RESEARCH CENTRES

Inria Lyon Centre

Inria Centre at Université Grenoble Alpes

IN PARTNERSHIP WITH:

Ecole normale supérieure de Lyon,
Université Claude Bernard (Lyon 1),
Université de Grenoble Alpes

2024
ACTIVITY REPORT

Project-Team
QINFO

Optimal Information Processing with Quantum Devices

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Algorithmics, Computer Algebra and Cryptology

Contents

Project-Team QINFO

Creation of the Project-Team: 2022 September 01

Keywords

Computer sciences and digital sciences

- A4.2. – Correcting codes
- A4.3.4. – Quantum Cryptography
- A7.1.4. – Quantum algorithms
- A7.3.1. – Computational models and calculability
- A8.6. – Information theory

Other research topics and application domains

- B5.11. – Quantum systems

1 Team members, visitors, external collaborators

Research Scientists

- Omar Fawzi [Team leader, INRIA, Senior Researcher]
- Alastair Abbott [INRIA, Researcher]
- Akshay Ramachandran [INRIA, Starting Research Position, from Oct 2024]
- Daniel Stilck Franca [INRIA, ISFP, until Aug 2024]
- V. Vilasini [INRIA, Researcher, from May 2024]
- Mischa Woods [INRIA, Researcher]

Faculty Member

- Guillaume Aubrun [UNIV LYON I, Associate Professor]

Post-Doctoral Fellows

- Tushar Bag [INRIA, Post-Doctoral Fellow]
- Qian Chen [INRIA, Post-Doctoral Fellow]
- Ngoc Hoang Anh Mai [INRIA, Post-Doctoral Fellow]
- Mizanur Rahaman [INRIA, Post-Doctoral Fellow]
- Sujit Rao [INRIA, Post-Doctoral Fellow, from Oct 2024]

PhD Students

- Pablo Alvarez Dominguez [UGA, from Jul 2024]
- Emily Beatty [INRIA]
- Emilien De Bank [UGA, from Oct 2024]
- Idris Delsol [INRIA, from Oct 2024]
- Amanda Maria Fonseca [UGA, from Dec 2024]
- Maarten Grothus [INRIA]
- Raphael Le Bihan [UGA, from Oct 2024]
- Tristan Le Roy-Deloison [INRIA, until Jun 2024]
- Victor Martinez [IBM, CIFRE]
- Raphael Mothe [CNRS, until Sep 2024]
- Pierre Pocreau [UGA]
- Mostafa Taheri [INRIA]

Interns and Apprentices

- Raphael Le Bihan [ENS PARIS-SACLAY, Intern, from Feb 2024 until Aug 2024]
- Corentin Moumard [INRIA, Intern, from Jun 2024 until Aug 2024]
- Thomas Perez [INRIA, Intern, from Feb 2024 until Jul 2024]

Administrative Assistants

- Elise Denoyelle [INRIA, Lyon]
- Maria Immaculada Presseguer [INRIA, Grenoble]

2 Overall objectives

Information-processing devices that can take advantage of the laws of quantum theory have an important potential in terms of computation, communication and secrecy. However, the quantum devices available today are all affected by unwanted noise: the actual behavior of the device only matches approximately with the model they were designed for. Such an unwanted deviation from the model can have devastating effects for the information processing applications: for example, in the context of quantum computation, the accumulation of noise can render the outcome of the computation completely useless. QINFO's research aims to develop methods and algorithms to optimally reduce the undesirable effect caused by noise on quantum information processing tasks, and to use fundamental concepts to explore new models that could allow quantum resources to be used to their full potential.

3 Research program

Our overarching objective is to develop mathematical techniques and algorithms to make full use of the potential of quantum technologies. Our research is decomposed into three research directions. The first axis aims to develop methods to characterize and certify the relevant quantum properties of currently available quantum information processing devices, including so-called noisy intermediate scale quantum (NISQ) devices, as well as explore their applications. The second axis is motivated by applications on a longer time scale and its objective is to develop general methods to correct the errors that occur in quantum devices and reduce/eliminate their effect on the computations. The third axis considers new quantum models and resources that promise to help in finding new applications of quantum technologies.

3.1 Axis 1: Characterization, certification and applications of noisy quantum devices

The last years have seen a dramatic increase in both the size and quality of quantum computing architectures. They have now reached a point where they are very hard to simulate even with the best classical computers available. Nevertheless, significant challenges have to be overcome to scale current technologies and use them to solve practically relevant problems. The first challenge is in obtaining accurate mathematical models of such quantum devices, including their inevitable imperfections. The second challenge is in understanding the information processing abilities of such models. The objective of this research axis is to tackle these two challenges by designing efficient methods for the characterization and certification of quantum devices, exploring the limitations imposed by noise on the computational power and studying the applications of current quantum devices to optimization algorithms and to device-independent cryptography.

3.1.1 Efficient methods for testing and characterizing quantum systems

Obtaining an accurate mathematical characterization of the quantum systems that are prepared in the lab is a pressing question for quantum technologies. For this reason, there has been very important progress on such statistical questions in the last few years. This includes the answer to foundational questions such as the number of samples needed to characterize an unknown quantum state, improved methods for characterizing quantum devices, and very recently techniques that can very efficiently predict multiple relevant properties of quantum systems. We plan to contribute to these lines of work by considering several questions all going in the direction of better characterization of quantum systems.

First, we will consider **basic statistical questions related to testing relevant properties** of quantum states. In particular, given a description of an ideal target state $|\psi\rangle$, how to efficiently test whether the state prepared by the device complies with $|\psi\rangle$? Another question is how to test whether the state prepared by the device is entangled or not? These are fundamental questions and for some of them the best known algorithm is to learn the whole state by performing a complete quantum tomography. We believe that this is far from optimal and that a better understanding of the geometry of quantum states can be turned into a significantly more efficient testing algorithm. Techniques from high-dimensional convex geometry [61] are likely to play an important role.

Building on that, we will then develop tools to characterize the noise affecting quantum devices. As the number of parameters and samples required to characterize an arbitrary noisy process grows exponentially in the number of qubits [97], it is of paramount importance to devise protocols to find an effective ansatz for the underlying structure. The first step we will take in this direction will be to devise scalable protocols that are able to **identify the correlation structure of the noise**. By singling out on which parts of the device the noise acts independently and on which the noise is correlated it is possible to substantially reduce the number of parameters that are required to effectively describe it, bringing it to a tractable number. Although finding the conditional independence structure of a set of random variables to a high precision is a difficult problem even classically, we will generalize to the quantum setting efficient classical techniques that employ convex relaxations [77] to obtain good approximate solutions.

The next step will then be to devise protocols inspired from machine learning techniques that can exploit the knowledge of the underlying correlation structure to efficiently learn its parameters. This will be combined with randomized benchmarking techniques [88, 92, 86]. Randomized benchmarking techniques are known to be robust and experimentally friendly, however current results either give very limited information or require stringent assumptions on the structure of the underlying noise. Thus, the goal of this part will be to overcome these two limitations, providing experimentalists with much needed tools to efficiently characterize large noisy quantum devices.

Such a line of research certainly also profits from inputs from experimentalists to **test the algorithms on real quantum hardware**. Thus, we plan to work with the local experimental group led by Benjamin Huard to test such methods on the devices they build. Moreover, it is invaluable to obtain input from experimentalists regarding what are the limitations and challenges they face in the lab when characterizing their devices.

An important aspect in this direction that we will consider is the design of measurements that can probe the physical property of interest without disturbing the state by much. This is the so-called **quantum non-demolition measurement** (QND) and is important when one has a continuous signal which one wants to measure, since one has to measure the same system repeatedly over time and, ideally, one wants the outcomes of later measurements to depend solely on the quantity one intends to measure, and not on any disturbances caused by prior measurements. QNDs have found usages in many areas, including quantum computing and, most prominently, proposals for gravitational wave detectors with improved sensitivity. We view the problem through the lens of quantum information theory, and in this way, it can be seen that the quantum system involved in the QND, is a quantum reference frame. What's more, there is a one-to-one relation between the reference frame imperfections, and its ability to act as a system for QND measurements. In [65, 115], we gave a construction of a QND where the error is a function of energy and dimension. Going forward, our objective is to determine whether this construction is optimal, determine the optimal tradeoff between error and energy and dimension and assess the extent to which such constructions can lead to an advantage for **quantum sensing**.

3.1.2 Limitations on the computational power of noisy quantum devices

In order to establish a quantum advantage for noisy quantum computers, it is important to study when **noisy quantum computers can be simulated classically**. Intuitively, it is clear that the noise present in a quantum device imposes a limit on the circuit depth we can implement before the device loses its usefulness when compared to classical devices. In order to understand the potential of noisy quantum devices, it is crucial to develop tools to characterize when this happens given a problem and noise model. In the context of optimization, such bounds were achieved by our work [87]. In short, the results of [87] show that sampling from the output of noisy quantum devices quickly becomes comparable to sampling from Gibbs states that are easy to simulate classically by giving stringent explicit bounds. This is showcased Figure 1, where we plot at which density of corrupted qubits the noisy quantum device loses advantage against classical methods. However, in their current version, our methods only allow for an

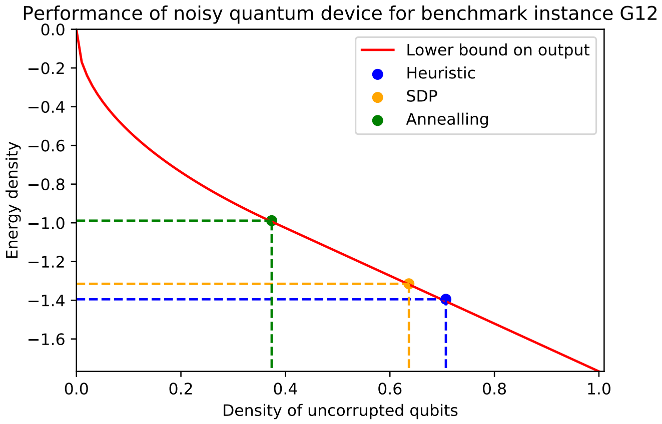

Figure 1: Estimate as to when a noisy quantum device loses advantage compared to established efficient classical methods in terms of the density of uncorrupted qubits for one instance of the GSET (a set of instances of hard combinatorial optimization problems that are used to benchmark solvers). We see that even when only a fraction of the qubits have been corrupted (roughly one in 4), the noisy quantum computer is already expected to loose advantage against heuristic methods.

analysis of the first moments. To extend the analysis and conclusions beyond optimization to other fields like quantum machine learning, it is imperative to obtain results for higher moments and concentration inequalities for the outputs of noisy quantum circuits. That is, to quantify how much noise a quantum system can tolerate before it behaves like a state that can be easily sampled from classically. To achieve this goal, we intend to resort to and further develop methods from the emerging field of quantum optimal transport [102, 78]. Optimal transport techniques are by now a well-established method to show powerful concentration inequalities [108]. They are known to combine well with other areas of expertise of the group, such as entropic and semigroup methods.

