IN PARTNERSHIP WITH:
CNRS

Ecole normale supérieure de Cachan

Activity Report 2016

Project-Team MEXICO

Modeling and Exploitation of Interaction and Concurrency

IN COLLABORATION WITH: Laboratoire specification et vérification (LSV)

RESEARCH CENTER
Saclay - Île-de-France

THEME
Proofs and Verification

Table of contents

Project-Team MEXICO

Creation of the Team: 2009 March 01, updated into Project-Team: 2011 January 01

Keywords:

Computer Science and Digital Science:

2.3. - Embedded and cyber-physical systems
2.4. - Verification, reliability, certification
4.5. - Formal methods for security
6.4.3. - Observability and Controlability
7.1. - Parallel and distributed algorithms
7.2. - Discrete mathematics, combinatorics
7.3. - Optimization
7.4. - Logic in Computer Science
7.9. - Graph theory
7.11. - Performance evaluation

Other Research Topics and Application Domains:

1.1.2. - Molecular biology
1.1.3. - Cellular biology
1.1.11. - Systems biology
1.1.12. - Synthetic biology
6.3.1. - Web
6.3.3. - Network Management
7.1. - Traffic management
7.2.1. - Smart vehicles

1. Members

Research Scientists

Stefan Haar [Team leader, Inria, Senior Researcher, HDR]
Benedikt Bollig [CNRS, Researcher]
Matthias Fuegger [CNRS, Researcher]

Faculty Members

Beatrice Berard [Univ. Paris VI, Professor, Inria *delegation* from Sep 2016]
Thomas Chatain [ENS Cachan, Associate Professor]
Paul Gastin [ENS Cachan, Professor, HDR]
Serge Haddad [ENS Cachan, Professor, HDR]
Claudine Picaronny [ENS Cachan, Associate Professor]
Stefan Schwoon [ENS Cachan, Associate Professor]

PhD Students

Yann Duplouy [Inst. de Recherche Technologique SystemX]
Engel Lefaucheux [ENS Cachan]
Marie Fortin [ENS Cachan, from Sep 2016]
Hugues Mandon [Inria, from Oct 2016]
Simon Theissing [Inria, until Aug 2016, granted by Institut de Recherche SystemX]

Administrative Assistant
Thida Iem [Inria]

Other
Clara Scherbaum [Inria, Internship student (ERASMUS) from Aachen University, Germany, from Mar 2016 until Jul 2016]

2. Overall Objectives

2.1. Scientific Objectives

2.1.1. Introduction

In the increasingly networked world, reliability of applications becomes ever more critical as the number of users of, e.g., communication systems, web services, transportation etc., grows steadily. Management of networked systems, in a very general sense of the term, therefore is a crucial task, but also a difficult one.

MExICo strives to take advantage of distribution by orchestrating cooperation between different agents that observe local subsystems, and interact in a localized fashion.

The need for applying formal methods in the analysis and management of complex systems has long been recognized. It is with much less unanimity that the scientific community embraces methods based on asynchronous and distributed models. Centralized and sequential modeling still prevails.

However, we observe that crucial applications have increasing numbers of users, that networks providing services grow fast both in the number of participants and the physical size and degree of spatial distribution. Moreover, traditional *isolated* and *proprietary* software products for local systems are no longer typical for emerging applications.

In contrast to traditional centralized and sequential machinery for which purely functional specifications are efficient, we have to account for applications being provided from diverse and non-coordinated sources. Their distribution (e.g. over the Web) must change the way we verify and manage them. In particular, one cannot ignore the impact of quantitative features such as delays or failure likelihoods on the functionalities of composite services in distributed systems.

We thus identify three main characteristics of complex distributed systems that constitute research challenges:

- *Concurrency* of behavior;
- *Interaction* of diverse and semi-transparent components; and
- management of *Quantitative* aspects of behavior.

2.1.2. Concurrency

The increasing size and the networked nature of communication systems, controls, distributed services, etc. confront us with an ever higher degree of parallelism between local processes. This field of application for our work includes telecommunication systems and composite web services. The challenge is to provide sound theoretical foundations and efficient algorithms for management of such systems, ranging from controller synthesis and fault diagnosis to integration and adaptation. While these tasks have received considerable attention in the *sequential* setting, managing *non-sequential* behavior requires profound modifications for existing approaches, and often the development of new approaches altogether. We see concurrency in distributed systems as an opportunity rather than a nuisance. Our goal is to *exploit* asynchronicity and distribution as an advantage. Clever use of adequate models, in particular *partial order semantics* (ranging from Mazurkiewicz traces to event structures to MSCs) actually helps in practice. In fact, the partial order vision allows us to make causal precedence relations explicit, and to perform diagnosis and test for the dependency between events. This is a conceptual advantage that interleaving-based approaches cannot match. The two key features of our work will be *(i)* the exploitation of concurrency by using asynchronous models with partial order semantics, and *(ii)* distribution of the agents performing management tasks.

2.1.3. Interaction

Systems and services exhibit non-trivial *interaction* between specialized and heterogeneous components. A coordinated interplay of several components is required; this is challenging since each of them has only a limited, partial view of the system's configuration. We refer to this problem as *distributed synthesis* or *distributed control*. An aggravating factor is that the structure of a component might be semi-transparent, which requires a form of *grey box management*.

2.1.4. Quantitative Features

Besides the logical functionalities of programs, the *quantitative* aspects of component behavior and interaction play an increasingly important role.

- *Real-time* properties cannot be neglected even if time is not an explicit functional issue, since transmission delays, parallelism, etc, can lead to time-outs striking, and thus change even the logical course of processes. Again, this phenomenon arises in telecommunications and web services, but also in transport systems.
- In the same contexts, *probabilities* need to be taken into account, for many diverse reasons such as unpredictable functionalities, or because the outcome of a computation may be governed by race conditions.
- Last but not least, constraints on *cost* cannot be ignored, be it in terms of money or any other limited resource, such as memory space or available CPU time.

2.1.5. Evolution and Perspectives

Since the creation of *MExICo*, the weight of *quantitative* aspects in all parts of our activities has grown, be it in terms of the models considered (weighted automata and logics), be it in transforming verification or diagnosis verdict into probabilistic statements (probabilistic diagnosis, statistical model checking), or within the recently started SystemX cooperation on supervision in multi-modal transport systems. This trend is certain to continue over the next couple of years, along with the growing importance of diagnosis and control issues.

In another development, the theory and use of partial order semantics has gained momentum in the past four years, and we intend to further strengthen our efforts and contacts in this domain to further develop and apply partial-order based deduction methods.

As concerns the study of interaction, our progress has been thus far less in the domain of *distributed* approaches than in the analysis of *system composition*, such as in networks of untimed or timed automata. While continuing this line of study, we also intend to turn more strongly towards distributed *algorithms*, namely in terms of parametrized verification methods.

3. Research Program

3.1. Concurrency

Participants: Benedikt Bollig, Thomas Chatain, Paul Gastin, Stefan Haar, Serge Haddad, Stefan Schwoon.

Concurrency; Semantics; Automatic Control ; Diagnosis ; Verification

Concurrency: Property of systems allowing some interacting processes to be executed in parallel.

Diagnosis: The process of deducing from a partial observation of a system aspects of the internal states or events of that system; in particular, *fault diagnosis* aims at determining whether or not some non-observable fault event has occurred.

Conformance Testing: Feeding dedicated input into an implemented system IS and deducing, from the resulting output of I, whether I respects a formal specification S.

3.1.1. Introduction

It is well known that, whatever the intended form of analysis or control, a *global* view of the system state leads to overwhelming numbers of states and transitions, thus slowing down algorithms that need to explore the state space. Worse yet, it often blurs the mechanics that are at work rather than exhibiting them. Conversely, respecting concurrency relations avoids exhaustive enumeration of interleavings. It allows us to focus on 'essential' properties of non-sequential processes, which are expressible with causal precedence relations. These precedence relations are usually called causal (partial) orders. Concurrency is the explicit absence of such a precedence between actions that do not have to wait for one another. Both causal orders and concurrency are in fact essential elements of a specification. This is especially true when the specification is constructed in a distributed and modular way. Making these ordering relations explicit requires to leave the framework of state/interleaving based semantics. Therefore, we need to develop new dedicated algorithms for tasks such as conformance testing, fault diagnosis, or control for distributed discrete systems. Existing solutions for these problems often rely on centralized sequential models which do not scale up well.

3.1.2. Diagnosis

Participants: Benedikt Bollig, Stefan Haar, Serge Haddad, Stefan Schwoon.

Fault Diagnosis for discrete event systems is a crucial task in automatic control. Our focus is on *event oriented* (as opposed to *state oriented*) model-based diagnosis, asking e.g. the following questions:
given a - potentially large - *alarm pattern* formed of observations,

- what are the possible *fault scenarios* in the system that *explain* the pattern ?
- Based on the observations, can we deduce whether or not a certain - invisible - fault has actually occurred ?

Model-based diagnosis starts from a discrete event model of the observed system - or rather, its relevant aspects, such as possible fault propagations, abstracting away other dimensions. From this model, an extraction or unfolding process, guided by the observation, produces recursively the explanation candidates.

In asynchronous partial-order based diagnosis with Petri nets [51], [52], [56], one unfolds the *labelled product* of a Petri net model $\mathcal{N}$ and an observed alarm pattern $\mathcal{A}$, also in Petri net form. We obtain an acyclic net giving partial order representation of the behaviors compatible with the alarm pattern. A recursive online procedure filters out those runs *(configurations)* that explain *exactly* $\mathcal{A}$. The Petri-net based approach generalizes to dynamically evolving topologies, in dynamical systems modeled by graph grammars, see [35]

3.1.2.1. Observability and Diagnosability

Diagnosis algorithms have to operate in contexts with low observability, i.e., in systems where many events are invisible to the supervisor. Checking *observability* and *diagnosability* for the supervised systems is therefore a crucial and non-trivial task in its own right. Analysis of the relational structure of occurrence nets allows us to check whether the system exhibits sufficient visibility to allow diagnosis. Developing efficient methods for both verification of *diagnosability checking* under concurrency, and the *diagnosis* itself for distributed, composite and asynchronous systems, is an important field for *MExICo*.

3.1.2.2. Distribution

Distributed computation of unfoldings allows one to factor the unfolding of the global system into smaller *local* unfoldings, by local supervisors associated with sub-networks and communicating among each other. In [52], [37], elements of a methodology for distributed computation of unfoldings between several supervisors, underwritten by algebraic properties of the category of Petri nets have been developed. Generalizations, in particular to Graph Grammars, are still do be done.

