Fluid Model Checking

Luca Bortolussi
Department of Mathematics and Geosciences
University of Trieste, Italy.
luca@dmi.units.it

Jane Hillston
Laboratory for the Foundations of Computer Science,
School of Informatics, University of Edinburgh, UK.
jane.hillston@ed.ac.uk

In this paper we investigate a potential use of fluid approximation techniques in the context of stochastic model checking of CSL formulae. We focus on properties describing the behaviour of a single agent in a (large) population of agents, exploiting a limit result known also as fast simulation. In particular, we will approximate the behaviour of a single agent with a time-inhomogeneous CTMC which depends on the environment and on the other agents only through the solution of the fluid differential equation. We will prove the asymptotic correctness of our approach in terms of satisfiability of CSL formulae and of reachability probabilities. We will also present a procedure to model check time-inhomogeneous CTMC against CSL formulae.
Keywords: Stochastic model checking, fluid approximation, mean field approximation, reachability probability.

1 Introduction

In the last years, there has been a growing interest in fluid approximation techniques in the formal methods community [7, 8, 10, 14, 27, 34]. These techniques, also known as mean field approximation, are useful for analysing quantitative models of systems based on continuous time Markov Chains (CTMC), possibly described in process algebraic terms. They work by approximating the discrete state space of the CTMC by a continuous one, and by approximating the stochastic dynamics of the process with a deterministic one, expressed by means of a set of differential equations. The asymptotic correctness of this approach is guaranteed by limit theorems [18, 19, 37], showing the convergence of the CTMC to the fluid ODE for systems of increasing sizes.

The notion of size can be different from domain to domain, yet in models of interacting agents, usually considered in computer science, the size has the standard meaning of population number. All these fluid approaches, in particular, require a shift from an agent-based description to a population-based one, in which the system is described by variables counting the number of agents in each possible state and so individual behaviours are abstracted. In fact, in large systems, the individual choices of single agents have a small impact, hence the whole system tends to evolve according to the average behaviour of agents. Therefore, the deterministic description of the fluid approximation is mainly related to the average behaviour of the model, and information about statistical properties is generally lost, although it can be partially recovered by introducing fluid equations of higher order moments of the stochastic process (moment closure techniques [24, 49]).

Differently to fluid approximation, the analysis of quantitative systems like those described by process algebras can be carried out using quantitative model checking. These techniques have a long tradition in computer science and are powerful ways of querying a model and extracting information about its behaviour. As far as stochastic model checking is considered, there are some consolidated approaches based mainly on checking Continuous Stochastic Logic (CSL) formulae [5, 6, 47], which led to widespread software tools [38]. All these methods, however, suffer (in a more or less relevant way)

Preliminary Report. Final version to appear in:

from the curse of state space explosion, which severely hampers their practical applicability. In order to mitigate these combinatorial barriers, many techniques have been developed, many of them based on some notion of abstraction or approximation of the original process [32, 33].

In this paper, we will precisely target this problem, trying to see to what extent fluid approximation techniques can be used to speed up the model checking of CTMC. We will not tackle this problem in general, but rather we will focus on a restricted subset of system properties: We will consider population models, in which many agents interact, and then focus on the behaviour of single agents. In fact, even if large systems behave almost deterministically, the evolution of a single agent in a large population is always stochastic. Single agent properties are interesting in many application domains. For instance, in performance models of computer networks, like client-server interaction, one is often interested in the behaviour and in quality-of-service metrics of a single client (or a single server), such as the waiting time of the client or the probability of a time-out.

Single agent properties may also be interesting in other contexts. For instance, in ecological models, one may be interested in the chances of survival or reproduction of an animal, or in its foraging patterns [50]. In biochemistry, there is some interest in the stochastic properties of single molecules in a mixture (single molecule enzyme kinetics [43, 48]). Other examples may include the time to reach a certain location in a traffic model of a city, or the chances to escape successfully from a building in case of emergency egress [39].

The use of fluid approximation in this restricted context is made possible by a corollary of the fluid convergence theorems, known under the name of *fast simulation* [19, 23], which provide a characterization of the behaviour of a single agent in terms of the solution of the fluid equation: the agent senses the rest of the population only through its "average" evolution, as given by the fluid equation. This characterization can be proved to be asymptotically correct.

Our idea is simply to use the CTMC for a single agent obtained from the fluid approximation instead of the full model with N interacting agents. In fact, extracting metrics from the description of the global system can be extremely expensive from a computational point of view. Fast simulation, instead, allows us to abstract the system and study the evolution of a single agent (or of a subset of agents) by decoupling its evolution from the evolution of its environment. This has the effect of drastically reducing the dimensionality of the state space by several orders of magnitude.

Of course, in applying the mean field limit, we are introducing an error which is difficult to control (there are error bounds but they depend on the final time and they are very loose [19]). However, this error in practice will not be too large, especially for systems with a large pool of agents. We stress that these are the precise cases in which current tools suffer severely from state space explosion, and that can mostly benefit from a fluid approximation. However, we will see in the following that in many cases the quality of the approximation is good also for small populations.

In the rest of the paper, we will basically focus on how to analyse single agent properties of two kinds:

- Reachability properties, i.e. the probability of reaching a set of states G, while avoiding unsafe states U.
- Branching temporal logic properties, i.e. verifying CSL formulae.

A central feature of the abstraction based on fluid approximation is that the limit of the model of a single agent has rates depending on time, via the solution of the fluid ODE . Hence, the limit models are time-inhomogeneous CTMC (ICTMC). This introduces some additional complexity in the approach, as model checking of ICTMC is far more difficult than the homogeneous-time case. To the best of the author's knowledge, in fact, there is no known algorithm to solve this problem in general, although related work is presented in Section 2. We will discuss a general method in Sections 4 and 5, based on the solution of variants of the Kolmogorov equations, which is expected to work for small state spaces and controlled dynamics of the fluid approximation. The main problem with ICTMC model checking is that the truth of a formula can depend on the time at which the formula is evaluated. Hence, we need to impose some regularity on the dependency of rates on time to control the complexity of time-dependent truth. We will see that the requirement, piecewise analyticity of rate functions, is intimately connected not only with the decidability of the model checking for ICTMC, but also with the lifting of convergence results from CTMC to truth values of CSL formulae (Theorems 5.1 and 5.3).

The paper is organized as follows: in Section 2 we discuss work related to our approach. In Section 3, we introduce preliminary notions, fixing the class of models considered (Section 3.1) and presenting fluid limit and fast simulation theorems (Sections 3.2 and 3.3). In Section 4, instead, we consider the reachability problem, discussing both how to solve it for ICTMC and the convergence of reachability probabilities for increasing population sizes. In Section 5, instead, we focus on the CSL model checking problem for ICTMC, exploiting the routines for reachability developed before. We also consider the convergence of truth values for formulae about single agent properties. Finally, in Section 6, we discuss open issues and future work.

2 Related work

Model checking (time homogeneous) Continuous Time Markov Chains (CTMC) against Continuous Stochastic Logics (CSL) specifications has a long tradition in computer science [5, 6, 47]. The line of approach for time-bounded properties followed here is similar to [6].

The case of time-inhomogeneous CTMCs, instead, has received much less attention. To the best of the authors' knowledge, there has been no previous proposal of an algorithm to model check CSL formulae on a ICTMC. However, related approaches include model checking of HML and LTL logics on ICTMC.

A model checking algorithm for Hennessy-Milner Logics on ICTCM has been proposed in [31], under the assumption of piecewise constant rates (with a finite number of pieces). It is based on the computation of integrals and the solution of algebraic equations with exponentials (for which a bound on the number of zeros can be found).

LTL model checking for ICTMC, instead, has been proposed in [16]. The approach works for time-unbounded formulae by constructing the product of the CTMC with a generalized Büchi automaton constructed from the LTL formula, and then reducing the model checking problem to computation of reachability of bottom strongly connected components in this larger (pseudo)-CTMC. The authors also propose an algorithm for solving time bounded reachability similar to the one considered in this paper (for time-constant sets).

Another approach related to this work is the verification of CTMC against deterministic time automata (DTA) specifications [17], in which the verification works by taking the product of the CTMC with the DTA, which is then converted into a Piecewise Deterministic Markov Process (PDMP, [20]), and then solving a reachability problem for the so obtained PDMP. Another related work is the verification of time-homogenenous CTMC agains MTL formulae [15].

As far as fast simulation results is concerned, it has been applied in different contexts [19], among which the study of policies to balance the load between servers [23]. In this direction, another related work is [25], in which the authors consider an approach similar to fast simulation to study first passage times in PEPA models.

3 Preliminaries

In this section, we will introduce some backgound material needed in the rest of the paper. First of all, we introduce a suitable notation to describe the population models we are interested in. This is done in Section 3.1. In particular, models will depend parametrically on the (initial) population size, so that we are in fact defining a sequence of models. Then, in Section 3.2, we present the classic fluid limit theorem, which proves convergence of a sequence of stochastic models to the solution of a differential equation. In Section 3.3, instead, we describe fast simulation, a consequence of the fluid limit theorem which connects the system view of the fluid limit to the single agent view, providing a description of single agent behaviour in the limit. Finally, in Section 3.4, we recall the basics of Continuous Stochastic Logics (CSL) model checking.

3.1 Modelling Language

In the following, we will describe a basic language for CTMC, in order to fix the notation. We have in mind population models, where a population of agents, possibly of different kinds, interact together through a finite set of possible actions. To avoid a notational overhead, we assume that the number of agents is constant during the simulation, and equal to N. Furthermore, we assume just one class of agents, having n internal state.

In particular, let $Y_i^{(N)} \in S$ represent the state of agent i, where $S = \{1,2,\dots,n\}$ is the state space of each agent. Multiple classes of agents can be represented in this way by suitably partitioning S into subsets, and allowing state changes only within a single class. Notice that we made explicit the dependence on N, the total population size.

A configuration of a system is thus represented by the tuple $(Y_1^{(N)},\dots,Y_N^{(N)})$. When dealing with population models, it is customary to assume that single agents in the same internal state cannot be distinguished, hence we can move from the agent representation to the system representation by introducing variables counting how many agents are in each state. To this purpose, define

$$X_j^{(N)} = \sum_{i=1}^{N} \mathbf{1}\{Y_i^{(N)} = j\}, \tag{1}$$

so that the system can be represented by the vector $\mathbf{X}^{(N)} = (X_1^{(N)},\dots,X_n^{(N)})$, whose dimension is independent of N. The domain of each variable $X_j^{(N)}$ is obviously $\{1,\dots,N\}$.

We will describe the evolution of the system by a set of transition rules at this global level. This simplifies the description of synchronous interactions between agents. The evolution from the perspective of a single agent will be reconstructed from the system level dynamics. In particular, we assume that $\mathbf{X}^{(N)}$ is a CTMC (Continuous-Time Markov Chain), with a dynamics described by a fixed number of transitions, collected in the set $\mathscr{T}^{(N)}$. Each transition $\tau \in \mathscr{T}^{(N)}$ is defined by a *multi-set* of *update rules* R_τ and by a rate function $r_\tau^{(N)}$. The multi-set[1] R_τ contains update rules $\rho \in R_\tau$ of the form $i \to j$, where $i, j \in S$. Each rule specifies that an agent changes state from ı to j. Let $m_{\tau,i\to j}$ denote the multiplicity of the rule $i \to j$ in R_τ. We assume that R_τ is independent of N, so that each transition involves a finite and fixed number of individuals. Given a multi-set of update rules R_τ, we can define the *update vector* $\mathbf{v}_\tau$ in the following way:

$$\mathbf{v}_{\tau,i} = \sum_{(i\to j)\in R_\tau} m_{\tau,i\to j}\mathbf{1}_j - \sum_{(i\to j)\in R_\tau} m_{\tau,i\to j}\mathbf{1}_i,$$

[1] The fact that R_τ is a multi-set, allows us to model events in which agents in the same state synchronise.

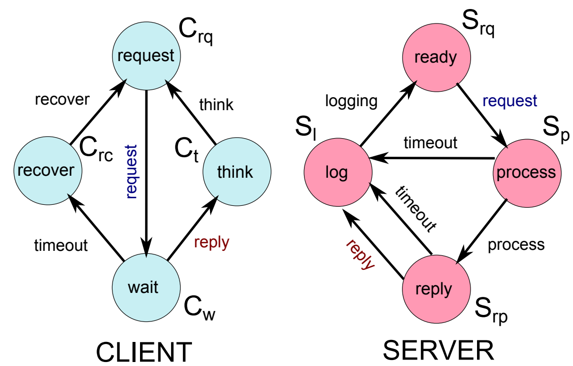


Figure 1: Visual representation of the client server system of the running example.

where $\mathbf{1}_i$ is the vector equal to one in position i and zero elsewhere. Hence, each transition changes the state from $\mathbf{X}^{(N)}$ to $\mathbf{X}^{(N)} + \mathbf{v}_\tau$. The rate function $r_\tau^{(N)}(\mathbf{X})$ depends on the current state of the system, and specifies the speed of the corresponding transition. It is assumed to be equal to zero if there are not enough agents available to perform a τ transition. Furthermore, it is required to be *Lipschitz continuous*. We indicate such a model by $\mathscr{X}^{(N)} = (\mathbf{X}^{(N)}, \mathscr{T}^{(N)}, \mathbf{x}_0^{(N)})$, where $\mathbf{x}_0^{(N)}$ is the initial state of the model.

Given a model $\mathscr{X}^{(N)}$, it is straightforward to construct the CTMC associated with it, exhibiting its infinitesimal generator matrix. First, its state space is $\mathscr{D} = \{(x_1, \ldots, x_n) \mid x_i \in \{1, \ldots, N\}, \sum_i x_i = N\}$. The infinitesimal generator matrix Q, instead, is the $\mathscr{D} \times \mathscr{D}$ matrix defined by

$$q_{\mathbf{x},\mathbf{x}'} = \sum \{r_\tau(\mathbf{x}) \mid \tau \in \mathscr{T},\ \mathbf{x}' = \mathbf{x} + \mathbf{v}_\tau\}.$$

We will indicate the state of such a CTMC at time t by $\mathbf{X}(t)$.

Example. We introduce now the main running example of the paper: we will consider a model of a simple client-server system, in which a pool of clients submits queries to a group of servers, waiting for a reply. In particular, the client asks for information from a server and waits for it to reply. It can time-out if too much time passes. The server, instead, after receiving a request does some processing and then returns the answer. It can time-out while processing and while it is ready to reply. After an action, it always logs data. The client and server agents are visually depicted in Figure 1. The global system is described by the following 8 variables:

- 4 variables for the client states: C_{rq}, C_w, C_{rc}, and C_t.
- 4 variables for the server states: S_{rq}, S_p, S_{rp}, and S_l.

Furthermore, there are 9 transitions in total, corresponding to all possible arrows of Figure 1. We list them in the following, stressing that synchronization between clients and servers has a rate computed using the minimum, in the PEPA style [26]. With $\mathbf{1}_X$ we denote a vector of length n which is equal to 1 for component X and zero elsewhere.

- request: $R_{request} = \{C_{rq} \to C_w, S_{rq} \to S_p\}$, $r_{request} = k_r \cdot \min(C_{rq}, S_{rq}))$;
- reply: $R_{reply} = \{C_w \to C_t, S_{rp} \to S_l\}$, $r_{reply} = \min(k_w C_w, k_{rp} S_{rp})$;
- timeout (client): $R_{timeout1} = \{C_w \to C_{rc}\}$, $r_{timeout1} = k_{to} C_w$;

- recover: $R_{recover} = \{C_{rc} \to C_{rq}\}$, $r_{recover} = k_{rec}C_{rc}$;
- think: $R_{think} = \{C_t \to C_{rq}, S_{rp} \to S_l\}$, $r_{think} = k_t C_t$;
- logging: $R_{logging} = \{S_l \to S_{rq}\}$, $R_{logging} = k_l S_l$;
- process: $\mathbf{v}_{process} = \{S_p \to S_{rp}\}$, $R_{process} = k_p S_p$;
- timeout (server processing): $R_{timeout2} = \{S_p \to S_l\}$, $r_{timeout2} = k_{sto}S_p$;
- timeout (server replying): $R_{timeout3} = \{S_{rp} \to S_l\}$, $r_{timeout3} = k_{sto}S_{rp}$;

The system-level models we have defined depend on the total population N and on the ration between server and clients, which is specified by the initial conditions. Increasing the total population N (keeping fixed the client-server ratio), we obtain a sequence of models, and we are interested in their limit behaviour, for N going to infinity.

In order to compare the models of such a sequence, we will normalize them to the same scale, dividing each variable by N and thus introducing the normalized variables $\hat{\mathbf{X}}^{(N)} = \frac{\mathbf{X}^{(N)}}{N}$. In case of a constant population, normalised variables are usually referred to as the *occupancy measure*, as they represent the fraction of agents in each state. Update vectors are scaled correspondingly. i.e. dividing them by N. Furthermore, we will also require a proper scaling (in the limit) of the rate functions of the normalized models. More precisely, let $\mathscr{X}^{(N)} = (\mathbf{X}^{(N)}, \mathscr{T}^{(N)}, \mathbf{X_0}^{(N)})$ be the N-th non-normalized model and $\hat{\mathscr{X}}^{(N)} = (\hat{\mathbf{X}}^{(N)}, \hat{\mathscr{T}}^{(N)}, \hat{\mathbf{X}}_{\mathbf{0}}^{(N)})$ the corresponding normalized model. We require that:

- initial conditions scale properly: $\hat{\mathbf{X}}_{\mathbf{0}}^{(N)} = \frac{\mathbf{X_0}^{(N)}}{N}$;
- for each transition $(\mathbf{v}_\tau, r_\tau^{(N)}(\mathbf{X}))$ of the non-normalized model, let $\hat{r}_\tau^{(N)}(\hat{\mathbf{X}})$ be the rate function expressed in the normalised variables (i.e., after a change of variables). The corresponding transition in the normalized model is $(R_\tau, \hat{r}_\tau^{(N)}(\hat{\mathbf{X}}))$, with update vector equal to $\frac{1}{N}\mathbf{v}_\tau$. We assume that there exists a bounded and Lipschitz continuous function $f_\tau(\hat{\mathbf{X}}) : E \to \mathbb{R}^n$ on normalized variables (where E contains all domains of all $\hat{\mathscr{X}}^{(N)}$), independent of N, such that $\frac{\hat{r}_\tau^{(N)}(\mathbf{x})}{N} \to f_\tau(\mathbf{x})$ *uniformly* on E.

In accordance to the previous subsection, we will denote the state of the CTMC of the N-th non-normalized (resp. normalized) model at time t as $\mathbf{X}^{(N)}(t)$ (resp. $\hat{\mathbf{X}}^{(N)}(t)$).

Example. Consider again the running example. If we want to scale the model with respect to the scaling parameter N, we can increase the initial population of clients and servers by a factor k (hence keeping the client-server ration constant), similarly to [52]. The condition on rates, in this case, automatically holds due to their (piecewise) linear nature. For non-linear rate functions, the convergence of rates can usually be enforced by properly scaling parameters with respect to total population N.

3.2 Deterministic limit theorem

In order to present the "classic" deterministic limit theorem, we need to introduce a few more concepts needed to construct the limit ODE. Consider a sequence of normalized models $\hat{\mathscr{X}}^{(N)}$ and let $\mathbf{v}_\tau$ be the (non-normalised) update vectors. The drift $F^{(N)}(\hat{\mathbf{X}})$ of $\hat{\mathscr{X}}$ is defined as

$$F^{(N)}(\hat{\mathbf{X}}) = \sum_{\tau \in \hat{\mathscr{T}}} \frac{1}{N}\mathbf{v}_\tau \hat{r}_\tau^{(N)}(\hat{\mathbf{X}}) \tag{2}$$

Furthermore, let $f_\tau : E \to \mathbb{R}^n$, $\tau \in \hat{\mathscr{T}}$ be the limit rate functions of transitions of $\hat{\mathscr{X}}^{(N)}$. We define the *limit drift* of the model $\hat{\mathscr{X}}^{(N)}$ as

$$F(\hat{\mathbf{X}}) = \sum_{\tau \in \hat{\mathscr{T}}} \mathbf{v}_\tau f_\tau(\hat{\mathbf{X}}) \tag{3}$$

It is easily seen that $F^{(N)}(\mathbf{x}) \to F(\mathbf{x})$ uniformly.

The limit ODE is $\frac{d\mathbf{x}}{dt} = F(\mathbf{x})$, with $\mathbf{x}(0) = \mathbf{x_0} \in S$. Given that F is Lipschitz in E (as all f_τ are), the ODE has a unique solution $\mathbf{x}(t)$ in E starting from $\mathbf{x_0}$. Then, the following theorem can be proved [18,37]:

Theorem 3.1 (Deterministic approximation [18, 37])**.** *Let the sequence $\hat{\mathbf{X}}^{(N)}(t)$ of Markov processes and $\mathbf{x}(t)$ be defined as before, and assume that there is some point $\mathbf{x_0} \in S$ such that $\hat{\mathbf{X}}^{(N)}(0) \to \mathbf{x_0}$ in probability. Then, for any* finite *time horizon $T < \infty$, it holds that:*

$$\mathbb{P}(\sup_{0 \le t \le T} ||\hat{\mathbf{X}}^{(N)}(t) - \mathbf{x}(t)|| > \varepsilon) \to 0.$$

Notice that the theorem can be specialised to subsets $E' \subseteq E$, in which case it can provide also an estimate of exit times from set E', see [18]. Furthermore, if the initial conditions converge almost surely, then also $(\sup_{0 \le t \le T} ||\hat{\mathbf{X}}^{(N)}(t) - \mathbf{x}(t)|| \to 0$ almost surely [36].

