Linear Algebra and its Applications 504 (2016) 64–107

Contents lists available at ScienceDirect

Linear Algebra and its Applications

www.elsevier.com/locate/laa

The complexity of divisibility

Johannes Bausch [a,*], Toby Cubitt [a,b]

[a] DAMTP, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge CB3 0WB, UK
[b] Department of Computer Science, University College London, Gower Street, London WC1E 6BT, UK

A R T I C L E I N F O

Article history:
Received 17 April 2015
Accepted 24 March 2016
Available online 8 April 2016
Submitted by V. Mehrmann

MSC:
60-08
81-08
68Q30

Keywords:
Stochastic matrices
CPTP maps
Probability distributions
Divisibility
Decomposability
Complexity theory

A B S T R A C T

We address two sets of long-standing open questions in linear algebra and probability theory, from a computational complexity perspective: stochastic matrix divisibility, and divisibility and decomposability of probability distributions. We prove that finite divisibility of stochastic matrices is an NP-complete problem, and extend this result to nonnegative matrices, and completely-positive trace-preserving maps, i.e. the quantum analogue of stochastic matrices. We further prove a complexity hierarchy for the divisibility and decomposability of probability distributions, showing that finite distribution divisibility is in P, but decomposability is NP-hard. For the former, we give an explicit polynomial-time algorithm. All results on distributions extend to weak-membership formulations, proving that the complexity of these problems is robust to perturbations.

* Corresponding author.
E-mail addresses: jkrb2@cam.ac.uk (J. Bausch), t.cubitt@ucl.ac.uk (T. Cubitt).

http://dx.doi.org/10.1016/j.laa.2016.03.041

1. Introduction and overview

People have pondered divisibility questions throughout most of Western science and philosophy. Perhaps the earliest written mention of divisibility is in *Aristotle's Physics* in 350 BC, in the form of the *Arrow paradox*—one of *Zeno of Elea's* paradoxes (ca. 490–430 BC). Aristotle's lengthy discussion of divisibility (he devotes an entire chapter to the topic) was motivated by the same basic question as more modern divisibility problems in mathematics: can the behaviour of an object—physical or mathematical—be subdivided into smaller parts?

For example, given a description of the evolution of a system over some time interval t, what can we say about its evolution over the time interval $t/2$? If the system is stochastic, this question finds a precise formulation in the *divisibility problem* for stochastic matrices [19]: given a stochastic matrix $\mathbf{P}$, can we find a stochastic matrix $\mathbf{Q}$ such that $\mathbf{P} = \mathbf{Q}^2$?

This question has many applications. For example, in information theory stochastic matrices model noisy communication channels, and divisibility becomes important in *relay coding*, when signals must be transmitted between two parties where direct end-to-end communication is not available [23]. Another direct use is in the analysis of chronic disease progression [3], where the transition matrix is based on sparse observations of patients, but finer-grained time-resolution is needed. In finance, changes in companies' credit ratings can be modelled using discrete time Markov chains, where rating agencies provide a transition matrix based on annual estimates—however, for valuation or risk analysis, a transition matrix for a much shorter time periods needs to be inferred [17].

We can also ask about the evolution of the system for *all* times up to time t, i.e. whether the system can be described by some continuous evolution. For stochastic matrices, this has a precise formulation in the *embedding problem*: given a stochastic matrix $\mathbf{P}$, can we find a generator $\mathbf{Q}$ of a continuous-time Markov process such that $\mathbf{P} = \exp(\mathbf{Q}t)$? The embedding problem seems to date back further still, and was already discussed by Elfving in 1937 [10]. Again, this problem occurs frequently in the field of systems analysis, and in analysis of experimental time-series snapshots [7,22,27].

Many generalizations of these divisibility problems have been studied in the mathematics and physics literature. For example, the question of square-roots of (entry-wise) nonnegative matrices is an old open problem in matrix analysis [24]: given an entry-wise nonnegative matrix $\mathbf{M}$, does it have an entry-wise nonnegative square-root? In quantum mechanics, the analogue of a stochastic matrix is a completely-positive trace preserving (CPTP) map, and the corresponding divisibility problem asks: when can a CPTP map $\mathbf{T}$ be decomposed as $\mathbf{T} = \mathbf{R} \circ \mathbf{R}$, where $\mathbf{R}$ is itself CPTP? The continuous version of this, whether a CPTP can be embedded into a completely-positive semi-group, is sometimes called the *Markovianity problem* in physics [8]—the latter again has applications to subdivision coding of quantum channels in quantum information theory [26].

Instead of dynamics, we can also ask whether the description of the static state of a system can be subdivided into smaller, simpler parts. Once again, probability theory provides a rich source of such problems. The most basic of these is the classic topic of