Computing diagnosis in a distributed way is only one aspect of a much vaster topic, that of *distributed diagnosis* (see [48], [60]). In fact, it involves a more abstract and often indirect reasoning to conclude whether or not some given invisible fault has occurred. Combination of local scenarios is in general not sufficient: the global system may have behaviors that do not reveal themselves as faulty (or, dually, non-faulty) on any local supervisor's domain (compare [34], [40]). Rather, the local diagnosers have to join all *information* that is available to them locally, and then deduce collectively further information from the combination of their views. In particular, even the *absence* of fault evidence on all peers may allow to deduce fault occurrence jointly, see [64], [65]. Automatizing such procedures for the supervision and management of distributed and locally monitored asynchronous systems is a long-term goal to which *MExICo* hopes to contribute.

3.1.3. Contextual nets

Participant: Stefan Schwoon.

Assuring the correctness of concurrent systems is notoriously difficult due to the many unforeseeable ways in which the components may interact and the resulting state-space explosion. A well-established approach to alleviate this problem is to model concurrent systems as Petri nets and analyse their unfoldings, essentially an acyclic version of the Petri net whose simpler structure permits easier analysis [50].

However, Petri nets are inadequate to model concurrent read accesses to the same resource. Such situations often arise naturally, for instance in concurrent databases or in asynchronous circuits. The encoding tricks typically used to model these cases in Petri nets make the unfolding technique inefficient. Contextual nets, which explicitly do model concurrent read accesses, address this problem. Their accurate representation of concurrency makes contextual unfoldings up to exponentially smaller in certain situations. An abstract algorithm for contextual unfoldings was first given in [36]. In recent work, we further studied this subject from a theoretical and practical perspective, allowing us to develop concrete, efficient data structures and algorithms and a tool (Cunf) that improves upon existing state of the art. This work led to the PhD thesis of César Rodríguez in 2014 .

Contexutal unfoldings deal well with two sources of state-space explosion: concurrency and shared resources. Recently, we proposed an improved data structure, called *contextual merged processes* (CMP) to deal with a third source of state-space explosion, i.e. sequences of choices. The work on CMP [66] is currently at an abstract level. In the short term, we want to put this work into practice, requiring some theoretical groundwork, as well as programming and experimentation.

Another well-known approach to verifying concurrent systems is *partial-order reduction*, exemplified by the tool SPIN. Although it is known that both partial-order reduction and unfoldings have their respective strengths and weaknesses, we are not aware of any conclusive comparison between the two techniques. Spin comes with a high-level modeling language having an explicit notion of processes, communication channels, and variables. Indeed, the reduction techniques implemented in Spin exploit the specific properties of these features. On the other side, while there exist highly efficient tools for unfoldings, Petri nets are a relatively general low-level formalism, so these techniques do not exploit properties of higher language features. Our work on contextual unfoldings and CMPs represents a first step to make unfoldings exploit richer models. In the long run, we wish raise the unfolding technique to a suitable high-level modelling language and develop appropriate tool support.

3.1.4. Dynamic and parameterized concurrent systems

Participants: Benedikt Bollig, Paul Gastin.

In the past few years, our research has focused on concurrent systems where the architecture, which provides a set of processes and links between them, is *static* and *fixed in advance*. However, the assumption that the set of processes is fixed somehow seems to hinder the application of formal methods in practice. It is not appropriate in areas such as mobile computing or ad-hoc networks. In concurrent programming, it is actually perfectly natural to design a program, and claim its correctness, independently of the number of processes that participate in its execution. There are, essentially, two kinds of systems that fall into this category. When the process architecture is static but unknown, it is a parameter of the system; we then call a system

parameterized. When, on the other hand, the process architecure is generated at runtime (i.e., process creation is a communication primitive), we say that a system is *dynamic*. Though parameterized and dynamic systems have received increasing interest in recent years, there is, by now, no canonical approach to modeling and verifying such systems. Our research program aims at the development of *a theory of parameterized and dynamic concurrent systems.* More precisely, our goal is a *unifying* theory that lays algebraic, logical, and automata-theoretic foundations to support and facilitate the study of parameterized and dynamic concurrent systems. Such theories indeed exist in non-parameterized settings where the number of processes and the way they are connected are fixed in advance. However, parameterized and dynamic systems lack such foundations and often restict to very particular models with specialized verification techniques.

3.1.5. Testing

Participants: Benedikt Bollig, Paul Gastin, Stefan Haar.

3.1.5.1. Introduction

The gap between specification and implementation is at the heart of research on formal testing. The general *conformance testing problem* can be defined as follows: Does an implementation $\mathcal{M}'$ conform a given specification $\mathcal{M}$? Here, both $\mathcal{M}$ and $\mathcal{M}'$ are assumed to have input and output channels. The formal model $\mathcal{M}$ of the specification is entirely known and can be used for analysis. On the other hand, the implementation $\mathcal{M}'$ is unknown but interacts with the environment through observable input and output channels. So the behavior of $\mathcal{M}'$ is partially controlled by input streams, and partially observable via output streams. The Testing problem consists in computing, from the knowledge of $\mathcal{M}$, *input streams* for $\mathcal{M}'$ such that observation of the resulting output streams from $\mathcal{M}'$ allows to determine whether $\mathcal{M}'$ conforms to $\mathcal{M}$ as intended.

In this project, we focus on distributed or asynchronous versions of the conformance testing problem. There are two main difficulties. First, due to the distributed nature of the system, it may not be possible to have a unique global observer for the outcome of a test. Hence, we may need to use *local* observers which will record only *partial views* of the execution. Due to this, it is difficult or even impossible to reconstruct a coherent global execution. The second difficulty is the lack of global synchronization in distributed asynchronous systems. Up to now, models were described with I/O automata having a centralized control, hence inducing global synchronizations.

3.1.5.2. Asynchronous Testing

Since 2006 and in particular during his sabbatical stay at the University of Ottawa, Stefan Haar has been working with Guy-Vincent Jourdan and Gregor v. Bochmann of UOttawa and Claude Jard of IRISA on asynchronous testing. In the synchronous (sequential) approach, the model is described by an I/O automaton with a centralized control and transitions labeled with individual input or output actions. This approach has known limitations when inputs and outputs are distributed over remote sites, a feature that is characteristic of , e.g., web computing. To account for concurrency in the system, they have developed in [58], [41] asynchronous conformance testing for automata with transitions labeled with (finite) partial orders of I/O. Intuitively, this is a "big step" semantics where each step allows concurrency but the system is synchronized before the next big step. This is already an important improvement on the synchronous setting. The non-trivial challenge is now to cope with fully asynchronous specifications using models with decentralized control such as Petri nets.

3.1.5.3. Near Future

Completion of asynchronous testing in the setting without any big-step synchronization, and an improved understanding of the relations and possible interconnections between local (i.e. distributed) and asynchronous (centralized) testing. This has been the objective of the *TECSTES* project (2011-2014), funded by a DIGITEO *DIM/LSC* grant, and which involved Hernán Ponce de Léon and Stefan Haar of *MExICo*, and Delphine Longuet at LRI, University Paris-Sud/Orsay. We have extended several well known conformance (ioco style) relations for sequential models to models that can handle concurrency (labeled event structures). Two semantics (interleaving and partial order) were presented for every relation. With the interleaving semantics, the relations we obtained boil down to the same relations defined for labeled transition systems, since they focus on sequences of actions. The only advantage of using labeled event structures as a specification formalism for testing remains in the conciseness of the concurrent model with respect to a sequential one.

As far as testing is concerned, the benefit is low since every interleaving has to be tested. By contrast, under the partial order semantics, the relations we obtain allow to distinguish explicitly implementations where concurrent actions are implemented concurrently, from those where they are interleaved, i.e. implemented sequentially. Therefore, these relations will be of interest when designing distributed systems, since the natural concurrency between actions that are performed in parallel by different processes can be taken into account. In particular, the fact of being unable to control or observe the order between actions taking place on different processes will not be considered as an impediment for testing. We have developped a complete testing framework for concurrent systems, which included the notions of test suites and test cases. We studied what kind of systems are testable in such a framework, and we have proposed sufficient conditions for obtaining a complete test suite as well as an algorithm to construct a test suite with such properties.

A mid-to long term goal (which may or may not be addressed by *MExICo* depending on the availability of staff for this subject) is the comprehensive formalization of testing and testability in asynchronous systems with distributed architecture and test protocols.

3.2. Interaction

Participants: Benedikt Bollig, Thomas Chatain, Paul Gastin, Stefan Haar, Serge Haddad.

3.2.1. Introduction

Systems and services exhibit non-trivial *interaction* between specialized and heterogeneous components. This interplay is challenging for several reasons. On one hand, a coordinated interplay of several components is required, though each has only a limited, partial view of the system's configuration. We refer to this problem as *distributed synthesis* or *distributed control*. An aggravating factor is that the structure of a component might be semi-transparent, which requires a form of *grey box management*.

Interaction, one of the main characteristics of systems under consideration, often involves an environment that is not under the control of cooperating services. To achieve a common goal, the services need to agree upon a strategy that allows them to react appropriately regardless of the interactions with the environment. Clearly, the notions of opponents and strategies fall within *game theory*, which is naturally one of our main tools in exploring interaction. We will apply to our problems techniques and results developed in the domains of distributed games and of games with partial information. We will consider also new problems on games that arise from our applications.

3.2.2. Distributed Control

Participants: Benedikt Bollig, Thomas Chatain, Paul Gastin, Stefan Haar.

Program synthesis, as introduced by Church [47] aims at deriving directly an implementation from a specification, allowing the implementation to be correct by design. When the implementation is already at hand but choices remain to be resolved at run time then the problem becomes controller synthesis. Both program and controller synthesis have been extensively studied for sequential systems. In a distributed setting, we need to synthesize a distributed program or distributed controllers that interact locally with the system components. The main difficulty comes from the fact that the local controllers/programs have only a partial view of the entire system. This is also an old problem largely considered undecidable in most settings [63], [59], [62], [53], [55].

Actually, the main undecidability sources come from the fact that this problem was addressed in a synchronous setting using global runs viewed as sequences. In a truly distributed system where interactions are asynchronous we have recently obtained encouraging decidability results [54], [45]. This is a clear witness where concurrency may be exploited to obtain positive results. It is essential to specify expected properties directly in terms of causality revealed by partial order models of executions (MSCs or Mazurkiewicz traces). We intend to develop this line of research with the ambitious aim to obtain decidability for all natural systems and specifications. More precisely, we will identify natural hypotheses both on the architecture of our distributed system and on the specifications under which the distributed program/controller synthesis problem is decidable. This should open the way to important applications, e.g., for distributed control of embedded systems.

3.2.3. Adaptation and Grey box management

Participants: Stefan Haar, Serge Haddad.

