Abstract Semantics by Observable Contexts

Filippo Bonchi

Dipartimento di Informatica, Università di Pisa
fibonchi@di.unipi.it

The operational behavior of interactive systems is usually given in terms of transition systems labeled with actions, which, when visible, represent both observations and interactions with the external world. The abstract semantics is given in terms of behavioral equivalences, which depend on the action labels and on the amount of branching structure considered. Behavioural equivalences are often congruences with respect to the operations of the language, and this property expresses the compositionality of the abstract semantics.

A simpler approach, inspired by classical formalisms like λ-calculus, Petri nets, term and graph rewriting, and pioneered by the Chemical Abstract Machine [1], defines operational semantics by means of *structural axioms* and *reaction rules*. Process calculi representing complex systems, in particular those able to generate and communicate names, are often defined in this way, since structural axioms give a clear idea of the intended structure of the states while reaction rules, which are often non-conditional, give a direct account of the possible steps. Transitions caused by reaction rules, however, are not labeled, since they represent evolutions of the system without interactions with the external world. Thus reduction semantics in itself is neither abstract nor compositional.

One standard solution, pioneered in [2], is that of defining a *saturated transition system* as follows:

a process p can do a move with label $C[-]$ and become p' iff $C[p] \rightsquigarrow p'$.

Saturated semantics, i.e., the abstract semantics defined over the saturated transition system, are always congruences, but they are usually untractable since they have to tackle all possible contexts of which there are usually an infinite number. Moreover, in several paradigmatic cases, saturated semantics are too coarse. For example, in Milner's Calculus of Communicating Systems (CCS, [3]), saturated bisimilarity cannot distinguish "always divergent processes" and for this reason Milner and Sangiorgi introduced *barbs* [4]. These are observations on the states representing the ability to interact over some channels.

In [5], Sewell introduced a different approach that consists in deriving a transition system where labels are not all contexts but just the minimal ones allowing a system to reach a rule. In such a way, one obtains two advantages: firstly one avoids considering all contexts, and secondly, labels precisely represent *interactions*, i.e., the portion of environment that is really needed to react. This idea was then refined by Leifer and Milner in the *theory of reactive systems* [6], where the categorical notion of *idem relative pushout* precisely captures this idea of minimal context.

The main theorem of this theory guarantees that if relative pushouts (RPOs) exist in the category representing the syntax of the formalism, then the abstract

H. Ehrig et al. (Eds.): ICGT 2008, LNCS 5214, pp. 478–480, 2008.

semantics defined over such a derived LTS are congruences with respect to the operators of the language. Since Lawvere-like categories usually do not have RPOs, Milner introduced *bigraphs* [7] with the aim of enconding process calculi whose operational behaviour is expressed by reaction rules and then derive a labeled transition semantics for them.

In this thesis, we try to use *borrowed contexts* rewriting [8] and some encodings of process calculi into graphs. In this perspective, spans of graphs represent reaction rules, double pushout rewrites mimic reduction of processes (represented as graphs) and borrowed contexts rewrites mimic labeled transitions of processes where, again, the labels represents the minimal contexts that is needed to perform a reaction. In [9], we have shown that in the case of CCS, this approach works well, i.e., the derived LTS is very close to the standard one, and the resulting bisimilarity coincides with the standard bisimilarity. Moreover, this approach has some interesting advantages with respect to bigraphs that we cannot detail in this abstract. However for several other interesting formalism the abstract semantics resulting from such approach are too strict. This is not due to our graphical encodings or to the borrowed contexts technique, but it is a bug of the general idea of considering the minimal contexts as labels.

In our opinion, considering as labels the minimal contexts that allow a certain reduction, allows the observer to observes too much, and thus the resulting semantics are usually too fine. One result of the thesis (presented in [10]) is that of providing evidence of this through several interesting formalisms modeled as reactive systems (without using borrowed contexts): Logic Programming, a fragment of open π-calculus, and an interactive version of Petri nets.

Moreover, we introduce two alternative definitions of bisimilarity that *efficiently* characterize saturated bisimilarity, namely *semi-saturated bisimilarity* and *symbolic bisimilarity* [10]. These allow us to reason about saturated semantics without considering all contexts, but saturated semantics are in several cases too coarse. In order to have a framework that is suitable for many formalisms, we add to the above approach *observations*. Indeed, in our opinion, labels cannot represent both interactions and observations, because these two concepts are in general different, like for example, in the asynchronous calculi where receiving is not observable. Thus, we believe that some notion of observation, either on transitions or on states (e.g. barbs [4]), is necessary.

