Project Acronym	**PACE**		
Project title (in French)	**P**rocessus non-standard: **A**nalyse, **C**oinduction, et **E**xpressivité		
Project title (in English)	beyond plain **P**rocesses: **A**nalysis techniques, **C**oinduction and **E**xpressiveness		
Multidisciplinary project	☐ YES ☒ NO		
Type of research	☒ Basic Research ☐ Industrial Research		
International cooperation	International cooperation with: ☐ Autriche ☐ Brésil FAPESP ☐ Brésil FACEPE ☐ Canada ☒ Chine ☐ Hong Kong ☐ Mexique ☐ Portugal ☐ Roumanie ☐ Taïwan		
Total funding requested **For French Partners** **For Foreign Partners**	€338416 €120000	**Project duration**	48 months

1. EXECUTIVE SUMMARY

Coinduction, expressiveness and analysis techniques are three fundamental ingredients in theories of concurrent processes. Coinduction is a tool used to define processes and to reason about them. The most widely applied coinductive concept is bisimulation: bisimilarity is used to study behavioural equalities, and the bisimulation proof method is used to prove such equalities. The study of expressiveness is motivated by the variety of process models, process constructs, behavioural equalities. An expressiveness framework is necessary to formally assess and compare this variety, and to separate the primitive concepts from the derived ones. Expressiveness can also shed light on language implementation; for instance when comparing a linguistic construct with other primitives, more directly implementable. Finally, analysis techniques bring in methods and tools to prove behavioural properties.

The three notions above - coinduction, expressiveness, analysis techniques - are at the heart of PACE. **Our objective is to enrich and adapt these methods, techniques, and tools to much broader forms of interactive models, well beyond the realm of "traditional" processes.** Specifically, we target models exhibiting one or more of the following features: probabilities, higher-order, quantum, constraints, knowledge, and confidentiality. These models are becoming increasingly more important for todays' applications. Although calculi for these formalisms have already been introduced, they are

much more complicated than ordinary processes and several foundational aspects still need to be investigated. Coinduction is intended to play a pivotal role in the project. As a consequence, we shall focus on approaches to expressiveness that are based on coinductive equalities, and on analysis techniques for coinductive notions.

The objectives related to coinduction are twofold. First, we will investigate coinduction in paradigms in which this concept is not yet settled, such as quantum processes, probabilistic higher-order processes, and metrics (to compute the behavioural distance between processes). Secondly, we aim at developing a general and unifying theory of enhancements of the bisimulation proof method (called "up to techniques"). The theory should be applicable to a broad range of languages in the paradigms studied in the project. The theory should be algebraic, enabling the composition of different enhancements into more sophisticated ones, and should shed light on the meaning of soundness for the enhancements. Applications of coinduction to security and confidentiality will also be investigated.

In the realm of expressiveness, first we aim at establishing a general theory of expressiveness for the paradigms investigated in the project, starting from the pioneering work on expressiveness for ordinary processes carried out by members of the project. Second, we will consider specific applications of the framework. In particular, we shall investigate the relative expressiveness of operators for describing distributed common knowledge, inspired by existing constructs in concurrent constraints, epistemic logics, probabilistic process calculi, distributed process calculi. We shall also test the expressiveness criteria in security scenarios where the goal is to guarantee the protection of private or confidential information.

Concerning the techniques and algorithms for analysis, we shall look for methods for automated or semi-automated analysis of processes, using the coinductive techniques introduced in the project, such as bisimulation enhancements, symbolic characterisations, or approximations of bisimulations. We aim at finding both correct and complete algorithms for various fragments of the considered calculi, but also generic tools and procedures allowing a user to prove complex properties by relying on powerful analytical tools, when the considered problem is not decidable.

2. CONTEXT, POSITION AND OBJECTIVES OF THE PROPOSAL

2.1. CONTEXT, SCIENTIFIC, SOCIAL AND ECONOMIC ISSUES

The rapid development of computer network and communication technology plays an important role in the emerging dynamics of social, economic and environmental change. To further enhance this development requires systematic methodologies for constructing highly reliable and secure software systems, which calls for foundational research on specifying, analyzing and verifying programs. In modern computation paradigms such as concurrent, probabilistic, and quantum computing, the programs rapidly become so complex and intricated that it is a pressing issue to discover tractable techniques to reason about them, in order to ensure reliable and secure functioning of systems.

2.2. POSITION OF THE PROJECT

Concurrency theory studies the description and the analysis of systems made of interacting processes. Processes are usually thought of as infinite objects, in the sense that they can produce arbitrary and possibly endless patterns of interactions with their environment. In a model of processes, a central notion is that of behavioural equivalence, which stipulates when two processes are indistinguishable. Defining processes and equality on them and reasoning on processes and their equalities therefore means dealing with, and comparing, infinite structures. For this, a widely used mathematical tool is **coinduction**. Coinduction is the dual of induction. While induction is a pervasive tool to reason about finite and stratified structures, coinduction offers similar strenths on structures that are circular or infinite.

A peculiar aspect of concurrency is the variety of ways to formalise the notion of process. Varieties emerge in all aspects of the formalisation: the way processes interact (via synchronous or asynchronous messages, shared variables, broadcasting, etc), the equalities imposed on them (bisimulation, branching bisimulation, simulation, failures, testing, etc), the operators used to compose processes (parallelism operators, disabling operators, hiding operators, etc.), the values exchanged (first-order values such as integers and booleans, channels, code and processes), the meaning of action (probabilities, time, quantum, etc). As a consequence, another fundamental activity in concurrency is the study of **expressiveness**. This means comparing models/languages and comparing constructs; but before that, it means finding the criteria for stipulating the outcome of a comparison. Expressiveness criteria and expressiveness results often rely on the notions of equality adopted for the processes (to reduce a process to an equivalent one, to map the equality on a model to the equality on another model).

A third fundamental issue in concurrency concerns the **analysis techniques**. That is, methods and tools to decide equivalence between behaviours, or more generally to prove behavioural properties of a concurrent system. The tractability of a technique is important: we need techniques which make proofs shorter, and reduce the number of cases to be examined when analysing a behaviour. Tools may be derived out of the techniques, to permit automatic or semi-automatic analysis (i.e., theorem prover formalisation of proofs).

The three above aspects - coinduction, expressiveness, analysis techniques - represent huge research topics. They have produced a large body of work and successful stories, that sometimes have even affected other areas of computer science. The introduction of coinduction itself is part of the story, since coinduction was discovered in concurrency, and has then been exported and used in several other areas, both within computer science (type theory, domain theory, databases, program verification, etc.), and outside it (mathematics, artificial intelligence, modal logic, epistemic logic, philosophy, etc.).

In the literature, the processes that are usually treated only interact by pure synchronisation, or they exchange first-order values (i.e., values made out of integers, booleans, as in CCS; or channels, as in the pi-calculus). These processes are called “plain” in this proposal. In PACE, we propose to examine coinduction, expressiveness, analysis techniques in the following specialised scenario, where we go beyond plain processes.

First we shall focus on a few emerging process paradigms, arising from the description of modern systems. More precisely, each language of processes examined will include one or more of these features:

- higher-order capabilities, that is the possibility of exchanging values that may include process terms; this means that the language will have constructs for abstractions (binders) that are supposed to be instantiated with code;
- probabilistic behaviours, to account for randomisation in distributed implementations or algorithms, to model fairness, to measure the reliability of a system or its performance, to quantify information leakage;
- quantum behaviour, to express processes working according to the postulates of quantum computing;
- distributed constraints, to model global or partially global information;
- spatial and epistemic features, for applications to social networks and cloud computing, and to model confidentiality properties.

Second, we shall restrict ourselves to coinduction, which is intended to play a pivotal role in the PACE project. As a consequence, we focus on approaches to expressiveness that are based on coinductive equalities; and we focus on analysis techniques that are specific to coinduction, that is, intended to help us in proving coinductive properties on the systems of interest.

Partners' Skills. The researchers involved in PACE are experts in concurrency theory, and have contributed to the development of the methods that are at the heart of this project. Indeed, the consortium puts together expertise in different points of view about coinduction (coinduction and bisimulation, proof techniques for bisimulation, coalgebras, quantitative versions of coinduction), expressiveness (expressiveness results about concurrent calculi, expressiveness criteria, unifying approaches for expressiveness), and analysis techniques (algorithms for bisimulation checking, symbolic and open bisimulations, partition refinement).

There are several research groups working on topics studied in PACE, either because they contribute to the techniques we plan to use, or because they address models of computation we are interested in, from a point of view that is more or less close to ours.

Relation with other ANR Projects. Some researchers involved in PACE are also working for the ANR project "PiCoq", which is about the formal verification of distributed components. We expect that some of the results in Task 3 could be useful for the PiCoq project. The PACE proposal addresses however more foundational questions than PiCoq (we work on models of computation rather than on the description of specific systems such as distributed components).

The ANR project "PANDA" (Parallel ANd Distributed Analysis) project ends in Sept. 2012. Its goals are also less foundational than the present proposal. We do not really expect results from the Panda project to be directly usable for PACE.

The ANR project "REVER" (Programming reversible recoverable systems) has in common with this project a focus on process calculi for concurrent computation. One of the scientific goals of REVER is to study behavioural equivalences for reversible systems. It is quite plausible, thus, that advances made in PACE could be used by researchers involved in REVER, to reason about reversible systems.

To the best of our knowledge, there are no other projects funded by the ANR that address questions related to the ones we put forward in this proposal.

European and International Competitors. We are not aware of other projects, at an international level, that address the questions we want to attack. There is, to our knowledge, no project focusing on the use of coinduction and/or expressiveness as its main tools.

The ERC Grant awarded to G. Winskel (Cambridge) for a project entitled *"Events, Causality and Symmetry - the next generation semantics"* focuses on denotational semantics (in particular, event structures and game semantics), and envisages the study of aspects of systems that we also want to analyse (quantitative properties, quantum). We believe that the mathematical tools we want to use provide an angle rather distinct from G. Winskel's project.

The group of J. Rutten at CWI (Netherlands) works actively on coinduction. Some interactions with people of this group (who already collaborate with F. Bonchi, from the Lyon site) are expected to occur along the development of our project (also, we might invite researchers from this group at project meetings). We can mention in particular the project "Practical Coinduction" (with D. Kozen's group at Cornell University, 2012-2016), whose main aim is to use the theory of coalgebras and Kleene algebras for the automatic verification of quantitative and probabilistic systems, interactive systems and advanced functional programs.

The Australian ARC Grant awarded to Ying, Y. Feng and R. Nagarajan (UTS, Australia) for a project entitled "Process algebra approach to distributed quantum computation and secure quantum communication" focuses on the development of appropriate quantum process algebra to model quantum systems and the study of model-checking problems. In PACE, we are more concerned about the co-inductive proof techniques to reason about quantum processes that may exhibit infinite behaviour. The study of quantum bisimulation would be interesting for both projects, and we expect some collaboration to happen.

2.3. STATE OF THE ART

Up-to Techniques

One of the main reasons for the success of bisimilarity is the strength of the associated proof method. A number of enhancements of the bisimulation proof methods have been put forward in the literature, with the goal of establishing bisimilarity results using "small" relations. Indeed, the enhancements allow proofs of bisimilarity using relations that are just **contained** in a bisimulation. These enhancements are referred to as `up-to techniques' [Mil89,SW01].

In certain languages, e.g., languages for mobility such as pi-calculus or higher-order languages such as Higher-Order pi-calculus [SW01] or Ambients [MZ05], the enhancements seem essential to obtain any non-trivial bisimilarity result. Moreover, in these languages bisimulation relations are usually enriched with an environment that collects the observer knowledge on the values exchanged with the processes. The appearance of environments brings up several additional forms of up-to techniques for manipulating them: e.g., techniques for shrinking or enlarging the environment, and techniques for replacing information in the environment (based for instance on subtyping) [SKSS11]. Proposals of bisimulation also have been made in which certain up-to techniques are so to say “hardwired” into the definition of bisimulation, precisely because of their importance in proofs [KW06]. [San98,Pous08] present attempts at developing algebras of enhancements, so to be able to compose enhancements, and derive the soundness of complex techniques; see [PS12] for a tutorial. These attempts only consider first-order labelled transitions systems (in which labels are uninterpreted actions, as in CCS).

