URL: http://www.elsevier.nl/locate/entcs/volume18.html 12 pages

Derivation of Characteristic Formulae

Markus Müller-Olm

Fachbereich Informatik
Universität Dortmund
44221 Dortmund, Germany

Abstract

This paper shows how modal mu-calculus formulae characterizing finite-state processes up to strong or weak bisimulation can be derived directly from the well-known greatest fixpoint characterizations of the bisimulation relations. Our derivation simplifies earlier proofs for the strong bisimulation case and, by virtue of derivation, immediately generalizes to various other bisimulation-like relations, in particular weak bisimulation.

1 Introduction

By a classic result of Hennessy and Milner [3,8] two (image-finite) processes are strongly bisimilar if and only if they satisfy exactly the same formulae of a simple modal logic, now often called *Henessy-Milner-Logic* (HML). In particular, for any two non-bisimilar processes P, Q there is an HML formula ϕ satisfied by P but not by Q. This result shows that HML is sufficiently expressive for distinguishing processes up to strong bisimulation. In another sense, however, the expressiveness of HML is too poor: there is in general no single formula, i.e. no *characteristic formula*, satisfied by just the processes bisimilar to a given process P. Bisimulation classes are thus only characterized by sets of formulae.

Graf and Sifakis [2] show that characteristic formulae can be constructed for finite, i.e. non-cyclic, CCS processes in the *modal mu-calculus*, an extension of HML with fixpoint formulae. This result has been extended to finite-state processes by Steffen and Ingólfsdóttir [10,11]. While Graf and Sifakis considered strong bisimulation and observational congruence, Steffen and Ingólfsdóttir are concerned with the so-called strong divergence preorder of CCS, a variant of strong bisimulation that takes information about divergence (i.e. internal non-termination) into account. It is not difficult to modify the latter in order to obtain characteristic formulae for strong bisimulation. It is, however, less obvious how to construct characteristic formulae for weak bisimulation-like relations. Actually, [10] proposes to treat weak bisimulation

by transforming the processes in such a way that weak bisimilarity of the original processes corresponds to strong bisimulation of the transformed ones. Then the characteristic formulae for strong bisimulation could be applied on the transformed processes. This approach, however, due to the necessity of transformation does not lead to actual characteristic formulae.

The contribution of this paper is a direct derivation of characteristic formulae from the classic greatest fixpoint characterization of (strong and weak) bisimulation. On the one hand, this provides a more elegant proof of the characterization property. On the other hand it immediately indicates how to construct characteristic formulae for other bisimulation-like process relations, like the various divergence relations discussed in [13], in particular for the weak versions.

We proceed as follows. In the next section we define the modal mu-calculus and labeled transition systems as basic model of processes and introduce equation systems. Section 3 defines the notion of strong bisimulation. In the following section we derive a characteristic equation system of a finite-state process from the fixpoint characterization of strong bisimulation. Section 5 generalizes this to weak bisimulation. In the section thereafter we indicate how to construct actual characteristic formulae from characteristic equation systems. The paper finishes with some concluding remarks.

2 Modal mu-Calculus, Processes, and Equation Systems

The modal mu-calculus [5] is a small, yet expressive process logic. It is defined over a given finite set A of *actions*. We consider in this paper modal mu-calculus formulae in positive normal form, which are constructed according to the following grammar:

$$\phi \ ::= \ \mathsf{true} \mid \mathsf{false} \mid \phi_1 \wedge \phi_2 \mid \phi_1 \vee \phi_2 \mid \langle a \rangle \phi \mid [a]\phi \mid X \mid \mu X \,.\, \phi \mid \nu X \,.\, \phi$$

Here, X ranges over an infinite set Var of variables and a over the assumed action set A. The two *fixpoint operators* μX and νX bind the respective variable X and we will apply the usual terminology of free and bound variables in a formula, closed formula etc. Moreover, we write for a finite set M of formulae $\bigwedge M$ and $\bigvee M$ for the conjunction and disjunction of the formulae in M. As usual, we agree that $\bigwedge \emptyset = \mathsf{true}$ and $\bigvee \emptyset = \mathsf{false}$.

