Behavioral Equivalences and Approximations

Alessandro Aldini
University of Urbino, Italy

Abstract

Several application domains require formal and flexible techniques for the comparison of different process models. Whenever classical equivalence checking does not provide a positive result, relaxed notions of approximation can be employed to evaluate the degree of similarity. In this extended abstract, we first discuss the state of the art in the setting of approximate behavioral equivalences. Then, as a step towards flexibility and usability, we present a relaxation of testing equivalence taking into account three orthogonal aspects of the process observations: execution time, event probability, and observed behavior.

1 Approximations of Behavioral Equivalences

Comparing process models through equivalence checking is a frequently used approach to the analysis of systems in many practical domains, ranging from model-based verification of software implementations to the analysis of noninterference based dependability properties. However, in real-world applications perfect equivalence is usually hard to achieve, e.g. because the models to compare are specified at different abstraction levels, or else they describe alternative implementations of the same ideal system. In order to evaluate how much these models are similar, we need to specify some quantitative aspect in such a way that the comparison can result in numbers giving a flavor of the degree of similarity.

Very often, the quantitative aspects that come into play are expressed in terms of probability distributions and/or temporal behaviors. In this case, fine-grain notions of behavioral equivalences are somehow relaxed in order to measure the distance between models. It is also possible to compare quantitatively models that are purely functional. This can be done, e.g., through a benchmark of testing scenarios and some kind of mathematical function that estimates the capability of the models in fitting the behaviors offered by the tests forming the benchmark.

In the setting of approximate notions of behavioral equivalences, two alternative research lines emerged in the formal methods community: pseudometrics and intransitive relations. In the former case, a function d, inspired by Hutchinson-like metrics on probability measures, is defined that yields a (real number) distance for the models under comparison, say P and Q, such that $d(P, Q) = 0$ if and only if P and Q are equivalent, d is symmetric and satisfies the triangular disequality. For instance, the typical notion of equivalence for labeled Markov processes that is relaxed through pseudometrics is bisimulation. One reason is that the classical logical characterization of bisimulation can be turned into an alternative characterization using a specific set of functions into the reals instead of the logic. Two models are bisimilar if and only if they satisfy the same logical formulas, if and only if they have the same values for each functional expression of the set. In the case they are not bisimilar, the set of functional expressions induces a distance function d with the three properties mentioned above. This approach is used, e.g., in [3]. The same metric can be obtained through a completely different approach in which it is derived by defining a coalgebra for a certain functor on the category of metric spaces (see, e.g., [6]).

While these approaches provide interesting results in terms of, e.g., non-expansiveness with respect to process combinators like parallel composition[1], they suffer from some practical limitations. For instance, the pseudometrics provide a distance between process states, but do not suggest which pairs of states it is worth comparing. This is because the process states are not compared through any relation relaxing bisimulation. Moreover, it is not easy to establish a clear relation between the measure estimating similarity and its interpretation in a practical, activity oriented setting.

Other approaches rely on relations approximating bisimulation equivalence (see, e.g., [1, 4, 5]). These relations cannot be transitive and, for this reason, their investigation did not receive attention for many years. However, they can offer an interesting framework for real application domains.

For instance, [1] proposes an intuitive relaxation of weak probabilistic bisimulation, which is in direct relation with approximate lumping for Markov chains. The characterization of lumpability is useful, because the knowledge of a lumpable partition of the states of a Markov chain allows the generation of a (smaller) aggregated Markov chain that leads to several results for the original one without an error. In this setting, approaches that rely on perturbation theory establish bounds on the error made when approximating lumpability. These bounds are related with the numerical analysis of Markov chains and, therefore, provide a clear interpretation of their impact upon the performance behavior of a system. On the other hand, meta-heuristics search techniques are needed to make the verification

[1] Non-expansiveness is an analogue of the congruence property of bisimulation.

algorithm of approximate weak probabilistic bisimulation tractable in practice.

On the contrary, [4] defines an approximate bisimulation for probabilistic processes with logic-based and game-theoretic characterizations, a poly-time verification algorithm, but strong usability limitations with respect to its aggregation power. Moreover, [5] introduces a relation approximating bisimulation in a framework in which the distance between processes is measured in terms of the norm of a linear operator applied to a matrix representation of the processes with respect to a classification operator based on the approximating relation. The computation of this relation is efficient, but the measure strictly depends on the chosen norms and classification linear operators, with an impact on the interpretation of the measure that is not completely intuitive.

