The Complexity of Divisibility

Johannes Bausch[1], Toby Cubitt[1]

1 Background and Motivation

In this work, we address two of the most long-standing open topics on divisibility: quantum channel and stochastic map divisibility, as well as divisibility and decomposability of probability distributions. We focus on the issue of computational complexity, and show which one of those questions we are able to solve efficiently, proving reductions to the famous P=NP-conjecture for the other cases.

CPTP and Stochastic Map Divisibility. The theory of stochastic processes plays an essential role in describing systems undergoing classical random dynamics. One of its main proponents are discrete time Markov chains, described by stochastic matrices, which are researched and applied in an extensive range of fields [Bas11]. The quantum analogue of stochastic processes—quantum channels—are used to describe physical systems with open quantum evolution, i.e. dissipative quantum systems. Such quantum channels are represented by linear trace preserving completely positive (CPTP) maps. Quantum channels are used ubiquitously in physics to model noisy quantum evolution, especially in the field of quantum information [NC10, Ch. I].

Both stochastic processes and quantum channels are used to describe a system evolution over a specific time interval T. An immediate question to ask is thus if there exists such a stochastic transition matrix or CPTP map describing how the system evolved in smaller time steps—say to time $T/2$. *More precisely, given a matrix or channel* $\mathbf{P}$*, can we factor it into the product* $\mathbf{P} = \mathbf{Q}^2$*, such that* $\mathbf{Q}$ *represents the evolution to this intermediate time* $T/2$*?*

Already the classical case is highly non-trivial. Historically, this has been a long-standing open problem, dating back at least as early as 1962 [Kin62]. The most complete result to date is a full characterization of 2×2 matrices (!), as given for example in [HG03].

The foundations for quantum channel divisibility were laid with [WC08]. *As in the classical case, the question of finite divisibility of* CPTP *maps is still an open question.*

Distribution Divisibility and Decomposability. Underlying stochastic and quantum channel divisibility—and a more fundamental topic to address—is the question of divisibility and decomposability of probability distributions and random variables.

To be more precise, a random variable X is said to be *divisible* if it can be written as $X = Y + Z$, where Y and Z are non-constant identically distributed independent random variables (iid), where n-divisibility is defined in a similar fashion. Analogously, *infinite divisibility* refers to the case where X can be written as an infinite sum of such iid random variables. Relaxing the condition that Y and Z be iid, and asking only whether X can be divided at all, we obtain the much weaker notion of *decomposability*.

[1] DAMTP, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge CB3 0WB, UK

Divisibility and decomposability have been studied extensively in various branches of probability theory and statistics. Early examples include *Cramer's theorem* [Cra36], proven in 1936, a result stating that a Gaussian random variable can only be decomposed into random variables which are also normally distributed. A related result on χ^2 distributions by *Cochran* [Coc34], dating back to 1934, has important implications for the analysis of covariance.

From a statistical and computational perspective, however, there does not yet exist a straightforward way of checking whether a discrete distribution is divisible or decomposable.

2 Main Results and Techniques

CPTP and Stochastic Map Divisibility. The following theorems summarize our main results on maps.

Theorem 1. *Given a (doubly) stochastic matrix* $\mathbf{P}$*, answering whether there exist a (doubly) stochastic matrix* $\mathbf{Q}$ *such that* $\mathbf{P} = \mathbf{Q}^2$ *is NP-hard.*

Theorem 2. *Given a* CPTP *map* $\mathbf{B}$*, answering whether there exist a* CPTP *map* $\mathbf{A}$ *such that* $\mathbf{B} = \mathbf{A}^2$ *is NP-hard.*

The proofs are based on a reduction of a well-known NP-complete problem—boolean satisfiability, or 1-IN-3SAT—to the question of divisibility of non-negative matrices.

To be more precise, starting from a 1-IN-3SAT instance, a non-negative matrix $\mathbf{M}$ is explicitly constructed, such that $\mathbf{M}$ is divisible if and only if the embedded 1-IN-3SAT instance can be answered with YES. The construction, being fairly involved, consists of multiple steps. First we need to translate the 1-IN-3SAT instance to the entry-wise non-negativity constraint of the root of $\mathbf{M}$. One difficulty to overcome is that every boolean term translates into two inequalities, which means we have to couple pairs of eigenvalues in such a fashion that non-negativity is necessarily broken if these pairs deviate. We then ensure to mask all unwanted inequalities and lift singularities, while ensuring that the bit complexity only grows polynomially.

Theorem 1 is proven using an embedding of $\mathbf{M}$ into a larger doubly stochastic matrix, ensuring the additional normalization condition, whereas theorem 2 follows using the *Choi*-isomorphism.

Distribution Divisibility and Decomposability. The following theorems summarize our main results on distributions.