Probabilistic and Higher-Order Languages

Randomized computation is central to several areas of theoretical computer science, including computational complexity, cryptography and the analysis of computation dealing with uncertainty. Bisimulation has been studied on probabilistic CCS-like languages or on mobile process calculi à la pi-calculus [Pana12]. Very little exists on higher-order languages, even the sequential ones. The majority of the literature on probabilistic functional programming views probability as a monad, in the sense of Moggi. An alternative and more direct way is to endow the lambda calculus with probabilistic choice, namely by enriching it with a binary choice, this way obtaining a probabilistic extension of pure, untyped lambda calculus. Lambda calculi for quantum computation can also be defined, based on constructions coming from linear logic [vT04,SV06,DlMZ09]. Noticeably, the well-known techniques allowing to tame the operational semantics of deterministic higher-order calculi and to relate it with bisimulation (e.g. Howe’s technique) have not been studied in the probabilistic nor in the quantum setting at the time of writing.

Quantum Processes

The theory of quantum computing has attracted considerable research efforts in the past twenty years. Benefiting from the superposition of quantum states and linearity of quantum operations, quantum computing may provide considerable speedup over its classical analogues [Sho94, Gro96,Gro97]. In view of the success that classical process algebras [Mil89,Hoa85,BW90] achieved in analyzing and verifying classical communication protocols, several research groups proposed various quantum process algebras [JL04,GN05,YFDJ09] with the purpose of modeling quantum communication protocols.

Although various notions of bisimulation have been proposed for quantum processes [FDJY07, YFDJ09,FDY11,GN05], the development of quantum process coinductive techniques is in its infancy. In particular, we are not aware of any algorithm that can decide quantum bisimulation, even for finite processes. An important reason is that almost all quantum bisimulations rely on the instantiation of quantum variables by arbitrary quantum states, which is intractable because all quantum states constitute a continuum.

Inspired by the idea of symbolic bisimulation developed in value-passing CCS and the pi-calculus [HL95,San96], Yuxin Deng and colleagues have obtained some preliminary results on open

bisimulations for quantum processes [FDY11]. If efficient algorithms can be found for checking symbolic bisimulation, they would open up an opportunity for tool development so as to help us with verifying behavioural equivalences of quantum processes.

Behavioural Metrics

The growing interest in quantitative properties has motivated the definition of quantitative models [Sch61,Rab63,Var85,PZ86,GJS90,SS90,LS91,SL94,GSS95,DG05] and related notions of behavioural equivalences [LS91,CSZ92,SL94,JY95,Buc08]. For many quantitative properties, equivalences are somehow inadequate since they only allow "boolean reasoning": either two systems are equivalent or they are not.

Motivated by these considerations, many authors have recently proposed several behavioural metrics or closely related notions [GJS90,DGJS04,BW05,AHM03,DCPP06,BSW08,DJGP02, GP07]. Differently from the ordinary equivalences, behavioural metrics express the distance between the behaviours of systems: if the distance is 0, then the systems are behaviourally equivalent.

Protection of Confidential Information

The protection of private or confidential information is one of the most compelling concerns in the modern information society, and has been an active area of research since some decades already. Reasoning about confidentiality is quite tricky: the situations in which the problem of confidentiality arises usually involve the presence of various agents interacting with each other, hence the setting is typically concurrent, with all the complexity that concurrency implies. Furthermore, the prevention of information leakage is an extremely difficult task, not only to achieve, but even to formalize: facts are often correlated in subtle ways and it is hard to predict what an adversary may infer from an apparently harmless piece of information.

There have been several proposals for formalisms to reason and verify secrecy. One of the most successful was the one by Abadi and Gordon [AG99]. They advocated the use of a variant of the pi-calculus to express the concurrent nature of protocols and systems, and the use of bisimulation to express secrecy. The idea is that a system S protects a secret value if the system S' that we obtain by substituting such value with another one is indistinguishable from (i.e. it is bisimilar to) S. This simple but ingenious idea has shown to be quite fertile and flexible: varius other works have adapted it to formalize a large variety of confidentiality properties [DKR06,DKR09,Co11].

In real systems it is practically impossible to prevent the leakage of information entirely, and for this reason it has been recognized that it is important to be able to quantify the amount of leakage. Quantitative approaches to information flow have been gaining popularity in recent years, we mention in particular those based on information theory [CHM05,Ma07,Sm09,BPP11,AAP12]. Also in this context process calculi and bisimulation (in this case, in their probabilistic variants) have been applied successfully, in particular by Palamidessi and her colleagues in the context of anonymity [BP05,APRS10,CPB12]. Natural extensions of this approach, using distances instead of equivalences, have been investigated by Dung, Pend and Wu [DPW06], and by Cai [Ca09, CG09].

Reasoning about Social Networks

In order to reason about and verify systems such as social networks, we need to be able to express concepts like information, space and knowledge.

Process calculi for dealing with information have been already considered in the literature. One of the most prominent representatives is concurrent constraint programming (CCP) [SRP91] where agents/processes interact with each other by adding and asking information in a global store. The most distinctive and appealing feature of CCP is that it unifies the operational view of processes based upon process calculi with a declarative one based upon first-order logic.

Nevertheless, the notion of a single centralized global store makes CCP unsuitable for modeling concurrent systems where information and processes can be shared or spatially distributed among

certain groups of agents. Spatial relationships and distributed knowledge cannot be faithfully expressed in a global store. Compelling examples include the increasingly popular social networks such as Facebook, Google+ and Twitter, as well as cloud store tools such as Dropbox. They can be viewed as huge concurrent systems with information distributed and shared among groups and applications. These networks raise important challenges such as the design and analysis of techniques to predict and prevent privacy breaches.

The partners of Bologna and Paris have provided CCP languages with proof techniques for verification [GPV10]. Furthermore, partners in Paris are currently developing a conservative extension of CCP, designed for social networks. The issue of extending CCP with a distributed notion of a store has been previously addressed in [BJPV09,BM07,Ret98]. None of the above extensions is, however, conservative in the sense that they no longer provide a logical view of processes. Furthermore, the extended processes do not have the traditional (closure-operator) semantics of CCP which is one of the sources of its elegance and simplicity.

Expressiveness in Concurrency.

In concurrency theory, several guiding principles and cogent classification criteria have been put forth in numerous works (e.g., [BGZ09,Gor08,GSV04,Nes97,Par08,Pal03,VPP05]). They consider questions such as whether a given variant can express certain behaviours, or whether a given fragment is as hard for some property as the full language. These expressiveness questions are of great interest as a variant may simplify the presentation of the calculus, be tailored to specific applications, or be used to single out important aspects of the calculus.

The partners from Bologna, Shanghai and Paris are among the main contributors to the study of expressiveness in concurrency. For instance, Palamidessi showed that one cannot encode the synchronous pi-calculus into the asynchronous one [Pal03], and one cannot encode the monadic pi-calculus into the zero-adic one [Pal06]. Similarly, replication is strictly less expressive than recursion in the zero-adic pi-calculus [BGZ09] and static scoping of local variables is also strictly less expressive than dynamic scoping in the zero-adic pi-calculus [GSV04].

Despite the research done in this area, there is not yet a general agreement as to which properties a taxonomy of process calculi must consider, in the way we have for the linguistic formalisms of computability, where the well-known notion of language (generation) can be taken as the canonical measure for expressiveness. Nevertheless, the Chinese partners have recently developed a robust process theory of equality and expressiveness [Fu12], as an extension of the standard recursion theory of computable functions. Because of its generality and coherence, their theory is suitable for conducting expressiveness studies of the models we propose.

Minimisation, Finite Automata Theory, and Concurrency

Minimization algorithms have been first introduced for finite automata [Brz62]. In particular, the partition-refinement method [Hop71] has been extensively exploited in concurrency theory. For instance, it has been applied to labeled transition systems (for CCS) [KS90] or to History Depended automata (for pi-calculus) w.r.t. different notions of equivalence (such as open [PS96] and asynchronous [MP99] bisimilarity). Its wide applicability can been easily explained in terms of "coalgebras", as shown in [FMT05, BM09 Sta09, ABHKMS12].

F. Bonchi and others recently looked at the initial Brzozowski algorithm from a more abstract perspective, to build extensions of it [BBRS12]; but there are currently no known minimisation algorithms for the kind of non-traditional processes we consider in PACE.

Algorithms for checking non deterministic finite automata universality and inclusions have been designed using the concept of antichain [WDHR06,ACHMV10]. F. Bonchi and D. Pous recently proposed an improved algorithm for this problem, by exploiting an up-to congruence technique [BP12]. Such up-to congruence techniques have also been used in the past to obtain decidability results for various classes of context-free grammars [Caucal90,CHS95].

Algorithms for Process Equivalence

Some algorithms have been proposed and implemented for checking the equivalence of CCS processes or pi-calculus processes (see, e.g., the concurrency [MS90] and mobility [VM94] workbenchs). These implementations are unmaintained, rather old, focused on a particular choice of processes and equivalences. On the contrary, the CADP toolbox [GLM01] is actively maintained; it consists in a rather large variety of tools and algorithms for studying processes, from trace-equivalence and bisimilarity checking to minimisation, visualisation, and model-checking. However, this toolbox is designed to work on first-order labelled transition systems, which precludes higher-order or quantum processes and probabilistic systems. In both cases, they do not exploit up-to techniques or advanced coinductive methods.

Similarly, algorithms for metrics have been studied for metrics which "discount the future" [DGJP04, BW06], and general on-the-fly algorithms have been introduced in [BSW08]. However, none of these algorithms exploit possibilities offered by up-to techniques.

2.4. OBJECTIVES, ORIGINALITY AND INNOVATIVE NATURE OF THE PROJECT

The techniques and the concepts which are at the heart of the PACE project are not new per se. Our objective is rather to enrich and adapt them to much broader forms of interactive models, well beyond the realm of “traditional” processes. Specifically, we target models encompassing one or more features such as higher-order abstractions, probabilites, distributed constraints, quantum. These models are becoming increasingly more important for todays' applications. Although calculi for these formalisms have been introduced some years ago, they are much more complicated than ordinary processes and there are several foundational aspects still to be investigated.

Our proposal focuses on two main concepts: conduction and expressiveness. On the one hand, coinduction is the most natural and powerful approach to define and reason about infinite or circular structures and computations, bringing in tools and methods that are dual and complementary to those of induction. In particular, coinduction is central in concurrency, where processes are naturally seen as entities that continuously interact with their environment. Coinduction, in the form of bisimulation, is used to define equality between processes, and the coinduction proof method, in the form of the bisimulation proof method, is employed to prove such equalities.

On the other hand, expressiveness is a central concern in concurrency because of the broad variety of process models and process operators. A framework is necessary to formally assess and compare this variety: to make sure that a ``new'' paradigms is really new, but also to individuate the interesting part of it, and separating for instance the basic linguistic constructs from the derived ones. A model needs to be as ``clean'' and simple as possible, in order to investigate its foundations without being distracted by unnecessary features. CCS and the pi-calculus, with a design based on a few orthogonal operators, are good examples of this strategy.

The objectives related to coinduction are twofold. First, we wish to investigate basic concepts of coinduction in paradigms in which these concepts are not yet settled. Quantum processes, probabilistic higher-order processes, and probabilistic metrics for computing the behavioural distance among processes are examples. Secondly, we aim at developing a general theory of enhancements of the bisimulation proof method. The theory should be applicable to a broad range of languages, with particular reference to the languages in the paradigms studied in the project. (The significance and importance of the enhancements is described in Section 2.3.) That is, we aim at a unifying framework in which several, apparently quite different, forms of enhancements can be accommodated, and enabling one to derive soundness of the enhancements but also to compose different enhancements into more sophisticated ones. This should substantially reduce the effort needed to prove process equalities, and may lead to new algorithms for automated or semi-automated verification.

