Model Checking Continuous Time Markov Chains

Adnan Aziz
The University of Texas at Austin
and
Kumud Sanwal
Lucent Technologies
and
Vigyan Singhal
Tempus-Fugit, Inc.
and
Robert Brayton
The University of California at Berkeley

We present a logical formalism for expressing properties of continuous time Markov chains. The semantics for such properties arise as a natural extension of previous work on discrete time Markov chains to continuous time. The major result is that the verification problem is decidable; this is shown using results in algebraic and transcendental number theory.

Categories and Subject Descriptors: D.2.4 [**Software/Program Verification**]: Model checking; F.3.1 [**Specifying and Verifying and Reasoning about Programs**]: Logics of Programs; C.2.2 [**Network Protocols**]: Protocol verification; G.1.5 [**Roots of Nonlinear Equations**]: Systems of equations; G.3 [**Probability and Statistics**]: Stochastic processes

General Terms: Verification, Markov Chains, Algebra

Additional Key Words and Phrases: Formal Verification, Model Checking, Real Time, Transcendental Number Theory

1. INTRODUCTION

Recent work on formal verification has addressed systems with stochastic dynamics. Certain models for discrete time Markov chains have been investigated in [Hansson and Jonsson 1994; Courcoubetis and Yannakakis 1988]. However, a large class of stochastic systems operate in continuous time. In a generalized decision and control

This paper is an expanded and revised version of an eponymous paper presented by the authors at the Computer-Aided Verification Conference held at Rutgers, NJ in 1996. Support from IBM, NSF, SRC, and The State of Texas is gratefully acknowledged.

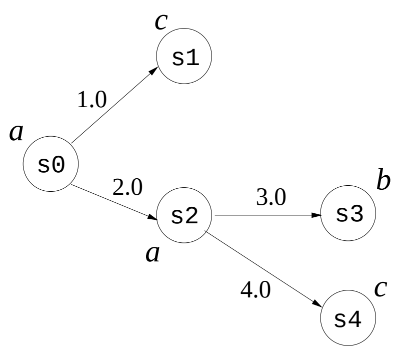

Fig. 1. A continuous time Markov chain: $S = \{s_0, s_1, s_2, s_3\}$, $A = \{a, b, c\}$. Only edges with positive weights are shown.

framework, continuous time Markov chains form a useful extension [Ross 1983]. We propose a logic for specifying properties of such systems, and describe a decision procedure for the model checking problem. Our result differs from past work on verifying continuous time Markov chains [Alur et al. 1991] in that quantitative bounds on the probability of events can be expressed in the logic.

2. CONTINUOUS TIME MARKOV CHAINS

Formally, a continuous time Markov chain M is a 4-tuple (S, Λ, A, θ), where $S = \{s_1, s_2, \ldots, s_n\}$ is a finite set of *states*, Λ is the *transition rate matrix*, A is a finite set of *outputs*, and $\theta : S \mapsto A$ is the *output function.* The transition rate matrix Λ is an $|S| \times |S|$ matrix. The off-diagonal entries are nonnegative rationals; the diagonal element $\lambda_{j,j}$ is constrained to be $-(\sum_{i \neq j} \lambda_{j,i})$. Consequently, the row sums of Λ are zero.

An example of a continuous time Markov chain is presented in Figure 1.

The notion of a continuous time Markov chain can be generalized to include rate matrices whose entries vary with time. We will restrict our attention to *homogeneous* continuous time Markov chains, for which the rate matrices are constants.

At state s_j, the probability of making a transition to state s_k (where $k \neq j$) in time dt is given by $\lambda_{j,k}\, dt$. This is the basis for formulating a stochastic differential equation for the evolution of the probability distribution whose solution is

$$D(t) \;=\; e^{\Lambda^T t} \cdot D_0$$

Here D_0 is a column vector of dimension $|\, S \,|$, with the constraint that $\sum_i D_0[i] = 1$.