Modal mu-calculus formulae are interpreted over processes, which are modeled by labeled transition systems with a designated start state. Formally, a *process* is a structure $P = (S, A, \rightarrow_P, s_0)$, where S is a set of *states*, A is the above (finite) set of *actions*, $\rightarrow_P \subseteq S \times A \times S$ is a *transition relation*, and s_0 is the *initial state*. Throughout this paper we assume that the constituting parts of a process named P are S, A, $\rightarrow_P$, and s_0 and the ones of a process named Q are T, A, $\rightarrow_Q$ and t_0. A process P is called *finite-state* if the underlying state set S is finite.

$$
\begin{aligned}
M_P(\mathsf{true})(\rho) &= S \\
M_P(\mathsf{false})(\rho) &= \emptyset \\
M_P(\phi_1 \wedge \phi_2)(\rho) &= M_P(\phi_1)(\rho) \cap M_P(\phi_2)(\rho) \\
M_P(\phi_1 \vee \phi_2)(\rho) &= M_P(\phi_1)(\rho) \cup M_P(\phi_2)(\rho) \\
M_P(\langle a \rangle \phi)(\rho) &= \{s \mid \exists s' : s \xrightarrow{a} s' \ \wedge \ s' \in M_P(\phi)(\rho)\} \\
M_P([a]\phi)(\rho) &= \{s \mid \forall s' : s \xrightarrow{a} s' \ \Rightarrow \ s' \in M_P(\phi)(\rho)\} \\
M_P(X)(\rho) &= \rho(X) \\
M_P(\mu X \,.\, \phi)(\rho) &= \bigcap \{x \subseteq S \mid M_P(\phi)(\rho[X \mapsto x]) \subseteq x\} \\
M_P(\nu X \,.\, \phi)(\rho) &= \bigcup \{x \subseteq S \mid M_P(\phi)(\rho[X \mapsto x]) \supseteq x\}
\end{aligned}
$$

Fig. 1. Semantics of modal mu-calculus

Suppose given a process P for the remainder of this section. The subset of states that satisfy a formula ϕ, denoted by $M_P(\phi)(\rho)$, is inductively defined in Fig. 1. As usual we refer to *environments*, partial mappings $\rho : \mathsf{Var} \stackrel{\text{part.}}{\longrightarrow} 2^S$ which interpret at least the free variables of ϕ by subsets of S, in order to explain the meaning of open formulas. For a set $x \subseteq S$ and a variable $X \in \mathsf{Var}$ we write $\rho[X \mapsto x]$ for the environment that maps X to x and that is defined on a variable $Y \neq X$ iff ρ is defined on Y and maps Y then to $\rho(Y)$.

Intuitively, true and false hold for all resp. no states and $\wedge$ and $\vee$ are interpreted by conjunction and disjunction. As in HML, $\langle a \rangle \phi$ holds for a state s if there is an a-successor of s which satisfies ϕ, and $[a]\phi$ holds for s if all its a-successors, satisfy ϕ. The interpretation of a variable X is as prescribed by the environment. The formula $\mu X \,.\, \phi$, called a *least fixpoint formula*, is interpreted by the smallest subset x of S that recurs when ϕ is interpreted with the substitution of x for X. Similarly, $\nu X \,.\, \phi$, called *greatest fixpoint formula*, is interpreted by the largest such set. Existence of such sets as well as their characterization used in Fig. 1 follows from the well-known Knaster-Tarski fixpoint theorem [12].

As the meaning of a closed formula ϕ does not depend on the environment, we sometimes write $M_P(\phi)$ for $M_P(\phi)(\rho)$ where ρ is an arbitrary environment. The set of processes *satisfying* a given closed formula ϕ is $P(\phi) = \{Q \mid t_0 \in M_Q(\phi)\}$.

We shall also refer to (closed) *equation systems* of modal mu-calculus formulae of the form

$$
\begin{aligned}
E : X_1 &= \phi_1 \\
&\vdots \\
X_n &= \phi_n \ ,
\end{aligned}
$$

where $X_1, \ldots, X_n$ are mutually distinct variables and $\phi_1, \ldots, \phi_n$ are mu-calculus formulae having at most $X_1, \ldots, X_n$ as free variables.

