

We prove the soundness of quotienting inside a single equation, i.e. we relate the elements in the semantics of some assertion A, to the elements of A/s_2, after the quotienting procedure.

Lemma 23 (soundness of quotienting on assertions)**.**
Let A be any assertion and let ρ_1, ρ_2 be any environments such that the following assumption holds:

$$(\forall X \in \mathsf{occ}(A)\ :\ (s_1, s_2) \in \rho_1(X) = s_1 \in \rho_2(X_{s_2}))$$

For any two systems $t_1 = (S_1, \to_1, i_1)$ and $t_2 = (S_2, \to_2, i_2)$ and for all $s_1 \in S, s_2 \in S_2$, it holds that:

$$(s_1, s_2) \in [\![A]\!]_{t_1 \,||\, t_2} \rho_1 \Leftrightarrow s_1 \in [\![A/s_2]\!]_{t_1} \rho_2$$

Proof. By structural induction on A:

- Case true:

$$\begin{aligned}
& (s_1, s_2) \in [\![\mathsf{true}]\!]_{\mathsf{t_1} \,||\, \mathsf{t_2}} \rho_1 \\
= & \{\text{def. 11}\} \\
& (s_1, s_2) \in S_1 \times S_2 \\
= & \{s_1 \in S_1, s_2 \in S'\} \\
& \mathsf{true} \\
= & \{s_1 \in S_1\} \\
& s_1 \in S_1 \\
= & \{\text{def. 11}\} \\
& s_1 \in [\![\mathsf{true}]\!]_{\mathsf{t_1}} \rho_2 \\
= & \{\text{def. 19}\} \\
& s_1 \in [\![\mathsf{true}/s_2]\!]_{t_1} \rho_2
\end{aligned}$$

- Case X:

$$\begin{aligned}
& (s_1, s_2) \in [\![X]\!]_{t_1 \,||\, t_2} \rho_1 \\
= & \{\text{def. 11}\} \\
& (s_1, s_2) \in \rho_1(X) \\
= & \{\text{assumption on } \rho_1, \rho_2\} \\
& s_1 \in \rho_2(X_{s_2}) \\
= & \{\text{def. 11}\} \\
& s_1 \in [\![X_{s_2}]\!]_{t_1} \rho_2 \\
= & \{\text{def. 19}\} \\
& s_1 \in [\![X/s_2]\!]_{t_1} \rho_2
\end{aligned}$$

- Case $\wedge$:

Induction Hypothesis: $(s_1, s_2) \in [\![A_1]\!]_{t_1 \,||\, t_2}\rho_1 \Leftrightarrow s_1 \in [\![A_1/s_2]\!]_{t_1}\rho_2$ and similarly for A_2

$$
\begin{aligned}
& (s_1, s_2) \in [\![A_1 \wedge A_2]\!]_{t_1 \,||\, t_2}\rho_1 \\
= & \{\text{def. 11}\} \\
& (s_1, s_2) \in [\![A_1]\!]_{t_1 \,||\, t_2}\rho_1 \cap [\![A_2]\!]_{t_1 \,||\, t_2}\rho_1 \\
= & \{\text{set theory}\} \\
& (s_1, s_2) \in [\![A_1]\!]_{t_1 \,||\, t_2}\rho_1 \wedge (s_1, s_2) \in [\![A_2]\!]_{t_1 \,||\, t_2}\rho_1 \\
= & \{\text{Induction Hypothesis}\} \\
& s_1 \in [\![A_1/s_2]\!]_{t_1}\rho_2 \wedge s_1 \in [\![A_2/s_2]\!]_{t_1}\rho_2 \\
= & \{\text{set theory}\} \\
& s_1 \in [\![A_1/s_2]\!]_{t_1}\rho_2 \cap [\![A_2/s_2]\!]_{t_1}\rho_2 \\
= & \{\text{def. 11}\} \\
& s_1 \in [\![A_1/s_2 \wedge A_2/s_2]\!]_{t_1}\rho_2 \\
= & \{\text{def. 19}\} \\
& s_1 \in [\![(A_1 \wedge A_2)/s_2]\!]_{t_1}\rho_2
\end{aligned}
$$

- Case $\langle a \rangle$:

$$
\begin{aligned}
& (s_1, s_2) \in [\![\langle a \rangle A]\!]_{t_1 \,||\, t_2}\rho_1 \\
= & \{\text{def. 11}\} \\
& (s_1, s_2) \in \{(x, y) \in S_1 \times S_2 \mid (\exists (x', y') \;:\; (x, y) \xrightarrow{a} (x', y') \;\wedge\; (x', y') \in [\![A]\!]_{t_1 \,||\, t_2}\rho_1)\} \\
= & \{\text{set theory, dummy renaming}\} \\
& (\exists (s_1', s_2') \;:\; (s_1, s_2) \xrightarrow{a} (s_1', s_2') \;\wedge\; (s_1', s_2') \in [\![A]\!]_{t_1 \,||\, t_2}\rho_1) \\
= & \{\text{def. 4, domain split}\} \\
& (\exists s_1' \;:\; s_1 \xrightarrow{a} s_1' \;\wedge\; (s_1', s_2) \in [\![A]\!]_{t_1 \,||\, t_2}\rho_2) \vee \\
& (\exists s_2' \;:\; s_2 \xrightarrow{a} s_2' \;\wedge\; (s_1, s_2') \in [\![A]\!]_{t_1 \,||\, t_2}\rho_2) \vee \\
& (\exists a_2 \sqsubset a, s_1', s_2' \;:\; s_1 \xrightarrow{a \setminus a_2} s_1' \;\wedge\; s_2 \xrightarrow{a_2} s_2' \;\wedge\; (s_1', s_2') \in [\![A]\!]_{t_1 \,||\, t_2}\rho_2) \\
= & \{\text{Induction Hypothesis}\} \\
& (\exists s_1' \;:\; s_1 \xrightarrow{a} s_1' \;\wedge\; s_1' \in [\![A/s_2]\!]_{t_1}\rho_2) \vee \\
& (\exists s_2' \;:\; s_2 \xrightarrow{a} s_2' \;\wedge\; s_1 \in [\![A/s_2']\!]_{t_1}\rho_2) \vee \\
& (\exists a_2 \sqsubset a, s_1', s_2' \;:\; s_1 \xrightarrow{a \setminus a_2} s_1' \;\wedge\; s_2 \xrightarrow{a_2} s_2' \;\wedge\; s_1' \in [\![A/s_2']\!]_{t_1}\rho_2) \\
= & \{\text{def. 11; correspondence } \exists \text{ and } \vee\} \\
& s_1 \in [\![\langle a \rangle (A/s_2)]\!]_{t_1}\rho_2 \vee \\
& s_1 \in [\![\bigvee_{s_2 \xrightarrow{a} s_2'} (A/s_2')]\!]_{t_1}\rho_2 \vee \\
& s_1 \in [\![\bigvee_{\substack{a_2 \sqsubset a \\ s_2 \xrightarrow{a_2} s_2'}} (\langle a \setminus a_2 \rangle (A/s_2'))]\!]_{t_1}\rho_2) \\
= & \{\text{def. 11; set theory; def. 19}\} \\
& s_1 \in [\![\langle a \rangle A/s_2]\!]_{t_1}\rho_2
\end{aligned}
$$

□

3.2.2 Relating $\mathcal{E}$ and $\mathcal{E}/t$

In this second step, we relate the original modal equation system $\mathcal{E}$, to $\mathcal{E}/t$, after the quotienting procedure. We show there is a relation between all bound variables X in the original and the variables $X_{s'_1}, \ldots, X_{s'_i}$ after the quotienting procedure. We assume this relation already holds for all unbound occurring variables.

Lemma 24.
Assumption: $(\forall X \in \mathsf{occ}(\mathcal{E}) \setminus \mathsf{bnd}(\mathcal{E}) \ : \ (s, s') \in \rho(X) = s \in \rho(X_{s'}))$
To show: $(\forall X \in \mathsf{occ}(\mathcal{E}) \ : \ (s, s') \in (\llbracket \mathcal{E} \rrbracket_{t \,||\, t'} \rho)(X) \Leftrightarrow s \in (\llbracket \mathcal{E}/t' \rrbracket_t \rho)(X_{s'}))$

Proof. By structural induction on $\mathcal{E}$:

- Case ϵ:

  Trivial, empty universal quantification

IH: $(\forall X \in \mathsf{occ}(\mathcal{E}) \ : \ (s, s') \in (\llbracket \mathcal{E} \rrbracket_{t \,||\, t'} \rho)(X) \Leftrightarrow s \in (\llbracket \mathcal{E}/t' \rrbracket_t \rho)(X_{s'}))$

- Case $(\sigma X = A)\mathcal{E}$ for X:

$$
\begin{aligned}
& s \in (\llbracket ((\sigma X = A)\mathcal{E})/t' \rrbracket_t \rho)(X_{s'_i}) \\
= \ & \{\text{def. 19}\} \\
& s \in (\llbracket (\sigma X_{s'_1} = A/s'_1) \ \ldots \ (\sigma X_{s'_n} = A/s'_2) \ (\mathcal{E}/t') \rrbracket_t \rho)(X_{s'_i}) \\
= \ & \{\text{Bekić Theorem}\} \\
& s \in (\llbracket (\sigma (X_{s'_1}, \ldots, X_{s'_n}) = (A/s'_1, \ldots, X_{s'_n})) \ (\mathcal{E}/t') \rrbracket_t \rho)(X_{s'_i}) \\
= \ & \{\text{def. 13}\} \\
& s \in (\llbracket \mathcal{E}/t' \rrbracket_t \rho[(X_{s'_1}, \ldots, X_{s'_n}) := \sigma(U_1, \ldots, U_n).\llbracket (A/s'_1, \ldots, X_{s'_n}) \rrbracket(\\
& \quad \llbracket \mathcal{E}/t' \rrbracket_t \rho[(X_{s'_1}, \ldots, X_{s'_n}) := (U_1, \ldots, U_n)])])(X_{s'_i}) \\
= \ & \{\text{def. 21}\} \\
& s \in \pi_i(\llbracket \mathcal{E}/t' \rrbracket_t \rho[(X_{s'_1}, \ldots, X_{s'_n}) := \sigma(U_1, \ldots, U_n).\llbracket (A/s'_1, \ldots, X_{s'_n}) \rrbracket(\\
& \quad \llbracket \mathcal{E}/t' \rrbracket_t \rho[(X_{s'_1}, \ldots, X_{s'_n}) := (U_1, \ldots, U_n)])])((A/s'_1, \ldots, X_{s'_n})) \\
= \ & \{\text{def. 10}\} \\
& s \in \pi_i(\sigma(U_1, \ldots, U_n).\llbracket (A/s'_1, \ldots, X_{s'_n}) \rrbracket(\llbracket \mathcal{E}/t' \rrbracket_t \rho[(X_{s'_1}, \ldots, X_{s'_n}) := (U_1, \ldots, U_n)])) \\
\dagger = \ & \{\text{Lemma 23}\} \\
& (s, s'_i) \in \sigma U.\llbracket A \rrbracket(\llbracket \mathcal{E} \rrbracket_{t \,||\, t'} \rho[X := U]) \\
= \ & \{\text{def. 10, noting that } X \notin \mathsf{bnd}(\mathcal{E})\} \\
& (s, s'_i) \in (\llbracket \mathcal{E} \rrbracket_{t \,||\, t'} \rho[X := \sigma U.\llbracket A \rrbracket(\llbracket \mathcal{E} \rrbracket_{t \,||\, t'} \rho[X := U])])(X) \\
= \ & \{\text{def. 13}\} \\
& (s, s'_i) \in (\llbracket (\sigma X = A) \ \mathcal{E} \rrbracket_{t \,||\, t'})(X)
\end{aligned}
$$

- Case $(\sigma X = A)\mathcal{E}$ for $Y \neq X$:

$$
\begin{aligned}
& s \in [\![((\sigma X = A)\mathcal{E})/t']\!]_t \rho(Y_{s'_i}) \\
= \; & \{\text{def. 19}\} \\
& s \in ([\![(\sigma X_{s'_1} = A/s'_1) \ \ldots \ (\sigma X_{s'_n} = A/s'_2) \ (\mathcal{E}/t')]\!]_t \rho)(Y_{s'_i}) \\
= \; & \{\text{Bekić Theorem}\} \\
& s \in ([\![(\sigma(X_{s'_1}, \ldots, X_{s'_n}) = (A/s'_1, \ldots, X_{s'_n})) \ (\mathcal{E}/t')]\!]_t \rho)(Y_{s'_i}) \\
= \; & \{\text{def. 13}\} \\
& s \in ([\![\mathcal{E}/t']\!]_t \rho[(X_{s'_1}, \ldots, X_{s'_n}) := \sigma(U_1, \ldots, U_n).[\![(A/s'_1, \ldots, X_{s'_n})]\!](\\
& \quad [\![\mathcal{E}/t']\!]_t \rho[(X_{s'_1}, \ldots, X_{s'_n}) := (U_1, \ldots, U_n)])])(Y_{s'_i}) \\
= \; & \{\text{def. 10}\} \\
& s \in ([\![\mathcal{E}/t']\!]_t \rho)(Y_{s'_i}) \\
= \; & \{\text{Induction Hypothesis}\} \\
& (s, s'_i) \in ([\![\mathcal{E}]\!]_{t \,||\, t'} \rho)(Y)
\end{aligned}
$$

Now, we show that the application of Lemma 23 at † is valid, i.e. that its assumption is satisfied:
$(\forall X \in \mathsf{occ}(A) \ : \ (s, s') \in \eta_1(X) = s \in \eta_2(X_{s'}))$,
where $\eta_1 = [\![\mathcal{E}]\!]_{t \,||\, t'} \rho[X := U]$
and $\eta_2 = [\![\mathcal{E}/t']\!]_t \rho[(X_{s'_1}, \ldots, X_{s'_n}) := (U_1, \ldots, U_n)]$

We distinguish three cases for X:

1. $X \in \mathsf{bnd}(\mathcal{E})$: the variables are related by Induction Hypothesis
2. $X \in \mathsf{occ}((\sigma X = A) \ \mathcal{E}) \setminus \mathsf{bnd}((\sigma X = A) \ \mathcal{E})$: the variables are related by the assumption on free variables
3. $X \in \mathsf{bnd}((\sigma X = A))$: this case requires more effort:

We may assume the following:

1. Free variables: $(\forall X \in \mathsf{occ}(\mathcal{E}) \setminus \mathsf{bnd}(\mathcal{E}) \ : \ (s, s') \in \rho(X) = s \in \rho(X_{s'}))$
2. Induction Hypothesis: $(\forall X \in \mathsf{occ}(\mathcal{E}) \ : \ (s, s') \in ([\![\mathcal{E}]\!]_{t \,||\, t'} \rho)(X) \Leftrightarrow s \in ([\![\mathcal{E}/t']\!]_t \rho)(X_{s'}))$

