The Complexity of Relating Quantum Channels to Master Equations

Toby S. Cubitt*[1,2], Jens Eisert[3,4], and Michael M. Wolf[5,6]

[1]*Department of Mathematics, University of Bristol*
University Walk, Bristol BS8 1TW, UK
[2]*Departamento de Análisis Matemático, Universidad Complutense de Madrid*
Plaza de Ciencias 3, Ciudad Universitaria, 28040 Madrid, Spain
[3]*Dahlem Center for Complex Quantum Systems*
Freie Universität Berlin, 14195 Berlin, Germany
[4]*Institute for Physics and Astronomy, Potsdam University, 14476 Potsdam, Germany*
[5]*Niels Bohr Institute, Blegdamsvej 17, 2100 Copenhagen, Denmark*
[6]*Zentrum Mathematik, Technische Universität München, 85748 Garching, Germany*

September 13, 2011

Abstract

Completely positive, trace preserving (CPT) maps and Lindblad master equations are both widely used to describe the dynamics of open quantum systems. The connection between these two descriptions is a classic topic in mathematical physics. One direction was solved by the now famous result due to Lindblad, Kossakowski Gorini and Sudarshan, who gave a complete characterisation of the master equations that generate completely positive semi-groups. However, the other direction has remained open: given a CPT map, is there a Lindblad master equation that generates it (and if so, can we find it's form)? This is sometimes known as the *Markovianity problem*. Physically, it is asking how one can deduce underlying physical processes from experimental observations.

We give a complexity theoretic answer to this problem: it is NP-hard. We also give an explicit algorithm that reduces the problem

*tcubitt@mat.ucm.es

to integer semi-definite programming, a well-known NP problem. Together, these results imply that resolving the question of which CPT maps can be generated by master equations is tantamount to solving P=NP: any efficiently computable criterion for Markovianity would imply P=NP; whereas a proof that P=NP would imply that our algorithm already gives an efficiently computable criterion. Thus, unless P does equal NP, there cannot exist any simple criterion for determining when a CPT map has a master equation description.

However, we also show that if the system dimension is fixed (relevant for current quantum process tomography experiments), then our algorithm scales efficiently in the required precision, allowing an underlying Lindblad master equation to be determined efficiently from even a single snapshot in this case.

Our work also leads to similar complexity-theoretic answers to a related long-standing open problem in probability theory.

Contents

1 Introduction

Noise abounds in quantum mechanical systems, so it's no surprise that the mathematics of open quantum systems permeates many areas of quantum theory. In quantum *information* theory, noisy evolution is usually modelled by completely positive, trace preserving (CPT) maps. CPT maps are often referred to as *quantum channels*, as they play the same role in quantum information theory as classical channels (stochastic maps) play in classical information theory: they give a discrete, black-box description of how input states are transformed into output states.

Just as in classical information theory, questions ranging from communication capacities to error-correction and fault-tolerant computation benefit from abstracting away the underlying physics in this way [1]. CPT maps also arise naturally in experimental measurement of quantum dynamics, when a complete "snapshot" of the dynamics is reconstructed via *quantum process tomography* [1]. The reconstructed snapshot is a CPT map describing how initial states are transformed by the evolution into states at the time of measurement.

Noisy evolution in other areas of quantum *physics*, on the other hand, is usually modelled by master equations. These directly describe the underlying physical processes governing the evolution, in the form of a differential equation for the time-evolution of the density matrix. They are frequently used to model realistic experimental set-ups, where external noise and dissipation must invariably be accounted for, especially in quantum optics [2] and condensed-matter physics [3].

In describing a noisy evolution by a master equation, there is an implicit assumption that the effect of the external environment on the system's evolution can be described in terms of the system's degrees of freedom alone. Given this assumption, the master equation must necessarily be *Markovian*. One justification for this is if the underlying physical processes are forgetful—as they commonly are to a good approximation. Conversely, if the Markovian assumption doesn't hold, then there is no way to decribe the evolution physically without enlarging the system being modelled to include (some of) the environment degrees of freedom.

Mathematically, a Markovian master equation generates a one-parameter (time t) semi-group (evolving for time t and then time s is equivalent to evolving for time $t + s$) of CPT maps (the evolution must be completely positive and trace preserving at all times if probabilities of measurement outcomes are to be positive and sum to one).

1.1 The Quantum Problem

The connection between these two descriptions of open quantum systems—the black-box, discrete-time description of CPT maps, and the continuous-time, physical description of master equations—is a classic topic in mathematical physics. Two questions naturally arise: given a master equation, does it generate a a completely positive evolution (and if so which CPT maps does it produce)? Conversely, given one or more CPT maps, is there an underlying Markovian master equation that generates them (and if so which one)? These questions can equivalently be stated more mathematically: given a linear operator, does it generate a completely positive semi-group? Conversely, given one or more CPT maps, are they members of a completely positive semi-group?

In seminal papers from the 1970's, Lindblad [4], Gorini, Kossakovski and Sudarshan [5] gave a complete answer to the first question (for finite dimensional systems*). They derived the general form—now known as the *Lindblad form*—for the generators of one-parameter completely positive semi-groups. Just as any discrete transformation of quantum states must be completely positive and trace-preserving if probabilities are to remain positive and normalised for any input state, a master equation *must* be of Lindblad form if it is to be physical, since an evolution that is not of this form will necessarily lead to negative probabilities.†

The converse question, however, has remained open. For the case of a single CPT map, we will refer to the problem of deciding whether it is a member of a completely positive semi-group as the *Markovianity problem*, since CPT maps that are generated by a Lindblad master equation are said to be *Markovian*.‡ The main result of this work is a complexity-theoretic answer to the Markovianity problem (which will be made more rigorous later):

---

*For subtleties invovled in finding the most general form of a generator in infinite-dimensional quantum systems, see Ref. [6].

†There exists a large literature on "non-Markovian master equations", which are not of Lindblad form. These can provide a useful phenomenological description of quantum evolution. But since they necessarily predict negative probabilities for some physical measurement outcomes, they are only valid for a restricted set of "allowed" initial states. If the system is prepared in a state outside of this allowed set, the non-Markovian master equation becomes invalid.

‡Note that this term is not used consistently throughout the literature. Here, we stick to the standard use of the term *Markovian* in the mathematical physics literature to mean the *time-homogeneous* Markovianity problem, in which the master equation is assumed to be time-independent. Sometimes, in particular in the context of condensed-matter physics, master equations are also referred to as being Markovian if they are of Lindblad form, but may be time-dependent. One could also adopt the established classical terminology and call the problem considered in this work the *quantum embedding problem*.

Theorem 1 *The Markovianity problem is NP-hard.*

Our proof easily extends to more general problems, such as deciding whether a family of CPT maps are members of the same completely positive semi-group, or computing any "measure" of Markovianity [7–12].

"Hardness" here is in the rigorous complexity-theoretic sense, which will be explained more precisely below. (See also Refs. [13, 14].) It concerns the scaling of computational effort as a function of the size of the problem, i.e. as a function of the total amount of information required to specify the CPT map. But a more refined analysis can break down the overall problem size here into two components: the dimension of the system, and the precision to which the CPT map is specified. We will analyse the complexity of the Markovianity problem with respect to both these parameters, and show that the NP-hardness is a consequence of scaling of the dimension.* We will also show—hinted at already in Ref. [7]—that for a *fixed* dimension, the Markovianity problem can be decided efficiently in the precision. Thus, though the problem in general is (very likely) intractable, in practical contexts arising in current quantum experiments, where the dimension is invariably small, the question of whether a given (family of) CPT map(s) is consistent with Markovian dynamics can be tested efficiently from even a single snapshot in time. We will give an explicit algorithm in this case, along with a careful analysis of its scaling:

Theorem 2 *For any fixed physical dimension the Markovianity problem can be solved in a run-time that scales polynomially (both in the number of digits to which the entries of the CPT map are specified, and the precision to which the answer should be given).*

Theorem 1 proves that deciding Markovianity is at least as hard as any problem in the complexity class NP. The algorithm of Theorem 2 reduces the problem to solving an integer semi-definite program, a problem that is contained in the class NP. Together, these results imply that:

Corollary 3 *Finding an efficiently computable criterion for Markovianity is equivalent to solving the (in)famous P=NP question; proving P=NP would imply the algorithm of Theorem 2 is efficient, whereas finding any efficiently computable criterion for Markovianity would prove P=NP.*

*Note that the relevant parameter here is the system dimension, not the number of qubits (the base-2 logarithm of the dimension), as the amount of information required to specify the CPT map—the problem size—scales with the (square of) the dimension. The time required to perform process tomography scales only polynomially in the dimension, so is efficient in this context.

1.2 The Classical Problem

The analogous questions can equally well be posed for *classical* dynamics. In fact, the resulting mathematical problems are even older and more extensively studied. The classical analogue of a CPT map is a stochastic map, which, in the context of information theory, also describes a classical communication channel. The classical analogue of a master equation is a continuous-time Markov chain, and the Markov-chain analogue of the Lindblad form can be found in any good text book on Markov processes (see e.g. Ref. [15]).

However, the converse question: given a stochastic map, can it be generated by a continuous-time Markov chain, has remained a thorny open problem in probability theory for over 70 years! It is known as the *embedding problem* for stochastic maps, and was first posed at least as long ago as 1937 by Elfving [16]. Though it has been the subject of investigation over the many intervening decades [17–19], the general embedding problem has remained open [20] until now.

Although there is a sense in which the classical embedding problem can be viewed as a special case of the quantum Markovianity problem, mathematically the two are inequivalent: a result concerning one does not necessarily imply anything about the other. However, it turns out that very similar techniques can be used to tackle both problems, allowing us to also show that:

Theorem 4 *The embedding problem is NP-hard.*

This finally resolves the long-standing embedding problem, in the sense that no efficiently computable (polynomial-time) criterion for embeddability can exist unless P=NP; the existence of any such efficiently computable criterion would imply P=NP. Rather than duplicating everything for the classical case, we will focus in this paper on the somewhat more complicated quantum problem, and then point out how the results can be adapted to the older classical embedding problem. A more detailed exposition of the classical result can be found in Ref. [21].

1.3 Implications for Physics

The Markovianity and embedding problems are not only of mathematical interest. They are also crucial problems in physics. What is the best possible measurement data that an experimentalist could conceivably gather about a system's dynamics? They could, for example, repeatedly prepare the system in any desired initial state, allow it to evolve for some period of time, and then perform any desired measurement. In fact, by choosing tomographically complete bases of initial states and measurements, and carrying out this procedure only a finite number of times, it is already possible to reconstruct a complete "snapshot" of the system dynamics at any particular time to arbitrary accuracy. In the quantum setting, this is *quantum process tomography* [1], but the general principle obviously applies equally well in the classical setting. Remarkably, thanks to the dramatic progress in experimental control and manipulation of quantum systems over recent years, this is no longer a theoretical pipe-dream even for quantum systems. Full quantum process tomography is now routinely carried out in many different physical systems, from NMR [8, 22–24] to trapped ions [25, 26], from photons [27, 28], to solid-state devices [29].

Each tomographic snapshot gives us a dynamical map, which tells us *everything* there is to know about the evolution at the time t when the snapshot was taken. If, on the time scale of observation, the discrete evolution is Markovian (i.e. doesn't depend on the history of its past) then the snapshot determines how any initial state of the system will evolve into a state at time t. This evolution is then described mathematically by a stochastic map in the classical setting and a CPT map in the quantum setting. In the quantum case, the indedepence from the history, which is equivalent to having an uncorrelated joint intial state of system and environment, can for instance be guaranteed if the tomographic scheme can be carried out with pure input states. This is certainly possible in principle, as we are assuming that the experimentalist has full control over the initial state of the system, and gives the best possible empirical description of the dynamics accessible by an experiment. The quantum process tomography experiments mentioned above [8, 22–29] have carried this out to a good degree of approximation in a variety of different physical systems.

Under this assumption, *all* physical properties of the system at time t are then fully determined by the tomographic snapshot. In the quantum case, the expectation value of *any* physical observable M is then given by Born's rule, whereas in the classical case it is given by a straight-forward average. Any physical measurement can therefore be viewed as an imperfect version of process tomography, since it gives partial information about the snapshot, and with sufficient measurement data the full snapshot can be reconstructed. Thus the most complete data that can be gathered about a system's dynamics consists of a set of snapshots, taken at different times during the evolution.

Given one or more snapshots, understanding the underlying physical processes typically amounts to reconstructing the system's dynamical equations and Liouvillian. If, over the time-scale of the experiment, the dynamics is described to good approximation by Markovian dynamics, then the dynamical equations take the form of a Lindblad master equation (in the quantum case) or a continuous-time Markov process (in the classical case). So to understand the physics underlying an experimental system, we must understand whether they can be described by a Markovian dynamics, and if so, what form the Markovian dynamical equations take. Clearly, if we can *find* a set of Markovian dynamical equations describing the dynamics whenever these exist (and there is no a priori way of knowing whether they exist or not), we can also determine *whether* they exist. So understanding the physics governing an experimental system implicitly involves solving the Markovianity or embedding problem (or their generalisations to a family of CPT or stochastic maps, in the case of multiple snapshots).

Thus the results of this work have a surprising implication for physics: no matter how much measurement data we might gather about the behaviour of a physical system, deducing its underlying Markovian dynamical equations—if the dynamics can be traced back to such a process—is fundamentally an intractable problem (assuming P≠NP). Indeed, already deciding whether or not the Markov approximation is a reasonable one given the experimental data is intractable. And this extends to various closely related physical problems, such as finding the dynamical equation that best approximates the data, or testing a dynamical model against experimental data.

Given their importance to physics, it is not surprising that numerous heuristic numerical techniques have been applied to tackle the Markovianity and embedding problems [8–12]. But these methods give no guarantee of finding the correct answer, or even any indication as to whether the correct answer has been found. One implication of the results of this work is that any such technique must necessarily fail in the general case (although for fixed physical problem dimension, they can of course prove valuable). The algorithm given in Section 5, which we prove is efficient for fixed dimension, improves on previous methods in that it guarantees to give the correct answer. It can also be extended to provide a similarly rigorous *measure* of the degree of Markovianity [7].

1.4 Outline

After introducing the necessary notation and recalling basic concepts in Section 2, Section 3 develops a careful and rigorous formulation of the Markovianity problem that will allow us to apply tools from complexity theory. Section 4 then gives a complexity-theoretic answer to the Markovianity problem: it is NP-hard. Technically, NP-hardness alone does not prove equivalence to P=NP; it could be that the Markovianity problem is *much* harder, so that even P=NP would not imply an efficient algorithm for Markovianity. Section 5 completes the proof of equivalence by giving an explicit algorithm that reduces the Markovianity problem to solving an NP-complete problem. We give a careful analysis of the complexity of this algorithm, thereby providing an explicit algorithmic solution to the Markovianity problem which would be efficient if P=NP. Indeed, we show that if the dimension is fixed, the algorithm scales polynomially in the precision. In Section 6 we briefly explain how these proofs can be adapted to show that the classical embedding problem, too, is NP-hard (a fuller version appears in Ref. [21]). Finally, Section 7 concludes with a discussion of consequences of these results.

As the full NP-hardness proof described in Sections 3 and 4 is somewhat involved, we give here an overview of the general structure of the argument, as an aid to navigating the details of the proof. The proof proceeds by defining a number of computational problems and proving a sequence of complexity-theoretic relationships between them, starting from the Markovianity problem itself, and ending with the NP-complete problem 1-in-3SAT. The computational problems defined in the proof, and the relationships we will establish between them, are illustrated in Fig. 1.

