A Note on the Approximation of Weak Probabilistic Bisimulation

Alessandro Aldini

Università di Urbino "Carlo Bo", Istituto STI, Italy

Abstract

The need for flexible and formal approaches to the comparison of different process models is motivated in several application domains and with respect to different system properties. They can be helpful to compare a web service with some desired qualitative/quantitative service description, to relate an implemented software architecture to a reference dependable architectural model, and to reveal the performability impact of one component over the whole system through the comparison of the two system views that are obtained by activating/deactivating the component (this is generally called noninterference analysis). As a further step towards the flexibility of equivalence checking based techniques, we advocate an approach that relies on an approximate notion of weak probabilistic bisimulation, through which to provide a measure of the approximation and diagnostic information supporting exact methods such as numerical analysis and state space minimization.

Comparing different process models is a frequently used approach to the analysis of system requirements in practical application domains. In order to bridge the gap between rigid equivalence checking techniques and more relaxed distinguishability oriented requirements of real systems, in the last decade much attention has been paid on approximation methods [5,9,4,7,10,2]. This can be done in a quantitative framework where fine-grain models describe, e.g., probability distributions of events or their timed behaviors. For instance, some of the proposals cited above deal with probabilistic notions of behavioral equivalence for deciding if two process models behave almost (up to small fluctuations) the same or, more formally, for measuring the distance between probabilistic transition systems. Based on this idea, one well-established approach uses pseudometrics, which give a measure of the similarity of systems that are not equivalent (see e.g. [7,9]). An alternative approach has been addressed in [10] in the framework of security analysis and of purely generative probabilistic systems. There, the quantifiable amount of distinguishability between process models is defined via a notion of approximate confinement, corresponding to a statistical measure of the power of the observer.

These approaches efficiently provide a measure of the distance between process models. However, they lack to define an approximation of the equivalence relation that, ideally, should relate the two systems to compare. In fact, as the purely functional approach relies on searching an equivalence relation between these two systems, it would be natural, when passing to the quantitative setting, to define an approximating relation, which may differ from the equivalence relation and, in a case such as this, provide a measure of this difference. Then, such a relation could be profitably used, e.g., for state space minimization, similarly as done in the setting of equivalence checking.

We face this problem in the setting of weak probabilistic bisimulation for generative labeled multi-transition systems. First, weak bisimulation semantics is sufficiently expressive to be sensitive to deadlock and properties that depend on the branching structure of the models, and to abstract from unnecessary details and internal behaviors, as required when comparing process models at different abstraction levels (like e.g. a design specification and an implementation model). Second, minimization modulo bisimulation is useful in a setting where the underlying semantic model is a Discrete Time Markov Chain (DTMC). In this case, (weak) bisimulation coincides with the notion of (τ-) lumping [8,13]. Similarly as the bisimulation for labeled transition systems, the characterization of lumpability is extremely useful, because the knowledge of a lumpable partition of the states of the DTMC allows the generation of an aggregated DTMC that is smaller than the original one, but leads to several results for the original DTMC without any error. In this setting, approximation techniques have been proposed based on relaxed notions of lumping. In particular, lumpability can be extended to nearly- (or quasi-) lumpability, which is a natural way to relax the exact notion of lumpability in order to allow small differences for the elements of the same partition group [8,11]. In essence, a tolerable threshold ε corresponds directly to the maximum difference among elements of the same partition group. Then, in a way inspired by the perturbation theory, such a threshold is used to determine bounds on the error made when calculating results for the original DTMC from the aggregated, approximate one [15,3].

Our idea is to relax the notion of bisimulation in a similar way, in order to minimize the state space (up to a threshold ε) at the level of the labeled transition system, and then pass to the underlying DTMC level with a clear understanding of the impact of ε on the results calculated on the Markov chain. Without the explicit definition of an approximating relation, as in the case e.g. of the pseudometrics mentioned above, it would not be straightforward to recast the lumpability-based approach. Formally, we consider finite-state finitely-branching Probabilistic multi-Transition Systems (PTSs).

Definition 0.1 A PTS is a tuple (S, Act, T, s_0), where S is a finite set of states, $s_0 \in S$ is the initial state, Act is a non-empty finite set of actions, and $T \subseteq S \times Act \times]0,1] \times S$ is a finite transition relation such that $\forall s \in S$ it holds that $\sum\{\!|\, p \,|\, \exists a \in Act, t \in S.\, (s,a,p,t) \in T \,|\!\} \in \{0,1\}$.