3.3 Fast simulation

We now turn our attention back to a single individual in the population. Even if the system-level dynamics, in the limit of a large population, becomes deterministic, the dynamics of a single agent remains a stochastic process. However, the fluid limit theorem implies that the dynamics of a single agent, in the limit, becomes essentially dependent on the other agents only through the global system state. This asymptotic decoupling allows us to find a simpler Markov Chain for the evolution of the single agent. This result is often known in literature [19] under the name of *fast simulation* [23].

To explain this point formally, let us focus on a single individual $Y_h^{(N)}$, which is a Markov chain on the state space $S = \{1, \ldots, n\}$. Let $Q^{(N)}(\mathbf{x})$ be the infinitesimal generator matrix of $Y_h^{(N)}$, described as a function of the normalized state of the population $\hat{\mathbf{X}}^{(N)} = \mathbf{x}$, i.e.

$$\mathbb{P}\{Y_h^{(N)}(t+dt) = j \mid Y_h^{(N)}(t) = i, \hat{\mathbf{X}}^{(N)}(t) = \mathbf{x}\} = q_{i,j}^{(N)}(\mathbf{x})dt.$$

We stress that this is the exact Markov Chain for $Y_h^{(N)}$, conditional on $\hat{\mathbf{X}}^{(N)}(t) = \mathbf{x}$ and that this process is *not independent* of $\hat{\mathbf{X}}^{(N)}(t)$. In fact, without conditioning on $\hat{\mathbf{X}}^{(N)}$, $Y_h^{(N)}(t)$ is not a Markov process. This means that in order to capture its evolution in a Markovian setting, one has to consider the Markov chain $(Y_h^{(N)}(t), \hat{\mathbf{X}}^{(N)}(t))$.

Example. Consider the running example, and suppose we want to construct the CTMC for a single client. For this purpose, we have to extract from the specification of global transitions a set of local transitions for the client. The state space of a client will consist of four states, $S_c = \{rq, w, t, rc\}$.

Then, we need to define its rate matrix $Q^{(N)}$. In order to do this, we need to take into account all global transitions involving a client, and then extract the rate at which a specific client can perform such a transition. As a first example, consider the `think` transition, changing the state of a client from t to rq. Its global rate is $r_{think} = k_t C_t$. As we have C_t clients in state t, the rate at which a specific one will perform a think transition is $\frac{k_t C_t}{C_t} = k_t$. Hence, we just need to divide the global rate of observing a think transition by the total number of clients in state t. Notice that, as we are assuming that one specific client is in state t, then $C_t \ge 1$, hence we are not dividing by zero.

Consider now a `reply` transition. In this case, the transition involves a server and a client in state w. The global rate is $r_{reply} = min(k_w C_w, k_{rp} S_{rp})$, and $C_w \geq 1$ (in the non-normalized model with total population N). Dividing this rate by C_w, we obtain $\min(k_w, k_{rp}\frac{S_{rp}}{C_w})$, which is defined for $C_w > 0$. If we switch to normalised variables, we obtain a similar expression: $\min(k_w, k_{rp}\frac{s_{rp}}{c_w})$, which is independent of N. However, in taking N to the limit we must be careful: even if in the non-normalized model C_w (and hence c_w) are always non-zero (if a specific agent is in state w), this may not be true in the limit: if only one client is in state w, then the limit fraction of clients in state w is zero (just take the limit of $\frac{1}{N}$). Hence, we need to take care of boundary conditions, guaranteeing that the single-agent rate is defined also in these circumstances. In this case, we can assume that the rate is zero if s_{rp} is zero (whatever the value of c_w), and that the rate is k_w if c_w is zero but $s_{rp} > 0$.

In order to treat the previous set of cases in a homogeneous way, we make the following assumption on rates:

Definition 3.1. Let $\tau \in \mathscr{T}$ be a transition such that its update rule set contains the rule $i \to j$, with multiplicity $m_{\tau,i\to j}$. The rate $r_\tau^{(N)}$ is *single-agent-i compatible* if there exists a Lipschitz continuous function $f_\tau^i(\mathbf{x})$ on normalized variables such that the limit rate on normalized variables $f_\tau(\mathbf{x})$ can be factorised as $f_\tau(\mathbf{x}) = x_i f_\tau^i(\mathbf{x})$. A transition τ is *single-agent compatible* if and only if it is single-agent-i compatible for any i (appearing in the left-hand side of an update rule).

Hence, the limit rate of observing a transition from i to j for a specific agent in state i is $m_{\tau,i\to j} f_\tau^i(\mathbf{x})$, where the factor $m_{\tau,i\to j}$ comes from the fact that it is one out of $m_{\tau,i\to j}$ agents changing state from i to j due to τ.[2]

Then, assuming all transitions τ are single-agent compatible, we can define the rate $q_{i,j}^{(N)}$ as

$$q_{i,j}^{(N)}(\mathbf{X}) = \sum_{\tau\in\mathscr{T} \mid \{i\to j\}\subseteq R_\tau} m_{\tau,i\to j} \frac{r^{(N)}\tau(\mathbf{X})}{X_i} = \sum_{\tau\in\hat{\mathscr{T}} \mid \{i\to j\}\subseteq R_\tau} m_{\tau,i\to j} \frac{\hat{r}^{(N)}\tau(\hat{\mathbf{X}})}{\hat{X}_i} = q_{i,j}^{(N)}(\hat{\mathbf{X}}).$$

It is then easy to check that

$$q_{i,j}^{(N)}(\mathbf{x}) \to q_{i,j}(\mathbf{x}) = \sum_{\tau\in\mathscr{T} \mid \{i\to j\}\subseteq R_\tau} m_{\tau,i\to j} \frac{f_\tau(\mathbf{x})}{x_i} = \sum_{\tau\in\hat{\mathscr{T}} \mid \{i\to j\}\subseteq R_\tau} m_{\tau,i\to j} f_\tau^i(\mathbf{x}).$$

In the following, we fix an integer $k > 0$ and let $Z_k^{(N)} = (Y_1^{(N)}, \ldots, Y_k^{(N)})$ be the CTMC tracking the state of k selected agents among the population, with state space $\mathscr{S} = S^k$. Notice that k is fixed and independent of N, so that we will track k individuals embedded in a population that can be very large.

Let $\mathbf{x}(t)$ be the solution of the fluid ODE, and assume to be under the hypothesis of Theorem 3.1. Consider now $z_k^{(N)}(t)$ and $z_k(t)$, the *time-inhomogeneous* CTMCs on $\mathscr{S}$ defined by the following infinitesimal generators (for any $h = 1, \ldots, k$):

$$\mathbb{P}\{z_k^{(N)}(t+dt) = (z_1, \ldots, j, \ldots, z_k) \mid z_k^{(N)}(t) = (z_1, \ldots, i, \ldots, z_k)\} = q_{i,j}^{(N)}(\mathbf{x}(t))dt,$$
$$\mathbb{P}\{z_k(t+dt) = (z_1, \ldots, j, \ldots, z_k) \mid z_k(t) = (z_1, \ldots, i, \ldots, z_k)\} = q_{i,j}(\mathbf{x}(t))dt,$$

Notice that, while $Z_k^{(N)}$ describes exactly the evolution of k agents, $z_k^{(N)}$ and $\mathbf{z}_k$ do not. In fact, they are CTMCs in which the k agents evolve independently, each one with the same infinitesimal generator, depending on the global state of the system via the fluid limit.

However, the following theorem can be proved [19]:

[2]The factor m stems from the following simple probabilistic argument: if we choose at random m agents out of X_i, then the probability to select a specific agent is $\frac{m}{X_i}$.

Theorem 3.2 (Fast simulation theorem)**.** *For any $T < \infty$, $\mathbb{P}\{Z_k^{(N)}(t) \neq z_k^{(N)}(t), \text{for some } t \leq T\} \to 0$, and $\mathbb{P}\{Z_k^{(N)}(t) \neq z_k(t), \text{for some } t \leq T\} \to 0$, as $N \to \infty$.*

This theorem states that, in the limit of an infinite population, each fixed set of k agents will behave independently, sensing only the mean state of the global system, described by the fluid limit $\mathbf{x}(t)$. Furthermore, those k agents will evolve independently, as if there was no synchronisation between them. This *asymptotic decoupling* of the system, holding for any set of k agents, is also known in the literature under the name of *propagation of chaos* [10]. In particular, this holds either if we define the rate of the limit CTMC by the single-agent rates for population N ($z_k^{(N)}$) or the limit rates (z_k). Notice that, when the CTMC has density dependent rates [36], then $z_k^{(N)}(t) = z_k(t)$, as their infinitesimal generators will be the same.

We stress once again that the process $Z_k^{(N)}(t)$ is not a Markov process. It becomes a Markov process when considered together with $\hat{\mathbf{X}}^{(N)}(t)$. This can be properly understood observing that it is the projection of the Markov process $(Y_1^{(N)}(t), \ldots, Y_N^{(N)}(t))$ on the first k coordinates, and recalling that a projection of a Markov process need not be Markov (intuitively, we can throw away some relevant information about the state of the process). However, being the projection of a Markov process, the probability of $Z_k^{(N)}(t)$ at each time t is perfectly defined. Yet, its non-Markovian nature has consequences for what concerns reachability probabilities and the satisfiability of CSL formulae.

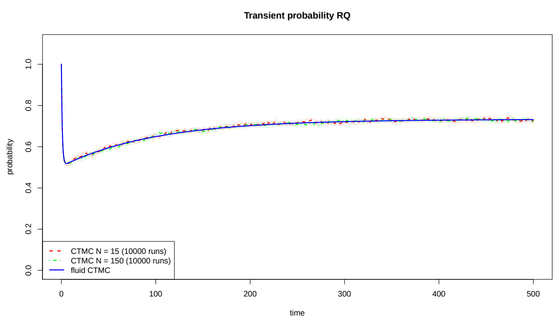
Example. Consider again the client-server example, and focus on a single client. As said before, its state space is $S_c = \{rq, w, t, rc\}$, and the non-null rates of the infinitesimal generator Q for the process z_1 are:

- $q_{rq,w}(t) = k_r \min\{1, s_{rq}(t)/c_{rq}(t)\}$ (with appropriate boundary conditions);
- $q_{w,t}(t) = \min\{k_w, k_{rp} s_{rp}(t)/c_w(t)\}$;
- $q_{w,rc}(t) = k_{to}$;
- $q_{t,rq}(t) = k_t$;
- $q_{rc,rq}(t) = k_{rc}$.

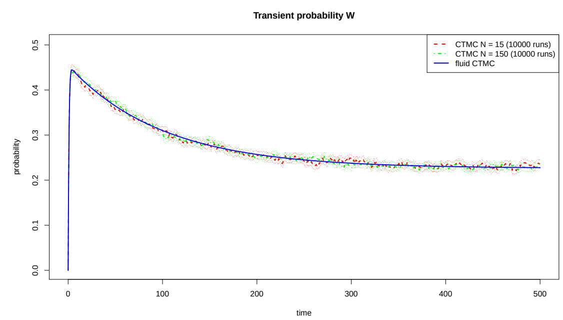
In Figure 2, we show a comparison of the transient probabilities for the approximating chain for a single client and the true transient probabilities, estimated by Monte Carlo sampling of the CTMC, for different population levels N. As we can see, the approximation in quite precise already for $N = 15$.

Remark 3.1. Single-agent consistency is not a very restrictive condition. However, there are cases in which it is not satisfied. One example is passive rates in PEPA [26]. In this case, in fact, the rate of the synchronization of $P = (\alpha, \top).P1$ and $Q = (\alpha, r).Q1$ is $rX_Q\mathbf{1}\{X_P > 0\}$. In particular, the rate is independent of the exact number of P agents. If we look at a single P-agent rate, it equals $r\frac{X_Q}{X_P}\mathbf{1}\{X_P > 0\}$. Normalising variables, we get the rate $r\frac{x_Q}{x_P}\mathbf{1}\{x_P > 0\}$, which approaches infinity as x_P goes to zero (for x_Q fixed). Hence, it cannot be extended to a Lipschitz continuous function. However, in the case $x_P = 0$ and $x_Q > 0$, if we look at a single agent, then the speed at which P changes state is in fact infinite. We can see this by letting $X_P = 1$ and $X_Q = Nq$, so that the rate of the transition from the point of view of P is $Nq \to \infty$. Thus, in the limit, the state P becomes vanishing.

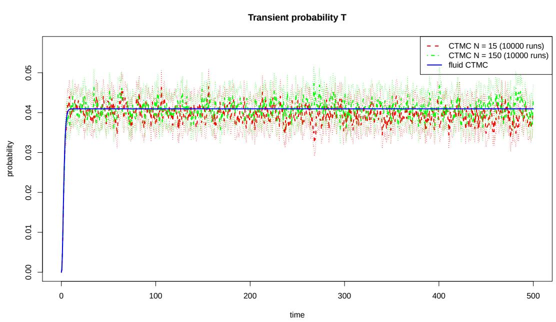
Remark 3.2. The hypothesis of constant population, i.e. the absence of birth and death, can be relaxed. The fluid approximation continues to work also in the presence of birth and death events, and so does the fast simulation theorem. In our framework, birth and death can be easily introduced by allowing rules of the form $\emptyset \to i$ (for birth) and $i \to \emptyset$ (for death). In terms of a single agent, death can be dealt with by adding a single absorbing state to its CTMC. Birth, instead, means that we can choose the time instant at



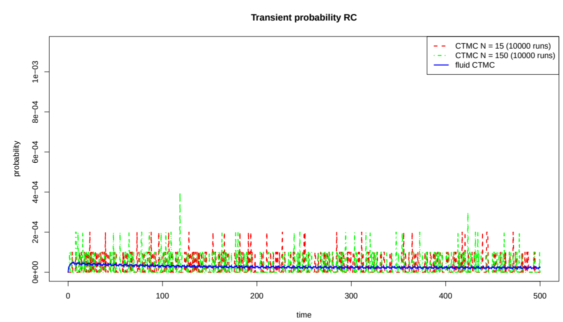
(a) $\mathbb{P}\{rq\}$



(b) $\mathbb{P}\{w\}$



(c) $\mathbb{P}\{t\}$



(d) $\mathbb{P}\{rc\}$

Figure 2: Comparison of the transient probability for all four states of the fluid model of the client server system, computed solving the Kolmogorov forward equations, and the transient probability of CTMC models for $N = 15$ and $N = 150$ (2:1 client server ratio). Parameters are $k_r = 1$, $k_w = 100$, $k_{to} = 0.01$, $k_t = 1$, $k_{rc} = 100$ $k_l = 10$, $k_p = 0.1$, $k_{sto} = 0.005$, initial conditions of the full system are $C_{rq} = n$, $S_{rq} = m$, while the single client CTMC starts in state rq.

which an agent enters the system (provided that there is a non-null rate for birth transitions at the chosen time).

Another solution would be to assume an infinite pool of agents, among which only finitely many can be alive, and the others are an infinite supply of "fresh souls". Even if this is plausible from the point of view of a global model, it creates problems in terms of a single agent perspective (what is the rate of birth of a soul?). A solution can be to assume a large but finite pool of agents. But in this case birth becomes a passive action (and it introduces discontinuities in the model, even if in many cases one can guarantee to remain far away the discontinuous boundary), hence we face the same issues discussed in Remark 3.1.

3.4 Continuous Stochastic Logics

In this section we consider labelled stochastic processes. A labelled stochastic process is a random process $Z(t)$, with state space $\mathcal{S}$ and a labelling function $L : \mathcal{S} \to 2^{\mathcal{P}}$, associating with each state $s \in \mathcal{S}$ a subset of atomic propositions $L(s) \subset \mathcal{P} = \{a_1, \dots, a_k \dots\}$ true in that state: each atomic proposition $a_i \in \mathcal{P}$ is true in s if and only if $a_i \in L(s)$. We require that all subsets of paths considered are measurable. This condition will be satisfied by all subsets considered in the paper. Usually, $Z(t)$ is a CTMC, defined by an infinitesimal generator matrix $Q(t)$ (possibly depending on time).

From now on, we always assume we are working with labelled stochastic processes.

A path of $Z(t)$ is a sequence $\sigma = s_0 \xrightarrow{t_0} s_1 \xrightarrow{t_1} \dots$, such that the probability of going from s_i to s_{i+1} at time $T_i = \sum_{j=0}^{i} t_i$, is greater than zero. For CTMCs, this condition is equivalent to $q_{s_i,s_{i+1}}(T_i) > 0$. Denote with $\sigma@t$ the state of σ at time t.

A time-bounded CSL formula φ is defined by the following syntax:

$$\varphi = a \mid \varphi_1 \wedge \varphi_2 \mid \neg\varphi \mid \mathcal{P}_{\bowtie p}(\varphi_1 U^{[T_1,T_2]} \varphi_2).$$

The satisfiability relation of φ with respect to a labelled stochastic process $Z(t)$ is given by the following rules:

- $s, t_0 \models a$ if and only if $a \in L(s)$;
- $s, t_0 \models \neg\varphi$ if and only if $s, t_0 \not\models \varphi$;
- $s, t_0 \models \varphi_1 \wedge \varphi_2$ if and only if $s, t_0 \models \varphi_1$ and $s, t_0 \models \varphi_2$;
- $s, t_0 \models \mathcal{P}_{\bowtie p}(\varphi_1 U^{[T_1,T_2]} \varphi_2)$ if and only if $\mathbb{P}\{\sigma \mid \sigma, t_0 \models \varphi_1 U^{[T_1,T_2]} \varphi_2\} \bowtie p$.
- $\sigma, t_0 \models \varphi_1 U^{[T_1,T_2]} \varphi_2$ if and only if $\exists \bar{t} \in [t_0+T_1, t_0+T_2]$ s.t. $\sigma@\bar{t}, \bar{t} \models \varphi_2$ and $\forall t_0 \le t < \bar{t}$, $\sigma@t, t \models \varphi_1$.

Notice that we are considering a fragment of CSL without the next temporal operator, and allowing only time-bounded properties. This last restriction is connected with the nature of convergence theorems 3.1 and 3.2, which hold only on finite time horizons, see however Remark 5.4 for possible relaxations of this restriction.

Model checking of an until CSL formula $\mathcal{P}_{\bowtie p}(\varphi_1 U^{[T_1,T_2]} \varphi_2)$ in a *time-homogeneous CTMC* $Z(t)$ can be reduced to the computation of two reachability problems, which themselves can be solved by transient analysis [6]. In particular, consider the sets of states $U = [\![\neg\varphi_1]\!]$ and $G = [\![\varphi_2]\!]$ and compute the probability of going from state $s_1 \notin U$ to a state $s_2 \notin U$ in T_1 time units, in the CTMC in which all U-states are made absorbing, $\pi^1_{s_1,s_2}(T_1)$. Furthermore, consider the modified CTMC in which all U and G states are made absorbing, and denote by $\pi^2_{s_2,s_3}(T_2 - T_1)$ the probability of going from a state $s_2 \notin U$ to a state $s_3 \in G$ in $T_2 - T_1$ units of time in such a CTMC. Then the probability of the until formula in state s can be computed as $P_s(\varphi) = \sum_{s_3 \in G, s_2 \notin U} \pi^1_{s_1,s_2}(T_1)\pi^2_{s_2,s_3}(T_2 - T_1)$. The probabilities π^1 and π^2 can be computed using standard methods for transient analysis (e.g. by uniformisation [28] or by solving the Kolmogorov equations [41]). Then, to determine the truth value of the formula φ in state s, one has just to solve the inequality $P_s(\varphi) \bowtie p$. The truth value of a generic CSL formula can therefore be computed recursively on the structure of the formula.

4 Reachability

In this section, we will focus on reachability properties of a single agent (or a fixed set of agents), in a population of increasing size. Essentially, we want to compute the probability of the set of traces reaching some goal state $G \subseteq \mathscr{S}$ within T units of time, starting at time t_0 and avoiding unsafe states in $U \subseteq \mathscr{S}$. The key point is that the reachability probability of the limit CTMC $z_k(t)$ obtained by Theorem 3.2 approximates the reachability probability of a single agent in a large population of size N, i.e. the reachability probability for $Z_k^{(N)}(t)$.

In the rest of the section, we will consider two versions of the reachability problem: one for constant goal and unsafe sets, and one in which G and U depend on time (i.e. a state may belong to G or U depending on time t). We will state these problems for a generic ICTMC $Z(t)$ on state space $\mathscr{S}$:

Definition 4.1. Let $Z(t)$ be a CTMC with state space $\mathscr{S}$ and infinitesimal generator matrix $Q(t)$.

1. Let $U, G \subseteq \mathscr{S}$. The *constant-set reachability* $P_{reach}(Z, t_0, T, G, U)[s]$ is the probability of the set of trajectories of Z reaching a state in G without passing through a state in U, within T time units, starting at time t_0 in state s. $P_{reach}(Z, t_0, T, G, U)$ is the reachability probability vector on $\mathscr{S}$.
2. Let $U, G : [t_0, t_1] \times \mathscr{S} \to \{0, 1\}$ be time-dependent sets, identified with their indicator function (i.e. $G(t), U(t)$ are the goal and the unsafe sets at time t). The *time-varying-set reachability* $P_{reach}(Z, t_0, T, G(t), U(t))[s]$ is the probability of the set of trajectories of Z reaching a state in $G(t)$ at time $t \in [t_0, t_0 + T]$ without passing through a state in $U(t')$, for $t' \in [t_0, t]$, starting at time t_0 in state s.

The interest in the time-varying set reachability is intimately connected with CSL model checking. In fact, the truth value of a CSL formula in a state s for the process $Z_k^{(N)}(t)$, where it is a non-Markov process, depends on the initial time at which we start evaluating the formula. This is because $Z_k^{(N)}(t)$ depends on time via the state of $\hat{\mathbf{X}}^{(N)}(t)$. Furthermore, time-dependence of truth values of CSL formulae manifests also for the limit process $z_k(t)$, which is a time-inhomogeneous Markov Process. Therefore, in the computation of the probability of an until formula, which can be reduced to the computation of two reachability problems, we need to consider time-varying-sets. As a matter of fact, we will see that dealing with time varying sets (like those obtained by solving the inequality $P_{reach}(Z, t_0, T, G(t), U(t)) \bowtie p$, for $\bowtie \in \{<, \leq, > \geq\}$) is much harder, and we will need to impose some additional regularity on the rate functions of Z and on the time-dependence of goal and unsafe sets.