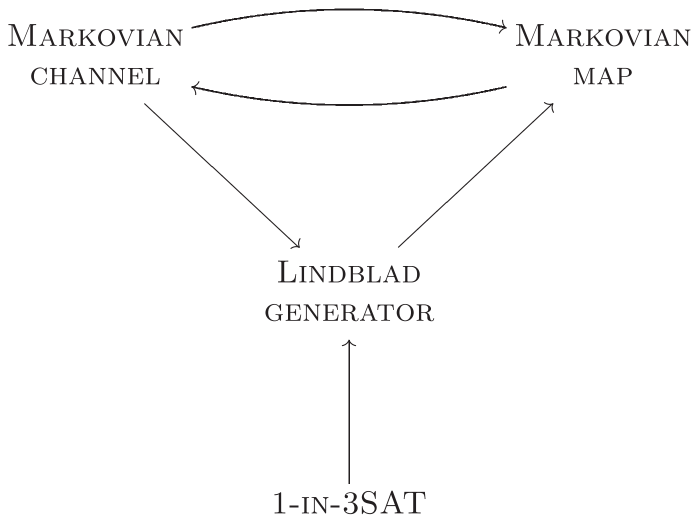


Figure 1: Computational problems defined in the proof, along with the complexity-theoretic reductions between them. Since 1-in-3SAT is NP-complete, taken together this sequence of reductions proves NP-hardness of the Markovianity problem.

Just as the dynamics of a closed quantum system governed by a Hamiltonian H is described formally by a unitary semi-group $U_t = e^{Ht}$ obtained by exponentiation, the dynamics of an open quantum system governed by a Liouvillian L of Lindblad form is described formally by a completely-positive semi-group $E_t = e^{Lt}$ obtained by exponentiation of the Liouvillian. However, unlike unitary dynamics, not every completely-positive map can be generated by a Lindblad master equation. The Markovianity problem is precisely the question of determining whether a given CPT map E *is* generated by some Lindblad master equation or not. In Section 3, we formulate this question rigorously as the computational problem MARKOVIAN CHANNEL. This is the first of our computational problems, and the one we are seeking to prove is NP-hard.

It turns out to be helpful for the proof to define another variant of this computational problem, called MARKOVIAN MAP, in which the map that we are given is not necessarily CPT. The first step in the proof is to show that these two problems, MARKOVIAN CHANNEL and MARKOVIAN MAP, are computationally equivalent; i.e. MARKOVIAN MAP can be reduced to MARKOVIAN CHANNEL (the reduction in the opposite direction is trivial, since MARKOVIAN CHANNEL is just a special case of MARKOVIAN MAP). This is not difficult, and we do so at the end of Section 3.1. This proves the first (and simplest) of the complexity-theoretic relationships illustrated in Fig. 1.

For the finite-dimensional systems with which we are concerned, the Liouvillian L is given by a finte-dimensional matrix, and the exponentiation $E_t = e^{Lt}$ is the standard matrix exponential. By inverting this relationship e.g. for $t = 1$, we obtain an expression for the Liouvillian $L = \log E_1$ in terms of the matrix logarithm. In this way, the Markovianity problem for CPT map E becomes one of determining whether $L = \log E$ is of Lindblad form. In Section 3.2, we show that there is a simple and computationally efficient algorithm for determining whether a given matrix L is of Lindblad form. The difficulty lies in the fact that the logarithm $\log E$ is not uniquely defined. Just as there are infinitely many logarithms $\log r + i\phi + 2\pi i n$ of a complex number $z = re^{i\phi}$, parameterised by an integer $n \in \mathbb{Z}$, there are infinitely many branches of the matrix logarithm, parameterised now by a vector of integers. Thus to solve the Markovianity problem for a map E, we must check whether *any one* of the infinitely many possible logarithms are of Lindblad form. In Section 3.2, we formulate this rigorously as the computational LINDBLAD GENERATOR.

It is worth pausing at this point to note that, already here, we see a hint as to why the Markovianity problem might be NP-hard. In terms of the Liouvillian, the problem is one of checking whether any element of a set parameterised by integers (the possible logarithms) has a particular property (the Lindblad form). There are of course many exceptions, but it is often the case that integer problems such as this are NP-hard. For example, linear programming problems can be solved efficiently, but *integer* linear programming is NP-complete. Indeed, it is trivial to express NP-complete satisfiability problems such as 3SAT as integer linear programs. Though the construction is significantly more complicated, the same idea lies behind our NP-hardness proof for the LINDBLAD GENERATOR problem.

The remainder of Section 3.2 is taken up with proving that the LINDBLAD GENERATOR problem is computationally equivalent to MARKOVIAN CHANNEL. In fact, we first prove that LINDBLAD GENERATOR can be reduced to MARKOVIAN MAP, implying that MARKOVIAN MAP is computationally least as difficult as LINDBLAD GENERATOR. Then we prove a reduction from MARKOVIAN CHANNEL to LINDBLAD GENERATOR, implying that LINDBLAD GENERATOR is computationally at least as hard as MARKOVIAN MAP. Since we have already seen that MARKOVIAN CHANNEL and MARKOVIAN MAP are computationally equivalent, this implies equivalence of all three problems. This is illustrated in Fig. 1.

Having proven that the Markovianity problems are equivalent to the LINDBLAD GENERATOR problem, the final stage is to prove NP-hardness of the latter. We do this in Section 4 by proving a reduction from a well-known NP-complete problem 1-IN-3SAT (a close cousin of the more famous 3SAT problem), implying that the LINDBLAD GENERATOR problem is at least as hard as 1-IN-3SAT. By the sequence of relationships already proven between LINDBLAD GENERATOR and MARKOVIAN CHANNEL, this implies NP-hardness of the Markovianity problem. The complete sequence of relationships is illustrated in Fig. 1.

2 Preliminaries

In what follows, we will restrict our attention to finite-dimensional spaces and maps. It will be convenient to choose a concrete representation for the CPT maps. Since a CPT map $\mathcal{E}$ is a linear map on the d^2–dimensional vector space $\mathcal{M}_d$ of operators on a d–dimensional Hilbert space $\mathcal{H}$, it can be represented by a $d^2 \times d^2$–dimensional matrix E in the usual way. More explicitly, if we reshape the density matrix ρ as a vector $\|\rho\rangle$ with elements $\langle i,j\|\rho\rangle = \rho_{i,j}$ in some orthonormal basis, E has matrix elements

$$E_{(i,j),(k,l)} = \langle i,j\|\mathcal{E}(|k\rangle\langle l|)\rangle. \tag{1}$$

The action of the channel $\mathcal{E}$ is then given by matrix multiplication, $\|\mathcal{E}(\rho)\rangle = E\|\rho\rangle$, and the composition $\mathcal{E}_1 \circ \mathcal{E}_2$ of two channels $\mathcal{E}_1$ and $\mathcal{E}_2$ is given in this linear operator representation by the matrix product E_1E_2.

The matrix E is also closely related to the more familiar Choi-Jamiołkowski state representation [30, 31], given by the state $\sigma = (\mathcal{E} \otimes \mathcal{I})(\omega)$ obtained by applying the channel to one half of the (unnormalised) maximally entangled state $\omega = \sum_{i,j} |i,i\rangle\langle j,j|$, defined in some fixed orthonormal product basis of $\mathcal{M}_d \otimes \mathcal{M}_d$ ($\mathcal{I}$ being the identity map). Define the involution Γ by its action on this basis,

$$|i,j\rangle\langle k,l|^\Gamma = |i,k\rangle\langle j,l| \,. \tag{2}$$

The Choi-Jamiołkowski and linear operator representations of $\mathcal{E}$ are then related by $E = \sigma^\Gamma$.

Completely positive semi-groups of CPT maps $\mathcal{E}_t$ arise naturally as solutions of a Markovian quantum *master equation* describing the dynamics of the density matrix ρ (indeed, the continuous semi-group structure is essentially the *only* possible one if we require the evolution to be describable at any time $t \geq 0$ [32, 33]):

$$\frac{\mathrm{d}\rho}{\mathrm{d}t} = \mathcal{L}(\rho), \tag{3}$$

where $\mathcal{L}$ is the system's Liouvillian. If the solutions $\rho(t) = \mathcal{E}_t(\rho(0))$ are to be completely positive for all $t \geq 0$, then the Liouvillian $\mathcal{L}$ must be of Lindblad form [4, 5]:

$$\frac{\mathrm{d}\rho}{\mathrm{d}t} = \mathcal{L}(\rho) = i[\rho, H] + \sum_{\alpha,\beta} G_{\alpha,\beta}\Big(F_\alpha \rho F_\beta^\dagger - \frac{1}{2}\{F_\beta^\dagger F_\alpha, \rho\}_+\Big). \tag{4}$$

Here, H is Hermitian, and can be interpreted as the Hamiltonian of the system, $G \geq 0$ and $\{F_\alpha\}$ describe the decoherence processes, and $\{A, B\}_+ = AB + BA$ denotes the anti-commutator. A *Markovian* channel is one that is a member of such a semi-group, i.e. one that is generated by some $\mathcal{L}$ of the above form.

It will again be convenient to represent the generator $\mathcal{L}$ by a matrix, in the same way as for the channels. In the linear operator representation, a Markovian channel $E = e^L$ is one with a generator L such that e^{Lt} is CPT for all $t \geq 0$. Note that we can without loss of generality rescale time such that E is generated by L at time $t = 1$. The fact that the generator and channel are related by standard matrix exponentiation in the linear operator representation makes this representation particularly convenient for our purposes. It is not difficult to translate Eq. (4) into conditions on L (see Section 3.2 or Ref. [7]).

The classical case is analogous. A stochastic map on a finite d–dimensional state space is represented by a $d \times d$–dimensional stochastic matrix P, which acts on d–dimensional probability vectors $\mathbf{p}$. An *embeddable* stochastic matrix $P = e^Q$ is then one with a generator Q such that e^{Qt} is stochastic for all $t \geq 0$, i.e. Q defines a continuous-time Markov chain. The conditions on Q

analogous to the Lindblad form of Eq. (4) (or, more precisely, to Lemma 8) are given by [15]:

(i). $Q_{i\neq j} \geq 0$,

(ii). $\sum_i Q_{i,j} = 0$.

For consistency with the quantum notation, we are adopting the convention that probability distributions are *column* vectors, and maps act on them to the right. Thus the normalisation condition applies to the column-sums rather than the row-sums. Note, however, that this runs counter to the convention in the probability theory literature of representing probability distributions by row-vectors.

We will also make use of some basic concepts from complexity theory. (See e.g. Refs. [13, 14] for an introduction to this field.) Complexity theory is concerned with how the computational resources (typically time or space) required to solve a problem scale with the problem size, where the size of a computational problem is the amount of information required to specify the problem. The most important complexity classes are defined for decision problems: problems with "yes" or "no" answers. For example, the complexity class P is defined as the class of all decision problems that can be solved on a classical computer in a time that scales as a polynomial of the problem size. We say that such problems can be solved in *polynomial time*, or *efficiently*. The notorious complexity class NP is defined as the class of all decision problems for which, if the answer is "yes", there exists a proof that can be *verified* in polynomial time. Clearly, any problem in P is also in NP. It is widely believed that P is a strict subset of NP; this is the famous P versus NP problem, which remains open to this day. A classic example of an NP problem that is not known to be in P is the satisfiability problem: deciding whether there exists an assignment of truth values to a set of boolean variables for which a given boolean expression evaluates to "true". Finding such an assignment may be difficult, but if such an assignment exists, then there clearly exists a proof of this fact which can be evaluated efficiently: namely, the list of truth assignments itself.

We say that a decision problem A can be *reduced* to a decision problem B if there exists an algorithm that transforms any instance of A into an instance of B, such that the answer to this B instance gives the answer to the orignal A instance. To give a meaningful hierarchy of complexity classes, the computational resources allowed in the reduction must be restricted in some way. For the complexity class NP, the appropriate reductions are *polynomial-time reductions.* * If A has a polynomial-time reduction to B, then B is in

*Strictly speaking, what we have described here is polynomial-time many-to-one reduca well-defined sense "harder" than A, since an efficient algorithm for solving B would also give an efficient algorithm for A. Reduction defines a partial order on computational problems, and we will write $A \leq B$ when A has a polynomial-time reduction to B. A problem A is called *NP-hard* if every problem in NP has a polynomial-time reduction to A. An NP-hard problem that is also contained in NP is called *NP-complete*. NP-complete problems are, in the above sense, the hardest problems in NP.

3 The Quantum Problem

3.1 The Computational Markovianity Problem

In order to apply tools from complexity theory to study the Markovianity problem, we will need to define the problem in such a way that the problem size—the amount of information needed to specify an instance of the problem—is well-defined. Even in the finite-dimensional case, this requires a little care. Since CPT maps form a continuous set, there may exist Markovian and non-Markovian channels that are arbitrarily close (in any distance measure). Thus, to guarantee an unambiguous answer in all cases, the channel would need to be specified to infinite precision.

There are essentially two standard ways of dealing with this in complexity theory. But, before we do so, it is instructive to first take a step back and recall some of physical motivation for the problem. In measuring a tomographic snapshot of a system's dynamics, there will always be some experimental error, and it makes little sense to require an answer that is more precise than this error. Mathematically, this suggests that we should consider the Markovianity problem solved if we can answer the question for some map that is a sufficiently close approximation to the one we were given.

This is the intuitive idea behind the following *weak-membership* formulation of the Markovianity problem (cf. Ref. [34], which uses a weak-membership formulation of the separability problem):

Problem 5 (MARKOVIAN CHANNEL)
Instance: *(E, ε): CPT map E, precision $\varepsilon \geq 0$.*
Question: *Assert either that:*

- *for some map E' with $\|E' - E\| \leq \varepsilon$, there exists a map L' such that $E' = e^{L'}$ and $e^{L't}$ is CPT for all $t \geq 0$;*

tion, or *Karp reduction*, the strongest form of reduction. This is the type of reduction used to define NP-hardness, and is the only form of reduction with which we will be concerned in this paper.

- *for some CPT map E' with $\|E' - E\| \leq \varepsilon$, no such L' exists.*

Here, we do not specify the matrix norm $\|.\|$ in the problem definition. However, given the equivalence of norms on finite-dimensional spaces, with at most a polynomial prefactor in the dimension relating one norm to the other, we can leave the choice of norm open for now. Again, we can always without loss of generality scale time such that, if a suitable L' exists, E' is generated by L' at time $t = 1$.

Note that, if E is close to the boundary of the set of Markovian channels, then it will be close to both Markovian and non-Markovian maps, and both assertions will be valid simultaneously. The physical interpretation in such a case would simply be that the snapshot was not measured to sufficient precision to allow an unambiguous answer. (There are other ways to formulate weak-membership problems, but they are essentially equivalent [35].) The other standard approach would be to restrict E to have rational entries, but this is less natural in the present context.

Because there are cases in which both answers may be valid, the weak-membership formulation of MARKOVIAN CHANNEL is not formally a decision problem. This by definition rules it out of the decision class NP, where it by rights belongs. Whilst it is possible to reformulate it as a decision problem, we will avoid getting bogged down in these complexity theoretic technicalities here, and accept that MARKOVIAN CHANNEL is not in NP. (In fact, the appropriate complexity class for weak membership problems is known as promise-NP, which is like NP but with an additional promise that the problem instance will never be in some set. The results of Section 5 show that the Markovianity problem is indeed in promise-NP, which, together with the NP-hardness result, implies that it is promise-NP-complete. See Ref. [35] for a discussion of similar issues in the context of the separability problem.)

