Weakly Extended Process Rewrite Systems

Vojtěch Řehák*

Masaryk University, Czech Republic, rehak@fi.muni.cz

Supervisor: Mojmír Křetínský, Masaryk University, Czech Republic
Keywords: Models of infinite state systems, process rewrite systems

Abstract. Our work is focused on properties of Process Rewrite Systems (PRS). Namely, we introduce an extension of PRS, so called *weakly extended Process Rewrite Systems* (wPRS). We compare the expressiveness of wPRS with original PRS classes and their known extensions. In addition, for wPRS classes, we study decidability and complexity of problems related to model checking and other formal verification procedures such as weak and strong bisimulation, the reachability problem, etc. The aim of our work is to extend expressive power of known modelling facilities while preserving decidability and maintaining complexity of problems in reasonable bounds.

1 Research Area

Automatic verification of current software systems often needs to model them as infinite-state systems, i.e. systems with an evolving structure (e.g. unbounded control structures such as recursive procedure calls and/or dynamic creation of concurrent processes) and/or operating on unbounded data types, e.g., a network of mobile phones is a concurrent system with evolving structure which dynamically changes its size (and can become very large). Robustness of the network requires that underlying protocols should work for an arbitrarily large (i.e. potentially infinite) number of client processes. A JAVA applet dynamically downloads classes over the network and executes their methods, the stack of activation records should be seen as potentially infinite.

Infinite-state systems can be specified in a number of ways with their respective advantages and limitations. Petri nets, pushdown automata, and process algebras like BPA, BPP, or PA all serve to exemplify this. However a unifying view is to interpret them as labelled transition systems (LTS) with possibly infinite number of states. LTS families are often specified via a variety of rewrite systems and form hierarchies (w.r.t. strong bisimulation equivalence), see for example [Cau92,BCS96,Mol96,May00]. Here we employ the classes of infinite-state systems defined by term rewrite systems and called *Process Rewrite Systems* (PRS) as introduced by Mayr [May00]. PRS subsume a variety of the formalisms studied in the context of formal verification (e.g. all the models mentioned above).

* The author has been partially supported by the Academy of Sciences of the Czech Republic, grant No. 1ET408050503.

A PRS is a finite set of rules $t \xrightarrow{a} t'$ where a is an action under which a subterm t can be reduced to a subterm t'. Terms are built up from an empty process ε and a set of process constants using (associative) sequential "." and (associative and commutative) parallel "||" operators. The semantics of PRS can be defined by labelled transition systems (LTS) – labelled directed graphs whose nodes (states of the system) correspond to terms modulo structural congruence by properties of "." and "||" and edges correspond to individual actions (computation steps) which can be performed in a given state. The relevance of various subclasses of PRS for modelling and analysing programs is shown e.g. in [Esp02], for automatic verification see e.g. surveys [BCMS01,Srb02,KJ02].

Mayr [May00] has shown that the reachability problem (i.e. given terms t, t': is t reducible to t'?) for PRS is decidable. In a context of reachability analysis one can see at least two approaches: (i) abstraction (approximate) analysis techniques on stronger 'models' such as sePA and its superclasses with undecidable reachability problem, e.g., see a recent work [BET03], and (ii) precise techniques for 'weaker' models, e.g., [LS98] and another recent work [BT03]. In the latter one, symbolic representations of a set of reachable states are built with respect to various term structural equivalences. Among others it is shown that for the PAD class and the same equivalence as in the setting presented here, when properties of sequential and parallel compositions are taken into account, one can construct non-regular representations based on counter tree automata.

Most research (with some recent exceptions, e.g. [BT03,Esp02]) has been devoted to the PRS classes from the lower part of the PRS hierarchy, especially to pushdown automata (PDA), Petri nets (PN) and their respective subclasses. We mention the successes of PDA in modelling recursive programs (without process creation), PN in modelling dynamic creation of concurrent processes (without recursive calls), and CPDS (communicating pushdown systems [BET03]) modelling both features. All of these formalisms subsume a notion of a finite-state control unit (FSU) keeping some kind of global information which is accessible to the redices (the ready to be reduced components) of a PRS term – hence an FSU can regulate rewriting. On the other hand, using an FSU to extend the PRS rewriting mechanism is very powerful since a state-extended version of PA processes (sePA) has full Turing-power [BEH95] – the decidability of reachability and other problems relevant for an automatic verification are lost for sePA, including all its superclasses (see Figure 1), and CPDS as well.