Contrary to mainframe systems or monolithic applications of the past, we are experiencing and using an increasing number of services that are performed not by one provider but rather by the interaction and cooperation of many specialized components. As these components come from different providers, one can no longer assume all of their internal technologies to be known (as it is the case with proprietary technology). Thus, in order to compose e.g. orchestrated services over the web, to determine violations of specifications or contracts, to adapt existing services to new situations etc, one needs to analyze the interaction behavior of *boxes* that are known only through their public interfaces. For their semi-transparent-semi-opaque nature, we shall refer to them as **grey boxes**. While the concrete nature of these boxes can range from vehicles in a highway section to hotel reservation systems, the tasks of *grey box management* have universal features allowing for generalized approaches with formal methods. Two central issues emerge:

- Abstraction: From the designer point of view, there is a need for a trade-off between transparency (no abstraction) in order to integrate the box in different contexts and opacity (full abstraction) for security reasons.
- Adaptation: Since a grey box gives a partial view about the behavior of the component, even if it is not immediately useable in some context, the design of an adaptator is possible. Thus the goal is the synthesis of such an adaptator from a formal specification of the component and the environment.

Our work on direct modeling and handling of "grey boxes" via modal models (see [49]) was halted when Dorsaf El-Hog stopped her PhD work to leave academia, and has not resumed for lack of staff. However, it should be noted that semi-transparent system management in a larger sense remains an active field for the team, witness in particular our work on diagnosis and testing.

3.3. Management of Quantitative Behavior

Participants: Benedikt Bollig, Thomas Chatain, Paul Gastin, Stefan Haar, Serge Haddad.

3.3.1. Introduction

Besides the logical functionalities of programs, the *quantitative* aspects of component behavior and interaction play an increasingly important role.

- *Real-time* properties cannot be neglected even if time is not an explicit functional issue, since transmission delays, parallelism, etc, can lead to time-outs striking, and thus change even the logical course of processes. Again, this phenomenon arises in telecommunications and web services, but also in transport systems.
- In the same contexts, *probabilities* need to be taken into account, for many diverse reasons such as unpredictable functionalities, or because the outcome of a computation may be governed by race conditions.
- Last but not least, constraints on *cost* cannot be ignored, be it in terms of money or any other limited resource, such as memory space or available CPU time.

Traditional mainframe systems were proprietary and (essentially) localized; therefore, impact of delays, unforeseen failures, etc. could be considered under the control of the system manager. It was therefore natural, in verification and control of systems, to focus on *functional* behavior entirely.

With the increase in size of computing system and the growing degree of compositionality and distribution, quantitative factors enter the stage:

- calling remote services and transmitting data over the web creates *delays*;
- remote or non-proprietary components are not “deterministic”, in the sense that their behavior is uncertain.

Time and *probability* are thus parameters that management of distributed systems must be able to handle; along with both, the *cost* of operations is often subject to restrictions, or its minimization is at least desired. The mathematical treatment of these features in distributed systems is an important challenge, which *MExICo* is addressing; the following describes our activities concerning probabilistic and timed systems. Note that cost optimization is not a current activity but enters the picture in several intended activities.

3.3.2. Probabilistic distributed Systems

Participants: Stefan Haar, Serge Haddad, Claudine Picaronny.

3.3.2.1. Non-sequential probabilistic processes

Practical fault diagnosis requires to select explanations of *maximal likelihood*. For partial-order based diagnosis, this leads therefore to the question what the probability of a given partially ordered execution is. In Benveniste et al. [39], [32], we presented a model of stochastic processes, whose trajectories are partially ordered, based on local branching in Petri net unfoldings; an alternative and complementary model based on Markov fields is developed in [57], which takes a different view on the semantics and overcomes the first model's restrictions on applicability.

Both approaches abstract away from real time progress and randomize choices in *logical* time. On the other hand, the relative speed - and thus, indirectly, the real-time behavior of the system's local processes - are crucial factors determining the outcome of probabilistic choices, even if non-determinism is absent from the system.

In another line of research [43] we have studied the likelihood of occurrence of non-sequential runs under random durations in a stochastic Petri net setting. It remains to better understand the properties of the probability measures thus obtained, to relate them with the models in logical time, and exploit them e.g. in *diagnosis*.

3.3.2.2. Distributed Markov Decision Processes

Participant: Serge Haddad.

Distributed systems featuring non-deterministic and probabilistic aspects are usually hard to analyze and, more specifically, to optimize. Furthermore, high complexity theoretical lower bounds have been established for models like partially observed Markovian decision processes and distributed partially observed Markovian decision processes. We believe that these negative results are consequences of the choice of the models rather than the intrinsic complexity of problems to be solved. Thus we plan to introduce new models in which the associated optimization problems can be solved in a more efficient way. More precisely, we start by studying connection protocols weighted by costs and we look for online and offline strategies for optimizing the mean cost to achieve the protocol. We have been cooperating on this subject with the SUMO team at Inria Rennes; in the joint work [33]; there, we strive to synthesize for a given MDP a control so as to guarantee a specific stationary behavior, rather than - as is usually done - so as to maximize some reward.

3.3.3. Large scale probabilistic systems

Addressing large-scale probabilistic systems requires to face state explosion, due to both the discrete part and the probabilistic part of the model. In order to deal with such systems, different approaches have been proposed:

- Restricting the synchronization between the components as in queuing networks allows to express the steady-state distribution of the model by an analytical formula called a product-form [38].
- Some methods that tackle with the combinatory explosion for discrete-event systems can be generalized to stochastic systems using an appropriate theory. For instance symmetry based methods have been generalized to stochastic systems with the help of aggregation theory [46].
- At last simulation, which works as soon as a stochastic operational semantic is defined, has been adapted to perform statistical model checking. Roughly speaking, it consists to produce a confidence interval for the probability that a random path fulfills a formula of some temporal logic [67] .

We want to contribute to these three axes: (1) we are looking for product-forms related to systems where synchronization are more involved (like in Petri nets), see [2]; (2) we want to adapt methods for discrete-event systems that require some theoretical developments in the stochastic framework and, (3) we plan to address some important limitations of statistical model checking like the expressiveness of the associated logic and the handling of rare events.

3.3.4. Real time distributed systems

Nowadays, software systems largely depend on complex timing constraints and usually consist of many interacting local components. Among them, railway crossings, traffic control units, mobile phones, computer servers, and many more safety-critical systems are subject to particular quality standards. It is therefore becoming increasingly important to look at networks of timed systems, which allow real-time systems to operate in a distributed manner.

Timed automata are a well-studied formalism to describe reactive systems that come with timing constraints. For modeling distributed real-time systems, networks of timed automata have been considered, where the local clocks of the processes usually evolve at the same rate [61] [44]. It is, however, not always adequate to assume that distributed components of a system obey a global time. Actually, there is generally no reason to assume that different timed systems in the networks refer to the same time or evolve at the same rate. Any component is rather determined by local influences such as temperature and workload.

3.3.4.1. Implementation of Real-Time Concurrent Systems

Participants: Thomas Chatain, Stefan Haar, Serge Haddad.

This was one of the tasks of the ANR ImpRo.

Formal models for real-time systems, like timed automata and time Petri nets, have been extensively studied and have proved their interest for the verification of real-time systems. On the other hand, the question of using these models as specifications for designing real-time systems raises some difficulties. One of those comes from the fact that the real-time constraints introduce some artifacts and because of them some syntactically correct models have a formal semantics that is clearly unrealistic. One famous situation is the case of Zeno executions, where the formal semantics allows the system to do infinitely many actions in finite time. But there are other problems, and some of them are related to the distributed nature of the system. These are the ones we address here.

One approach to implementability problems is to formalize either syntactical or behavioral requirements about what should be considered as a reasonable model, and reject other models. Another approach is to adapt the formal semantics such that only realistic behaviors are considered.

These techniques are preliminaries for dealing with the problem of implementability of models. Indeed implementing a model may be possible at the cost of some transformation, which make it suitable for the target device. By the way these transformations may be of interest for the designer who can now use high-level features in a model of a system or protocol, and rely on the transformation to make it implementable.

We aim at formalizing and automating translations that preserve both the timed semantics and the concurrent semantics. This effort is crucial for extending concurrency-oriented methods for logical time, in particular for exploiting partial order properties. In fact, validation and management - in a broad sense - of distributed systems is not realistic *in general* without understanding and control of their real-time dependent features; the link between real-time and logical-time behaviors is thus crucial for many aspects of *MExICo*'s work.

3.3.5. Weighted Automata and Weighted Logics

Participants: Benedikt Bollig, Paul Gastin.

Time and probability are only two facets of quantitative phenomena. A generic concept of adding weights to qualitative systems is provided by the theory of weighted automata [31]. They allow one to treat probabilistic or also reward models in a unified framework. Unlike finite automata, which are based on the Boolean semiring, weighted automata build on more general structures such as the natural or real numbers (equipped with the usual addition and multiplication) or the probabilistic semiring. Hence, a weighted automaton associates with any possible behavior a weight beyond the usual Boolean classification of "acceptance" or "non-acceptance". Automata with weights have produced a well-established theory and come, e.g., with a characterization in terms of rational expressions, which generalizes the famous theorem of Kleene in the unweighted setting. Equipped with a solid theoretical basis, weighted automata finally found their way into numerous application areas such as natural language processing and speech recognition, or digital image compression.

What is still missing in the theory of weighted automata are satisfactory connections with verification-related issues such as (temporal) logic and bisimulation that could lead to a general approach to corresponding satisfiability and model-checking problems. A first step towards a more satisfactory theory of weighted systems was done in [42]. That paper, however, does not give definite answers to all the aforementioned problems. It identifies directions for future research that we will be tackling.

4. Application Domains

4.1. Telecommunications

Participants: Stefan Haar, Serge Haddad.

MExICo's research is motivated by problems of *system management* in several domains, such as:

- In the domain of service oriented computing, it is often necessary to insert some Web service into an existing orchestrated business process, e.g. to replace another component after failures. This requires to ensure, often actively, conformance to the interaction protocol. One therefore needs to synthesize adaptators for every component in order to steer its interaction with the surrounding processes.
- Still in the domain of telecommunications, the supervision of a network tends to move from out-of-band technology, with a fixed dedicated supervision infrastructure, to in-band supervision where the supervision process uses the supervised network itself. This new setting requires to revisit the existing supervision techniques using control and diagnosis tools.

Currently, we have no active cooperation on these subjects.

4.2. Transport Systems

Participants: Stefan Haar, Serge Haddad, Yann Duplouy, Simon Theissing.