MARKOVIAN CHANNEL carries the implicit promise that E is a CPT map. It is natural to ask whether this affects the complexity of the problem. After all, if a tomographic snapshot is measured experimentally, it is very unlikely to be either precisely trace-preserving or completely positive. This motivates the definition of the following variant of the Markovianity problem, which accounts for non-CPT maps E:

Problem 6 (MARKOVIAN MAP)
Instance: $(E, \varepsilon, \varepsilon')$*: Map E, precision parameters $\varepsilon > \varepsilon' > 0$.*
Question: *Assert either that:*

- *for some map E' with $\|E' - E\| \leq \varepsilon$, there exists a map L' such that $E' = e^{L'}$ and $e^{L't}$ is CPT for all $t \geq 0$;*

- *for some CPT map E' with $\|E' - E\| \leq \varepsilon$, no such L' exists;*
- *no CPT map E' exists for which $\|E' - E\| \leq \varepsilon'$.*

It is not difficult to see that the two problems, Markovian channel and Markovian map, are in fact equivalent. Clearly, Markovian channel is a special case of Markovian map, in which the third assertion is always false (E itself fulfils the requirements of one or other of the first two assertions). Conversely, complete-positivity of a map E is equivalent to positivity of the Choi-Jamiołkowski matrix $\rho = E^\Gamma$, and E is trace-preserving iff the partial trace of ρ is the identity matrix. So finding the closest CPT map E' to E is equivalent to finding the closest positive-semi-definite, suitable matrix ρ' to ρ. Indeed, if we fix the norm in Markovian map to be the Frobenius norm* $\|A\|_{\mathrm{F}} := (\sum_{i,j} A_{i,j}^2)^{1/2}$, then not only do we have $\|E' - E\|_{\mathrm{F}} = \|\rho' - \rho\|_{\mathrm{F}}$, but also, if we minimise $\|\rho' - \rho\|_{\mathrm{F}}^2$ subject to the above semi-definite constraints, the objective function becomes a convex quadratic form. The problem can therefore be transformed into a semi-definite program using standard techniques [36], allowing it to be solved efficiently to give E' and $\|E' - E\|_{\mathrm{F}}$. (More precisely, we can compute a bound on $\|E' - E\|_{\mathrm{F}}$ that can be made exponentially tight with only polynomial overhead.) Thus, either we will conclude that the third assertion is valid, or we will succeed in transforming the problem into a Markovian channel instance. This proves the following complexity-theoretic (Karp) equivalence†:

Theorem 7 *Markovian map = Markovian channel.*

3.2 The Computational Lindblad Generator Problem

It is not immediately clear how one would go about solving a Markovian channel or Markovian map instance. In order to answer this, we will need to establish certain properties of the generators L of Markovian maps $E = e^{Lt}$. We will call such L *Lindblad generators*. The following Lemma is taken directly from Ref. [7], which in turn is a slight modification of the argument given in Ref. [4], and gives an efficient criterion for deciding whether

*The Frobenius norm is convenient for two reasons: firstly, the square of the norm-distance $\|A - B\|_{\mathrm{F}}^2$ is strictly convex; secondly, it is invariant under permutation of matrix elements, in particular $\|A^\Gamma\|_{\mathrm{F}} = \|A\|_{\mathrm{F}}$.

†Throughout this paper, we will only consider Karp-reductions—i.e. polynomial-time reductions which transform one problem directly into a single instance of another—and Karp-equivalence. These are the strongest forms of reduction and equivalence, and are the ones used to define NP-hardness.

or not L generates a one-parameter CPT semi-group, i.e. whether it is of Lindblad form.

Lemma 8 *A map L is a Lindblad generator iff all of the following hold:*

(i). L^Γ *is Hermitian.*

(ii). *L fulfils the normalisation $\langle\omega|\, L = 0$, where the maximally entangled state vector $|\omega\rangle = \sum_i |i,i\rangle/\sqrt{d}$ is expressed in the same basis in which the involution Γ is defined.*

(iii). *L satisfies*

$$(\mathbb{1}\| - \|\omega)L^\Gamma(\mathbb{1} - \omega) \geq 0 \tag{5}$$

where $\omega = |\omega\rangle\langle\omega|$.

Maps L^Γ satisfying Eq. (5) are called *conditionally completely positive* (ccp).

We can assume without loss of generality that the matrix E in a Markovian map or Markovian channel instance is diagonalisable (with respect to similarity transforms), non-degenerate, and full-rank. (Such matrices are dense in the set of all matrices, so we can always replace E with a neighbouring map that has these properties, and decrease ε (keeping ε' fixed in the case of Markovian map) such that the outcome is unchanged.) The Jordan decomposition of a diagonalisable channel has the form

$$E = \sum_r \lambda_r\, |r_r\rangle\langle l_r| + \sum_c \lambda_c\, |r_c\rangle\langle l_c| + \bar{\lambda}_c\, \mathbb{F}(|r_c\rangle\langle l_c|). \tag{6}$$

where r labels the real eigenvalues, c the complex ones, and $|r_k\rangle\langle l_k|$ are orthonormal (but typically not self-adjoint) spectral projectors formed from the left and right eigenvectors $\langle l_k|$ and $|r_k\rangle$ of E associated with the same eigenvalue λ_k. The fact that the eigenvalues come in conjugate pairs and that the corresponding spectral projectors are related via the "flip" operation,

$$\mathbb{F}\Big(\sum_{i,j} c_{i,j}\, |i,j\rangle\Big) = \sum_{i,j} \bar{c}_{i,j}\, |i,j\rangle \tag{7}$$

extended to operators as

$$\mathbb{F}\Big(\sum_{(i,j),(k,l)} c_{(i,j),(k,l)}\, |i,j\rangle\, \langle k,l|\Big) = \sum_{(i,j),(k,l)} c_{(i,j),(k,l)}\, |j,i\rangle\, \langle k,l|\,, \tag{8}$$

is a straightforward consequence of Hermiticity of CPT maps. It is easy to show that all CPT maps are necessarily Hermitian.

Inverting the relationship $E = e^L$, we obtain a generator $L = \log E$ from any channel E, where the matrix logarithm is defined via the logarithm of the eigenvalues. Of course, the logarithm is not unique. It has a countable infinity of branches, since the phase of each eigenvalue is only determined modulo 2π. E is Markovian iff there exists *some* branch of the logarithm that has Lindblad form, i.e. that satisfies Lemma 8. So, to check if a channel is Markovian, we must check whether *any* branch of its logarithm has Lindblad form.

Some of the branches can be ruled out immediately, using the condition that Lindblad generators must also be Hermitian maps (Condition (i) from Lemma 8), which imposes that eigenvalues come in conjugate pairs. The remaining set of possible Lindblad generators for E can be parametrised by

$$L_m := \log E = L_0 + 2\pi i \sum_c m_c\big(\,|l_c\rangle\langle r_c| - \mathbb{F}(|l_c\rangle\langle r_c|)\big) = L_0 + \sum_c m_c A_c, \quad (9)$$

where L_0 is any fixed branch of the logarithm, e.g. the principle branch (defined by taking the principle branch in the logarithm of each eigenvalue), and each branch is characterised by a set of at most $d^2/2$ integers m_c (one for each pair of complex eigenvalues). We introduce the matrices A_c, defined by

$$A_c := 2\pi i\big(|l_c\rangle\langle r_c| - \mathbb{F}(|l_c\rangle\langle r_c|)\big) \quad (10)$$

for notational convenience.

The A_c are fully determined by L_0, or, equivalently, by E. The following lemma summarises those properties of A_c and L_0 that are easy to check, and follows immediately from the first two conditions of Lemma 8 and Eqs. (9) and (10):

Lemma 9 *If $L_m = L_0 + \sum_c m_c A_c$ parametrise the logarithms of a CPT map E as in Eq.* (9)*, then L_0 and A_c necessarily satisfy the following properties:*

(i). *L_0 and A_c are simultaneously diagonalisable.*

(ii). *A_c are mutually orthogonal, rank-2 matrices with non-zero eigenvalues $\pm 2\pi i$.*

(iii). *L_0 and A_c satisfy the normalisation $\langle\omega|\,L_0 = \langle\omega|\,A_c = 0$.*

(iv). *The two eigenvalues of L_0 corresponding to the non-zero eigenvalues of any A_c form a conjugate pair.*

(v). *The right and left eigenvectors $|r_{1,2}\rangle$ and $\langle l_{1,2}|$ associated with a conjugate pair of eigenvalues are related by $|r_2\rangle = \mathbb{F}(|r_1\rangle)$ and $\langle l_2| = \mathbb{F}(\langle l_1|)$.*

The last two properties of pairs of eigenvalues and eigenvectors can be stated more concisely as:

(iv') L_0^Γ and A_c^Γ are Hermitian matrices.

Together with the ccp condition of Lemma 8,

$$(\mathbb{1}-\omega)L_0^\Gamma(\mathbb{1}-\omega)+\sum_c m_c(\mathbb{1}-\omega)A_c^\Gamma(\mathbb{1}-\omega)\geq 0, \tag{11}$$

this gives a criterion for deciding whether $L_m = L_0 + \sum_c m_c A_c$ generates a CPT semi-group. Note that it is possible for L_m to be ccp even if L_0 is not.

The characterisation of Lindblad generators in Lemma 8 motivates the definition of a new weak-membership problem:

Problem 10 (LINDBLAD GENERATOR)
Instance: *(L_0, δ): Map L_0, precision δ.*
Promise: *There exists a map L_0' with $\|L_0 - L_0'\| \leq f(\delta)$ such that $e^{L_0'}$ is a quantum channel. ($f(\delta)$ is a strictly increasing function of δ which will be specified later.)*
Question: *Assert either that:*

- *for some map L_0' with $\|L_0' - L_0\| \leq \delta$, there exists a set of integers $\{m_c\}$ such that L_m' as defined in Eq. (9) satisfies Lemma 8;*
- *for some map L_0' where $e^{L_0'}$ is a quantum channel and $\|L_0' - L_0\| \leq \delta$, no such L_m' exists.*

The bound $f(\delta)$ in the promise will be a somewhat complicated monotonically increasing function of δ whose definition we defer until later (see Theorem 16), when it will make more sense. But, essentially, the promise guarantees that L_0 is close to the generator of *some* CPT map. This definition of LINDBLAD GENERATOR might appear somewhat arbitrary. And indeed it would be, were we interested in the problem of deciding Lindblad form per se. (In that case, it would make more sense to replace the promise by an extra assertion, analogous to the third assertion of MARKOVIAN MAP.) But we will only use LINDBLAD GENERATOR as a stepping-stone to results concerning MARKOVIAN CHANNEL and MARKOVIAN MAP, and the above definition fulfils this purpose. In a slight abuse of terminology, we will also refer to maps L_0 for which there exists an L_m satisfying Lemma 8 as *Lindblad generators*, even if L_0 itself is not of Lindblad form.

The preceding discussion suggests that LINDBLAD GENERATOR and MARKOVIAN MAP are equivalent. Clearly, the map $E = e^{L_0}$ is Markovian iff there exists at least one L_m satisfying Lemma 8. However, a little care is required in order to show that the reductions in both directions can be performed efficiently. In particular, we must show that appropriate precision parameters ε and δ can be computed efficiently, as well as accounting for the fact that the exponential and logarithm can not be computed to infinite precision. This will require strong continuity properties of the matrix exponential and logarithm, and whilst these are easily established in the case of the exponential, they are somewhat more complicated to establish for the logarithm.

A proof of Lipschitz continuity of the exponential can be found in standard texts (see e.g. Ref. [37, Corollary 6.2.32]).

Lemma 11 *For any matrices A and B and any matrix norm $\|.\|$*

$$\left\|e^A - e^B\right\| \le \exp(\|A\|)\exp(\|A-B\|)\,\|A-B\|\,. \tag{12}$$

For the logarithm, we will need the following definition and theorems from Refs. [38] and [39].

Definition 12 *For closed linear operators A, B on a Banach space, define*

$$d(A,B) = \max[\delta(A,B), \delta(B,A)], \tag{13}$$

$$\delta_1(A,B) = \sup_{0<\lambda\le 1} \delta(\lambda A, \lambda B), \tag{14}$$

$$d_1(A,B) = \max[\delta_1(A,B), \delta_1(B,A)], \tag{15}$$

(taken directly from Refs. [38, 39], following the notation of Ref. [39]). $\delta(A,B)$ is Kato's δ measure [38, IV.§2.4].[*]

Note that none of these measures obey the triangle inequality, so none are proper distance measures (though they can readily be turned into such; see Ref. [38, IV.§2.2,2.4]). The following theorem shows that, on bounded operators, the topology generated by δ is equivalent to the norm topology of the Banach space (see [38, §IV, Theorems 2.13 and 2.14]).

[*]The distance-like measure d (which Kato calls $\hat{\delta}$) goes variously by the names "gap", "aperture" or "opening". Here,

$$\delta(A,B) = \sup_x \operatorname{dist}((\mathbf{x}, A\mathbf{x}), G(B)), \tag{16}$$

where $G(B)$ is the graph of B, and the supremum is taken over all $\mathbf{x}$ in the domain of A, normalised such that $\|\mathbf{x}^2\| + \|A\mathbf{x}\|^2 = 1$. This distance-like measure generates the correspondingly named topology. This topology can equivalently be defined as the standard graph topology on the graphs of the operators.

Theorem 13 *If A and B are bounded operators on a Banach space with norm $\|.\|$, then*

$$d(A, B) \leq \|A - B\| \tag{17}$$

and, if in addition $d(A, B) < (1 + \|A\|^2)^{1/2}$,

$$\|A - B\| \leq \frac{(1 + \|A\|^2)\delta(A, B)}{1 - (1 + \|A\|^2)^{1/2}\delta(A, B)}. \tag{18}$$

Continuity of the logarithm can now be stated in terms of the distance-like measures of Definition 12 (see [39, Theorem 3.1]).

Theorem 14 *If $A, B \in \mathscr{P}_1(M)$ are operators on a Banach space with norm $\|.\|$, then for $M > 0$*

$$d_1(\log A, \log B) \leq 134(1 + M^2)\delta_1(A, B), \tag{19}$$

where $\mathscr{D} = \{A \mid \operatorname{dom} A \text{ dense}\}$ and

$$\mathscr{P}_1(M) = \{A \in \mathscr{D} \mid \lambda \in \rho(A) \text{ and } (1 - \lambda)\,\|R(\lambda, A)\| \leq M \text{ for } \lambda \leq 0\} \tag{20}$$

are subsets of operators on the Banach space, $R(\lambda, A)$ is the resolvent of A, and $\rho(A)$ its resolvent set.

For the case of finite-dimensional Hilbert spaces that we are concerned with here, $\mathscr{P}_1(M)$ becomes the set of complex matrices whose eigenvalues do *not* lie on or close to the negative real axis. This amounts to taking the branch-cut of the logarithm to be along that axis. (Since this rules out zero eigenvalues, these matrices are also necessarily non-singular.)

Because we defined our computational problems in terms of norm-distance, rather than the distance-like measures of Definition 12, we need to transform Theorem 14 into a statement about norm-distance.