A *path* through M is a function on domain $[0, \infty)$ and range S. any state s, we will denote by U^s the set of all paths beginning at s. We will later see how to compute the probability of a set of paths Π starting from a given state s using the rate transition matrix; this probability will be denoted by $\mu^s(\Pi)$. Given a set β of functions from $[0, \infty)$ to A, we will abuse notation and refer to $\mu^s(\beta)$ when we mean the probability of the set of paths starting at s whose images under θ map to elements in β. We will not dwell on the technicalities of measure theory; all sets of paths considered in this paper will be measurable.

3. CSL SYNTAX AND SEMANTICS

Let $M = (S, \Lambda, A, \theta)$ be a continuous time Markov chain. In this section, we develop formal syntax and semantics for CSL (Continuous Stochastic Logic). This logic is inspired by the logic CTL [Emerson 1990], and its extensions to discrete time stochastic systems (pCTL [Hansson and Jonsson 1994]), and continuous time nonstochastic systems (tCTL [Alur et al. 1990]).

There are two types of formulae in CSL: state formulae (which are true or false in a specific state), and path formulae (which are true or false along a specific path). A state formula is given by the following syntax:

(1) $\mathbf{a}$ for $a \in A$

(2) If f_1 and f_2 are state formula, then so are $\neg f_1, f_1 \vee f_2$

(3) If g is a path formula, then $Pr_{>c}(g)$ is a state formula, where c is a rational between 0 and 1 expressed as the ratio of two binary coded integers.

Path formulas are formulas of the form

—$f_1 U_{[a_1,b_1]} f_2 U_{[a_2,b_2]} \cdots f_n$, where $f_1, f_2, \ldots f_n$ are state formulas, and $a_1, b_1, \ldots, a_{n-1}, b_{n-1}$ are nonnegative rationals expressed as the ratio of two binary coded integers.

CSL is the set of state formulae that are generated by the above rules.

Let f be a state formula, and g be a path formula. We now define the satisfaction relation ($\models_M$) using induction on the length of the formula. For a state formula f we use $[\![f]\!]_M$ to denote the set of states satisfying f.

(1) f is of the form $\mathbf{a}$: $s \models_M f$ iff $\theta(s) = a$.

(2) f is of the form $(\neg f_1)$: $s \models_M f$ iff $s \not\models_M f$.

(3) f is of the form $(f_1 \vee f_2)$: $s \models_M f$ iff $s \models_M f_1$ or $s \models_M f_2$.

(4) f is of the form $Pr_{>c}(g)$: $s \models_M f$ iff $\mu^s(\{\pi \in U^s \mid \pi \models_M g\}) > c$.

(5) g is a path formula of the form $f_1 U_{[a_1,b_1]} f_2 U_{[a_2,b_2]} \cdots f_n$: $\pi \models_M g$ iff there exist real numbers $t_1, \ldots, t_{n-1}$ such that for each integer in $[1, n]$ we have $(a_i \leq t_i \leq b_i) \wedge \left(\forall t' \in [t_{i-1}, t_i)\right) \left(\pi(t) \in [\![f_i]\!]_M\right)$, where t_{-1} is defined to be 0 for notational convenience.

Example 1. The formula $\phi = Pr_{>0.3}(a U_{[0.0,4.0]} b)$ is a state formula for the Markov chain in Figure 1. It formally expresses the property that with probability greater than 0.3, the system will remain in a state where the output is a before making a transition before 4.0 time units have elapsed to a state where the output is b.

The probability of the set of paths starting at s_0 on which the output is a before becoming b before time 4.0 is given by the following integral:

$$\int_0^{4.0} e^{-3x} \cdot 3 \cdot \frac{2}{3} \cdot \left(1 - e^{-7\cdot(4-x)}\right) \cdot \frac{3}{7} \cdot dx$$

This simplifies to $\frac{1}{14}\left(4 - 7 \cdot e^{-12} + 3 \cdot e^{-28}\right)$, which is smaller than 0.3, and so ϕ is false at s_0.

4. CSL MODEL CHECKING

The CSL model checking problem is as follows: given a continuous time Markov chain M, a state s in the chain, and a CSL formula f, is it the case that $s \models_M f$? In this section we establish that there is an effective procedure for model checking CSL.