It remains to show that $(s, s'_i) \in \sigma U.[\![A]\!]([\![\mathcal{E}]\!]_{t \,||\, t'} \rho[X := U])$ if and only if,
$s \in \pi_i(\sigma(U_1, \ldots, U_n).[\![(A/s'_1, \ldots, X_{s'_n})]\!]([\![\mathcal{E}/t']\!]_t \rho[(X_{s'_1}, \ldots, X_{s'_n}) := (U_1, \ldots, U_n)]))$

We show this by proving the stronger notion that at every approximation of the fixed points in the Kleene chain, the variables X and X_{s_i} are related. This means we show this for the first approximation, and, given it holds in the x^{th} approximation, that it holds in the $(x+1)^{\text{th}}$ approximation.

- First approximation:

$$
\begin{aligned}
& (s, s'_i) \in U^0 \\
= \; & \{\text{bottom element of sets is the empty set}\} \\
& (s, s'_i) \in \emptyset \\
= \; & \{\text{set theory}\} \\
& \mathsf{false} \\
= \; & \{\text{set theory}\} \\
& s \in \emptyset \\
= \; & \{\text{bottom element of tuples of sets is the tuple of empty sets}\} \\
& s \in \pi_i((\emptyset, \ldots, \emptyset)) \\
= \; & \{\text{first approximation is bottom element}\} \\
& s \in \pi_i((U_1^0, \ldots, U_n^0))
\end{aligned}
$$

- Next approximation:

Assumption on previous approximation: $(s, s'_i) \in U^x \equiv s \in \pi_i((U_1^x, \ldots U_n^x))$

$$
\begin{aligned}
& (s, s'_i) \in U^{x+1} \\
= \; & \{\text{take next approximation by applying the monotone function}\} \\
& (s, s'_i) \in [\![A]\!]([\![\mathcal{E}]\!]_{t \,||\, t'} \rho[X := U^x]) \\
\ddagger = \; & \{\text{Lemma 23}\} \\
& s \in [\![A/s'_i]\!]([\![\mathcal{E}/t']\!]_t \rho[(X_1, \ldots, X_n) := (U_1^x, \ldots, U_n^x)]) \\
= \; & \{\text{projection}\} \\
& s \in \pi_i((U_1^{x+1}, \ldots, U_n^{x+1}))
\end{aligned}
$$

Again, we show that the application of Lemma 23 in step ‡ is sound:
$(\forall X \in \mathsf{occ}(A) \,:\, (s, s') \in \rho[X := U^x](X) = s \in \pi_i(\rho[(X_{s_1}, \ldots, X_{s_n}) := (U_1^x, \ldots, U_n^x)](X_{s_1}, \ldots, X_{s_n})))$

1. $X \in \mathsf{bnd}(\mathcal{E})$: the variables are related by Induction Hypothesis
2. $X \in \mathsf{occ}((\sigma X = A)\ \mathcal{E}) \setminus \mathsf{bnd}((\sigma X = A)\ \mathcal{E})$: the variables are related by the assumption on free variables
3. $X \in \mathsf{bnd}((\sigma X = A))$: the variables are related by the assumption on the previous approximation.

This concludes the proof of Lemma 24. □

For *closed* modal equation systems, the assumption on free variables is trivially fulfilled:

Corollary 25 (relating *closed* $\mathcal{E}$ and $\mathcal{E}/t'$)**.**
For a closed *modal equation system* $\mathcal{E}$*, it holds that* $(s, s') \in ([\![\mathcal{E}]\!]_{t \,||\, t'} \rho)(X) \Leftrightarrow s \in ([\![\mathcal{E}/t']\!]_t \rho)(X_{s'})$.

3.2.3 Soundness of quotienting

In this third step, we arrive at the main conclusion: quotienting is sound with respect to satisfaction.

Theorem 26 (soundness of quotienting)**.**
Quotienting is sound for closed modal equation systems, i.e. for any closed modal equation system $\mathcal{E}$, $t \,||\, t' \models \mathcal{E} \downarrow X$ *if and only if,* $t \models (\mathcal{E} \downarrow X)/t'$.