An environment $\rho : \{X_1, \ldots, X_n\} \to 2^S$ is *a solution* of an equation system E, if $\rho(X_i) = M_P(\phi_i)(\rho)$. That solutions always exist, is again a consequence of the Knaster-Tarski fixpoint theorem. For, consider the set of environments that are candidates for solutions, $\mathsf{Env}_P = \{\rho \mid \rho : \{X_1, \ldots, X_n\} \to 2^S\}$. Env_P together with the lifting $\sqsubseteq$ of the inclusion order on 2^S, defined by

$$\rho \sqsubseteq \rho' \text{ iff } \rho(X_i) \subseteq \rho'(X_i) \text{ for } i = 1, \ldots, n$$

forms a complete lattice. Now, we can define the *equation functional* $F_P^E : \mathsf{Env}_P \to \mathsf{Env}_P$ by $F_P^E(\rho)(X_i) = M_P(\phi_i)(\rho)$ for $i = 1, \ldots, n$, the fixpoints of which are just the solutions of E. Certainly, F_P^E is monotonic as $M_P(\phi_i)$ is monotonic such that the Knaster-Tarski fixpoint theorem guarantees existence of solutions. In particular, there is the largest solution νF_P^E of E (w.r.t. $\sqsubseteq$), in which we are particularly interested and which we denote by $M_P(E)$. This definition interprets equation systems on the states of a given process P. We lift this to processes by agreeing that a process satisfies an equation system E, if its initial state is in the largest solution of the first equation. Thus the set of processes satisfying equation system E is $P(E) = \{Q \mid t_0 \in M_Q(E)(X_1)\}$.

3 Strong Bisimulation

As transition systems provide a too fine-grained model of processes, various equivalences have been studied in the literature that identify processes on the basis of their behavior. A classic example is strong bisimulation [9,8] denoted by $\sim$.

Suppose given two processes P and Q. Bisimulation is first defined as a relation between the state sets S and T and then lifted to the processes themselves. A relation $R \subseteq S \times T$ is called a *(strong) bisimulation* if for all $(s,t) \in R$ the following two conditions hold:

a) $\forall a, s' : s \xrightarrow{a}_P s' \Rightarrow \exists t' : t \xrightarrow{a}_Q t' \wedge (s', t') \in R$, and

b) $\forall a, t' : t \xrightarrow{a}_Q t' \Rightarrow \exists s' : s \xrightarrow{a}_P s' \wedge (s', t') \in R$.

Now, $\sim$ is defined to be the union of all bisimulations R. The processes P and Q are called *bisimilar* if $s_0 \sim t_0$. By abuse of notation we denote this relationship by $P \sim Q$ and view $\sim$ also as a relation between processes.

The relation $\sim \subseteq S \times T$ can also be characterized as the greatest fixpoint $\nu F_\sim$ of the following monotonic functional $F_\sim$ on the complete lattice of relations $R \subseteq S \times T$ ordered by set inclusion:

$$F_\sim(R) \stackrel{\text{def}}{=} \{(s,t) \mid s, t \text{ satisfy the bisimulation conditions a) and b)}\} \ .$$

For, it is easy to see that a relation R is a bisimulation iff $R \subseteq F_\sim(R)$, i.e. if R is a *post-fixpoint* of $F_\sim$. And, by the Knaster-Tarski fixpoint theorem, $\nu F_\sim$ is just the union of all post-fixpoints of $F_\sim$, i.e. bisimulations, and, therefore, equals $\sim$. This also establishes the well-known fact, that $\sim$ is again a bisimulation,

viz. the largest one, as the largest fixpoint of $F_\sim$ clearly is also its largest post-fixpoint.

4 Characteristic Equation Systems

Assume now, that a finite-state process P is given, that $s_1, \ldots, s_n$ are its $|S| = n$ states, and that $s_1 = s_0$ is its initial state. The goal of this paper is to show how a formula characterizing P up to strong bisimulation can be derived from the fixpoint characterization of bisimulation. While the existence and construction of such formulae is well-known [10,11], their derivation rather than postulation provides a more elegant proof of the characterization property and shows, moreover, how corresponding formulae for other bisimulation-like equivalences and preorders may be constructed. We illustrate this point by treating also weak bisimulation (see Section 5).