Theorem 3. *Let* X *be a finite discrete random variable. Answering whether* X *is* n*-divisible is in P.*

Theorem 4. *Let* X *be a finite discrete random variable, and* $\epsilon > 0$*. Answering whether there exists a random variable* Y ϵ*-close to* X *such that either* Y *is* n*-divisible—or nondivisible—is in P.*

Theorem 5. *Let* X *be a finite discrete random variable. Answering whether* X *is decomposable is NP-hard.*

Theorem 6. *Let* X *be a finite discrete random variable, and* $\epsilon > 0$*. Answering whether there exists a random variable* Y ϵ*-close to* X *such that either* Y *is decomposable—or indecomposable—is NP-hard.*

In order to prove the above results, we define a new quantity associated with discrete distributions, the so-called *characteristic polynomial*, which is closely related to the *Mellin* transform of the probability mass function. In contrast to the *Fourier* or *Laplace* transform, the characteristic polynomial exposes the algebraic structure of the distribution and allows us to use powerful algebraic methods to address the problem at hand.

For theorem 3 and 4, we construct an algorithm based on a *Taylor* expansion of this characteristic polynomial, which allows us to answer the divisibility question of the associated random variable X in polynomial run-time, and in case of a YES-answer, enables us to explicitly calculate the n^{th} root—exactly, or the closest one in any suitable norm. It in fact answers a dual question as well, i.e. the distance of X to the closest n-divisible random variable.

In a similar fashion to the hardness results of maps, we further embed a series of NP-complete problems—variants of Subset Sum and Partition—into characteristic functions. For theorem 5, we then show that the corresponding distributions are decomposable if and only if the embedded hard instance can be answered with YES.

The proof, being significantly more involved, makes use of various algebraic properties of polynomials—an example is the algebraic variety defined by the roots of the characteristic polynomial, which induces a locally smooth isomorphism to the associated probability distribution. This additional structure allows us to extend the result to the weak formulation given in theorem 6.

Finally, for the continuous case, we prove that both non-divisible and indecomposable distributions are dense in the set of all distributions. Therefore, in this setting, the weak membership version of divisibility and decomposability can be trivially answered. Moreover, this shows that the question of infinite divisibility—which only makes sense for continuous random variables—is trivial as a computational problem.

3 Relevance and Conclusion

In addition to solving historically long-standing open questions in mathematics—yielding a *complete complexity hierarchy* for divisibility and decomposability for probability distributions, discrete and continuous—the constructive nature of our proposed algorithms on distributions are valuable for a range of applications [SK79]. One example of n-divisibility is in modelling, for example of bug populations in entomology, or in financial aspects of various insurance models. Both examples regard the overall distribution and ask if it is compatible with the underlying subdivision into smaller random events.

For maps, both infinite divisibility problems in the classical and quantum case—known as *Elfving's* or *embedding* problem[Elf37] and *Markovianity* condition on a CPTP map, respectively—have recently been shown to be NP-hard to solve [CEW12]. With our new results, there now exists a *full characterization* of infinite and finite divisibility for stochastic maps and quantum channels.

A notable surprise is the different complexity for divisibility, which is an NP-hard problem for maps, but lies in P for distributions.

Finally, the new idea of characteristic polynomials has proven very fruitful. While related in nature to characteristic and moment-generating functions, the use of polynomials emphasizes the algebraic structure of the distribution and allows for a new perspective to address problems, which might be useful for other applications as well.

References

[Bas11] Richard F. Bass. *Stochastic Processes.* 1st ed. Cambridge University Press, 2011, p. 404.

[CEW12] Toby S. Cubitt, Jens Eisert, and Michael M. Wolf. “The Complexity of Relating Quantum Channels to Master Equations”. In: *Communications in Mathematical Physics* 310.2 (Jan. 2012), pp. 383–418.

[Coc34] W. G. Cochran. “The distribution of quadratic forms in a normal system, with applications to the analysis of covariance”. English. In: *Mathematical Proceedings of the Cambridge Philosophical Society* 30.02 (Oct. 1934), pp. 178–191.

[Cra36] Harald Cramér. “Über eine Eigenschaft der normalen Verteilungsfunktion”. In: *Mathematische Zeitschrift* 41.1 (Dec. 1936), pp. 405–414.

[Elf37] Gustav Elfving. “Zur Theorie der Markoffschen Ketten”. In: *Acta Soc. Sci. Fennicae n. Ser. A* 2.8 (1937), pp. 1–17.

[HG03] Qi-Ming He and Eldon Gunn. “A note on the stochastic roots of stochastic matrices”. In: *Journal of Systems Science and Systems Engineering* 12.2 (June 2003), pp. 210–223.

[Kin62] John Frank Charles Kingman. “The imbedding problem for finite Markov chains”. In: *Probability Theory and Related Fields* 24.iV (1962), pp. 14–24.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information.* Cambridge University Press, 2010, p. 676.

[SK79] FW Steutel and JT Kent. “Infinite divisibility in theory and practice”. In: *Scandinavian Journal of . . .* 6.2 (1979), pp. 57–64.

[WC08] Michael M. Wolf and J. Ignacio Cirac. “Dividing Quantum Channels”. In: *Communications in Mathematical Physics* 279.1 (Feb. 2008), pp. 147–168.