THEOREM 1. *CSL model checking is decidable.*

PROOF. The nontrivial step in model checking is to model check formula of the form $Pr_{>c}(g)$. In order to do this we need to be able to effectively reason about the quantity $\mu^s(\{\text{paths } \pi \mid \pi(0) = s_0 \wedge \pi \models_M g\})$.

First we review some elementary algebra. An *algebraic complex number* is any complex number which is the root of a polynomial with rational coefficients. We will denote the set of algebraic complex numbers by $\mathcal{A}$. Properties of the algebraic numbers are derived in [Niven 1956]; of particular interest to us is the fact that they constitute a field, and that the real and imaginary parts of an algebraic number are also algebraic.

We will denote the set of complex numbers which are finite sums of the form $\sum_j \eta_j e^{\delta_j}$ where the η_j and δ_j are algebraic by $E_{\mathcal{A}}$. The set $E_{\mathcal{A}}$ is trivially closed under finite sums, and is easily seen to be closed under multiplication; consequently it is a ring.

Tarski [Tarski 1951] proved that the theory of the field of complex numbers was decidable; an effective (in the recursion-theoretic sense) procedure for converting formulas to a logically equivalent quantifier-free form was given. Consequences of this result include the existence of effective procedures for determining the number of distinct roots of a polynomial, and testing the equality of algebraic numbers defined by formulas.

We now demonstrate how to compute the probability of the set of paths which start at a designated state and satisfy a specified path formula. Consider a path formula of the form $\psi_0 U_{[a_1,b_1]} \psi_1 U_{[a_2,b_2]} \psi_2 \ldots$

First, consider the case where the time intervals $[a_1, b_1]$, $[a_2, b_2], \ldots$ are non overlapping.

We define the following matrices.

—a transition rate matrix $Q_{i,i}$ obtained from Λ, that treats $[\![\psi_i]\!]_M^c$ as an absorbing set of states. This is obtained by using

$$\begin{aligned} q(j,k) &= \lambda_{j,k} \ \text{ if } \ s_j \in [\![\psi_i]\!]_M \\ &= 0 \quad \text{ if } \ s_j \in [\![\psi_i]\!]_M^c \end{aligned}$$

this enables us to model the transitions where the Markov chain remains in $[\![\psi_i]\!]_M$.

—a transition rate matrix $Q_{i-1,i}$ obtained from Λ, that treats $[\![\psi_{i-1}]\!]_M^c \cap [\![\psi_i]\!]_M^c$ as an absorbing set of states. For this we use

$$\begin{aligned} q(j,k) &= \lambda_{j,k} \ \text{ if } \ s_j \in [\![\psi_i]\!]_M \cup [\![\psi_{i-1}]\!]_M \\ &= 0 \quad \text{ if } \ s_j \in [\![\psi_i]\!]_M^c \cap [\![\psi_{i-1}]\!]_M^c \end{aligned}$$

this allows us to model the transitions from $[\![\psi_{i-1}]\!]_M$ to $[\![\psi_i]\!]_M$.

—An indicator matrix I_i for $[\![\psi_i]\!]_M$, such that

$$\begin{aligned} I_i(j,k) &= 1 \quad \text{if } s_j = s_k \in [\![\psi_i]\!]_M \\ &= 0 \quad \text{otherwise} \end{aligned}$$

Hence, the probability of a formula of the form

$$f_1 = \psi_0 U_{[a_1,b_1]} \psi_1 U_{[a_2,b_2]} \psi_2 \cdots U_{[a_n,b_n]} \psi_n \tag{1}$$

is given by

$$\begin{aligned} \mu^s(f_1) = \pi_s \cdot P_{0,0}(a_1) \cdot I_0 \cdot P_{0,1}(b_1 - a_1) \cdot I_1 \cdot P_{1,1}(a_2 - b_1) \cdot \\ I_1 \cdot P_{1,2}(b_2 - a_2) \cdot I_2 \cdots P_{n-1,n}(b_n - a_n) \cdot I_n \cdot \underline{1} \end{aligned} \tag{2}$$

where $P_{l,m}(t), t \geq 0$ is the one step transition matrix for time t corresponding to the transition rate matrix $Q_{l,m}$, π_s is the starting probability distribution, which in our case has unity for state s and zeros otherwise, and $\underline{1}$ is the column vector whose elements are all 1.