Proof.

$$
\begin{aligned}
& t \,||\, t' \models \mathcal{E} \downarrow X \\
= & \{\text{def. 15}\} \\
& (i_t, i_{t'}) \in \mathcal{E} \downarrow X \\
= & \{\text{def. 14}\} \\
& (i_t, i_{t'}) \in (\llbracket \mathcal{E} \rrbracket_{t \,||\, t'}[])(X) \\
= & \{\text{Corollary 25}\} \\
& i_t \in (\llbracket \mathcal{E}/t' \rrbracket_t[])(X_{i_{t'}}) \\
= & \{\text{def. 15}\} \\
& t \models (\mathcal{E}/t' \downarrow X_{i_{t'}}) \\
= & \{\text{def. 19}\} \\
& t \models (\mathcal{E} \downarrow X)/t'
\end{aligned}
$$

□

4 Extending quotienting

The quotient operator as defined in Andersen[2] is not immediately applicable to the models of mCRL2. We extend the quotient operator with support for sets and the communication and allow operators. Since these extensions only alter the kind of transitions that can be taken, the validity of the property to be checked only changes with respect to the modal operators $[\cdot]$ and $\langle\cdot\rangle$. We therefore only consider the quotient rule for the case $\langle\alpha\rangle A$; the case $[\alpha]A$ is its immediate dual and the other cases are trivial.

4.1 Sets

We want to reason about states being able to perform an action from a set of actions, instead of a specific single action. The property $\langle\alpha\rangle A$, with $\alpha \subseteq Act$ and α finitely large, holds in those states $s \in S$ for which $s \xrightarrow{a} s'$ for some $a \in \alpha$ and A holds in state s'. We formally define this in Definition 27.

Definition 27 (modal operators for sets of actions)**.**
For $\alpha \subseteq Act$*:*

$$s \in \llbracket \langle\alpha\rangle A \rrbracket_t = (\exists a \in \alpha \;:\; s \xrightarrow{a} s' \wedge s' \in \llbracket A \rrbracket_t)$$

The definition for $[\alpha]$ *is the immediate dual.*

Now, we use the soundness of the quotienting rule for this case as a specification and derive the correct definition for $(\langle\alpha\rangle A)/s_2$.

Let the specification be as follows:

$$(s_1, s_2) \in \llbracket \langle\alpha\rangle A \rrbracket_{t_1 \,||\, t_2} = s_1 \in \llbracket (\langle\alpha\rangle A)/s_2 \rrbracket_{t_1}$$

We derive the definition by structural induction, i.e. assuming that quotienting is already well-defined on smaller terms. Let the induction hypothesis be:

$$(\forall (x,y) \in S_1 \times S_2 \ : \ (x,y) \in [\![A]\!]_{t_1 \,||\, t_2} = x \in [\![A/y]\!]_{t_1})$$

Now we derive the correct definition for $(\langle\alpha\rangle A)/s_2$ as follows:

$$\begin{aligned}
&(s_1,s_2) \in [\![\langle\alpha\rangle A]\!]_{t_1 \,||\, t_2} \\
=\ &\{\text{def. 27}\} \\
&(\exists a \in \alpha \ : \ (s_1,s_2) \xrightarrow{a}{}' (s_1',s_2') \wedge (s_1',s_2') \in [\![A]\!]_{t_1 \,||\, t_2}) \\
=\ &\{\text{Induction Hypothesis}\} \\
&(\exists a \in \alpha \ : \ (s_1,s_2) \xrightarrow{a}{}' (s_1',s_2') \wedge s_1' \in [\![A/s_2']\!]_{t_1}) \\
=\ &\{\text{def. 4; split domain}\} \\
&(\exists a \in \alpha \ : \ s_1 \xrightarrow{a}_1 s_1' \wedge s_1' \in [\![A/s_2]\!]_{t_1}) \vee \\
&(\exists a \in \alpha \ : \ s_2 \xrightarrow{a}_2 s_2' \wedge s_1 \in [\![A/s_2']\!]_{t_1}) \vee \\
&(\exists a \in \alpha \ : \ (\exists a_1 \sqsubset a \ : \ s_1 \xrightarrow{a_1}_1 s_1' \wedge s_2 \xrightarrow{a \setminus a_1}_2 s_2' \wedge s_1' \in [\![A/s_2']\!]_{t_1})) \\
=\ &\{\text{def. 27; correspondence } \exists \text{ and } \vee\} \\
&s_1 \in [\![\langle\alpha\rangle(A/s_2)]\!]_{t_1} \vee \\
&\bigvee_{s_2 \xrightarrow{a}_2 s_2'}^{a \in \alpha} (s_1 \in [\![A/s_2']\!]_{t_1}) \vee \\
&\bigvee_{a \in \alpha} \bigvee_{s_2 \xrightarrow{a_2}_2 s_2'}^{a_2 \sqsubset a} (s_1' \in [\![\langle a \setminus a_2\rangle(A/s_2')]\!]_{t_1}) \\
=\ &\{\text{def. 19}\} \\
&s_1 \in [\![\langle\alpha\rangle(A/s_2) \vee \\
&\bigvee_{s_2 \xrightarrow{a}_2 s_2'}^{a \in \alpha} (A/s_2') \vee \\
&\bigvee_{a \in \alpha} \bigvee_{s_2 \xrightarrow{a_2}_2 s_2'}^{a_2 \sqsubset a} (\langle a \setminus a_2\rangle(A/s_2'))]\!]_{t_1}
\end{aligned}$$

So, let the quotient operator for this case be defined as:

Definition 28 (quotienting for sets of actions in modal operators)**.**

$$\begin{aligned}
(\langle\alpha\rangle A)/s_2 = \langle\alpha\rangle(A/s_2) \vee \\
&\bigvee_{s_2 \xrightarrow{a}_2 s_2'}^{a \in \alpha} (A/s_2') \vee \\
&\bigvee_{a \in \alpha} \bigvee_{s_2 \xrightarrow{a_2}_2 s_2'}^{a_2 \sqsubset a} (\langle a \setminus a_2\rangle(A/s_2'))
\end{aligned}$$

The case for $([\alpha]A)/s_2$ is defined dually.