3.1.3 Efficient optimization using noisy quantum computers

Identifying good use cases for the noisy quantum devices expected to be available in the near future is one of the main current challenges faced by the quantum computing community. One possible candidate for such an application are quantum Gibbs state-sampling based methods. Quantum Gibbs states are at the core of powerful classical and quantum algorithms for optimization and machine learning based on mirror descent or the matrix multiplicative weight method [70, 66, 67]. These iterative algorithms can be understood as a variation of simulated annealing, in which one starts with a (quantum) Gibbs state at infinite temperature and decreases the temperature to converge to the solution of an optimization problem. That is, we begin with a state that is supported everywhere on the state space and slowly zoom into regions that contain solutions to the problem of interest by tuning the Gibbs state. This intuitive picture conveys one feature of such methods: they are robust, especially at the first iterations, as we only need to ensure that we are zooming in the right direction. This robustness translates into them only requiring the preparation of states with relatively small precision to make progress.

On the other hand, this picture also showcases the issue noise imposes for such methods: after a while, the noise will make it impossible to zoom in further, imposing fundamental barriers onto how well we can characterize the region of solutions. Thus, it is expected that noisy quantum computers can offer useful advice as to which direction to go up to a level that naturally depends on the noise present in the device. Thus, we will design hybrid quantum-classical algorithms that explicitly take into account this limitation. They will only use the quantum computer to identify a region of a relatively small dimension that contains the solution.

At this stage, it is then possible to use powerful randomized linear algebra techniques to take advantage of the initial zooming in performed by the noisy quantum device. Techniques from randomized linear algebra offer significant speedups for basic operations under the promise that the involved matrices are supported on a small dimensional space [113]. Thus, after doing the first iterations efficiently on the noisy quantum device and identifying a low-dimensional space that contains the solutions, a classical device takes over with this input and runs the later iterations much faster. Such a hybrid algorithm would lead to more efficient solvers for convex optimization problems. Although such problems can usually be solved in polynomial time, in practice it is still challenging to solve larger dimensional instances, impeding their more widespread use. **Such a hybrid algorithm will increase the practicality of solving large-dimensional semidefinite programs, as the classical computer would only have to operate in the low-dimensional regime.** It would also lead to provable speedups for quantum devices under noise, a goal that has so far remained elusive.

The main technical challenges that need to be overcome for the success of such an algorithm are threefold: first, carrying out a detailed analysis of the trade-offs as to when it becomes more efficient to transition from performing the optimization on the noisy quantum device to the classical computer. Second, the development of improved quantum Gibbs sampler for noisy devices to prepare the required states. Third, the identification of practically relevant problems that offer a good opportunity window for quantum speedups. The first and third challenges will profit from and are connected to the result of the previously discussed Goals 3.1.1 and 3.1.2. The second, the development of better quantum Gibbs samplers, as current proposals for Gibbs samplers require quantum circuits that are unlikely to be implementable in the near term, will certainly yield results that find applications in many other directions. Indeed, efficient classical Gibbs samplers are the bread the butter of most Monte Carlo techniques, and it is to be expected that quantum Gibbs samplers will find similar widespread application.

3.1.4 Certification of quantum devices

In the **device-independent framework** of quantum cryptography, protocols offer security by relying on minimal assumptions. Namely, they are secure even when the devices used within the protocol are completely untrusted or uncharacterized. The main idea behind many device-independent protocols, such as randomness expansion and quantum key distribution, is that there are certain correlations between multiple separate systems that (i) could only have been produced by entangled quantum systems and (ii) are intrinsically random. The fundamental question underlying the analysis of such protocols is how to certify entanglement or randomness from the observed measurement statistics of the untrusted device?

This question of certification is recurrent when assessing the behaviour of quantum devices (and particularly of noisy ones), as highlighted by the issues that Goals 3.1.1 and 3.1.2 address. We plan to develop techniques to address the certification of quantum systems with minimal assumptions. Our objective is to first build mathematical tools in the continuity of the Entropy Accumulation Theorem [**81**] that allow us to make accurate statistical statements about large quantum systems. The second objective is to design computational methods [**69**] to certify in a quantitative way the relevant quantum properties that are consistent with the observed statistics.

For the context of device-independent cryptography, this will allow us to obtain protocols with improved noise tolerance and finite-length analysis to reach the realm of what can be done with current quantum technologies. But we believe these techniques will be applicable in the wider setting of **certifying properties of quantum networks and quantum computing devices**.

3.2 Axis 2: Error correction methods for quantum information processing

Noisy quantum devices are unlikely to reach the full potential of quantum computation unless some software mechanisms for correcting the errors are used. The aim of this research axis is to develop general methods to use physical quantum devices to perform logical quantum operations that are reliable even if the physical devices themselves are imperfect.

For this, we plan to build algorithmic methods to find error correction mechanisms that are tailored to a given noise model, and explore various approaches to fault-tolerant quantum computation going from Low-Density Parity-Check quantum codes to more recent methods using quantum reference frames.

3.2.1 Optimal error correction tailored to noise model

Shannon's 1948 seminal theorem [104] modeled the problem of communication (or storage) over a given noisy channel and determined precisely its ultimate limit. Shannon's noisy coding theorem relates the maximum rate at which information can be transmitted reliably over a noisy channel $\mathscr{W}_{X\to Y}$ to a simple entropic expression $I(X:Y)$ measuring the correlations between the input and output of the channel. More precisely, it states that as $n\to\infty$, the maximum number of bits that can be sent using n independent copies of $\mathscr{W}_{X\to Y}$ is asymptotically given by

$$\lim_{n\to\infty}\frac{\text{Maximum number of bits communicated using }\mathscr{W}_{X\to Y}^{\otimes n}}{n} = \max_{P_X} I(X:Y)\,, \tag{1}$$

where the right hand side is a maximization over distributions P_X over the input of the channel and $I(X:Y)$ is a correlation measure, the exact definition of which we will omit in this document. Setting the fundamental limits for reliable communication, Shannon's theorem was instrumental in the discovery of good error correcting codes which are used in virtually every device or communication link today. One of the goals of the field of information theory is to characterize the optimal communication rates in the form (1) for various information processing tasks.

Devices that make use of the laws of quantum theory are also affected by noise, in fact even more so. Determining the optimal method in order to communicate (or store information) reliably over a noisy quantum channel is thus of fundamental importance in order to exploit the full potential of a quantum computer, or more generally a quantum device. However, despite the problem's importance and more than 40 years of efforts in quantum information theory [94, 112], it is fair to say that we do not have a quantum analogue of Shannon's theorem Eq. (1). Indeed, a formula analogous to Eq. (1) for quantum channels is known only in very special cases. As an illustration, even for the simplest possible quantum channel, called the qubit depolarizing channel, the asymptotic maximum rate of quantum communication is still unknown [79]. The qubit depolarizing channel can be thought of as the quantum analogue of the channel that flips the input bit with some probability f.

The main difficulty in understanding the ability of a quantum channel in transmitting information is the *non-additivity* of the quantum entropic quantities having the form of the right hand side of Eq. (1) [79, 95, 93, 105]. This challenge is due in many cases to the quantum property of entanglement and we believe that a new approach is needed to overcome this difficulty.

Faced with these difficulties, we propose a new framework for studying communication over noisy channels. Instead of trying to determine the optimal rate of communication *asymptotically* as the number of channel uses $n\to\infty$ (as in the left hand side of Eq. (1)), we assume we have a description of a finite channel $\bar{\mathscr{W}}_{\bar{X}\to\bar{Y}}$ (a particular case of which is $\bar{\mathscr{W}}_{\bar{X}\to\bar{Y}} = \mathscr{W}_{X\to Y}^{\otimes n}$ for some finite n, but it could be much more general). Our objective is then to design an *efficient algorithm* that determines the maximum number of bits or qubits that can be sent reliably using $\bar{\mathscr{W}}_{\bar{X}\to\bar{Y}}$.

For the problem of classical communication over a classical channel, we have characterized this computational complexity precisely in our previous work **[64]** and this led to interesting connections between information theory and combinatorial optimization. The main objective here is to extend this approach to quantum channels, thereby designing algorithms that can find **the best error correction schemes for a given noise model**. These algorithms can naturally then be used on the noise models that are estimated using the methods developed in Axis 3.1.1. In particular, we will focus on relevant noise models that appear in current devices. For this we plan to collaborate with Benjamin Huard in the physics lab of ENS Lyon, and the presence of Cyril Élouard in the team significantly helps in this regard. To start in this direction, Cyril has given talks within the group to explain the mathematics of superconducting qubits and we are at the moment discussing specific dissipative models that can be reasonably implemented in hardware and for such different models compare their ability to store quantum information reliably.

3.2.2 Error correction and fault-tolerance with LDPC codes

Having a coding strategy for a given noise model with good performance is not enough: for a strategy to be applicable, it is important to be able to implement the error correction operations efficiently. An efficient decoding algorithm is not only important to establish fast and reliable communication networks but it is also crucial for fault-tolerant computing. In fact, the basic idea of fault-tolerant computing schemes is to perform computations on data encoded in an error correcting code. To prevent the errors that occurred during the computation from spreading, a decoding operation has to be regularly applied to correct these errors. For this reason, it is crucial for the decoding operation to be very fast to prevent the accumulation of errors. We focus here on an important class of quantum error correcting codes called Low-Density Parity-Check (LDPC) codes [71, 106] defined by two *sparse* binary parity-check matrices H_X and H_Z satisfying $H_X H_Z^T = 0$. Our first objective is to design **efficient decoding algorithms for quantum LDPC codes**.

Quantum LDPC codes are particularly well suited to achieve *fault-tolerant* quantum computation. This is because the sparsity of the parity check matrices allows us to bound the error rate of the syndrome measurements. In fact, currently the leading candidate error correcting code to be used in future quantum computers is the surface code, a special kind of LDPC code. Even though the surface code can be embedded on a surface with only nearest neighbour interactions, it suffers from a very poor encoding rate, and thus using it for fault-tolerant constructions incurs a very large memory overhead. Our previous work [**85**] shows that in principle the memory overhead can be significantly reduced by using constant-rate LDPC codes based on expander graphs. The general idea of using constant-rate codes is illustrated in Figure 2. Our objective is to make **fault-tolerant constructions with LDPC codes practical** by finding fault-tolerant gadgets for such codes and using decoding algorithms with better performance.

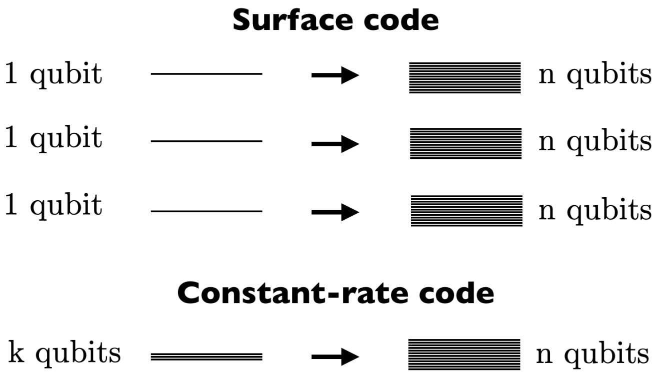

Figure 2: When using the surface code for fault-tolerance, each qubit of the original circuit is encoded in a separate block, leading to a large memory overhead. When using constant-rate codes, all the qubits of the original circuit are encoded in the same block which leads to important savings in terms of overhead.

3.2.3 New approaches for fault-tolerance

As mentioned before, the currently leading approach for fault-tolerance is using surface codes. In contrast to the previous goal 3.2.2, our objective here is to explore radically different approaches to fault-tolerance that could provide new avenues towards achieving fault-tolerance. In particular, we will look at one based on quantum polar codes and the other one based on quantum reference frames.