Our derivation proceeds via a *characteristic equation system*

$$\begin{aligned} E_\sim : X_{s_1} &= \phi^\sim_{s_1} \\ &\vdots \\ X_{s_n} &= \phi^\sim_{s_n} \end{aligned}$$

consisting of one equation for each of the states $s_1, \ldots, s_n \in S$. The construction of actual characteristic formulae from the characteristic equation system is deferred to Section 6. The goal is to define the formulae $\phi^\sim_s$ such that the largest solution $M_Q(E_\sim)$ of $E_\sim$ on an arbitrary process Q associates the variables X_s just with the states of Q bisimilar to s, i.e. such that $M_Q(E_\sim)(X_s) = \{t \in T \mid s \sim t\}$.

The construction of $E_\sim$ is based on the observation that Env_Q, the set of candidates for solutions of $E_\sim$, is order-isomorphic to $2^{S\times T}$, the set of relations that are candidates to be bisimulations between S and T. Actually, the mapping $\alpha : \mathsf{Env}_Q \to 2^{S\times T}$ defined by

$$\alpha(\rho) \;=\; \{(s,t) \in S \times T \mid t \in \rho(X_s)\}$$

is an order isomorphism between Env_Q and $2^{S\times T}$, the inverse of which is the mapping $\beta : 2^{S\times T} \to \mathsf{Env}_Q$ defined by $\beta(R)(X_s) = \{t \in T \mid (s,t) \in R\}$.

The idea is now to define $E_\sim$ such that $F_\sim$, the bisimulation functional, and $F_Q^{E_\sim}$, the functional belonging to $E_\sim$, are equal up to the isomorphism induced by (α, β), i.e. such that

$$F_Q^{E_\sim} = \beta \circ F_\sim \circ \alpha \;\; . \tag{1}$$

Then their largest fixpoints are also related by the isomorphism, which yields:

$$\begin{aligned} & M_Q(E_\sim)(X_s) \\ = \;\; & \text{[Definition of } M_Q(E_\sim)\text{]} \\ & (\nu F_Q^{E_\sim})(X_s) \end{aligned}$$

$=$ [Fixpoints of $F_Q^{E_\sim}$ and $F_\sim$ are related by the isomorphism]
$\beta(\nu F_\sim)(X_s)$
$=$ [Definition of β]
$\{t \in T \mid (s,t) \in (\nu F_\sim)\}$
$=$ [$\sim$ equals $\nu F_\sim$]
$\{t \in T \mid s \sim t\}$,

as required. By the definition of $F_Q^{E_\sim}$, (1) amounts to defining ϕ_s such that

$$t \in M_Q(\phi_s^\sim)(\rho) \quad \text{iff} \quad t \in (\beta \circ F_\sim \circ \alpha)(\rho)(X_s) \ .$$

The strategy for making this equivalence hold is to start a calculation with the right hand side and to stepwise transform it into the direction of a formula:

$t \in (\beta \circ F_\sim \circ \alpha)(\rho)(X_s)$
iff [Definition of β]
$(s,t) \in (F_\sim \circ \alpha)(\rho)$
iff [Definition of $F_\sim$]
$\forall a : \forall s' : s \xrightarrow{a}_P s' \ \Rightarrow \ \exists t' : t \xrightarrow{a}_Q t' \wedge (s',t') \in \alpha(\rho)$, and
$\forall a : \forall t' : t \xrightarrow{a}_Q t' \ \Rightarrow \ \exists s' : s \xrightarrow{a}_P s' \wedge (s',t') \in \alpha(\rho)$
iff [Definition of α]
$\forall a : \forall s' : s \xrightarrow{a}_P s' \ \Rightarrow \ \exists t' : t \xrightarrow{a}_Q t' \wedge t' \in \rho(X_{s'})$, and
$\forall a : \forall t' : t \xrightarrow{a}_Q t' \ \Rightarrow \ \exists s' : s \xrightarrow{a}_P s' \wedge t' \in \rho(X_{s'})$
iff [Definition of $M_Q(X_{s'})$]
$\forall a : \forall s' : s \xrightarrow{a}_P s' \ \Rightarrow \ \exists t' : t \xrightarrow{a}_Q t' \wedge t' \in M_Q(X_{s'})(\rho)$, and
$\forall a : \forall t' : t \xrightarrow{a}_Q t' \ \Rightarrow \ \exists s' : s \xrightarrow{a}_P s' \wedge t' \in M_Q(X_{s'})(\rho)$
iff [Definition $\langle a \rangle$, Definition $\bigvee$]
$\forall a : \forall s' : s \xrightarrow{a}_P s' \ \Rightarrow \ t \in M_Q(\langle a \rangle X_{s'})(\rho)$, and
$\forall a : \forall t' : t \xrightarrow{a}_Q t' \ \Rightarrow \ t' \in M_Q(\bigvee\{X_{s'} \mid s \xrightarrow{a}_P s'\})(\rho)$
iff [Definition $\bigwedge$, Definition $[a]$]
$\forall a : t \in M_Q(\bigwedge\{\langle a \rangle X_{s'} \mid s \xrightarrow{a}_P s'\})(\rho)$, and
$\forall a : t \in M_Q([a]\bigvee\{X_{s'} \mid s \xrightarrow{a}_P s'\})(\rho)$
iff [Definition $\bigwedge$]
$t \in M_Q(\bigwedge\{\bigwedge\{\langle a \rangle X_{s'} \mid s \xrightarrow{a}_P s'\} \mid a \in A\})(\rho)$, and
$t \in M_Q(\bigwedge\{[a]\bigvee\{X_{s'} \mid s \xrightarrow{a}_P s'\} \mid a \in A\})(\rho)$