2 Directions of the work

Our work presents a hierarchy of PRS classes and their respective extensions of three types: PRS with finite constraint systems (fcPRS [Str02], motivated by concurrent constraint programming, see e.g. [SR90]), state-extended PRS classes [JKM01], and our new formalism of *weakly extended PRS* (wPRS, introduced in [KŘS04b]). In [KŘS04b], we have shown that all the just mentioned extensions increase the expressive power of those PRS subclasses which do not subsume the notion of a finite control. The classes in the hierarchy (depicted in Figure 1) are

related by their expressive power with respect to (strong) bisimulation equivalence.

The notion of a weak FSU within wPRS formalism is inspired by weak automata as introduced in [MSS92], but used here as a nondeterministic (NFA) rather than alternating one. A NFA $A = (Q, \Sigma, \delta, q_0, F)$ is *weak* if its state space is partitioned into a disjoint union $Q = \bigcup Q_i$, and there is a partial order $\geq$ on the collection of the Q_i. The set Σ is the input alphabet and the transition function $\delta : Q \times \Sigma \to \mathcal{P}(Q)$ is such that if $q \in Q_i$ and $q' \in \delta(q, a)$ then $q' \in Q_j$, where $Q_i \geq Q_j$ (this requirement on the transition structure is also known as an *acyclicity condition*). The set F of final states satisfies that $Q_i \subseteq F$ or $Q_i \cap F = \emptyset$ for each Q_i.

As we are not interested in language equivalence, the set of final states does not play any role in our application, hence all the states of a weak NFA could belong to one class and the formalism would coincide with an arbitrary NFA. Thus we have chosen to employ a 1-weak (also known as very weak) variant of the restriction where each partition block contains exactly one state. In other words, although a weak FSU can cycle in any of its control state, each wPRS rewriting sequence can only change its state a finitely many times.

Figure 1 describes the hierarchy of PRS classes and their extended counterparts with respect to strong bisimulation equivalence. The depicted hierarchy is then the upward oriented Hasse diagram of a partial order relation '$\subseteq$' between these sets of labelled transition systems modulo strong bisimulation equivalence. In other words, a line connecting X and Y with Y placed higher than X means that every transition system definable in X can be (up to bisimulation equivalence) defined in Y while the reverse does not hold – we write $X \subsetneq Y$. The dotted lines represent the facts $X \subseteq Y$, where the relation $X \subsetneq Y$ is only our conjecture.

The wPRS classes refine the presented hierarchy of extended PRS formalisms and so it motivates us to focus on borders of decidability and complexity of some interesting problems. By interesting problems we mean reachability, strong and weak bisimulation equivalence, model checking problems for linear or branching time logics, etc.

3 Results

Besides of the results on the classification of expressive power of extended PRS classes [KŘS04b,KŘS04a], we have shown that the *reachability problem* remains decidable for the very expressive class of wPRS [KŘS04a]. Let us mention that Hüttel and Srba [HS05] define a replicative variant of a calculus for Dolev and Yao's ping-pong protocols [DY83]. They show that the reachability problem for these protocols is decidable as it can be reduced to the reachability problem for wPRS, more precisely their replicative ping-pong protocols belong to the wPAD class. Further, we mention another application of our decidability result exemplifying that the introduction of wPRS was well-motivated and contributes to the results on infinite-state systems. The decidability of the reachability for