The class of **quantum polar codes** that has recently been proposed in [82] can be promising candidates for fault-tolerant quantum computing. The construction relies on a channel combining and splitting procedure, where a two-qubit gate randomly chosen from the Clifford group is used to combine two single-qubit channels. Applied recursively, this procedure allows synthesizing a set of so-called virtual channels from several instances of the quantum channel. When the code length goes to infinity, the virtual channels polarize, in the sense that they tend to become either noiseless or completely noisy. Interestingly, polar codes feature several extremely desirable properties: they protect a high number of logical qubits, and they have efficient decoding algorithms. In addition, logical Clifford operations can be easily performed by using code deformation like techniques. However, there are a number of challenging issues to be addressed in the fault-tolerant computing context. First, quantum channel polarization needs to be investigated by taking into account the fact that Clifford gates used for channel-combining are faulty. Second, we need to construct a universal set of fault-tolerant gates, which can be tackled by using magic state distillation. For this approach, we plan to collaborate closely with Mehdi Mhalla (CNRS, LIG).

The second approach we consider here is based one a way of **circumventing the famous Eastin-Knill theorem**. In the early days of quantum computing, one of the key ideas for building a quantum computer whose errors can be corrected, was the notion of transversal logic gates. The idea was to devise a scheme in which all the gates needed for universal quantum computation could be applied on non-overlapping subspaces in such a way that all the locally occurring errors were correctable. More specifically, the objective is to find an encoding $\mathcal{E}$ mapping the logical space to the physical space such that for any unitary $\mathcal{V}$ acting on the logical space, there exist unitaries $\mathcal{V}_1, \ldots, \mathcal{V}_n$ acting on the physical space such that

$$\mathcal{E} \circ \mathcal{V} = \mathcal{V}_1 \otimes \cdots \otimes \mathcal{V}_n \circ \mathcal{E}\,.$$

This scheme would allow for errors in the implementation of the gates to be corrected before they have propagated through the computation and rendered its results useless. Unfortunately, transversality of all the gates needed for universal computation and local correctability within the blocks cannot both be simultaneously satisfied for finite dimensional codes. This was proven by Eastin and Knill in a landmark paper in 2009 [83]. Subsequently, workarounds have been found. For example, one of the current frontrunner approaches is to apply all but one of the gates needed for universal computation transversally, while the remaining gate is applied in a non-transversal way using other costly techniques.

We have developed in a series of two papers [**114, 116**], a new method for quantum error correction which is not based on this approach. In this technique, all of the gates in the set needed for universal computation are treated on an equal footing. More precisely, rather than circumventing the Eastin-Knill theorem by having one non-transversal gate, all gates from the universal set can be applied transversally, and local errors corrected, but at the price of an error in the decoding. As long as the error in the decoding is kept small, it will not disrupt the computation and is thus not significant from a practical point of view. To do so, it uses quantum reference frames and randomness to encode the information about which gate was applied during the computation. As the quality of the reference frame increases, the error in the decoding approaches zero. The concept of a quantum reference frame was introduced in the field of quantum foundations in the context of sharing so-called "unspeakable information", such as the relative orientation of two distant observes. While it has been used over the years in various problems in quantum information theory, its use in quantum error correction has yet to be fully explored.

While this work on the circumvention of the Eastin-Knill theorem has attracted a lot of attention and follow up work by other research groups (see e.g. Refs. [99, 117, 109] and [98]), it is not yet ready for primetime. The reason for this, it that while the encoded states are readily fault tolerant (due to the transversality of its gates), the current protocol for applying the encoding and decoding channels are not fault tolerant. This is down to the method in which the quantum reference frames are constructed. However, we believe that finding protocols for implementing the encoder and decoder in a fault tolerant way is a surmountable challenge. We plan to use a recent construction of unitary t-designs that use a constant number of non-Clifford gates. Implementing the Clifford gates in the circuit can be done in a transversal way and for the non-Clifford gates, a constant number of magic states can be used. This is analogous in some ways to the entanglement needed to perform magic state distillation [68], which is the building block of one of the leading proposals for fault tolerant quantum computation. However, there are many potential benefits to the proposed use of the initial entanglement resource over that of the magic state distillation approach — it is these benefits, which are the key to why this approach could become the chosen method to implement error correction. This includes the fact that the amount of entanglement needed is independent of the computation as well as the high adaptability of this method.

3.3 Axis 3: New models and applications from fundamental approaches

The predominant model of quantum computation is that of quantum circuits, and the previous two axes stay within this standard framework in their goals centered around designing and building quantum devices. In contrast to classical computation, however, in the quickly-evolving landspace of quantum information there remains significant insight to be gained by studying alternative models of computation. They may, for example, be more tolerant to realistic types of noise, provide new insight into algorithms and applications, or be better able to exploit certain quantum resources. As concrete examples, both adiabatic and measurement-based quantum computing have been extensively studied, leading to a number of important insights that have been fed back more generally into quantum information research.

By considering a higher level of abstraction, this axis explores novel models of quantum information processing in order to identify new avenues for exploiting quantum effects and outperforming classical devices, even in the presence of noise. One of the primary avenues for this is the study of higher-order quantum operations, allowing an abstract understanding of what quantum transformations are possible in principle, and the use of new resources such as quantumly-controlled operations to implement such computations.

This axis thus explores more fundamental aspects of quantum information processing, as we believe these to be highly valuable in providing new insight in quantum computing and communication. We aim to use the new models and approaches we will study to provide new techniques to mitigate noise in quantum devices, certify their behaviour more efficiently, and develop algorithms or protocols providing better quantum advantages in applications of interest. It will thus provide important insight for the previous two axes, and at the same time will make use of mathematical tools and approaches common to the themes of the project.

3.3.1 Quantum control in quantum information processing

One of the intrinsic limitations of the standard quantum circuit model is that the structure of the circuit, and hence of the flow of information, is fixed prior to computation; quantum circuits do not allow for the possibility of a “quantum `if`-statement”. In this research goal we study new models to quantum computation that, in contrast, have explicit *quantum control structures*. These models, in particular, have the potential to provide new approaches to mitigate noise can lead to stronger quantum advantages in certain applications.

To study quantum control structures we work within the framework of higher-order quantum operations [72, 101], which formalise the types of ways quantum circuits or channels can themselves be transformed within quantum theory. This approach has developed rapidly in recent years [**110**] since it was first used to show that one can indeed formulate quantum computations in which the *order* of two quantum gates is superposed with the help of a quantum control system, a gadget known as the *quantum switch* [73] (see Fig. 3).

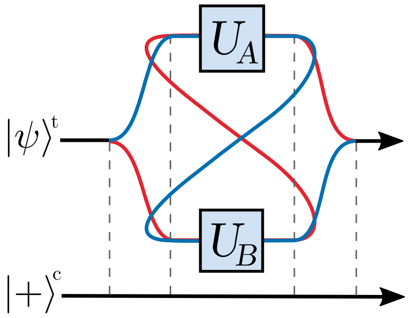

Figure 3: By allowing the structure of a circuit to be controlled by a quantum system, one can perform certain computations more efficiently. Such “quantum control structures” can be formally studied as higher-order quantum operations, leading to a generalisation of quantum circuits.

The quantum switch and related computations have since been shown to provide new types of quantum advantages in several information-theoretical tasks [75, 60, 91], where they outperform even “standard” quantum circuits. Moreover, its relevance for improving noise tolerance has recently come to light in a number of works showing how quantum control can be used to improve communication over noisy quantum channels [84, 74],[**59**].

This progress emphasises the potential benefits in studying such models of quantum information processing, and motivates a more systematic study of quantum control models in this context. In a first step in this direction we recently formalised a computational model strictly generalising quantum circuits, called *quantum circuits with quantum control of causal order (QC-QC)* that incorporate – and generalise – quantum control structures [111]. This model will serve as the base for a **systematic study of the computational power of quantum computations exploiting quantum control**, allowing us to understand the types of advantages this new resource of quantum control can provide.

With a better understanding of quantum computations with quantumly controlled operations, we will aim to develop algorithms for several problems where quantum control appears to be a promising problem. Of particular interest, we will look to use it to provide **new algorithms for quantum metrology and parameter estimation** – both key problems that are seen as near-to-mid-term applications for quantum information – that are more efficient than existing approaches and, in particular, are more robust in the noisy versions of these problems. An important first step we are undertaking in this direction is to generalise existing advantages obtainable with quantum circuits with quantum control of causal order from problems in a noiseless regime – where the controlled operations are unitary – to a noisy regime, where the controlled operations are noisy quantum channels.

In order to obtain such results, the mathematical tools being studied and developed in the other research axes of the proposed team, most notably convex optimisation, will be of utmost importance (e.g., Goals 3.1.3, 3.1.4 and 3.2.1). These research goals also build on existing collaborations on quantum control of causal order with physicists at the Institut Néel in Grenoble (including on the development of QC-QCs [**111**]), in order to transfer physical insight on quantum control towards new application for information processing. We likewise plan to collaborate with the CAPP team at LIG to study diagrammatic calculi to understand how these new types of computations can be composed and compiled, building on existing collaborations with Mehdi Mhalla on quantum control [**59**].

The quantum control of quantum operations has potential as a resource throughout quantum information processing: not just for quantum computation but, e.g., also for quantum communication [91]. As an example, it can be used to send messages through a quantum network in a superposition of different paths, amounting to a novel extension of quantum Shannon theory [74]. By doing so, it has recently been shown in a simple, proof-of-principle setting, that one can notably **reduce the effect of noise on the message as it traverses a network** [84] [**59**] and the effect experimentally verified [**103**]. We will study this possibility further, looking at how it can be extended to practical network topologies and aim to show how it can be exploited to improve quantum communication protocols and lead to novel approaches for quantum cryptography.

One can also generalize the model of computation one step further. In causally indefinite models of computations such as QC-QCs the relative order between gates is rendered indefinite through the use of quantum control systems. Nonetheless, the computation itself still proceeds in the presence of a fixed, causal clock or external control. We will seek to go one step further in the quantum-classical divide and allow for this external control to also be quantum and autonomous. This would require the addition of another quantum system implementing the quantum gates themselves. In the case of a fixed causal order, this autonomous device needs its own internal notion of time, hence it should also be an accurate quantum clock [**115**]. Since it is quantum, this clock which controls the interactions can be prepared in a superposition of different time states, leading to new types of non-casually implemented gates and potentially novel applications.

3.3.2 Multipartite entanglement and its applications

Multipartite entanglement plays an important role in quantum protocols and in quantum games, and is likewise a key resource for measurement-based quantum computing. Nonetheless, our understanding of multipartite entanglement as a resource is much less developed than for the simpler, but important, case of bipartite entanglement. The objective of this task is develop our understanding of multipartite entanglement, how it can contribute to reducing the effect of noise in communication, computation and more generally how it can improve coordination in multipartite scenarios.

In particular, we plan consider communication problems over noisy classical networks and quantify the extent to which multipartite nonlocality can improve the transmission rates [100]. Focussing on relevant classical network communication scenarios, we will ask whether entanglement between some of the involved parties significantly improve the rates.

In a related direction, we plan to study game-theoretic settings with players with divergent interests and the advantage that can be achieved by using multipartite entangled states and, in particular, quantum graph states [90]. In collaboration with Mehdi Mhalla, we will aim to use such advantages to provide new approaches to certify multipartite entangled states, and in particular to self-test quantum graph states – important resources in certain quantum computational models – by certifying them solely from the correlations they produce [63, 62]. We plan to use progress towards Goal 3.1.4 to provide a finer analysis of the problem.