The execution probabilities are governed by the generative model of probabilities [12]: the system autonomously decides, on the basis of a probability distribution, which action to perform. For the comparison between PTSs, we consider a probabilistic variant of the weak bisimulation, which replaces the classical weak transitions of the Milner's weak bisimulation by the probability $Prob(s, \tau^* a, C)$ of reaching classes of equivalent states through weak transitions, see e.g. [1,6] for details.

Definition 0.2 An equivalence relation $R \subseteq S \times S$ is a weak probabilistic bisimulation if and only if, whenever $(s, s') \in R$, then for all C in the quotient set $S_{/R}$ and $\forall a \in Act$: $Prob(s, \tau^* a, C) = Prob(s', \tau^* a, C)$. The union of all the weak probabilistic bisimulations is the largest weak probabilistic bisimulation, called weak probabilistic bisimilarity and denoted by $\approx_{\rm PB}$.

Weak probabilistic bisimilarity is therefore useful to relate different systems that are expected to behave the same, like e.g. in the case of a formal model and its real implementation. Aggregating states that behave the same on the basis of $\approx_{\rm PB}$ is a commonly used approach to the minimization of the state space of large systems where unnecessary details are abstracted. However, when two PTSs behave almost the same but not exactly the same, the outcome of the comparison based on $\approx_{\rm PB}$ is negative. Since $\approx_{\rm PB}$ is too precise, we relax it by means of an approximating relation R that allows states with slightly different weak transition probabilities to belong to the same class. A pair $(s, s') \in R$ of states that do not satisfy the condition of Def. 0.2 would effectively express a tolerance to differences which make the relation between them via $\approx_{\rm PB}$ impossible. The easiest approach to a relaxation such as this consists in replacing the equality condition of Def. 0.2 with a disequality "up to ε" between the weak transition probabilities. The threshold ε represents an upper bound to the tolerable distance between quasi-bisimilar states that are related by R. However, in such a way we would obtain a restrictive, local estimate of the distance between s and s' that does not take into account the probability of being in s and in s'. As an example, consider the case in which s and s' are the initial states of the two PTSs under comparison. Therefore, their distance should somehow receive more attention with respect to the case in which these states are instead reachable with negligible probabilities. Similar intuitions are employed in system theories with discounting and, in particular, in the reward-based specification of instant-of-time performance measures for DTMCs. In the case of steady-state analysis, e.g., the reward associated with a state is multiplied by the probability of being in that state on the long run. Here, we use function $Reach : S \to [0, 1]$, such that $Reach(s) = 1$ if s is the initial state s_0 and, otherwise, $Reach(s)$ represents the aggregate probability of reaching s from s_0 via states different from s itself.

Definition 0.3 The weighted distance between two states s and s' with respect to $a \in Act$ and a set of states C is defined as:

$$d(s, s', a, C) = Reach(s) \cdot Reach(s') \cdot \mid Prob(s, \tau^* a, C) - Prob(s', \tau^* a, C) \mid$$

Then, the definition of $\approx_{\mathrm{PB}}$ is relaxed on the basis of this notion of weighted distance that provides a global estimate of the difference between states s and s' belonging to the same partition group.

Definition 0.4 A relation $R \subseteq S \times S$ is a weak probabilistic bisimulation with ε precision if and only if, whenever $(s, s') \in R$, then for all C in the partition induced by R and $\forall a \in Act$: $d(s, s', a, C) \leq \varepsilon$.

Such a notion is conservative with respect to $\approx_{\mathrm{PB}}$: two states that are indistinguishable according to $\approx_{\mathrm{PB}}$ have distance equal to zero with respect to every action and set of the partition induced by $\approx_{\mathrm{PB}}$. Given a relation R, the estimate of the minimum ε such that R is a weak probabilistic bisimulation with ε precision is expressed by the pair of states in R that maximally differ.

Definition 0.5 Given $R \subseteq S \times S$ and P_R the partition induced by R, the closeness of R with respect to $\approx_{\mathrm{PB}}$ is defined as:

$$\varepsilon_R = \max\{d(s, s', a, C) \mid (s, s') \in R, a \in Act, C \in P_R\}$$

Among all the possible relations, the most interesting one is given by the closest approximation of $\approx_{\mathrm{PB}}$, which corresponds to $\min_{R \in \mathcal{R}} \varepsilon_R$, where $\mathcal{R}$ is the set of relations including the pair (s_0, s'_0) of initial states.