In the realm of expressiveness, first, we aim at establishing a general theory of expressiveness, applicable to the paradigms investigated in PACE. For this, we shall lift Fu's recent expressiveness framework for ordinary processes [Fu12a-d]. The cases of quantum processes and of processes with

distributed constraints and partial knowledge appear particularly challenging. Besides the definition of the framework itself, the challenge here is also to explore the tradeoff between the expressiveness of a formalism and the decidability of behaviourial properties (equality, but also reachability, for instance). In Fu's framework, the key ingredients are coinductive notions such as bisimilarity equality and codivergence. Thus the relationship with the work on coinduction will be strong. A further novelty here will be the application of the expressiveness framework to implementations or interpreters of languages. Whenever feasible we shall carry out comparisons with other approaches to expressiveness, notably Palamidessi's [Pal97], and Gorla's [Gor08]. We expect that new criteria for assessing expressiveness (in addition to the standard ones, such as the interaction capabilities) will have to be introduced. In particular, we intend to consider the security properties of a system, and specifically the capability of guaranteeing the protection of private or confidential information. These properties are typically formulated in terms of (probabilistic) knowledge, hence we expect that in order to carry over this novel line of research the standard class of problems used to asses interaction capabilities (dining philosophers, leader election etc.) will not be sufficient, and a new class of problems of epistemic and/or probabilistic nature will have to be devised.

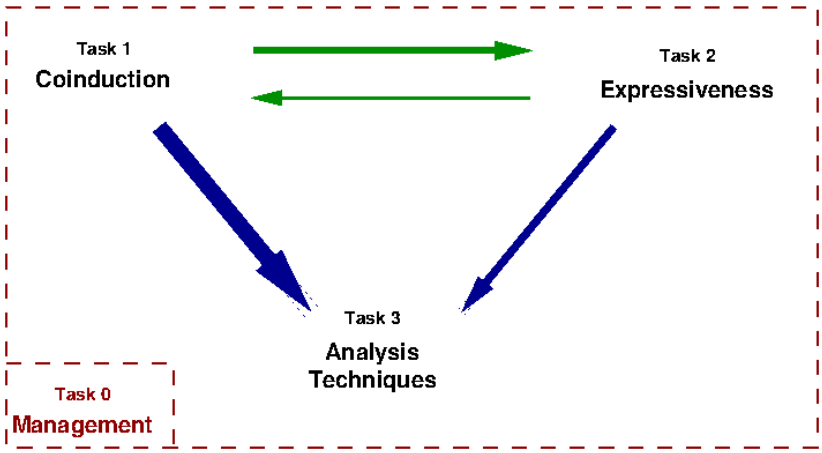
On analysis techniques, the general objective is to develop algorithmic presentations of the coinductive notions studied in PACE. First, we shall study the integration of bisimulation enhancements into algorithms for the analysis of processes. In existing tools for bisimulation verification, up-to techniques play a minor role (e.g., they may be used to identify two states up-to the garbage collection of terminated processes). The usefulness of up-to techniques seems however higher in the paradigms investigated in PACE, such as higher-order concurrency. We will also develop semi-automated tools for assisting the development of proofs based on bisimulation enhancements. Secondly, we will produce symbolic characterisations of bisimulations, with fewer transitions emanating for the processes and with more effective checks in the bisimulation clauses. This line of work will be particularly relevant for quantum processes, in which existing bisimulations involve an heavy mechanism of variable instantiation. When exact symbolic characterisations cannot be obtained, we shall consider symbolic approximations. We expect that this will be necessary for higher-order probabilistic languages; symbolic versions, in the "open" or "normal form" style, might be related to tree representation of terms (e.g., Levy-Longo trees for the lambda calculus). Related to this line of work, we shall study minimisation algorithms for symbolic bisimulations. The difficulty here is that symbolic bisimulations are usually asymmetric (e.g., the labels of matching transitions need not be identical), hence standard minimisation algorithms are not applicable.

3. SCIENTIFIC AND TECHNICAL PROGRAMME, PROJECT ORGANISATION

3.1. SCIENTIFIC PROGRAMME, PROJECT STRUCTURE

The diagram below sums up the overall organisation of the PACE project. The contributions we want to obtain in each task, as well as the relationships between the tasks, are explained in the follwing sections (the "thickness" of arrows is an indication for the measure of the dependency).

Task 0 is devoted to management (see Sect. 3.2 below). The three scientific tasks have relations between them that are explained in Sections 3.3 (Description by task) and 3.4 (Task schedule). In overview, the contributions of Task 1 and Task 2 will help designing new analysis methods for processes that combine features like higher-order, probabilistic, constraints, quantum, etc. As the diagram shows, we expect Task 1 to play a more important role than Task 2 in providing new analysis techniques. Tasks 1 and 2 are interdependent, Task 2 focusing on linguistic constructs for which we need to introduce behavioural equivalences (Task 1).



3.2. PROJECT MANAGEMENT

Coordinator of the PACE project: Daniel Hirschkoff (Lyon site).

A special task, Task 0, will take care of project management. This will consist in

- monitoring exchanges, visits, and, more generally, scientific collaboration between the partners involved in PACE. This will be done jointly with the Task coordinators.
- planning and organising the two PACE symposia, one in France and one in Shanghai.
- preparing the project deliverables.

For this task, D. Hirschkoff, as coordinator of the Lyon site, will be helped by coordinators for the INRIA site (D. Sangiorgi) and the BASICS site (Y. Fu). Overall, considering that the project involves relatively few sites, we expect Task 0 to be lightweight.

3.3. DESCRIPTION BY TASK

For each sub-task below, we give the involved partners within brackets. The order in which they appear represents their degree of involvement.

3.3.1 TASK 1: ADVANCED COINDUCTIVE TECHNIQUES

Task leader: Davide Sangiorgi **Deputy Task leader:** Xu Xian

T1.1 Up-to techniques [INRIA,Lyon,Shanghai]

We have explained in earlier sections the importance of up-to techniques. Three further aspects for them need to be emphasized. First, up-to techniques need to be composed, to yield more powerful techniques. Secondly, the proof of validity of a technique, particularly if it is a composed one, can be tedious, and delicate. Thirdly, the form of possible bisimulation enhancements (and their validity) is very specific to the language under consideration and to the definition of bisimulation (for instance, if the definition of bisimulation uses environments, as in higher-order languages or typed languages, then one needs up-to techniques for manipulating these). Indeed it may even happen that a certain technique is valid in a language but then breaks in extensions of it [PS12]. Hence, the theory of enhancements for a language must be carefully scrutinised and (at best) refined if the language is modified. The variety of enhancements represents a richness but at the same time is a major obstacle to their applicability: a certain enhancement could alleviate the work needed to obtain a bisimilarity result, but one prefers not to adopt the enhancement because of the work needed to prove (or dispove) its soundness. This needed work can be particularly discouraging when the up-to technique is the composition of more basic techniques. Another obstacle to the applicability of up-to techinques is the lack of tool support for them.

A major goal in this subtask is to develop a general theory of up-to techinques and corresponding tool support. The theory should be applicable to a broad range of languages, including languages for mobility such as the pi-calculus, higher-order languages such as the Higher-Order pi-calculus but also lambda-calculi with references, languages for security such as spi-calculus and applied pi-calculus. It should allow us to infer easily, for a certain language and definition of bisimilarity, whether a given enhancement is valid, possibly exploiting basic properties of the bisimilarity such as transitivity and congruence. Moreover, the theory should tell us whether and how two given techniques can be combined into a more powerful techinque. Finally, the theory should be applicable to both strong forms of bisimulation and weak forms.

We shall investigate the possibility of mapping the non-standard LTSs needed for the processes examined in the project to first order (CCS-like) LTSs, so to transfer the metatheories of up-to techniques, e.g., [Pou08]. We shall first look at higher-order languages, for which a number of specific up-to techniques have been proposed. In the setting of (typed and sequential) higher-order languages, we will also compare the strength of the proof techniques provided by the enhancements of the bisimulation proof method against that given by logical relations. There has been a good deal of progress in recent years in adapting bisimulation and logical relations to ML-like languages; combinations of them have also been proposed recently [KDNV12]. Still, we believe that the possibilities offered by bisimulation can be considerably strengthened via bisimulation enhancements. We will also study the possibility of transplanting the methods based on logical relations onto concurrent languages.

In certain classes of processes, e.g., probabilistic processes and quantum processes, or for certain form of bisimulation, e.g., metric bisimulations, the investigation of bisimulation and coinduction is still in the early stages, and up-to techniques have not been considered yet. In these areas, our investigation of bisimulation enhancements will first aim at identifying what are the potentially useful forms of enhancement and the proof techniques needed for their soundness. On these aspects, the models seem particularly challenging. We expect that the differences will have a strong impact on the theory of enhancements.

Later, but more speculatively, we will study metatheories for enhancements. Enhancements will be studied also in connection with metrics, see below.

T1.2 From Equivalences to Metrics [Lyon, INRIA and Shangai]

The general goal of this subtask is to study if and when the coinductive methods and techniques developed for equivalences can be lifted to metrics. More specifically, we will consider the following aspects.

Behavioural metrics provide a useful proof technique for over-approximating the behavioural distance between two systems. Indeed, it is sometimes enough to check that the distance between two systems is bounded by some threshold rather than knowing the exact distance. Metric bisimulations have been already the subject of some preliminary studies (e.g. [DCPP06,BSW08]). We would like to obtain a more general treatment with the help of the theory of coalgebras [Rut00], that provides an abstract definition of bisimulation [AM89].

A fundamental property when dealing with behavioural equivalences is compositionality and, indeed, a lot of efforts have been spent in defining general frameworks for guaranteeing it [Sim85,TP97,GM99,LM00, BKM06,BM08,HJS08]. In the setting of metrics, compositionality is related to non-expansiveness [DGJP04]. We aim at defining some abstract criteria for ensuring non-expansiveness by extending existing frameworks [TP97,HJS08] to metric spaces.

Developing up-to techniques for metric bisimulations is a challenging task since classical up-to techniques, such as up-to equivalence, cannot be naively extended to metrics. For instance, we should generalize “up-to transitivity” (which is meaningless for metrics) to “up-to triangular inequality”. We

will also investigate the relationship between "metric bisimulations up-to context" and "non-expansiveness of metrics".

We intend to apply the result of this study (non-expansiveness and up-to techniques) to confidentiality. First we will lift the bisimulation-based approach to secrecy by Abadi and Gordon [AG99] to bisimulation metrics, thus moving from a qualitative approach to a more informative quantitative one. Then we will consider concrete examples in which the non-expansiveness conditions hold, thus ensuring compositionality of secrecy properties. Furthermore, we will investigate the benefits of using up-to techniques in the context of confidentiality. We expect, in particular, to be able to model more sophisticated properties. The setting of confidentiality protocols will also be a good source of examples to check the efficiency of the proposed up-to techniques.

T1.3 Probabilistic and quantum higher-order languages [INRIA ,Shangai]

As explained in Section 2.3, little exists on the bisimulation semantics of probabilistic or quantum higher-order languages. We shall approach this problem by first examining the simpler sequential setting of the lambda-calculus. Later, we shall look at concurrency.

We aim at finding a notion of probabilistic applicative bisimulation suitable for the probabilistic untyped lambda calculus, starting from the works by Larsen and Skou on discrete probabilistic bisimulation [LS91] and by Abramsky on applicative bisimulation for the lazy lambda calculus [A90]. We will then analyse in which relation probabilistic applicative bisimulation is with the obvious generalization of Morris-style contextual equivalence to the probabilistic setting, namely the one in which two terms are defined to be equivalent if the probability of converging is the same in every possible context. To obtain compositionality of the bisimilarity, we will look at the generalizations of Howe's method to deal with probabilities. An alternative could be to adopt the idea of environmental bisimulation [SKS11], for which compositionality is simpler.

Once these correspondence results have been proved for the plain, probabilistic, lambda calculus, one can go beyond and look for similar theorems for quantum lambda calculi [SV06,DLMZ09].

T1.4 Quantum processes [Shanghai,INRIA]

A major objective is to study notions of bisimulation for quantum processes that are amenable to algorithmic verification. In particular, we shall look for symbolic characterisations, to alleviate the problem of the infinity of all quantum states. For this we shall first consider a quantum extension of value-passing CCS (qCCS). We will investigate super-operator valued distributions, which can potentially be used to fold the operational semantics of qCCS into a symbolic version where, to check the bisimilarity of two quantum processes, only a finite number of process super-operator pairs need to be considered - without appealing to concrete quantum states.