3.3.3 Quantum frequential computing

This is a new reserach direction of the team, which focuses on developing a new type of quantum computer that achieves speed-ups in both quantum and classical computation. In a nutshell, it will focus on showing that when the bit/qubit control is quantum, then a large quadratic speedup, as a fuction of the underlying resources, is achievable. This constitutes a new type of quantum resource since traditioanlly the bit/qubit control is considered to be classical or semi-calssical.

We are developing two intertwined directions of research with this objective in mind:

Direction A: Establishing and Understanding the quantum speedup We aim to demonstrate a quantum advantage by proving that quantum control can achieve clock frequencies scaling linearly with power ($f \sim P$), as opposed to the classically optinal scaling of $f \sim \sqrt{P}$. Importantly, this should be achieved without necessitating an increase in interaction strength. This involves modeling the dynamics of the control of the bits/qubits and examining unavoidable entropy production during high-frequency operations. Tailored error correction methods will be developed for this system, addressing unique challenges associated with the quantum control's interaction with logical space. This work will provide the theoretical foundations necessary to understand the interplay between quantum control, energy consumption, and heat dissipation. We will also establish the advantage from a different perpective: they types of bit/qubit-control interactions whic are required to garner said speedup.

Direction B: Developing Proof-of-Principle Proposals In parallel with Direction A, we will focus on designing proof-of-concept models to experimentally realize these quantum systems. This involves creating ultra-coherent lasers optimized for quantum control, which will serve as test beds for our ideas. The coherence and power efficiency of these lasers will be enhanced using innovative light-matter interactions and geometrically induced Berry phases. We will explore the transition from laser cavities to high-frequency quantum control, proposing experimental setups to couple these systems with computational logic.

By bridging fundamental quantum theory with practical realizations, our research will set the stage for a transformative leap in computational power and efficiency. This will not only advance theoretical physics but also open avenues for real-world applications in quantum and classical computing.

4 Application domains

Our work is of theoretical nature but can have an important applications on the development of quantum technologies for the near future as explained in the research directions. This includes in particular:

- The development of algorithms and analysis techniques for benchmarking and certifying properties of quantum technologies
- The development of applications of NISQ devices
- The development of error correction mechanisms that will allow us to reach large scale quantum (LSQ) computing faster
- The development of algorithms automatically certifying the security and/or performance of quantum cryptographic protocols, which could eventually lead to software packages that are widely used in the deployment of such systems.

5 Highlights of the year

5.1 Awards

- Omar Fawzi received the Lovelace-Babbage prize awarded by the Académie des Sciences.
- Daniel Stilck França received an ERC Starting Grant for his project Gifneq.

6 New results

6.1 Characterization, certification and applications of noisy quantum devices

Participants: Alastair Abbott, Omar Fawzi, Daniel Stilck Franca, Mischa Woods, V. Vilasini.

Learning quantum states beyond the i.i.d. assumption In [16], we develop a framework for learning properties of quantum states beyond the assumption of independent and identically distributed (i.i.d.) input states. We prove that, given any learning problem (under reasonable assumptions), an algorithm designed for i.i.d. input states can be adapted to handle input states of any nature, albeit at the expense of a polynomial increase in training data size (aka sample complexity). Importantly, this polynomial increase in sample complexity can be substantially improved to polylogarithmic if the learning algorithm in question only requires non-adaptive, single-copy measurements. Among other applications, this allows us to generalize the classical shadow framework to the non-i.i.d. setting while only incurring a comparatively small loss in sample efficiency. We use rigorous quantum information theory to prove our main results. In particular, we leverage permutation invariance and randomized single-copy measurements to derive a new quantum de Finetti theorem that mainly addresses measurement outcome statistics and, in turn, scales much more favorably in Hilbert space dimension.

Classical algorithms for estimating equilibriuim properties of quantum system Predicting observables in equilibrium states is a central yet notoriously hard question in quantum many-body systems. In the physically relevant thermodynamic limit, certain mathematical formulations of this task have even been shown to result in undecidable problems. Using a finite-size scaling of algorithms devised for finite systems often fails due to the lack of certified convergence bounds for this limit. In [14], we design certified algorithms for computing expectation values of observables in the equilibrium states of local quantum Hamiltonians, both at zero and positive temperature. Importantly, our algorithms output rigorous lower and upper bounds on these values. This allows us to show that expectation values of local observables can be approximated in finite time, contrasting related undecidability results. When the Hamiltonian is commuting on a 2-dimensional lattice, we prove fast convergence of the hierarchy at high temperature and as a result for a desired precision ε, local observables can be approximated by a convex optimization program of quasi-polynomial size in

Security of differential phase shift quantum key distribution The design of quantum protocols for secure key generation poses many challenges: On the one hand, they need to be practical concerning experimental realisations. On the other hand, their theoretical description must be simple enough to allow for a security proof against all possible attacks. Often, these two requirements are in conflict with each other, and the differential phase shift (DPS) QKD protocol exemplifies these difficulties: It is designed to be implementable with current optical telecommunication technology, which, for this protocol, comes at the cost that many standard security proof techniques do not apply to it. After about 20 years since its invention, [28] presents the first full security proof of DPS QKD against general attacks, including finite-size effects. The proof combines techniques from quantum information theory, quantum optics, and relativity. We first give a security proof of a QKD protocol whose security stems from relativistic constraints. We then show that security of DPS QKD can be reduced to security of the relativistic protocol. In addition, we show that coherent attacks on the DPS protocol are, in fact, stronger than collective attacks.

Our results have broad implications for the development of secure and reliable quantum communication technologies, as they shed light on the range of applicability of stateof-the-art security proof techniques.

6.2 Error correction methods for quantum information processing

Participants: Omar Fawzi, Mischa Woods.

Fault-tolerant quantum input/output Usual scenarios of fault-tolerant computation are concerned with the fault-tolerant realization of quantum algorithms that compute classical functions, such as Shor's algorithm for factoring. In particular, this means that input and output to the quantum algorithm are classical. In contrast to stand-alone single-core quantum computers, in many distributed scenarios, quantum information might have to be passed on from one quantum information processing system to another one, possibly via noisy quantum communication channels with noise levels above fault-tolerant thresholds. In such situations, quantum information processing devices will have quantum inputs, quantum outputs or even both, which pass qubits among each other. Working in the fault-tolerant framework of [96], we show in [40] that any quantum circuit with quantum input and output can be transformed into a fault-tolerant circuit that produces the ideal circuit with some controlled noise applied at the input and output. The framework allows the direct composition of the statements, enabling versatile future applications. We illustrate this with two concrete applications. The first one concerns communication over a noisy channel with faulty encoding and decoding operations [76]. For communication codes with linear minimum distance, we construct fault-tolerant encoders and decoders for general noise (including coherent errors). For the weaker, but standard, model of local stochastic noise, we obtain fault-tolerant encoders and decoders for any communication code that can correct a constant fraction random errors. In the second application, we use our result for a state preparation circuit within the construction of [89] to establish that fault-tolerant quantum computation for general noise can be achieved with constant space overhead.

A Shannon theory approach to dynamic quantum error correction Given a quantum Markovian noise model, we study in [45] the maximum dimension of a classical or quantum system that can be stored for arbitrarily large time. We show that, unlike the fixed time setting, in the limit of infinite time, the classical and quantum capacities are characterized by efficiently computable properties of the peripheral spectrum of the quantum channel. In addition, the capacities are additive under tensor product, which implies in the language of Shannon theory that the one-shot and the asymptotic i.i.d. capacities are the same.

6.3 Understanding quantum entanglement

Participants: Alastair Abbott, Guillaume Aubrun.

Norm estimates for k-positive maps Quantum entanglement can be characterized as the discepancy between the classes of positive vs completely positive maps. When interpolating between these families, we obtain the classes of k-positive maps, parametrized by an integer k. In [9] we studied the discrepancy between the norm and the completely bounded norm of a map between matrix algebras under assumptions of k-positivity, using techniques from operator algebra.

Entanglement resources in quantum games Entanglement is one of the primary quantum resources behind many quantum advantages, but many applications focus on bipartite entanglement shared between only two parties, in part due to the simplicity of this setting. In [6] we studied multipartite entanglement in the context of non-collaborative game theory, to understand how it can be used as a resource in tasks where there are conflicts of interest. We showed how quantum entanglement can lead to higher “social welfare” – a measure of the quality of a Nash equilibrium – than could be obtained with classical resources. Moreover, this setting allowed us to uncover surprising and nuanced differences between having direct access to quantum resources, and indirect access via some idealised black boxes. Technically, a key novelty of this work was to use the technique of self-testing correlations in a new way to show the separation between these types of quantum resource.

6.4 Causal structure of quantum information processing

Participants: Alastair Abbott, Mischa Woods, V. Vilasini.

Connecting causal inference and space-time geometry via information-theoretic signalling Causality is pivotal across scientific disciplines, presenting itself in different forms: information-theoretic, linked to information flow, and relativistic linked to the structure of space-time. Causal modelling and inference is a prominent approach for the former, which has seen applications across classical data-driven disciplines and recent growing interest in quantum information. In [47], we study the interplay between causal models and space-time structure in general theories of information-processing, which has been relatively little understood on a formal level. First, we improve the characterization of information-theoretic signalling relations studied in [107], introducing conditions for operationally identifying redundant information in different parts of such a relation. We thereby introduce new techniques for causal inference in unfaithful causal models (where the observable data does not "faithfully" reflect the causal dependences) which demonstrates the possibility of causal inference using the absence of signalling between certain nodes. Second, we define an order-theoretic property called conicality, that distinguishes the geometry of light cones in Minkowski space-times with $d > 1$ vs $d = 1$ spatial dimensions. Finally, we study the embedding of information-theoretic causal models in space-time without violating relativistic principles such as no superluminal signalling (NSS). In general, we observe that constraints imposed by NSS in a space-time and those imposed by purely information-theoretic causal inference behave differently. However, we demonstrate that in conical space-times and in faithful causal models, these two types of constraints exhibit certain similar and useful properties. This offers new insights on the fundamental role of different space-time geometries for information processing possibilities, while generating new causal inference methods which could have independent applications in classical statistics.

How relativistic principles constrain information-processing tasks Relativistic causality principles fundamentally constrain information processing possibilities in space-time. No superluminal causation (NSC) and no superluminal signaling (NSS) are two such principles which, although often conflated, are distinct. In [55], we study the consequence of these principles for information-processing by considering the tasks of generating non-classical correlations within two space-time configurations. We show that the first task is impossible in any classical theory while the second is impossible in any (possibly non-classical) theory constrained by NSC. However, we construct a protocol enabling non-classical correlations to be generated in both configurations in a theory restricted by the NSS principle (which is weaker than NSC). We show that in any theory that admits this protocol, the violation of NSC without violating NSS would be operationally verifiable, and these findings link two distinct post-quantum resources: jamming non-local correlations and PR-box correlations. Our work informs a new research direction while providing insights and methods to explore it: how different relativistic principles lead to distinct constraints on the information processing power of physical theories.