In the following sections, we will first deal with the specific reachability problem for a generic ICTMC $Z(t)$, presenting an effective way of computing such probability, and then studying the relationship between the reachability probabilities of $Z_k^{(N)}(t)$ and $z_k(t)$.

4.1 Constant-set reachability

We consider constant-set reachability, as defined in Def. 4.1. For the rest of this section let $Z(t)$ be an ICTMC on $\mathscr{S}$, with rate matrix $Q(t)$ and initial state $Z(0) = Z_0 \in \mathscr{S}$. We will solve the reachability problem in a standard way, by reducing it to the computation of transient probabilities in a modified ICTMC [6]. The solution is similar to the one proposed in [16].

Let $\Pi(t_1,t_2)$ be the probability matrix of $Z(t)$, in which entry $\pi_{s_1,s_2}(t_1,t_2)$ gives the probability of being in state s_2 at time t_2, given that we were in state s_1 at time t_1. The *Kolmogorov forward and backward equations* describe the time evolution of $\Pi(t_1,t_2)$ as a function of t_2 and t_1, respectively. More precisely, the forward equation is $\frac{\partial \Pi(t_1,t_2)}{\partial t_2} = \Pi(t_1,t_2)Q(t_2)$, while the backward equation is $\frac{\partial \Pi(t_1,t_2)}{\partial t_1} = -Q(t_1)\Pi(t_1,t_2)$.

The constant-set reachability problem, for a given initial time t_0, can be solved by integration of the forward Kolmogorov equation (with initial value given by the identity matrix) in the modified ICTMC $Z'(t)$, with infinitesimal generator matrix $Q'(t)$, in which all unsafe states and goal states are made absorbing [6] (i.e., $q'_{s_1,s_2}(t) = 0$, for each $s_1 \in G \cup U$). In particular, $P_{reach}(Z,t_0,T,G,U) = \Pi'(t_0,t_0+T)\mathbf{e}_G$, where $\mathbf{e}_G$ is an $n \times 1$ vector equal to 1 if $s \in G$ and 0 otherwise, and Π' is the probability matrix of the modified ICTMC Z'.[3] We underline that, in order for the initial value problem defined by the Kolmogorov forward equation to be well posed, the infinitesimal generator matrix $Q(t)$ has to be sufficiently regular (e.g. bounded and integrable).

As already remarked, the reachability probability for ICTMC can depend on the initial time t_0 at which we start the process, in contrast with time-homogeneous CTMC. Consider now the problem of computing $P(t) = P_{reach}(Z,t,T,G,U)$ as a function of $t \in [t_0,t_1]$. To this end, we can solve the forward equation for t_0 and then use the chain rule to define a differential equation for $\Pi(t,t+T)$, solving it using $\Pi(t_0,t_0+T)$ as the initial condition. The above mentioned equation is

$$\frac{d\Pi(t,t+T)}{dt} = \frac{\partial \Pi(t,t+T)}{\partial t} + \frac{\partial \Pi(t,t+T)}{\partial (t+T)}\frac{d(t+T)}{dt} = -Q(t)\Pi(t,t+T) + \Pi(t,t+T)Q(t+T).$$

Using a numerical solver for ODE, this gives an effective algorithm to compute the probability of interest (with any fixed error bound). Furthermore, if we can guarantee that the number of zeros of the equation $P(t) - p$ is finite, then we also have an effective procedure to compute the truth value of $P(t) \bowtie p$, for $\bowtie \in \{<,\leq,\geq,>\}$.

Consider now the sequence of processes $Z_k^{(N)}$ defined in Section 3.3. We are interested in the asymptotic behaviour of $P_{reach}(Z_k^{(N)},t,T,G,U)$. The following result is a consequence of Theorem 3.2:

Proposition 4.1. *Let $\mathscr{X}^{(N)}$ be a sequence of CTMC models, as defined in Section 3.1, and let $Z_k^{(N)}$ and z_k be defined from $\mathscr{X}^{(N)}$ as in Section 3.3. Assume that the infinitesimal generator matrix $Q(t)$ of z_k is bounded and integrable in every compact interval $[0,T]$. Then*

- $P_{reach}(Z_k^{(N)},t,T,G,U) \to P_{reach}(z_k,t,T,G,U)$ *in probability, as $N \to \infty$.*
- *For any $0 \leq t_0 < t_1 < \infty$, $\sup_{t\in[t_0,t_1]} \|P_{reach}(Z_k^{(N)},t,T,G,U) - P_{reach}(z_k,t,T,G,U)\| \to 0$ in probability, as $N \to \infty$.*

Proof. The proposition follows from Theorem 3.2, which states that $\mathbb{P}\{Z_k^{(N)}(t) \neq z_k(t), \text{for some } t \leq T'\} \to 0$. By a standard coupling argument, we can assume that the processes $Z_k^{(N)}$ and z_k are defined on the same probability space Ω. Therefore, there exists sequence $\varepsilon_N \in \mathbb{R}_+$, $\varepsilon_N \to 0$, such that $\mathbb{P}\{\omega \in \Omega \mid \forall t \leq T', Z_k^{(N)}(\omega,t) = z_k(\omega,t)\} \geq 1 - \varepsilon_N$. This means that with probability $1-\varepsilon_N$, the trajectories of the two processes are the same up to time T'.

[3] Clearly, alternative ways of computing the transient probability, like uniformization for ICTMC [3], can be used as well. However, we stick to the ODE formulation in order to deal with dependency on initial time t_0.

Now, we can define a (measurable) function $\chi = \chi_{t,T,G,U}$ on the trajectories of the CTMCs which equals 1 if they satisfy the reachability property, and 0 otherwise. Therefore, it holds that $P_{reach}(Z_k^{(N)}, t, T, G, U) = \mathbb{E}[\chi(Z_k^{(N)})]$, and similarly for z_k. Now, let $\Omega_1 = \{\omega \mid Z_k^{(N)}(t,\omega) = z_k(t,\omega), \forall t \leq t_0 + T\}$, $\Omega_0 = \{\omega \mid Z_k^{(N)}(t,\omega) \neq z_k(t,\omega)\}$, and μ_Ω be the probability measure in Ω (i.e. in the trajectory space). Observe that $\chi(Z_k^{(N)}) = \chi(z_k)$ on Ω_1 and $\mathbb{P}(\Omega_0) \leq \varepsilon_N$, hence

$$\begin{aligned}
|\mathbb{E}[\chi(Z_k^{(N)})] - \mathbb{E}[\chi(z_k)]| &\leq \mathbb{E}[|\chi(Z_k^{(N)}) - \chi(z_k)|] \\
&= \int_{\Omega_1} |\chi(Z_k^{(N)}) - \chi(z_k)| d\mu_\Omega + \int_{\Omega_0} |\chi(Z_k^{(N)}) - \chi(z_k)| d\mu_\Omega \\
&\leq \varepsilon_N \to 0.
\end{aligned}$$

Similar reasoning allows us to prove point two of the proposition: just apply Theorem 3.2 for $t \leq T + t_1$ (the point is that the convergence implied by Theorem 3.2 is uniform, i.e. the sequence ε_N does not depend on the initial and final time of the reachability property, if they are both less than $T + t_1$). ■

The previous proposition shows that the reachability probability for $Z_k^{(N)}$ converges to the reachability probability for z_k, hence for large N we can approximate the former with the latter.

It is interesting to observe how the reachability probability for $Z_k^{(N)}(t)$ depends on the initial time. As already remarked, $Z_k^{(N)}(t)$ is not a Markov-process, but $(Z_k^{(N)}, \hat{\mathbf{X}}^{(N)})(t)$ is. Furthermore, we can obtain $Z_k^{(N)}(t)$ by projecting on the first component of $(Z_k^{(N)}, \hat{\mathbf{X}}^{(N)})(t)$. The reachability probability for $Z_k^{(N)}(t)$ can be obtained from that of $(Z_k^{(N)}, \hat{\mathbf{X}}^{(N)})(t)$ in the following way: compute the reachability probability $P_{U,G}(s,x,T)$ for each state $(s,\mathbf{x})$ of $(Z_k^{(N)}, \hat{\mathbf{X}}^{(N)})$ with time horizon T. As $(Z_k^{(N)}, \hat{\mathbf{X}}^{(N)})$ is a time-homogeneous CTMC, this probability is independent of the initial time. Fix a state $s \in \mathscr{S}$ of $Z_k^{(N)}$, and consider the probability $P_{s,\mathbf{x}}(t|s) = \mathbb{P}\{(Z_k^{(N)}, \hat{\mathbf{X}}^{(N)})(t) = (s,x) \mid Z_k^{(N)}(t) = s\}$ of being in (s,x) at time t, conditional on being in s, i.e. $P_{s,\mathbf{x}}(t|s) = \mathbb{P}\{(Z_k^{(N)}, \hat{\mathbf{X}}^{(N)})(t) = (s,x)\} / \sum_{\mathbf{x}} \mathbb{P}\{(Z_k^{(N)}, \hat{\mathbf{X}}^{(N)})(t) = (s,x)\}$. Then, this is the initial distribution of $(Z_k^{(N)}, \hat{\mathbf{X}}^{(N)})$ that we have to take into account when computing the reachability probability $P_{reach}(Z_k^{(N)}, t, T, G, U)[s]$, starting at time t. It follows that

$$P_{reach}(Z_k^{(N)}, t, T, G, U)[s] = \sum_{\mathbf{x} \in \hat{\mathscr{D}}} P_{s,\mathbf{x}}(t|s) P_{U,G}(s,x,T), \tag{4}$$

which depends on t via $P_{s,\mathbf{x}}(t|s)$.
As a consequence, the answer to a question like $P_{reach}(Z_k^{(N)}, t, T, G, U)[s] > p$, $p \in [0,1]$, for $Z_k^{(N)}$ depends on the initial time t: *truth is time-dependent in* $Z_k^{(N)}$.

Example. We consider again the client-server example of Section 3.1, and focus on two reachability probabilities for a single client:

1. The probability of observing a time-out before being served for the first time within time T. This is a reachability problem with goal set $G = \{rc\}$ and unsafe set $U = \{rq, w\}$.
2. The probability of observing a timeout within time T. This is a reachability problem with goal set $G = \{rc\}$ and unsafe set $U = \emptyset$.[4]

[4] In fact, this is a first passage time problem.

In Figures 3(a), 3(b), 4(a) and 4(b) we can observe a comparison between the values computed for the limit CTMC z and the exact CTMC $Z^{(N)}$, for $N = 15$ or $N = 150$ (with a client-server ratio of 2:1), as a function of the time horizon T. As can be seen, the probability for z is in very good agreement with that of $Z^{(N)}$ (computed using a statistical approach, from a sample of 10000 traces) even for N very small. As far as running time is concerned, the fluid model checking is 100 times faster for $N = 15$ and 1000 times faster for $N = 150$ than the stochastic simulation. What is even more important is that the complexity of the fluid approach is independent of N, hence its computational cost (on the order of 200 milliseconds for all cases considered here) can scale to much larger systems. Furthermore, another advantage of the fluid approach is that, by solving a set of differential equations, we are computing the reachability probability for each $t \in [0,T]$ (or better for any finite grid of points in $[0,T]$), while a method based on uniformisation (as in PRISM [38]) has to deal with each time point separately.

In Figures 3(c), 3(d), 4(c) and 4(d), instead, we focus on the reachability probability for both problem 1 and 2 for $T = 50$ as a function of the initial time $t_0 \in [0,25]$. The value for the fluid model is compared with the probability of $Z_k^{(N)}$ obtained by simulating the full CTMC up to time t_0 and then focussing attention on a specific client in state *request* and starting the computation of the reachability probability.[5] As we can see, the agreement is good also in this case.

Finally, in Figures 3(e), 3(f), 4(e) and 4(f), we compare the reachability probability for $T = 100$ (reachability problem 1) or $T = 250$ (reachability problem 2) of the CTMC for different populations N and different proportions of clients (n) and servers (m), with the fluid limit. This data confirms that the agreement is good also for small populations for this model.

4.2 Time-varying set reachability

Now we turn our attention to the reachability problem for time-varying sets. First, we will focus on solving the problem for a generic ICTMC $Z(t)$, considering then the limit behaviour of $Z_k^{(N)}$.

In order to deal with the reachability problem for time varying sets, the main difficulty is that, at each time T_i in which the goal or the unsafe set changes, also the modified Markov chain that we need to consider to compute the reachability probability changes structure. This can have the effect of introducing a discontinuity in the probability matrix.

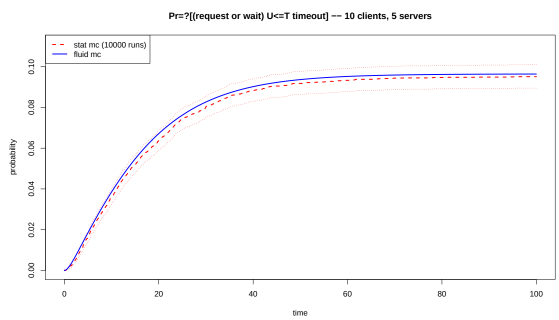
In particular, if at time T_i a state s becomes a goal state, then the probability $\pi_{s_1,s}(t,T_i)$ suddenly needs to be added to the reachability probability of s_1. Therefore, a change in the goal set at time T_i introduces a discontinuity in the reachability probability at time T_i. Similarly, if a state s was safe and then becomes unsafe, we have to discard the probability of trajectories that are in it at time T_i, as those trajectories become suddenly unsafe.

In the following, let $G(t)$ and $U(t)$ be the goal and unsafe sets, and assume for the moment that the set of time points in which G or U change value (at least in one state) is finite and equal to $T_1 \leq T_2 \ldots \leq T_k$. Let $T_0 = t$ and $T_{k+1} = t + T$.

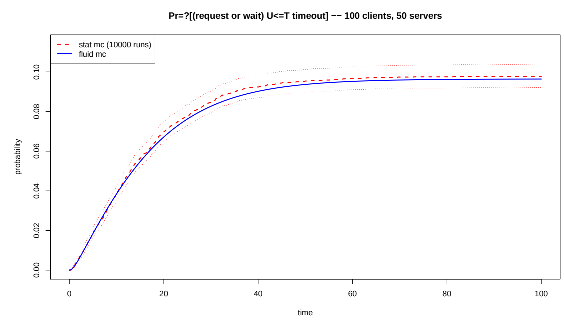
In order to compute the reachability probability, we can exploit the semi-group property of the Markov process, stating that $\Pi(T_0,T_{k+1}) = \prod_{i=0}^{k} \Pi(T_i,T_{i+1})$. Then, we also need to properly deal with the above mentioned discontinuity effects at each time T_i. We proceed in the following way:

1. We double the state space, letting $\tilde{\mathscr{S}} = \mathscr{S} \cup \bar{\mathscr{S}}$, where a state $\bar{s} \in \bar{\mathscr{S}}$ represents state s when it is a goal state. Hence, in the probability matrix $\tilde{\Pi}$, $\tilde{\pi}_{s_1,\bar{s}_2}$ is the probability of having reached s_2 avoiding unsafe states, while s_2 was a goal state.

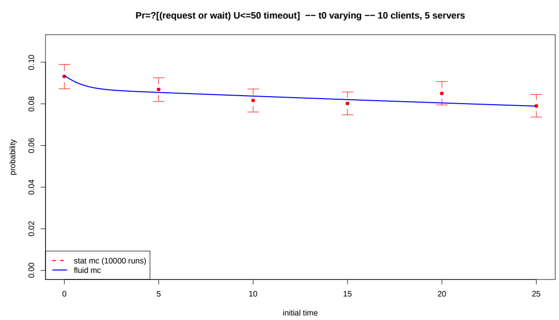
[5] This is done by using two indicator variables X_G and X_U that are set equal to one when a trajectory reaches a goal or an unsafe set, respectively. Then, we estimate the reachability probability of by the sample mean of X_G at the desired time.



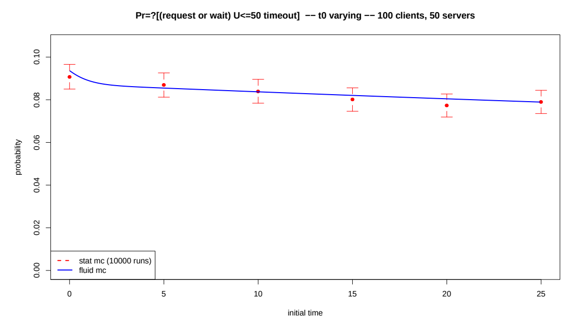
(a) T varying,$n = 10$,$m = 5$



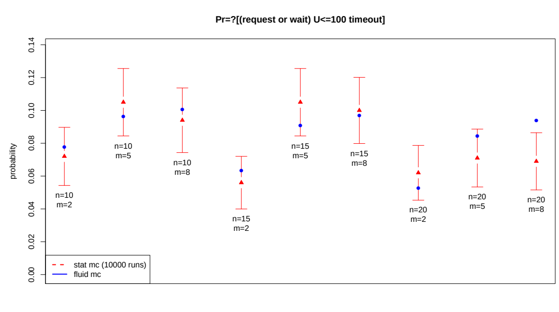
(b) T varying,$n = 100$,$m = 50$



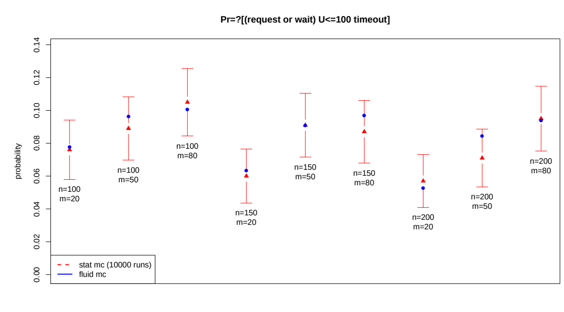
(c) t_0 varying,$n = 10$,$m = 5$



(d) t_0 varying,$n = 100$,$m = 50$

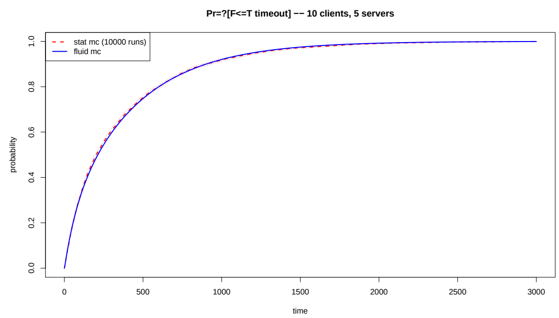


(e) n,m varying

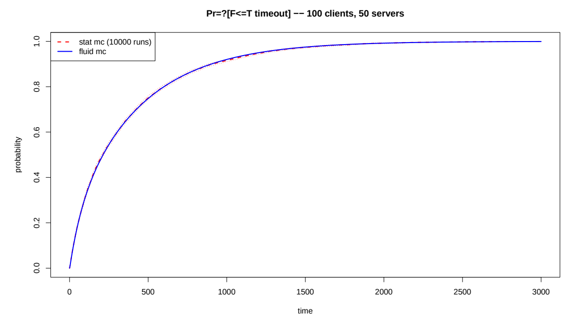


(f) n,m varying

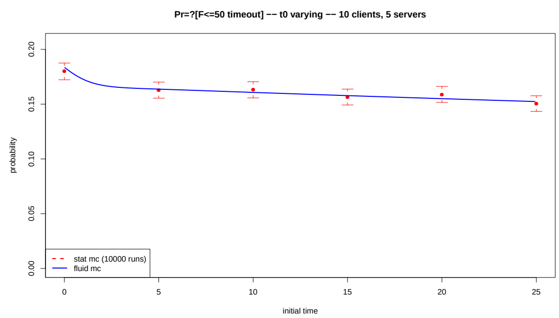
Figure 3: Client-Server model of Section 3.1, single client CTMC. First line: comparison of time-out before being served probability (point 1) for fluid and CTMC models as a function of time horizon T. Second line: comparison of time-out before being served probability (point 1) for fixed time horizon $T = 50$ and variable initial time t_0. Third line: time-out before being served probability (point 1) at time $T = 250$, and variable number of client and servers.



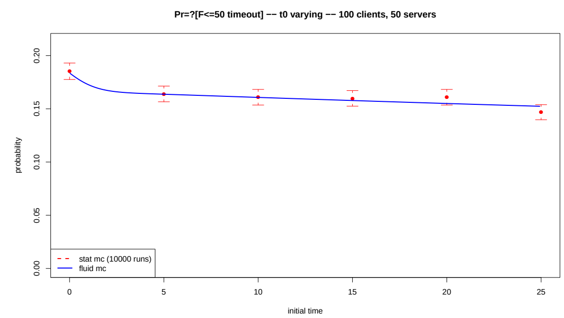
(a) T varying,$n = 10$,$m = 5$



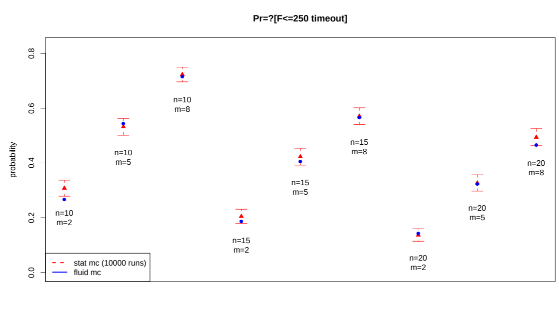
(b) T varying,$n = 100$,$m = 50$



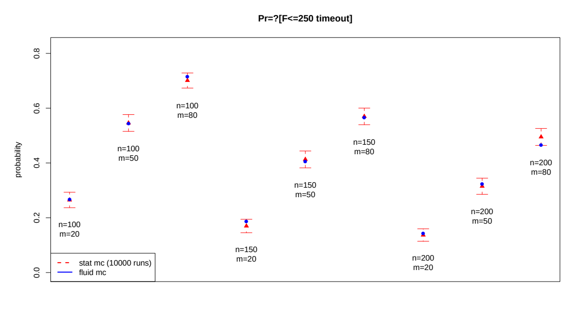
(c) t_0 varying,$n = 10$,$m = 5$



(d) t_0 varying,$n = 100$,$m = 50$



(e) n,m varying



(f) n,m varying

Figure 4: Client-Server model of Section 3.1, single client CTMC. First line: comparison of time-out probability (point 2) for fluid and CTMC models as a function of time horizon T. Second line: comparison of time-out probability (point 2) for fixed time horizon $T = 50$ and variable initial time t_0. Third line: comparison of time-out probability (point 2) at time $T = 250$, and variable number of client and servers.