Example 29 (sets extension)**.** Suppose we would like to check if in the parallel system of Figure 1, it holds that a transition with label of the set $\{a, a|b\}$ can be taken. We use t for t_1 and t' for t_2. This can be expressed in the following modal equation system:

$$\mathcal{E} = (\mu X = \langle\{a, a|b\}\rangle \mathsf{true}) \downarrow X$$

The question we wish to answer is whether $t \,||\, t' \models \mathcal{E}$. We can quotient out the system t_2 and obtain:

$$\mathcal{E}/t' = \begin{pmatrix} (\mu X_{s'_3} = \langle\{a, a|b\}\rangle \mathsf{true} \vee \langle a\rangle \mathsf{true}) \\ (\mu X_{s'_4} = \langle\{a, a|b\}\rangle \mathsf{true}) \end{pmatrix}$$

Quotienting out t yields:

$$\mathcal{E}/t'/t = \begin{pmatrix} (\mu X_{s'_{3_{s_1}}} = \langle\{a, a|b\}\rangle \mathsf{true} \vee \mathsf{true} \vee \langle b\rangle \mathsf{true} \vee \mathsf{true}) \\ (\mu X_{s'_{3_{s_2}}} = \langle\{a, a|b\}\rangle \mathsf{true}) \\ (\mu X_{s'_{4_{s_1}}} = \langle\{a, a|b\}\rangle \mathsf{true} \vee \mathsf{true} \vee \langle b\rangle \mathsf{true}) \\ (\mu X_{s'_{4_{s_2}}} = \langle\{a, a|b\}\rangle \mathsf{true}) \end{pmatrix}$$

This can be solved to true, proving that $t \,||\, t' \models \mathcal{E}$.

4.2 Communication

The quotienting rule for the communication operator is quite different from the other quotienting rules. Since the communication operator is a function from one labeled transition system to another, we are not quotienting out a parallel system but the operator itself: we want to define the quotient operator on the communication operator such that the property we want to verify on $\Gamma_{\{\alpha_1 \to a_1, \ldots, \alpha_n \to a_n\}(t)}$ is expressed as a property on t.

We again use the soundness as specification and derive the correct definition for $(\langle\alpha\rangle A)/\Gamma\{\alpha_1 \to a_1, \ldots, \alpha_n \to a_n\}$.

The specification for $(\langle\alpha\rangle A)/\Gamma\{\alpha_1 \to a_1, \ldots, \alpha_n \to a_n\}$ is as follows:

$$s \in [\![\langle\alpha\rangle A]\!]_{\Gamma_{\{\alpha_1 \to a_1, \ldots, \alpha_n \to a_n\}(t)}} = s \in [\![(\langle\alpha\rangle A)/\Gamma_{\{\alpha_1 \to a_1, \ldots, \alpha_n \to a_n\}}]\!]_t$$

We again use structural induction, i.e. we assume the quotient operator the be well-defined on smaller terms:

$$(\forall x \in S \;:\; x \in [\![A]\!]_{\Gamma_{\{\alpha_1 \to a_1, \ldots, \alpha_n \to a_n\}(t)}} = x \in [\![A/\Gamma_{\{\alpha_1 \to a_1, \ldots, \alpha_n \to a_n\}}]\!]_t)$$

Now we derive the correct definition:

$$
\begin{aligned}
& s \in [\![\langle\alpha\rangle A]\!]_{\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}}(t)} \\
= & \{\text{def. 27}\} \\
& (\exists a \in \alpha, s' \in S_t \ : \ s \xrightarrow{a}{}' s' \wedge s' \in [\![A]\!]_{\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}}(t)}) \\
= & \{\text{Induction Hypothesis}\} \\
& (\exists a \in \alpha, s' \in S_t \ : \ s \xrightarrow{a}{}' s' \wedge s' \in [\![A/\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}}]\!]_t) \\
= & \{\text{def. 6}\} \\
& (\exists a \in \alpha, s' \in S_t \ : \ (s \xrightarrow{a} s' \wedge (\forall\ 1 \le i \le n \ : \ \alpha_i \not\sqsubseteq a)) \vee \\
& \quad (\exists\ 1 \le i \le n \ : \ s \xrightarrow{\alpha_i|(a\setminus a_i)} s') \wedge s' \in [\![A/\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}}]\!]_t) \\
= & \{\text{logic}\} \\
& (\exists a \in \alpha \ : \ (\exists s' \in S_t \ : \ (s \xrightarrow{a} s' \wedge (\forall\ 1 \le i \le n \ : \ \alpha_i \not\sqsubseteq a)) \wedge s' \in [\![A/\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}}]\!]_t) \vee \\
& \quad (\exists\ s' \in S_t, 1 \le i \le n \ : \ s \xrightarrow{\alpha_i|(a\setminus a_i)} s' \wedge s' \in [\![A/\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}}]\!]_t)) \\
= & \{\text{logic}\} \\
& (\exists a \in \alpha \ : \ ((\forall\ 1 \le i \le n \ : \ \alpha_i \not\sqsubseteq a) \wedge (\exists s' \in S_t \ : \ s \xrightarrow{a} s' \wedge s' \in [\![A/\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}}]\!]_t)) \vee \\
& \quad (1 \le i \le n \ : \ (\exists s' \in S_t \ : \ s \xrightarrow{\alpha_i|(a\setminus a_i)} s' \wedge s' \in [\![A/\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}}]\!]_t))) \\
= & \{\text{correspondence } \exists/\vee \text{ and } \forall/\wedge\} \\
& \bigvee_{a\in\alpha} \left((\bigwedge_{1\le i\le n} (\alpha_i \not\sqsubseteq a) \wedge (\exists s' \in S_t \ : \ s \xrightarrow{a} s' \wedge s' \in [\![A/\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}}]\!]_t)) \vee \right. \\
& \quad \left. \bigvee_{1\le i\le n} \left((\exists s' \in S_t \ : \ s \xrightarrow{\alpha_i|(a\setminus a_i)} s' \wedge s' \in [\![A/\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}}]\!]_t) \right) \right) \\
= & \{\text{case distinction on } \bigwedge_{1\le i\le n} (\alpha_i \not\sqsubseteq a)\} \\
& \bigvee_{a\in\alpha} \left(\left(\left(\begin{cases} (\exists s' \in S_t \ : \ s \xrightarrow{a} s' \wedge s' \in [\![A/\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}}]\!]_t) & \text{, if } \bigwedge_{1\le i\le n} (\alpha_i \not\sqsubseteq a) \\ \mathsf{false} & \text{, otherwise} \end{cases} \right) \vee \right. \right. \\
& \quad \left. \left. \bigvee_{1\le i\le n} \left((\exists s' \in S_t \ : \ s \xrightarrow{\alpha_i|(a\setminus a_i)} s' \wedge s' \in [\![A/\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}}]\!]_t) \right) \right) \right) \\
= & \{\text{def. 27, twice}\} \\
& s_1 \in [\![\bigvee_{a\in\alpha} \left(\left(\left(\begin{cases} \langle a\rangle (A/\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}}) & \text{, if } \bigwedge_{1\le i\le n} (\alpha_i \not\sqsubseteq a) \\ \mathsf{false} & \text{, otherwise} \end{cases} \right) \vee \right. \right. \\
& \quad \left. \left. \bigvee_{1\le i\le n} \left(\langle \alpha_i|(a\setminus a_i)\rangle (A/\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}}) \right) \right) \right)]\!]_t
\end{aligned}
$$

So, we define the quotient operator for this case as follows:

Definition 30 (quotienting for communication operator)**.**

$$(\langle\alpha\rangle A)/\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}} = \bigvee_{a\in\alpha}\left(\left(\begin{cases}\langle a\rangle(A/\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}}) & \text{, if } \bigwedge_{1\le i\le n}(\alpha_i \not\sqsubseteq a)\\ \mathsf{false} & \text{, otherwise}\end{cases}\right) \vee \bigvee_{1\le i\le n}\left(\langle\alpha_i|(a\setminus a_i)\rangle(A/\Gamma_{\{\alpha_1\to a_1,\ldots,\alpha_n\to a_n\}})\right)\right)$$

The case for $([\alpha]A)/\Gamma_{\{\alpha_1\to a_1\}}$ *is defined dually.*

Example 31 (communication extension)**.** Consider the system $\Gamma_{\{a|b\to c\}}(t\,||\,t')$ of Figure 2. We wish to check if this system satisfies the property that a c-action is possible, which can be expressed in a modal equation system as follows:

$$\mathcal{E} = (\mu X = \langle c\rangle\mathsf{true})$$

The question is whether $\Gamma_{\{a|b\to c\}}(t\,||\,t') \models \mathcal{E}$. Quotienting out the communication operator yields:

$$\mathcal{E}/\Gamma_{a|b\to c} = (\mu X = \langle a|b\rangle\mathsf{true} \vee \langle c\rangle\mathsf{true})$$

What remains to check is whether $t\,||\,t' \models \mathcal{E}/\Gamma_{\{a|b\to c\}}$. This is as usual and yields true.