We participate in the IRT System X's system of systems program TMM, in two projects:

- project MIC (terminated in November 2016) on multi-modal transport systems with academic partners UPMC, IFSTTAR and CEA, and several industrial partners including Alstom (project leader), COSMO and Renault. Transportation operators in an urban area need to plan, supervise and steer different means of transportation with respect to several criteria:
  - Maximize capacity;
  - guarantee punctuality and robustness of service;
  - minimize energy consumption.

The systems must achieve these objectives not only under ideal conditions, but also be robust to perturbations (such as a major cultural or sport event creating additional traffic), modifications of routes (roadwork, accidents, demonstrations, ...) and tolerant to technical failures. Therefore, systems must be enabled to raise appropriate alarms upon detection of anomalies, diagnose the type of anomaly and select the appropriate response. While the above challenges belong already to the tasks of individual operators in the unimodal setting, the rise of and increasing demand for multi-modal transports forces to achieve these planning, optimization and control goals not in isolation, but in a cooperative manner, across several operators. The research task here is first to analyze the transportation system regarding the available means, capacities and structures, and so as to identify the impacting factors and interdependencies of the system variables. Based on this analysis, the task is to derive and implement robust planning, with tolerance to technical faults; diagnosis and control strategies that are optimal under several, possibly different, criteria (average case vs worst case performance, energy efficiency, etc.) and allow to adapt to changes e.g. from nominal mode to reduced mode, sensor failures, etc.

- the project SVA (Simulation pour la Sécurité du Véhicule Autonome), where the PhD Thesis of Yann Duplouy targets the application of formal methods to the development of embedded systems for autonomous vehicles.

4.3. Biological Systems

Participants: Thomas Chatain, Stefan Haar, Serge Haddad, Stefan Schwoon.

We have begun in 2014 to examine concurrency issues in systems biology, and are currently enlarging the scope of our research's applications in this direction. To see the context, note that in recent years, a considerable shift of biologists' interest can be observed, from the mapping of static genotypes to gene expression, i.e. the processes in which genetic information is used in producing functional products. These processes are far from being uniquely determined by the gene itself, or even jointly with static properties of the environment; rather, regulation occurs throughout the expression processes, with specific mechanisms increasing or decreasing the production of various products, and thus modulating the outcome. These regulations are central in understanding cell fate (how does the cell differenciate ? Do mutations occur ? etc), and progress there hinges on our capacity to analyse, predict, monitor and control complex and variegated processes. We have applied Petri net unfolding techniques for the efficient computation of attractors in a regulatory network; that is, to identify strongly connected reachability components that correspond to stable evolutions, e.g. of a cell that differentiates into a specific functionality (or mutation). This constitutes the starting point of a broader research with Petri net unfolding techniques in regulation. In fact, ,he use of ordinary Petri nets for capturing regulatory network (RN) dynamics overcomes the limitations of traditional RN models : those impose e.g. Monotonicity properties in the influence that one factor had upon another, i.e. always increasing or always decreasing, and were thus unable to cover all actual behaviours (see [75]). Rather, we follow the more refined model of boolean networks of automata, where the local states of the different factors jointly detemine which state transitions are possible. For these connectors, ordinary PNs constitute a first approximation, improving greatly over the literature but leaving room for improvement in terms of introducing more refined logical connectors. Future work thus involves transcending this class of PN models. Via unfoldings, one has access – provided efficient techniques are available – to all behaviours of the model, rather than over-or under-approximations as previously. This opens the way to efficiently searching in particular for determinants of the cell fate : which attractors are reachable from a given stage, and what are the factors that decide in favor of one or the other attractor, etc. The list of potential applications in biology and medicine of such a methodology would be too long to reproduce here.

5. Highlights of the Year

5.1. Highlights of the Year

Diagnosis, Anti-alignments and Coverability

DIAGNOSIS

Several new advances were obtained, concerning Diagnosis in Infinite-State Probabilistic Systems, Approximate Diagnosability of Stochastic Systems, and Diagnosability of Repairable Faults; see the 'New Results' section for a detailed description.

ANTI-ALIGNMENTS IN CONFORMANCE CHECKING – THE DARK SIDE OF PROCESS MODELS

Conformance checking techniques asses the suitability of a process model in representing an underlying process, observed through a collection of real executions. These techniques suffer from the well-known state space explosion problem, hence handling process models exhibiting large or even infinite state spaces remains a challenge. One important metric in conformance checking is to asses the precision of the model with respect to the observed executions, i.e., characterize the ability of the model to produce behavior unrelated to the one observed. By avoiding the computation of the full state space of a model, current techniques only provide estimations of the precision metric, which in some situations tend to be very optimistic, thus hiding real problems a process model may have. In [15], [25] we present the notion of anti-alignment as a concept to help unveiling traces in the model that may deviate significantly from the observed behavior. Using anti-alignments, current estimations can be improved, e.g., in precision checking. We show how to express the problem of finding anti-alignments as the satisfiability of a Boolean formula, and provide a tool which can deal with large models efficiently. In [19], [20], a novel approach to measure precision and generalization is presented, which relies on the notion of anti-alignments. We propose metrics for precision and generalization that resemble the leave-one-out cross-validation techniques, where individual traces of the log are removed and the computed anti-alignment assess the model's capability to describe precisely or generalize the observed behavior.

APPROACHING THE COVERABILITY PROBLEM CONTINUOUSLY

The coverability problem for Petri nets plays a central role in the verification of concurrent shared-memory programs. However, its high EXPSPACE-complete complexity poses a challenge when encountered in real-world instances. In [13], we develop a new approach to this problem which is primarily based on applying forward coverability in continuous Petri nets as a pruning criterion inside a backward coverability framework. A cornerstone of our approach is the efficient encoding of a recently developed polynomial-time algorithm for reachability in continuous Petri nets into SMT. We demonstrate the effectiveness of our approach on standard benchmarks from the literature, which shows that our approach decides significantly more instances than any existing tool and is in addition often much faster, in particular on large instances.

6. New Software and Platforms

6.1. DarkSider

FUNCTIONAL DESCRIPTION

DarkSider computes anti-alignments between a Petri net model and a log of observed traces, as described in [15], [25].

- Participant: Thomas Chatain
- Contact: Thomas Chatain
- URL: http://www.lsv.ens-cachan.fr/~chatain/darksider/

6.2. COSMOS

FUNCTIONAL DESCRIPTION

COSMOS is a statistical model checker for the Hybrid Automata Stochastic Logic (HASL). HASL employs Linear Hybrid Automata (LHA), a generalization of Deterministic Timed Automata (DTA), to describe accepting execution paths of a Discrete Event Stochastic Process (DESP), a class of stochastic models which includes, but is not limited to, Markov chains. As a result HASL verification turns out to be a unifying framework where sophisticated temporal reasoning is naturally blended with elaborate reward-based analysis. COSMOS takes as input a DESP (described in terms of a Generalized Stochastic Petri Net), an LHA and an expression Z representing the quantity to be estimated. It returns a confidence interval estimation of Z, recently, it has been equipped with functionalities for rare event analysis. COSMOS is written in C++

- Participants: Benoît Barbot, Hilal Djafri, Paolo Ballarini, Marie Duflot-Kremer and Serge Haddad
- Contact: Hilal Djafri
- URL: http://www.lsv.ens-cachan.fr/~barbot/cosmos/

6.3. CosyVerif

FUNCTIONAL DESCRIPTION

CosyVerif is a platform dedicated to the formal specification and verification of dynamic systems. It allows to specify systems using several formalisms (such as automata and Petri nets), and to run verification tools on these models.

- Participants: Serge Haddad, Fabrice Kordon, Laure Petrucci and Alban Linard
- Partners: LIP6 - LIPN (Laboratoire d'Informatique de l'Université Paris Nord) - LSV
- Contact: Serge Haddad
- URL: http://www.cosyverif.org/

6.4. Mole

FUNCTIONAL DESCRIPTION

Mole computes, given a safe Petri net, a finite prefix of its unfolding. It is designed to be compatible with other tools, such as PEP and the Model-Checking Kit, which are using the resulting unfolding for reachability checking and other analyses. The tool Mole arose out of earlier work on Petri nets.

- Participant: Stefan Schwoon
- Contact: Stefan Schwoon
- URL: http://www.lsv.ens-cachan.fr/~schwoon/tools/mole/

7. New Results

7.1. Analyzing Timed Systems Using Tree Automata

Timed systems, such as timed automata, are usually analyzed using their operational semantics on timed words. The classical region abstraction for timed automata reduces them to (untimed) finite state automata with the same time-abstract properties, such as state reachability. In [10], we propose a new technique to analyze such timed systems using finite tree automata instead of finite word automata. The main idea is to consider timed behaviors as graphs with matching edges capturing timing constraints. Such graphs can be interpreted in trees opening the way to tree automata based techniques which are more powerful than analysis based on word automata. The technique is quite general and applies to many timed systems. In this paper, as an example, we develop the technique on timed pushdown systems, which have recently received considerable attention. Further, we also demonstrate how we can use it on timed automata and timed multi-stack pushdown systems (with boundedness restrictions).

7.2. Interrupt Timed Automata with Auxiliary Clocks and Parameters

Interrupt Timed Automata (ITA) are an expressive timed model, introduced to take into account interruptions according to levels. Due to this feature, this formalism is incomparable with Timed Automata. However several decidability results related to reachability and model checking have been obtained. In , we add auxiliary clocks to ITA, thereby extending its expressive power while preserving decidability of reachability. Moreover, we define a parametrized version of ITA, with polynomials of parameters appearing in guards and updates. While parametric reasoning is particularly relevant for timed models, it very often leads to undecidability results. We prove that various reachability problems, including robust reachability, are decidable for this model, and we give complexity upper bounds for a fixed or variable number of clocks, levels and parameters.

7.3. One-Counter Automata with Counter Observability

In a one-counter automaton (OCA), one can produce a letter from some finite alphabet, increment and decrement the counter by one, or compare it with constants up to some threshold. It is well-known that universality and language inclusion for OCAs are undecidable. In [14], we consider OCAs with counter observability: Whenever the automaton produces a letter, it outputs the current counter value along with it. Hence, its language is now a set of words over an infinite alphabet. We show that universality and inclusion for that model are PSPACE-complete, thus no harder than the corresponding problems for finite automata. In fact, by establishing a link with visibly one-counter automata, we show that OCAs with counter observability are effectively determinizable and closed under all boolean operations.