2. Consider a discontinuity time T_i and let $t_1 \in [T_{i-1}, T_i)$ and $t_2 \in (T_i, T_{i+1}]$. Define $W(t) = S \setminus (G(t) \cup U(t))$. Then, for $s_1 \in W(t_1)$ and $s_2 \in W(t_2)$, the probability of being in s_2 at time t_2, given that we were in s_1 at time t_1 and avoiding both unsafe and goal sets, can be written as $\tilde{\pi}_{s_1,s_2}(t_1,t_2) = \sum_{s \in W(t_1) \cap W(t_2)} \tilde{\pi}_{s_1,s}(t_1,T_i)\tilde{\pi}_{s,s_2}(T_i,t_2)$. Hence, we have to appropriately restrict the summation set at time T_i, to account for changes in W.
3. Consider again a discontinuity time T_i and let $t_1 \in [T_{i-1}, T_i)$ and $t_2 \in (T_i, T_{i+1}]$. Suppose $s_2 \in W(t_1)$ and $s_2 \in G(t_2)$. Then, the probability of reaching the goal state s_2 at time t_2, given that at time t_1 we were in s_1, can be written as $\tilde{\pi}_{s_1,s_2}(t_1,T_i) + \sum_{s \in W(t_1) \cap W(t_2)} \tilde{\pi}_{s_1,s}(t_1,T_i)\tilde{\pi}_{s,\bar{s}_2}(T_i,t_2)$. The first term is needed because all safe trajectories that are in state s_2 at time T_i suddenly become trajectories satisfying the reachability problem, hence we have to add them to compute the reachability probability.

All the previous remarks can be formally incorporated into the semi-group expansion of $\tilde{\Pi}(t,t+T)$ by multiplying on the right each term $\tilde{\Pi}(T_i,T_{i+1})$ by a suitable 0/1 matrix, depending only on the structural changes at time T_{i+1}. Let $|\mathscr{S}| = n$ and let $\zeta_W(T_i)$ be the $n \times n$ matrix equal to 1 only on the diagonal elements corresponding to states s_j belonging to both $W(T_i^-)$ and $W(T_i^+)$ (i.e. states that are safe and not goals both before and after T_i), and equal to 0 elsewhere. Furthermore, let $\zeta_G(T_i)$ be the $n \times n$ matrix equal to 1 in the diagonal elements corresponding to states s_j belonging to $W(T_i^-) \cap G(T_i^+)$, and zero elsewhere. Finally, let $\zeta(T_i)$ be the $2n \times 2n$ matrix defined by:

$$\zeta(T_i) = \begin{pmatrix} \zeta_W(T_i) & \zeta_G(T_i) \\ 0 & I \end{pmatrix}.$$

Consider now the following ICTMC $\tilde{Z}$ on $\tilde{\mathscr{S}}$, with rate matrix $\tilde{Q}(t)$, where

1. for $\bar{s}_1 \in \bar{\mathscr{S}}$ and any $s_2 \in \tilde{\mathscr{S}}$, $\tilde{q}_{\bar{s}_1,s_2}(t) = 0$;
2. for $s_1 \notin W(t)$ and all $s_2 \in \tilde{\mathscr{S}}$, $\tilde{q}_{s_1,s_2}(t) = 0$
3. for $s_1 \in W(t)$ and $s_2 \in S \setminus G(t)$, $\tilde{q}_{s_1,s_2}(t) = q_{s_1,s_2}(t)$, while $\tilde{q}_{s_1,\bar{s}_2}(t) = 0$;
4. for $s_1 \in W(t)$ and $s_2 \in G(t)$, $\tilde{q}_{s_1,\bar{s}_2}(t) = q_{s_1,s_2}(t)$, while $\tilde{q}_{s_1,s_2}(t) = 0$.

In the previous chain, all unsafe and goal states are absorbing, while transitions leading from a safe state s to a goal state are readdressed to the copy $\bar{s}$ of s. States in $\bar{\mathscr{S}}$ are absorbing, too.

Now let $\tilde{\Pi}(t_1,t_2)$ be the probability matrix associated with the ICTCM $\tilde{Q}(t)$. Given the interval $I = [t, t+T]$, we indicate with $T_1, \ldots, T_{k_I}$ the ordered sequence of discontinuity points of goal and unsafe sets internal to I. Let

$$\Upsilon(t,t+T) = \tilde{\Pi}(t,T_1)\zeta(T_1)\tilde{\Pi}(T_1,T_2)\zeta(T_2)\cdots\zeta(T_{k_I})\tilde{\Pi}(T_{k_I},t+T).$$

Then, we have that

$$P_s(t) = P_{reach}(Z,t,T,G,U)[s] = \sum_{\bar{s}_1 \in \bar{\mathscr{S}}} \Upsilon_{s,\bar{s}_1}(t,t+T) + \mathbf{1}\{s \in G(t)\},$$

where the first term takes into account the probability of reaching a goal state starting from a non-goal state, while the second term is needed to properly account for states $s \in G(t)$, for which $P_s(t)$ has to be equal to 1 (a formal proof can be given by induction on the number of discontinuity points). $\Upsilon(t,t+T)$ can be obtained by computing each $\tilde{\Pi}(T_i,T_{i+1})$ solving the associated forward Kolmogorov equation and then multiplying those matrices and the appropriate ζ ones, according to the definition of Υ.

If we want to compute $P(t)$ as a function of t, instead, we need a way to compute $\Upsilon(t,t+T)$ as a function of t. This can be done by observing that Υ depends on t only from the first and last factors in the multiplication. Defining $\Gamma(T_1,T_k) = \zeta(T_1)\tilde{\Pi}(T_1,T_2)\zeta(T_2)\cdots\tilde{\Pi}(T_{k-1},T_k)\zeta(T_k)$, writing $\Upsilon(t,t+T) = \tilde{\Pi}(t,T_1)\Gamma(T_1,T_k)\tilde{\Pi}(T_k,t+T)$, differentiating with respect to t and applying the forward or backward equation for $\tilde{\Pi}$, we find the following differential equation for Υ:

$$\frac{d\Upsilon(t,t+T)}{dt} = -\tilde{Q}(t)\Upsilon(t,t+T) + \Upsilon(t,t+T)\tilde{Q}(t+T).$$

This equation holds until either t or $t+T$ becomes equal to a discontinuity point. When this happens, the integration has to be stopped and restarted, recomputing Υ accordingly.

Practically, to solve this problem we can proceed as follows:

1. Given an interval $[t_0,t_1]$ of interest for the initial time of the reachability, find all discontinuity points of the sets G and U contained in $[t_0,t_1+T]$, and let them be $t_0 = T_0 < T_1 < \ldots < T_k < T_{k+1} = t_1+T$. Furthermore, let $T_i' = T_i + T$ for $i = 0,\ldots,k$, and let $pre(T_i')$ be the greatest T_j preceding T_i'.
2. Compute $\tilde{\Pi}(T_i,T_{i+1})$ and $\tilde{\Pi}(pre(T_i'),T_i')$ for $i \leq k$, using the forward Kolmogorov equations[6]. Compute also each $\zeta(T_i)$.
3. Compute $\Upsilon(t_0,t_0+T)$ and integrate until time $t = \min\{T_1, T_{j+1}-T\}$, where $t_0+T \in [T_j,T_{j+1}]$.
4. If $t+T = T_{j+1}$, multiply Υ on the right by $\zeta(T_{j+1})$ and continue the integration. If $t = T_1$, then recompute Υ as $\tilde{\Pi}(T_1,T_2)\Gamma(T_2,T_j)\tilde{\Pi}(T_j,T_1+T)$, where $\tilde{\Pi}(T_j,T_1+T) = \tilde{\Pi}(pre(T_1'),T_1')$.
5. Integrate piecewise using the previous rules until time t_1.

Notice that, if the infinitesimal generator matrix $Q(t)$ of Z is sufficiently well-behaved (for instance, Lipschitz continuous), then the function $P(t)$ will be at least piecewise continuous, with a finite number of discontinuity points at instants T_i and T_i'.

Remark 4.1. The precise behaviour of G and U functions at their discontinuity points (i.e. if they are left-continuous or right-continuous) is irrelevant for the computation of Υ: the set of trajectories of Z differing in those time points has probability 0.

Remark 4.2. In the previous method, we need to integrate repeatedly a set $4n^2$ differential equations. However, most of these variables are redundant. In fact, we only need n^2 variables for the probability transition matrix Π on $\mathcal{S}$ and an additional n variables to store the reachability probability vector. The method presented above can be easily reconfigured to this restricted set of variables.

Limit behaviour

We consider now the limit behaviour of time-varying reachability probability for $Z_k^{(N)}$, proving that it converges (almost everywhere) to that of z_k. We state this result in a more general form, assuming that also the goal and unsafe sets depend on N, and converge (in a sense specified below) to some limit sets G and U. This is needed to reason about CSL model checking.

However, both the previous algorithm to compute reachability for time-varying sets and the convergence proof rely on some regularity assumptions of the functions involved. In particular, we want a guarantee that the number of discontinuities in goal and unsafe sets, hence the number of zeros of

[6] Notice, that, if $T_j = pre(T_i')$, then $\tilde{\Pi}(T_j,T_i')$ and $\tilde{\Pi}(T_j,T_{j+1})$ can be computed during the same numerical integration of the forward equation.

$P(t) - p$, where $P(t)$ is the reachability probability, is finite in any compact time interval $[0,T]$. This is unfortunately not true in general, as even a smooth function can be equal to zero on an uncountable and nowhere dense set of Lebesgue measure 0 (for instance, on the Cantor set [46]).

Therefore, we have to introduce some restrictions on the class of functions that we can use. In particular, we will require that the rate functions of z_k and of $Z_k^{(N)}$ are *piecewise real analytic functions*.

A function $f : I \to \mathbb{R}$, I an open subset of $\mathbb{R}$, is said to be analytic [35] in I if and only if for each point t_0 of I there is an open neighbourhood of I in which f coincides with its Taylor series expansion around t_0. Hence, f is locally a power series. For a piecewise analytic function, we intend a function from $I \to \mathbb{R}$, I interval, such that there exists $I_1, \ldots, I_k$ disjoint open intervals, with $I = \bigcup_j \bar{I}_j$, such that f is analytic in each I_j. A similar definition holds for functions from $\mathbb{R}^n$ to $\mathbb{R}$, considering their multi-dimensional Taylor expansion.

Analytic functions are a class of functions closed by addition, product, composition, division (for non-zero analytic functions), differentiation and integration. Piecewise analytic functions also satisfy these closure properties, by considering the intersections of their analytic sub-domains. Many functions are analytic: polynomials, the exponential, logarithm, sine, cosine. Using the previous closure properties, one can show that most of the functions we work with in practice are analytic.

Analytic functions have two additional properties that make them particularly suitable in this context:

1. The zeros of an analytic function$f$ in I, different from the constant function zero, are isolated. In particular, if I is bounded, then the number of zeros is finite. This is true also for the derivatives of any order of the function f.
2. If f is analytic in a set E, then the solution $\mathbf{x}$ of $\frac{d\mathbf{x}}{dt} = f(\mathbf{x})$ in E is also analytic (this is a consequence of the Cauchy-Kowalevski theorem [21]).

This second property, in particular, guarantees that, if the rate functions of z_k and $Z_k^{(N)}$ are piecewise analytic, then all the probability functions computed solving the differential equations introduced in the previous section are piecewise analytic.

In the following, we will need the following straightforward property of piecewise analytic functions:

Proposition 4.2. *Let $f : I \to \mathbb{R}$ be a piecewise analytic function, with $I \subseteq \mathbb{R}$ a compact interval. Let $E_f = \{x \in \mathbb{R} \mid \mu_\ell(f^{-1}(x)) = 0\}$ be the set of all values x such that f is not locally constantly equal to x, where μ_ℓ is the Lebesgue measure. Furthermore, let $Z_x = f^{-1}(\{x\})$ be the set of solutions of $f(t) = x$ and and let $DZ_f = \{x \in \mathbb{R} \mid \forall t \in Z_x, f'(t) \neq 0\}$. Then*

1. *$\forall x \in E_f$, Z_x is* finite.
2. *$\mu_\ell(E_f \cap DZ_f) = 1$*

Proof. Point 1 follows from basic properties of the piecewise analytic function $(f - x)$: in any analytic piece, either the function is constantly equal to zero, or it has only a finite number of zeros. Point 2, instead, follows from the fact that the derivative $f'(t)$ of t is piecewise analytic, hence has only a finite number of zeros (in the analytic pieces in which f is not constant). ■

In addition, we need to impose some regularity also on the time-dependency of goal and unsafe sets (at least for the limit model) and on the way goal and unsafe sets at level N converge to these limit sets. In particular, we will require that (limit) goal and unsafe sets are *robust* in the following sense:

Definition 4.2. A time-dependent subset $V(t)$ of $\mathcal{S}$, $t \in I$, is *robust* if and only if for each $s \in \mathcal{S}$, the indicator function $V_s : I \to \{0,1\}$ of s has only a finite number of discontinuities and it is either right or left continuous in those discontinuity points.

In the following, we will usually indicate with $V(t)$ both a time dependent set V and its indicator function (with values in $\{0,1\}^m$, $m = |\mathscr{S}|$).
Moreover, denote by $Disc(V) = \{\bar{t} \mid V_s(\bar{t})$ is discontinuous for some $s \in \mathscr{S}\}$, the set of discontinuity points of V. As we will see later on, the notion of robustness is tightly connected with the computability of the reachability probability for time-varying sets and with the decidability of the model checking algorithm for ICTMCs, both discussed in Section 5.

Furthermore, we need the following notion of convergence for time-varying sets:

Definition 4.3. A sequence of time-varying sets $V^{(N)}(t)$, $t \in I$, converges *robustly* to a time-varying set $V(t)$, $t \in I$, if and only if, for each open neighbourhood U of $Disc(V)$ (i.e., the set of discontinuity points of V), $V^{(N)}(t) \to V(t)$ *uniformly* in $I \setminus U$.

Connecting the notions of robust set and robust convergence, we have the following:

Proposition 4.3. *Let $V^{(N)}(t)$ be a sequence of time varying sets converging robustly to a robust set $V(t)$, $t \in I$. Let $D_V^{(N)} = \{t \mid V^{(N)}(t) \neq V(t)\}$. Then $\mu_\ell(D_V^{(N)}) \to 0$, where μ_ℓ is the Lebesgue measure on $\mathbb{R}$.*

Proof. A straightforward consequence of the definition of robust convergence is that, for each open neighbourhood U of $Disc(v)$, there exists an N_0 such that, for all $N \geq N_0$, $V^{(N)}(t) = V(t)$ for $t \in I \setminus U$. Now, as V is robust, then $|Disc(V)| = m < \infty$. Fix $\varepsilon > 0$ and define $U_\varepsilon = \bigcup_{\bar{t} \in Disc(V)} B(\bar{t}, \varepsilon)$, where $B(\bar{t}, \varepsilon)$ is the open ball centred in $\bar{t}$ of radius ε. Then $\mu_\ell(U_\varepsilon) \leq 2m\varepsilon$. Now, fix $\varepsilon_k \to 0$. For each k, there is an N_k such that, for all $N \geq N_k$ $V^{(N)}(t) = V(t)$ for $t \in I \setminus U_{\varepsilon_k}$, and therefore $D_V^{(N)} \subseteq U_{\varepsilon_k}$. ■

In the following, we will present the convergence result for the reachability problem with respect to robust (limit) goal and unsafe sets. This lemma, which is also the basic inductive step to prove convergence for CSL model checking formulae, relies on the functions involved being piecewise analytic.

Lemma 4.1. *Let $\mathscr{X}^{(N)}$ be a sequence of CTMC models, as defined in Section 3.1, and let $Z_k^{(N)}$ and z_k be defined from $\mathscr{X}^{(N)}$ as in Section 3.3, with piecewise analytic rates, in a compact interval $[0,T']$, for T' sufficiently large.*
Let $G(t)$, $U(t)$, $t \in [t_0, t_1 + T]$ be robust *time-varying sets, and let $G^{(N)}(t)$, $U^{(N)}(t)$ be sequences of time-varying sets converging robustly to G and U, respectively.*
Furthermore, let $P(t) = P_{reach}(z_k, t, T, G, U)$ and $P^{(N)}(t) = P_{reach}(Z_k^{(N)}, t, T, G^{(N)}, U^{(N)})$, $t \in [t_0, t_1]$.
Finally, fix $p \in [0,1]$, $\bowtie \in \{\leq, <, >, \geq\}$, and let $V_p(t) = I\{P(t) \bowtie p\}$, $V_p^{(N)}(t) = I\{P^{(N)}(t) \bowtie p\}$. Then

1. *For all but finitely many $t \in [t_0, t_1]$, $P^{(N)}(t) \to P(t)$ in probability, with uniform speed (i.e. independently of t).*
2. *For almost every $p \in [0,1]$, V_p is robust and the sequence $V_p^{(N)}$ converges robustly to V_p.*

Proof. By a standard coupling argument, assume that z_k and $Z_k^{(N)}$ are defined on the same probability space Ω. Then, letting Y be either z_k or $Z_k^{(N)}$, for $\omega \in \Omega$, let $\chi(t, Y(\omega))$ be equal to one if trajectory $Y(\omega)$ satisfies the reachability problem with respect to G and U and zero otherwise, starting at time t and $\chi^{(N)}(t, Y(\omega))$ be 1 if $Y(\omega)$ satisfies the reachability problem for $G^{(N)}$, $U^{(N)}$, and zero otherwise, starting at time t. Then $P(t) = \mathbb{E}[\chi(t, z_k)]$, and $P^{(N)}(t) = \mathbb{E}[\chi^{(N)}(t, Z_k^{(N)})]$, hence

$$|\mathbb{E}[\chi(t,z_k)] - \mathbb{E}[\chi^{(N)}(t,Z_k^{(N)})]| \quad \leq \quad \underbrace{\mathbb{E}[|\chi(t,z_k) - \chi^{(N)}(t,z_k)|]}_{(1)} + \underbrace{\mathbb{E}[|\chi^{(N)}(t,z_k) - \chi^{(N)}(t,Z_k^{(N)})|]}_{(2)}$$

Consider term (2) above. Applying theorem 3.2 up to time t_1+T, and reasoning as in Proposition 4.1, we have that the set of trajectories $\Omega_1 = \{\omega \in \Omega \mid z_k(t,\omega) = Z_k^{(N)}(t,\omega), t \leq t_1+T\}$ has probability $1-\varepsilon_N$, with $\varepsilon_N \to 0$. Now, for $\omega \in \Omega_1$, clearly $\chi^{(N)}(t,z_k(\omega)) = \chi^{(N)}(t,Z_k^{(N)}(\omega))$, hence $(2) \leq \varepsilon_N$, for any t.

Let us focus now on term (1) in the inequality above. Let $T_1 < T_2 < \ldots < T_h$ be all the points in $Disc(G) \cup Disc(U)$ (which is finite as G and U are robust), and suppose neither t nor $t+T$ coincide with one of the previous points (i.e., all discontinuities are internal in the time domain). As $G^{(N)}$ (resp. $U^{(N)}$) converges robustly to G (resp. U), for $N \geq N_0$ they differ only in small disjoint balls $B(T_i,\varepsilon)$ internal to $[t,t+T]$. Furthermore, if G (or U) has a discontinuity for state s in T_i, then the value of G (or U) on the left of $B(T_i,\varepsilon)$ is different from the value of G (or U) on the right of $B(T_i,\varepsilon)$. It follows that the only trajectories of z_k for which $\chi(t,z_k) \neq \chi^{(N)}(t,z_k)$ are those jumping within the set $D^{(N)} = D_G^{(N)} \cup D_U^{(N)}$.[7] As the rate functions of z_k are piecewise analytic, they are bounded by a constant Λ, thus the probability of a trajectory jumping in $D^{(N)}$ is bounded by $\int_{D^{(N)}} e^{-\Lambda t}dt \leq \int_{D^{(N)}} 1dt = \mu_\ell(D^{(N)}) \to 0$ (independently of t). It follows that, if $t \notin T_d$, with $T_d = \{T_1,\ldots,T_h,T_1-T,\ldots,T_h-T\}$, then

$$|\mathbb{E}[\chi(t,z_k)] - \mathbb{E}[\chi^{(N)}(t,Z_k^{(N)})]| \leq \delta_N,$$

with $\delta_N = \varepsilon_N + \mu_\ell(D^{(N)}) \to 0$.

