Information and Computation 215 (2012) 68–87

Contents lists available at SciVerse ScienceDirect

Information and Computation

www.elsevier.com/locate/yinco

Multiset rewriting for the verification of depth-bounded processes with name binding ☆

Fernando Rosa-Velardo *, María Martos-Salgado *

Sistemas Informáticos y Computación, Universidad Complutense de Madrid, Facultad de Informática, C/Prof. José García Santesmases, s/n, 28040 Madrid, Spain

ARTICLE INFO

Article history:
Received 3 June 2011
Available online 13 April 2012

Keywords:
Multiset rewriting
Depth-boundedness
WSTS
Verification
Decidability
Petri nets
Process algebra

ABSTRACT

We combine two of the existing approaches to the study of concurrency by means of multiset rewriting: multiset rewriting with existential quantification (MSR) and constrained multiset rewriting. We obtain ν-MSR, where we rewrite multisets of atomic formulae, in which terms can only be pure names, where some names can be restricted. We consider the subclass of depth-bounded ν-MSR, for which the interdependence of names is bounded. We prove that they are strictly Well Structured Transition Systems, so that coverability, termination and boundedness are all decidable for depth-bounded ν-MSR. This allows us to obtain new verification results for several formalisms with name binding that can be encoded within ν-MSR, namely polyadic ν-PN (Petri nets with tuples of names as tokens), the π-calculus, MSR or Mobile Ambients.

1. Introduction

MSR. Dynamic name generation has been thoroughly studied in the last decade, mainly in the fields of security [1,2] and mobility [3]. The paper [1] presents a meta-notation for the specification and analysis of security protocols. This meta-notation involves facts and transitions, where facts are first-order atomic formulae and transitions are given by means of rewriting rules, with a precondition and a postcondition. For instance, the rule

$$A_0(k), Ann(k') \to \exists x.(A_1(k,x), N(enc(k', \langle x, k\rangle)), Ann(k'))$$

specifies the first rule of the Needham-Schroeder protocol, in which a principal A with key k ($A_0(k)$) decides to talk to another principal, with a key k' that has been announced ($Ann(k')$), for which it creates a nonce x and sends to the network the pair $\langle x, k\rangle$ ciphered under k'. This notation gave rise to the specification language for security protocols MSR [4].

CMRS. In [5] *Constraint Multiset Rewriting Systems* (CMRS) are defined. As in [1], facts are first-order atomic formulae, but the terms that can appear as part of such formulae must belong to a *constraint system*. For instance, the rule $count(x), visit \to count(x+1), enter(x+1)$ could be used to count the number of visits to a web site. For a comprehensive survey of CMRS see [6]. In CMRS, there is no mechanism for name binding or name creation, so that it has to be simulated using the order in the constraint system (for instance, simulating the creation of a fresh name by taking a value greater than any of the values that have appeared so far, or as in [7]). Thus, in an unordered version of CMRS, in which only the equality predicate between atoms is used, there is no way of ensuring that a name is fresh.

☆ Authors partially supported by the Spanish projects DESAFIOS10 TIN2009-14599-C03-01 and PROMETIDOS S2009/TIC-1465.
* Corresponding authors.
E-mail addresses: fernandorosa@sip.ucm.es (F. Rosa-Velardo), mrmartos@estumail.ucm.es (M. Martos-Salgado).

0890-5401/$ – see front matter
http://dx.doi.org/10.1016/j.ic.2012.03.004

Our goal. It is our goal in this paper to find a minimal set of primitives that allows us to specify concurrent formalisms with name binding. This specification may be achieved by means of some encoding, provided this encoding preserves concurrency and name topology. This will allow us to obtain new decidability results for those concurrent formalisms in a common framework.

We combine the features of the meta-notation MSR and CMRS, obtaining ν-MSR. On the one hand, we maintain the existential quantifications in [1] to keep a compositional approach, closer to that followed in process algebra with name binding. On the other hand, we restrict terms in atomic formulae to be pure names, that can only be compared with equality or inequality, unlike the arbitrary terms over some syntax, as in [1], or terms in a constraint system, as in CMRS.

Depth boundedness. In the field of process algebra, there are many recent works that look for subclasses of the π-calculus for which some properties, such as termination, are decidable [8–12]. In this paper we will consider the results in [10] about depth-bounded π-calculus processes.