Bridging indefinite causality and composable quantum protocols in space-time The concept of quantum processes with indefinite causal orders (ICO) have garnered much interest due to their potential advantages for information processing. However, there have remained longstanding open questions regarding the physical realisability of ICO processes. Moreover, it was previously observed that composition of such processes is not so straightforward, which raises the question of how this connects with the observed composability of physical experiments. In [27], we address these questions by bridging these information-theoretic approaches for causality, with spacetime structure which constraints physical implementations. Specifically, we connect the formalism of quantum circuits with quantum control of causal order (QC-QC), which models an important class of ICO processes, with that of causal boxes, which models composable quantum information protocols in spacetime. We incorporate the set-up assumptions of the QC-QC framework into the spatiotemporal perspective and show that every QC-QC can be mapped to a causal box that satisfies these set up assumptions and acts on a Fock space while reproducing the QC-QC's behaviour in a relevant subspace. We show that the causal box corresponds to a fine-grained description of the QC-QC, which unravels the original ICO of the QC-QC into a set of quantum operations with a well-defined and acyclic causal order, compatible with the spacetime's light cone structure. Through this mapping, we clarify how the composability of physical experiments is recovered, and the role of relativistic causality.

Device-independent certification of indefinite causal orders The strongest form of certification possible in quantum information theory is device-independent certification, which certifies the presence of a resource without making any assumptions about the devices used to perform the certification. This type of certification has been well-studied for entanglement and is exploited in cryptographic applications, for example, and there has been growing interest in applying it to different resources. While it is known that the causal indefiniteness of some quantum processes can be certified in a device-independent way through the violation of causal inequalities, it has been unclear whether more physical processes such as QC-QCs – which do not violate causal inequalities – can be certified in this way. Building on our previous work showing how one can certify causal indefiniteness in a "semi-device-independent" manner [80], we showed in [12] how this certification can be made stronger and transformed into a fully device-independent certification technique, in which no assumptions are made about the devices being used, other than the network structure describing how certain devices are connected. This shows that some important processes, like the quantum switch, can be certified in a device-indepndent manner, despite this being believed impossible until recently.

Query complexity of causally indefinite computation Indefinite causal order opens interesting possibilities for information processing, such as the possibility to obtain computational advantages using causally indefinite quantum computations beyond what is possible with standards (causally ordered) quantum circuits. In [7] we study the computational advantages of causal indefiniteness in query complexity problems using the framework of quantum supermaps. Using semi-definite programming approaches, we are able to calculate the exact query complexity of different types of computations for small input sizes (4-bit Boolean functions with 2 queries to the oracle): standard quantum circuits, circuits with quantum control of causal order, and more general causally indefinite supermaps. We find that, for certain functions, causally indefinite supermaps can provide an advantage in query complexity, uncovering a new computational advantage of causal indefiniteness that, in contrast to previously known advantages, is formulated in a more standard complexity-theoretic setting. However, we prove that the class of quantum circuits with quantum control of causal order is unable to improve upon standard quantum circuits in this query complexity setting. In a work in preparation we study causally indefinite classical processes, and show that in this setting an asymptotic advantage in deterministic query complexity can be obtained.

Consistent multi-agent reasoning in Wigner's Friend Scenarios It is natural to expect a complete physical theory to have the ability to consistently model agents as physical systems of the theory. With this motivation, Extended Wigner's Friend Scenarios (EWFSs) consider multiple quantum agents, who can perform quantum agents on each others' labs. These have been the subject of several no-go theorems: Frauchiger and Renner (FR) identified logical paradoxes arising from reasoning quantum agents, while other results highlight challenges for having an objective notion of measurement events and for causal reasoning in EWFSs. This raises the question: is it possible to reliably make and test scientific predictions, and consistently reason about the world when applying quantum theory universally? In [54], we give a positive answer by developing a general quantum circuit framework for EWFSs. By formalising the concept of Heisenberg cuts, we prove that FR-type paradoxes can be fully resolved and thereby provide concrete rules by which quantum agents can reason and make predictions in a logically and causally consistent manner. Our framework describes all predictions of an EWFS within a single, well-defined causal structure, while allowing events to be fundamentally subjective. Yet we show that an objective notion of measurement events emerges in real-world experiments. This provides a platform to consistently extend quantum information methods to Wigner's Friend Scenarios, and establishes that quantum computers playing the role of reasoning agents can in-principle be programmed consistently, while preserving the axioms of quantum theory and those of classical logic and probability theory.

6.5 Quantum frequential computing

Quadratically increasing computation speed without increasing interaction strengh nor power consumed In [58], an initial invertigation kicking-off the research of Direction A of the quantum frequential computing program, has been performed. It was demostrated that there is indeed an advantage concerning the speed at which computation can be performed, if the control of the qubits/bits is quantum mechanical as opposed to the conventional setting where it is classical. It was proven that there is a quadratic speedup for quantum and classical algorithms alike, when the optimal quantum control state is used. The quantum advantage stems from the quantum resource of squeezing.

7 Partnerships and cooperations

Participants: Alastair Abbott, Omar Fawzi, Mizanur Rahaman, Daniel Stilck França, Vilasini V., Mischa Woods.

7.1 International research visitors

7.1.1 Visits of international scientists

Frédéric Dupuis

Status Associate Professor

Institution of origin: Université de Montréal

Country: Canada

Dates: April 15 - May 15

Context of the visit: Research collaboration on security proofs for quantum cryptography

Mobility program/type of mobility: Sabbatical research stay

7.2 European initiatives

7.2.1 Horizon Europe

PENNSION PENNSION project on cordis.europa.eu

Title: Partition and accumulation of ENtropy in infinite-dimeNSIONs

Duration: From August 1, 2023 to July 31, 2025

Partners:

- INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE (INRIA), France

Inria contact: Omar Fawzi

Coordinator: Mizanur Rahaman

Summary: The foundation of today's information-oriented society is based on Information Theory. Entropy is a fundamental concept in both classical and quantum information theory, measuring the uncertainty and the information content present in the state of a physical system. The Asymptotic Equipartition Property (AEP) asserts that the entropy of smaller parts accumulates to produce the total entropy of the entire system, under the assumption that the individual parts are identical and independent. A remarkable generalization of this property is the Entropy Accumulation Theorem (EAT) which states that entropy accumulation occurs more generally without an independence assumption, provided one quantifies the uncertainty about the individual systems by the von Neumann entropy of suitably chosen conditional states. These two results are central in the asymptotic analysis of entropy measures in finite-dimensional quantum systems with a wide range of applications in data compression, source coding, and Quantum Key Distribution.

Despite major advances in the study of entropy in quantum information theory, the fundamental limitations of extending the above concepts to infinite-dimensional systems are far from being understood. The main objective of this project is to develop novel mathematical tools to overcome these difficulties and extend these ideas in the framework of abstract von Neumann algebras. In particular, our essential goal will be to establish two main concepts- Asymptotic Equipartition and Entropy Accumulation in von Neumann algebras acting on infinite-dimensional Hilbert spaces. As a consequence, the generalized version of these two concepts will have direct applications in continuous variable Quantum Key Distribution and other cryptographic protocols, representing a small but important contribution to the European Commission's Quantum Technologies Flagship supporting pioneering research on quantum science.

QSNP QSNP project on cordis.europa.eu

Title: Quantum Secure Networks Partnership

Duration: From March 1, 2023 to August 31, 2026

Partners:

- ECOLE POLYTECHNIQUE (EP), France
- INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE (INRIA), France
- DEUTSCHE TELEKOM TECHNIK GMBH, Germany
- INSTITUTO DE TELECOMUNICACOES (IT), Portugal
- FRIEDRICH-ALEXANDER-UNIVERSITAET ERLANGEN-NUERNBERG (FAU), Germany
- UNIWERSYTET WARSZAWSKI (UNIWARSAW), Poland
- NEXTWORKS, Italy
- AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH (AIT), Austria
- MICRO PHOTON DEVICES SRL (MPD), Italy
- THINKQUANTUM SRL (THINKQUANTUM), Italy
- UNIVERSITE COTE D'AZUR, France
- ORANGE SA (Orange), France
- ETHNIKO KAI KAPODISTRIAKO PANEPISTIMIO ATHINON (UOA), Greece
- FUNDACIO INSTITUT DE CIENCIES FOTONIQUES (ICFO-CERCA), Spain
- INSTITUT POLYTECHNIQUE DE PARIS, France
- UNIVERSITAT WIEN (UNIVIE), Austria
- QUSIDE TECHNOLOGIES SL, Spain
- FRAUNHOFER GESELLSCHAFT ZUR FORDERUNG DER ANGEWANDTEN FORSCHUNG EV (Fraunhofer), Germany

- COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (CEA), France
- INTERUNIVERSITAIR MICRO-ELECTRONICA CENTRUM (IMEC), Belgium
- CRYPTONEXT (CRYPTONEXT SECURITY), France
- POLITECNICO DI BARI (POLIBA), Italy
- LUXQUANTA TECHNOLOGIES SL, Spain
- Alea Quantum Technologies ApS (Alea Quantum Technologies ApS), Denmark
- UNIVERSITA DEGLI STUDI DI PADOVA (UNIPD), Italy
- UNIVERSITE LIBRE DE BRUXELLES (ULB), Belgium
- INSTITUT MINES-TELECOM, France
- TELEFONICA INNOVACION DIGITAL SL, Spain
- DANMARKS TEKNISKE UNIVERSITET (TECHNICAL UNIVERSITY OF DENMARK DTU), Denmark
- UNIVERZITA PALACKEHO V OLOMOUCI (UP), Czechia
- Q* BIRD BV (Q*Bird B.V.), Netherlands
- NOKIA NETWORKS FRANCE, France
- UNIVERSITE PARIS CITE (UPCité), France
- UNIVERSITA TA MALTA (UNIVERSITY OF MALTA), Malta
- TECHNISCHE UNIVERSITEIT EINDHOVEN (TU/e), Netherlands
- TELECOM ITALIA SPA O TIM SPA (TIM), Italy
- CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE CNRS (CNRS), France
- KATHOLIEKE UNIVERSITEIT LEUVEN (KU Leuven), Belgium
- EREVNITIKO PANEPISTIMIAKO INSTITOUTO SYSTIMATON EPIKOINONION KAI YPOLOGISTON (RESEARCH UNIVERSITY INSTITUTE OF COMMUNICATION AND COMPUTER SYSTEMS), Greece
- UNIVERSITY COLLEGE CORK - NATIONAL UNIVERSITY OF IRELAND, CORK (UCC), Ireland
- VPIPHOTONICS GMBH, Germany
- UNIVERSIDAD POLITECNICA DE MADRID (UPM), Spain
- INSTITUTO SUPERIOR TECNICO (IST), Portugal
- TECHNISCHE UNIVERSITEIT DELFT (TU Delft), Netherlands
- UNIVERSIDAD DE VIGO (UVIGO), Spain
- UNIVERSITAET PADERBORN (UPB), Germany
- SORBONNE UNIVERSITE, France

Inria contact: Alastair Abbott

Coordinator: Valerio Pruneri

Summary: The Quantum Secure Networks Partnership (QSNP) project aims at creating a sustainable European ecosystem in quantum cryptography and communication. A majority of its partners, which include world-leading academic groups, research and technology organizations (RTOs), quantum component and system spin-offs, cybersecurity providers, integrators, and telecommunication operators, were members of the European Quantum Flagship projects CIVIQ, UNIQORN and QRANGE. QSNP thus gathers the know-how and expertise from all technology development phases, ranging from innovative designs to development of prototypes for field trials. QSNP is structured around three main Science and Technology (ST) pillars. The first two pillars, “Next Generation Protocols” and “Integration”, focus on frontier research and innovation, led mostly by academic partners and RTOs. The third ST pillar “Use cases and Applications” aims at expanding the industrial and economic impact of QSN technologies and is mostly driven by companies. In order to achieve the specific objectives within each pillar and ensure that know-how transfer and synergy between them are coherent and effective, QSNP has established ST activities corresponding to the three main layers of the technology value chain, “Components and Systems”, “Networks” and “Cryptography and Security”. This framework will allow achieving the ultimate objective of developing quantum communication technology for critical European infrastructures, such as EuroQCI, as well as for the private information and communication technology (ICT) sectors. QSNP will contribute to the European sovereignty in quantum technology for cybersecurity. Additionally, it will generate significant economic benefits to the whole society, including training new generations of scientists and engineers, as well as creating high-tech jobs in the rapidly growing quantum industry.