7.4. Diagnosis in Infinite-State Probabilistic Systems

In a recent work, we introduced four variants of diagnosability (FA, IA, FF, IF) in (finite) probabilistic systems (pLTS) depending whether one considers (1) finite or infinite runs and (2) faulty or all runs. We studied their relationship and established that the corresponding decision problems are PSPACE-complete. A key ingredient of the decision procedures was a characterisation of diagnosability by the fact that a random run almost surely lies in an open set whose specification only depends on the qualitative behaviour of the pLTS. In [12], we investigate similar issues for infinite pLTS. We first show that this characterisation still holds for FF-diagnosability but with a Gδ set instead of an open set and also for IF-and IA-diagnosability when pLTS are finitely branching. We also prove that surprisingly FA-diagnosability cannot be characterised in this way even in the finitely branching case. Then we apply our characterisations for a partially observable probabilistic extension of visibly pushdown automata (POpVPA), yielding EXPSPACE procedures for solving diagnosability problems. In addition, we establish some computational lower bounds and show that slight extensions of POpVPA lead to undecidability.

7.5. Accurate Approximate Diagnosability of Stochastic Systems

Diagnosis of partially observable stochastic systems prone to faults was introduced in the late nineties. Diagnosability, i.e. the existence of a diagnoser, may be specified in different ways: (1) exact diagnosability (called A-diagnosability) requires that almost surely a fault is detected and that no fault is erroneously claimed while (2) approximate diagnosability (called ε-diagnosability) allows a small probability of error when claiming a fault and (3) accurate approximate diagnosability (called AA-diagnosability) requires that this error threshold may be chosen arbitrarily small. In [11], we mainly focus on approximate diagnoses. We first refine the almost sure requirement about finite delay introducing a uniform version and showing that while it does not discriminate between the two versions of exact diagnosability this is no more the case in approximate diagnosis. Then we establish a complete picture for the decidability status of the diagnosability problems: (uniform) ε-diagnosability and uniform AA-diagnosability are undecidable while AA-diagnosability is decidable in PTIME, answering a longstanding open question.

7.6. Diagnosability of Repairable Faults

The diagnosis problem for discrete event systems consists in deciding whether some fault event occurred or not in the system, given partial observations on the run of that system. Diagnosability checks whether a correct diagnosis can be issued in bounded time after a fault, for all faulty runs of that system. This problem appeared two decades ago and numerous facets of it have been explored, mostly for permanent faults. It is known for example that diagnosability of a system can be checked in polynomial time, while the construction of a diagnoser is exponential. In [21], we examine the case of transient faults, that can appear and be repaired. Diagnosability in this setting means that the occurrence of a fault should always be detected in bounded time, but also before the fault is repaired. Checking this notion of diagnosability is proved to be PSPACE-complete. It is also shown that faults can be reliably counted provided the system is diagnosable for faults and for repairs.

7.7. Optimal constructions for active diagnosis

The task of diagnosis consists in detecting, without ambiguity, occurrence of faults in a partially observed system. Depending on the degree of observability, a discrete event system may be diagnosable or not. Active diagnosis aims at controlling the system in order to make it diagnosable. Solutions have already been proposed for the active diagnosis problem, but their complexity remains to be improved. In [8], we solve the active diagnosability decision problem and the active diagnoser synthesis problem, proving that (1) our procedures are optimal w.r.t. to computational complexity, and (2) the memory required for the active diagnoser produced by the synthesis is minimal. Furthermore, focusing on the minimal delay before detection, we establish that the memory required for any active diagnoser achieving this delay may be highly greater than the previous one. So we refine our construction to build with the same complexity and memory requirement an active diagnoser that realizes a delay bounded by twice the minimal delay.

7.8. Verification of parameterized communicating automata via split-width

In [16] study verification problems for distributed systems communicating via unbounded FIFO channels. The number of processes of the system as well as the communication topology are not fixed a priori. Systems are given by parameterized communicating automata (PCAs) which can be run on any communication topology of bounded degree, with arbitrarily many processes. Such systems are Turing powerful so we concentrate on under-approximate verification. We extend the notion of split-width to behaviors of PCAs. We show that emptiness, reachability and model-checking problems of PCAs are decidable when restricted to behaviors of bounded split-width. Reachability and emptiness are EXPTIME-complete, but only polynomial in the size of the PCA. We also describe several concrete classes of bounded split-width, for which we prove similar results.

7.9. Cyclic Ordering through Partial Orders

The orientation problem for ternary cyclic order relations has been attacked in the literature from combinatorial perspectives, through rotations, and by connection with Petri nets. In [7], we propose a two-fold characterization of orientable cyclic orders in terms of symmetries of partial orders as well as in terms of separating sets (cuts). The results are inspired by properties of non-sequential discrete processeses, but also apply to dense structures of any cardinality.

7.10. Predicting Traffic Load in Public Transportation Networks

This work is part of an ongoing effort to understand the dynamics of passenger loads in modern, multimodal transportation networks (TNs) and to mitigate the impact of perturbations, under the restrictions that the precise number of passengers in some point of the TN that intend to reach a certain destination (i.e. their distribution over different trip profiles) is unknown. In [29], we introduce an approach based on a stochastic hybrid automaton model for a TN that allows to compute how such probabilistic load vectors are propagated through the TN. In [23], [30], develop a computation strategy for forecasting the network's load a certain time in the future.

In [22], [28], we continue our work on perturbation analysis of multimodal transportation networks (TNs) by means of a stochastic hybrid automaton (SHA) model. We focus here on the approximate computation , in particular on the major bottleneck consisting in the high dimensionality of systems of stochastic differential balance equations (SDEs) that define the continuous passenger-flow dynamics in the different modes of the SHA model. In fact, for every pair of a mode and a station, one system of coupled SDEs relates the passenger loads of all discrete points such as platforms considered in this station, and all vehicles docked to it, to the passenger flows in between. In general, such an SDE system has many dimensions, which makes its numerical computation and thus the approximate computation of the SHA model intractable. We show how these systems can be canonically replaced by lower-dimensional ones, by decoupling the passenger flows inside every mode from one another. We prove that the resulting approximating passenger-flow dynamics converges to the original one, if the replacing set of balance equations set up for all decoupled passenger flows communicate their results among each other in vanishing time intervals.

For more information about the whole project, see [27].

7.11. Unfolding of Parametric Logical Regulatory Networks

In systems biology, models of cellular regulatory processes such as gene regulatory networks or signalling pathways are crucial to understanding the behaviour of living cells. Available biological data are however often insufficient for full model specification. In [18], we focus on partially specified models where the missing information is abstracted in the form of parameters. We introduce a novel approach to analysis of parametric logical regulatory networks addressing both sources of combinatoric explosion native to the model. First, we introduce a new compact representation of admissible parameters using Boolean lattices. Then, we define the unfolding of parametric regulatory networks. The resulting structure provides a partial- order reduction of concurrent transitions, and factorises the common transitions among the concrete models. A comparison is performed against state-of-the-art approaches to parametric model analysis.

7.12. Relationship between the Reprogramming Determinants of Boolean Networks and their Interaction Graph

In [24], we address the formal characterization of tar- gets triggering cellular trans-differentiation in the scope of Boolean net- works with asynchronous dynamics. Given two fixed points of a Boolean network, we are interested in all the combinations of mutations which allow to switch from one fixed point to the other, either possibly, or in- evitably. In the case of existential reachability, we prove that the set of nodes to (permanently) flip are only and necessarily in certain connected components of the interaction graph. In the case of inevitable reachabil- ity, we provide an algorithm to identify a subset of possible solutions.

7.13. D-SPACES: An Implementation of Declarative Semantics for Spatially Structured Information

We introduce in [17] D-SPACES, an implementation of constraint systems with space and extrusion operators. Constraint systems are algebraic models that allow for a semantic language-like representation of information in systems where the concept of space is a primary structural feature. We give this information mainly an epistemic interpretation and consider various agents as entities acting upon it. D-SPACES is coded as a c++11 library providing implementations for constraint systems, space functions and extrusion functions. The interfaces to access each implementation are minimal and thoroughly documented. D-SPACES also provides property-checking methods as well as an implementation of a specific type of constraint systems (a boolean algebra). This last implementation serves as an entry point for quick access and proof of concept when using these models. Furthermore, we offer an illustrative example in the form of a small social network where users post their beliefs and utter their opinions.

7.14. Belief, Knowledge, Lies and Other Utterances in an Algebra for Space and Extrusion

The notion of constraint system (cs) is central to declarative formalisms from concurrency theory such as process calculi for concurrent constraint programming (ccp). Constraint systems are often represented as lattices: their elements, called constraints, represent partial information and their order corresponds to entailment. Recently a notion of n-agent spatial cs was introduced to represent information in concurrent constraint programs for spatially distributed multi-agent systems. From a computational point of view a spatial constraint system can be used to specify partial information holding in a given agent's space (local information). From an epistemic point of view a spatial cs can be used to specify information that a given agent considers true (beliefs). Spatial constraint systems, however, do not provide a mechanism for specifying the mobility of information/processes from one space to another. Information mobility is a fundamental aspect of concurrent systems. In [6] we develop the theory of spatial constraint systems with operators to specify information and processes moving from a space to another. We shall investigate the properties of this new family of constraint systems and illustrate their applications. From a computational point of view the new operators provide for process/information extrusion, a central concept in formalisms for mobile communication. From an epistemic point of view extrusion corresponds I to a notion we shall call utterance; a piece of information that an agent communicate to others but that may be inconsistent with the agent's beliefs. Utterances can then be used to express instances of epistemic notions such as hoaxes or intentional lies which are common place in social media. Spatial constraint system can express the epistemic notion of belief by means of space functions that specify local information. We shall also show that spatial constraint can also express the epistemic notion of knowledge by means of a derived spatial operator that specifies global information.

7.15. Goal-Driven Unfolding of Petri Nets

Unfoldings provide an efficient way to avoid the state-space explosion due to interleavings of concurrent transitions when exploring the runs of a Petri net. The theory of adequate orders allows one to define finite prefixes of unfoldings which contain all the reachable markings. In this paper we are interested in reachability of a single given marking, called the goal. In [26], We propose an algorithm for computing a finite prefix of the unfolding of a 1-safe Petri net that preserves all minimal configurations reaching this goal. Our algorithm combines the unfolding technique with on-the-fly model reduction by static analysis aiming at avoiding the exploration of branches which are not needed for reaching the goal. We present some experimental results.

8. Partnerships and Cooperations

8.1. National Initiatives

We will be participating in the ANR Project ALGORECELL that starts in 2017.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

Serge Haddad is participating in the ERC EQualIS, 'Enhancing the Quality of Interacting Systems', directed by Patricia Bouyer.

8.3. International Initiatives

8.3.1. Inria Associate Teams Not Involved in an Inria International Labs

8.3.1.1. LifeForm

Title: Life Sciences need formal Methods !