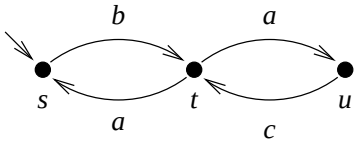

Fig. 2. An example process.

iff [Definition $\wedge$]

$$t \in M_Q(\bigwedge\{\bigwedge\{\langle a\rangle X_{s'} \mid s \xrightarrow{a}_P s'\} \mid a \in A\} \wedge \bigwedge\{[a]\bigvee\{X_{s'} \mid s \xrightarrow{a}_P s'\} \mid a \in A\})(\rho) \ .$$

Thus, (1) becomes valid if we define $\phi_s^\sim$ by

$$\phi_s^\sim \stackrel{\text{def}}{=} \bigwedge\{\bigwedge\{\langle a\rangle X_{s'} \mid s \xrightarrow{a}_P s'\} \mid a \in A\} \wedge \bigwedge\{[a]\bigvee\{X_{s'} \mid s \xrightarrow{a}_P s'\} \mid a \in A\}$$

and this gives us the desired theorem.

Theorem 4.1 (Char. eq. sys. on states) $M_Q(E_\sim)(X_s) = \{t \in T \mid s \sim t\}$.

This theorem holds for all processes Q as $E_\sim$ does not depend on Q. In particular, a process Q is bisimilar to P iff its initial state t_0 is contained in $M_Q(E_\sim)(X_{s_1})$ (recall that s_1 is the initial state of P). Thus we have the following corollary.

Corollary 4.2 (Char. eq. system on processes) $P(E_\sim) = \{Q \mid P \sim Q\}$.

For illustration, we consider the small process pictured in Fig. 2 with state set $S = \{s, t, u\}$ and action alphabet $A = \{a, b, c\}$. After removing conjuncts reading false, its characteristic equation system reads as follows:

$$\begin{aligned} E_\sim : X_s &= \langle b\rangle X_t \wedge [a]\mathsf{false} \wedge [b]X_t \wedge [c]\mathsf{false} \\ X_t &= \langle a\rangle X_s \wedge \langle a\rangle X_u \wedge [a](X_s \vee X_u) \wedge [b]\mathsf{false} \wedge [c]\mathsf{false} \\ X_u &= \langle c\rangle X_t \wedge [a]\mathsf{false} \wedge [b]\mathsf{false} \wedge [c]X_t \end{aligned}$$

5 Weak Bisimulation

Strong bisimulation requires that every step of a process is matched by a corresponding step of a bisimilar process. Weak bisimulation [8] denoted by $\approx$ relaxes this requirement for internal computation steps represented by a distinguished action $\tau \in A$, which can be matched by zero of more internal steps. The definition of weak bisimulations relies on a derived transition relation $\stackrel{a}{\Rightarrow}$ that allows arbitrarily many τ-transitions before and after an a-transition. In addition, the relation $\stackrel{\varepsilon}{\Rightarrow}$ is used that represents zero or more τ-transitions:

$$\stackrel{\varepsilon}{\Rightarrow} \stackrel{\text{def}}{=} \xrightarrow{\tau}{}^* \qquad\qquad \stackrel{a}{\Rightarrow} \stackrel{\text{def}}{=} \stackrel{\varepsilon}{\Rightarrow}; \xrightarrow{a}; \stackrel{\varepsilon}{\Rightarrow}$$

Here, the operator ; denotes relational composition. In the following, we let $\hat{\tau} = \varepsilon$ and for actions $a \neq \tau$, $\hat{a} = a$.