A further result of the thesis (presented in [11]) is that of providing a generalization of the above theory starting not just from purely reaction rules, but from transition systems labeled with observations. Here we can easily reuse saturated transition systems by defining them as follows:

$$\text{a process } p \text{ can do a move with context } C[-] \text{ and observation } o \text{ and become } p' \\ \text{iff } C[p] \xrightarrow{o} p'.$$

Again, saturated semantics, i.e. abstract semantics defined over the above transition systems, are congruences. Analogously to the case of reactive systems, we can define semi-saturated bisimilarity and symbolic bisimilarity as efficient characterizations of saturated semantics. The definition of symbolic bisimilarity which arises from this generalization is similar to the abstract semantics

of several works [12,13,14,15]. Here (and in [11]) we consider open [14] and asynchronous [12,16] π-calculus, by showing that their abstract semantics are instances of our general concepts of saturated and symbolic semantics. We also apply our approach to open Petri nets [17] (that are an interactive version of P/T Petri nets) obtaining a new symbolic semantics for them, that efficiently characterizes their abstract semantics.

References

1. Berry, G., Boudol, G.: The chemical abstract machine. Theoretical Computer Science 96, 217–248 (1992)
2. Montanari, U., Sassone, V.: Dynamic congruence vs. progressing bisimulation for ccs. Fundamenta Informaticae 16(1), 171–199 (1992)
3. Milner, R.: Communication and Concurrency. Prentice-Hall, Englewood Cliffs (1989)
4. Milner, R., Sangiorgi, D.: Barbed bisimulation. In: Kuich, W. (ed.) ICALP 1992. LNCS, vol. 623, pp. 685–695. Springer, Heidelberg (1992)
5. Sewell, P.: From rewrite to bisimulation congruences. In: Sangiorgi, D., de Simone, R. (eds.) CONCUR 1998. LNCS, vol. 1466, pp. 269–284. Springer, Heidelberg (1998)
6. Leifer, J.J., Milner, R.: Deriving bisimulation congruences for reactive systems. In: Palamidessi, C. (ed.) CONCUR 2000. LNCS, vol. 1877, pp. 243–258. Springer, Heidelberg (2000)
7. Milner, R.: Bigraphical reactive systems. In: Larsen, K.G., Nielsen, M. (eds.) CONCUR 2001. LNCS, vol. 2154, pp. 16–35. Springer, Heidelberg (2001)
8. Ehrig, H., König, B.: Deriving bisimulation congruences in the DPO approach to graph rewriting. In: Walukiewicz, I. (ed.) FOSSACS 2004. LNCS, vol. 2987, pp. 151–166. Springer, Heidelberg (2004)
9. Bonchi, F., Gadducci, F., König, B.: Process bisimulation via a graphical encoding. In: Corradini, A., Ehrig, H., Montanari, U., Ribeiro, L., Rozenberg, G. (eds.) ICGT 2006. LNCS, vol. 4178, pp. 168–183. Springer, Heidelberg (2006)
10. Bonchi, F., König, B., Montanari, U.: Saturated semantics for reactive systems. In: Logic in Computer Science, pp. 69–80. IEEE, Los Alamitos (2006)
11. Bonchi, F., Montanari, U.: Symbolic semantics revisited. In: Amadio, R. (ed.) FOSSACS 2008. LNCS, vol. 4962, pp. 395–412. Springer, Heidelberg (2008)
12. Amadio, R.M., Castellani, I., Sangiorgi, D.: On bisimulations for the asynchronous pi-calculus. In: Sassone, V., Montanari, U. (eds.) CONCUR 1996. LNCS, vol. 1119, pp. 147–162. Springer, Heidelberg (1996)
13. Buscemi, M., Montanari, U.: Cc-pi: A constraint-based language for specifying service level agreements. In: De Nicola, R. (ed.) ESOP 2007. LNCS, vol. 4421, pp. 18–32. Springer, Heidelberg (2007)
14. Sangiorgi, D.: A theory of bisimulation for the pi-calculus. Acta Informatica 33(1), 69–97 (1996)
15. Wischik, L., Gardner, P.: Explicit fusions. Theoretical Computer Science 340(3), 606–630 (2005)
16. Honda, K., Tokoro, M.: An object calculus for asynchronous communication. In: America, P. (ed.) ECOOP 1991. LNCS, vol. 512, pp. 133–147. Springer, Heidelberg (1991)
17. Baldan, P., Corradini, A., Ehrig, H., Heckel, R.: Compositional semantics for open petri nets based on deterministic processes. Mathematical Structures in Computer Science 15(1), 1–35 (2005)