International Partner (Institution - Laboratory - Researcher):

Newcastle University (United Kingdom) - School of Computing Science - Victor Khomenko

Start year: 2016

See also: http://projects.lsv.ens-cachan.fr/LifeForm/

This project extends an existing cooperation between the MEXICO team and Newcastle University on partial-order based formal methods for concurrent systems. We enlarge the partnership to bioinformatics and synthetic biology. The proposal addresses addresses challenges concerning formal specification, verification, monitoring and control of synthetic biological systems, with use cases conducted in the Center for Synthetic Biology and the Bioeconomy (CSBB) in Newcastle. A main challenge is to create a solid modelling framework based on Petri-net type models that allow for causality analysis and rapid state space exploration for verification, monitoring and control purposes; a potential extension to be investigated concerns the study of attractors and cell reprogramming in Systems Biology.

8.3.2. Participation in Other International Programs

UMI with CMI, India, starting in 2017; currently LIA INFORMEL, see below.

8.4. International Research Visitors

8.4.1. Visits of International Scientists

- Visits by Victor Khomenko and Maciej Koutny within the LifeForm associated team

8.4.2. Internships

- **Juraj Kolcˇák** from Masaryk University, Brno, Czech Republic, on *Efficient Analysis of Boolean Networks under Parameter Uncertainty*, Spring/summer of 2016 (Master's thesis research); director: Stefan Haar
- **Clara Scherbaum** from Aachen University, Germany, on *Computing Cut Sets for Petri Nets*, Spring 2016, LSV (ENS Cachan),
- **Hugues Mandon**: Algorithms for cellular reprogramming.

8.4.3. Visits to International Teams

8.4.3.1. Research Stays Abroad

Paul Gastin is visiting IIT Bombay and Chennay Mathematical Institute, India, from October 10, 2016 to March 10, 2017.

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. LIA INFORMEL

The Indo-French Formal Methods Lab is an International Associated Laboratory (LIA) fostering the scientific collaboration between India and France in the domain of formal methods and applications to the verification of complex systems. Our research focuses on theoretical foundations of games, automata, and logics, three important tools in formal methods. We study applications to the verification of safety-critical systems, with an emphasis on quantitative aspects (time, cost, energy, etc.), concurrency, control, and security protocols. The Laboratory was founded in 2012 by a consortium of researchers from the French Centre for Scientific Research (CNRS), Ecole Normale Supérieure de Cachan (ENS Cachan), Université Bordeaux 1, the Institute of Mathematical Sciences Chennai (IMSc), the Chennai Mathematical Institute (CMI), and the Indian Institute of Science Bangalore (IISc). It is directed by Paul Gastin (ENS Cachan, MExICo team) and Madhavan Mukund (CMI). The LIA has been scientifically extremely active and productive since its creation. The LIA has supported numerous scientific exchanges and joint research papers, see here. Among many other activities, the LIA organised another edition of the ACTS workshop.

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

- Thomas Chatain was a member of the program committee of *(ACSD 2016)*.
- Matthias Függer was a member of the PCs of DDECS'16 and ASYNC'16.
- Stefan Haar was a member of the PCs of *13th International Workshop on Discrete Event Systems WODES 2016*, the *16th International Conference on Applications of Concurrency to Systems Design (ACSD 2016)*, *Int. WS on Petri Nets and Software Engineering PNSE 2016*, ATAED Workshop on Analysis of Event Data 2016, and *IEEE Int. Conf. on Emerging Technologies and Factory Automation (ETFA)* 2016.
- Serge Haddad was a member of the PC of the 10th International Workshop on Verification and Evaluation of Computer and Communication Systems (VECOS 2016),Tunis, Tunisia.
- Stefan Schwoon was a member of the PC of the 37th International Conference on Applications and Theory of Petri Nets and Concurrency (PN 2016).
- Claudine Picaronny was a PC member for the Eighth International Conference on Advances in System Simulation (SIMUL'16)

9.1.2.2. Reviewer

- Matthias Függer was a reviewer for ICALP, ASYNC, DISC, DDECS, and IPDPS.
- Stefan HAAR was a reviewer for MFCS 2016.
- Stefan Schwoon acted as a reviewer for the following conferences taking place in 2016 : TACAS, ACSD, CONCUR, FSTTCS.

9.1.3. Journal

9.1.3.1. Member of Editorial Boards

- Stefan Haar is an associate editor of the *Journal of Discrete Event Dynamic Systems: Theory and Applications*, and a guest editor (with R. Meyer) of the upcoming special issue on ACSD 2015 in *ACM Transactions on Embedded Computing Systems (TECS)*.

9.1.3.2. Reviewer - Reviewing Activities

- Matthias Függer was a reviewer for the Journal *Energies*.

- Stefan Haar was a reviewer for *LMCS*, *MSCS*, *IEEE Transactions on Automatic Control* and *Journal of Discrete Event Dynamic Systems*.
- Stefan Schwoon acted as a reviewer for the following journals in 2016 : Fundamenta Informaticae, Transactions on Software Engineering.

9.1.4. Invited Talks

- Serge Haddad gave the following invited talks:
  - at the Joint AFSEC/ANR PACS workshop on May 26, 2016, Paris, France, on "Polynomial Interrupt Timed Automata";
  - at the VECOS 2016 conference, Tunis, Tunisia, on October 6, 2016, "Active Diagnosis";
  - at IDC 2016 (10th International Symposium on Intelligent Distributed Computing), October 11, 2016, Paris, France, on "Fault Diagnosis in Probabilistic Systems".
- Benedikt Bollig gave an invited tutorial at Highlights, Brussels, Belgium, 2016, on Automata and Logics for Distributed Systems

9.1.5. Research Administration

- Paul Gastin is one of the directors of the LIA INFORMEL.
- Stefan Haar is the head of the *SCILEX* axis within the *DIGICOSME* Labex. He was the Inria center of Saclay's correspondent for european partnerships until the summer of 2017, when he stepped down from this position to accept the presidency of Inria's COST-GTRI (international relations working group).
- Serge Haddad was a member of the recruitment committee for a professorship at INSA Toulouse.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Serge Haddad and Paul Gastin are professors at ENS Cachan (now ENS Paris-Saclay), Claudine Picaronny, Thomas Chatain and Stefan Schwoon are associate professors of the same university. Serge Haddad is the head of the Computer Science Department, and Stefan Schwoon is in charge of the L3 class. Claudine Picaronny is a co-director of the ENS Paris-Saclay's Mathematics department and a member of the juries of 'l'agrégation interne de Mathématiques' and of the second 'concours de Mathématiques' of ENS Cachan; she is also the coordinator of the mathematics/computer science examination of E3A, parts MP and MC.

Master : Benedikt Bollig, Non-sequential Theory of Distributed Systems, 36, M2, MPRI, ENS Cachan, France.

9.2.2. Supervision

Defended theses:

- PhD ([3])by Salim Perchy , 'Opinions, Lies and Knowledge. An Algebraic Approach to Mobility of Information and Processes', E´cole Polytechnique, defended October 4, supervised by Stefan Haar and Franck Valencia (COMETE team).
- PhD by Simon Theissing [4], 'Supervision for Multimodal Tranport Systems', ENS Cachan, defended December 5, supervised by Stefan Haar.

PhD in progress:

- Tymofii PROKOPENKO, Ecole Polytechnique since Oct 1, 'Privacy', jointly supervised by Catuscia Palamidessi (COMETE team) and Serge Haddad;
- Engel Lefaucheux, ENS Paris-Saclay since 2015, 'controlling information in probabilistic systems', jointly supervised by Nathalie Bertrand (SUMO team) and Serge Haddad

- Yann Duplouy, ENS Paris-Saclay since 2015,'application of formal methods to the development of embedded systems for autonomous vehicles', supervised by Béatrice Bérard and Serge Haddad. Marie Fortin (ENS Paris-Saclay since Oct 1); 'Tree-automata techniques for the analysis of distributed systems', co-supervised by Benedikt Bollig and Paul Gastin.
- Hugues Mandon (ENS Paris-Saclay since Oct 1, Digicosme Grant), Computational Models and Algorithms for the Prediction of Cell Reprogramming Strategies; supervised by Stefan Haar, co-supervision by Loic Paulevé (LRI).
- Robert Najvirt (TU Wien, Austrian FWF SIC project), *realistic delay models with applications in high-speed and low-power circuits*, co-supervised by Matthias Függer and Andreas Steininger.
- Martin Perner (TU Wien, Austrian FWF SIC project), *clock generation on-chip and formalisms suitable to prove correct VLSI circuits*, co-supervised by Matthias Függer and Ulrich Schmid.
- Juergen Maier (TU Wien, Austrian FWF SIC project), *on realistic delay models with applications in high-speed and low-power circuits, with focus on noise and high-order models*, co-supervised by Matthias Függer and with Ulrich Schmid.

9.2.3. Juries

- Benedikt bollig was
  - reviewer and jury member of the PhD thesis Logics on Data Words: Expressivity, Satisfiability, Model Checking by Ahmet Kara (Supervisor: Thomas Schwentick), Universität Dortmund, Germany, 2016, and
  - Reviewer of the PhD thesis Probabilistic Logic, Probabilistic Regular Expressions, and Constraint Temporal Logic by Thomas Weidner (Supervisor: Manfred Droste), Universität Leipzig, Germany, 2016
- Thomas Chatain was a member of the jury for the PhD defense of María Martos-Salgado, Universidad Complutense de Madrid, in January 2016.
- In addition to the juries of the two supervised students, Stefan Haar was the president of the jury for the PhD of Hassan Ibrahim, on 'SAT-based Diagnosability and Predictability Analysis in Centralized and Distributed Discrete Event Systems' at Université Paris-Sud on December 16.
- Serge Haddad was
  - a member of the juries for the PhD of Amira Methni on 'Méthodes de vérification de logiciel système critique", on July 7, 2016, at CNAM,
  - the president of the PhD jury for Hadrien Bride on "Verifying Modal Specifications of Workflow Nets" on October 24, 2016, at Université de Franche-Comté, and
  - a member of the HdR jury for Yann Thierry-Mieg, "From Symbolic Verification To Domain Specific Languages", on December 7, 2016, at Université Paris 6.

9.3. Popularization

- Stefan Haar gave a talk entitled 'Post hoc sed non propter hoc, or: why you should care about causality', in the Seminar@SystemX series of IRT SystemX on September 14, 2016.