Now, a relation $R \subseteq S \times T$ between the state sets of two processes P and Q is called a *weak bisimulation* [8] if for all $(s,t) \in R$ the following two conditions hold:

a) $\forall a, s' : s \xrightarrow{a}_P s' \Rightarrow \exists t' : t \stackrel{\hat{a}}{\Rightarrow}_Q t' \wedge (s',t') \in R$, and

b) $\forall a, t' : t \xrightarrow{a}_Q t' \Rightarrow \exists s' : s \stackrel{\hat{a}}{\Rightarrow}_P s' \wedge (s',t') \in R$.

$\approx$ is defined to be the union of all weak bisimulations R and is the largest weak bisimulation. As for strong bisimulation, P and Q are called bisimilar, $P \approx Q$ for short, if $s_0 \approx t_0$.

Again, we can define a monotonic functional $F_{\approx} : 2^{S \times T} \to 2^{S \times T}$ on relations from the two conditions in the definition of weak bisimulations, the greatest fixpoint of which equals $\approx$. Moreover, an equation system characterizing a process up to weak bisimulation,

$$\begin{aligned} E_{\approx} : X_{s_1} &= \phi^{\approx}_{s_1} \\ &\vdots \\ X_{s_n} &= \phi^{\approx}_{s_n} \ , \end{aligned}$$

i.e. that satisfies $M_Q(E_{\approx})(X_s) = \{t \mid s \approx t\}$, can be constructed along the lines of the construction for strong bisimulation. The only difference is the occurrence of the derived transition relations $\stackrel{\hat{a}}{\Rightarrow}$ in the corresponding places. In order to tackle them we rely on 'weak' analogies $\langle\!\langle a \rangle\!\rangle$ of the modality $\langle a \rangle$, which can be introduced as abbreviations:

$$\langle\!\langle \varepsilon \rangle\!\rangle \phi \stackrel{\text{def}}{=} \mu X \,.\, \phi \vee \langle \tau \rangle X \qquad\qquad \langle\!\langle a \rangle\!\rangle \phi \stackrel{\text{def}}{=} \langle\!\langle \varepsilon \rangle\!\rangle \langle a \rangle \langle\!\langle \varepsilon \rangle\!\rangle \phi \ .$$

The following proposition shows that they indeed correspond to $\stackrel{\varepsilon}{\Rightarrow}$ and $\stackrel{a}{\Rightarrow}$.

Proposition 5.1 (Weak diamond)

- $M_P(\langle\!\langle \varepsilon \rangle\!\rangle \phi)(\rho) = \{s \mid \exists s' : s \stackrel{\varepsilon}{\Rightarrow}_P s' \ \wedge \ s' \in M_P(\phi)(\rho)\}$.
- $M_P(\langle\!\langle a \rangle\!\rangle \phi)(\rho) = \{s \mid \exists s' : s \stackrel{a}{\Rightarrow}_P s' \ \wedge \ s' \in M_P(\phi)(\rho)\}$.

Using these weak modalities it is now straightforward to redo the calculation that lead to an adequate definition of $\phi^{\sim}_s$ also for weak bisimulation, which results in the following definition for $\phi^{\approx}_s$:

$$\begin{aligned} \phi^{\approx}_s \stackrel{\text{def}}{=} \ & \bigwedge \{ \bigwedge \{ \langle\!\langle \hat{a} \rangle\!\rangle X_{s'} \mid s \xrightarrow{a}_P s' \} \mid a \in A \} \wedge \\ & \bigwedge \{ [a] \bigvee \{ X_{s'} \mid s \stackrel{\hat{a}}{\Rightarrow}_P s' \} \mid a \in A \} \ . \end{aligned}$$

The derivation shows in particular where to use strong and weak modalities and which set construction have to range over strong and weak successors.