4.3 Allow

As with the communication operator, we want to define the quotient operator on the allow operator such that the property we want to verify on $\nabla_H(t)$ is expressed as a property on t. More formally, we want to define the quotient operator / such that

$$\nabla_H(t) \models \mathcal{E} \qquad \text{if and only if,} \qquad t \models \mathcal{E}/\nabla_H$$

The system $\nabla_H(t)$ is obtained from t by removing all transitions with a label that does not occur in H. So, the property $\langle a\rangle A$ on the system $\nabla_H(t)$ is only true for those states s for which $s \xrightarrow{a} s'$ in the system t *and* it must not have been removed by the allow operator, so $a \in H$ must hold also.

We derive the correct definition for $(\langle\alpha\rangle A)/\nabla_H$, using the soundness of the quotient rule as specification:

$$s \in [\![\langle\alpha\rangle A]\!]_{\nabla_H(t)} = s \in [\![(\langle\alpha\rangle A)/\nabla_H]\!]_t$$

We again assume the quotient operator the be well-defined on smaller terms:

$$(\forall x \in S \;:\; x \in [\![A]\!]_{\nabla_H(t)} = x \in [\![A/\nabla_H]\!]_t)$$

Now we derive the correct definition:

$$
\begin{aligned}
& s \in [\![\langle\alpha\rangle A]\!]_{\nabla_H(t)} \\
= & \{\text{def. 27}\} \\
& (\exists a \in \alpha \ : \ s \xrightarrow{a}{}' s' \wedge s' \in [\![A]\!]_{\nabla_H(t)}) \\
= & \{\text{Induction hypothesis}\} \\
& (\exists a \in \alpha \ : \ s \xrightarrow{a}{}' s' \wedge s' \in [\![A/\nabla_H]\!]_t) \\
= & \{\text{def. 8; case distinction } a \in H\} \\
& (\exists a \in \alpha \ : \ a \in H \wedge s \xrightarrow{a} s' \wedge s' \in [\![A/\nabla_H]\!]_t) \vee \\
& \mathsf{false} \\
= & \{\text{def. 27; correspondence } \exists \text{ and } \vee\text{; set theory}\} \\
& s \in [\![\langle\alpha \cap H\rangle(A/\nabla_H)]\!]_t
\end{aligned}
$$

So we define the quotient operator in this case as:

Definition 32 (quotienting for allow operator)**.**

$$(\langle\alpha\rangle A)/\nabla_H = \langle\alpha \cap H\rangle(A/\nabla_H)$$

The case for $([\alpha]A)/\nabla_H$ *is defined dually.*

Example 33 (allow extension)**.** Consider the system $\nabla_{\{a,b\}}(t \,||\, t')$ of Figure 2. We wish to check whether this system satisfies the property that an $a|b$-action is possible, which can be expressed in a modal equation system as follows:

$$\mathcal{E} = (\mu X = \langle a|b\rangle \mathsf{true})$$

The question is whether $\nabla_{\{a,b\}}(t \,||\, t') \models \mathcal{E}$. Quotienting out the allow operator yields:

$$\mathcal{E}/\nabla_{\{a,b\}} = (\mu X = \mathsf{false})$$

What remains to check is whether $t \,||\, t \models \mathcal{E}/\nabla_{\{a,b\}}$. This is as usual and obviously yields false.

Conclusion

We adapted the quotienting procedure by Andersen [2] to match the semantics of labeled transition systems used by the model checking tool mCRL2. We then proved the quotienting procedure was indeed sound in this setting. Then we extended the quotienting procedure to be able to use modal operators with sets of actions rather than single actions, and to strip off two mCRL2-specific operators working on the combined systems. This exposes the underlying structure of systems working in parallel, and this structure can be further exploited by the quotienting procedure. This soundness proof and the extensions makes it possible to implement the quotienting procedure in mCRL2.

Future work

We have laid out some ground work for including the quotienting procedure in the mCRL2 model checking tool, but we have not actually done so. It should be interesting to implement the quotienting procedure in mCRL2 and see if the improvement is consistent with earlier experiments.

The model checking tool mCRL2 uses labeled transition systems only as an intermediate, which it generates from a smaller description of the system. These system descriptions can be used to describe systems with an infinite state space, meaning the labeled transition system would be infinitely large. For these system descriptions, we have not yet explored whether quotienting can work. We think this could be done, but this obviously requires a more symbolic approach.

References

[1] Henrik Reif Andersen, *Verification of temporal properties of concurrent systems*, PhD Thesis DAIMI PB–445, Department of Computer Science, Aarhus University, DK–8000 Aarhus C, Denmark, June 1993, ISSN 0105–8517.

[2] Henrik Reif Andersen, *Partial model checking (extended abstract)*, In Proceedings, Tenth Annual IEEE Symposium on Logic in Computer Science, IEEE Computer Society Press, 1995, pp. 398–407.

[3] Hans Bekić, *Definable operation in general algebras, and the theory of automata and flowcharts*, Programming Languages and Their Definition, 1984, pp. 30–55.

[4] Jan Friso Groote and Michel Reniers, *Course reader 2IW26 - System Validation*, (2010).

[5] Angelika Mader, *Verification of modal properties using boolean equation systems*, Edition versal 8, Bertz Verlag, Berlin, 1997.