Corollary 15 *If A, B are bounded operators on a Banach space with norm $\|.\|$, and if $kA, kB \in \mathscr{P}_1(M)$ with*

$$k = \min\left[1, \left(134^2(1 + M)^2\|A - B\|^2 - \|A\|^2\right)^{1/2}\right], \tag{21}$$

then

$$\begin{aligned} &\|\log A - \log B\| \\ &\leq 134k(1 + M^2)\left(1 + k\|A\| + k\|A - B\|(1 + k^2\|A\|^2)^{1/2}\right)\|A - B\|. \end{aligned} \tag{22}$$

Proof Assume first that $d(\log A, \log B) < (1 + \|\log A\|^2)^{1/2}$, so that the condition of Theorem 13 holds and Eq. (18) is valid. From Definition 12, and rearranging Eq. (18), we have

$$\begin{aligned} d_1(\log A, \log B) &\geq \delta_1(\log B, \log A) = \sup_{0<\lambda\leq 1} \delta(\lambda \log B, \lambda \log A) \\ &\geq \delta(\log B, \log A) \geq \frac{\|\log A - \log B\|}{1 + \|A\| + \|A - B\| \, (1 + \|A\|^2)^{1/2}} \end{aligned} \tag{23}$$

and

$$\begin{aligned} \delta_1(A, B) &= \sup_{0<\lambda\leq 1} \delta(\lambda A, \lambda B) \leq \sup_{0<\lambda\leq 1} d(\lambda A, \lambda B) \\ &\leq \sup_{0<\lambda\leq 1} \|\lambda A - \lambda B\| = \|A - B\| \,. \end{aligned} \tag{24}$$

Using these inequalities in Theorem 14 gives Eq. (22) of the Corollary with $k = 1$, under the assumption that $d(\log A, \log B)$ obeys the condition of Theorem 14.

Otherwise, we can rescale A and B until they do obey the condition. Let

$$0 < k < \left(134^2(1 + M^2)^2 \|A - B\|^2 - \|A\|^2\right)^{-1/2}. \tag{25}$$

Then, using Eq. (24) and Theorem 14,

$$\begin{aligned} d\big(\log(kA), \log(kB)\big) &\leq d_1\big(\log(kA), \log(kB)\big) \leq 134(1 + M^2)\delta_1(kA, kB) \\ &\leq 134|k|(1 + M^2)\|A - B\| < (1 + |k|^2\|A\|^2)^{1/2} \\ &= (1 + \|kA\|^2)^{1/2}, \end{aligned}$$

so $d\big(\log(kA), \log(kB)\big)$ does satisfy the condition of Theorem 14, and by the preceding argument Eq. (22) applies to $\|\log(kA) - \log(kB)\|$. But

$$\begin{aligned} \|\log(kA) - \log(kB)\| &= \|\log A + \log(k\mathbb{1}) - \log B - \log(k\mathbb{1})\| \\ &= \|\log A - \log B\|, \end{aligned} \tag{26}$$

which completes the proof. □

Note that if A or B happens to have an eigenvalue on the negative real axis, we can always rotate the branch-cut, or equivalently the eigenvalues. Multiplying by a scalar root of unity z rotates the eigenvalues away from the real axis, without changing the bound in Corollary 15: $\|\log(zA) - \log(zB)\| = \|\log A - \log B\|$, but $\|zA - zB\| = \|A - B\|$.

We are now in a position to prove the main results of this section.

Theorem 16 Markovian map $\geq$ Lindblad generator.

Proof Assume first that we are given an instance (L_0, δ) of Lindblad generator that is unambiguous, i.e. either all neighbouring generators of channels are Lindblad generators, or none are. In that case we know that one or other of the assertions is valid, but not both. Now, using Corollary 15, we can calculate (efficiently) an ε such that for $\log E = L_0$, $\log E' = L_0'$, and $\|E - E'\| \leq \varepsilon$, we have $\|\log E - \log E'\| \leq \delta$. (Indeed, it is not difficult to solve Eq. (22) for ε and obtain an explicit expression.) Then the pre-image of an ε-ball around $E = e^{L_0}$ is contained within the δ-ball around L_0 (as illustrated in Fig. 2). Since a map $E' = e^{L_0'}$ is Markovian iff L_0' is a Lindblad generator, and we are assuming the Lindblad generator instance is unambiguous, any channels within this ε-ball must either all be Markovian or all be non-Markovian.

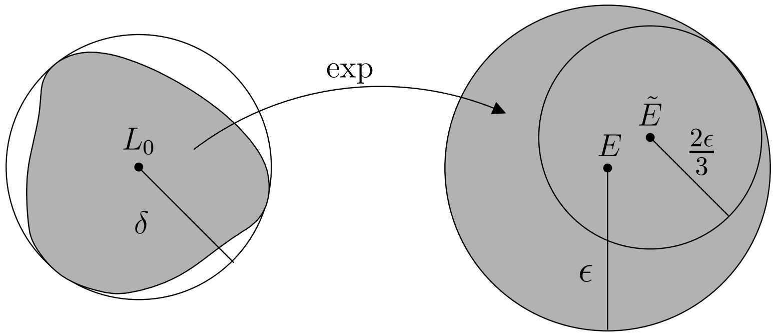


Figure 2: The pre-image of an ε-ball around $E = e^{L_0}$ is contained within a δ-ball around L_0. If $\tilde{E}$ is within $\varepsilon/3$ of E, then everything within a $2\varepsilon/3$-ball around $\tilde{E}$ is within the ε-ball around E.

To deal with the fact that $E = e^{L_0}$ can not be calculated to infinite precision, let $\tilde{E}$ be the exponential of L_0 calculated to within precision $\varepsilon/3$ (which can be done efficiently [40]); i.e. $\|\tilde{E} - E\| \leq \varepsilon/3$. If E' is within a $2\varepsilon/3$-ball around $\tilde{E}$, we have $\|E' - E\| \leq \varepsilon$. Therefore, assuming for the moment that there exists some channel within this ball (i.e. assuming its third assertion is *not* valid), the Markovian map instance $(\tilde{E}, 2\varepsilon/3, \varepsilon')$ with any $\varepsilon' \leq 2\varepsilon/3$ will return its first (second) assertion iff the first (second) assertion of the original Lindblad generator instance was valid (always under the assumption that the original Lindblad generator instance was unambiguous). This is illustrated in Fig. 2.

We must now justify the assumption that the third assertion of the Markovian map instance $(\tilde{E}, 2\varepsilon/3, \varepsilon')$ is always false. Recall that the Lindblad generator promise guarantees existence of a generator L_0' of a quantum channel within an $f(\delta)$-ball around L_0. For the assumption to be justified, this must imply existence of at least one quantum channel within an ε'-ball around $\tilde{E}$. We now take $f(\delta)$ to be defined implicitly using Lemma 11, such that for $\|L_0 - L_0'\| \leq f(\delta)$ we have $\|e^{L_0} - e^{L_0'}\| \leq \varepsilon/3$. (Once again, substituting the explicit expression for ε into Eq. (22) and solving for $f(\delta)$ would give an explicit definition for the latter, if so desired.) Then $\|\tilde{E} - E'\| \leq 2\varepsilon/3$, so that E' fulfils the requirements with $\varepsilon' = 2\varepsilon/3$. Figure 3 illustrates this.

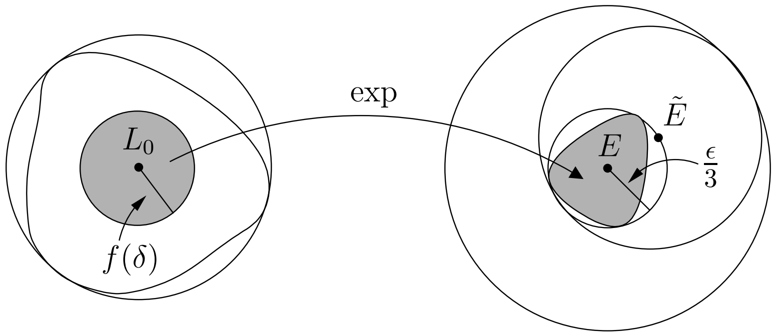


Figure 3: Everything within an $f(\delta)$-ball around L_0 is mapped into an $\varepsilon/3$-ball around E, which itself is contained within a $2\varepsilon/3$-ball around $\tilde{E}$. (See also Fig. 2.)

Finally, it remains to consider the case of Lindblad generator instances that *are* ambiguous; i.e. there exist generators of both Markovian and non-Markovian channels within a δ-ball around L_0. In that case, the Markovian map instance $(\tilde{E}, 2\varepsilon/3, \varepsilon' = 2\varepsilon/3)$ could return either assertion. But the original Lindblad generator instance is also allowed to return either assertion in this case, which completes the proof of the reduction. □

Theorem 17 Lindblad generator $\geq$ Markovian channel.

Proof The reduction from Markovian channel to Lindblad generator is very similar to the proof of Theorem 16, reversing the roles of Lemma 11 and Corollary 15. The Lindblad generator promise is automatically fulfilled, since $L_0 = \log E$ is itself necessarily a generator of a quantum channel (namely, E). □

Together, Theorems 7, 16 and 17 imply the following corollary:

Corollary 18 Lindblad generator = Markovian map = Markovian channel.

4 NP-hardness

We are now in a position to consider the computational complexity of the problems defined in the previous sections. Although the ccp condition of Eq. (5) is an integer semi-definite program, and it is well known that even linear integer programming is NP-complete, this by no means proves that Lindblad generator is NP-hard. Linear programming is the special case of semi-definite programming in which the coefficient matrices are diagonal. But the matrices L_0 and A_c defining a Lindblad generator instance must satisfy a number of highly non-trivial constraints, as listed in Lemma 9, which certainly cannot be satisfied by diagonal matrices. Instead, our approach will be to restrict to a special case of Lindblad generator, for which the relation between L_0 and L_0^Γ is somewhat easier to analyse, then show that this special case can be used to encode 1-in-3SAT, a standard NP-complete satisfiability problem [14], simpler even than its better-known cousin 3SAT in that it does not require any boolean negation:*

4.1 Encoding 1-in-3SAT

Problem 19 (1-in-3SAT)
Instance: *(n_v, n_C): n_v boolean variables; n_C clauses each with exactly 3 variables.*
Question: *Is there a truth assignment of the variables such that each clause contains exactly one true variable?*

1-in-3SAT can be transformed into a set of simultaneous linear integer inequalities in the standard way. Identify each boolean variable with an integer variable m_c, and identify the values 1 and 0 with "true" and "false". For each m_c, write the inequalities

$$m_c \geq -\frac{1}{2}, \quad -m_c \geq -\frac{7}{6}, \tag{27}$$

and for each 1-in-3SAT clause involving variables i, j and k, write the following inequalities:

$$m_i + m_j + m_k \geq \frac{1}{2}, \quad -m_i - m_j - m_k \geq -\frac{3}{2}. \tag{28}$$

*Note that the use of the term 1-in-3SAT is not entirely consistent in the literature. Here we mean the variant that does not involve any negation, as originally formulated in Ref. [41].

The non-integer constants are chosen for later convenience. These inequalities are satisfied for integer m_c if precisely one m_i from each clause is equal to one and the others are all zero.

We now restrict the matrices L_0 and A_c that define a Lindblad Generator instance (cf. Eq. (9)) to have the following special forms:

$$L_0 = \sum_{i,j} Q_{i,j} \left|i,i\right\rangle\left\langle j,j\right| + \sum_{i\neq j} P_{i,j} \left|i,j\right\rangle\left\langle i,j\right|, \tag{29}$$

$$A_c = 2\pi \sum_{i\neq j} B^c_{i,j} \left|i,i\right\rangle\left\langle j,j\right|, \tag{30}$$

with

$$\begin{aligned} Q = \sum_r \mathbf{x}_r\mathbf{x}_r^T \otimes \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} k+\lambda_r & \lambda_r \\ \lambda_r & k+\lambda_r \end{pmatrix} \\ + \sum_c \mathbf{v}_c\mathbf{v}_c^T \otimes \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \begin{pmatrix} k & -\frac{1}{3} \\ \frac{1}{3} & k \end{pmatrix} \\ + \sum_{c'} \mathbf{v}_{c'}\mathbf{v}_{c'}^T \otimes \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \begin{pmatrix} k & 0 \\ 0 & k \end{pmatrix}, \end{aligned} \tag{31}$$

$$B^c = \mathbf{v}_c\mathbf{v}_c^T \otimes \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{32}$$

$\{\mathbf{x}_r\}$ and $\{\mathbf{v}_c, \mathbf{v}_{c'}\}$ are two complete sets of mutually-orthogonal, real vectors, whilst k and λ_r are real. Note that Q and B^c are normal matrices, as are L_0 and A_c. Since $[L_0, A_c^\dagger] = 0$, the $\{L_m = L_0 + \sum_c m_c A_c\}$ are also normal. The factor of 2π in Eq. (30) is for later convenience. Figures 4 and 5 give a graphical representation of the structure of L_0 and A_c.

It is a simple matter to verify that the properties required by Lemma 9 are indeed satisfied by the forms given in Eqs. (29) to (32), as long as

$$\mathbf{w}^T Q = 0, \tag{33}$$

and $P = P^\dagger$ is Hermitian, where $\mathbf{w} = (1,1,\ldots,1)^T/\sqrt{d}$ for $d \times d$-matrix Q. Furthermore, the ccp condition of Lemma 8 reduces to the pair of conditions

$$2\pi \sum_c B^c_{i,j}\, m_c + Q_{i,j} \geq 0, \qquad i \neq j, \tag{34a}$$

$$(\mathbb{1} - \mathbf{w}\mathbf{w}^T) K (\mathbb{1} - \mathbf{w}\mathbf{w}^T) \geq 0, \tag{34b}$$

where K denotes the $d \times d$-dimensional matrix with diagonal elements $K_{i,i} = Q_{i,i}$ and off-diagonal elements $K_{i\neq j} = P_{i,j}$.

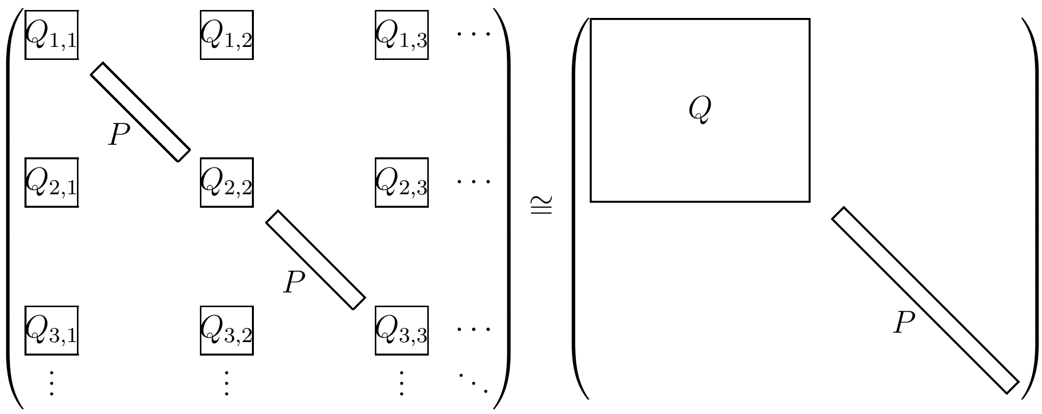


Figure 4: The structure of L_0 from Eq. (29) is most apparent if we reorder the rows and columns so that all the $(i,i),(j,j)$ elements are in the top, left corner. We can then think of $L_0 \cong Q \oplus \operatorname{diag} P$ as being composed of a matrix Q and a vector P.

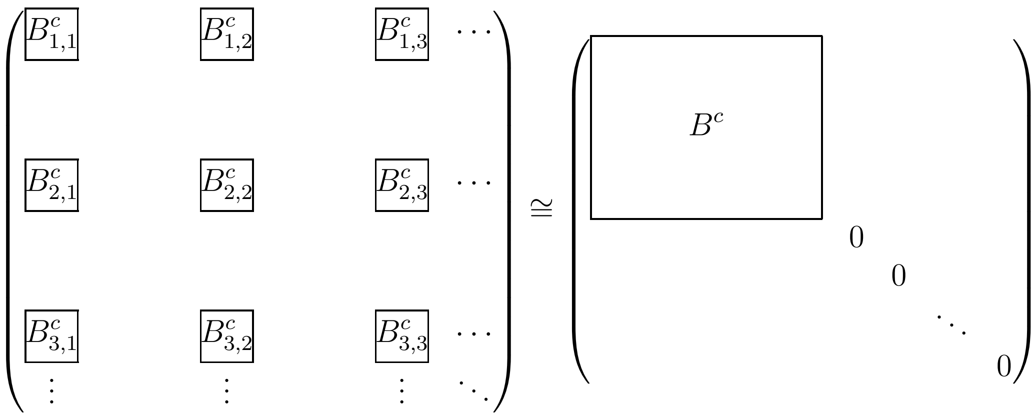


Figure 5: Reordered in the same way, A_c from Eq. (30) is composed of just a matrix part: $A_c \cong B^c \oplus 0$.