Theorem 5.2 (Char. eq. sys. on states) $M_Q(E_{\approx})(X_s) = \{t \in T \mid s \approx t\}$.

Corollary 5.3 (Char. eq. system on processes) $P(E_{\approx}) = \{Q \mid P \approx Q\}$.

$$
\begin{array}{lll}
F: \quad X_1 = \phi_1 & G: \quad X_1 = \phi_1[\phi_n/X_n] & H: \quad X_1 = \phi_1 \\
\quad\vdots & \quad\vdots & \quad\vdots \\
X_{n-1} = \phi_{n-1} & X_{n-1} = \phi_{n-1}[\phi_n/X_n] & X_{n-1} = \phi_{n-1} \\
X_n = \nu X_n \,.\, \phi_n & X_n = \phi_n &
\end{array}
$$

Fig. 3. Results of the transformation rules

6 Towards Characteristic Formulae

Up to now processes were characterized up to strong or weak bisimulation by an appropriately defined equation system. Actual *characteristic formulae*, i.e. *single* formulae characterizing processes can be constructed by applying simple semantics-preserving transformation rules on equation systems, which are provided in this section. Together these rules allow to reduce an equation system stepwise by ever more equations. These rules are similar to the ones used by A. Mader in [7] as a means of solving Boolean equation systems (with alternation) by Gauss elimination.

In Fig. 3 we show the equation systems resulting from applying the three needed transformation rules on an equation system of the form

$$
\begin{array}{c}
E: X_1 = \phi_1 \\
\vdots \\
X_n = \phi_n \ .
\end{array}
$$

For notational convenience, we describe the transformations only w.r.t. the last equation in an equation system.

The first rule, transforming E to F, allows to eliminate the recursive dependency of the right hand side formula in an equation from the left hand side variable of that same equation. It is not difficult to show that, albeit F might have fewer solutions than E, their greatest solutions coincide on every process Q.

Proposition 6.1 $M_Q(E) = M_Q(F)$.

The second rule, that transforms E to G, allows to replace the variable on the left hand side of an equation by the formula on the right hand side in the other equations. As usual, $\phi[\psi/X]$ denotes the substitution of ψ for the free occurrences of X in ϕ. Being an instance of a substitution of 'equals for equals', E and G have the same solutions, as expected.

Proposition 6.2 *E and G have the same solutions, in particular,* $M_Q(E) = M_Q(G)$.

Our third and last rule, transforming E to H, allows to remove unnecessary equations from an equation system. It relies on the side condition that the variable X_n does not appear free in $\phi_1, \ldots, \phi_n$. Note that by this side condition

H is indeed a closed equation system. Removal of unnecessary equations does not affect the interpretation of the other variables in solutions.

Proposition 6.3 *Suppose X_n does not appear free in $\phi_1, \ldots, \phi_n$.*

An environment ρ is a solution of H if and only if $\rho[X_n \mapsto M_Q(\phi_n)(\rho)]$ is a solution of E. In particular, $M_Q(E) = M_Q(H)[X_n \mapsto M_Q(\phi_n)(M_Q(H))]$.

Now, applying to an equation system E the first rule followed by the second rule results in an equation system that satisfies the side condition of the third rule. Thus the last equation can be removed; the result is the equation system:

$$\begin{aligned} \tilde{E}: \quad X_1 &= \phi_1[\nu X_n \,.\, \phi_n / X_n] \\ &\vdots \\ X_{n-1} &= \phi_{n-1}[\nu X_n \,.\, \phi_n / X_n] \ . \end{aligned}$$

This procedure can be iterated until an equation system with just one equation $X_1 = \psi$ is obtained. A final application of the first rule results in the equation system with just the equation $X_1 = \nu X_1 \,.\, \psi$. The only solution of this equation system on a process Q is the environment ρ defined by $\rho(X_1) = M_Q(\nu X_1 \,.\, \psi)$ as $\nu X_1 \,.\, \psi$ is a closed formula. By the correctness of the transformation rules, $\nu X_1 \,.\, \psi$ is thus a formula, the interpretation of which coincides with the interpretation of X_1 in the greatest solution of the original equation system E. Therefore, any set of processes that can be characterized by an equation system can also be characterized by a single formula. Note, however, that the iterated application of the second transformation rule can lead to an exponential blow-up of the size of the formula.