Depth-boundedness is a semantic restriction on π-calculus processes. Intuitively, a process is depth-bounded whenever the interdependence of names is bounded in any process reachable from it. As a simple example, and assuming that the reader is familiar with the following π-calculus syntax, if starting from some process P the processes

$$\nu a_1.\cdots.a_n.\big(a_1\langle a_2\rangle \mid a_2\langle a_3\rangle \mid \cdots \mid a_i\langle a_{i+1}\rangle \mid \cdots \mid a_{n-1}\langle a_n\rangle\big) \mid Q_n$$

are reachable for every $n > 0$, then P is a depth-unbounded process. However, the fact that processes

$$\nu a.a_1.\cdots.a_n.\big(a\langle a_1\rangle \mid a\langle a_2\rangle \mid \cdots \mid a\langle a_i\rangle \mid \cdots \mid a\langle a_n\rangle\big) \mid Q_n$$

can be reached from P for every n does not allow us to conclude that P is depth-unbounded, since though an unbounded number of names can appear in reachable processes, those names do not depend one another, as happened in the previous example. Depth-bounded processes are enough to model systems with a dynamic topology in which only a bounded number of topologies appear at runtime, called structurally stationary in [9].

Meyer proved in [10] that depth-bounded π-calculus processes are Well Structured Transition Systems (WSTS), which essentially means that the transition relation is monotonic with respect an ordering that is a well-quasi order [13]. In this paper we adapt those results to ν-MSR. More precisely, we will consider depth-bounded ν-MSR, that is, ν-MSR for which the interdependence of bound names is bounded in every reachable term. We will prove that this subclass of ν-MSR is well structured by following the same steps followed in [10]. Unfortunately, we will see that this property itself is undecidable for ν-MSR, as it is for the π-calculus [14].

Then we will study the complexity of the decision procedures for depth-bounded ν-MSR, proving that they are all non-primitive recursive, thus rising the exponential space lower bound given in [10].

Models of concurrency with names. Two of the most well established models for concurrency are Petri nets and process algebra. The π-calculus is the paradigmatic example of process algebra with name binding. Names in the π-calculus can be used to build a dynamic communication topology. Two approaches to the dynamic generation of names in the field of Petri nets are ν-PNs [15] and Data Nets [16].

In ν-PNs, tokens are pure names that can move along the places of the net, be used to restrict the firing of transitions to happen only when some names match, and be created fresh. ν-PNs are (strictly) Well Structured Transition Systems (WSTS) [17,13], but $p\nu$-PNs, its polyadic version, in which tokens are *tuples* of pure names, are not. Actually, $p\nu$-PNs are Turing-complete [18], even in the binary case.

In Data Nets, tokens are taken from a linearly ordered and dense domain, and whole-place operations (like transfers or resets) are allowed. However, in Data Nets (which are also WSTS), fresh name creation has to be simulated using the linear order, as happens in CMRS. Actually, CMRS and Data Nets are equivalent up to coverability languages (with coverability as accepting condition), even if the former cannot perform whole-place operations [19].

Though ν-PN have better decidability properties than $p\nu$-PN, some works need to use the model of $p\nu$-PN to model features like instance isolation in architectures with multiple concurrent conversations [20] or transactions in data bases [21]. We will prove that ν-MSRs are equivalent to $p\nu$-PNs. We will see that this equivalence is a rather strong one (isomorphism between the transitions systems). Moreover, the subclass of monadic ν-MSRs is equivalent to ν-PNs, so that coverability, boundedness and termination are decidable for them.

Next, we will see that processes of the π-calculus can be simulated, in a very natural way, by ν-MSRs. This translation is inspired by the results by Meyer about *structural stationary* π-calculus processes, that can be mapped to P/T nets [9]. As a corollary, depth-bounded π-calculus processes are well structured, which was already known. Finally, we apply the same techniques to other formalisms, like MSR [1] and Mobile Ambients [22].

In [1], positive results are obtained for bounded theories, for which, in particular, the number of uses of each existential is bounded. In our setting we can extend this result with unboundedly many uses of each existential, provided their interdependence is bounded. In the case of Mobile Ambients (MA), we obtain in particular the decidability of the name convergence problem, which is undecidable in general, even for the subclass without name restriction and in which ambients cannot be opened [23].