We encode the 1-IN-3SAT inequalities of Eqs. (27) and (28) by writing them directly into the $\{\mathbf{v}_c\}$. We associate a single $\mathbf{v}_c$ to each boolean variable of the problem. For each clause l, write a "1" in the l'th element of the three $\mathbf{v}_c$'s corresponding to the variables appearing in that clause, and write a "0" in the same element of all the other $\mathbf{v}_c$. Since there are n_C clauses in total, at the end of this process the vectors each have n_C elements. Now for each $\mathbf{v}_c$, write a "1" in its $n_C + c$'th element, writing a "0" in the corresponding element of all the other vectors. So far, we have defined the first $n_C + n_v$ elements of the vectors. Finally, extend the vectors so that they are mutually orthogonal and all have the same Euclidean norm $\mathbf{v}_c^T\mathbf{v}_c$. This can always be done, and will require at most a further n_v elements, producing vectors with at most $n_C + 2n_v$ elements. This procedure encodes the coefficients for the 1-IN-3SAT inequalities into some of the on-diagonal 4×4 blocks of the B^c. Specifically, if we imagine colouring B^c in a chess-board pattern (starting with a "white square" in the top-leftmost element), then the coefficients for one inequality are duplicated in all the "black squares" of one 4×4 block (see Fig. 6).

Colouring Q in the same chess-board pattern, the contribution to its "black squares" from the first term of Eq. (31) is generated by the off-diagonal elements λ_r:

$$\sum_r \mathbf{x}_r\mathbf{x}_r^T \otimes \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} \cdot & \lambda_r \\ \lambda_r & \cdot \end{pmatrix} = S \otimes \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} \cdot & 1 \\ 1 & \cdot \end{pmatrix}. \tag{35}$$

(The dots emphasise that the "white squares" generated by those entries will be specified later.) Since $\{\mathbf{x}_r\}$ and $\{\lambda_r\}$ can be chosen freely, the first tensor factor in this expression is just the eigenvalue decomposition of an arbitrary real, symmetric matrix S. If we choose the first n_C diagonal elements of S to be $1/2$, and choose the next n_v diagonal elements of S to be $5/6$, then it is straightforward to verify that the equations in the ccp condition of Eq. (34a) corresponding to the "black squares" in on-diagonal 4×4 blocks are exactly the 1-IN-3SAT inequalities of Eqs. (27) and (28) (see Figs. 8 and 9). Note that the off-diagonal elements of S are not specified yet.

We have successfully encoded the correct coefficients and constants into certain matrix elements of B^c and Q. But all the other elements of these matrices also generate inequalities via Eq. (34a). To "filter out" these unwanted inequalities, we choose the remaining diagonal elements and all off-diagonal elements of the symmetric matrix S to be large and positive, thereby ensuring all unwanted inequalities are slack.

The matrices A_c from Eq. (30) automatically satisfy the normalisation condition of Lemma 9, but L_0, as constructed so far, will not. We use the

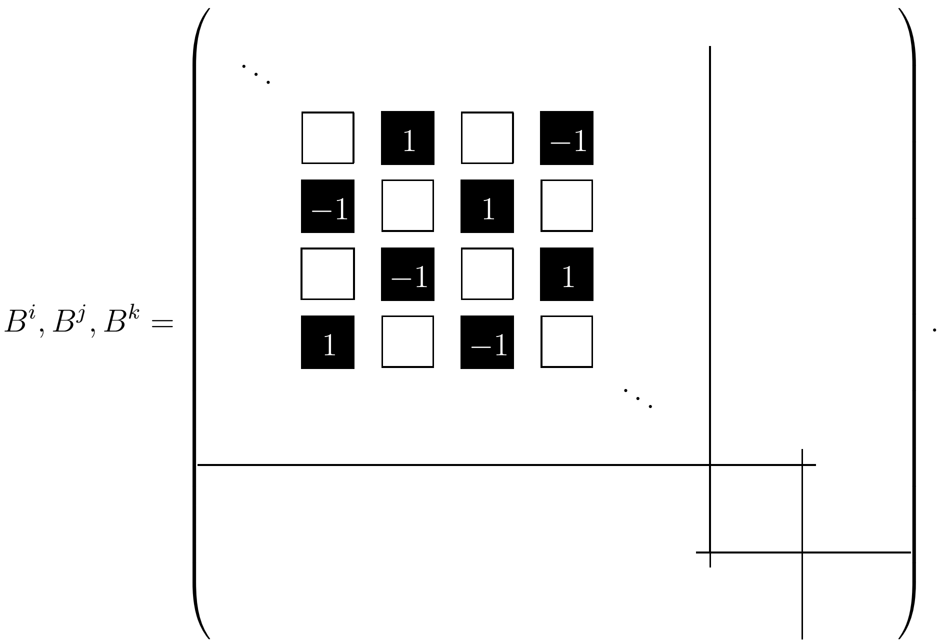


Figure 6: If the n'th 1-IN-3SAT clause involves variables i, j, k, the construction encodes the coefficients from the inequalities of Eqs. (28) into the n'th on-diagonal 4×4 block of B^i, B^j and B^k. All other B^c corresponding to variables that do not appear in that clause will have zeros in that particular block.

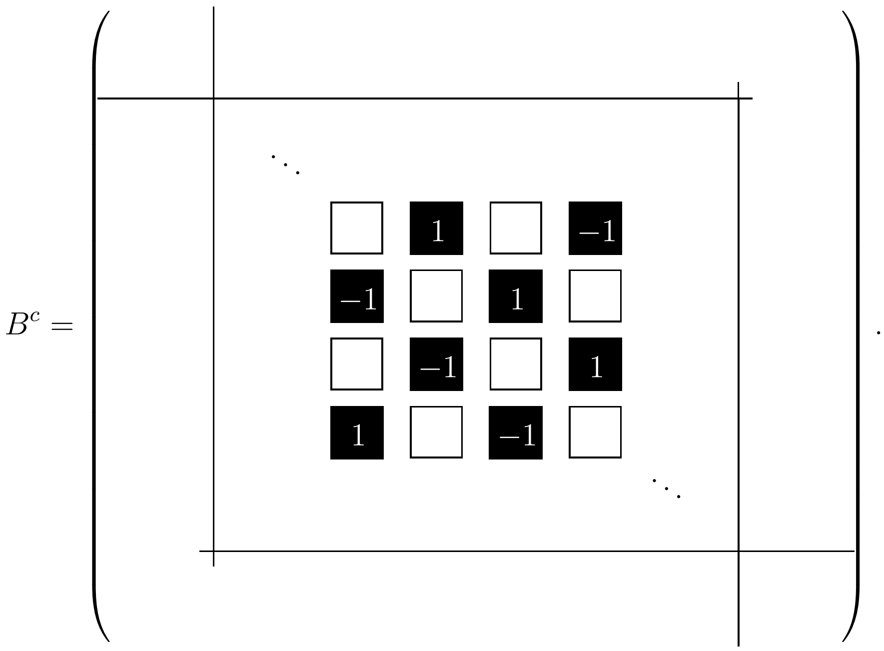


Figure 7: Each B^c contains a unique block of non-zero entries in the second set of on-diagonal 4×4 blocks, corresponding to the 1-IN-3SAT boolean constraints of Eqs. (27).

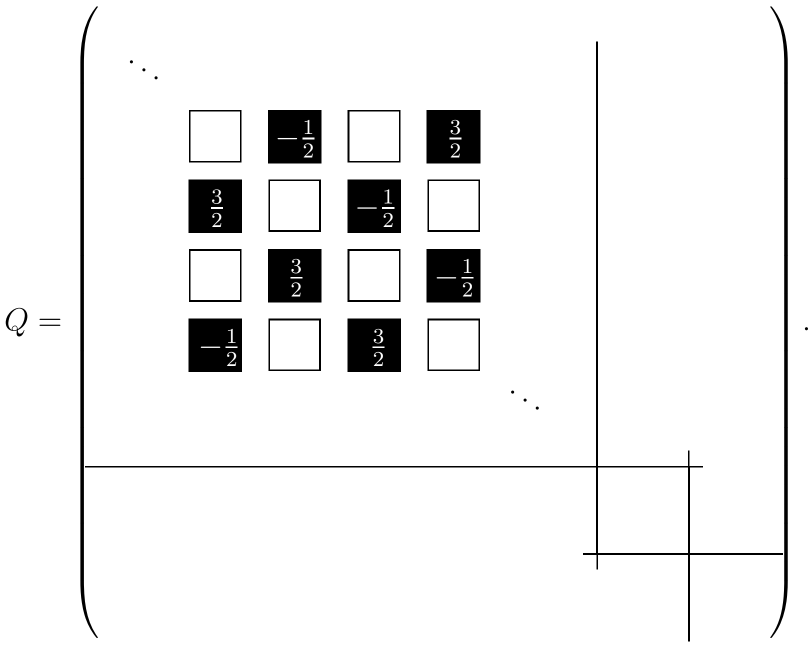
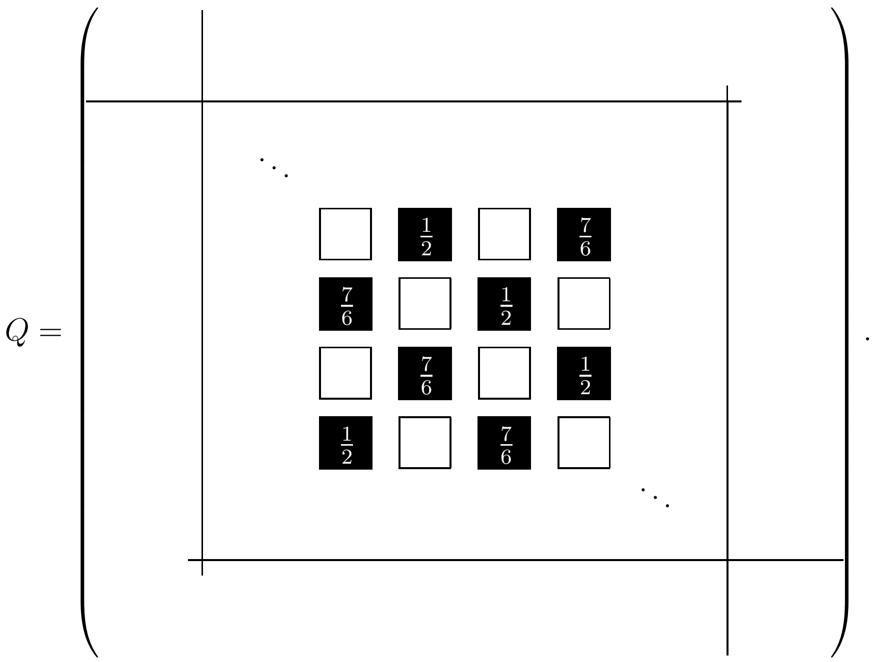


Figure 8: The first set of on-diagonal 4×4 blocks of Q contain the constants for the 1-IN-3SAT clause inequalities of Eqs. (28)...



(36)

Figure 9: ...whilst the second set of on-diagonal 4×4 blocks of Q contain the constants for the 1-IN-3SAT boolean inequalities of Eqs. (27).

"white squares" of Q (see Figs. 8 and 9), generated by the diagonal elements in the third tensor factors of Eq. (31), to renormalise the column sums to zero. Recall that both $\{\mathbf{x}_r\}$ and $\{\mathbf{v}_c, \mathbf{v}_{c'}\}$ are complete sets of mutually orthogonal vectors. Rearranging Eq. (31), Q is therefore given by

$$Q = k\mathbb{1} + S \otimes \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} + \sum_c \mathbf{v}_c \mathbf{v}_c^T \otimes \begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix} \otimes \begin{pmatrix} 0 & -\frac{1}{3} \\ \frac{1}{3} & 0 \end{pmatrix}. \quad (37)$$

Now, the only requirement on the off-diagonal elements of S is that they be sufficiently positive. Also, from the form of Eq. (37), the columns in any individual 4×4 block of Q sum to the same value. Thus, by adjusting the elements of S, we can ensure that all columns of $Q - k\mathbb{1}$ sum to the *same* positive value, which we call σ. Choosing $k = -\sigma$, the negative on-diagonal element in each column (generated by the $k\mathbb{1}$ term) will cancel the positive contribution from the off-diagonal elements, thereby satisfying the normalisation condition, as required.

Finally, we must ensure that the second ccp condition of Eq. (34b) is always satisfied, for which we require a simple lemma.

Lemma 20 *If $D \geq -\sigma\mathbb{1}$ is a diagonal $d \times d$-dimensional matrix, then there exists a symmetric matrix P such that $P_{i,i} = 0$ for all i and*

$$(\mathbb{1} - \mathbf{w}\mathbf{w}^T)(D + P)(\mathbb{1} - \mathbf{w}\mathbf{w}^T) \geq 0, \quad (38)$$

where $\mathbf{w} = (1, 1, \ldots, 1)^T/\sqrt{d}$.

Proof Choose $P = \alpha(\mathbb{1} - \mathbf{w}\mathbf{w}^T) + \alpha(1-d)\mathbf{w}\mathbf{w}^T$. Then the diagonal elements of P are

$$P_{i,i} = \alpha \left(1 - \frac{1}{d}\right) + \alpha(1-d)\frac{1}{d} = 0, \quad (39)$$

and

$$(\mathbb{1} - \mathbf{w}\mathbf{w}^T)(D + P)(\mathbb{1} - \mathbf{w}\mathbf{w}^T) \geq (\alpha - \sigma)(\mathbb{1} - \mathbf{w}\mathbf{w}^T), \quad (40)$$

which is positive semi-definite for $\alpha \geq \sigma$. □

The coefficients $P_{i,j}$ in Eq. (29) can be chosen freely, since these coefficients play no role in either the normalisation or in encoding 1-IN-3SAT, so the matrix P in the ccp condition of Eq. (34b) can be chosen to be any matrix with zeros down the main diagonal. Eq. (34b) is exactly of the form given in Lemma 20 with

$$D_{i,i} = Q_{i,i} \quad (41)$$

and choosing P accordingly ensures that it is always satisfied.

4.2 Perturbations

In the discussion preceding the definition of LINDBLAD GENERATOR, we argued that we need only consider non-singular, non-degenerate channels. Generators of such channels are necessarily bounded and non-degenerate as well, and the proof of equivalence of LINDBLAD GENERATOR and MARKOVIAN MAP, leading to Theorem 16, breaks down if these properties do not hold, since additional branches of the matrix logarithm arise: applying an arbitrary similarity transformation to a degenerate Jordan block will give another logarithm. The matrix L_0 we have constructed is clearly bounded, but it is highly degenerate.

We will now slightly modify the above construction, removing the mentioned degeneracies. In fact, most of the degeneracies can easily be lifted by as large a margin as desired by perturbing suitable elements of L_0, without affecting the conditions of Lemma 9. The only ones that require more care are degeneracies due to the final two terms of Eq. (31), as some of those matrix elements were used to encode 1-IN-3SAT.