T1.5 Spatial-epistemic CCP [INRIA,Shanghai,Lyon]

We are investigating spatial-epistemic CCP models (see Section 2.3), for the specification of agents posting and querying information in systems with spatial hierarchies for sharing information and knowledge. A natural notion of observable behaviour for the spatial processes of this calculus involves information constructed as a limit of finite approximations. These limits may result in infinite (or non-compact) objects involving arbitrary nesting of spaces, infinite data structures, or epistemic specifications such as common-knowledge. We believe that coinduction techniques should help in analyzing the observable behaviour of such processes. We expect to avoid complex concepts such as fairness and limits by replacing them with simpler algebraic reasoning, i.e., showing that some property is preserved by one step of the approximation and then infer, by the co-induction principle, that the property also holds for the infinite limit object [Koz06].

3.3.2 TASK 2: EXPRESSIVENESS

Task leader: Yuxi Fu **Deputy Task leader:** Catuscia Palamidessi

The general objective of this task is the development of a general and coherent theory for expressiveness applicable to the paradigms investigated in PACE, and of expressive power taxonomies for such models. More specific goals include establishing the foundations of a theory of expressiveness for process calculi unifying interaction and confidentiality issues, and comparing the discrimination power of our approaches with the ones currently used in the literature. In connection with Task 1, Task 2 will help us to simplify the presentation of a model, to tailor it to specific applications, and to single out its fundamental aspects. In connection with Task 3, it may also give us insights about efficient decision procedures for properties of the models.

T2.1 Absolute Theory [Shanghai, INRIA]

There are two fundamental relations in process theory, the expressiveness relation between models and the equality relation between the processes of a model. A model independent characterization of these two relations is of paramount importance. We have developed a process theory, hereafter called Theory of Interaction [Fu12a-d,FZ12], based on the two universal relations (absolute equality and sub-bisimilarity). A coherent theory of equality, expressiveness and completeness has been established. Both the absolute equality and the sub-bisimilarities make use of the coinduction technique in a very abstract fashion since one has to develop a proof technique that is essentially model independent. Our coinduction takes care of divergence by imposing what we call codivergence condition. Using the apparatus developed in Theory of Interaction, we have studied the basic recursion theory of processes and the nondeterministic structure of computation. The former is based on an approach of defining universal processes in a complete model. The latter makes full use of our definition of completeness and reveals that in all Turing-Milner models the nondeterministic structures are the same.

Our primary goal here is to test the robustness of the above framework by testing it on the paradigms investigated in PACE. This should also provide feedback on the framework itself, improving our understanding of the dimensions of the absolute equality and sub-bisimilarity and their roles in applications. For this, whenever feasible we shall make comparisons with other approaches to expressiveness in the literature, some of which developed by members of PACE [BGZ09, Gor08, GSV04, Nes97, Par08, Pal03, VPP05].

In certain cases, notably with quantum processes, finding the suitable model-independent notion of absolute equality is a research issue on its own. In other cases, notably higher-order concurrency, absolute equality can be readily applied. Then it will be interesting to compare this equality, defined using the model independent coinductive approach, to the ones defined using a more concrete coinductive approach (as in Task 1).

Another important concern here is the relationship with implementations. There has been quite a number of translations from programming languages to process models. Walker's interpretation of POOL into the pi-calculus is a leading example. These translations however do not offer any implementations. If one thinks of pi-calculus as a machine model, an implementation of say POOL in pi-calculus is an interpreter of the former in the latter. The interpreter should be able to pick up (the code of) a source program and execute the (encoded) program. Our introduction of universal processes makes it possible to study implementations into process models. We plan to carry out a project to implement the (industrial) higher-order concurrent language Erlang (a core of it, to begin with) into a more basic first-order process model. The goal is to showcase the importance of the theoretical developments (absolute equality, expressiveness, completeness) to the programming theory of process models.

Recently, there has been great efforts [HDNV12,KFF12] for developing composable inter-language equivalences (bisimulations, simulations) to reason about the equality between concurrent programs in different languages. We believe that a model-independent method will help. Therefore, absolute equality and sub-bisimilarity of concurrent languages might be candidates for such kind of equivalences. And the most challenging task is to investigate how to efficiently verify these equivalences.

T2.2 Expressivenes in Social Networks [INRIA, Lyon, Shanghai]

New application domains, such as social networks, present several aspects that cannot be expressed with the traditional process calculi, and require the introduction of new concepts. E.g., we need to specify agents posting and querying information in presence of spatial hierarchies for sharing information and knowledge. In PACE we intend to investigate the addition of spatial and epistemic operators to process calculi, in particular CCP (cf. Section 2.3), its applications to security and confidentiality, and the implications for expressiveness.

The spatial operator may specify a process, or a local store of information, that resides within the space of a given agent (e.g., an application in some user's account, some private data shared with a specific group). The epistemic operator may specify that the information computed by a given process will be known to a given agent. To the best of our knowledge, other process calculi can only express these epistemic concepts and the spatial distribution of information indirectly.

These new operators can give rise, in the hiding-free fragment, to complex and meaningful epistemic and spatial specifications, as well as data-structures that are inherently infinite. We conjecture, however, that fundamental properties such as behavioral equivalence and reachability may be decidable in this hiding-free spatial-epistemic CCP due to certain regularities we have observed in its underlying transition system. Investigating these conjecture will provide us with crucial insights about the limitations, redundancies and capabilities of our calculus and it may also provide us decision procedures for analyzing the behaviour of a meaningful class of systems under consideration.

Another interesting aspect that distinguishes social networks from traditional concurrent models is that, when a new information is published, it is distributed according to a publish-subscribe mechanism. This mechanism is closer to a selective broadcast than to the traditional point-to-point interaction considered in traditional process calculi like CCS or the pi-calculus. As already observed in [DSZ10], the spatial distribution of the nodes communicating by means of selective broadcast has an impact on the classical results on the expressive power of broadcast communication studied, for instance, in [EFM99] for broadcast protocols Interestingly, in [DSZ10] it is also shown a strong relationship between selective broadcast and foundational results on graph theory, like the study on the induced subgraph ordering by Ding [D92]. We plan to use similar techniques to investigate, from a foundational point of view, the impact on the expressive power of the new interaction mechanisms typical of social networks.

Our goals are thus to identify and classify significant fragments of the spatial-epistemic calculus capable of expressing meaningful situations in social networks, and to establish the (un)decidability of central behavioural properties for these fragments. We plan to use the theory of well-structured transition systems to derive decidability results for behavioural properties such as those mentioned above. As with other models of PACE, we shall also use the framework in Task 2.1, Theory of Interaction, to determine what cannot be expressed in the full language of spatial-epistemic CCP.

T2.3 Applications to Privacy, Confidentiality, and Anonymity [INRIA, Shangai]

As argued before, process calculi can be used as a specification language to represent (a) systems and protocols which aim at protecting confidential information, (b) external or internal attackers, and (c) security properties. Consequently, the expressiveness of the process calculus has impact on our specifications at all these three levels.

More precisely, the notion of absolute equality, described in Task 2.1, will be important to express security properties which need to equate adversaries in different models (for instance, to represent the fact that having a certain capability does not increase the attacking power of the adversary with respect to a given security property).

We also intend to explore the theory of expressiveness underlying Task 2.1 in the context of confidentiality. We expect the theory to be sound, in the sense that the expressiveness distinctions based on interaction capabilities will carry over when security concerns are taken into account.

However we also expect that security will introduce more distinctions between formalisms to express systems, protocols, and adversaries. Hence one of the goals of this task is to refine the theory so to establish adequate foundations for reasoning about the expressiveness of formalisms for secure concurrent systems.

The topics of Task 2.2 also bear a strong interest for privacy, confidentiality, and anonymity. The common denominator of these properties is that certain information should not be *known* by certain entities. Hence epistemic formalisms are the natural frameworks for expressing these properties. The addition of epistemic and spatial capabilities to CCP is therefore very appealing, because it will provide a unique formalisms where we can specify concurrent behaviour, and dynamic evolution of knowledge, both in time and space (where "space'' is intended in the large sense of spatial calculi. In our case we are mainly interested in the accessibility of information from a certain location/ambient). We also intend to study the particular setting of social networks as a source of concrete examples of situations in which privacy concerns arise, and are intertwined with concurrency an spatial issues.

The goals here are as follows. (a) To establish the foundations of a theory of expressiveness for process calculi unifying interaction and confidentiality issues. (b) To study the applicability of the theory of absolute equivalence developed in Task 2.2 to the framework of confidentiality properties. (c) To investigate the expressiveness of the spatial-epistemic calculus with respect to confidentiality properties.

The activities of this task will proceed in parallel with those of Tasks 2.1 and 2.2. The idea is that this task will build on the results of the tasks above, but also provide input for them in terms of examples and perspective. In particular, for the case of the spatial-epistemic calculus, the examples stemming from confidentiality scenarios are among the most natural to test the expressiveness of the operators, and we expect therefore a strong intertwining between these two tasks.

3.3.3 TASK 3: ANALYSIS TECHNIQUES

Task leader: Damien Pous **Deputy Task leader:** Yuxin Deng

The objective in this task is to develop computational tools for the coinductive notions studied in PACE, following three main strands. First, the integration of bisimulation enhancements into algorithms for the analysis of processes, including algorithms for metrics bisimulations and codivergence checking. Second, verification algorithms for symbolic forms of bisimulations. Thirdly, minimisation algorithms for symbolic bisimulations.

T3.1 Algorithms relying on up-to techniques [Lyon, INRIA, Shanghai]

Up-to techniques have been used in the past to obtain decidability results for various classes of processes [Caucal90,CHS95]. More recently, F. Bonchi and D. Pous discovered that up to techniques could be used to drastically improve standard algorithms for checking language equivalence of non-deterministic finite automata (NFA) [BP12]. Indeed, while standard methods require to first determinise the automata, yielding an exponential blow-up, one can use an "up to congruence" technique to cut a lot of branches in this state-space.

We plan to pursue this work in several directions, to apply these ideas to a wider range of both models and coinductive objects.

For models, we would like to investigate whether up-to techniques that are specific to probabilistic languages, like "up to probabilistic distribution", can be turned into concrete and efficient algorithms. Similarly, a challenging problem is to isolate fragments of higher order calculi such that specific techniques like "up to environment" can yield decidability of contextual equivalence (cf. T1.1). Last, in the case of spatial-epistemic calculi (cf. T1.5, T2.2), we would like to use up-to techniques to reduce the state-space explored by standard algorithms, by exploiting the complete lattice structure of the underlying order.

For coinductive objects, while there are standard tools concerning strong and weak bisimilarity (e.g., CADP and the concurrency and mobility workbenchs), very few concern other forms of equivalences

like branching or progressing bisimulations; we would thus like to fill this gap by providing appropriate and efficient algorithms for these relations. We also plan to study algorithms for reachability, codivergence, and other coinductive properties. Indeed, up-to techniques could reveal themselves as extremely useful for these problems. For instance, the efficient antichain-based algorithm proposed in [CAV06] for checking universality of NFA can be seen as a coinductive algorithm exploiting an up-to congruence technique [BP12].

The study of algorithms for branching bisimilarity and codivergence proposed in this sub-task are particularly important in the PACE project: these notions play a central role in the generic framework to be developed by Shangai in T2.1 Moreover, while we usually need to consider fragments of the considered calculi to obtain decidability results and effective algorithms, we also plan to develop semi-automated tools for assisting the search for proofs based on bisimulation techniques. Such tools are typically required in a proof assistant like Coq, where we should alleviate as much as possible the end-user work.

T3.2 Up-to techniques in algorithms for Metrics [Lyon, Shanghai]

Equivalence of finite automata can be checked either via minimisation [Hop71,Brz62], or via “on-the-fly” algorithms [HK71,AHU74]. While minimization algorithms compute the largest bisimulation, on-the-fly algorithms check the equivalence of only two given states: they iteratively attempt to build a bisimulation equating them, constructing a least fixed-point rather than the largest one.

These two approaches can be extended to labeled transition systems [KS90,FM92]. However, when moving from equivalences to metrics, they happen to be quite different. Greatest fixed-point computations give as result the behavioural distance, while on-the-fly algorithms attempt to build a metric bisimulation (see T1.2) that just provides an over approximation of the distance. In the case of behavioural metrics, the first approach is effective only for metrics which "discount the future" [DGJP04, BW06]. Indeed, for metrics without discount, computing the greatest fixed-point would require infinitely many iterations. For avoiding this problem, an on-the-fly algorithm is introduced in [BSW08], relying on Tarski’s decision procedure [Tar51] for the first order theory over reals.