For a continuous time Markov chain with a transition rate matrix Q, the one step transition matrix for time t is given by $P(t) = e^{Qt}$. Note that entries of Q are rationals, and the arguments of $P_{i-1,i}$ are rationals (since a_i, b_i are rational). This observation leads to the following lemma:

LEMMA 1. *Each element of the $P_{l,m}(t)$ matrices as specified in Equation 2 may be expressed as a finite sum $\sum_j \eta_j e^{\delta_j}$ where η_j and δ_j are algebraic complex numbers.*

PROOF. Let B be any square matrix whose entries are rationals. The matrix B can always be expressed in Jordan canonical form [Kaliath 1980], i.e., in the form $C \cdot J \cdot C^{-1}$. Here J is an upper block diagonal matrix as shown below:

$$\begin{bmatrix} J_1 & 0 & \cdots & & 0 \\ 0 & J_2 & 0 & \cdots & 0 \\ 0 & \cdots & J_3 & \cdots & 0 \\ & & & \ddots & \\ 0 & & \cdots & & J_n \end{bmatrix}$$

The diagonal entries of each J_i are the eigenvalues of B, and the remaining entries of J_i are unity, as shown below:

$$\begin{bmatrix} \lambda_i & 1 & 0 & \ldots & 0 \\ 0 & \lambda_i & 1 & \ldots & 0 \\ & & & \ddots & \\ 0 & & \cdots & 0 & \lambda_i \end{bmatrix}$$

The size of J_i is equal to the multiplicity of λ_i. Since the eigenvalues are the solutions of the characteristic equation of B and the entries of B are rationals, the eigenvalues are, by definition, algebraic complex numbers. The entries of C and C^{-1} can be computed using linear algebra, and thus are also algebraic complex numbers.

The matrix e^{Bt} is equal to $C \cdot e^{Jt} \cdot C^{-1}$ and e^{Jt} is of the following form:

$$\begin{bmatrix} e^{J_1 t} & 0 & \cdots & & 0 \\ 0 & e^{J_2 t} & 0 & \cdots & 0 \\ 0 & \cdots & e^{J_3 t} & \cdots & 0 \\ & & & \ddots & \\ 0 & & \cdots & & e^{J_n t} \end{bmatrix}$$

The sub-matrix $e^{J_i t}$ is of the form

$$\begin{bmatrix} e^{\lambda_i t} & te^{\lambda_i t} & (t^2 e^{\lambda_i t})/2! & \cdots & (t^{m_i} e^{\lambda_i t})/(m_i)! \\ 0 & e^{\lambda_i t} & te^{\lambda_i t} & \cdots & (t^{m_i - 1} e^{\lambda_i t})/(m_i - 1)! \\ & & & \ddots & \\ & & & & e^{\lambda_i t} \end{bmatrix}$$

By inspection, the elements of $e^{J_i t}$ are members of $E_{\mathcal{A}}$. Since $E_{\mathcal{A}}$ is a ring, it is closed under products and finite sums. Hence the lemma follows. □

Applying Lemma 1 to Equation 3 we see that $\mu^s(f_1)$ is a member of $E_{\mathcal{A}}$, i.e., equal to an expression of the form $\sum_k \eta_k e^{\delta_k}$ where the η_k, δ_k are algebraic. Since are effective procedures for checking the equality of algebraic numbers, $\mu^s(f_1)$ can be effectively simplified to an expression of the form $\sum_{k'} \eta_{k'} e^{\delta_{k'}}$ where the $\eta_{k'}$'s are non zero, and the $\delta_{k'}$'s are distinct.

In general, it is extremely difficult to verify relationships between transcendental numbers [Richardson 1997]; skeptics are invited to check if $e^{\pi\sqrt{163}}$ is equal to 262537412640768744. Indeed, the theory of the real exponential field is conjectured to be decidable, but no complete proof exists of this fact [Wilkie 1995].