It is not difficult to verify that m_c will be constrained to the same set of integer values if the perturbation to any constant in the set of inequalities is less than 1/6 (the second inequality in Eqs. (27) being the most sensitive). The constants are given directly by matrix elements of L_0, so we are free to lift the remaining degeneracies in L_0 by perturbing each summand in the final two terms of Eq. (31) by a different amount, as long as we ensure that no element of L_0 is perturbed by more than 1/6. This can be achieved by perturbing each off-diagonal element* of the final tensor factor by a different integer multiple of

$$\frac{2}{9d}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{42}$$

No element of L_0 is then perturbed by more than 1/18 (this is deliberately stricter than necessary by a factor of three, for reasons that will become clearer later), and the minimum eigenvalue separation for the perturbed L_0 is $2/(9d)$.

By construction, L_0 is a Lindblad generator iff the original 1-IN-3SAT instance was satisfiable, so we have achieved the first half of the reduction. It remains to choose a value of δ such that this also holds for any L_0' in the δ-ball around L_0. As noted above, the inequalities in Eqs. (27) and (28) are insensitive to small perturbations. Specifically, one can verify that the set of feasible m_c will be unchanged if each coefficient and constant (this time

*We avoid perturbing the diagonal elements, as that would make satisfying the normalisation condition far more difficult.

including zero coefficients, i.e. coefficients of variables that do not appear explicitly in Eqs. (27) and (28)) is perturbed by less than $\min[1/18(n_v + 1), 5/18(2n_v + 1)]$. (Recall that we already perturbed the constants by (up to) 1/18 to lift eigenvalue degeneracies. This bound is deliberately stronger by a factor of two than would appear to be necessary at this stage, but in any case it is certainly stronger than is strictly necessary.)

The constants in the inequalities are given by matrix elements of L_0. If we choose the norm in LINDBLAD GENERATOR to be the l_∞ norm, then is is sufficient to require

$$\delta \leq \min\left[\frac{1}{18(n_v+1)}, \frac{5}{18(2n_v+1)}\right]. \tag{43}$$

The coefficients in the inequalities are given by matrix elements of A_c, which are formed from the eigenvectors of L_0. Thus, to bound perturbations of the coefficients, we must bound perturbations of the eigenvectors in terms of the perturbation to L_0, which is less trivial. We will need the following result from Ref. [42], and a simple corollary.

Lemma 21 *Suppose A is a normal matrix, with E an arbitrary matrix of the same dimension. Let $Q = (\mathbf{v}_1, Q_2)$ be unitary, such that $\mathbf{v}_1$ is an eigenvector of A, and partition the matrix $Q^\dagger EQ$ conformally with $Q^\dagger AQ$, so that**:

$$Q^\dagger AQ = \begin{pmatrix} \lambda_1 & 0 \\ 0 & A_{2,2} \end{pmatrix}, \quad Q^\dagger EQ = \begin{pmatrix} E_{1,1} & E_{1,2} \\ E_{2,1} & E_{2,2} \end{pmatrix}, \tag{44}$$

where $\{\lambda_i\}$ denote the eigenvalues of A, with λ_1 the eigenvalue associated with $\mathbf{v}_1$. Let

$$\Delta = \min_{i\neq 1} |\lambda_1 - \lambda_i| - \|E_{1,1}\|_{\mathrm{F}} - \|E_{2,2}\|_{\mathrm{F}}\,, \tag{45}$$

where $\|X\|_{\mathrm{F}}^2 = \sum_{i,j} |X_{i,j}|^2$ is the Frobenius (or Hilbert-Schmidt) norm. If $\Delta > 0$, and

$$\frac{\|E_{2,1}\|_{\mathrm{F}}\,\|E_{1,2}\|_{\mathrm{F}}}{\Delta^2} \leq \frac{1}{4}, \tag{46}$$

then there exists a matrix P satisfying

$$\|P\|_{\mathrm{F}} \leq 2\frac{\|E_{2,1}\|_{\mathrm{F}}}{\Delta} \tag{47}$$

such that $\mathbf{v}' = (\mathbf{v}_1 + Q_2P)(\mathbb{1} + P^\dagger P)^{-1/2}$ is a unit eigenvector of $A + E$ (in the Frobenius norm).

*$Q^\dagger AQ$ must be of this form, as the Schur decomposition of a normal matrix is diagonal.

Proof This is a slight generalisation of Theorem 8.1.12 from Ref. [43], or slight restriction of Theorem 4.11 from Ref. [42], to the case of normal A. □

Corollary 22 *Suppose A is a normal matrix, with E an arbitrary matrix of the same dimension. If $\mathbf{v}$ is a unit (in Frobenius norm) eigenvector of A associated with a non-degenerate eigenvalue, and the requirements of Lemma 21 are fulfilled, then there exists a unit eigenvector $\mathbf{v}'$ of $A+E$ such that*

$$\left\|\mathbf{v}\mathbf{v}^\dagger - \mathbf{v}'\mathbf{v}'^\dagger\right\|_{\mathrm{F}} \leq K \left\|E\right\|_{\mathrm{F}}, \tag{48}$$

with

$$K = \frac{4\left(d\left\|E\right\|_{\mathrm{F}} + \sqrt{d-1}\Delta\right)}{\Delta^2 - 4\left\|E\right\|_{\mathrm{F}}^2} \tag{49}$$

and Δ as defined in Lemma 21.

Proof From Lemma 21, we have

$$\begin{aligned}
\left\|\mathbf{v}'\mathbf{v}'^\dagger - \mathbf{v}\mathbf{v}^\dagger\right\|_{\mathrm{F}} &= \left\|\frac{(\mathbf{v}_1 + Q_2P)(\mathbf{v}_1 + Q_2P)^\dagger}{\mathbb{1} + P^\dagger P} - \mathbf{v}_1\mathbf{v}_1^\dagger\right\|_{\mathrm{F}} && (50)\\
&\leq \frac{2\|\mathbf{v}\|_{\mathrm{F}}\|Q_2\|_{\mathrm{F}} + \|P\|_{\mathrm{F}}\left(\|\mathbf{v}\|_{\mathrm{F}}^2 + \|Q_2\|_{\mathrm{F}}^2\right)}{1 - \|P^\dagger P\|_{\mathrm{F}}}\|P\|_{\mathrm{F}} && (51)\\
&\leq \frac{2\sqrt{d-1} + d\|P\|_{\mathrm{F}}}{1 - \|P\|_{\mathrm{F}}^2}\|P\|_{\mathrm{F}}. && (52)
\end{aligned}$$

in which we have used Lemma 2.3.3 from Ref. [43] to bound $(\mathbb{1} + P^\dagger P)^{-1}$, and the fact that $\|U\|_{\mathrm{F}} = \sqrt{d}$ for any $d \times d$ unitary U. The result follows by substituting the bound on $\|P\|_{\mathrm{F}}$ from Lemma 21, and using $\|E_{2,1}\|_{\mathrm{F}} \leq \|E\|_{\mathrm{F}}$. □

Now, each A_c is a sum of two eigenprojectors, and L_0 happens to be normal. Applying Corollary 22, and using the fact that $\|X\|_\infty \leq \|X\|_{\mathrm{F}}$, we see that it suffices to restrict

$$\delta \leq \frac{1}{2K}\min\left[\frac{1}{18(n_v+1)}, \frac{5}{18(2n_v+1)}\right]. \tag{53}$$

We must also satisfy the two requirements of Lemma 21. Recalling that the minimum eigenvalue separation of L_0 is $2/(9d)$, we see that it is sufficient to impose

$$\delta < \frac{1}{9d^2} \quad \text{and} \quad \delta \leq \frac{\min_{i\neq j}|\lambda_i - \lambda_j|}{4d} = \frac{1}{18d}. \tag{54}$$

For L_0, satisfying the inequalities is equivalent to satisfying the ccp condition of Lemma 8. However, even choosing δ to satisfy Eqs. (43), (53) and (54), this may no longer be the case for all L'_0 within the δ-ball around L_0. If the inequalities are infeasible, then at least one diagonal element of any $(\mathbb{1}-\omega){L'_m}^\Gamma(\mathbb{1}-\omega)$ must be negative, and it is still the case that the ccp condition is violated (since non-negativity of the diagonal elements is a necessary condition for a matrix to be positive semi-definite). But if the inequalities *can* be satisfied, the most we can say is that all diagonal elements of $(\mathbb{1}-\omega){L'_m}^\Gamma(\mathbb{1}-\omega)$ are lower-bounded by 1/18.

Now

$$L'_m = L'_0 + \sum_c m_c A'_c \tag{55}$$

with $0 \leq m_c \leq 1$ integer, and the A'_c are perturbations of A_c. The off-diagonal elements of the latter are zero. Therefore, we can control the magnitude of the off-diagonal elements of the n_v different A'_c by applying Corollary 22 again, whilst controlling the off-diagonal elements of L'_0 by restricting δ directly, as before. Putting all this together, we see that imposing

$$\delta \leq \frac{1}{18d} \quad \text{and} \quad \delta \leq \frac{1}{32Kn_v d} \tag{56}$$

ensures that the off-diagonal elements of any L'_m are upper-bounded by $1/(18d)$. However, this implies that $(\mathbb{1}-\omega){L'_m}^\Gamma(\mathbb{1}-\omega)$ is diagonally-dominant, which is sufficient to guarantee positive-semi-definiteness.

Thus, if $\delta > 0$ is chosen to satisfy Eqs. (43), (53), (54) and (56), then for any L'_0 within a δ-ball around L_0 (in the l_∞ norm), satisfying the ccp condition is equivalent to satisfying the original 1-in-3SAT problem. Comparing the bounds on δ from Eqs. (43), (53), (54) and (56), we have

$$\delta = O(n_v^{-1}(n_C + 2n_v)^{-3}). \tag{57}$$

Sufficient bounds for any other norm can easily be obtained via equivalence of norms in finite-dimensional spaces, and will at worst introduce additional factors polynomial in the dimension (i.e. polynomial in n_v and n_C). The fact that δ^{-1} has to scale only polynomially makes our results far more compelling; it cannot be claimed that they are a consequence of unreasonable precision demands. Even this mild scaling may be an artifact of the construction, and it would be interesting to know if a construction exists in which δ can be taken constant.

Finally, it remains to consider the promise required in the definition of Lindblad generator. Assume that the promise is *not* satisfied. In that case, L_0 itself clearly cannot be the generator of a CPT map. But L_0 satisfies the Hermiticity and normalisation requirements of Lemma 8 by construction, so it must fail to satisfy the ccp condition. Thus failing to satisfy the promise implies that the 1-IN-3SAT instance must have been unsatisfiable. Combining the arguments used in the proofs of Theorems 7 and 16 gives an efficient procedure for deciding whether (L_0, δ) satisfies the promise, thereby deciding these instances. This leaves only instances that do satisfy the promise, as required.

We have reduced satisfiable instances of 1-IN-3SAT to LINDBLAD GENERATOR instances that return the first assertion, and have either efficiently decided unsatisfiable instances of 1-IN-3SAT (because they fail to satisfy the promise)*, or reduced them to LINDBLAD GENERATOR instances that return the second assertion. This completes the proof that

Lemma 23 1-IN-3SAT $\leq$ LINDBLAD GENERATOR

and, since 1-IN-3SAT is NP-complete,

Corollary 24 LINDBLAD GENERATOR *is NP-hard.*

But, by the chain of equivalences proven in Theorem 7 and Corollary 18, this implies our main result:

Theorem 25 MARKOVIAN CHANNEL *and* MARKOVIAN MAP *are NP-hard.*

Theorem 25 tells us that the Markovianity problem is NP-hard. What of the more general question of determining whether a given family of maps are members of the same continuous, one-parameter, completely positive semigroup? Formulated rigorously, this is a generalised version of MARKOVIAN MAP, in which a family of maps E_t is given, along with their associated times t (up to some precision), and the answer should assert the existence or otherwise of a *common* Lindblad generator for all the maps up to precision $\varepsilon > 0$ (or assert that at least one of the E_t is not CPT up to precision $\varepsilon' > 0$).

A first trivial observation is that, since we know there exists a special case of this problem that is NP-hard, namely MARKOVIAN MAP itself, the general problem is automatically NP-hard. However, this leaves open the question of whether the complexity depends on the number of maps in the family. Recalling the physical motivation behind the problem, one might expect that, given more information about the dynamics (e.g. by taking many tomographic snapshots), the problem would become easier to resolve.

In fact, in proving the NP-hardness of MARKOVIAN MAP, we have already done all the work necessary to prove NP-hardness of the general problem for

*It is amusing, but probably of no practical value, to note that this provides a new "gadget" for efficiently deciding certain non-satisfiable instances of 1-IN-3SAT.

any number of maps. Instead of computing a single map $E = e^L$ to reduce LINDBLAD GENERATOR to MARKOVIAN MAP, we can compute a family of any number of maps $E_t = e^{Lt}$. (To make this rigorous, the arguments of Theorem 16 can straightforwardly be extended to the case of a family of maps E_t.) So the problem for an arbitrary (finite) number of maps is essentially no different to the problem for a single map as far as the worst-case complexity is concerned.

5 An Algorithm

The NP-hardness proof of Section 4 implies that we are unlikely to find an efficient algorithm for solving the Markovianity problem. Nonetheless, there are two reasons to develop an algorithm for solving it, even though it will be inefficient. The first reason is in some sense a technicality. We would like to prove that solving the Markovianity problem is equivalent to solving P=NP. That is, we want to show that (i) any efficient algorithm for solving the Markovianity problem would imply P=NP, and conversely (ii) *if P=NP then there exists an efficient algorithm for solving the Markovianity problem.* NP-hardness proves (i). But the weak-membership formulations of the Markovianity problem (MARKOVIAN CHANNEL/MAP) are not technically members of the class NP, thus it is not clear whether proving P=NP would be sufficient to provide an efficient algorithm for solving them. Weak-membership problems do not belong to NP, for the simple reason that NP is a decision class, but weak-membership problems are not decision problems since they have instances in which both "yes" and "no" answers are simultaneously valid. (As mentioned above, the appropriate complexity class for weak-membership problems is called promise-NP; the additional promise is that the instance will not be one of the ambiguous ones.) Giving an explicit algorithm for MARKOVIAN CHANNEL which reduces to solving an NP-complete problem resolves this technicality.

The second reason for developing an algorithm is that the NP-hardness proof of Section 4 requires the dimension to scale polynomially with the size of the 1-IN-3SAT problem being encoded. So, although the general Markovianity problem for CPT maps and embedding problem for stochastic matrices are NP-hard, it is interesting to ask how the complexity scales if the dimension is fixed (in which case the problem size scales only with the precision). By giving an explicit algorithm, we show that *for fixed dimension* the Markovianity problem can be solved efficiently, i.e. the complexity scales only polynomially with the precision. This is also the basis for the proposed measure of Markovianity in Ref. [7].

One motivation for considering the case of fixed dimension is current experimental limitations. A snapshot of a quantum evolution is measured by performing full quantum process tomography. Tomography of a d–dimensional system requires measuring a total of $d^4 - d^2$ different expectation values [1, §8.4.2], and the expectation value of each observable must be estimated by averaging over many runs. The experimental overhead for all of this scales polynomially with the dimension of the system, but a polynomial scaling can still be prohibitive in practice! Current experiments can only perform full process tomography for systems up to a few qubits, before the time required becomes exorbitant. It is quite reasonable in this context to regard dimension as a fixed parameter.

Since Markovian map is equivalent to Markovian channel by Theorem 7, a Markovian map instance can be solved by first efficiently reducing it to Markovian channel, then solving the Markovian channel instance. We now describe an algorithm which solves Markovian channel in polynomial time for fixed dimension. (The present treatment presents a detailed and rigorous proof of the result already reported in Ref. [7].) It is not difficult to adapt this algorithm to the classical Embeddability problem of Section 6. For convenience, we will take the matrix norm in the definition of Markovian channel to be the Frobenius norm $\|.\|_\mathrm{F}$.*

Algorithm 26 (MARKOVIAN CHANNEL)
Input: (E, ε): Quantum channel E, precision ε.
Output: One of the two assertions from Problem 5.