We plan to investigate how the up-to techniques developed in T1.2 for metrics can be used to improve such minimisation and on-the-fly algorithms. For instance, we want to exploit the triangular inequalities which hold for such metrics, to reduce the state-space.

T3.3. Algorithms for quantum bisimulations [Shanghai, Lyon, INRIA]

With the existing notions of bisimulation for quantum processes, checking whether two processes are bisimilar requires instantiating their free quantum variables with arbitrary quantum states, and to verify that the resultant configurations are bisimilar. This makes checking bisimilarity infeasible from an algorithmic point of view, because quantum states constitute a continuum. We plan to exploit the symbolic operational semantics and the up-to techniques proposed in T1.4 for quantum processes to develop efficient algorithms to check if two such processes are equivalent.

In particular, the ability to combine both a symbolic operational semantics, and specific up-to techniques like "up to superposition of quantum states" should make it possible to obtain decidability for a non-trivial fragment of qCCS (or other quantum process algebra - see T1.4). An auxiliary but important question will then be to characterise the expressive power of this decidable fragment, which we will answer using the tools developed in T2.

As an extension of this subtask, we shall also study algorithms for observational equivalence of quantum versions of the lambda-calculus [vT04,SV06,DLMZ09], where the combination of both higher order and quantum states seems particularly challenging.

T3.4 Minimization algorithms for symbolic bisimulation [Lyon, INRIA]

Symbolic bisimilarity, as proposed in [HL95,San96] and exploited in other tasks of PACE, make it possible to avoid an intractable universal quantification over all possible contexts (or instantiations)

into which systems can be embedded. Unfortunately, symbolic bisimilarity has an asymmetric shape: in the bisimulation game, when a player proposes a transition, the opponent can answer with a move with a different label. For this reason, the standard minimization algorithm [KS90] cannot be reused for symbolic bisimilarity. Inspired by [PS96,MP99] who developed ad hoc minimization algorithms for open and asynchronous bisimilarity, the authors of [BM09] introduced an abstract framework describing a general minimization algorithm for symbolic bisimilarity. This framework encompasses many formalisms and has also allowed the implementation of a minimization algorithm for concurrent constraint programming [ABPPV11,ABPV12] (see T1.5).

In this task we would like to study minimization algorithms for weak symbolic semantics. Indeed, while it suffices to "saturate" [SR12] the labeled transition system for standard weak bisimilarity, this is not enough for weak symbolic semantics [VM94]. As a first step, we would like to develop a minimization algorithm for the weak semantics of CCP and qCCS (see T1.3, T1.4). We hope that these case studies will make it possible to define an abstract algorithm in a more general framework.

3.4. TASK SCHEDULE, DELIVERABLES AND MILESTONES

The three scientific tasks of PACE will proceed mostly in parallel. However the role of Task 3, on analysis, will be minor during year 1, as the main activities in the task depend on results to be produced elsewhere, notably the coinductive techniques of Task 1.

Task 1 plays a pivotal role in the project. The results and methods defined in the task will be the main subject of the analysis in Task 3. Task 2 will complement the other two tasks. However, it will also affect their development. If the study on expressiveness brings up the interest of certain languages or certain linguistic constructs, then these languages and constructs will also be scrutinized and analyzed in the other two tasks. Conversely, the outcomes of Task 1 may drive some of the work in Task 2: for instance, the study of expressiveness makes use of coinductive notions of behavioural equivalence; also, if some promising coinductive technique is found for certain linguistic operators, then we will want to understand their expressive power.

We plan to hold two general project meetings ("symposia"), one in France and the other one in China; the first at mid-term, the second towards the end of the project. These will be complemented by a number of task-specific meetings, which will be organized on a by-need basis, and by regular visits among the different partners and teams. Each task has a coordinator, who is in charge of ensuring the correct development in the task and monitoring the relationship with the other two tasks.

The table below summarizes the allocation of resources (man.months) from each partner to each task. Lyon has some extra resources allocated for project management. We intend to keep management fairly lightweight. In the table, figures between parentheses correspond to manmonths provided by non-permanent members of PACE (these include the 36 months of "PACE postdocs", funded by the ANR for the french partners).

Partner	Task 1	Task 2	Task 3	Total
Lyon	31(+18)	5	22(+12)	58(+30)
INRIA	14(+21)	28(+27)	6(+15)	48(+63)
Shanghai	40(+30)	31(+38)	37(+30)	108(+98)
Total	95(+69)	59(+65)	70(+57)	214(+191)

We plan to provide each year deliverables that reflect the progress on each task. More specifically, we plan to provide three deliverables each year, in addition to a short annual Project Report. Each deliverable will be a report summarizing the results obtained during the year, a discussion on their relevance to the project goal and objectives, and the publications produced. We give below a summary description of these deliverables.

Deliverables for Task 1

Year 1.

- D1.1.1 A metatheory of bisimulation enhancements for pure Higher-Order pi-calculus with only process passing
- D1.1.2 Accounts of metric bisimulations using coalgebras
- D1.1.3 A probabilistic bisimulation for untyped lambda-calculus along the lines of applicative bisimulation
- D1.1.4 Symbolic characterisations of strong bisimulation on a quantum CCS

Year 2.

- D1.2.1 A metatheory of bisimulation enhancements applicable to several higher-order calculi, ranging from the full Higher-Order pi-calculus to the lambda calculus with or without references.
- D1.2.2 Definition of some abstract criteria for ensuring non-expansiveness of metrics for ensuring compositionality
- D1.2.3 A form of environmental bisimulation for the probabilistic lambda-calculus and for the higher-order pi-calculus
- D1.2.4 Weak versions of the symbolic bisimulation for quantum CCS
- D1.2.5 Definition of labelled transition system and of a contextual form of bisimulation (barbed congruence) for the spatial-epistemic CCP.

Year 3.

- D1.3.1 Comparison between bisimulation enhancements and methods based on logical relations for higher-order imperative languages.
- D1.3.2 Concrete bisimulation enhancements for probabilistic and quantistic bisimulations.
- D1.3.3 A metatheory of bisimulation enhancements for languages with information hiding mechanisms (types, security primitives)
- D1.3.4 Environmental bisimulation for a probabilistic Higher-Order pi-calculus
- D1.3.5 Symbolic forms of bisimulation on extensions of CCS, possibly pi-calculus-likex
- D1.3.6 Definition of a labelled bisimilarity for the spatial-epistemic CCP that should coincide with contextual bisimulation

Year 4.

- D1.4.1 Attempts at a metatheory of bisimulation enhancements for probabilistic and quantistic bisimulations.
- D1.4.2 Enhancements for metric bisimulation
- D1.4.3 Proposal for a bisimulation for quantum lambda-calculus, possibly also a symbolic characterisation of it, and an attempt at transporting these onto some higher-order process calculus
- D1.4.4 A study of the application of up-to bisimulations and metric bisimulations to confidentiality.

Deliverables for Task 2.

Year 1.

- D2.1.1 Extend Fu's expressiveness framework to probabilistic processes and higher-order processes. There should be several coincidence results relating the model independent equivalence to the concrete equivalence.

D2.1.2 An implementation of Erlang into a more basic first-order process model.
D2.1.3 A model-independent equivalence based on subbisimilarity for reasoning about inter-language equivalences
D2.1.4 Proof that hiding-free fragments of the spatial-epistemic language are not Turing complete.

Year 2.
D2.2.1 Extend Fu's expressiveness framework to other paradigms, including quantum processes and spatial-epistemic processes.
D2.2.2 Proof systems for absolute equality on some of the PACE paradigms.
D2.2.3 Expressiveness results for PACE paradigms (e.g., on higher-order concurrency or probabilistic processes) using subbisimilarity.
D2.2.4 Comparisons between Fu's expressiveness framework and more traditional frameworks.
D2.2.5 A first classification of the interaction mechanisms typical of social networks based on expressiveness

Year 3.
D2.3.1 A reasoning system for Erlang based on the process implementation.
D2.3.2 A theory of inter concurrent programming language equivalence, including congruence property and axiom systems.
D2.3.3 Foundations of a theory of expressiveness for process calculi unifying interaction and confidentiality

Year 4.
D2.4.1 Applications of well-structured transition systems and expressiveness frameworks to derive (un)decidability results on languages of the PACE paradigms
D2.4.2 Completeness results of some PACE paradigms.
D2.4.3 Expressiveness taxonomy for non-standard models based on interaction and confidentiality.

Deliverables for Task 3.

Year 1.
D3.1.1 Finite automata algorithms based on up-to techniques
D3.1.2 Basic algorithms for probabilistic bisimulation for untyped lambda-calculus

Year 2.
D3.2.1 Mechanised tools for standard up-to techniques in higher-order languages
D3.2.2 Basic algorithms for metric bisimulations
D3.2.3 Basic algorithms for symbolic strong bisimulation on a quantum CCS
D3.2.4 Algorithms for branching bisimulation and codivergence checking

Year 3.
D3.3.1 Algorithms for weak symbolic bisimulations,
D3.3.2 Minimisation algorithms

Year 4.
D3.4.1 Advanced algorithms for metrics, symbolic, and quantum bisimulations, using up-to techniques
D3.4.2 (possibly, depending on the results of the project) prototype implementations of some of our analysis techniques

Milestones.

The milestones of the project correspond to the above deliverables. In Task 1, the deliverables at Year 1 are particularly important, since the start of many activities in Task 3 depend on them. Also important, but less critical, are the deliverables at Year 2. In Task 2, the deliverables at Year 1 is

central as it lays the foundations for the expressiveness studies for following years. Similarly, the deliverable of Year 3 with the foundations for expressiveness studies based on confidentiality is fundamental for the studies in Year 4. In Task 3, the basic algorithms in the deliverables for Year 2 are the most important milestones, since they correspond to the first step towards the integration of advanced up-to techniques, during Year 3.

4. DISSEMINATION AND EXPLOITATION OF RESULTS, DATA MANAGEMENT. INTELLECTUAL PROPERTY

We expect our results to be the subject of articles in international journals and to be presented at international conferences. Typical journals are: Information and Computation, Theoretical Computer Science, Mathematical Structures in Computer Science, Logical Methods in Computer Science. Typical conferences are: POPL, LICS, CONCUR, ESOP, ICALP, FOSSACS.

We plan to distribute the implementation of the algorithms produced in Task 3 under the Gnu Public Licence (GPL).

Links with higher education. On the occasion of the symposium organised in Lyon, we plan to organise a one week-research school focusing on the research themes of PACE. This event could be hosted by the Masters in Computer Science of École Normale Supérieure de Lyon, which proposes such scientific events every year in the curriculum of its students (see the page http://www.ens-lyon.fr/DI/?cat=19). Such research schools are usually attended by PhD students, researchers, as well as the Masters students of ENS Lyon; most of the latter plan to make a PhD in computer science after their Masters studies, and are thus a public of choice for such an event.

There are no issues related to intellectual property in the PACE project.

5. CONSORTIUM DESCRIPTION

5.1. DESCRIPTION, SUITABILITY AND COMPLEMENTARITY OF THE PARTNERS. NECESSITY AND ADDED VALUE OF THE INTERNATIONAL COOPERATION

BASICS, the Laboratory for **Ba**sic **S**tudies **i**n **C**omputer **S**cience, is a research laboratory under the auspices of the Education Commission of Shanghai Government. It gathers researchers across the universities in Shanghai who work on fundamental aspects of computer science. Researchers of Basics participating to the project provide expertise in models for higher-order concurrent computation (Fu, Xu and Cai), probabilistic and quantum process calculi (Deng), expressiveness (Fu) and analysis techniques (Li).

INRIA is the French National Institute for Research in Computer Science and Control. Two INRIA teams will be involved in the project, Comete and Focus.

Comete. The research of the Comete team focuses on the theoretical foundations of concurrent and distributed languages. The team provides expertise in expressiveness, in probabilistic versions of process calculi, and in the analysis of confidentiality properties.