However, we can effectively decide if $\mu^s(f_1) > c$, by exploiting a celebrated theorem of transcendental number theory [Niven 1956].

Theorem 2 (Lindemann-Weierstrass). *Let $c_1, \ldots c_n$ be pairwise distinct algebraic complex numbers numbers. Then there exists no equation $a_1 e^{c_1} + \cdots + a_n e^{c_n} = 0$ in which $a_1, \ldots, a_n$ are algebraic numbers and are not all zero.* [1]

Suppose the expression $\sum_{k'} \eta_{k'} e^{\delta_{k'}}$ is degenerate, i.e., it consists of a single term of the form η_0. Then the expression denotes an algebraic number, and it can be effectively checked if it is greater than c.

If it is not degenerate, invoking the Lindemann-Weierstrass theorem and noting that c is rational, we see that $\mu^s(f_1)$ can not be equal to c and so $\mid \mu^s(f_1) - c \mid > 0$.

Decidability of model checking follows from the following lemma.

Lemma 2. *Given a transcendental real r of the form $\sum_j \eta_j e^{\delta_j}$ where the η_j and δ_j are algebraic complex numbers, and the δ_j's are pairwise distinct, there is an effective procedure to test if $r > c$ for rational c.*

Proof. Suppose a sequence of algebraic numbers $S_1, S_2, \ldots$ such that $|r - S_k| < 2^{-k}$ can be effectively constructed. Let $|r - c| = a > 0$. By the triangle inequality, $|r - c| \leq |r - \texttt{Re}(S_k)| + |\texttt{Re}(S_k) - c|$. Hence $|r - \texttt{Re}(S_k)| + |\texttt{Re}(S_k) - c|$ is

[1]This result implies the transcendence of π (take $n = 2$, $c_1 = 0, c_2 = i\pi$); it was the first proof of the nonalgebraic nature of π. For a highly readable account of the development of this theorem, refer to [Ewing 1991].

bounded away from 0 by a. Since r is real, $|\, r - \mathtt{Re}(S_k) \,| \leq |\, r - (S_k) \,| < 2^{-k}$, and $|\, r - \mathtt{Re}(S_k) \,| + |\, \mathtt{Re}(S_k) - c \,|$ is bounded away from 0 by a, for sufficiently large k, it must be that $|\, \mathtt{Re}(S_k) - c \,| > 2^{-k}$. The sign of of $\mathtt{Re}(S_k) - c$ is the sign of $r - c$.

In order to construct the sequence $S_1, S_2, \ldots$ we use the fact that e^z can be approximated with an error of less than ϵ (when $\epsilon < 1$) by taking the first $\lceil (3 \cdot |\, z \,|^2 \,/ \epsilon) \rceil + 1$ terms of the Maclaurin expansion for e^z. This can be extended to obtain an upper bound on the number of terms needed to approximate r to within ϵ. Since the individual terms in the Maclaurin expansion are algebraic functions of the δ_j's, it follows that the approximations are algebraic. □

Now consider the case in which the successive intervals $[a_i, b_i]$ where the transitions are desired are allowed to overlap. Since a formula is finite, we can have a finite number of overlapping intervals. A key observation is that the finite number of overlaps allows us to partition the time in a finite number of nonoverlapping intervals and write the probability of the specification (set of acceptable paths) as a sum of the probabilities of disjoint events. This enables us to write $\mu^s(f_1)$ as the sum of exponentials of algebraic complex numbers, weighted by algebraic coefficients. To illustrate this, consider the formula

$$f_2 = \psi_0 U_{[a_1,b_1]} \psi_1 U_{[a_2,b_2]} \psi_2$$

where $0 < a_1 < a_2 < b_1 < b_2$. In this case, we may realize f_2 as one of four disjoint cases and hence we can write

$$\begin{aligned} \mu^s(f_2) \;=\; & \mu^s(\psi_0 U_{[a_1,a_2]} \psi_1 U_{[a_2,b_1]} \psi_2) + \mu^s(\psi_0 U_{[a_1,a_2]} \psi_1 U_{[b_1,b_2]} \psi_2) \\ & + \mu^s(\psi_0 U_{[a_2,b_1]} \psi_1 U_{[b_1,b_2]} \psi_2) + \mu^s(\psi_0 U_{[a_2,b_1]} \psi_1 U_{[a_2,b_1]} \psi_2) \end{aligned} \tag{3}$$