10. Bibliography

Major publications by the team in recent years

[1] B. BARBOT, S. HADDAD, C. PICARONNY. *Coupling and Importance Sampling for Statistical Model Checking*, in "Proceedings of the 18th International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS'12)", Tallinn, Estonia, C. FLANAGAN, B. KÖNIG (editors), Lecture Notes in Computer Science, Springer, March 2012, vol. 7214, pp. 331-346, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BHP-tacas12.pdf

[2] S. HADDAD, J. MAIRESSE, H.-T. NGUYEN. *Synthesis and Analysis of Product-form Petri Nets*, in "Fundamenta Informaticae", 2013, vol. 122, n° 1-2, pp. 147-172, https://hal.archives-ouvertes.fr/hal-00925774

Publications of the year

Doctoral Dissertations and Habilitation Theses

[3] S. PERCHY. *Opinions, Lies and Knowledge. An Algebraic Approach to Mobility of Information and Processes*, Université Paris-Saclay, October 2016, https://hal.inria.fr/tel-01413970

[4] S. THEISSING. *Supervision in Multimodal Transportation Systems*, Université Paris-Saclay, December 2016, https://hal.inria.fr/tel-01419126

Articles in International Peer-Reviewed Journals

[5] É. ANDRÉ, T. CHATAIN, C. RODRIGUEZ. *Preserving Partial Order Runs in Parametric Time Petri Nets*, in "ACM Transactions on Embedded Computing Systems (TECS)", 2016, vol. 16, 25 p. [*DOI :* 10.1145/3012283], https://hal.inria.fr/hal-01425696

[6] M. GUZMAN, S. HAAR, S. PERCHY, C. RUEDA, F. VALENCIA. *Belief, Knowledge, Lies and Other Utterances in an Algebra for Space and Extrusion*, in "Journal of Logical and Algebraic Methods in Programming", September 2016 [*DOI :* 10.1016/J.JLAMP.2016.09.001], https://hal.inria.fr/hal-01257113

[7] S. HAAR. *Cyclic Ordering through Partial Orders* *, in "Journal of Multivalued-Logic and Soft Computing", September 2016, vol. 27, n° 2-3, pp. 209-228, https://hal.inria.fr/hal-01360144

[8] S. HAAR, S. HADDAD, T. MELLITI, S. SCHWOON. *Optimal constructions for active diagnosis*, in "Journal of Computer and System Sciences", 2017, vol. 83, n° 1, pp. 101-120 [*DOI :* 10.1016/J.JCSS.2016.04.007], https://hal.archives-ouvertes.fr/hal-01408047

[9] F. KORDON, H. GARAVEL, L. M. HILLAH, E. PAVIOT-ADET, L. JEZEQUEL, C. RODRÍGUEZ, F. HULIN-HUBARD. *MCC'2015 – The Fifth Model Checking Contest*, in "Transactions on Petri Nets and Other Models of Concurrency", 2016, vol. 9930, pp. 262-273 [*DOI :* 10.1007/978-3-662-53401-4_12], https://hal.inria.fr/hal-01361274

International Conferences with Proceedings

[10] S. AKSHAY, P. GASTIN, S. N. KRISHNA. *Analyzing Timed Systems Using Tree Automata*, in "27th International Conference on Concurrency Theory (CONCUR 2016)", Québec City, Canada, Proceedings of the 27th International Conference on Concurrency Theory (CONCUR 2016), Leibniz-Zentrum für Informatik, 2016, vol. 59, pp. 27:1–27:14 [*DOI :* 10.4230/LIPICS.CONCUR.2016.27], https://hal.archives-ouvertes.fr/hal-01407942

[11] N. BERTRAND, S. HADDAD, E. LEFAUCHEUX. *Accurate approximate diagnosability of stochastic systems*, in "10th International Conference on Language and Automata Theory and Applications", Prague, Czech Republic, Springer, March 2016, https://hal.inria.fr/hal-01220954

[12] N. BERTRAND, S. HADDAD, E. LEFAUCHEUX. *Diagnosis in Infinite-State Probabilistic Systems* , in "27th International Conference on Concurrency Theory (Concur 2016)", Québec city, Canada, 27th International Con-

ference on Concurrency Theory (Concur 2016), August 2016 [*DOI :* 10.4230/LIPIcs.CONCUR.2016.37], https://hal.inria.fr/hal-01373354

[13] M. Blondin, A. Finkel, C. Haase, S. Haddad. *Approaching the Coverability Problem Continuously*, in "22nd International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS 2016)", Eindhoven, Netherlands, Proceedings of the 22nd International Conference on Tools and Algorithms for Construction and Analysis of Systems (TACAS 2016), 2016, vol. LNCS 9636, pp. 480-496, https://hal.archives-ouvertes.fr/hal-01408044

[14] B. Bollig. *One-Counter Automata with Counter Observability*, in "36th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2016)", Chennai, India, Proceedings of the 36th IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS 2016), December 2016 [*DOI :* 10.4230/LIPIcs.FSTTCS.2016], https://hal.archives-ouvertes.fr/hal-01407932

[15] T. Chatain, J. Carmona. *Anti-Alignments in Conformance Checking - The Dark Side of Process Models*, in "37th International Conference on Applications and Theory of Petri Nets (PETRI NETS 2016)", Torún, Poland, Proceedings of the 37th International Conference on Applications and Theory of Petri Nets (PETRI NETS 2016), 2016, vol. LNCS 9698, pp. 240-258, https://hal.archives-ouvertes.fr/hal-01408043

[16] M. Fortin, P. Gastin. *Verification of parameterized communicating automata via split-width*, in "19th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS 2016)", Eindhoven, Netherlands, Proceedings of the 19th International Conference on Foundations of Software Science and Computation Structures (FoSSaCS 2016), 2016, vol. LNCS 9634, pp. 197-213, https://hal.archives-ouvertes.fr/hal-01408041

[17] S. Haar, S. Perchy, F. Valencia. *D-SPACES: Implementing Declarative Semantics for Spatially Structured Information*, in "11th International Conference on Semantic Computing", San Diego, California, United States, IEEE ICSC 2017, IEEE, January 2017, vol. 11, https://hal.inria.fr/hal-01328189

[18] J. Kolčák, D. Šafránek, S. Haar, L. Paulevé. *Unfolding of Parametric Logical Regulatory Networks*, in "The Seventh International Workshop on Static Analysis and Systems Biology (SASB 2016)", Edimbourg, United Kingdom, Electronic Notes in Theoretical Computer Science, Elsevier, September 2016, forthcoming, https://hal.archives-ouvertes.fr/hal-01354109

[19] B. F. Van Dongen, J. Carmona, T. F. Chatain. *A Unified Approach for Measuring Precision and Generalization Based on Anti-alignments*, in "14th International Conference on Business Process Management (BPM'16)", Rio de Janeiro, Brazil, Proceedings of the 14th International Conference on Business Process Management (BPM'16), September 2016, pp. 39 - 56 [*DOI :* 10.1007/978-3-319-45348-4_3], https://hal.archives-ouvertes.fr/hal-01406850

[20] B. van Dongen, J. Carmona, T. Chatain. *Alignment-based Quality Metrics in Conformance Checking*, in "7th International Workshop on Enterprise Modelling and Information Systems Architectures (EMISA'16)", Vienna, Austria, Proceedings of the 7th Int. Workshop on Enterprise Modelling and Information Systems Architectures (EMISA'16), October 2016, https://hal.archives-ouvertes.fr/hal-01406813

Conferences without Proceedings

[21] E. FABRE, L. HÉLOUËT, E. LEFAUCHEUX, H. MARCHAND. *Diagnosability of Repairable Faults*, in "13th International Workshop on Discrete Event Systems", Xi'an, China, 2016, pp. 256-262, (Version Longue), https://hal.inria.fr/hal-01302562

[22] S. HAAR, S. THEISSING. *Decoupling Passenger Flows for Improved Load Prediction*, in "13th International Conference on Quantitative Evaluation of SysTems (QEST 2016)", Québec City, Canada, August 2016, https://hal.inria.fr/hal-01330136

[23] S. HAAR, S. THEISSING. *Predicting Traffic Load in Public Transportation Networks*, in "2016 American Control Conference", Boston, United States, July 2016, https://hal.inria.fr/hal-01329632

[24] H. MANDON, S. HAAR, L. PAULEVÉ. *Relationship between the Reprogramming Determinants of Boolean Networks and their Interaction Graph*, in "Fifth International Workshop on Hybrid Systems Biology (HSB 2016)", Grenoble, France, E. CINQUEMANI, A. DONZÉ (editors), Lecture Notes in Computer Science, Springer International Publishing, October 2016, vol. 9957, pp. 113-127 [*DOI :* 10.1007/978-3-319-47151-8_8], https://hal.archives-ouvertes.fr/hal-01354079

Research Reports

[25] T. CHATAIN, J. CARMONA. *Anti-Alignments in Conformance Checking – The Dark Side of Process Models*, LSV, ENS Cachan, CNRS, Inria, Université Paris-Saclay, Cachan (France) ; Universitat Politècnica de Catalunya, Barcelona (Spain), January 2016, https://hal.inria.fr/hal-01267015

Other Publications

[26] T. CHATAIN, L. PAULEVÉ. *Goal-Driven Unfolding of Petri Nets*, October 2016, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01392203

[27] S. HAAR, S. THEISSING. *A Passenger-centric Multi-agent System Model for Multimodal Public Transportation*, May 2016, working paper or preprint, https://hal.inria.fr/hal-01322956

[28] S. HAAR, S. THEISSING. *Decoupling Passenger Flows for Improved Load Prediction*, March 2016, working paper or preprint, https://hal.inria.fr/hal-01294498

[29] S. HAAR, S. THEISSING. *Forecasting Passenger Loads in Transportation Networks*, January 2016, working paper or preprint, https://hal.inria.fr/hal-01259585

[30] S. HAAR, S. THEISSING. *Predicting traffic load in public transportation networks*, March 2016, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01286476

References in notes

[31] W. KUICH, H. VOGLER, M. DROSTE (editors). *Handbook of Weighted Automata*, EATCS Monographs in Theoretical Computer Science, Springer, 2009

[32] S. ABBES, A. BENVENISTE, S. HAAR. *A Petri net model for distributed estimation*, in "Proc. MTNS 2004, Sixteenth International Symposium on Mathematical Theory of Networks and Systems, Louvain (Belgium), ISBN 90-5682-517-8", 2004

[33] S. AKSHAY, N. BERTRAND, S. HADDAD, L. HELOUET. *The steady-state control problem for Markov decision processes*, in "Qest 2013", Buenos Aires, Argentina, K. R. JOSHI, M. SIEGLE, M. STOELINGA, P. R. D'ARGENIO (editors), Springer, September 2013, vol. 8054, pp. 290-304, https://hal.inria.fr/hal-00879355

[34] R. ALUR, K. ETESSAMI, M. YANNAKAKIS. *Realizability and Verification of MSC Graphs*, in "Theor. Comput. Sci.", 2005, vol. 331, n^{o} 1, pp. 97–114