Focus. The Focus research team is part of INRIA Sophia Antipolis site, with most membes physically located at the University of Bologna. The Focus members broadly study models, languages and techniques for distributed systems. Sangiorgi, head of Focus, has expertise on various topics investigated in the project, particularly higher-order concurrency (where he has made some pioneering contributions), and coinduction (he has recently published a book on coinduction, and edited another book on more advanced topics of coinduction). Other permanent members of Focus taking part in this project are Zavattaro, who is an expert in questions related to expressiveness and decidability, Dal Lago, who is working on models for probabilistic and quantum computation, Gabbrielli, an expert in concurrent constraints.

The **ENSL** (École Normale Supérieure de Lyon) is one of the best *grandes écoles* (higher education institutions) in France. The Plume research group of ENSL will act as coordinator for the project. Researchers of Plume are interested in the semantics of programming language and in proof theory. Permanent members of Plume who participate in this project are specialised in the study of concurrent systems. D. Hirschkoff and D. Pous work on questions of expressiveness and on proof techniques for coinductive proofs, with an interest in the mechanisation of these proofs. Along these lines, D. Pous and F. Bonchi also study algorithms for the decision of coinductively defined behavioural equivalences. F. Bonchi also brings an expertise in category theoretically-based coalgebraic models of concurrency.

Another important aspect of the Plume team is its involvement in the local Department of Computer Science, which makes a link with the pupils of ENSL, which are very bright students interested in research careers.

Existing relationships between the partners involved in the project

Since its establishment in 2000, BASICS has formed a research network with several partners in France and in particular with INRIA. Yuxin Deng was among the early group of students sent by BASICS to France to pursue PhD's. Since then he has kept a close and active working relationship with Palamidessi's group and Sangiorgi's group (Sangiorgi having been Deng's PhD advisor). Xu and Sangiorgi have shared for a long time interest in higher order process calculus and have exchanged research ideas over the years. Xu will start a sabbatical year in Sangiorgi's group in a few months under a grant from China Scholarship Council.

The interaction during the BASICS 2009 Workshop, organized by BASICS and attended by Palamidessi and Sangiorgi (INRIA site), made it apparent to the participants from INRIA and BASICS that some of the ongoing researches carried out in the two sides cover a number of common issues with shared interest, although different angles of investigation, different techniques and different methodologies have been adopted. These research activities are highly complementary. For example Cai and Fu's fully abstract interpretation of the full pi-calculus offers a different encoding technique than the one used in Sangiorgi's translation of several variants of the pi-calculus. The research activities on expressiveness carried out in Fu's group, Palamidessi's group and to some extent Sangiorgi's group have led to different criteria, reflecting different aspects of the investigated issue. The early work on termination of pi-calculus by Deng and Sangiorgi has been further generalized by Hirschkoff□s group at Lyon in recent years. There is also complementarity between Deng's work on probabilistic bisimulation and Pous' work on up-to techniques for classical concurrency theory. It is apparent that joint research efforts would produce further synergy and promote new integration.

Among the french partners, the groups in Lyon and Bologna have a long standing close collaboration. Regular visits, together with the joint supervision of five PhD students have resulted in numerous co-publications, about models of concurrency, behavioural equivalences, modal logics and type systems for concurrent behaviours. D. Hirschkoff (coordinator, Lyon site) is external collaborator of the INRIA Focus team. There are also collaborations between the teams in Lyon and Paris (Bonchi, Valencia, Palamidessi).

As a conclusion, we believe that by building a platform for the related research activities, deeper insights, more powerful techniques, converging methodology, and new research issues will emerge as a result of stimulated cooperation, leading to a stronger international visibility of the participants in the targeted fields. To achieve the goal a frequent interaction among the partners should be maintained, and it is crucial that new PhD's and postdoc's should join in our effort.

5.2. QUALIFICATION OF THE PROJECT COORDINATOR

D. Hirschkoff has a good experience in managing research teams and research projects. He has been scientific leader of the Plume team between 2006 and 2009, and since 2009 he is vice-head of the LIP (Laboratoire de l'Informatique du Parallélisme, ENS Lyon; about 55 permanent staff and 80 students and collaborators on a contract) research lab. He has taken part in several french and european

research projects, notably FET-Global Computing Profundis, action Procope, projet Opiddum, ACI Geocal, ANR Choco (site leader), ANR Complice, ANR PiCoq, PEPS Cogip.

His research interests cover several of the topics of the project. In particular, he has published about behavioural equivalences, up-to techniques, expressiveness, and mechanisations of bisimulation proofs. Relevant publications on these subjects include:

- D. Hirschkoff, D. Pous: On Bisimilarity and Substitution in Presence of Replication. ICALP (2) 2010: 454-465 (2010)
- Daniel Hirschkoff, Étienne Lozes, Davide Sangiorgi: On the Expressiveness of the Ambient Logic. Logical Methods in Computer Science 2(2): (2006)
- Christine Röckl, Daniel Hirschkoff: A fully adequate shallow embedding of the [pi]-calculus in Isabelle/HOL with mechanized syntax analysis. J. Funct. Program. 13(2): 415-451 (2003)
- D. Hirschkoff: Bisimulation verification using the up-to techniques. STTT 3(3):271-285 (2001)
- Daniel Hirschkoff: A Full Formalisation of pi-Calculus Theory in the Calculus of Constructions. TPHOLs 1997: 153-169 (1997)

5.3. QUALIFICATION AND CONTRIBUTION OF EACH PARTNER

Partner	Country	Name	First name	Current Position	Field of research*	Person months	Role and Contribution to the project
Lyon	France	HIRSCHKOFF	Daniel	Maître de Conférences, HDR	Enhancements of bisimulation, expressiveness, algorithms using up-to techniques	24	Coordinator/ Principal Investigator
Lyon	France	BONCHI	Filippo	CR CNRS	Algorithms using up-to techniques, quantum, symbolic bisimulation, expressiveness	16	Member
Lyon	France	POUS	Damien	CR CNRS	Enhancements of bisimulation, algorithms using the up-to techniques	20	Task 3 coordinator
INRIA	France	SANGIORGI	Davide	Professor	Enhancements of bisimulation, expressiveness	12	Task 1 and site coordinator
INRIA	France	DAL LAGO	Ugo	Ricercatore	Probabilities, Quantum, Coinduction	8	Member
INRIA	France	ZAVATTARO	GianLuigi	Professor	Expressiveness	7	Member
INRIA	France	GABBRIELLI	Maurizio	Professor	Expressiveness	7	Member
INRIA	France	PALAMIDESSI	Catuscia	DR INRIA	Expressiveness, confidentiality properties	5	Member
INRIA	France	VALENCIA	Frank	CR CNRS	Expressiveness, constraints and social networks, symbolic bisimulation	9	Member
Shanghai	China	FU	Yuxi	Professor	Computation and interaction models; equality, expressiveness and completeness	26	Task 2 and site coordinator
Shanghai	China	DENG	Yuxin	Associate Professor	Semantic models; probabilistic approach	22	Member
Shanghai	China	XU	Xian	Associate Professor	Coinduction for higher-order models	20	Member
Shanghai	China	LI	Guoaqiang	Assistant Professor	Codivergence checking, analysis techniques	20	Member
Shanghai	China	CAI	Xiaojuan	Assistant Professor	Concurrent programming language, inter-language equivalence	20	Member

See also the following Section for a presentation of the expected contributions of each site. Section 8 (in annex) collects the curriculum vitae of the researchers involved in PACE.

6. SCIENTIFIC JUSTIFICATION OF REQUESTED RESOURCES

6.1. PARTNER 1: ECOLE NORMALE SUPERIEURE DE LYON

The Lyon site will contribute with a work force of 3 permanent researchers: Daniel Hirschkoff (project coordinator, 24 p/m), Damien Pous (20 p/m), Filippo Bonchi (16 p/m).

Postdoc Lyon. This site asks for 12 months of support for one postdoctoral student, to work on the main objectives of Tasks 3. However the postdoc is expected to have interactions also with the other tasks, and help keeping the links with the whole proposal.

This postdoc will be supervised by Daniel Hirschkoff and Damien Pous, and will work on the development and implementation of up-to techniques for models featuring higher-order and/or probabilistic and quantum computation (Tasks 1 and 3).

In addition to the above mentioned researchers and postdocs, the Lyon team has one PhD student, JM Madiot, who works on topics related to this project, under joint supervision by D. Hirschkoff (Lyon) and D. Sangiorgi (INRIA, Bologna). More precisely, JM Madiot works on proof techniques to help in bisimulation proofs (Task 1), with an emphasis on the mechanisation of these techniques (Task 3). This student already has a PhD grant (starting sept. 2011) and therefore will have cost 0 for the project. We expect that JM Madiot will contribute to the project for 12 p/m.

As for travel costs, we estimate that this site will need 15K € for each year: 9kE will be devoted to visiting the other partners and participating in the project meetings, and 6kE will be used for dissemination of the results of PACE. Hence in total this site asks for 4 x 15 = 60K € for travels.

In addition, the Lyon site asks for 10K € (in total) for various organizational expenses related to the management of the project. This sum will be devoted mostly to the organisation of the a symposium devoted to the PACE project, after two years. This symposium will possibly include a research school, at Master level, mainly targeting the students of École Normale Supérieure de Lyon, and addressing the topics of PACE.

6.2. PARTNER 2: INRIA

The INRIA site will contribute with a work force of 6 permanent researchers: Davide Sangiorgi (coordinator for the INRIA site, 12 p/m), Ugo Dal Lago (8 p/m), Maurizio Gabbrielli (7 p/m), Catuscia Palamidessi (5 p/m), Frank S. Valencia (9 p/m) and Gianluigi Zavattaro (7 p/m).

We ask for 2x12 = 24 months of support for two postdoctoral students, to work on the main objectives of Tasks 1 and 2. This association between postdocs and tasks however is not exclusive: the research activities of each postdocs will be transversal to some extent, so to help keeping the link between the various tasks, and contributing to maintainig a unified perspective. More specifically, the research plan for the postdoc is the following:

Postdoc INRIA 1. This postdoc will be supervised by Davide Sangiorgi and will work on the development of the theory of bisimulation enhancements, in higher-order and and in probabilistic languages, including the comparison of these enhancements with logical relations (Task 1).

Postdoc INRIA 2. This postdoc will be supervised by Catuscia Palamidessi and Frank Valencia, and will work on confidentiality and privacy. More precisely, he will: a) apply the conceptual framework proposed in Task 2.2 to reasoning about the epistemologic aspects of confidentiality and privacy in a concurrent setting; b) investigate the foundations of a theory process expressiveness based on security crieria in addition to the standard interaction criteria (Task 2.3, also related to Task 2.1); c) help to identify possible applications of coinduction and up-to techniques to express and verify privacy and confidentiality properties (Task 1 and 3).

In addition to the above mentioned researchers and postdocs, the INRIA teams have some PhD students who work on topics related to this project. These students already have a PhD grant and therefore will have cost 0 for the project. They are:

- Nicolas Bordenabe. He is working on privacy, on tiopics closely related to Task 2.3 and 1. We estimate that he will contribute to the project for 12 p/m.
- Ornela Dardha, who is currently working on expressiveness of behavioural type systems and of higher-order process calculi. We expect that she will contribute to the project for 12 p/m, on issues related to Task 2 and possibly also Task 3
- Luis Pino Duque. He is working on Concurrenct Constraint Programming, on topics related to Task 3.3. We judge his contribution to PACE to be 12 p/m.
- Sophia Knight. She is working in combining concurrency and epistemic logic, a topic which is at the hearth of Task 2.2. We expect her to collaborate on the project for 6 p/m.
- Paolo Parisen Toldin. He is working on probabilistic higher-order lambda calculus, and is expected to contribute on the work on coinduction for higher-order languages. We estimate that he will contribute to the project for 9 p/m.

As for travel costs, we estimate that we will need 14K € per year in order to visit the other partners and participate in the project meetings, and 8K per year to disseminate the results at conferences and symposia. Hence in total we ask for 4 x 22 = 88K €.

Finally, we ask 2 x 2.5 = 5K € to purchase a laptop for the postdocs that will work for our site.