On the contrary, if $t \in T_d$, then a discontinuity of G or U happens exactly at the boundary of the time domain $[t,t+T]$ in which we have to verify the formula. In this case, the value of sets $G^{(N)}$ and G (or $U^{(N)}$ and U) may never be the same at this extreme point t^*, whatever small neighbourhood of t^* in $[t,t+T]$ one takes into account[8]. Therefore, there can be a set of trajectories of measure >0 that are accepted by $\chi^{(N)}$ and refused by χ (or vice versa). In particular, this can happen if and only if $P(t)$ has a discontinuity in one of those points. Hence, for these time points, convergence may not hold. However, the set T_d is finite, hence it has measure zero and point 1 of the Lemma is proved.
Let us turn now to point 2 of the theorem.
Fix a $p \in E_P \cap DZ_P \cap \{p \mid P(T_j^+) = p \vee P(T_j^-) = p$ for a discontinuity point T_j of $P\}$, which is a set of Lebesgue measure 1 due to Prop. 4.2 (in fact, it is finite). Then, as P is piecewise analytic (it is piecewise the solution of ODEs with an analytic vector field), the number of zeros of the functions $P(t)-p$ is finite and those zeros are simple (i.e., the derivative of P in those points is non null). Furthermore, the truth value of $P(t)-p$ can change around those points T_j in which $P(T_j)$ is discontinuous (and hence convergence does not hold), if $p \in [P(T_j^-),P(T_j^+)]$. Hence, the set A of points in which V_p has a discontinuity is finite. In addition, if V_p has a discontinuity for state s at time T_i, then it has to be either right or left-continuous. In fact, if in this point $P_s(T_i)-p=0$, then P_s crosses zero, as its derivative is non-null ($p \in DZ_P$). Instead, if T_i is a discontinuity point for P_s, then p is different from $P_s(T_i^-)$ and $P_s(T_i^+)$. It follows that V_p is a robust set.
Fix ε and define A_ε to be $\bigcup_{t\in A} B(t,\varepsilon)$, where $B_\varepsilon(t) = (t-\varepsilon,t+\varepsilon)$. Now, if W is a neighbourhood of A, then for an $\varepsilon > 0$, $A_\varepsilon \subset W$. Let now $f_p(t) = P(t)-p$ and consider the sets $I_\varepsilon^+ = f_p^{-1}([0,1]) \cap (I \setminus A_\varepsilon)$ and $I_\varepsilon^+ = f_p^{-1}([-1,0]) \cap (I \setminus A_\varepsilon)$. Both sets are compact, and $\min\{P(t) \mid t \in I_\varepsilon^+\} = m_\varepsilon^+ > 0$, $\max\{P(t) \mid t \in I_\varepsilon^-\} = m_\varepsilon^- < 0$, as P is different from zero both in I_ε^+ and I_ε^- (by Weierstrass theorem [46]). Letting

[7] If G or U are not robust, then even if they have a finite number of discontinuity points, the previous argument may not hold. In fact, they may have a discontinuity point T_i such that $G_s(T_i) = 1$ but $G_s(t) = 0$ in a neighbourhood $W \setminus \{T_i\}$ of T_i. In this case, it is possible that $G_s^{(N)}(t) = 0$ on all W, which implies that $\chi(t,z_k)) \neq \chi^{(N)}(t,z_k)$ for all those trajectories that are in state s at time T_i.

[8] For instance, if $t^* = T_i$ is the left extreme of the time domain, it may happen that all changes of $G^{(N)}$ occur before this point.

$m_\varepsilon = \min\{m_\varepsilon^+, m_\varepsilon^-\}$, as $P^{(N)}$ converges to P in $I_\varepsilon = I_\varepsilon^+ \cup I_\varepsilon^-$ with uniform speed,[9] there is N_0 such that, for all $N \geq N_0$ and all $t \in I_\varepsilon$, $|P^{(N)}(t) - P(t)| \leq \frac{m_\varepsilon}{2}$, hence for all $N \geq N_0$ and all $t \in I_\varepsilon$, $V_p(t) = V_p^{(N)}(t)$. It follows that $V_p^{(N)}(t)$ converges robustly to $V_p(t)$. ■

Example. If we consider our running example, then it is easy to check that the rate functions defining the infinitesimal generator matrices of interest are piecewise analytic. In fact, even if the vector field of the fluid ODE is not analytic, due to the minimum function, the two functions $g_1(\mathbf{x})$ and $g_2(\mathbf{x})$ of which we take the minimum are analytic. Piecewise analyticity follows from the fact that the solutions of the associated ODE cross the surface $g_1(\mathbf{x}) - g_2(\mathbf{x}) = 0$ (where the minimum is not analytic) only a finite number of times.

5 CSL Model Checking

We turn now to consider the model checking of CSL formulae and the relationship between the truth of formulae for $Z_k^{(N)}$ and z_k.

Consider an until CSL formula $\varphi = \mathscr{P}_{\bowtie p}(\varphi_1 U^{[0,T]} \varphi_2)$, where φ_1 and φ_2 are boolean combination of atomic propositions. The major consequence of the time-inhomogeneity of z_k is that the truth value of φ in a state s depends on the time t at which we evaluate such a formula. In particular, φ may be true in state s at time t_1, but false at a different time t_2. Consequently, the set of states that satisfy a CSL formula φ can be time dependent, and this introduces an additional layer of complexity to the analysis of z_k. Indeed, this requires the solution of reachability problems for time-varying sets. Notice that we have the same issue about time-dependence also for model checking CSL formulae against $Z_k^{(N)}(t)$.

The method we put forward in the previous section can cope with this issue, but may require a large computational effort (the solution of systems of ODE quadratic in the size of the state space of the ICTMC, and it depends on the number of discontinuity points of the sets U and G). However, in our setting we are interested in z_k, which is an abstract and approximate model of the behaviour of a single agent. Usually, a single agent has a very small state space, hence the previous approach to reachability of time-varying sets should be feasible in practice.

An orthogonal issue is the asymptotic correctness of CSL model checking, when considering the sequence $Z_k^{(N)}$ and the limit z_k. As boolean operators pose no real problem, we only need to concentrate on until formulae $\varphi = \mathscr{P}_{\bowtie p}(\varphi_1 U^{[0,T]} \varphi_2)$, with time varying sets satisfying φ_1 and φ_2.

In particular, we can reduce this problem to the computation of the probabilities $P^{(N)}(t) = P_{reach}(Z_k^{(N)}, t, T, G^{(N)}, U^{(N)})$ and $P(t) = P_{reach}(z_k, t, T, G, U)$, where $G^{(N)}(t)$ $(U^{(N)}(t))$ is the set

[9] The set I_ε may contain time instants in which the convergence of $P^{(N)}$ to P does not hold, but that do not generate a discontinuity in V_p. These time instants $\tilde{t}$ are points in which the reachability interval $[t, t+T]$ starts or terminates in a discontinuity point of G or U. In those cases, it may be that the discontinuity in $G^{(N)}$ or $U^{(N)}$ (eventually, there will be only one close to $\tilde{t}$) eventually always follows that of G or U, and in this case $P^{(N)}(\tilde{t}) \to P(\tilde{t}^-)$, or eventually always precedes that of G or U, and in this case $P^{(N)}(\tilde{t}) \to P(\tilde{t}^+)$, or for some N follows it and for some N precedes it. Hence, for those points we can only say that $[\liminf_{N\to\infty} P^{(N)}(\tilde{t}), \limsup_{N\to\infty} P^{(N)}(\tilde{t})] \subseteq [\underline{P}(\tilde{t}), \overline{P}(\tilde{t})]$, where $\underline{P}(\tilde{t}) = \min\{P(\tilde{t}^-), P(\tilde{t}^+)\}$ and $\overline{P}(\tilde{t}) = \max\{P(\tilde{t}^-), P(\tilde{t}^+)\}$. From equation 4 of Section 4.1, adapted to time varying $G^{(N)}$ and $U^{(N)}$ (so that the probability $P_{U,G}(s, \mathbf{x}, T)$ depends on the initial time and is piecewise analytic), we can deduce that $P^{(N)}(t)$ is a piecewise analytic function. As $P^{(N)}(\tilde{t} \pm \varepsilon)$ converges to $P(\tilde{t} \pm \varepsilon)$ for any ε small enough, we can easily deduce that $\liminf P^{(N)}(\tilde{t})$ and $\limsup P^{(N)}(\tilde{t})$ converge uniformly. To see this, suppose for instance that $P(\tilde{t}^-) < P(\tilde{t}^+)$ and $G^{(N)}$ or $U^{(N)}$ do not eventually always have a discontinuity before $\tilde{t}$ (other cases are treated similarly). Given $\varepsilon > 0$, as $|\tilde{t} - \varepsilon - \tilde{t}| = \varepsilon$, then $|P^{(N)}(\tilde{t}) - P^{(N)}(\tilde{t} - \varepsilon)| \leq L^N \varepsilon$, where L^N is the Lipschitz constant for $P^{(N)}$, which converges to L, the Lipschitz constant of P. Then $|\liminf P^{(N)}(\tilde{t}) - P(\tilde{t}^-)| \leq |\liminf P^{(N)}(\tilde{t}) - P^{(N)}(\tilde{t} - \varepsilon)| + |P^{(N)}(\tilde{t} - \varepsilon) - P(\tilde{t} - \varepsilon)| + |P(\tilde{t} - \varepsilon) - P(\tilde{t}^-)| \leq L^N \varepsilon + L\varepsilon + \varepsilon < 4L\varepsilon$, for N large enough not depending on $\tilde{t}$.

of states satisfying φ_2 ($\neg\varphi_1$) at time t for $Z_k^{(N)}$, while G and U are defined similarly for z_k.[10] Then, we may resort to Lemma 4.1 to prove convergence of $P^{(N)}(t)$ to $P(t)$.

However, in CSL model checking we are interested in truth values rather than in probabilities, and lifting the previous convergence to truth values is not so straightforward. Consider the path formula $\varphi_1 U^{[0,T]} \varphi_2$. The problem is that we have to compute its probability $P(t)$ (depending on the initial time t) for z_k and then solve the algebraic equation $P_s(t) - p = 0$ for each state s, to identify for which time instants state s satisfies the formula. Now, the point is that, even in case $P^{(N)}(t) \to P(t)$ uniformly, we are not guaranteed that $P^{(N)}(t) \bowtie p \to P(t) \bowtie p$. For instance, if $P(t) = p$, and $\bowtie$ is $\leq$, then if $P^{(N)}(t)$ converges to $P(t)$ from above, it never satisfies $P^{(N)}(t) \bowtie p$ for any N, hence convergence of $P^{(N)}(t) \bowtie p$ to $P(t) \bowtie p$ does not hold. However, things can go wrong only when $P(t) = p$, and the main point of the convergence theorem is to prove that this happens sufficiently "rarely" not to impact on the computation of probabilities of an until formula in which φ is one of the two sub-formulas.

In the following, we first outline an algorithm for CSL model checking of ICTMC, and then discuss convergence in more detail. Finally, at the end of the section, we will compare in more detail the CSL model checking problem for $Z_k^{(N)}$ and $(Z_k^{(N)}, \hat{\mathbf{X}}^{(N)})$.

5.1 Model Checking CSL for ICTMC

The algorithm of Section 4.2 for computing reachability in the presence of piecewise constant goal and update sets is the core procedure to compute the probability of an until formula. In fact, consider the path formula $\varphi_1 U^{[T,T']} \varphi_2$. To compute its probability for initial time in $[t_0, t_1]$,[11] we solve two reachability problems separately and then combine the results.

The first reachability problem is for unsafe set $U = [\![\neg\varphi_1]\!]$ and goal set $G(t+T) = [\![\varphi_1]\!]$ (only at the final time) and empty before. In fact, this reachability problem can be solved in a simpler way: it just requires trajectories not to enter an unsafe state, and then collects the probability to be in a safe state at the time $t+T$, for $t \in [t_0, t_1]$.[12] Let Υ^1 be the probability matrix of this reachability problem computed with a variant of the procedure of the previous section.

The second reachability problem is for unsafe set $U = [\![\neg\varphi_1]\!]$ and goal set $G = [\![\varphi_2]\!]$, and is solved for initial time $t \in [t_0 + T, t_1 + T]$, and time horizon $T' - T$. Let Υ^2 be the function computed by the algorithm in Section 4.2 for this second problem. Then, for each state s, safe at time t, we compute $\sum_{s_1 \in \neg U(t+T)} \sum_{s_2 \in S} \Upsilon^1_{s,s_1}(t, t+T) \Upsilon^2_{s_1,\bar{s}_2}(t+T, t+T')$, which is the probability of the until formula in state s. Then, we can determine if state s at time t satisfies $\mathscr{P}_{\bowtie p}(\varphi_1 U^{[T,T']} \varphi_2)$ by solving the inequality $P_s(t) \bowtie p$.

This provides an algorithm to approximately solve the CSL model checking for ICTMC recursively on the structure of the formula, provided that the number of discontinuities of sets satisfying a formula is finite and that we are able to find all the zeros of the computed probability functions, to construct the proper time-dependent satisfiability sets (or approximations thereof).

In order to study in more detail the previous algorithm, in particular for what concerns its correctness and its termination, we will stick to the following assumption for what concerns the numerical algorithms used by it.

---

[10] We can restrict our attention to until formulae with time between $[0, T]$, as intervals $[T_1, T_2]$ can be dealt with by essentially solving two reachability problems of this kind and combining their solution (or better, by computing two transient probabilities and then combining the two so obtained probabilities, see [6]).

[11] The appropriate value of t_0 and t_1 are to be deduced from φ_1, φ_2 and the superformula of the until, in a standard way [29]

[12] In particular, we can get rid of the copy $\bar{\mathscr{S}}$ of the state space, and define a simplified Υ function using ζ_W matrices instead of ζ ones.

Assumption 1. There are interval arithmetic routines that can compute bounding sets for the rate functions of z_k and $Z_k^{(N)}$, in such a way that the approximation error can be made arbitrary small. We call such function *interval computable*.

Notice that this assumption is not so restrictive. It works for all the standard functions, and works for solutions of ODE of functions which satisfy it, for derivatives of these functions and for their integrals [2, 40]. In particular, if the rate functions are interval computable, then so will be all the probabilities computed by solving reachability problems.

The approach presented above relies, in addition to the solution of ODEs, also on two other key numerical operations: given a computable real number p, determine if p is zero and and given an analytic function f, find all the zeros of such a function (or better an interval approximation of these zeros of arbitrary accuracy). However, it is not clear if these two operations can be carried out effectively for any input that we can generate, see Remark 5.2 for further comments. Therefore, we need some further assumption. Instead of restricting the class of functions (which seems a difficult problem as we have to consider solution of differential equations), we will follow the approach of [22], introducing a notion of *robust CSL formula* and proving decidability for this subset of formulae. This will not solve the decidability problem in theory, but makes it quasi-decidable [22], which may be enough in practice. As we will see, the set of CSL formulae which is not robust has measure zero (see Theorem 5.2).

In order to introduce the concept of robust CSL formula, consider a CSL formula φ and let $p_1,\ldots,p_k$ be the constants appearing in the $\mathscr{P}_{\bowtie p}$ operators of until sub-formulae of φ. We will treat $\varphi = \varphi(p_1,\ldots,p_k)$ as a function of those $p_1,\ldots,p_k$. Furthermore, we will call the until sub-formulae of φ *top until sub-formulae* if they are not sub-formulae of other until formulae. The other until formulae will be called *dependent*. Finally, given two robust time-varying sets V_1 and V_2, we say that V_1 and V_2 are *boolean compatible* if they do not have discontinuities for the same state s happening at the same time instant t.

Definition 5.1. A CSL formula $\varphi = \varphi(\mathbf{p})$, $\mathbf{p} \in [0,1]^k$ is robust if and only if

1. there is an open neighbourhood W of $\mathbf{p}$ in $[0,1]^k$ such that for each $\mathbf{p_1} \in W$,

$$s,0 \models \varphi(\mathbf{p}) \Leftrightarrow s,0 \models \varphi(\mathbf{p_1}).$$

2. The time-varying sets of states in which any dependent until sub-formula of φ holds are *robust* and *boolean compatible* among them.

We prove now the following theorem, which states that the CSL model checking algorithm we put forward works at least for robust formulae:

Theorem 5.1. *The CSL model checking for ICTMC, for piecewise analytic interval computable rate functions, is decidable for a robust CSL formula $\varphi(p_1,\ldots,p_k)$.*

Proof. First of all, we prove that we can approximate the function $P(t)$ for any top until formula φ with arbitrary small precision. To start, notice that procedures for integrating ODEs and doing matrix multiplication can be computed with arbitrary precision, due to the assumptions of interval computability. Hence, let us focus on the set of zeros of $P(t) - p$, for a dependent until formula φ_1. We want to prove that we can find those zeros with arbitrary precision, and that in doing this we will be able to compute the probability of any until formula which contains φ_1 as a sub-formula with arbitrary precision. If φ is robust, then the time-varying truth of formula φ_1 is robust. This means that $P(t) - p$ has a finite number of simple zeros (i.e., their derivatives do not go to zero). Hence, it is possible to effectively encapsulate them in disjoint intervals of size as small as desired [51][13]. Therefore, we can compute the time-varying truth value of the set of states satisfying the formula φ_1 with arbitrary precision, in the sense that for each $\varepsilon > 0$, we can provide intervals of size at most ε, each containing a single discontinuity point of the set in which one or more states change truth status. The condition on boolean compatibility ensures that we can combine such approximation of time-varying sets and still obtain robust sets[14], with the further property that we can always assume that there is a zero in every approximation interval[15]. Consider now the problem of computing the probability of an until formula, having two approximations of time-varying truth as described above. Reasoning as in the proof of Lemma 4.1, we can see that if we choose an arbitrary point in each interval wrapping a discontinuity point in spite of the correct one, we commit an error in computing the probability of the until which is uniformly bounded by the total size of the approximation intervals. Hence, we can make such error as small as desired. Reasoning inductively, we can therefore compute with any arbitrary precision the probability $P(0)$ of any top until formula.

Given this value, we then have to solve the inequality $P_s(0) < p_i$ (or $P_s(0) > p_i$) for any s and any top until formula φ_i. By the robustness of the CSL formula φ, it cannot be that $P_s(0) = p_i$, hence we can effectively solve that problem by computing $P_s(0)$ with precision $\varepsilon_i < |P_s(0) - p_i|$. As we are doing interval arithmetic computations, we can increase the precision until each p_i will be outside the approximation interval for $P_s(0)$. This proves that the algorithm presented is effective for robust formulae and eventually computes the exact answer. ■

The following corollary is a straightforward consequences of the proof of the previous theorem:

Corollary 5.1. *The algorithm for CSL model checking presented in this section is correct for robust CSL formulae.* ■

We turn now to characterise the set of robust formulae from a topological and measure-theoretic point on view. We have the following

Theorem 5.2. *Given a CSL formula $\varphi(\mathbf{p})$, with $\mathbf{p} \in [0,1]^k$, then the set $\{\mathbf{p} \mid \varphi(\mathbf{p})$ is robust$\}$ is relatively open[16] in $[0,1]^k$ and has Lebesgue measure 1.*

Proof. We will prove the theorem by structural induction on the formula φ.

Base case: The base case corresponds to (boolean combinations of) atomic formulae, which are robust for each $\mathbf{p} \in [0,1]^k$.

[13] As the number of zeros is finite and their derivative is non-zero, the function $f_p(t) = P(t) - p$ crosses zero in those points. Furthermore, notice that the absolute minimum value of the derivative in those zero points is > 0. Hence, there is an ε such that each interval of size ε containing a zero point has different signs at the extremes and the derivative is provably different from zero. By iterated bisection, we can always find such intervals after a finite number of steps. Furthermore, all intervals J not containing a zero can be eventually discarded by bisection, computing an upper bound L on the absolute value of the derivative in such intervals and bisecting them until we can prove that they are disjoint from zero using the Lipschitz condition with Lipschitz constant L (compute f_p on a single point x in J of length δ, and discard J if $|f_p(x)| - L\delta > 0$).

[14] This may fail if we take the minimum (conjunction) of two truth sets which have a discontinuity for s in the same time point T: we can obtain a function which is neither left nor right continuous.

[15] If we take the minimum (conjunction) of two truth sets which have a discontinuity for s in the same time point T, then even if the conjunction is robust, when we have an approximation of the time-varying truth function, we can never know if both discontinuities happen in the same time point or in different ones.

[16] A set $U \subset V$ is relatively open in $V \subset W$, where W is a topological space, if it is open in the subspace topology, i.e. if there exists an open subset $U_1 \subseteq W$ such that $U = V \cap U_1$.

Until formulae: Let $\varphi = \mathscr{P}_{\bowtie p_k}(\varphi_1 U^{[T_1,T_2]} \varphi_2)$, and let $I = \{1,\ldots,k-1\}$. By inductive hypothesis, the set $R' \subset [0,1]^{k-1}$ for which φ_1 and φ_2 are robust is open and has measure 1.[17] Fix a point $\mathbf{q} \in R'$, and let $U \subseteq R'$ be an open neighbourhood of $\mathbf{q}$. Define the set-valued function $b : U \to 2^{[0,1]}$ in the following way: Given $\mathbf{q}$, $b(\mathbf{q})$ is the set of values p which causes the time-varying truth set of φ to be non-robust. Therefore, $b(\mathbf{q})$ contains the values of $P_s(t)$ for which $P_s'(t) = 0$ is zero, the values $P_s(t^-)$ and $P_s(t^+)$ for each discontinuity point t, and the values of constant pieces of P_s, plus the value $P_s(0)$, hence it is finite. Now let $h_R : [0,1]^k \to \{0,1\}$ be the indicator function of the set R in which φ is robust. By Fubini's theorem:

$$\mu_\ell(R) = \int_{[0,1]^k} h_R(\mathbf{q},p)\mu_\ell(d\mathbf{q},dp) = \int_{[0,1]^{k-1}} \int_{[0,1]} h_R(\mathbf{q},p)\mu_\ell(dp)\mu_\ell(d\mathbf{q}) = \int_{R'} \mu_\ell(d\mathbf{q}) = 1,$$

which proves that R has measure 1. To prove that it is open, observe that in U the number of discontinuities of time-varying truth sets of φ_1 and φ_2 does not change (φ_j is robust for each point in U) and the time-instants in which such discontinuities happen depend continuously on $\mathbf{q}$. Hence, there is a neighbourhood $U' \subseteq U$ of $\mathbf{q}$ such that the number of points in $b(\mathbf{q}')$, $\mathbf{q}' \in U'$ does not increase[18] and the value of such points depend continuously on $\mathbf{q}'$. Therefore, the set-valued map $b : U \to 2^{[0,1]}$ is upper-semicontinuous[19] in $\mathbf{q}$. Fix now $p \notin b(\mathbf{q})$, and choose a neighbourhood V of p such that $V \cap b(\mathbf{q}) = \emptyset$. Then, by the upper-semicontinuity of b, there exists $W \subset U'$ such that $b(W) \cap V = \emptyset$, hence φ is robust in $W \times V$. By the arbitrary choice of $\mathbf{p} = (\mathbf{q},p)$, the openness of R follows.