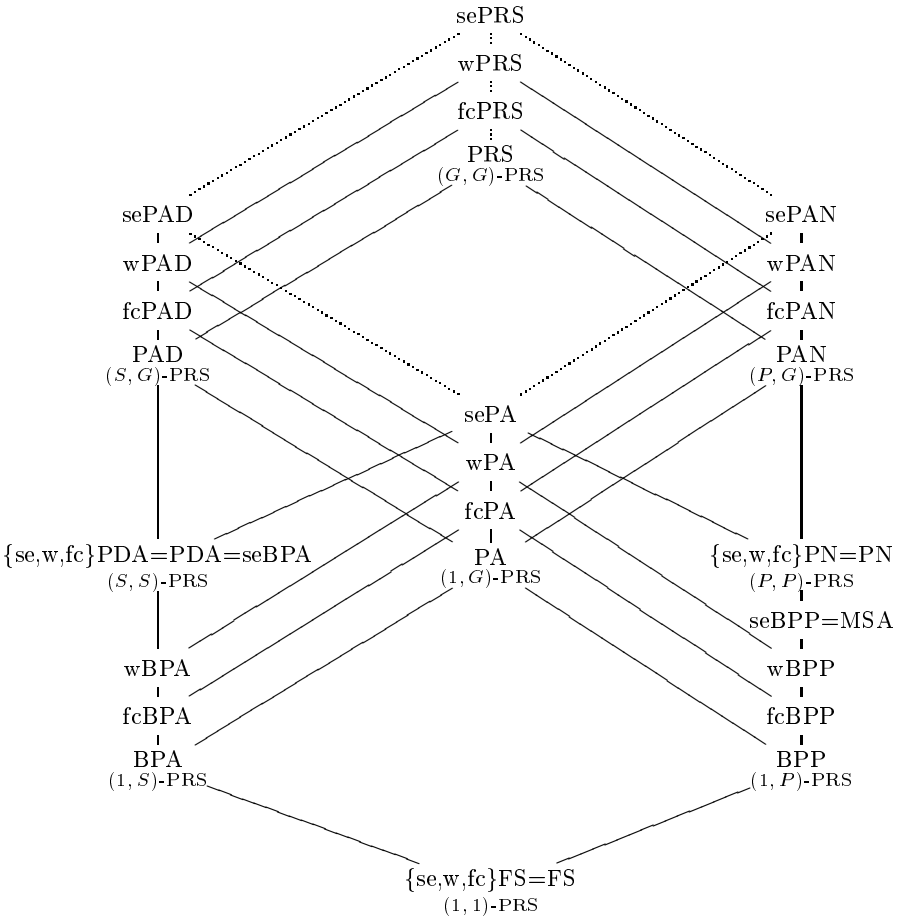

Fig. 1. The hierarchy of classes defined by extended process rewrite systems with respect to the strong bisimulation equivalence.

wPRS opens an easy way how to solve an open problem of a weak trace non-equivalence (for definition see, e.g. [JEM99]) for wPRS and its subclasses.

A *reachability property problem*, for a given system Δ and a given formula φ, is to decide whether $\mathsf{EF}\varphi$ holds in the initial state of Δ. Hence, these problems are parametrized by the class to which the system Δ belongs, and by the type of the formula φ. In most of practical situations, φ specifies error states and the reachability property problem is a formalization of a natural verification problem whether some error state is reachable in a given system.

We recall that the (full) EF logic is decidable for PAD [May98] (PAD subsumes both PA and PDA). It is undecidable for PN [Esp94]; an inspection of the proof moves this undecidability border down to seBPP (also known as *multiset*

automata, MSA). If we consider the *reachability HM property problem*, i.e., the reachability property problem where φ is a formula of Hennessy–Milner logic (HM formula), then this problem has been shown to be decidable for the classes of PN [JM95] and PAD [JKM01]. In [KŘS05], we lift the decidability border for this problem to the wPRS class. This results also move the decidability border for the *reachability simple property problem*, i.e., the reachability property problem where φ is a HM formula without any nesting of modal operators $\langle a \rangle$, as the problem has been known to be decidable only for PRS [May00] so far.

Let us recall that the (full) EG logic is decidable for PDA (a consequence of [MS85] and [Cau92]), whilst undecidability has been obtained for its $\mathsf{EG}\varphi$ fragment on (deterministic) BPP [EK95], where φ is a HM formula. In [KŘS05], we show that this problem remains undecidable for (deterministic) BPP even if we restrict φ to a HM formula without nesting of modal operators $\langle a \rangle$.

As a corollary of decidability of the reachability HM property problem for wPRS, we observe that the problem of strong bisimilarity between wPRS systems and finite-state ones is decidable. As PRS and its subclasses are proper subclasses of wPRS, it follows that we positively answer the question of the reachability HM property problem for the PRS class and hence the questions of bisimilarity checking the PAN and PRS processes with finite-state ones, which have been open problems, see for example [Srb02]. Their relevance to program specification and verification is advocated, for example, in [JKM01,KS04].

References

[BCMS01] O. Burkart, D. Caucal, F. Moller, and B. Steffen. Verification on infinite structures. In *Handbook of Process Algebra*, pages 545–623. Elsevier, 2001.

[BCS96] O. Burkart, D. Caucal, and B. Steffen. Bisimulation collapse and the process taxonomy. In *Proc. of CONCUR'96*, volume 1119 of *LNCS*, pages 247–262. Springer, 1996.

[BEH95] A. Bouajjani, R. Echahed, and P. Habermehl. On the verification problem of nonregular properties for nonregular processes. In *Proc. of LICS'95*. IEEE, 1995.

[BET03] A. Bouajjani, J. Esparza, and T. Touili. A generic approach to the static analysis of concurrent programs with procedures. *International Journal on Foundations of Computer Science*, 14(4):551–582, 2003.