In this presentation we will consider two main aspects. First, it is interesting to relate the proposed approach to the pseudometrics analogue of $\approx_{\mathrm{PB}}$ [9]. Second, it is worth noting that the estimation of the similarity between PTSs depends on the definition of an adequate approximating relation. We will discuss an algorithm that calculates, with time complexity $\mathcal{O}(n^5)$ with respect to the number n of states, a good candidate relation R together with the estimation ε_R of the closeness to $\approx_{\mathrm{PB}}$. For this purpose, we point out that computing the approximate weak bisimulation through the Paige and Tarjan partition refinement algorithm [14], whose complexity in the case of generative probabilistic systems is $O(n^3)$ [6], is not straightforward. The intuition is that the approximate bisimulation cannot be a transitive relation: if the distance $d(s_1, s_2)$ between states s_1 and s_2 is equal to ε and the same holds for s_2 and s_3, then we do not have any apparent (and based on local information) principle to prefer the splitting $(s_1, s_2), (s_3)$ with respect to the splitting $(s_1), (s_2, s_3)$. On the other hand, transitivity is one of the basic principles underlying the Paige and Tarjan algorithm, which characterizes the equivalence relation as a fixed point of successively finer relations, starting from the initial partition with a single group including all the states. By following an opposite strategy, R is constructed starting from a symmetric relation including the identity and the pair of initial states, because they must be related by the approximate weak probabilistic bisimulation. Then, we will show how to perform, for each pair of states related by R, the aggregations of groups that allow the distance between the systems with respect to these states to be minimized. Finally, we will highlight how meta-heuristic techniques can be successfully applied to guarantee the convergence towards the closest approximation of $\approx_{\mathrm{PB}}$.

References

[1] A. Aldini, M. Bravetti, R. Gorrieri. *"A Process-algebraic Approach for the Analysis of Probabilistic Noninterference"*, J. of Comp. Sec. **12**:191–245, 2004.

[2] A. Aldini, A. Di Pierro. *"Estimating the Maximum Information Leakage"*, J. of Information Security 7(3):219–242, 2008.

[3] E. Altman, K. E. Avrachenkov, R. Nunez-Queija. *"Perturbation Analysis for Denumerable Markov Chains With Application to Queueing Models"*, Adv. in Applied Probability 36(3):839–853, 2004.

[4] M. Backes. *"Quantifying Probabilistic Information Flow in Computational Reactive Systems"*, Eur. Symp. on Research in Computer Security, LNCS 3679:336–354, 2005.

[5] C. Baier, J.-P. Katoen, H. Hermanns. *"Approximate Symbolic Model Checking of Continuous Time Markov Chains"*, Conf. on Concurrency Theory LNCS 1664:146–162, 1999.

[6] C. Baier, H. Hermanns. *"Weak Bisimulation for Fully Probabilistic Processes"*, Conf. on Computer Aided Verification, LNCS 1254:119–130, 1997.

[7] F. van Breugel, C. Hermida, M. Makkai, J. Worrell. *"An Accessible Approach to Behavioural Pseudometrics"*, Colloquium on Automata, Languages, and Programming, LNCS 3580:1018–1030, 2005.

[8] P. Buchholz. *"Exact and Ordinary Lumpability in Finite Markov Chains"*, J. of Applied Probability 31:59–75, 1994.

[9] J. Desharnais, V. Gupta, R. Jagadeesan, P. Panangaden. *"The Metric Analogue of Weak Bisimulation for Probabilistic Processes"*, Symp. on Logic in Computer Science, pp. 413–422, 2002.

[10] A. Di Pierro, C. Hankin, H. Wiklicky. *"Measuring the Confinement of Probabilistic Systems"*, Theoretical Computer Science 340(1):3–56, 2005.

[11] G. Franceschinis, R. Muntz. *"Bounds for Quasi-Lumpable Markov Chains"*, Performance Evaluation 20(1-3):223–243, 1994.

[12] R.J. van Glabbeek, S.A. Smolka, B. Steffen. *"Reactive, Generative and Stratified Models of Probabilistic Processes"*, Inf. and Comp. 121:59-80, 1995.

[13] J. Markovski, N. Trcka. *"Lumping Markov Chains with Silent Steps"*, Conf. on Quantitative Evaluation of Systems, pp. 221–232, 2006.

[14] R. Paige, R.E. Tarjan. *"Three Partition Refinement Algorithms"*, SIAM J. on Computing 16(6):973–989, 1987.

[15] G. W. Stewart. *"On the Perturbation of Markov Chains With Nearly Transient States"*, Numer. Math. 65(1):135–141, 1993.