The first three terms are equivalent to the case with nonoverlapping intervals. The last term involves having both the $[\![\psi_0]\!]_M \rightarrow [\![\psi_1]\!]_M$ and $[\![\psi_1]\!]_M \rightarrow [\![\psi_2]\!]_M$ transitions in the same interval $[a_2, b_1]$ in the correct order. This may be evaluated by integrating the probabilities over the time of the first transition.

$$\mu^s(\psi_0 U_{[a_2,b_1]} \psi_1 U_{[a_2,b_1]} \psi_2) \;=\; \pi_s P_{0,0}(a_2) I_0 \int_{a_2}^{b_1} P_{0,0}(t - a_2) I_0 Q_{0,1} I_1 P_{1,2}(b_1 - t) I_2 dt$$

It is clear that since the integrand involved algebraic terms and and exponentials in algebraic complex numbers and t, the definite integral with rational limits can be written in the form of a sum of exponentials of algebraic numbers with algebraic coefficients. Hence, this term is in $E_{\mathcal{A}}$. The other three terms in Equation 3 correspond to forms equivalent to the nonoverlapping intervals case, and hence already satisfy the decidability criteria.

5. CONCLUSIONS AND FUTURE WORK

We have defined a logic for specifying properties of finite state continuous time Markov chains. The model checking problem for this logic was shown to be decidable through a combination of results in algebraic and transcendental number theory.

In practice, we expect that rational approximations to the expression on the right hand side of Equation 3 as computed by standard numerical methods should suffice. Baier *et al.* [Baier et al. 1999] describe an implementation of such a model checker;

by clever choice of data structures, their procedure avoids some of the complexity of verifying systems which result from the composition of individual Markov chains.

REFERENCES

ALUR, R., COURCOUBETIS, C., AND DILL, D. 1990. Model Checking for Real-Time Systems. In *Proc. IEEE Symposium on Logic in Computer Science* (1990), pp. 414–425.

ALUR, R., COURCOUBETIS, C., AND DILL, D. 1991. Model Checking for Probabilistic Real Time Systems. In *Proc. of the Colloquium on Automata, Languages, and Programming* (1991), pp. 115–126.

BAIER, C., KATOEN, J.-P., AND HERMANNS, H. 1999. Approximate Symbolic Model Checking of Continuous-Time Markov Chains. In *Proc. of the Conference on Concurrency* (1999).

COURCOUBETIS, C. AND YANNAKAKIS, M. 1988. Verifying Temporal Properties of Finite State Probabilistic Programs. In *Proc. IEEE Conference on Decision and Control* (1988), pp. 338–345.

EMERSON, E. A. 1990. Temporal and Modal Logic. In J. VAN LEEUWEN Ed., *Formal Models and Semantics*, Volume B of *Handbook of Theoretical Computer Science*, pp. 996–1072. Elsevier Science.

EWING, J. H. 1991. *Numbers.* Springer-Verlag.

HANSSON, H. AND JONSSON, B. 1994. A Logic for Reasoning about Time and Reliability. *Formal Aspects of Computing 6*, 512–535.

KALIATH, T. 1980. *Linear Systems.* Prentice-Hall.

NIVEN, I. 1956. *Irrational Numbers.* John-Wiley.

RICHARDSON, D. 1997. How to recognize zero. *Journal of Symbolic Computation 24*, 6 (Dec.).

ROSS, S. 1983. *Stochastic Processes.* John-Wiley.

TARSKI, A. 1951. *A Decision Procedure for Elementary Algebra and Geometry.* University of California Press.

WILKIE, A. J. 1995. On the Decidability of the Real Exponential Field. In *Conference on Order in Algebra and Logic* (Oxford, UK, 1995).