7.2.2 H2020 projects

AlgoQIP AlgoQIP project on cordis.europa.eu

Title: Algorithm from optimal Quantum Information Processing

Program: ERC Starting Grant

Duration: From January 1, 2021 to December 31, 2026

PI: Omar Fawzi

Summary: The large overhead needed to correct errors caused by unwanted noise hinders the exploitation of quantum theory in information technology. Although there has been progress in designing better error-correcting codes and fault-tolerant schemes, the limits of communication over a quantum noisy medium are still not understood. The EU-funded AlgoQIP project aims to build an algorithmic theory of optimal information processing that goes beyond the statistical approach of Shannon’s theory. It will achieve this by developing efficient algorithms that take as input a description of a noise model and output a near-optimal method for reliable communication under this model. These algorithms will have direct applications in the development of quantum technologies.

7.2.3 Other european programs/initiatives

VERIqTAS

Title: Verification of quantum technologies, systems and applications

Program: QuantERA call 2021

Contact Inria: O. Fawzi

Partners: Center for Theoretical Physics, Polish Academy of Sciences (coordinator), Université Libre de Bruxelles, Austrian Academy of Sciences, University of Copenhagen, The Institute of Photonic Sciences, Inria

Duration: April 1, 2022 - March 31, 2025

Touqan

Title: Towards a useful quantum advantage

Program: QuantERA call 2023

Contact Inria: M. Woods

Partners: Instituto de Fisica Teorica UAM (coordinator), Inria, Hamburg U. Technology, Universität Tübingen, Center for Theoretical Physics Polish Academy of Sciences

Duration: June 1, 2024 - May 31, 2024

MODIC

Title: Modern Device Independent Cryptography

Program: CHIST-ERA call 2022

Contact Inria: O. Fawzi

Partners: University of Gdansk (coordinator), Inria, ATOMKI, Swiss Federal Institute of Technology in Zürich

Duration: April 1, 2024 - March 31, 2027

7.3 National initiatives

PEPR DIQKD

Title: Device-independent quantum key distribution

Program: PEPR on Quantum Technologies

Contact Inria: O. Fawzi

Partners: CEA (coordinator), CNRS, Université Côte D'Azur, Sorbonne Université

Duration: July 1, 2022 - June 30 2026

PEPR NISQ2LSQ

Title: From NISQ to LSQ: Bosonic and LDPC codes

Program: PEPR on Quantum Technologies

Contact Inria: A. Leverrier (team COSMIQ)

Contact QInfo: O. Fawzi

Partners: Inria (coordinator), CNRS, CEA

Duration: January 1, 2022 - December 2026

PEPR EPIQ

Title: Study of the quantum stack: Algorithm, models, and simulation for quantum computing

Program: PEPR on Quantum Technologies

Contact Inria: S. Perdrix (team MOCQUA)

Contact QInfo: O. Fawzi

Partners: Inria (coordinator), CNRS, CEA

Duration: January 1, 2022 - December 2026

PEPR HQI

Title: Hybrid HPC Quantum Initiative

Program: PEPR on Quantum Technologies

Contact QInfo: D. Stilck Franca

Partners: Inria, CPU, GENCI, CNRS, CEA (coordinator)

Duration: April 1, 2023 - March 2028

ANR TaQC

Title: Taming Quantum Causality

Program: AAP Générique 2022

Contact QInfo: A. Abbott

Partners: CNRS (Institut Néel; coordinator), Inria QINFO, Université Paris-Saclay (LMF, Inria QUACS), CEA (IRFU/LARSIM)

Duration: January 1, 2023 - December 2026

8 Dissemination

8.1 Promoting scientific activities

8.1.1 Scientific events: organisation

General chair, scientific chair

- Fundamental Limitations to Quantum Computation Workshop, Banff International Research Station (D. Stilck França)
- QuantAlps Days 2024, Grenoble, France (A. Abbott)

Member of the organizing committees

- Causalworlds 2024: The second international conference on quantum, classical and relativistic causality, held at the Perimeter Institute for Theoretical Physics, Waterloo, Canada (V. Vilasini)
- QEI 2025: Second Quantum Energy Initiative conference, Grenoble, France (M. Woods)

8.1.2 Scientific events: selection

Chair of conference program committees

- Causalworlds 2024: The second international conference on quantum, classical and relativistic causality, held at the Perimeter Institute for Theoretical Physics, Waterloo, Canada (V. Vilasini)
- QCTIP 2024: Quantum Computing Theory in Practice conference, held at Quantum Software Lab and the University of Edinburgh (D. Stilck Franca).

Member of the conference program committees

- QPL 2024, held in Buenos Aires in July 2024 (V. Vilasini)
- Causalworlds 2024, held at the Perimeter Institute for Theoretical Physics, Waterloo, Canada (A. Abbott)
- QCRYPT 2024, held in Vigo in September 2024 (O. Fawzi)
- STACS 2025, to be held in Jena in March 2025 (O. Fawzi)

8.1.3 Journal

Member of the editorial boards

- *Quantum*, editor (O. Fawzi)

8.1.4 Invited talks

- G. Aubrun, course given at the research school Random quantum channels: entanglement and entropies, Marseille (CIRM), July 2024
- G. Aubrun, invited speaker at the International Congress on Mathematical Physics, Strasbourg, July 2024
- G. Aubrun, mini-course given at the conference Random tensors and related topics, Paris (IHP), Oct 2024
- O. Fawzi, Symposium on Quantum Optimization and Geometry, Amsterdam, January 2024
- O. Fawzi, Quantum Information Workshop, Les Diablerets, February 2024
- O. Fawzi, Workshop Quantum Cryptography and Quantum Networks, Berlin, May 2024
- O. Fawzi, Quantum Error Correction meets Operator Algebras, Oslo, June 2024
- O. Fawzi, Focused workshop on quantum Reńyi divergences, July 2024
- O. Fawzi, Fault-Tolerant Quantum Technologies, Benasque, August 2024
- O. Fawzi, IWOTA 2024, Canterbury, August 2024
- O. Fawzi, Journées Scientifiques Inria, Grenoble, August 2024
- O. Fawzi, Workshop on Machine Learning and Quantum Information, Marseille (CIRM), September 2024
- O. Fawzi, Séminaire Parisien d'Optimisation, December 2024
- V. Vilasini, From Quantum Materials to Quantum Information: Symposium on Trans-Scale Quantum Science and Quantum Materials Synthesis (QMQI2024) held at Okinawa Institute for Science and Technology in November 2024.
- V. Vilasini, Vienna Foundations Conference, Vienna in September 2024.
- V. Vilasini, Invited Plenary talk at Relativistic Quantum Information North, Prague in August 2024.
- V. Vilasini, Emergence of Classicality: New Perspectives on Measurements in Quantum Theory, held at Trinity College Dublin in July 2024.
- V. Vilasini, A look at the interface between gravity and quantum theory, held in San Vito di Cadore in July 2024.
- V. Vilasini, Invited talk at Laboratoire Kastler Brossel, Paris in June 2024.
- D. Stilck Franca, Quantum Gibbs Sampling Tutorial, Simons Instute Berkeley, April 2024.
- M. Woods, invited speaker at Geometry of Quantum States, Siegen, August 2024
- M. Woods, invited speaker at Foundations of Quantum Computing, Royal Holloway, University of London, September 2024.
- M. Woods, invited speaker at QMQI, Okinawa Institute of Science and Technology, Japan November 2024.

8.1.5 Leadership within the scientific community

- V. Vilasini is a co-leader of a research working group in the European COST Action for Relativistic Quantum Information

8.1.6 Scientific expertise

- Alastair Abbott: Member of the selection committee for Inria CRCN and ISFP recrutement competitions, Inria Saclay Centre
- Alastair Abbott: Member of the selection committee for Assistant Professor in Quantum Computing, CentraleSupélec
- Omar Fawzi: Member of the selection commitee for Inria CRCN and ISFP recruitment competitions, Inria Paris
- Omar Fawzi: Member of the selection commitee for a Professor at ENS de Lyon.

8.1.7 Research administration

- Alastair Abbott is a member of the governing board of the QuantAlps Research Federation
- Alastair Abbott is a member of the governing board of the TIQuA CD Tools Programme

8.2 Teaching - Supervision - Juries

8.2.1 Teaching

- L3: G. Aubrun, *Probability*, 32 hours, course given for the first year students in computer science, ENS Lyon.
- Master: A. Abbott, *Fundamental Computer Science*. M1 MOSIG/M1 INFO UGA, 27 hours lectures and tutorials.
- Master: O. Fawzi, *Quantum Computer Science*. Master 1 Informatique ENS Lyon, 28 hours lectures.

8.2.2 Supervision

- PhD: Raphaël Mothe, *Causal indefiniteness and dynamicality in quantum mechanics* (A. Abbott with C. Branciard)
- PhD: Sarah Timhadjelt, *Liberté asymptotique forte de matrices de perturbations aléatoires, indépendantes et uniformes* (G. Aubrun, co-supervisor)
- PhD in progress: Pierre Pocreau, *Implications of causal indefiniteness for quantum communication* (A. Abbott with M. Mhalla)
- PhD in progress: Maarten Grothus, *Exploiting causal indefiniteness in quantum computational models* (A. Abbott with C. Branciard)
- PhD in progress: Raphaël le Bihan, *Compositionality and applications of quantum supermaps* (A. Abbott with M. Echenim)
- PhD in progress: Emilien de Bank, (V. Vilasini with C. Branciard)
- PhD in progress: Amanda Maria Fonseca, (V. Vilasini with C. Branciard)
- PhD in progress: Pablo Alvarez Dominguez, (M. Woods)
- PhD in progress: Emily Beatty, *Quantum Optimal Transposrt* (G. Aubrun, D. Stilck Franca)
- PhD in progress: Victor Martinez, *Quantum algorithms and combinatorial optimization* (O. Fawzi, D. Stilck Franca)
- PhD in progress: Mostafa Taheri, (O. Fawzi)
- PhD in progress: Idris Delsol, (O. Fawzi)

- PhD thesis submitted (defense on 17th February 2025): Victor Gitton, ETH Zürich (co-supervisor: V. Vilasini with supervisor: Renato Renner)
- Master's internship: Raphaël le Bihan, *Compositionality of quantum supermaps* (A. Abbott)

8.2.3 Juries

- PhD: Harold Nieuwboer, Classical and quantum algorithms for scaling problems, University of Amsterdam, 31 January 2024
- PhD: Gergely Bunth, On quantum Rényi divergences, Budapest University of Technology and Economics, 23 July 2024
- PhD: Emanuel-Cristian Boghiu Crihan, Bell non-locality and causal networks, Institute of Photonic Sciences (ICFO) Barcelona, 9th July 2024 (V. Vilasini, external examiner).
- PhD: Raphaël Mothe, Causal indefiniteness and dynamicality in quantum mechanics, Université Grenoble Alpes, 18th October 2024 (V. Vilasini, internal examiner)
- PhD: Isaac Friend, Causal identification for quantum networks, University of Oxford, U.K., 6th of December 2024 (V. Vilasini, external examiner)
- HDR: Alantha Newman, Cuts, orders and partitions through the lens of relaxation, rounding and approximation, Université Grenoble Alpes, 4 December 2024 (O. Fawzi examiner)

8.3 Popularization

8.3.1 Productions (articles, videos, podcasts, serious games, ...)

- V. Vilasini, popular science article in Phys.org and Physicsworld based on recent publications [29, 30] and interview with science journalist.
- A. Abbott, Explorations Quantiques 2050, les récits. Technological analysis of scenarios and their basis in the scientific literature [32].
- M. Woods, interview with science jouralist Karmela Padavic-Callaghan for comments in her popular science article in New Scientist.