In general, the main difficulties behind a practical definition of approximate bisimulation concern the tradeoff between efficiency of the verification algorithms and interpretation of the obtained measures in terms of, e.g., influence of the degree of similarity on the observable differences between the quantitative profiles of the models under comparison.

2 Approximate Testing Equivalence

With the aim of overcoming the limitations mentioned above, we propose an approach based on an approximate relation in the setting of testing semantics for a Markovian process calculus. The reason for this choice is that testing equivalence provides in a natural and explicit way an ideal framework for the definition of the degree of similarity with respect to three orthogonal aspects: time, probability, and observed behavior. To give some intuitive insights, testing equivalence for Markovian processes is based on the comparison of the probabilities of observing successful test-driven computations (i.e. they somehow "pass" tests) that satisfy temporal constraints about the amount of time needed to pass these tests. Therefore, by relaxing in turn each of these parameters – durations associated with specific computations, probability distributions of these computations, and kind of tests elucidating them – we easily obtain different notions of approximate testing equivalence under the three considered dimensions.

Formally, we first observe that the temporal behavior of a test-driven computation is described in terms of average sojourn times in the states traversed by the computation. Hence, relaxing time in this setting amounts to matching computations with stepwise average durations that are similar up to a threshold ϵ.

Second, the probabilistic behavior of a test-driven computation is defined by the product of the execution probabilities of the transitions of the computation. The relaxation of this aspect consists of checking whether the difference between the probabilities of corresponding computations is confined by a threshold ν.

Third, the observed behavior of a test-driven computation is explicitly specified by the test that guides the system execution. The family of tests with respect to which the analysis is conducted represents the observations that parameterize the comparison between processes. For instance, a family of tests may be formally characterized in terms of a modal logic formula ϕ that must be satisfied by each test. Introducing approximation at this level consists of matching computations that pass different but similar tests in a given family. The notion of similarity for tests is inspired by [2] and is based on two fitness functions, called precision and recall, that take into account all enabled transitions at any point in each test.

The unification of these approaches to the approximation problem results in a unique definition, checkable in poly-time, which is formalized as follows.

Definition. Let P_1, P_2 be two process terms and $\mathbb{T}_\phi$ a finite set of canonical tests parameterized by a modal logic formula ϕ. We say that P_2 is Markovian testing similar to P_1 with precision $p \in [0,1]$, recall $r \in [0,1]$, temporal threshold $\epsilon \in \mathbb{R}_{\geq 0}$, and probability threshold $\nu \in \mathbb{R}_{\geq 0}$ iff for each test $T \in \mathbb{T}_\phi$ there exists a test $T' \in \mathbb{T}_\phi$ such that for all sequences $\theta \in (\mathbb{R}_{>0})^*$ of average amounts of time:

1. $precision(T, T') \geq p$ and $recall(T, T') \geq r$
2. $|prob(\mathcal{SC}^{|\theta|}_{\leq\theta\pm\epsilon,\mathcal{SC}^{|\theta|}(P_2,T')}(P_1,T)) - prob(\mathcal{SC}^{|\theta|}_{\leq\theta\pm\epsilon,\mathcal{SC}^{|\theta|}(P_1,T)}(P_2,T'))| \leq \nu.$

References

[1] A. Aldini and A. Di Pierro, *Estimating the Maximum Information Leakage*, Journal of Information Security 7:219–242, 2008.

[2] A.K.A. de Medeiros, W.M.P. van der Aalst, and A.J.M.M. Weijters, *Quantifying Process Equivalence Based on Observed Behavior*, Data & Knowledge Engineering 64:55–74, 2008.

[3] J. Desharnais, V. Gupta, R. Jagadeesan, and P. Panangaden, *Metrics for Labelled Markov Processes*, Theoretical Comp. Sci. 318:323–354, 2004.

[4] J. Desharnais, F. Laviolette, and M. Tracol, *Approximate Analysis of Probabilistic Processes: Logic, Simulation and Games*, Int. Conf. on Quantitative Evaluation of Systems (QEST'08), IEEE-CS, pp. 264–273, 2008.

[5] A. Di Pierro, C. Hankin, and H. Wiklicky, *Quantifying Timing Leaks and Cost Optimisation*, Conf. on Information and Comm. Security (ICICS'08), Springer LNCS 5308:81–96, 2008.

[6] F. van Breugel and J. Worrell, *A Behavioural Pseudometric for Probabilistic Transition Systems*, Theoretical Comp. Sci. 331:115–142, 2005.