Boolean combinations: The only non-trivial cases are the conjunction or disjunctions of until formulae. In this case, we have to guarantee that the discontinuity times of truth-valued functions are disjoint for each pair of until formulae. Consider two until formulae φ_1 and φ_2, and let $\mathbf{p} = (\mathbf{q_1}, p_1, \mathbf{q_2}, p_2)$, where p_j is the threshold for formula φ_j and $\mathbf{q_j}$ is the set of constants which φ_j depends on. By inductive hypothesis, the robust sets R_j for φ_j are open and have measure 1. Now, let $P_j = P_j(t,\mathbf{q_j})$ be the probability of the until path formula in φ_j, and fix a robust point $\mathbf{q} = (\mathbf{q_1}, p_1, \mathbf{q_2})$. Let $g(\mathbf{q})$ be the set valued function $g(\mathbf{q}) = P_2(\{t \mid P_1(t,\mathbf{q_1}) = p_1\}, \mathbf{q_2}) \cup b_2(\mathbf{q_2})$, where b_2 is the set of non-robust points for φ_2. The set $g(\mathbf{q})$ contains all thresholds for φ_2 for which φ_2 is non-robust and all thresholds that would make non-robust the boolean combination. By properties of the analytic functions, it follows that $g(\mathbf{q})$ is finite, hence we can apply Fubini's theorem and conclude that the robust set R for the boolean combination of φ_1 and φ_2 has measure 1. Furthermore, by arguments similar to the one used for the until formula case above, the function g is upper-semicontinuous[20] in $\mathbf{q}$. Therefore, letting $p_2 \notin g(\mathbf{q})$ and $V \cap g(\mathbf{q}) = \emptyset$ a neighbourhood of p_2 in $[0,1]$, we can find a neighbourhood U of $\mathbf{q}$ such that $g(U) \cap V = \emptyset$, so that $W = U \times V$ is an open neighbourhood of $\mathbf{p} = (\mathbf{q_1}, p_1, \mathbf{q_2}, p_2)$ which contains only robust points, which proves that R is open. If we have a

[17] Observe that $R' = R_1 \times R_2$, where R_j is robust for φ_j.

[18] We have to restrict U to avoid the appearance of further zeros of the derivatives.

[19] A set valued function $b : X \to 2^Y$ is upper-semicontinuous in $x \in X$ if and only if, for each neighbourhood V of $F(x)$, there is a neighbourhood U of x such that $F(U) \subseteq V$.

[20] The number of solutions of $P_1(t,\mathbf{q_1}) = p_1$ in a sufficiently small neighbourhood U_1 of $(p_1,\mathbf{q_1})$ is constant and the set-valued function $g_1(p_1,\mathbf{q_1}) = \{t \mid P_1(t,\mathbf{q_1}) = p_1\}$ is upper semicontinuous. Furthermore, in a sufficiently small neighbourhood U_2 of $\mathbf{q_2}$, the function $P_2(t,\mathbf{q_2})$ is continuous in $\mathbf{q_2}$ for each continuity point t of $P_2(t,\mathbf{q_2})$. Points for which $P_2(t,\mathbf{q_2})$ is not continuous are covered by b, hence both $P_2(t^+,\mathbf{q_2})$ and $P_2(t^-,\mathbf{q_2})$ are in $g(\mathbf{q})$. Now, for each neighbourhood V of $g(\mathbf{q})$, by piecewise analyticity and right/left continuity of P_2, we can find a neighbourhood U_2 of $\mathbf{q_2}$ and a neighbourhood V_1 of $g_1(p_1,\mathbf{q_1})$ such that $b_2(U_2) \subseteq V$ and both $\{p \mid P_2(t^+,\mathbf{q_2}), t \in V_1\} \subseteq V$ and $\{p \mid P_2(t^-,\mathbf{q_2}), t \in V_1\} \subseteq V$. Now, by upper-semicontinuity of g_1, there is a neighbourhood U_1 of $(\mathbf{q_1}, p_1)$ such that $g_1(U_1) \subseteq V_1$. It follows that $g(U_1 \times U_2) \subseteq V$, hence g is upper-semicontinuous in $\mathbf{q}$.

boolean combination of $j > 2$ until formulae, simply reason pairwise and then take the intersection of the so obtained robust sets, thus getting an open set of measure 1. ∎

The openness of the set of robust thresholds for a formula allows us to prove the following corollary about quasi-decidability. In this paper, we consider a notion of quasi-decidability, which is slightly different than the one defined in [22]. In fact, we take advantage of the fact that out input values belong to a compact subset $K \subseteq \mathbb{R}^n$, for which a standard notion of measure exists.

Definition 5.2. A problem with inputs in a compact subset $K \subseteq \mathbb{R}^n$, is *quasi-decidable* if there is an algorithm that solves it correctly for an open subset $U \subset K$, with $\mu_\ell(U)/\mu_\ell(K) = 1$.

Combining Theorems 5.1 and 5.2, we obtain the following:

Corollary 5.2. *The CSL model checking for ICTMC, for piecewise analytic interval computable rate functions, is quasi-decidable for any formula* $\varphi(\mathbf{p})$. ∎

Remark 5.1. The notions of robustness and quasi-decidability have a practical side. First, the openness property of the set of robust thresholds for a formula $\varphi(\mathbf{p})$ guarantees that if we "perturb" a formula (by varying the set $\mathbf{p}$ of threshold constants of the path probability operators), then the formula remains robust. Furthermore, by the definition of robustness, also its truth value remains the same (as the notion of quasi-decidability of [22] requires). This explains the use of the terminology "robust".

Secondly, the characterisation of the set R of robust thresholds for a formula φ provided in Theorem 5.2, implies that if we choose thresholds at "random", we are likely to select a robust formula. In fact, consider the grid of rational numbers with $\frac{1}{n}$ in $[0,1]$, i.e. $GR_n = \{\frac{m}{n} \mid m < n, m, n \in \mathbb{N}\}$, and take the Cartesian product $GR_n^k \subset [0,1]^k$. Let μ_n be the uniform distribution in GR_n^k, then $\mu_n \to \mu$, the uniform distribution on $[0,1]^k$ (which coincides with the Lebesgue measure on Borel sets). Now, as R is open and has Lebesgue measure 1, then $\mu(R) = 1$ and $\mu(\partial R) = 0$, hence R is a continuity set for μ. Therefore, $\mu_n(R) \to \mu(R) = 1$ by the Portmanteau theorem [13]. This means that, fixing $\varepsilon > 0$, if we choose the thresholds of the until sub-formulas from the set GR_n^k, for n large enough, the probability of choosing a bad set of thresholds, for which the formula is not robust and the CSL model checking algorithm may not terminate, will be less than ε.

Remark 5.2. The semi-decidability result presented here is in sharp contrast with the decidability result of model checking for time-homogeneous CTMC. However, in that case the result follows because $P_s(0)$ has a special form allowing the application of Lindeman-Weierstass theorem for transcendental numbers (together with zero testing procedures for algebraic numbers) [4]. This, in turn, is a consequence of having constant (rational) rates. In our case, instead, rates are piecewise analytic functions, and we cannot rely on the method of [4] anymore. In fact, in the algorithm for computing the probability, there are two numerical operations that are potential sources of undecidability:

1. Given a number p, which is the analytic image of a rational, decide if it is zero. This is a classical problem whose decidability is not known, even restricting to expressions made up by polynomials and exponentials only [44,45]. Indeed, its decidability is connected with the truth of the Schanuel conjecture [44,45], which is in turn connected with decidability of the theory of reals extended by the exponential. However, even in case the Schanuel conjecture holds, it is not clear if the zero problem will be decidable for any analytic function.

2. Detecting the zeros of an analytic function with arbitrary precision. In this case the problem is caused by non-simple zeros, i.e. points in which the function and some of its derivatives are zero. The method sketched in a footnote of the proof of theorem 5.1 does not work, as it relies on the fact that we can bound the derivative away from zero on null points of the function. Furthermore, in the presence of non-simple zeros, detecting if a compact interval is bound away from zero is semi-decidable (the decision procedure fails if the interval contains a non-simple zero). Whether there is a decidable algorithm for this problem is not known to the authors (even assuming the Schanuel conjecture is true). It may be possible, however, to find algorithms for some subclass of analytic functions large enough for practical purposes. For instance, if we know a lower bound on the radius of convergence of power series in each analytic point, we can effectively extend the real analytic function to an open ball in the complex plane, and then use methods developed for complex analytic functions [30] which can effectively compute the number of zeros in any sufficiently simple open set, by integrating a function on its boundary with interval arithmetic routines [1, 30].

Our conjecture is that the model checking problem for time-inhomogeneous CTMC is not decidable in general, although it may be decidable for some restricted subclass of rate functions if the Schaunel conjecture is true. Further investigations on this issue are required.

Finding an upper bound on the complexity of the approximation algorithm, when it converges, requires us to find an upper bound on the number of zeros of the solution of a linear differential equation with piecewise analytic rates. This is a non trivial problem. However, we can rely on a result for linear systems with bounded analytic rate functions [42], which gives an upper bound Ψ on the number of zeros, expressible as an elementary function of the upper bound on coefficients of the ODE. For piecewise analytic rate functions, simply multiply this bound for the number of analytic pieces. The number of analytic pieces is $K_Q + K$, where K_Q comes from the piecewise analytic nature of rate functions, and K from the number of structural changes of $[\![\neg\varphi_1]\!]$ and $[\![\varphi_2]\!]$ sets. Hence, the number of zeros of $P(t) - p$ can be bounded by $(K + K_Q)\Psi$. By induction, if h is the degree of a formula φ and h_u is the number of nested until subformulae,[21] then the total complexity is upper bounded by $C(n, T_{max}, \varepsilon)(2^h\Psi^{h_u}K_Q)$, where the constant $C(n, T_{max}, \varepsilon)$ hides the cost of integrating ODEs and finding roots in each analytic piece. It is proportional to n^3 (matrix multiplication), time T_{max} for which the ODEs have to be solved, and the precision ε of root finding and numerical integration[22].

However, this is a theoretical upper bound, and we will not expect a complexity like that in practice.

5.2 Convergence for CSL formulae

We are now ready to state a convergence result for CSL model checking. Also in this case, we will restrict our attention to robust CSL formulae. This is reasonable, as we want to use Lemma 4.1, which requires robustness of time-varying sets.

Theorem 5.3. *Let $\mathscr{X}^{(N)}$ be a sequence of CTMC models, as defined in Section 3.1, and let $Z_k^{(N)}$ and z_k be defined from $\mathscr{X}^{(N)}$ as in Section 3.3.*
Assume that $Z_k^{(N)}$, z_k have piecewise analytic infinitesimal generator matrices.
Let $\varphi(p_1, \ldots, p_k)$ be a robust CSL formula. Then, there exists an N_0 such that, for $N \geq N_0$ and each

[21] Notice that, for until formulae not containing any other until subformulae, $K = 0$.

[22] The precision ε depends on the specific analytic functions considered. However, we can imagine a procedure which takes an ε as input and does not provide an answer if the precision is not small enough.

$s \in \mathscr{S}$

$$s, 0 \vDash_{Z_k^{(N)}} \varphi \Leftrightarrow s, 0 \vDash_{z_k} \varphi.$$

Proof. We prove by structural induction that, for each formula φ, the time-varying truth sets $V_\varphi^{(N)}$ of φ in $Z_k^{(N)}$ converge robustly to the robust time-varying truth set V_φ of φ in z_k.

Base case: The case for atomic propositions is trivial, as $V_\varphi^{(N)}$ and V_φ are constant and equal.

Negation: Let $\varphi = \neg\varphi_1$. The result follows because $V_\varphi(t) = 1 - V_{\varphi_1}$ and $V_\varphi^{(N)}(t) = 1 - V_{\varphi_1}^{(N)}$.

Conjunction/Disjunction: Let $\varphi = \varphi_1 \circ \varphi_2$, $\circ \in \{\wedge, \vee\}$. Due to the boolean compatibility condition of robustness of φ with respect to z_k, the set $V_\varphi(t) = mm\{V_{\varphi_1}(t), V_{\varphi_2}(t)\}$, $mm \in \{\min, \max\}$ is robust, with $Disc(V_\varphi) \subseteq Disc(V_{\varphi_1}) \cup Disc(V_{\varphi_2})$. Using the inductive hypothesis, it easily follows that $V_\varphi^{(N)}(t) = mm\{V_{\varphi_1}^{(N)}(t), V_{\varphi_2}^{(N)}(t)\}$ converges robustly to $V_\varphi(t)$.

Until: Let $\varphi = \mathscr{P}_{\bowtie p}(\varphi_1 U^I \varphi_2)$. By inductive hypothesis, we can apply Lemma 4.1[23] and deduce that V_φ is robust and $V_\varphi^{(N)}$ converges robustly to V_φ.

The fact that $V_\varphi^{(N)}$ converges robustly to the robust set V_φ, combined with property 1 of robustness of φ, let us conclude that the truth value of φ at level N converges to the truth value of the limit ICTMC at time zero (if 0 was a point in which convergence of probability fails, then a small perturbation in $\mathbf{p}$ could change the truth value of φ in the limit ICTMC, contradicting the robustness of φ; furthermore, robustness of φ forbids that $P_s(0) = p$). ■

Corollary 5.3. *Given a CSL formula $\varphi(\mathbf{p})$, with $\mathbf{p} \in [0,1]^k$, then the subset of $[0,1]^k$ in which convergence holds has Lebesgue measure 1 and is open in $[0,1]^k$.* ■

The previous theorem shows that the results that we obtain abstracting a single agent in a population of size N with the fluid approximation is consistent. However, the theorem excludes the sets of constants $\mathbf{p}$ for which the formula is not robust. Interestingly, this is the same condition required for decidability of the model checking problem for ICTMC, a fact that shows how these two aspects are intimately connected. Notice that, contrary to decidability, this limitation is unavoidable and is present also in case of sequences of processes converging to a time-homogeneous CTMC. In this case, in fact, the reachability probability is constant with respect to the initial time, and its value p (in the limit model) can cause convergence of truth values to fail.

However, notice that the constants p appearing in a formula that can make convergence fail depend only on the limit CTMC z_k, hence we can detect potentially dangerous situations while solving the CSL model checking for the limit process (in these cases the model checking algorithm may fail to provide an answer).

[23] We need to apply it twice for the two reachability problems involved in computing the probability of an until formula, noticing that the probability of the path formula within φ is an analytic combination of the two so-computed probabilities. Robustness of V_φ and robust convergence of $V_\varphi^{(N)}$ to V_φ follows from the same arguments of Lemma 4.1. Alternatively, one can modify Lemma 4.1 and tailor it to the reachability involved in the until case (which reduces the time window in which one can reach the goal set), by a straightforward modification of the definition of $\chi^{(N)}$ and χ.

Remark 5.3. The version of CSL considered in this paper lacks the (time bounded) next operator. However, it can be easily included in our framework. As for the model checking of ICTMC, time bounded next operator $\mathbf{X}^I\varphi_1$ can be dealt with by computing an integral of the rate functions (taking into account discontinuities of $[\![\varphi_1]\!]$). Finally, to compute its probability as a function of time, we can obtain a set of ODEs by taking the derivative of the integrals. The convergence of probabilities and truth values of the next operator follows from arguments similar to the ones used in this paper.

Remark 5.4. In this paper, we are considering only time bounded operators. This limitation is a consequence of the very nature of the approximation theorem 3.2, which holds only for a finite time horizon. However, there are situations in which we can extend the validity of the theorem to the whole time domain, but this extension depends on properties of the phase space of the fluid ODE [9, 11, 12].

In those cases, we can prove convergence of the steady state behaviour of $Z_k^{(N)}$ to that of z_k, hence we can incorporate also operators dealing with steady state properties.

In order to deal with time unbounded operators, instead, convergence to steady state is not enough. We also need to ensure that the equation $P(t) - p$ has a finite number of zeros on the whole positive time axis. Piecewise analyticity is not sufficient in this case (think about sine and cosine), and stronger conditions have to be required. However, for periodic functions, we may reason similarly to [16], if we can prove that periodicity of rate functions implies periodicity in the reachability probabilities as a function of initial time.

Example. Going back to the running example, consider the until path formula $trueU^{[0,50]}timeout$, where $timeout$ is true only in state rc. Its probability, as a function of the initial time, is shown in Figures 5(a), 5(b), and 5(c), for the states rq, w, and t, respectively. In the same figures, we also show the time-dependent truth of the CSL formula $\mathscr{P}_{<0.167}(trueU^{[0,50]}timeout)$, which is obtained by solving the inequality $P_s(t) < 0.167$, where $P_s(t)$ is one of the previous time-dependent probability functions. In this case, we can observe that for time $t_0 \in [0, 100]$, there is only one solution, as the probability is monotone. This depends on the solution of the fluid equations. In this case, in fact, they converge to a steady state, hence we do expect that also the time dependent truth value of CSL until formulae stabilises (when the fluid ODE are close to steady state, the rates of the CTMC are practically constant). This suggests that in many practical cases, the number of changes of truth value of until formulae will be very small, as in the running example. Notice that in the case of the running example, if we had chosen a threshold bigger, say, than 0.25, then the time-dependent truth formulae would have been a constant function.

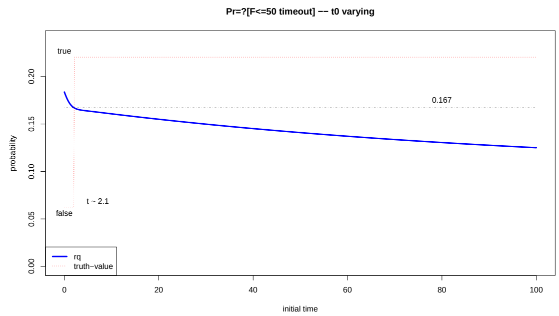
In Figure 5, instead, we show the probability of the path formula

$$true\ U^{[0,T]}(\mathscr{P}_{<0.167}(true\ U^{[0,50]}\ timeout)),$$

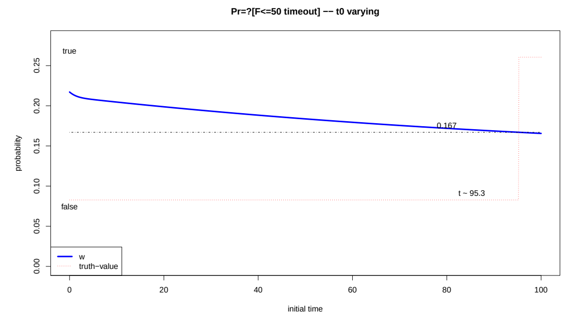
as a function of the time horizon T. In the plot, it is evident how this probability has discontinuities in those time instants in which the truth values function of its until sub-formula change. These discontinuities differentiate the model checking of ICTMC from the one for time-homogeneous CTMC.

5.3 Comparison of CSL model checking for $Z_k^{(N)}$ and $(Z_k^{(N)}, \hat{\mathbf{X}}^{(N)})$

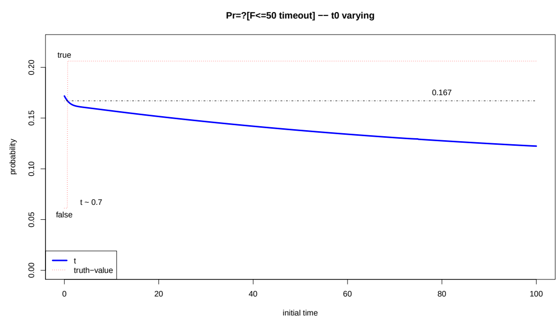
In this paper we have considered two possible descriptions of a single agent at a fixed population level N, i.e. $Z_k^{(N)}(t)$ and $(Z_k^{(N)}(t), \hat{\mathbf{X}}^{(N)}(t))$. From the discussion in Sections 3.3 and 4, we already know that, while $(Z_k^{(N)}(t), \hat{\mathbf{X}}^{(N)}(t))$ is a CTMC with finite (but extremely large) state space, $Z_k^{(N)}(t)$ has a much smaller state space but it is not a Markov process. Furthermore, its behaviour is time dependent. The non-Markovian nature of $Z_k^{(N)}(t)$ has consequences for its reachability probability (see Section 4.2), making



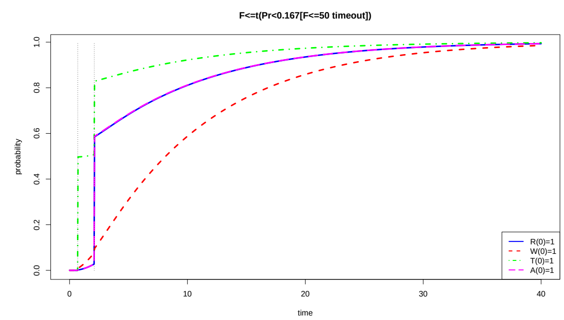
(a) $trueU^{[0,50]}timeout - rq$



(b) $trueU^{[0,50]}timeout - w$



(c) $trueU^{[0,50]}timeout - t$



(d) $trueU^{[0,T]}(\mathscr{P}_{<0.167}(trueU^{[0,50]}timeout))$

Figure 5: Figures 5(a), 5(b), and 5(c). Probability of the formula $trueU^{[0,50]}timeout$, for varying initial time, and different initial states (rq, w, and t respectively). The dotted line shows the time varying truth function for the CSL formula $\mathscr{P}_{<0.167}(trueU^{[0,50]}timeout))$, which is obtained by finding the zeros of the initial-time dependent probability. Figure 5. Probability of the until path formula $trueU^{[0,T]}(\mathscr{P}_{<0.167}(trueU^{[0,50]}timeout))$, as a function of time bound T. Vertical dotted lines show the discontinuity points time-dependent truth of the until sub-formula.

its value dependent on the initial time at which we compute it. This implies that the satisfiability of a CSL formula (with truth value of atomic propositions depending only on $\mathscr{S}$) for $Z_k^{(N)}(t)$ can depend on the time at which we evaluate it, hence we need to consider time-dependent sets to compute the probabilities of until path formulae. But time-dependent sets can introduce discontinuities in reachability probabilities, as discussed in Section 4.2. On the other hand, $(Z_k^{(N)}(t), \hat{\mathbf{X}}^{(N)}(t))$ is a time-homogeneous CTMC, hence its reachability probability does not depend on time and no time-dependent notion of satisfaction has to be considered in this case. In particular, while considering $(Z_k^{(N)}(t), \hat{\mathbf{X}}^{(N)}(t))$, its reachability probability is always a continuous function. This implies that the truth value of a CSL formula containing nested until sub-formulae, can be different if we consider its satisfiability with respect to $Z_k^{(N)}(t)$ or $(Z_k^{(N)}(t), \hat{\mathbf{X}}^{(N)}(t))$.