Theorem 6.4 *For any equation system E there is a formula ϕ such that $P(E) = P(\phi)$.*

The above procedure can, in particular, be applied to $E_\sim$ and $E_\approx$ which shows that there are indeed characteristic formulae describing processes up to strong or weak bisimulation.

Theorem 6.5 (Characteristic formulae) *For all finite-state processes P there are modal mu-calculus formulae $\psi^\sim$ and $\psi^\approx$ such that $P(\psi^\sim) = \{Q \mid P \sim Q\}$ and $P(\psi^\approx) = \{Q \mid P \approx Q\}$.*

7 Conclusion

We have shown how equation systems and formulae that characterize finite-state processes up to strong or weak bisimulation can be derived directly from the greatest fixpoint characterizations of these relations. The existence of such formulae for strong bisimulation was well-known. By virtue of derivation, however, our simpler and more elegant proof generalizes immediately to weak bisimulation and can also easily be adapted to various other behavioral equivalences and preorders (like simulation and the preorders studied in [13]).

Do characteristic formulae exist also for some class of infinite-state processes? The answer is no. Any mu-calculus formula ψ representing a certain process P up to bisimulation has – by the finite model property of the modal mu-calculus [6] – also a finite model Q. Thus P must be bisimilar to Q, i.e. be a finite-state process up to bisimulation.

What is the use of characteristic equation systems and formulae? On the theoretical side, their existence provides specific expressiveness results for the modal mu-calculus. Combined with the fact that model checking the modal mu-calculus is decidable for certain classes of infinite-state processes, in particular push-down processes [14,1], this immediately implies that strong and weak bisimulation (and various other relations for which characteristic formulae can easily be constructed, e.g. simulation) are decidable between finite-state processes and push-down processes. More far-reaching decidability results of this kind have recently been studied by Jančar, Kučera, and Mayr [4].

On the practical side, characteristic formulae allow to employ model checkers as bisimulation checkers. For this application the exponential blow-up experienced in the transition from characteristic equation systems to characteristic formulae seems to be particularly unfortunate. However, many model checkers are based on equation systems rather than formulae, such that they can be applied directly on characteristic equation systems.

Acknowledgement

I thank Bernhard Steffen for a number of discussions on topics related to this paper and anonymous referees of MFCS for valuable comments that helped to improve this paper.

References

[1] O. Burkart and B. Steffen. Model-checking the full-modal mu-calculus for infinite sequential processes. In *ICALP '97*, LNCS 1256, pages 419–429. Springer-Verlag, 1997.

[2] S. Graf and J. Sifakis. A modal characterization of observational congruence on finite terms of CCS. *Information and Control*, 68:125–145, 1986.

[3] M. C. B. Hennessy and R. Milner. Algebraic laws for nondeterminism and concurrency. *JACM*, 32(1):137–161, 1985.

[4] P. Jančar, A. Kučera, and R. Mayr. Deciding bisimulation-like equivalences with finite-state processes. In *ICALP '98*, LNCS 1443, pages 200–211. Springer-Verlag, 1998.

[5] D. Kozen. Results on the propositional mu-calculus. *TCS*, 27:333–354, 1983.

[6] D. Kozen. A finite model theorem for the propositional μ-calculus. *Studia Logica*, 47:233–241, 1988.

[7] A. Mader. Modal μ-calculus, model checking and Gauss elimination. In *TACAS'95*, LNCS 1019, pages 72–88. Springer-Verlag, 1995.

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

[9] D. M. R. Park. Concurrency and automata on infinite sequences. In LNCS 154, pages 561–572. Springer-Verlag, 1981.

[10] B. Steffen. Characteristic formulae. In: *Concur'89*, LNCS 372, pages 723–732. Springer-Verlag, 1989.

[11] B. Steffen and A. Ingólfsdóttir. Characteristic formulae for processes with divergence. *Information and Computation*, 110(1):149–163, 1994.

[12] A. Tarski. A lattice-theoretical fixpoint theorem and its application. *Pacific Journal of Mathematics*, 5:285–309, 1955.

[13] D. J. Walker. Bisimulations and divergence in CCS. *Information and Computation*, 85(2):202–241, 1990.

[14] I. Walukiewicsz. Pushdown processes: games and model-checking. In *CAV'96*, LNCS 1102. Springer-Verlag, 1996.