8.3.2 Participation in Live events

- Alastair Abbott, invited introductory talk for general public and researchers in social sciences and humanities in a program creating dialogue with citizens about the implications of quantum technologies, "Quantum Dates: Quantique, Cybersecurité et Data" (November 2024).
- Emily Beatty and Mizanur Rahaman organized a booth in the event "Science is Wonderful" that is held each year by the EU for the Marie-Curie fellows. In this event, researchers are chosen to explain their scientific work to the public (mainly high school students) through interactive experiments, hands-on activities, science shows, games and quizzes. More than 500 students visiting our booth who came and participated in our presentation.

9 Scientific production

9.1 Major publications

[1] H. Fawzi, O. Fawzi and S. O. Scalet. 'Certified algorithms for equilibrium states of local quantum Hamiltonians'. In: *Nature Communications* 15.1 (2024), p. 7394. DOI: `10.1038/s41467-024-51592-3`. URL: `https://hal.science/hal-04682901`.

[2] O. Fawzi, R. Kueng, D. Markham and A. Oufkir. 'Learning properties of quantum states without the IID assumption'. In: *Nature Communications* 15.1 (8th Nov. 2024), p. 9677. DOI: `10.1038/s41467-024-53765-6`. URL: `https://hal.science/hal-04824975`.

[3] B. Romera-Paredes, M. Barekatain, A. Novikov, M. Balog, M. P. Kumar, E. Dupont, F. Ruiz, J. Ellenberg, P. Wang, O. Fawzi, P. Kohli and A. Fawzi. 'Mathematical discoveries from program search with large language models'. In: *Nature* 625.7995 (14th Dec. 2023), pp. 468–475. DOI: `10.1038/s41586-023-06924-6`. URL: `https://hal.science/hal-04682926`.

[4] D. Stilck Franca, L. A. Markovich, V. V. Dobrovitski, A. H. Werner and J. Borregaard. 'Efficient and robust estimation of many-qubit Hamiltonians'. In: *Nature Communications* 15.311 (8th Jan. 2024). DOI: `10.1038/s41467-023-44012-5`. URL: `https://hal.science/hal-03675783`.

[5] V. Vilasini and R. Renner. 'Fundamental Limits for Realizing Quantum Processes in Spacetime'. In: *Physical Review Letters* 133.8 (22nd Aug. 2024), p. 080201. DOI: `10.1103/PhysRevLett.133.080201`. URL: `https://inria.hal.science/hal-04676775`.

9.2 Publications of the year

International journals

[6] A. A. Abbott, M. Mhalla and P. Pocreau. 'Improving social welfare in non-cooperative games with different types of quantum resources'. In: *Quantum* 8 (17th June 2024), p. 1376. DOI: `10.22331/q-2024-06-17-1376`. URL: `https://inria.hal.science/hal-03839608` (cit. on p. 14).

[7] A. A. Abbott, M. Mhalla and P. Pocreau. 'Quantum query complexity of Boolean functions under indefinite causal order'. In: *Physical Review Research* 6.3 (26th July 2024), p. L032020. DOI: `10.1103/PhysRevResearch.6.L032020`. URL: `https://inria.hal.science/hal-04672768` (cit. on p. 16).

[8] G. Aubrun, K. Davidson, A. Müller-Hermes, V. Paulsen and M. Rahaman. 'Completely bounded norms of k-positive maps'. In: *Journal of the London Mathematical Society* 109.6 (June 2024), e12936. DOI: `10.1112/jlms.12936`. URL: `https://hal.science/hal-04454872`.

[9] G. Aubrun, A. Müller-Hermes and M. Plávala. 'Monogamy of entanglement between cones'. In: *Math.Ann.* 391.1 (2025), pp. 1591–1609. DOI: `10.1007/s00208-024-02935-4`. URL: `https://hal.science/hal-03720803` (cit. on p. 14).

[10] S. Bäuml, C. Pascual-García, V. Wright, O. Fawzi and A. Acín. 'Security of discrete-modulated continuous-variable quantum key distribution'. In: *Quantum* 8 (17th July 2024), pp. 1–37. DOI: `10.22331/q-2024-07-18-1418`. URL: `https://hal.science/hal-04824981`.

[11] P. Brown, H. Fawzi and O. Fawzi. 'Device-independent lower bounds on the conditional von Neumann entropy'. In: *Quantum* 8 (27th Aug. 2024), p. 1445. DOI: `10.22331/q-2024-08-27-1445`. URL: `https://hal.science/hal-03581631`.

[12] H. Dourdent, A. A. Abbott, I. Šupić and C. Branciard. 'Network-Device-Independent Certification of Causal Nonseparability'. In: *Quantum* 8 (30th Oct. 2024), pp. 1–24. DOI: `10.22331/q-2024-10-30-1514`. URL: `https://inria.hal.science/hal-04193227` (cit. on p. 16).

[13] H. Fawzi, O. Fawzi and S. Scalet. 'Entropy constraints for ground energy optimization'. In: *Journal of Mathematical Physics* 65.3 (2024), p. 032201. DOI: `10.1063/5.0159108`. URL: `https://hal.science/hal-04682903`.

[14] H. Fawzi, O. Fawzi and S. O. Scalet. 'Certified algorithms for equilibrium states of local quantum Hamiltonians'. In: *Nature Communications* 15.1 (2024), p. 7394. DOI: `10.1038/s41467-024-51592-3`. URL: `https://hal.science/hal-04682901` (cit. on p. 13).

[15] O. Fawzi and P. Fermé. 'Broadcast Channel Coding: Algorithmic Aspects and Non-Signaling Assistance'. In: *IEEE Transactions on Information Theory* 70 (Nov. 2024), pp. 7563–7580. DOI: `10.1109/TIT.2024.3410047`. URL: `https://hal.science/hal-04232851`.

[16] O. Fawzi, R. Kueng, D. Markham and A. Oufkir. 'Learning properties of quantum states without the IID assumption'. In: *Nature Communications* 15.1 (8th Nov. 2024), p. 9677. DOI: `10.1038/s41467-024-53765-6`. URL: `https://hal.science/hal-04824975` (cit. on p. 13).

[17] V. Gitton and M. P. Woods. 'On the System loophole of generalized noncontextuality'. In: *Physical Review Research* 6.4 (18th Dec. 2024), p. 043289. DOI: `10.1103/PhysRevResearch.6.043289`. URL: `https://hal.science/hal-04886263`.

[18] D. Harley, I. Datta, F. R. Klausen, A. Bluhm, D. Stilck França, A. H. Werner and M. Christandl. 'Going beyond gadgets: the importance of scalability for analogue quantum simulators'. In: *Nature Communications* 15.1 (2nd Aug. 2024), p. 6527. DOI: `10.1038/s41467-024-50744-9`. URL: `https://hal.science/hal-04672149`.

[19] Y. Hu, M. Lock and M. Woods. 'On the feasibility of detecting quantum delocalization effects on relativistic time dilation in optical clocks'. In: *Quantum Science and Technology* 9 (24th Sept. 2024), p. 045052. DOI: `10.1088/2058-9565/ad752c`. URL: `https://hal.science/hal-04235647`.

[20] D. Kribs, J. Levick, R. Pereira and M. Rahaman. 'Operator algebra generalization of a theorem of Watrous and mixed unitary quantum channels'. In: *Journal of Physics A: Mathematical and Theoretical* 57 (7th Mar. 2024), p. 115303. DOI: `10.1088/1751-8121/ad2cb0`. URL: `https://hal.science/hal-04390457`.

[21] L. A. Markovich, V. V. Dobrovitski, A. H. Werner, J. Borregaard and D. Stilck França. 'Efficient and robust estimation of many-qubit Hamiltonians'. In: *Nature Communications* 15.311 (8th Jan. 2024). DOI: `10.1038/s41467-023-44012-5`. URL: `https://hal.science/hal-03675783`.

[22] T. Metger, O. Fawzi, D. Sutter and R. Renner. 'Generalised Entropy Accumulation'. In: *Communications in Mathematical Physics* 405.11 (12th Oct. 2024), p. 261. DOI: `10.1007/s00220-024-05121-4`. URL: `https://hal.science/hal-04838274`.

[23] R. Mothe, C. Branciard and A. A. Abbott. 'Reassessing the advantage of indefinite causal orders for quantum metrology'. In: *Physical Review A* 109.6 (25th June 2024), p. 062435. DOI: `10.1103/PhysRevA.109.062435`. URL: `https://inria.hal.science/hal-04360267`.

[24] A. Piveteau, A. A. Abbott, S. Muhammad, M. Bourennane and A. Tavakoli. 'Weak entanglement improves quantum communication using only product measurements'. In: *Physical Review Applied* 21 (25th Mar. 2024), p. 034053. DOI: `10.1103/PhysRevApplied.21.034053`. URL: `https://inria.hal.science/hal-04029621`.

[25] C. Rouzé and D. Stilck França. 'Learning quantum many-body systems from a few copies'. In: *Quantum* 8 (2024), p. 1319. DOI: `10.22331/q-2024-04-30-1319`. URL: `https://hal.science/hal-04622145`.

[26] C. Rouzé, D. Stilck França, E. Onorati and J. Watson. 'Efficient learning of ground and thermal states within phases of matter'. In: *Nature Communications* 15.1 (5th Sept. 2024), p. 7755. DOI: `10.1038/s41467-024-51439-x`. URL: `https://hal.science/hal-04896032`.

[27] M. Salzger and V. Venkatesh. 'Mapping indefinite causal order processes to composable quantum protocols in a spacetime'. In: *New Journal of Physics* (2025), pp. 1–54. DOI: `10.1088/1367-2630/ad9d6f`. URL: `https://inria.hal.science/hal-04885749`. In press (cit. on p. 15).

[28] M. Sandfuchs, M. Haberland, V. Vilasini and R. Wolf. 'Security of differential phase shift QKD from relativistic principles'. In: *Quantum* (2025). URL: `https://inria.hal.science/hal-04907376`. In press (cit. on p. 13).

[29] V. Vilasini and R. Renner. 'Embedding cyclic information-theoretic structures in acyclic spacetimes: No-go results for indefinite causality'. In: *Physical Review A* 110.2 (29th Aug. 2024), p. 022227. DOI: `10.1103/PhysRevA.110.022227`. URL: `https://inria.hal.science/hal-04720652` (cit. on p. 25).