[35] P. BALDAN, TH. CHATAIN, S. HAAR, B. KÖNIG. *Unfolding-based Diagnosis of Systems with an Evolving Topology*, in "Information and Computation", October 2010, vol. 208, n^{o} 10, pp. 1169-1192, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BCHK-icomp10.pdf

[36] P. BALDAN, A. CORRADINI, B. KÖNIG, S. SCHWOON. *McMillan's complete prefix for contextual nets*, in "Transactions on Petri Nets and Other Models of Concurrency", November 2008, vol. 1, pp. 199–220, Volume 5100 of Lecture Notes in Computer Science

[37] P. BALDAN, S. HAAR, B. KOENIG. *Distributed Unfolding of Petri Nets*, in "Proc.FOSSACS 2006", LNCS, Springer, 2006, vol. 3921, pp. 126-141, Extended version: Technical Report CS-2006-1. Department of Computer Science, University Ca' Foscari of Venice

[38] F. BASKETT, K. M. CHANDY, R. R. MUNTZ, F. G. PALACIOS. *Open, Closed, and Mixed Networks of Queues with Different Classes of Customers*, in "J. ACM", April 1975, vol. 22, pp. 248–260, http://doi.acm.org/10.1145/321879.321887

[39] A. BENVENISTE, É. FABRE, S. HAAR. *Markov Nets: Probabilistic Models for distributed and concurrent Systems*, in "IEEE Transactions on Automatic Control", 2003, vol. 48 (11), pp. 1936-1950, Extended version: IRISA Research Report 1538

[40] P. BHATEJA, P. GASTIN, M. MUKUND, K. NARAYAN KUMAR. *Local testing of message sequence charts is difficult*, in "Proceedings of the 16th International Symposium on Fundamentals of Computation Theory (FCT'07)", Budapest, Hungary, E. CSUHAJ-VARJÚ, Z. ÉSIK (editors), Lecture Notes in Computer Science, Springer, August 2007, vol. 4639, pp. 76-87 [*DOI :* 10.1007/978-3-540-74240-1_8], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BGMN-fct07.pdf

[41] G. V. BOCHMANN, S. HAAR, C. JARD, G.-V. JOURDAN. *Testing Systems Specified as Partial Order Input/Output Automata*, in "Proc. TESTCOM/Fates 08, 20th IFIP International Conference on Testing of Communicating Systems and 8th International Workshop on Formal Approaches to Testing of Software", LNCS, Springer, 2008, vol. 5047, pp. 169-183

[42] B. BOLLIG, P. GASTIN. *Weighted versus Probabilistic Logics*, in "Proceedings of the 13th International Conference on Developments in Language Theory (DLT'09)", Stuttgart, Germany, V. DIEKERT, D. NOWOTKA (editors), Lecture Notes in Computer Science, Springer, June-July 2009, vol. 5583, pp. 18-38 [*DOI :* 10.1007/978-3-642-02737-6_2], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BG-dlt09.pdf

[43] A. BOUILLARD, S. HAAR, S. ROSARIO. *Critical paths in the Partial Order Unfolding of a Stochastic Petri Net*, in "Proceedings of the 7th International Conference on Formal Modelling and Analysis of Timed Systems (FORMATS'09)", Budapest, Hungary, J. OUAKNINE, F. VAANDRAGER (editors), Lecture Notes in Computer Science, Springer, September 2009, vol. 5813, pp. 43-57 [*DOI :* 10.1007/978-3-642-04368-0_6], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BHR-formats09.pdf

[44] P. BOUYER, S. HADDAD, P.-A. REYNIER. *Timed Unfoldings for Networks of Timed Automata*, in "Proceedings of the 4th International Symposium on Automated Technology for Verification and Analysis (ATVA'06)", Beijing, ROC, S. GRAF, W. ZHANG (editors), Lecture Notes in Computer Science, Springer, October 2006, vol. 4218, pp. 292-306, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/BHR-atva06.pdf

[45] TH. CHATAIN, P. GASTIN, N. SZNAJDER. *Natural Specifications Yield Decidability for Distributed Synthesis of Asynchronous Systems*, in "Proceedings of the 35th International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM'09)", Špindlerův Mlýn, Czech Republic, M. NIELSEN, A. KUČERA, P. BRO MILTERSEN, C. PALAMIDESSI, P. TŮMA, F. VALENCIA (editors), Lecture Notes in Computer Science, Springer, January 2009, vol. 5404, pp. 141-152 [*DOI :* 10.1007/978-3-540-95891-8_16], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/CGS-sofsem09.pdf

[46] G. CHIOLA, C. DUTHEILLET, G. FRANCESCHINIS, S. HADDAD. *Stochastic Well-Formed Colored Nets and Symmetric Modeling Applications*, in "IEEE Transactions on Computers", November 1993, vol. 42, n^{o} 11, pp. 1343-1360, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PS/CDFH-toc93.ps

[47] A. CHURCH. *Logic, arithmetics, and automata*, in "Proc. of Int. Congr. of Mathematicians", 1962, pp. 23–35

[48] R. DEBOUK, D. TENEKETZIS. *Coordinated decentralized protocols for failure diagnosis of discrete-event systems*, in "Journal of Discrete Event Dynamical Systems: Theory and Application", 2000, vol. 10, pp. 33–86

[49] D. EL HOG-BENZINA, S. HADDAD, R. HENNICKER. *Process Refinement and Asynchronous Composition with Modalities*, in "Proceedings of the 2nd International Workshop on Abstractions for Petri Nets and Other Models of Concurrency (APNOC'10)", Braga, Portugal, N. SIDOROVA, A. SEREBRENIK (editors), June 2010, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/EHH-apnoc10.pdf

[50] J. ESPARZA, K. HELJANKO. *Unfoldings - A Partial-Order Approach to Model Checking*, EATCS Monographs in Theoretical Computer Science, Springer, 2008

[51] É. FABRE, A. BENVENISTE, C. JARD, S. HAAR. *Diagnosis of Asynchronous Discrete Event Systems, a Net Unfolding Approach*, in "IEEE Trans. Aut. Control", 2003, vol. 48 (5), pp. 714-727

[52] É. FABRE, A. BENVENISTE, C. JARD, S. HAAR. *Distributed monitoring of concurrent and asynchronous systems*, in "Discrete Event Dynamic Systems: theory and application", 2005, vol. 15 (1), pp. 33-84, Preliminary version: Proc. CONCUR 2003, LNCS 2761, pp.1–28, Springer

[53] B. FINKBEINER, S. SCHEWE. *Uniform distributed synthesis*, in "Proc. of the 20th IEEE Annual Symposium on Logic in Computer Science (LICS'05)", IEEE Computer Society Press, 2005, pp. 321–330

[54] P. GASTIN, B. LERMAN, M. ZEITOUN. *Distributed games with causal memory are decidable for series-parallel systems*, in "Proceedings of the 24th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'04)", Chennai, India, K. LODAYA, M. MAHAJAN (editors), Lecture Notes in Computer Science, Springer, December 2004, vol. 3328, pp. 275-286, http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/GLZ-fsttcs04.pdf

[55] P. GASTIN, N. SZNAJDER, M. ZEITOUN. *Distributed synthesis for well-connected architectures*, in "Proceedings of the 26th Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'06)", Kolkata, India, N. GARG, S. ARUN-KUMAR (editors), Lecture Notes in Computer Sci-

ence, Springer, December 2006, vol. 4337, pp. 321-332 [*DOI :* 10.1007/11944836_30], http://www.lsv.ens-cachan.fr/Publis/PAPERS/PDF/GSZ-fsttcs2006.pdf

[56] S. HAAR, A. BENVENISTE, É. FABRE, C. JARD. *Partial Order Diagnosability Of Discrete Event Systems Using Petri Net Unfoldings*, in "42nd IEEE Conference on Decision and Control (CDC)", 2003

[57] S. HAAR. *Probabilistic Cluster Unfoldings*, in "Fundamenta Informaticae", 2003, vol. 53 (3-4), pp. 281-314

[58] S. HAAR, C. JARD, G.-V. JOURDAN. *Testing Input/Output Partial Order Automata*, in "Proc. TESTCOM/FATES", LNCS, Springer, 2007, vol. 4581, pp. 171-185, LNCS 4581

[59] O. KUPFERMAN, M. Y. VARDI. *Synthesizing Distributed Systems*, in "Proc. of the 16th IEEE Annual Symposium on Logic in Computer Science (LICS'01)", IEEE Computer Society Press, 2001

[60] S. LAFORTUNE, Y. WANG, T.-S. YOO. *Diagnostic Decentralisé Des Systèmes A Evénements Discrets*, in "Journal Europeen des Systèmes Automatisés (RS-JESA)", August 2005, vol. 99, n^{o} 99, pp. 95–110

[61] K. G. LARSEN, P. PETTERSSON, W. YI. *Compositional and symbolic model-checking of real-time systems*, in "Proc. of RTSS 1995", IEEE Computer Society, 1995, pp. 76-89

[62] S. MOHALIK, I. WALUKIEWICZ. *Distributed Games*, in "Proc. of the 23rd Conference on Foundations of Software Technology and Theoretical Computer Science (FSTTCS'03)", LNCS, Springer, 2003, vol. 2914, pp. 338–351

[63] A. PNUELI, R. ROSNER. *Distributed reactive systems are hard to synthesize*, in "Proc. of the 31st Annual IEEE Symposium on Foundations of Computer Science (FOCS'90)", IEEE Computer Society Press, 1990, vol. II, pp. 746–757

[64] L. RICKER, K. RUDIE. *Know Means No: Incorporating Knowledge into Discrete-Event Control Systems*, in "IEEE Transactions on Automatic Control", September 2000, vol. 45, n^{o} 9, pp. 1656–1668

[65] L. RICKER, K. RUDIE. *Knowledge Is a Terrible Thing to Waste: Using Inference in Discrete-Event Control Problems*, in "IEEE Transactions on Automatic Control", MarchSeptember 2007, vol. 52, n^{o} 3, pp. 428–441

[66] C. RODRÍGUEZ, S. SCHWOON, V. KHOMENKO. *Contextual Merged Processes*, in "34th International Conference on Applications and Theory of Petri Nets (ICATPN'13)", Italy, Lecture Notes in Computer Science, Springer, 2013, vol. 7927, pp. 29-48 [*DOI :* 10.1007/978-3-642-38697-8_3], https://hal.archives-ouvertes.fr/hal-00926202

[67] H. L. S. YOUNES, R. G. SIMMONS. *Statistical probabilistic model checking with a focus on time-bounded properties*, in "Inf. Comput.", September 2006, vol. 204, pp. 1368–1409 [*DOI :* 10.1016/J.IC.2006.05.002], http://dl.acm.org/citation.cfm?id=1182767.1182770