1: Calculate approximations $\bar{L}_0$ and $\bar{A}_c$ to $L_0 = \log E$ and A_c (cf. Lemma 8) to any precision κ, so that $\|\bar{L}_0 - L_0\|_\mathrm{F} \leq \kappa$ and $\|\bar{A}_c - A_c\|_\mathrm{F} \leq \kappa$ ($\bar{L}_0$ and $\bar{A}_c$ can be obtained e.g. by calculating the eigenvalues and eigenvectors of E).

2: Calculate $\tilde{\delta}$ by solving

$$\exp\Big(\|\bar{L}_0\|_\mathrm{F} + M\sum_c \|\bar{A}_c\|_\mathrm{F}\Big)\exp\Big(\kappa + \frac{Md\kappa}{2}\Big)\,\tilde{\delta}\,e^{\tilde{\delta}} = \varepsilon, \qquad (58)$$

where M depends polynomially on ε (discussed in more detail below) and d is the dimension of E.

3: Calculate approximations $\tilde{\lambda}_i$ to the logarithms λ_i of eigenvalues e^{λ_i} of E, and to the eigenprojectors $|\tilde{r}_i\rangle\langle\tilde{l}_i|$ of E, to precision sufficient to ensure

*It is straightforward to generalise these results to other norms.

that

$$\left\|\sum_i \tilde{\lambda}_i \, |\tilde{r}_i\rangle\langle\tilde{l}_i| - \sum_i \lambda_i \, |r_i\rangle\langle l_i|\right\| \leq \frac{\tilde{\delta}}{12d\|\mathbb{1}-\omega\|_{\mathrm{F}}^3}, \tag{59}$$

$$\left\||\tilde{r}_i\rangle\langle\tilde{l}_i| - |r_i\rangle\langle l_i|\right\|_{\mathrm{F}} \leq \frac{\tilde{\delta}}{24\pi M d^2\|\mathbb{1}-\omega\|_{\mathrm{F}}^3}, \tag{60}$$

$$|\tilde{\lambda}_i - \lambda_i| < \min_{j\neq k} \frac{\tilde{\lambda}_j - \tilde{\lambda}_k}{4}. \tag{61}$$

4: Use the results to calculate $\tilde{L}_0 = \sum_i \tilde{\lambda}_i \, |\tilde{r}_i\rangle\langle\tilde{l}_i|$ and the corresponding $\tilde{A}_c$ (cf. Lemma 8).

5: Solve the following mixed integer semi-definite program, in integer variables m_c and real variable t:

minimise $\quad t$

subject to $\quad (\mathbb{1}-\omega)\tilde{L}_0^{\Gamma}(\mathbb{1}-\omega) + \sum_c m_c(\mathbb{1}-\omega)\tilde{A}_c^{\Gamma}(\mathbb{1}-\omega) + t\mathbb{1} \geq 0.$

6: **if** $t \leq -\tilde{\delta}/(6d\|\mathbb{1}-\omega\|_{\mathrm{F}})$ **then**
7:     **return** "Markovian" (1st assertion of Problem 5).
8: **else if** $t > \tilde{\delta}/(6d\|\mathbb{1}-\omega\|_{\mathrm{F}})$ **then**
9:     **return** "non-Markovian" (2nd assertion of Problem 5).
10: **else if** $t \leq \tilde{\delta}/(3d\|\mathbb{1}-\omega\|_{\mathrm{F}})$ **then**
11:     **return** "Markovian" (1st assertion of Problem 5).
12: **end if**

To prove correctness of Algorithm 26, first note that, from lines 2 to 4, $\|\tilde{L}_0 - L_0\|_{\mathrm{F}} \leq \tilde{\delta}/(12d\|\mathbb{1}-\omega\|_{\mathrm{F}}^3)$. Also, if $\max_c m_c \leq M$, then from line 3 we have

$$\begin{aligned}\|\tilde{L}_m - L_m\|_{\mathrm{F}} &\leq \|\tilde{L}_0 - L_0\|_{\mathrm{F}} + 2\pi\sum_c |m_c| \| \, |\tilde{r}_i\rangle\langle\tilde{l}_i| - |r_i\rangle\langle l_i| \, \|_{\mathrm{F}} \\ &= \frac{\tilde{\delta}}{6d\|\mathbb{1}-\omega\|_{\mathrm{F}}^3}.\end{aligned} \tag{62}$$

We will assume throughout the following that M is an upper bound on the values m_c returned by the integer program of line 5, i.e. that $\max_c |m_c| \leq M < \infty$, an assumption that will be justified later.

Now consider the three cases in lines 6 to 11. To deal with the first two, we will need the following simple lemma (see e.g. Ref. [44, Corollary 6.3.4]):

Lemma 27 *Let A be normal, E be an arbitrary matrix. If λ' is an eigenvalue of $A+E$, then there exists some eigenvalue λ of A such that $|\lambda' - \lambda| \leq \|E\|_{\mathrm{F}}$.*

If $t \leq -\tilde{\delta}/(6d\|\mathbb{1} - \omega\|_{\mathrm{F}})$, then, from the definition of the integer program in line 5 of Algorithm 26, we know that all eigenvalues of $(\mathbb{1} - \omega)\tilde{L}_m^{\Gamma}(\mathbb{1} - \omega)$ are greater than $\tilde{\delta}/(6d\|\mathbb{1} - \omega\|_{\mathrm{F}})$. Also, from Eq. (62), $\|(\mathbb{1} - \omega)(\tilde{L}_m^{\Gamma} - L_m^{\Gamma})(\mathbb{1} - \omega)\|_{\mathrm{F}} \leq \tilde{\delta}/(6d\|\mathbb{1} - \omega\|_{\mathrm{F}})$. Lemma 27 then implies that the minimum eigenvalue of $(\mathbb{1} - \omega)L_m^{\Gamma}(\mathbb{1} - \omega)$ is non-negative, i.e. L_m is ccp. L_0 is therefore a Lindblad generator by Lemma 8, thus the original channel E must itself be Markovian. Similarly, if $t > \tilde{\delta}/(6d\|\mathbb{1} - \omega\|_{\mathrm{F}})$, then the minimum eigenvalue of *any* $(\mathbb{1} - \omega)L_m^{\Gamma}(\mathbb{1} - \omega)$ is strictly negative. Thus all L_m fail the ccp condition of Lemma 8, L_0 is not a Lindblad generator, and the original channel E is non-Markovian.

Dealing with the final case in line 10 of Algorithm 26 requires the following result:

Lemma 28 *If L is Hermitian and normalised (in the sense of Lemma 8), and the minimum eigenvalue of $(\mathbb{1} - \omega)L^{\Gamma}(\mathbb{1} - \omega)$ is bounded by $\lambda_{\min} \geq -\varepsilon$, then there exists a Lindblad generator L' such that $\|L' - L\|_{\mathrm{F}} \leq \varepsilon\, d\, \|\mathbb{1} - \omega\|_{\mathrm{F}}$, where d is the dimension of L.*

Proof Consider the map $L' = L + \varepsilon(d\,\omega - d\mathbb{1})$. Since L is Hermitian and normalised in the above sense, we have $(L'^{\Gamma})^{\dagger} = L'^{\Gamma}$ and $\langle\omega|\, L' = 0$, so these properties carry over to L'. But we also have

$$\begin{aligned}(\mathbb{1} - \omega)L'^{\Gamma}(\mathbb{1} - \omega) &= (\mathbb{1} - \omega)L^{\Gamma}(\mathbb{1} - \omega) + \varepsilon(\mathbb{1} - \omega)(\mathbb{1} - d^2\omega)(\mathbb{1} - \omega) \\ &= (\mathbb{1} - \omega)L^{\Gamma}(\mathbb{1} - \omega) + \varepsilon(\mathbb{1} - \omega).\end{aligned} \tag{63}$$

Since $(\mathbb{1} - \omega)L^{\Gamma}(\mathbb{1} - \omega)$ has support only on the orthogonal complement of $|\omega\rangle$, and $(\mathbb{1} - \omega)$ acts as identity on that subspace, the minimum eigenvalue of $(\mathbb{1} - \omega)L'^{\Gamma}(\mathbb{1} - \omega)$ is non-negative. Thus L' also satisfies the ccp condition, and, by Lemma 8, is a Lindblad generator. □

If $t \leq \tilde{\delta}/(3d\|\mathbb{1} - \omega\|_{\mathrm{F}})$, then the minimum eigenvalue of $(\mathbb{1} - \omega)\tilde{L}_m^{\Gamma}(\mathbb{1} - \omega)$ is greater than $-\tilde{\delta}/(3d\|\mathbb{1} - \omega\|_{\mathrm{F}})$, thus Lemma 27 and Eq. (62) imply that the minimum eigenvalue of $(\mathbb{1} - \omega)L_m^{\Gamma}(\mathbb{1} - \omega)$ is *lower*-bounded by

$$\lambda_{\min} \geq -\tilde{\delta}/(3d\|\mathbb{1} - \omega\|_{\mathrm{F}}) - \tilde{\delta}/(6d\|\mathbb{1} - \omega\|_{\mathrm{F}}) = -\tilde{\delta}/(2d\|\mathbb{1} - \omega\|_{\mathrm{F}}). \tag{64}$$

Applying Lemma 28 to L_m yields a Lindblad generator L' such that $\|L' - L_m\|_{\mathrm{F}} \leq d\|\mathbb{1} - \omega\|_{\mathrm{F}}\tilde{\delta}/(d\|\mathbb{1} - \omega\|_{\mathrm{F}}) = \tilde{\delta}$ and, since L' is a Lindblad generator,

$E' = e^{L'}$ is a Markovian channel. But, using Lemma 11, we have

$$\begin{aligned}\|E' - E\|_{\mathrm{F}} &\leq e^{\|L_m\|_{\mathrm{F}}} e^{\|L' - L_m\|_{\mathrm{F}}} \|L' - L_m\|_{\mathrm{F}} \\ &\leq \exp\Big(\|L_0\|_{\mathrm{F}} + M \sum_c \|A_c\|_{\mathrm{F}}\Big) \tilde{\delta}\, e^{\tilde{\delta}} \\ &\leq \exp\left(\|\tilde{L}_0\|_{\mathrm{F}} + M \sum_c \|\tilde{A}_c\|_{\mathrm{F}}\right) \exp\left(\kappa + \frac{Md\kappa}{2}\right) \tilde{\delta}\, e^{\tilde{\delta}} \\ &= \varepsilon,\end{aligned} \tag{65}$$

(with the inequality in the penultimate line resulting from line 1 of Algorithm 26—recall that there are at most $d/2$ matrices $\tilde{A}_c$—and the final equality from line 2). Therefore, E' is a Markovian channel within distance ε of the original channel E, and the first assertion of Problem 5 is valid.

This proves correctness of Algorithm 26. What of its run-time? All but a few steps can obviously be performed in polynomial-time. Recall that we are assuming, without loss of generality, that E is non-degenerate and non-singular, which, more rigorously stated, requires the condition number of E to be upper-bounded by some constant. The eigenvalue and eigenvector calculations of E in lines 3 and 1 can therefore be done efficiently in ε^{-1} and also the dimension [43, §7.2], with the eigenvalue and eigenvector condition numbers of E [43, §7.2.2–5] contributing a (possibly large) constant factor.

A question arises in calculating $\tilde{A}_c$: $\tilde{L}_0$ is not necessarily a Hermitian map, so how can the eigenvalue pairs from which to form $\tilde{A}_c$ (cf. Eq. (10)) be identified? But L_0 *is* Hermitian, and the bound on $|\tilde{\lambda}_i - \lambda_i|$ in line 3 ensures that the $2\|\tilde{\lambda}_i - \lambda_i\|_{\mathrm{F}}$-disc around λ_i^*, within which the conjugate partner of λ_i must lie, is guaranteed to contain a single $\tilde{\lambda}_j$, allowing approximately conjugate pairs of eigenvalues to be identified.

The key step in the algorithm is the mixed integer semi-definite program in line 5. (If Algorithm 26 is adapted to solve the classical Embeddability problem, this becomes a mixed *linear* integer program instead.) In a generalisation of a famous result by Lenstra [45] for linear integer programming, Khachiyan and Porkolab proved that for any *fixed* number of variables, integer semi-definite feasibility problems can be solved in polynomial time [46, 47]. In our case, fixing the number of variables corresponds to fixing the system's dimension. The integer semi-definite program can therefore be solved by applying the Khachiyan-Porkolab algorithm to the feasibility problem for given t, combined with binary search on t. From Corollary 1.3 of Ref. [46], the run-time of the Khachiyan-Porkolab part scales polynomially with the number of digits of precision to which the elements of the coefficient matrices are specified. But the coefficient matrices in our case are $\tilde{L}_0$ and $\tilde{A}_c$, and their description size is independent of the precision to which the original E was specified, depending only on the precision parameter ε. So the run-time of the Khachiyan-Porkolab step scales polynomially in ε^{-1}, as required.

We can now also justify the assumption that an upper bound $\max_c m_c \leq M$ can be placed on the integers m_c resulting from the integer program. Theorem 1.1 of Ref. [46] proves that such a bound exists and, in the case of integer semi-definite programming ([46, Corollary 1.3]), that it scales as

$$\log \max_c |m_c| = 2^{O(d^4)} \log l, \tag{66}$$

where l is the maximum bit-length of the entries of the coefficient matrices $\tilde{L}_0$ and $\tilde{A}_c$, and we have translated other parameters into our notation. Since we have already argued that the size of the description of these matrices scales polynomially with ε^{-1}, this gives a bound M that scales as

$$\max_c |m_c| = \varepsilon^{(2^{O(d^4)})O(1)} = M, \tag{67}$$

i.e. polynomially in ε^{-1} as claimed.

Since the calculations in each line of Algorithm 26 have run-times that scale at most polynomially in ε^{-1}, and are independent of the number of digits to which E was specified, the entire algorithm has run-time polynomial in the precision and independent of the size of the description of E. This, together with Theorem 7, proves the main practical result of this section:

Theorem 29 *For any fixed dimension,* MARKOVIAN CHANNEL *and* MARKOVIAN MAP *can be solved in a run-time that scales polynomially in both the problem size (the size of the description of the channel) and the precision parameter ε^{-1}.*

It is worth remembering that proving an algorithm has polynomial run-time does not necessarily imply that it is the best algorithm to use in practice. In fact, considering the first few branches of the logarithm is often sufficient for practically relevant cases. Indeed, it would be interesting to try to flesh out heuristics or a proof as to why this simple approach is so successful. If E is an experimentally measured tomographic snapshot, the truncation errors in computing $\log E$, that Algorithm 26 expends much effort in accounting for, will, in all likelihood, be swamped by experimental error. It is probably reasonable to calculate L_0 and A_c numerically, without worrying about numerical errors, and solve the resulting mixed integer semi-definite program using standard integer programming algorithms (which work well in practise even though their scaling may theoretically not be polynomial in the precision). If the t thus obtained is comparable to the estimated error, the most reasonable conclusion is that the experimental data simply are not precise enough to give any definitive answer. In fact, a more sophisticated answer is to quote the value of t itself, as it is (related to) a natural measure of "Markovianity". This is discussed in more detail in Ref. [7].