However, despite this discrepancy for finite N, we will prove that the satisfiability for $Z_k^{(N)}(t)$ and $(Z_k^{(N)}(t), \hat{\mathbf{X}}^{(N)}(t))$ is asymptotically the same, at least if we restrict to robust CSL formulae. In order to show this, we will combine the convergence results of the previous sections with additional results relative to $(Z_k^{(N)}(t), \hat{\mathbf{X}}^{(N)}(t))$ and $(z(t), \mathbf{x}(t))$.

Example. If we observe Figures 4(c) and 4(d), we can easily convince ourselves that the reachability probability for $Z_k^{(N)}$ in the running example for the formula $\varphi_1 = trueU^{[0,50]}timeout$ depend on the initial time, hence it gives rise to a time-dependent set of the satisfiability of the formula $\varphi_2 = \mathscr{P}_{<0.167}(\varphi_1)$. This implies that for $Z_k^{(N)}$, the probability of the formula $\varphi = trueU^{[0,T]}\varphi_2$ will have discontinuities as a function of T, similarly to the case for z_k. However, if we compute the reachability probability for φ in $(Z_k^{(N)}, \hat{\mathbf{X}}^{(N)})$, in a state $s, \mathbf{x}_0$, this will be a continuous function of T, hence the two probabilities are different.

We now turn to prove the convergence of the standard CSL model checking for $\mathbf{Y}^{(N)}(t) = (Z_k^{(N)}(t), \hat{\mathbf{X}}^{(N)}(t))$ in state $s, \mathbf{x}_0$, to the equivalent CSL model checking procedure for $\mathbf{y}(t) = (z(t), \mathbf{x}(t))$. This procedure requires us to compute, given an until formula $\varphi = \varphi_1 U^I \varphi_2$, its probability $P(s,\mathbf{x})$ starting from time 0, in each point $(s,\mathbf{x})$ of the state space $\mathscr{S} \times E$ of $\mathbf{y}(t)$, and then solving the inequality $P(s,\mathbf{x}) \bowtie p$, to determine the truth of $\mathscr{P}_{\bowtie p}(\varphi)$ in $(s,\mathbf{x})$. This defines a subset of $\mathscr{S} \times E$ where $\mathscr{P}_{\bowtie p}(\varphi)$ is true.

The intuition behind the proof is that the truth value of an until formula in a state $(s, \mathbf{x}_0)$ for $\mathbf{y}(t)$ does not depend on the whole state space $\mathscr{S} \times E$, but only on the points of E intersected by the solution of the fluid ODE starting in $\mathbf{x}_0$, i.e. on $\mathscr{S} \times \Phi([0,T], \mathbf{x}_0)$, where $\Phi(t, \mathbf{x}_0)$ is the flow of the differential equation (i.e., the solution of the fluid ODE at time t starting in $\mathbf{x}_0$ at time 0). Furthermore, the convergence of $\hat{\mathbf{X}}^{(N)}(t)$ to $\mathbf{x}(t)$ allows us to restrict the attention to an arbitrary small neighbourhood of $\Phi([0,T], \mathbf{x}_0)$, in order to solve the model checking problem for $\mathbf{Y}^{(N)}(t)$, for N large enough.

In the following, we need some additional concepts and definitions.

Consider the domain $\hat{\mathscr{D}}^{(N)} \subset E$ of $\hat{\mathbf{X}}^{(N)}$. To each point $\mathbf{x} \in E$, we associate a point $\nu^{(N)}(\mathbf{x}) \in \hat{\mathscr{D}}^{(N)}$, such that $\|\mathbf{x} - \nu^{(N)}(\mathbf{x})\| < \frac{1}{N}$. The existence of such a point is guaranteed by the definition of E. Now, we further assume that, given a point $(s,\mathbf{x}) \in E$, the initial state $\mathbf{Y}^{(N)}(0)$ is $(s, \nu^{(N)}(\mathbf{x}))$, so that $\mathbf{Y}^{(N)}(0)$ converges to $(s,\mathbf{x})$ uniformly in space. This choice of $\mathbf{Y}^{(N)}(0)$ guarantees uniform bounds in space for Kurtz theorem and fast simulation theorem, both for convergence in probability and for almost sure convergence.[24].

Now, consider the fluid limit differential equation, and let $\Phi(t, \mathbf{x}_0)$ be its flow. We assume that $\Phi(t, \mathbf{x}_0)$ is a piecewise analytic function with respect to t and $\mathbf{x}$. The *T,ε-flow tube* for $\mathbf{x}_0$ is the set $E_0 \subset E$, defined by $E_0 = \Phi([0,T], B_\varepsilon(\mathbf{x}_0))$, i.e. the set of all trajectories up to time T starting in a ball of radius ε centred in $\mathbf{x}_0$. Now, consider a T,ε-flow tube E_0 for $\mathbf{x}_0$. For any $\mathbf{x} \in E_0$, let $T_{\mathbf{x}}^+ = T_{\mathbf{x}}^+(E_0) = \sup\{t \mid \Phi([0,t], \mathbf{x}) \in E_0\}$ be the time at which the trajectory starting in $\mathbf{x}$ leaves E_0. Furthermore, let $T_{\mathbf{x}}^- = T_{\mathbf{x}}^-(E_0) = \inf\{t \mid \Phi([t,0], \mathbf{x}) \in E_0\}$ be the time at which the trajectory starting in $\mathbf{x}$ enters E_0.

A closed subset $D \subseteq \mathscr{S} \times E_0$ is a *d-set* for E_0 if and only if, for each $\mathbf{x} \in E_0$, it holds that $\{s\} \times \Phi([T_{\mathbf{x}}^-(E_0), T_{\mathbf{x}}^+(E_0)], \mathbf{x}) \cap D$ contains at most k points in each state s. In other words, a d-set is a set that intersects each trajectory in at most k points. It can be easily checked that each d-set has (Lebesgue) measure zero.[25]

We also introduce a notion of *robust subset* of $\mathscr{S} \times E_0$, for a T,ε-flow tube E_0 in $\mathbf{x}_0$. Consider a subset $V \subset \mathscr{S} \times E_0$. We say that V is robust in $\mathscr{S} \times E_0$ if and only if, for each $(s,\mathbf{x}) \in \mathscr{S} \times E_0$, the time-varying set $V_{\mathbf{x}}[s](t) = \mathbf{1}\{(s, \Phi(t,\mathbf{x})) \in V\}$, $T_{\mathbf{x}}^- < t < T_{\mathbf{x}}^+$, is robust in the sense of Definition 4.2, and contains at most $k < \infty$ discontinuity points (where k does not depend on $\mathbf{x}$).

[24]The speed of convergence to the fluid limit depends on the initial conditions only through $\|\hat{\mathbf{X}}^{(N)}(0) - \mathbf{x}(0)\|$; the choice of $\nu^{(N)}(\mathbf{x})$ guarantees the uniform convergence of this quantity with respect to $\mathbf{x}$.

[25]For instance, we can reason as follows: each flow tube is locally diffeomorphic to $A \times [t_1, t_2]$ and, for each such local representation, the set D has measure zero by an application of Fubini's theorem [13].

Furthermore, let $Disc(V) = \bigcup_{\mathbf{x}\in E_0} Disc(V_{\mathbf{x}})$ be the discontinuity set of V, i.e. the union of the discontinuity sets of each trajectory in E_0. Clearly, $Disc(V)$ is a d-set in E_0.

Similarly to Section 4.2, we say that a sequence of sets $V^{(N)} \subset \mathscr{S} \times E_0$ *converges robustly* to a robust set $V \subseteq \mathscr{S} \times E_0$, with E_0 a T,ε-flow tube in $\mathbf{x}_0$, if and only if, for each open neighbourhood U of $Disc(V)$, there is $N_0 > 0$ such that, $\forall N \geq N_0$ and all $\mathbf{x} \in E_0 \setminus U$, $\mathbf{x} \in V^{(N)}$ if and only if $\mathbf{x} \in V$.

We are now ready to state the following lemma, which is a space-version of Lemma 4.1 on time-varying sets and is the key to the induction step of Lemma 5.2.

Lemma 5.1. *Let $E_0 \subset E$ be a T,ε_0-flow tube for $\mathbf{x}_0$. Let U and G two robust subsets of $\mathscr{S} \times E_0$, and $U^{(N)}$, $G^{(N)}$ be sequences of subsets of $\mathscr{S} \times E_0$ that converge robustly to U and G, respectively.*

Let $P(s,\mathbf{x}) = P_{reach}(\mathbf{y}, s, \mathbf{x}, T_1, T_2, U, G)$ be the probability that $\mathbf{y}(t)$ reaches a state in G within time $[T_1, T_2]$, avoiding any unsafe state in U, given that $\mathbf{y}$ started at time $t = 0$ in state $(s,\mathbf{x}) \in \mathscr{S} \times E_0$, and let $P^{(N)}(s,\mathbf{x}) = P^{(N)}_{reach}(\mathbf{Y}^{(N)}, s, \nu^{(N)}(\mathbf{x}), T_1, T_2, U^{(N)}, G^{(N)})$ be defined similarly, with G, U, $\mathbf{x}$ replaced by $G^{(N)}$, $U^{(N)}$, and $\nu^{(N)}(\mathbf{x})$, respectively. Furthermore, define $V = \{(s,\mathbf{x}) \mid P(s,\mathbf{x}) \bowtie p\}$ and $V^{(N)} = \{(s,\mathbf{x}) \mid P^{(N)}(s,\mathbf{x}) \bowtie p\}$. Then there exists $\varepsilon_1 > 0$ such that, in E_1, the $(T-T_2),\varepsilon_1$-flow tube for $\mathbf{x}_0$:

1. *$P^{(N)}(s,\mathbf{x}) \to P(s,\mathbf{x})$ for all $\mathbf{x} \in E_1 \setminus D$, where D is a d-set, uniformly in $(s,\mathbf{x})$.*
2. *If $V_{\mathbf{x}_0}(t)$, $t \in [T^-_{\mathbf{x}_0}(E_1), T^+_{\mathbf{x}_0}(E_1)]$, is a robust time-varying set, then V is robust in E_1 and $V^{(N)}$ converges robustly to V.*

Proof. First, notice that we can always restrict on an arbitrary small neighbourhood of $\Phi(t,\mathbf{x}_0)$, i.e. on a T,ε_1-flow tube E_1 for $\mathbf{x}_0$, with ε_1 as small as desired. This follows from almost sure convergence of Kurtz Theorem 3.1, which guarantees that with probability 1, for N large enough, all trajectories of $\hat{\mathbf{X}}^{(N)}(t)$, (with initial conditions $\nu^{(N)}(\mathbf{x})$ close enough to $\mathbf{x}$) will be contained in E_1. Furthermore, we can choose such an index N independently of $\mathbf{x}$. Hence, given E_0, if we consider a flow tube E_1 for $\mathbf{x}_0$ with radius $\varepsilon_1 < \varepsilon_0/2$, each flow tube of radius ε_1 wrapping a trajectory in E_1 will be contained in E_0. This guarantees that the reachability problem for $\mathbf{Y}^{(N)}$ for any point in $\mathscr{S} \times E_1$ will eventually depend only on the goal sets $G^{(N)}$ and $U^{(N)}$ within $\mathscr{S} \times E_0$.

We first prove point 1 of the lemma in a $(T-T_2),\varepsilon_1$-flow tube E_1 for x_0, for an $\varepsilon_1 < \varepsilon_0/2$ (ε_1 will be fixed in the following). Consider the d-set D in E_0, $D = Disc(G) \cup Disc(U) \cup \Phi^{-1}(T_1, Disc(G)) \cup \Phi^{-1}(T_1, Disc(U)) \cup \Phi^{-1}(T_2, Disc(G)) \cup \Phi^{-1}(T_2, Disc(U))$ containing the discontinuity points of G and U and all points that are mapped by the flow to $Disc(G) \cup Disc(U)$ after T_1 or T_2 units of time.
We will prove convergence of $P^{(N)}$ to P for each $(s,\mathbf{x}) \in (\mathscr{S} \times E_1) \setminus D$.
For each trajectory $\Phi([T^-_{\mathbf{x}}(E_0), T^+_{\mathbf{x}}(E_0)], \mathbf{x})$, $\mathbf{x} \in E_1$, consider the time points $Disc(s,\mathbf{x})$ in which it intersects $Disc(G) \cup Disc(U)$, $Disc(s,\mathbf{x}) = \{t \in [T^-_{\mathbf{x}}(E_0), T^+_{\mathbf{x}}(E_0)] \mid (s, \Phi(t,\mathbf{x})) \in Disc(G) \cup Disc(U)\}$, and for each $\varepsilon' > 0$ define $D_{s,\mathbf{x},\varepsilon'} = \bigcup_{t \in Disc(s,\mathbf{x})} \Phi(B_{\varepsilon'}(t), \mathbf{x})$. Let now $D_{\varepsilon'} = \bigcup_{(s,\mathbf{x}) \in \mathscr{S} \times E_1} D_{s,\mathbf{x},\varepsilon'}$, which is an open neighbourhood of D in $\mathscr{S} \times E_1$. As the fluid vector field is bounded in E_0, hence its flow is Lipschitz continuous in t, with Lipschitz constant uniform in $\mathbf{x}$, it follows that $D_{\varepsilon'} \to D$, as $\varepsilon' \to 0$.
Due to robustness of G and U, the time-varying sets $G_{\mathbf{x}}(t) \subset \mathscr{S}$ and $U_{\mathbf{x}}(t) \subset \mathscr{S}$ (defined with respect to $\mathbf{y}$) are robust (in the sense of Definition 4.2). Furthermore, as $G^{(N)}$ and $U^{(N)}$ converge robustly to G and U, if follows that the time-varying sets $G^{(N)}_{\mathbf{x}}(t) \subset \mathscr{S}$ and $U^{(N)}_{\mathbf{x}}(t) \subset \mathscr{S}$ converge robustly to $G_{\mathbf{x}}(t)$ and $U_{\mathbf{x}}(t)$, respectively.

We will now use an argument similar to the one of Lemma 4.1. Let χ (resp. $\chi^{(N)}$) be random variables defined on sample trajectories and equal to one if the trajectory satisfies the reachability problem of the Lemma with respect to G, U (resp. $G^{(N)}, U^{(N)}$). Then, as $P(s,\mathbf{x}) = \mathbb{E}[\chi(s,\mathbf{x},\mathbf{y}(\omega))]$, where $\mathbf{y}(0) = (s,\mathbf{x})$, and similarly for $P^{(N)}(s,\mathbf{x})$, to show convergence we just need to prove that $|\mathbb{E}[\chi(s,\mathbf{x},\mathbf{y})] -$

$\mathbb{E}[\chi^{(N)}(s,\mathbf{x},\mathbf{Y}^{(N)})]| \rightarrow 0$. It holds that:

$$|\mathbb{E}[\chi(s,\mathbf{x},\mathbf{y})]-\mathbb{E}[\chi^{(N)}(s,\mathbf{x},\mathbf{Y}^{(N)})]| \quad \leq \quad \underbrace{\mathbb{E}[|\chi(s,\mathbf{x},\mathbf{y})-\chi^{(N)}(s,\mathbf{x},\mathbf{y})|]}_{(1)}+\underbrace{\mathbb{E}[|\chi^{(N)}(s,\mathbf{x},\mathbf{y})-\chi^{(N)}(s,\mathbf{x},\mathbf{Y}^{(N)})|]}_{(2)},$$

Term (1) can be treated as in Lemma 4.1, observing that for each ε', the only trajectories of $\mathbf{y}$ for which χ and $\chi^{(N)}$ can have a different value are those jumping in the ε'-neighbourhood $Disc(s,\mathbf{x},\varepsilon')$ of $Disc(s,\mathbf{x})$, i.e. in $Disc(s,\mathbf{x},\varepsilon') = \bigcup_{t\in Disc(s,\mathbf{x})} B'_{\varepsilon}(t)$, and this event has a probability that is bounded by $2\varepsilon'|\bigcup_s Disc(s,\mathbf{x})| \leq 2nk\varepsilon'$, where k is the uniform bound for the robustness of G and U. The bound on term (2), instead, follows from the convergence of $\mathbf{Y}^{(N)}$ to $\mathbf{y}$, but it requires a slightly different treatment than in Lemma 4.1, as now the time varying sets for $\mathbf{Y}^{(N)}$ depend on the sample trajectories of $\hat{\mathbf{X}}^{(N)}$, hence they are random quantities. However, we can reason in the following way. Consider $D_{2\varepsilon'}$, and let N be large enough so that trajectories of $\hat{\mathbf{X}}^{(N)}(t)$, starting from $\nu^{(N)}(\mathbf{x})$, are ε'-close to $\Phi(t,\mathbf{x})$ with probability 1. It follows that, with probability one, the time-varying sets $G^{(N)}_{\mathbf{x},\hat{\mathbf{X}}^{(N)}}(t)$ and $U^{(N)}_{\mathbf{x},\hat{\mathbf{X}}^{(N)}}(t)$, defined with respect to trajectories of $\mathbf{Y}^{(N)}(t)$, coincide with $G_{\mathbf{x}}(t)$ and $U_{\mathbf{x}}(t)$ outside $D_{2\varepsilon'}$, and thus with $G^{(N)}_{\mathbf{x}}(t)$ and $U^{(N)}_{\mathbf{x}}(t)$ (again, for N large enough). Now, with probability converging to one (independently of $(s,\mathbf{x})$), the trajectories of z_k and $Z_k^{(N)}$ are the same, hence for N large enough this probability is larger than $1-\varepsilon'$. For these trajectories, we can see that the only ones for which $\chi^{(N)}(s,\mathbf{x},\mathbf{y}) \neq \chi^{(N)}(s,\mathbf{x},\mathbf{Y}^{(N)})$ are those jumping in $Disc(s,\mathbf{x},2\varepsilon')$[26], and the probability of this event can be bounded by $4nk\varepsilon'$. Concluding, for N large enough, we have that $|\mathbb{E}[\chi(s,\mathbf{x},\mathbf{y})]-\mathbb{E}[\chi^{(N)}(s,\mathbf{x},\mathbf{Y}^{(N)})]| \leq (6nk+1)\varepsilon'$, which proves that $P^{(N)}(s,\mathbf{x}) \rightarrow P(s,\mathbf{x})$, and this convergence is uniform with respect to $(s,\mathbf{x})$, as the bound derived above in independent of it.

As for point 2 of the lemma, observe that by the fact that the fluid trajectory $\Phi(t,\mathbf{x}_0)$ is robust for V and by piecewise analyticity of P, we can choose an ε_1 sufficiently small such that all trajectories in the flow tube E_1 are robust, i.e. their time varying set with respect to P is robust (just observe that the function $P(s,\Phi(t,\mathbf{x}))$ is piecewise analytic in t and $\mathbf{x}$ for each s). Furthermore, we can choose ε_1 so that the number of intersections of $\Phi(t,\mathbf{x})$ with V in each state s, i.e. the number of time s $P(s,\Phi(t,\mathbf{x}))-p$ changes sign, is the same as that of $\Phi(t,\mathbf{x}_0)$. It follows that V is robust for this choice of ε_1. As for the robust convergence of $V^{(N)}$ to V, notice that $Disc(V)$ is a d-set, hence we can use uniform convergence of $P^{(N)}$ to P outside an open neighbourhood of $Disc(V)$. Additionally, notice that, as in the proof of Lemma 4.1, the points in which we do not have convergence of $P^{(N)}$ to P and that are not in $Disc(V)$, do not create problems, as in a small neighbourhood of those points, P is always strictly above or below p, hence the limsup or the liminf of $P^{(N)}$ in those points will be uniformly satisfying the inequality defining $V^{(N)}$.■

The previous lemma is the key argument used in the structural induction to prove the following result.