[BT03] A. Bouajjani and T. Touili. Reachability Analysis of Process Rewrite Systems. In *Proc. of FSTTCS 2003*, volume 2914 of *LNCS*, pages 74–87. Springer, 2003.

[Cau92] D. Caucal. On the regular structure of prefix rewriting. *Theor. Comput. Sci.*, 106:61–86, 1992.

[DY83] D. Dolev and A. Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.

[EK95] J. Esparza and A. Kiehn. On the model checking problem for branching time logics and basic parallel processes. In *CAV*, volume 939 of *LNCS*, pages 353–366. Springer, 1995.

[Esp94] J. Esparza. On the decidability of model checking for several mu-calculi and petri nets. In *CAAP*, volume 787 of *LNCS*, pages 115–129. Springer, 1994.

[Esp02] J. Esparza. Grammars as processes. In *Formal and Natural Computing*, volume 2300 of *LNCS*. Springer, 2002.

[HS05] H. Hüttel and J. Srba. Recursion vs. replication in simple cryptographic protocols. In *Proceedings of SOFSEM 2005: Theory and Practice of Computer Science*, volume 3381 of *LNCS*, pages 178–187. Springer, 2005.

[JEM99] P. Jančar, J. Esparza, and F. Moller. Petri nets and regular behaviours. *Journal of Computer and System Sciences*, 59(3):476–503, 1999.

[JKM01] P. Jančar, A. Kučera, and R. Mayr. Deciding bisimulation-like equivalences with finite-state processes. *Theor. Comput. Sci.*, 258:409–433, 2001.

[JM95] P. Jancar and F. Moller. Checking regular properties of petri nets. In *CONCUR*, volume 962 of *LNCS*, pages 348–362. Springer, 1995.

[KJ02] A. Kučera and P. Jančar. Equivalence-checking with infinite-state systems: Techniques and results. In *Proc. SOFSEM'2002*, volume 2540 of *LNCS*. Springer, 2002.

[KŘS04a] M. Křetínský, V. Řehák, and J. Strejček. Extended process rewrite systems: Expressiveness and reachability. In *Proceedings of CONCUR'04*, volume 3170 of *LNCS*, pages 355–370. Springer, 2004.

[KŘS04b] M. Křetínský, V. Řehák, and J. Strejček. On extensions of process rewrite systems: Rewrite systems with weak finite-state unit. In *Proceedings of INFINITY'03*, volume 98 of *ENTCS*, pages 75–88. Elsevier, 2004.

[KŘS05] Mojmír Křetínský, Vojtěch Řehák, and Jan Strejček. Reachability of Hennessy-Milner properties for weakly extended PRS. In *Proceedings of FSTTCS 2005*, volume 3821 of *LNCS*, pages 213–224. Springer, 2005.

[KS04] A. Kučera and Ph. Schnoebelen. A general approach to comparing infinite-state systems with their finite-state specifications. In *CONCUR*, volume 3170 of *LNCS*, pages 371–386. Springer, 2004.

[LS98] D. Lugiez and Ph. Schnoebelen. The regular viewpoint on PA-processes. In *Proc. of CONCUR'98*, volume 1466 of *LNCS*, pages 50–66. Springer, 1998.

[May98] R. Mayr. *Decidability and Complexity of Model Checking Problems for Infinite-State Systems*. PhD thesis, Technische Universität München, 1998.

[May00] R. Mayr. Process rewrite systems. *Information and Computation*, 156(1):264–286, 2000.

[Mol96] F. Moller. Infinite results. In *Proc. of CONCUR'96*, volume 1119 of *LNCS*, pages 195–216. Springer, 1996.

[MS85] D. Muller and P. Schupp. The theory of ends, pushdown automata, and second-order logic. *Theor. Comput. Sci.*, 37:51–75, 1985.

[MSS92] D. Muller, A. Saoudi, and P. Schupp. Alternating automata, the weak monadic theory of trees and its complexity. *Theor. Comput. Sci.*, 97(1–2):233–244, 1992.

[SR90] V. A. Saraswat and M. Rinard. Concurrent constraint programming. In *Proc. of 17th POPL*, pages 232–245. ACM Press, 1990.

[Srb02] J. Srba. Roadmap of infinite results. *EATCS Bulletin*, (78):163–175, 2002. `http://www.brics.dk/~srba/roadmap/`.

[Str02] J. Strejček. Rewrite systems with constraints, in: Proc. of EXPRESS'01. *ENTCS*, 52 (2002), 2002.