6.3. PARTNER 3: SJTU

Expenses of Shanghai will be as depicted in the following table:

Subject	Funding requested	Notes
1. Conducting Research		
a) Conferences and Travels	RMB250K	
b) Publications, Bibliographies, and Information Dissemination	RMB100k	
c) Others	RMB100K	
2. Experimental Materials	RMB50K	
3. International Travels by Chinese Participants	RMB200K	International travel costs for 6 Chinese participants
4. Attending Conference Abroad	RMB100K	
6. Salaries	RMB150K	4 PhD students, 1 postdoc, partially supported by this project
7. Management Fee	RMB50K	
Total	RMB1000K	

The contribution in terms of manmonths from the SJTU site is given in Section 5.3 above, regarding permanent members. PhD students involved in the PACE project, and partially funded by the project; are: Jianxin Xue (18 manmonths), Hao Huang (20 manmonths), Qiang Yin (30 manmonths), Yang Wang (30 manmonths).

6.4. SUM-UP OF REQUESTED FUNDING.

The collaboration between the Chinese and French partners could be an opportunity to hire a PhD student, possibly under co-supervision between people involved in the project. If such a situation arises, we are confident that we will have access to resources to support the PhD student. For this reason, the requested funding in terms of scientific staff consists only in postdoctoral contracts, to carry over the research effort required in PACE.

Partner	Country	Partner's organisation	Total permanent staff in person months	Total non-permanent staff in person months*	Total funding requested
ENS Lyon	France		60 **not** payed by the project	30 = 18 PhD p/m, **not** payed by the project + 12 postdoc p/m payed by the project	70K € + 12 months postdoc (60K€)
INRIA	France		48 **not** payed by the project	75 = 51 PhD p/m, **not** payed by the project + 24 postdoc p/m payed by the project	93K € + 24 months postdoc (102.4 K€)
SJTU	China	Shanghai Jiao Tong University	108 **not** payed by the project	98 *partially* (36 mm) payed by the project	RMB1000K

7. REFERENCES

[A90] Samson Abramsky. The Lazy Lambda-Calculus. In D. Turner, editor, Research Topics in Functional Programming. Pages 65−117. Addison Wesley. 1990.
[AAP10] M. S. Alvim, M. E. Andres, C. Palamidessi: Probabilistic Information Flow. Proc. of LICS 2010: 314-321, IEEE Computer Society.
[AAP12] M. S. Alvim, M. E. Andres, C. Palamidessi: Information Flow in Interactive Systems. Journal of Computer Security. To appear. 2012.
[AACP11] M. S. Alvim, M. E. Andres, K. Chatzikokolakis, C. Palamidessi: Probabilistic Information Flow versus Differential Privacy. Proc. of ICALP 2011. LNCS 6756, pp. 60-76, Springer.
[ABHKMS12] J. Adamek, F. Bonchi, M. Hulsbusch, Barbara Konig, Stefan Milius, A. Silva. A Coalgebraic Perspective on Minimization and Determinization. To appear in the proceedings of FOSSACS2012.
[ABPPV11] Andrés Aristizábal, Filippo Bonchi, Catuscia Palamidessi, Luis Pino, Frank D. Valencia: Deriving Labels and Bisimilarity for Concurrent Constraint Programming. FOSSACS 2011: 138-152
[ABPV12] A. Aristizabal, F. Bonchi, L. Pino, F. Valencia. Partition Refinement for Bisimilarity in CCP. To appear in the 27th ACM Symposium On Applied Computing (SAC 2012).
[ABZ10] Lucia Acciai, Michele Boreale, Gianluigi Zavattaro.: On the Relationship between Spatial Logics and Behavioral Simulations. In FOSSACS 2010: 146-160
[ACHMV10] P. A. Abdulla, Y.-F. Chen, L. Hol´ık, R. Mayr, and T. Vojnar. When simulation meets antichains. In Proc. TACAS, volume 6015 of LNCS,pages 158–174. Springer, 2010.
[AG99] Martín Abadi and Andrew D. Gordon. A Calculus for Cryptographic Protocols: The Spi Calculus. Information and Computation,148, pp. 1-70, 1999.
[AHM03] L. de Alfaro, T. A. Henzinger, and R. Majumdar. Discounting the future in systems theory. In ICALP, volume 2719 of LNCS, pages 1022–1037. Springer, 2003.

[AHU74] A. V. Aho, J. E. Hopcroft, and J. D. Ullman. The Design and Analysis of Computer Algorithms. Addison-Wesley, 1974.
[AM89] P. Aczel and N. P. Mendler. A final coalgebra theorem. In Category Theory and Computer Science, volume 389 of LNCS, pages 357–365. Springer, 1989.
[APRS11] M. E. Andres, C. Palamidessi, P. van Rossum, A. Sokolova. Information hiding in probabilistic concurrent systems. Theoretical Computer Science, 412(28):3072-3089, 2011.
[BBRS12] F. Bonchi, M. Bonsangue, J. Rutten and A. Silva. Brzozowski's algorithm (co)algebraically. To appear in the festschrift for Dexter Kozen. LNCS, Springer, 2012.
[BGZ09] N. Busi, M. Gabbrielli, and G. Zavattaro. On the expressive power of recursion, replication and iteration in process calculi. to appear in Mathematical Structures in Computer Science, 2009.
[BJPV09] Jesper Bengtson, Magnus Johansson, Joachim Parrow, and Björn Victor.
Psi-calculi: Mobile processes, nominal data, and logic. In LICS, pages 39–48, 2009.
[BKM06] F. Bonchi, B. König, and U. Montanari. Saturated semantics for reactive systems. In Logic in Computer Science, pages 69–80. IEEE, 2006.
[BM07] Maria Grazia Buscemi and Ugo Montanari. Cc-pi: A constraint-based language for specifying service level agreements. In ESOP, pages 18–32, 2007
[BM08] F. Bonchi and U. Montanari. Symbolic semantics revisited. In FoSSaCS, volume 4962 of LNCS, pages 395–412. Springer, 2008.
[BM09] F. Bonchi and U. Montanari. Minimization algorithm for symbolic bisimilarity. In ESOP, volume 5502 of LNCS, pages 267–284. Springer, 2009.
[Buc08] P. Buchholz. Bisimulation relations for weighted automata. Theoretical Computer Science, 393(1-3):109–123, 2008.
[BP05] Mohit Bhargava and Catuscia Palamidessi. Probabilistic Anonymity. Proc. of CONCUR. LNCS 3653, pp. 171-185, Springer, 2005.
[BP12] F. Bonchi, D. Pous. Checking NFA equivalence with bisimulations up to congruence. Tech. report, available from HAL, 2012.
[BPP11] Michele Boreale, Francesca Pampaloni, and Michela Paolini, Asymptotic Information Leakage under One-Try Attacks. Proc. of FOSSACS. LNCS 6604, pp. 396-410, Springer, 2011.
[Brz62] J. A. Brzozowski. Canonical regular expressions and minimal state graphs for definite events. In Mathematical Theory of Automata, volume 12(6), pages 529–561. Polytechnic Press, NY, 1962
[BSW08]74. F. van Breugel, B. Sharma, and J.Worrell. Approximating a behavioural pseudometric without discount for probabilistic systems. Logical Methods in Computer Science, 4(2), 2008.
[Buc08] P. Buchholz. Bisimulation relations for weighted automata. Theor. Comp. Sc., 393(1-3):109–123, 2008.
[BW90] Jos C. M. Baeten and W. P. Weijland. Process Algebra, volume 18 of Cambridge Tracts in Theoretical Computer Science. Cambridge University Press, 1990.
[BW05] F. van Breugel and J. Worrell. A behavioural pseudometric for probabilistic transition systems. Theoretical Computer Science, 331(1):115–142, 2005.
[BW06] F. van Breugel and J. Worrell. Approximating and computing behavioural distances in probabilistic transition systems. Theoretical Computer Science, 360(1-3):373–385, 2006.
[Ca09] Xiaojuan Cai. Measuring Anonymity. In Proceedings of the 5th Information Security Practice and Experience Conference (ISPEC'09), LNCS 5451, pages 183-194, 2009.
[CG09] Xiaojuan Cai and Yonggen Gu. Measuring Anonymous Systems in the Probabilistic Applied Pi Calculus. In Proceedings of the 2009 International Conference on Computational Science and Its Applications (ICCSA 2009), LNCS 5593, pages 614 - 629, 2009.
[CHL11] W. Czerwiński, P. Hofman, S. Lasota, Decidability of branching bisimulation on normed commutative context-free processes. In Proceedings of CONCUR'11, 2011.
[CHM05] David Clark, Sebastian Hunt, and Pasquale Malacaria. Quantified Interference for a While Language, Proc. of QAPL. ENTCS 112, pp. 149-166, 2005.
[Co11] Véronique Cortier: Secure Composition of Protocols. Proc. of TOSCA. pp. 29-32, 2011.
[CPB12] Konstantinos Chatzikokolakis, Catuscia Palamidessi, and Christelle Braun. Compositional Methods for Information-Hiding. MSCS. To appear, 2012.
[CRS11] G. Castiglione, A. Restivo, M. Sciortino. Nondeterministic Moore Automata and Brzozowski's Algorithm. CIAA 2011: 88-99
[CSZ92] R. Cleaveland, S. A. Smolka, and A. E. Zwarico. Testing preorders for probabilistic processes. In ICALP, volume 623 of LNCS, pages 708–719. Springer, 1992.
[D92] Guoli Ding: Subgraph and well-quasi-ordering. Journal of Graph Theory, vol 16(5): 489:502. 1992
[DCPP06] Y. Deng, T. Chothia, C. Palamidessi, and J. Pang. Metrics for action-labelled quantitative transition systems. Electr. Notes Theor. Comput. Sci., 153(2):79–96, 2006.

[DG05] M. Droste and P. Gastin. Weighted automata and weighted logics. In ICALP, volume 3580 of LNCS, pages 513–525. Springer, 2005.
[DGJP04] J. Desharnais, V. Gupta, R. Jagadeesan, and P. Panangaden. Metrics for labelled markov processes. Theoretical Computer Science, 318a(3):323–354, 2004.
[DJGO02] J. Desharnais, R. Jagadeesan, V. Gupta, and P. Panangaden. The metric analogue of weak bisimulation for probabilistic processes. In Logic in Computer Science, pages 413–422. IEEE, 2002.
[DKR06] Stéphanie Delaune, Steve Kremer, and Mark Ryan. Coercion-Resistance and Receipt-Freeness in Electronic Voting. Proc. of FCSW. pp. 28-42, 2006.
[DKR09] Stéphanie Delaune, Steve Kremer, and Mark Ryan. Verifying privacy-type properties of electronic voting protocols. Journal of Computer Security, 17 , pp. 435-487, 2009.
[DLMZ09] Ugo Dal Lago, Andrea Masini, Margherita Zorzi: On a measurement-free quantum lambda calculus with classical control. Mathematical Structures in Computer Science 19(2): 297-335 (2009)
[DPW06] Yuxin Deng, Jun Pang and Peng Wu. Measuring Anonymity with Relative Entropy. Proc. of FAST. LNCS 4691, pp. 65-79, Springer, 2006.
[DSZ10] Giorgio Delzanno, Arnaud Sangnier, Gianluigi Zavattaro: Parameterized Verification of Ad Hoc Networks. In CONCUR 2010: 313-327
[EFM99] Javier Esparza, Alain Finkel, Richard Mayr: On the Verification of Broadcast Protocols. In LICS 1999: 352-359
[FDJY07] Y. Feng, R. Duan, Z. Ji, and M. Ying. Probabilistic Bisimulations for Quantum Processes. Information and Computation, 205(11):1608-1639, 2007.
[FDY11] Y. Feng, R. Duan, and M. Ying. Bisimulations for quantum processes. In Proceedings of the 38th ACM Symposium on Principles of Programming Languages (POPL'11), pages 523–534, 2011.
[FM92] J.-C. Fernandez and L. Mounier. "on the fly" verification of behavioural equivalences and preorders. In CAV, volume 575 of LNCS, pages 18a1–191. Springer, 1992.
[FMT05] G. L. Ferrari, U. Montanari, and E. Tuosto. Coalgebraic minimization of hd-automata for the pi-calculus using polymorphic types. Theoretical Computer Science, 331(2-3):325 365, 2005.
[Fu12a] Y. Fu. The Universal Process. Available at http://basics.sjtu.edu.cn/~yuxi/ .
[Fu12b] Y. Fu. The Value Passing calculus. Available at http://basics.sjtu.edu.cn/~yuxi.
[Fu12c] Yuxi Fu. Nondeterministic Structure of Computation. Available at http://basics.sjtu.edu.cn/~yuxi/ .
[Fu12d] Yuxi Fu. Theory of Interaction. Available at http://basics.sjtu.edu.cn/~yuxi/ .
[FZ12] Y. Fu and H. Zhu. The Name Passing Calculus. Available at http://basics.sjtu.edu.cn/~yuxi/ .
[GJS90] A. Giacalone, C.-C. Jou, and S. Smolka. Algebraic reasoning for probabilistic concurrent systems. In North-Holland, editor, IFIP W.G. 2.2/2.3 Working Conference on Programming Concepts and Methods, pages 443–458, 1990.
[GLM01] H. Garavel, F. Lang, R. Mateescu. An overview of CADP. EASST 4:13-24, 2001
[GM99] F. Gadduci and U. Montanari. The tile model. In Proof, Language and Interaction: Essays in honour of Robin Milner. MIT Press, 1999.
[GN05] S. J. Gay and R. Nagarajan. Communicating quantum processes. In Proceedings of the 32nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL), pages 145–157, 2005.
[Gor08] Towards a unified approach to encodability and separation results
for process calculi. In Proceedings of CONCUR 2008 volume 5201 of Lecture Notes in Computer Science. Springer, 2008.pages 492–507.
[GP07] A. Girard and G. J. Pappas. Approximate bisimulation relations for constrained linear systems. Automatica, 43(8):1307–1317, 2007.
[GPV10] Maurizio Gabbrielli, Catuscia Palamidessi, Frank D. Valencia: Concurrent and Reactive Constraint Programming. 25 Years GULP 2010: 231-253
[Gro96] L. K. Grover. A fast quantum mechanical algorithm for database search. In Proc. ACM STOC, pages 212–219, 1996.
[Gro97] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. Physical Review Letters, 78(2):325, 1997.
[GSS95] R. J. van Glabbeek, S. A. Smolka, and B. Steffen. Reactive, generative and stratified models of probabilistic processes. Information and Computation, 121(1):59–80, 1995.
[GSV04] Pablo Giambiagi, Gerardo Schneider and Frank D. Valencia. On the Expressiveness of Infinite Behavior and Name Scoping in Process Calculi. FoSSaCS 2004: 226-240. Springer-Verlag. 2004.
[HDNV12] C. Hur, D. Dreyer, G. Neis, and V. Vafeiadis. The Marriage of Bisimulations and Kripke Logical Relations. In Proceedings of POPL'12, pages 59–72, 2012.
[HJS08] I. Hasuo, B. Jacobs, and A. Sokolova. The microcosm principle and concurrency in coalgebra. In FoSSaCS, volume 4962 of LNCS, pages 246–260. Springer, 2008.