Lemma 5.2. *Let $\mathscr{X}^{(N)}$ be a sequence of CTMC models, as defined in Section 3.1, and let $Z_k^{(N)}$ and z_k be defined from $\mathscr{X}^{(N)}$ as in Section 3.3.*
Assume that there is a flow tube E_0 of $\mathbf{x}_0$ such that all trajectories in E_0 are piecewise analytic.
Let $\varphi = \varphi(\mathbf{p})$ be a robust CSL formula for the trajectory $\Phi(t,\mathbf{x}_0)$. Then, there is an N_0 such that, for all $N \geq N_0$,

$$s,\mathbf{x}_0 \models_{\mathbf{y}} \varphi \;\Leftrightarrow\; s,\nu^{(N)}(\mathbf{x}_0) \models_{\mathbf{Y}^{(N)}} \varphi.$$

[26] This is a consequence of the robustness of $G_{\mathbf{x}}(t)$ and $U_{\mathbf{x}}(t)$: in any point $\bar{t} \in \bigcup_s Disc(s,\mathbf{x})$, one state s' changes status (either for G or U), hence the value of $G_{\mathbf{x}}(t)$ or $U_{\mathbf{x}}(t)$ for that state is different before $\bar{t}-2\varepsilon'$ and after $\bar{t}+2\varepsilon'$, for ε' small enough. and so are the values of $G^{(N)}_{\mathbf{x}}(t)$ or $U^{(N)}_{\mathbf{x}}(t)$, for N large enough.

Proof. We will prove by structural induction on the formula φ, that there is a T,ε-flow tube E_φ of $\mathbf{x}_0$ such that $V_\varphi^{(N)}$ converges to V_φ robustly, where V_φ is the set of points $(s,\mathbf{x}) \in \mathscr{S} \times E_\varphi$ such that $s,\mathbf{x} \models_{\mathbf{y}} \varphi$ and $V_\varphi^{(N)}$ is the set of points $(s,\mathbf{x}) \in \mathscr{S} \times E_\varphi$ such that $s, \nu^{(N)}(\mathbf{x}_0) \models_{\mathbf{Y}^{(N)}} \varphi$.

Base case: the result for atomic formulae is trivial as their truth value depends only on s, hence we can choose $E_\varphi = E_0$ and $V_\varphi = V_\varphi^{(N)} = \mathscr{S}_\varphi \times E_0$, where $\mathscr{S}_\varphi = \{s \mid s \models \varphi\}$.

Negation: If $\varphi = \neg\varphi_1$, we can choose $E_\varphi = E_{\varphi_1}$, and simply observe that robust convergence of $V_{\varphi_1}^{(N)}$ to V_{φ_1} implies robust convergence of $V_\varphi^{(N)} = E_{\varphi_1} \setminus V_{\varphi_1}^{(N)}$ to $V_\varphi = E_{\varphi_1} \setminus V_{\varphi_1}$.

Conjunction and Disjunction: If $\varphi = \varphi_1 \circ \varphi_2$, $\circ \in \{\wedge, \vee\}$, consider E_{φ_i}, a T,ε_i-flow tube, and sets $V_{\varphi_i}^{(N)} \to V_{\varphi_i}$. As φ is robust for the trajectory starting in $\mathbf{x}_0$ and $\mathbf{x}_0 \in E_{\varphi_i}$, by the boolean compatibility condition of φ there exists an ε such that the d-sets of V_{φ_1} and V_{φ_2} are disjoint in $\mathscr{S} \times E_\varphi$, for E_φ the T,ε-flow tube in $\mathbf{x}_0$. It easily follows that $V_\varphi = V_{\varphi_1} \bullet V_{\varphi_2}$ is robust in $\mathscr{S} \times E_\varphi$, $\bullet \in \{\cap, \cup\}$, and $V_{\varphi_1}^{(N)} \bullet V_{\varphi_2}^{(N)} \to V_{\varphi_1} \bullet V_{\varphi_2}$ robustly.

Until: If $\varphi = \mathscr{P}_{\bowtie p}(\varphi_1 U^{[T1,T_2]} \varphi_2)$, let E_{φ_i} be T,ε_i-flow tubes for φ_i, $i = 1,2$, and robust sets V_{φ_i}, such that $V_{\varphi_i}^{(N)} \to V_{\varphi_i}$ robustly. By letting $\varepsilon_0 = \min\{\varepsilon_1, \varepsilon_2\}$, considering the ε, T-flow tube E_j for $\mathbf{x}_0$, and using the robustness of φ, we satisfy the hypothesis of Lemma 5.1, hence there is an $(T - T_2), \varepsilon$-flow tube E_φ for $\mathbf{x}_0$ such that V_φ is robust in $\mathscr{S} \times E_\varphi$ and $V_\varphi^{(N)} \to V_\varphi$ robustly.

Given a formula φ, and the flow-tube E_φ for $\mathbf{x}_0$, such that V_φ is robust in $\mathscr{S} \times E_\varphi$ and $V_\varphi^{(N)} \to V_\varphi$ robustly, then the lemma follows by observing that, due to robustness of φ, $\mathbf{x}_0$ does not belong to the d-set of V_φ, hence there is an N_0 such that, for all $N \geq N_0$, $(s,\mathbf{x}_0) \in V_\varphi^{(N)} \Leftrightarrow (s,\mathbf{x}_0) \in V_\varphi$. ■

We now turn to consider the relationship between the model checking problem of a CSL formula φ for $z_k(t)$ and the model checking problem for the same formula with respect to $\mathbf{y}(t)$. In this case, it is easy to see that a formula is true for $z_k(t)$ if and only if it is true for $\mathbf{y}(t)$. In fact, in this process the truth value of a formula in state $(s,\mathbf{x}_0)$ depends only on the trajectory $\Phi(t,\mathbf{x}_0)$ starting in $\mathbf{x}_0$. Furthermore, if we fix a time $\bar{t}$ and consider the point $\mathbf{x}_{\bar{t}} = \Phi(\bar{t},\mathbf{x}_0)$, then the process $\bar{z}_k(t)$, defined with respect to the trajectory $\Phi(t,\mathbf{x}_{\bar{t}})$ starting in point $\mathbf{x}_{\bar{t}}$ at time zero, equals the process $z(t+\bar{t})$, starting in $\mathbf{x}_0$ at time zero, due to the semi-group property of the flow $\Phi(\cdot,\cdot)$. Hence, any reachability probability for $\mathbf{z}_k$ with respect to the initial time $\bar{t}$ equals the reachability probability for $\bar{z}_k$ at time 0: We can always turn a time-dependent reachability problem into a more classical space-dependent one. From the previous discussion, the following lemma follows:

Lemma 5.3. *Let $\mathscr{X}^{(N)}$ be a sequence of CTMC models, as defined in Section 3.1, and let $Z_k^{(N)}$ and z_k be defined from $\mathscr{X}^{(N)}$ as in Section 3.3.*
Let $\varphi = \varphi(\mathbf{p})$ be a robust CSL formula for the piecewise analytic trajectory $\Phi(t,\mathbf{x}_0)$, and let z_k be the ICTMC defined on $\mathscr{S}$ with respect to trajectory $\Phi(t,\mathbf{x}_0)$. Then,

$$s,\mathbf{x}_0 \models_{\mathbf{y}} \varphi \Leftrightarrow s \models_{z_k} \varphi.$$

■

Using the previous lemmas, we can easily show the following theorem.

Theorem 5.4. *Let $\mathscr{X}^{(N)}$ be a sequence of CTMC models, as defined in Section 3.1, and let $Z_k^{(N)}$ and z_k be defined from $\mathscr{X}^{(N)}$ as in Section 3.3.*
Assume that there is a flow tube E_0 of $\mathbf{x}_0$ such that all trajectories in E_0 are piecewise analytic.
Let $\varphi = \varphi(\mathbf{p})$ be a robust CSL formula for the trajectory $\Phi(t,\mathbf{x}_0)$, let $Z_k^{(N)}(t)$ and $z_k(t)$ be the stochastic processes on $\mathscr{S}$ defined as in Section 3.3, and let $\mathbf{y}(t)$ and $\mathbf{Y}^{(N)}(t)$ be defined as in this section. Then, there is an N_0 such that, for all $N \geq N_0$,

$$s \models_{Z_k^{(N)}} \varphi \;\Leftrightarrow\; s, \nu^{(N)}(\mathbf{x}_0) \models_{\mathbf{Y}^{(N)}} \varphi.$$

Proof. There exists an N_0, such that, for all $N \geq N_0$,

$$s \models_{Z_k^{(N)}} \varphi \;\Leftrightarrow\; s \models_{z_k} \;\Leftrightarrow\; s, \mathbf{x}_0 \models_{\mathbf{y}} \varphi \;\Leftrightarrow\; s, \nu^{(N)}(\mathbf{x}_0) \models_{\mathbf{Y}^{(N)}} \varphi,$$

where the first equivalence follows from Theorem 5.3, the second equivalence from Lemma 5.3, and the third equivalence from Lemma 5.2, while N_0 can be chosen as the largest one between that of Theorem 5.3 and that of Lemma 5.2. ■

Inspecting the proof of the previous theorem, the following corollary is straightforward.

Corollary 5.4. *Let $\varphi = \varphi(\mathbf{p})$ be a robust CSL formula for the trajectory $\Phi(t,\mathbf{x}_0)$. Then, there is an N_0 such that, for all $N \geq N_0$,*

$$s, \nu^{(N)}(\mathbf{x}_0) \models_{\mathbf{Y}^{(N)}} \varphi \Leftrightarrow s \models_{z_k} \varphi.$$

■

6 Conclusions

In this paper we exploited a corollary of fluid limit theorems to approximate properties of the behaviour of single agents in large population models. In particular, we focussed on reachability and stochastic model checking of CSL formulae. The method proposed requires us to model check a time-inhomogeneous CTMC of size equal to the number of internal states of the agent (which is usually very small). Hence, it gives a large improvement in terms of computational efficiency.

We then focussed on the reachability problem for ICTMC, both in the case of time constant and time varying sets. We provided algorithms to tackle both cases, and we also proved convergence of the reachability probabilities computed for the single agent in a finite population of size N to those of the limit fluid CTMC. Finally, we focussed on model checking CSL formulae for ICTMC proposing an algorithm working for a subset of CSL with only the time bounded until operator. We also showed a decidability and a convergence result for robust formulae, proving that the set of non-robust formulae has measure zero.

There are many issues that we wish to tackle in the future. First, we would like to better understand the quality of convergence. This can be accomplished by trying to derive theoretical error bounds (which may be too loose to be of practical interest) and by running many experiments to identify situations in which the approximation performs well (in terms of classes of formulae and model structure). In addition, we would like to provide a working implementation of the model checking algorithm for ICTMC, studying its computational cost in practice (and how easy it is in practice to find a non computable instance). Furthermore, we want to investigate the connections between single agent properties and system level properties. We believe this approach can become a powerful tool to investigate the relationship between microscopic and macroscopic characterisations of systems, and to understand their emergent behaviour.

As far as CSL model checking for ICTMC is concerned, we aim at extending it to include the time bounded next operator, and time unbounded and steady state operators, at least for those subsets of rate functions in which the algorithm can be shown to be decidable. We also need to consider rewards, at least for a finite time horizon (here we expect their inclusion to be relatively straightforward). Then, we would like to show convergence results also for this larger subset of CSL, under the hypothesis required for steady state convergence of the fluid approximation.

Another line of investigation would be to consider different temporal logics, like MTL. For this logic, asymptotic correctness is relatively easy to prove, along the lines of Proposition 4.1. What is more difficult is to find an effective algorithm to model check MTL properties for ICTMC. One possibility may be to combine the approaches of [15–17], and exploit algorithms and approaches to compute reachability of PDMP [20].

References

[1] L. Ahlfors (1953): *Complex Analysis, 1st ed.* McGraw Hill, Cambridge.

[2] G. Alefeld & G. Mayer (2000): *Interval analysis: theory and applications*. Journal of Computational and Applied Mathematics 121, pp. 421–464.

[3] A. Andreychenko, P. Crouzen & V. Wolf (2011): *On-the-fly Uniformization of Time-Inhomogeneous Infinite Markov Population Models*. In: Proceedings Ninth Workshop on Quantitative Aspects of Programming Languages, QAPL 2011, EPTCS 57, p. 1. Available at http://arxiv.org/abs/1006.4425.

[4] A. Aziz, K. Sanwal, V. Singhal & R. Brayton (2000): *Model-Checking Continuous Time Markov Chains*. ACM Trans. Comp. Logic 1, pp. 162–170.

[5] A. Aziz, V. Singhal, F. Balarin, R. Brayton & A. Sangiovanni-Vincentelli (1996): *Verifying Continuous Time Markov Chains*. In: Proceedings of CAV96.

[6] C. Baier, B. Haverkort, H. Hermanns & J.P. Katoen (2000): *Model Checking Continuous-Time Markov Chains by Transient Analysis*. In: Proceedings of Computer Aided Verification, Lecture Notes in Computer Science 1855, pp. 358–372, doi:10.1007/10722167_28.

[7] R. Bakhshi, L. Cloth, W. Fokkink & B.R. Haverkort (2009): *Mean-Field Analysis for the Evaluation of Gossip Protocols*. In: Proceedings of the Sixth International Conference on the Quantitative Evaluation of Systems, QEST 2009, IEEE Computer Society, pp. 247–256. Available at 10.1109/QEST.2009.38.

[8] R. Bakhshi, L. Cloth, W. Fokkink & B.R. Haverkort (2011): *Mean-field framework for performance evaluation of push-pull gossip protocols*. Perform. Eval. 68(2), pp. 157–179. Available at 10.1016/j.peva.2010.08.025.

[9] M. Benaïm (1998): *Recursive algorithms, urn processes and chaining number of chain recurrent sets*. Ergodic Theory and Dynamical Systems .

[10] M. Benaïm & J. Le Boudec (2008): *A Class of Mean Field Interaction Models for Computer and Communication Systems*. Performance Evaluation .

[11] M. Benaïm & J.Y. Le Boudec (2011): *On Mean Field Convergence and Stationary Regime*. CoRR abs/1111.5710. Available at http://arxiv.org/abs/1111.5710.

[12] M. Benaïm & J. Weibull (2003): *Deterministic Approximation of Stochastic Evolution in Games*. Econometrica .

[13] P. Billingsley (1979): *Probability and Measure*. John Wiley and Sons.

[14] L. Bortolussi & A. Policriti (2009): *Dynamical systems and stochastic programming — from Ordinary Differential Equations and back*. Transactions of Computational Systems Biology XI.

[15] T. Chen, M. Diciolla, M.Z. Kwiatkowska & A. Mereacre (2011): *Time-Bounded Verification of CTMCs against Real-Time Specifications*. In: Proceedings of the 9th International Conference on Formal Modeling and Analysis of Timed Systems - FORMATS 2011, pp. 26–42. Available at `10.1007/978-3-642-24310-3_4`.

[16] T. Chen, T. Han, J.P. Katoen & A. Mereacre (2009): *LTL Model Checking of Time-Inhomogeneous Markov Chains*. In: Proceedings of the 7th International Symposium on Automated Technology for Verification and Analysis, ATVA 2009, Lecture Notes in Computer Science 5799, Springer, pp. 104–119. Available at `10.1007/978-3-642-04761-9_10`.

[17] T. Chen, T. Han, J.P. Katoen & A. Mereacre (2011): *Model Checking of Continuous-Time Markov Chains Against Timed Automata Specifications*. Logical Methods in Computer Science 7(1). Available at `10.2168/LMCS-7(1:12)2011`.

[18] R.W.R. Darling (2002): *Fluid Limits of Pure Jump Markov Processes: A Practical Guide*. `arXiv.org` .

[19] R.W.R. Darling & J.R. Norris (2008): *Differential equation approximations for Markov chains*. Probability Surveys 5.

[20] M.H.A. Davis (1993): *Markov Models and Optimization*. Chapman & Hall.

[21] G.B. Folland (1995): *Introduction to Partial Differential Equations*. Princeton University Press.

[22] P. Franek, S. Ratschan & P. Zgliczynski (2011): *Satisfiability of systems of equations of real analytic functions is quasi-decidable*. In: Proceedings of the 36th international conference on Mathematical foundations of computer science, MFCS'11, pp. 315–326.

[23] N. Gast & B. Gaujal (2010): *A mean field model of work stealing in large-scale systems*. In: Proceedings of ACM SIGMETRICS 2010, pp. 13–24. Available at `http://doi.acm.org/10.1145/1811039.1811042`.

[24] R. Hayden & J. T. Bradley (2010): *A fluid analysis framework for a Markovian process algebra*. Theoretical Computer Science .

[25] R.A. Hayden, A. Stefanek & J.T. Bradley (2012): *Fluid computation of passage-time distributions in large Markov models*. Theor. Comput. Sci. 413(1), pp. 106–141. Available at `10.1016/j.tcs.2011.07.017`.

[26] J. Hillston (1996): *A Compositional Approach to Performance Modelling*. Cambridge University Press.

[27] J. Hillston (2005): *Fluid Flow Approximation of PEPA models*. In: Proceedings of the Second International Conference on the Quantitative Evaluation of Systems (QEST 2005).

[28] A. Jensen (1953): *Markov chains as an aid in the study of Markov processes*. Skandinavisk Aktuarietidskriff 36.

[29] S. K. Jha, E. M. Clarke, C. J. Langmead, A. Legay, A. Platzer & P. Zuliani (2009): *A Bayesian Approach to Model Checking Biological Systems*. In: Proceedings of the 7th International Conference on Computational Methods in Systems Biology, CMSB 2009, Lecture Notes in Computer Science 5688, pp. 218–234, doi:10.1007/978-3-642-03845-7_15.

[30] T. Johnson & W. Tucker (2009): *Enclosing all zeros of an analytic function — A rigorous approach*. Journal of Computational and Applied Mathematics 228(1), pp. 418–423, doi:10.1016/j.cam.2008.10.014.

[31] J.-P. Katoen & A. Mereacre (2008): *Model Checking HML on Piecewise-Constant Inhomogeneous Markov Chains*. In: Proceedings of the 6th International Conference on Formal Modeling and Analysis of Timed Systems, FORMATS 2008, Lecture Notes in Computer Science 5215, Springer, pp. 203–217. Available at `10.1007/978-3-540-85778-5_15`.

[32] M. Kattenbelt, M.Z. Kwiatkowska, G. Norman & D. Parker (2008): *Game-Based Probabilistic Predicate Abstraction in PRISM*. Electr. Notes Theor. Comput. Sci. 220(3), pp. 5–21. Available at `10.1016/j.entcs.2008.11.016`.

[33] M. Kattenbelt, M.Z. Kwiatkowska, G. Norman & D. Parker (2009): *Abstraction Refinement for Probabilistic Software*. In: Proceedings of the 10th International Conference on Verification, Model Checking,

and Abstract Interpretation, VMCAI 2009, *LNCS* 5403, Springer, pp. 182–197. Available at `10.1007/978-3-540-93900-9_17`.

[34] A. Kolesnichenko, A. Remke, P.T. de Boer & B.R. Haverkort (2011): *Comparison of the Mean-Field Approach and Simulation in a Peer-to-Peer Botnet Case Study*. In: *Proceedings of 8th European Performance Engineering Workshop, EPEW 2011*, *LNCS* 6977, Springer, pp. 133–147. Available at `10.1007/978-3-642-24749-1_11`.

[35] S. Krantz & P.R. Harold (2002): *A Primer of Real Analytic Functions (Second ed.)*. Birkhäuser.

[36] T. Kurtz & S. Ethier (1986): *Markov Processes - Characterisation and Convergence*. Wiley.

[37] T. G. Kurtz (1970): *Solutions of Ordinary Differential Equations as Limits of Pure Jump Markov Processes*. *Journal of Applied Probability* 7, pp. 49–58.

[38] M. Kwiatkowska, G. Norman & D. Parker (2004): *Probabilistic Symbolic Model Checking with PRISM: A Hybrid Approach*. *International Journal on Software Tools for Technology Transfer* 6(2), pp. 128–142.

[39] M. Massink, D. Latella, A. Bracciali, M. Harrison & J. Hillston (in print): *Scalable context-dependent analysis of emergency egress models*. *Formal Aspects of Computing* , pp. 1–36doi:10.1007/s00165-011-0188-1.

[40] A. Neumaier (1990): *Interval Methods for Systems of Equations*. University Press, Cambridge.

[41] J. R. Norris (1997): *Markov Chains*. Cambridge University Press.

[42] D. Novikov (2000): *Systems of linear ordinary differential equations with bounded coefficients may have very oscillating solutions*. *ArXiv Mathematics e-prints* .

[43] H. Qian & E.L. Elson (2002): *Single-molecule enzymology: stochastic Michaelis?Menten kinetics*. *Biophysical Chemistry* 101, p. 565?576.

[44] D. Richardson (1991): *Effective methods in algebraic geometry*, chapter Finding roots of equations involving functions defined by first order differential equations. Birkhäuser.

[45] D. Richardson (2007): *Zero Tests for Constants in Simple Scientific Computation*. *Mathematics in Computer Science* 1(1), pp. 21–37. Available at `10.1007/s11786-007-0002-x`.

[46] W. Rudin (1976): *Principles of Mathematical Analysis*. McGraw-Hill.

[47] J. Rutten, M. Kwiatkowska, G. Norman & D. Parker (2004): *Mathematical Techniques for Analyzing Concurrent and Probabilistic Systems*. *CRM Monograph Series* 23, American Mathematical Society.

[48] K.R. Sanft, D.T. Gillespie & L.R. Petzold (2011): *Legitimacy of the stochastic Michaelis-Menten approximation*. *IET Syst. Biol.* 5(1), pp. 58–69.

[49] A. Singh & J.P. Hespanha (2006): *Lognormal Moment Closures for Biochemical Reactions*. In: *Proceedings of 45th IEEE Conference on Decision and Control*.

[50] D.T.J. Sumpter (2000): *From Bee to Society: An Agent-based Investigation of Honey Bee Colonies*. Ph.D. thesis, University of Manchester.

[51] P. Taylor (2010): *A Lambda Calculus for Real Analysis*. *Journal of Logic and Analysis* 2(5), pp. 1–115, doi:10.4115/jla.2010.2.5.

[52] M Tribastone, S. Gilmore & J. Hillston (2010): *Scalable Differential Analysis of a Process Algebra Model*. *Transactions on Software Engeneering* .