All the steps of Algorithm 26 also scale efficiently with the dimension of E, apart from solving the mixed integer semi-definite program in line 5. Since integer semi-definite programming is in NP, this (together with Theorem 7) proves the other main result of this section:

Theorem 30 *Solving* MARKOVIAN CHANNEL *or* MARKOVIAN MAP *is equivalent to solving P=NP: an efficient algorithm for* MARKOVIAN CHANNEL *or* MARKOVIAN MAP *would imply P=NP; conversely, P=NP would imply existence of efficient algorithms for* MARKOVIAN CHANNEL *and* MARKOVIAN MAP*.*

6 The Classical Problem

The classical analogue of the Markovianity problem is called the *embedding problem*, but it is much older, dating back to at least 1937 [16]. For a given stochastic matrix P, the problem is to determine whether or not P can be embedded into a continuous-time Markov chain, i.e. whether it is a member of a continuous-time, one-parameter semigroup of stochastic matrices. Equivalently, does there exist a generator Q such that $P = e^Q$ and e^{Qt} is stochastic for all $t \geq 0$?

There is a long literature on the embedding problem, of which we do not presume to give a comprehensive account here. (See [21] for a more extended history.) Simple necessary and sufficient conditions can easily be derived for 2×2 stochastic matrices (this result seems to originally have been reported by Kingman [17], who attributes it to Kendall), the 3×3 case was eventually solved [48–50], and certain properties are known for the general case [18, 19, 51]. However, the problem has remained open in general until now [20, 52].

In order to discuss the complexity of the problem in a rigorous sense, it is necessary to formulate the embedding problem as a weak-membership problem, analogous to MARKOVIAN CHANNEL or MARKOVIAN MAP, for the same reasons discussed in Section 3.1 in relation to the quantum problem:

Problem 31 (Embeddability)
Instance: (P, ε)*: Stochastic matrix* P*; precision* $\varepsilon \geq 0$*.*
Question: *Assert either that:*

- *for some matrix P' with $\|P' - P\| \leq \varepsilon$, there exists a generator Q' such that $P' = e^{Q'}$ and $e^{Q't}$ is stochastic for all $t \geq 0$;*
- *for some stochastic matrix P' with $\|P' - P\| \leq \varepsilon$, no such Q' exists.*

Again, we could also formulate a variant analogous to Markovian map, which drops the requirement that the given P be stochastic.

Now, stochastic maps are a special case of CPT maps in the following sense. The diagonal entries of a density matrix form a probability distribution, and every stochastic map can be extended to a CPT map whose action on the subspace of diagonal density matrices is the same as the action of the original stochastic map on the probability distribution formed by those diagonal elements. For example, we can take the composition of the CPT map that erases all off-diagonal elements of the density matrix, with the original stochastic map acting on the diagonal elements.

However, it does not follow that NP-hardness of the quantum problem implies NP-hardness of the embedding problem, as that would require precisely the opposite: encoding a CPT map into a stochastic map. But nor would NP-hardness of the embedding problem imply NP-hardness of the Markovianity problem, since the above argument showing that any stochastic map can be extended to a CPT map does not "preserve" embeddability (more precisely, it does not map the set of stochastic maps into the set of Markovian CPT maps, and the set of non-embeddable maps into the set of non-Markovian CPT maps). The embedding problem for stochastic matrices and the Markovianity problem for CPT maps are inequivalent problems, and the complexity of each must be resolved separately.

Fortuitously, it turns out that a proof of NP-hardness for the embedding problem is already "buried" within the NP-hardness proof for the Markovianity problem. We now give a sketch of the reduction from the NP-complete 1-in-3SAT problem to the Embeddability problem of Problem 31, which closely follows the analogous reduction to Markovian map. For a full account, see Ref. [21].

Recall the conditions for Q to be a generator of a continuous-time Markov chain (a *Q-matrix*): (i) $Q_{i\neq j} \geq 0$, (ii) $\sum_i Q_{i,j} = 0$. Comparing these with the conditions in Lemma 9 and Eqs. (34a) and (34b) satisfied by Q and B^c from Eqs. (31) and (32), we see that $Q_m = Q + 2\pi m_c B^c$ always satisfy the normalisation condition (ii) for any integers m_c. But, from Eq. (34a) and the discussion thereafter, Q_m will satisfy condition (i) for some m_c iff the original 1-in-3SAT used to construct Q and B^c was satisfiable. In other words, there exist integers m_c such that Q_m is a Q-matrix iff the 1-in-3SAT problem was satisfiable. But Q_m parametrise logarithms of the same matrix $P = e^{Q_m}$.

In fact, the only branches of the logarithm that are missing are branches that could never generate a continuous-time Markov chain in any case. So, either P is not stochastic (which can easily be checked), in which case the 1-IN-3SAT problem cannot be satisfiable, or P is stochastic, in which case it is embeddable iff the 1-IN-3SAT problem was satisfiable.

To make this reduction rigorous, Lemma 11 and Corollary 15 must be applied in very much the same way as in the reduction from LINDBLAD GENERATOR to MARKOVIAN MAP in Theorem 16, to show that a weak-membership formulation of the Q-matrix problem can be reduced to the weak-membership formulation of the EMBEDDABILITY problem (Problem 31). (See Ref. [21] for a detailed treatment.) Similar arguments to those given at the end of Section 4 show that the generalisation of the embedding problem to the problem of determining whether a family of stochastic matrices are all generated by the same continuous-time Markov process is also NP-hard, for any number of matrices. Finally, it is clear how to adapt the algorithm of Section 5 to the classical embedding problem, thereby proving equivalence to P=NP.

7 Conclusions

We have shown that the Markovianity problem for CPT maps and the analogous embedding problem for stochastic matrices are both NP-hard and, indeed, have shown full equivalence between solutions to these problems and a solution to the famous P=NP problem. Therefore, either P=NP, or there exists no efficiently decidable criterion for deciding whether a CPT map is generated by some underlying Markovian master equation, that is, whether it is a member of a completely positive semi-group. Similarly for deciding whether a stochastic matrix can be embedded in a continuous-time homogeneous Markov process.

An interesting corollary of the NP-hardness proofs for the MARKOVIAN CHANNEL and EMBEDDABILITY weak-membership problems is that:

Corollary 32 *Both the set of Markovian and the set of non-Markovian CPT maps have non-empty interior, hence non-zero measure, as do the sets of embeddable and non-embeddable stochastic matrices, in any finite dimension.*

So a randomly chosen CPT map has a finite probability of being non-Markovian, but also of being Markovian. The analogous property holds for a randomly chosen stochastic map. Ref. [7] estimates these probabilities numerically for the simplest quantum case of qubits, i.e. CPT maps on $\mathbb{C}^2$. This fact alone may not be so surprising: After all, generators being ccp can have neighbourhoods of generators that are ccp, which under exponentiation are mapped to neighbourhoods of channels, giving rise to a finite volume. The above corollary makes this argument rigorous.

One consequence of these results to physics is that to decide whether a given physical process at a shapshot in time—or for many snapshots for that matter—is consistent with being forgetful cannot be decided efficiently. This is because there is no *a priori* way of knowing whether the dynamics of an open system are Markovian or not, but finding the dynamical equations (master equations) would answer this question, and we now know this to be NP-hard for both the classical and quantum cases, requiring infeasibly long computation time (unless P=NP, of course). Whether this poses more practical difficulties is less clear. The results of Section 5 show that it at least does not pose a problem for the current generation of quantum experiments, since other purely practical limitations on the dimension of the systems being studied are more significant. More generally, one might argue that the average-case complexity is more relevant in practice, whereas NP-hardness only tells us about the worst-case complexity. What is the average-case complexity of the Markovianity and embedding problems? We close with this intriguing open problem, which we commend to the reader.

8 Acknowledgements

The authors would like to thank Ignacio Cirac for numerous valuable discussions relating to this work. TSC would like to thank Andreas Winter for asking about classical analogues, and to an anonymous QIP conference referee for pointing out a flaw in a previous treatment of the classical case, which observation ultimately led to the NP-hardness proof for the much older classical embedding problem. TSC also thanks Christina Goldschmidt and James Martin for devoting time and patience to answering his very basic questions about the relevant concepts in probability theory. TSC was supported by a Leverhulme early career fellowship, and by the European Commission QAP project, JE by the European Commission (QAP, MINOS, COMPAS) and the EURYI, and MMW by QUANTOP and the Danish Research Council.

References

[1] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* CUP, 2000.

[2] Howard J. Carmichael. *Statistical Methods in Quantum Optics*, volume 1. Springer, 2003.

[3] U. Weiss. *Quantum dissipative systems.* Series in Modern Condensed Matter Physics. World Scientific, 1999.

[4] G. Lindblad. On the generators of quantum dynamical semigroups. *Commun. Math. Phys.*, 48:119, 1976.

[5] V. Gorini, A. Kossakowski, and E. C. G. Sudarshan. Completely positive dynamical semigroups of N-level systems. *J. Math. Phys.*, 17:821, 1976.

[6] A. S. Holevo. *Statistical structure of quantum theory.* Springer, 2001.

[7] M. M. Wolf, J. Eisert, T. S. Cubitt, and J. I. Cirac. Assessing non-Markovian quantum dynamics. *Phys. Rev. Lett.*, 101:150402, 2008.

[8] N. Boulant, T.F. Havel, M.A. Pravia, and D.G. Cory. Robust method for estimating the Lindblad operators of a dissipative quantum process from measurements of the density operator at multiple time points. *Phys. Rev. A*, 67:042322, 2003.

[9] N. Boulant, J. Emerson, T. F. Havel, and D. G. Cory. Incoherent noise and quantum information processing. *Journ. Chem. Phys.*, 121(7):2955, 2004.

[10] M. Howard et al. Quantum process tomography and linblad estimation of a solid-state qubit. *New Journ. Phys.*, 8:33, 2006.

[11] Yaakov S. Weinstein et al. Quantum process tomography of the quantum fourier transform. *J. Chem. Phys.*, 121:6117, 2004.

[12] Daniel A. Lidar, Zsolt Bihary, and K. Birgitta Whaley. From completely positive maps to the quantum Markovian semigroup master equation. *Chem. Phys.*, 268:35, 2001.

[13] Christos H. Papadimitriou. *Computational Complexity.* Addison Wesley, 1993.

[14] M. R. Garey and D. S. Johnson. *Computers and Intractability: A Guide to the Theory of NP-Completeness.* W. H. Freeman, 1979.

[15] J. R. Norris. *Markov Chains.* CUP, 1997.

[16] G. Elfving. Zur theorie der Markoffschen ketten. *Acta Soc. Sei. Fennicae*, 2(8), 1937.

[17] J. F. C. Kingman. The imbedding problem for finite Markov chains. *Z. Wahrscheinlichkeitstheorie*, 1:14, 1962.

[18] J. F. C. Kingman and David Williams. The combinatorial structure of non-homogeneous Markov chains. *Z. Wahrscheinlichkeitstheorie*, 26:77, 1973.

[19] B. Fuglede. On the imbedding problem for stochastic and doubly stochastic matrices. *Probab. Th. Rel. Fields*, 80:241, 1988.

[20] Arunava Mukherjea. The role of nonnegative idempotent matrices in certain problems in probability. In Charles R. Johnson, editor, *Matrix theory and applications*. American Mathematical Society, Providence, R.I., 1990.

[21] Toby S. Cubitt. The embedding problem for stochastic matrices is NP-hard. (Manuscript in preparation).

[22] M.A. Nielsen, E. Knill, and R. Laflamme. Complete quantum teleportation using nuclear magnetic resonance. *Nature*, 396:52, 1998.

[23] L. M. K. Vandersypen and I. L. Chuang. NMR techniques for quantum control and computation. *Rev. Mod. Phys.*, 76:1037, 2004.

[24] J. Emerson et al. Symmetrized characterization of noisy quantum processes. *Science*, 317:1893, 2007.

[25] M. Riebe et al. Process tomography of ion trap quantum gates. *Phys. Rev. Lett.*, 97:220407, 2006.

[26] T. Monz et al. Realization of the quantum Toffoli gate with trapped ions. *Phys. Rev. Lett.*, 102:040501, 2009.

[27] J. L. O'Brien et al. Quantum process tomography of a controlled-not gate. *Phys. Rev. Lett.*, 93:080502, 2004.

[28] J. S. Lundeen et al. Tomography of quantum detectors. *Nature Physics*, 5:27, 2009.

[29] M. Howard et al. Quantum process tomography and Linblad estimation of a solid-state qubit. *New J. Phys.*, 8:33, 2006.

[30] M.D. Choi. Completely positive linear maps on complex matrices. *Lin. Alg. Appl.*, 10:285, 1975.

[31] A. Jamiolkowski. Linear transformations which preserve trace and positive semidefiniteness of operators. *Rep. Math. Phys.*, 3:275, 1972.

[32] Michael M. Wolf and J. Ignacio Cirac. Dividing quantum channels. *Commun. Math. Phys.*, 279:147, 2008.

[33] L.V. Denisov. Infinitely divisible markov mappings in quantum probability theory. *Th. Prob. Appl.*, 33:392, 1988.

[34] L. Gurvits. Classical deterministic complexity of Edmonds problem and quantum entanglement. In *Proceedings of the thirty-fifth ACM symposium on Theory of computing*, pages 10–19, New York, 2003. ACM Press.

[35] Lawrence M. Ioannou. Computational complexity of the quantum separability problem. *Quant. Inf. Comp.*, 7(4):335–370, 2007.

[36] Lieven Vandenberghe and Stephen Boyd. Semidefinite programming. *SIAM Rev.*, 38(1):49–95, 1996.

[37] Roger A. Horn and Charles R. Johnson. *Topics in Matrix Analysis.* CUP, 1994.

[38] T. Kato. *Perturbation Theory for Linear Operators.* Springer, second edition, 1976.

[39] J. Weilenmann. Continuity properties of fractional powers, of the logarithm, and of holomorphic semigroups. *Journ. Func. Anal.*, 27:1–20, 1978.

[40] C. Moler and C. Van Loan. Nineteen dubious ways to compute the exponential of a matrix, twenty-five years later. *SIAM Rev.*, 45:3–49, 2003.

[41] T. J. Schaefer. The complexity of satisfiability problems. In *Proceedings of the 10th Annual ACM Symposium on Theory of Computing (STOC'78)*, page 216, 1978.

[42] G. W. Stewart. Error and perturbation bounds for subspaces associated with certain eigenvalue problems. *SIAM Review*, 15(4):727–764, 1973.

[43] Gene H. Golub and Charles F van Loan. *Matrix Computations.* Johns Hopkins University Press, third edition, 1996.

[44] Roger A. Horn and Charles R. Johnson. *Matrix Analysis.* CUP, 1990.

[45] Alexander Schrijver. *Theory of Linear and Integer Programming*. Wiley, 1986.

[46] L. Porkolab and L. Khachiyan. Computing integral points in convex semi-algebraic sets. In *Proceedings of the 38th Annual Symposium on Foundations of Computer Science (FOCS '97)*, page 162. IEEE, 1997.

[47] L. Porkolab. *On the Complexity of Real and Integer Semidefinite Programming*. PhD thesis, Rutgers, 1996.

[48] James R. Cuthbert. The logarithm function for finite-state Markov semigroups. *J. London Math. Soc.*, 6(2):524, 1973.

[49] Søren Johansen. Some results on the imbedding problem for finite markov chains. *J. London Math. Soc.*, 8(2):345, 1974.

[50] Philippe Carette. Characterizations of embeddable 3x3 stochastic matrices with a negative eigenvalue. *New York J. Math.*, 1:120, 1995.

[51] James R. Cuthbert. On uniqueness of the logarithm for Markov semigroups. *J. London Math. Soc.*, 4(2):623, 1972.

[52] E B Davies. Embeddable Markov matrices. *Electronic J. Prob.*, 15:1474, 2010.