[HK71] J. E. Hopcroft and R. M. Karp. A linear algorithm for testing equivalence of finite automata. Technical Report 114, Cornell Univ., December 1971.
[HL95] M. Hennessy and H. Lin. Symbolic bisimulations. Theoretical Comp. Science, 138(2):353–389, 1995.
[Hoa85] C. A. R. Hoare. Communicating Sequential Processes. Prentice Hall, 1985.
[Hop71] J. E. Hopcroft. An n log n algorithm for minimizing in a finite automaton. In Proc. International Symposium of Theory of Machines and Computations, pages 189–196. Academic Press, 1971.
[HPPPD] C. Hundt, P. Panangaden, J. Pineau, D. Precup, M. Dinculescu. The Duality of State and Observations. Unpublished notes. Available at http://www.cs.mcgill.ca/~prakash/Pubs/alpha.pdf
[Hut81] J. Hutchinsons. Fractals and self similarity. Indiana University Math. Journal, 30(5):713–747, 1981.
[KDNV12] Chung-Kil Hur, Derek Dreyer, Georg Neis, Viktor Vafeiadis: The marriage of bisimulations and Kripke logical relations. POPL 2012, ACM, 59-72.
[JM00] J. J. Leifer and R. Milner. Deriving bisimulation congruences for reactive systems. In CONCUR, volume 18a77 of LNCS, pages 243–258. Springer, 2000.
[JL04] P. Jorrand and M. Lalire. Toward a quantum process algebra. In Proceedings of the 2nd International Workshop on Quantum Programming Languages, 2004.
[JY95] B. Jonsson and W. Yi. Compositional testing preorders for probabilistic processes. In Logic in Computer Science, pages 431–441. IEEE, 1995.
[Kan42] L. Kantorovich. On the translocation of masses. Doklady Akademii Nauk SSSR, 37(7 8):227– 229, 1942.
[KR07] Dexter Kozen and Nicholas Ruozzi. Applications of metric coinduction. Proc. 2nd Conf. Algebra and Coalgebra in Computer Science (CALCO 2007), volume 4624 of LNCS, pages 327–341. Springer, August 2007.
[Koz06] Dexter Kozen. Coinductive proof principles for stochastic processes. In Rajeev Alur, editor, Proc. 21st Symp. Logic in Computer Science (LICS'06), pages 359–366. IEEE, August 2006.
[KS90] P. C. Kanellakis and S. A. Smolka. CCS expressions, finite state processes, and three problems of equivalence. Information and Computation, 86(1):43–68, 1990.
[KW06] Vasileios Koutavas, Mitchell Wand: Small bisimulations for
reasoning about higher-order imperative programs. POPL 2006, ACM 141-152.
[LFF12] H. Liang, X. Feng, and M. Fu. A Rely-Guarantee-Based Simulation for Verifying Concurrent Program Transformations. In Proceedings of POPL'12, pages 455–468, 2012.
[LS91] K. G. Larsen and A. Skou. Bisimulation through probabilistic testing. Information and Computation, 94(1):1–28, 1991.
[Ma07] Pasquale Malacaria. Assessing security threats of looping constructs. Proc. of POPL, pp. 225-235, 2007.
[Mil89] R. Milner. Communication and Concurrency. Prentice-Hall, 1989.
[MP99] Ugo Montanari, Marco Pistore: Finite State Verification for the Asynchronous pi-Calculus. TACAS 1999: 255-269
[MS90] F. Moller, P. Stevens. The Edinburgh Concurrency
Workbench. http://homepages.inf.ed.ac.uk/perdita/cwb/
[MZ05]Massimo Merro, Francesco Zappa Nardelli: Behavioral theory for mobile ambients. J. ACM 52(6): 961-1023 (2005)
[Nes97] U. Nestmann. What is a 'good' encoding of guarded choice? Electr. Notes Theor. Comput. Sci., 7, 1997.
[Pal03] C. Palamidessi. Comparing the expressive power of the synchronous and asynchronous pi-calculi. Mathematical Structures in Computer Science, 13(5):685–719, 2003.
[Pal06] C. Palamidessi, V. Saraswat, F. Valencia, B. Victor. On the expressiveness of linearity vs persistence in the asynchronous pi-calculus. In Proc. of LICS'06, IEEE, 59-68, 2006.
[Pana12] P. Panangaden. Probabilistic bisimulation. In [SR12], 2012.
[Par08] J. Parrow. Expressiveness of Process Algebras. Electr. Notes Theor. Comput. Sci. 209: 173-186 (2008)
[Pou08] D. Pous. Techniques modulo pour les bisimulations, PhD Thesis, ENS Lyon, 2008.
[PS96] Marco Pistore, Davide Sangiorgi: A Partition Refinement Algorithm for the pi-Calculus (Extended Abstract). CAV 1996: 38-49
[PS12] D. Pous, D. Sangiorgi. Enhancements of the bisimulation proof method, in [SR12]
[PZ86] A. Pnueli and L. D. Zuck. Probabilistic verification by tableaux. In Logic in Computer Science, pages 322–331. IEEE, 1986.
[Rab98] M. O. Rabin. Probabilistic automata. Information and Control, 6(3):230–245, 1963. [Rut98] J. J. M. M. Rutten. Relators and metric bisimulations. Electr. Notes Theor. Comput. Sci., 11, 1998.
[Ret98] Jean-Hugues Réty. Distributed concurrent constraint programming. Fundam. Inf., 34(3):323–346, 1998.
[Rut00] J. J. M. M. Rutten. Universal coalgebra: a theory of systems. Theor. Comp. Science, 249(1):3–80, 2000.
[San12] D. Sangiorgi. Introduction to bisimulation and coinduction. Cambridge University Press, 2012.
[San96] D.Sangiorgi. A theory of bisimulation for the pi-calculus. Acta Informatica,33(1):69– 97, 1996.

[San98] D. Sangiorgi. On the bisimulation proof method. Jour. MSCS, 8:447-479, 1998.
[Sch61] M. Schützenberger. On the definition of a family of automata. Information and Control, 4(2-3):245–270, 1961.
[Sho94] P. W. Shor. Algorithms for quantum computation: discrete log and factoring. In Proceedings of the 35th IEEE FOCS, pages 124–134, 1994.
[Sim85] R. D. Simone. Higher level synchronizing devices in meije-sccs. Theoretical Computer Science, 37:245–267, 1985.
[SKS11] D. Sangiorgi, N. Kobayashi, E. Sumii: Environmental bisimulations for higher-order languages. ACM Trans. Program. Lang. Syst. 33(1): 5, 2011.
[SL94] R. Segala and N. A. Lynch. Probabilistic simulations for probabilistic processes. In CONCUR, volume 836 of LNCS, pages 481–496. Springer, 1994.
[Sm09] Geoffrey Smith On the Foundations of Quantitative Information Flow. Proc. of FOSSACS, LNCS 5504, pp. 288-302, Springer, 2009.
[SR12] D. Sangiorgi, J. Rutten (eds) Advanced topics in bisimulation and coinduction. Camb. Univ. Press. 2012.
[SRP91] Vijay A. Saraswat, Martin C. Rinard, Prakash Panangaden: Semantic Foundations of Concurrent Constraint Programming. POPL 1991: 333-352
[Sta09] S. Staton. Relating coalgebraic notions of bisimulation. In Proc. of CALCO '09, pages 191–205. Springer, 2009. LNCS 5728
[SS90] S. A. Smolka and B. Steffen. Priority as extremal probability. In CONCUR, volume 458 of LNCS, pages 456–466. Springer, 1990.
[Sta09] S. Staton. Relating coalgebraic notions of bisimulation. In CALCO, volume 5728 of LNCS, pages 191–205. Springer, 2009.
[SV06] Peter Selinger, Benoît Valiron: A lambda calculus for quantum computation with classical control. Mathematical Structures in Computer Science 16(3): 527-552 (2006)
[SW01] Sangiorgi D., Walker D. The pi-calculus: a Theory of Mobile Processes. Cambridge Univ. Press, 2001.
[Tar51] A. Tarski. A decision method for elementary algebra and geometry. Univ. of California Press, 1951.
[TP97] D. Turi and G. D. Plotkin. Towards a mathematical operational semantics. In Logic in Computer Science, pages 280–291. IEEE, 1997.
[Var85] M. Y. Vardi. Automatic verification of probabilistic concurrent finite-state programs. In FOCS, pages 327–338. IEEE, 1985.
[Var69] L. Vaserstein. Markov processes on countable space products describing large systems of automata. Problems of Information Transmission, 5(3):271–293, 1969.
[VM94] Björn Victor, Faron Moller: The Mobility Workbench - A Tool for the pi-Calculus. CAV 1994: 428-440
[VPP05] M. Vigliotti, I. Phillips, and C. Palamidessi. Separation results via leader election problems. Proc. Of FMCO, volume 4111 of Lecture Notes in Computer Science, pages 172–194. Springer, 2005.
[vT04] A. van Tonder: A Lambda Calculus for Quantum Computation. SIAM Journ. of Comp. 33(5): 1109-1135 (2004)
[WDHR06] M. De Wulf, L. Doyen, T. A. Henzinger, and J.-F. Raskin. Antichains: A new algorithm for checking universality of finite automata. In Proc. CAV: Computer-Aided Verification, volume 4144 of LNCS, pages 17–30. Springer, 2006
[Wor00] J. Worrell. Coinduction for recursive data types: partial orders, metric spaces and omegacategories. Electr. Notes Theor. Comput. Sci., 33, 2000.
[YFDJ09] M Ying, Y Feng, R Duan, and Z Ji. An algebra of quantum processes. ACM Transactions on Computational Logic (TOCL), 10(3):1–36, 2009.