[30] V. Vilasini and R. Renner. 'Fundamental Limits for Realizing Quantum Processes in Spacetime'. In: *Physical Review Letters* 133.8 (22nd Aug. 2024), p. 080201. DOI: `10.1103/PhysRevLett.133.080201`. URL: `https://inria.hal.science/hal-04676775` (cit. on p. 25).

International peer-reviewed conferences

[31] M. Berta, O. Fawzi and A. Oufkir. ‘Optimality of meta-converse for channel simulation’. In: ISIT 2024 - IEEE International Symposium on Information Theory. Athens, Greece: IEEE, 10th Oct. 2024, pp. 1209–1214. DOI: `10.1109/ISIT57864.2024.10619187`. URL: `https://hal.science/hal-04824978`.

Scientific book chapters

[32] A. A. Abbott, P. Engerran, F. Forest, O. Gravier and R. S. Whitney. ‘L’analyse technologique’. In: *Explorations quantiques 2050: Les récits*. Mar. 2024. URL: `https://inria.hal.science/hal-04907881` (cit. on p. 25).

Reports & preprints

[33] K. Abdukhalikov, T. Bag and D. Panario. *Quantum Codes from Group Ring Codes*. 17th Dec. 2024. URL: `https://hal.science/hal-04844287`.

[34] A. Artymowicz, H. Fawzi, O. Fawzi and S. O. Scalet. *Certified algorithms for quantum Hamiltonian learning via energy-entropy inequalities*. 30th Oct. 2024. URL: `https://hal.science/hal-04825343`.

[35] G. Aubrun and A. Müller-Hermes. *Limit formulas for norms of tensor power operators*. 30th Oct. 2024. URL: `https://hal.science/hal-04778166`.

[36] T. Bag, H. Q. Dinh and D. Panario. *Some New Non-binary Quantum Codes from One-generator Quasi-cyclic Codes*. 17th Dec. 2024. URL: `https://hal.science/hal-04843861`.

[37] E. Beatty and D. Stilck França. *Order p quantum Wasserstein distances from couplings*. 26th Feb. 2024. URL: `https://hal.science/hal-04479963`.

[38] S. Becker, N. Galke, R. Salzmann and L. van Luijk. *Convergence rates for the Trotter-Kato splitting*. 4th July 2024. URL: `https://hal.science/hal-04840625`.

[39] H.-C. Cheng, N. Datta, N. Liu, T. Nuradha, R. Salzmann and M. M. Wilde. *An invitation to the sample complexity of quantum hypothesis testing*. 16th May 2024. URL: `https://hal.science/hal-04840569`.

[40] M. Christandl, O. Fawzi and A. Goswami. *Fault-tolerant quantum input/output*. 2024. URL: `https://hal.science/hal-04825338` (cit. on p. 14).

[41] K. Fang, H. Fawzi and O. Fawzi. *Generalized quantum asymptotic equipartition*. 6th Nov. 2024. URL: `https://hal.science/hal-04825342`.

[42] M. Fanizza, C. Rouzé and D. S. França. *Efficient Hamiltonian, structure and trace distance learning of Gaussian states*. 2024. DOI: `10.48550/arXiv.2411.03163`. URL: `https://hal.science/hal-04896054`.

[43] O. Fawzi, A. Oufkir and R. Salzmann. *Optimal Fidelity Estimation from Binary Measurements for Discrete and Continuous Variable Systems*. 6th Sept. 2024. URL: `https://hal.science/hal-04840385`.

[44] O. Fawzi, M. Rahaman and M. Taheri. *Capacities of quantum Markovian noise for large times*. 2024. DOI: `10.48550/arXiv.2408.00116`. URL: `https://hal.science/hal-04844850`.

[45] O. Fawzi, M. Rahaman and M. Taheri. *Capacities of quantum Markovian noise for large times*. 2024. DOI: `10.48550/arXiv.2408.00116`. URL: `https://inria.hal.science/hal-04836984` (cit. on p. 14).

[46] L. Gao and M. Rahaman. *Generalized Stein’s lemma and asymptotic equipartition property for subalgebra entropies*. 2024. DOI: `10.48550/arXiv.2401.03090`. URL: `https://hal.science/hal-04390449`.

[47] M. Grothus and V. Vilasini. *Characterizing Signalling: Connections between Causal Inference and Space-time Geometry*. 2024. URL: `https://inria.hal.science/hal-04720646` (cit. on p. 15).

[48] C. Rouzé, D. S. França and Á. Alhambra. *Efficient thermalization and universal quantum computing with quantum Gibbs samplers.* 2024. DOI: `10.48550/arXiv.2403.12691`. URL: `https://hal.science/hal-04896046`.

[49] C. Rouzé, D. S. França and Á. Alhambra. *Optimal quantum algorithm for Gibbs state preparation.* 2024. DOI: `10.48550/arXiv.2411.04885`. URL: `https://hal.science/hal-04896053`.

[50] T. L. Roy-Deloison, E. P. Lobo, J. Pauwels and S. Pironio. *Device-independent quantum key distribution based on routed Bell tests.* 1st Apr. 2024. URL: `https://hal.science/hal-04595717`.

[51] R. Salzmann. *Quantitative Quantum Zeno and Strong Damping Limits in Strong Topology.* 10th Sept. 2024. URL: `https://hal.science/hal-04840639`.

[52] R. Salzmann, B. Bergh and N. Datta. *Robustness of Fixed Points of Quantum Channels and Application to Approximate Quantum Markov Chains.* 2nd May 2024. URL: `https://hal.science/hal-04840595`.

[53] S. Singh, M. Rahaman and N. Datta. *Zero-error communication under discrete-time Markovian dynamics.* 2024. DOI: `10.48550/arXiv.2402.18703`. URL: `https://hal.science/hal-04844856`.

[54] V. Vilasini and M. P. Woods. *A general quantum circuit framework for Extended Wigner's Friend Scenarios: logically and causally consistent reasoning without absolute measurement events.* 11th Nov. 2024. URL: `https://hal.science/hal-04837301` (cit. on p. 16).

[55] V. Vilasini and R. Colbeck. *Information-processing in theories constrained by no superluminal causation vs no superluminal signalling.* Feb. 2024. URL: `https://inria.hal.science/hal-04885726` (cit. on p. 15).

[56] V. Vilasini and R. Colbeck. *The standard no-signalling constraints in Bell scenarios are neither sufficient nor necessary for preventing superluminal signalling with general interventions.* 27th Jan. 2025. URL: `https://hal.science/hal-04913241`.

[57] G. Wang, D. S. França, G. Rendon and P. Johnson. *Faster ground state energy estimation on early fault-tolerant quantum computers via rejection sampling.* 11th Jan. 2024. DOI: `10.48550/arXiv.2304.09827`. URL: `https://hal.science/hal-04386720`.

[58] M. Woods. *Quantum Frequential Computing: a quadratic run time advantage for all algorithms.* 2024. DOI: `10.48550/arXiv.2403.02389`. URL: `https://hal.science/hal-04529846` (cit. on p. 17).

9.3 Cited publications

[59] A. A. Abbott, J. Wechs, D. Horsman, M. Mhalla and C. Branciard. 'Communication through coherent control of quantum channels'. In: *Quantum* 4 (2020), p. 333. DOI: `10.22331/q-2020-09-24-333`. arXiv: `1810.09826 [quant-ph]` (cit. on pp. 10, 11).

[60] M. Araújo, F. Costa and Č. Brukner. 'Computational Advantage from Quantum-Controlled Ordering of Gates'. In: *Phys. Rev. Lett.* 113.25 (Dec. 2014), p. 250402. DOI: `10.1103/PhysRevLett.113.250402`. arXiv: `1401.8127 [quant-ph]` (cit. on p. 10).

[61] G. Aubrun and S. J. Szarek. *Alice and Bob meet Banach.* Vol. 223. American Mathematical Soc., 2017 (cit. on p. 4).

[62] F. Baccari, R. Augusiak, I. Šupić and A. Acín. 'Device-Independent Certification of Genuinely Entangled Subspaces'. In: *Phys. Rev. Lett.* 125 (2020), p. 260507. DOI: `10.1103/PhysRevLett.125.260507`. arXiv: `2003.02285 [quant-ph]` (cit. on p. 12).

[63] F. Baccari, R. Augusiak, I. Šupić, J. Tura and A. Acín. 'Scalable Bell inequalities for qubit graph states and robust self-testing'. In: *Phys. Rev. Lett.* 124 (2020), p. 020402. DOI: `10.1103/PhysRevLett.124.020402`. arXiv: `1812.10428 [quant-ph]` (cit. on p. 12).

[64] S. Barman and O. Fawzi. 'Algorithmic Aspects of Optimal Channel Coding'. In: *tit* 64.2 (2017), pp. 1038–1045. URL: `http://arxiv.org/abs/1508.04095` (cit. on p. 7).

[65] S. Boulebnane, M. P. Woods and J. M. Renes. *Approximate quantum non-demolition measurements.* To appear in Phys. Rev. Lett. 2019. eprint: `arXiv:1909.05265` (cit. on p. 4).

[66] F. G. Brandao and K. M. Svore. 'Quantum speed-ups for solving semidefinite programs'. In: *2017 IEEE 58th Annual Symposium on Foundations of Computer Science (FOCS)*. IEEE, 2017, pp. 415–426 (cit. on p. 5).

[67] F. G. S. L. Brandão, R. Kueng and D. S. França. 'Faster quantum and classical SDP approximations for quadratic binary optimization'. In: *arXiv:1909.04613 [quant-ph]* (Aug. 2020). arXiv: 1909.04613. URL: `http://arxiv.org/abs/1909.04613` (visited on 29/06/2021) (cit. on p. 5).

[68] S. Bravyi and A. Kitaev. 'Universal quantum computation with ideal Clifford gates and noisy ancillas'. In: *Phys. Rev. A* 71 (2 Feb. 2005), p. 022316. DOI: `10.1103/PhysRevA.71.022316`. URL: `https://link.aps.org/doi/10.1103/PhysRevA.71.022316` (cit. on p. 9).

[69] P. Brown, H. Fawzi and O. Fawzi. 'Device-independent lower bounds on the conditional von Neumann entropy'. In: *arXiv preprint arXiv:2106.13692* (2021) (cit. on p. 6).

[70] S. Bubeck. 'Convex Optimization: Algorithms and Complexity'. en. In: *Foundations and Trends® in Machine Learning* 8.3-4 (2015), pp. 231–357. DOI: `10.1561/2200000050`. URL: `http://www.nowpublishers.com/article/Details/MAL-050` (visited on 24/12/2020) (cit. on p. 5).

[71] A. R. Calderbank and P. W. Shor. 'Good quantum error-correcting codes exist'. In: *pra* 54.2 (1996), p. 1098 (cit. on p. 8).

[72] G. Chiribella, G. M. D'Ariano and P. Perinotti. 'Quantum Circuit Architecture'. In: *Phys. Rev. Lett.* 101 (6 Aug. 2008), p. 060401. DOI: `10.1103/PhysRevLett.101.060401`. arXiv: `0712.1325 [quant-ph]`. URL: `https://link.aps.org/doi/10.1103/PhysRevLett.101.060401` (cit. on p. 10).

[73] G. Chiribella, G. M. D'Ariano, P. Perinotti and B. Valiron. 'Quantum computations without definite causal structure'. In: *Phys. Rev. A* 88 (2013), p. 022318. DOI: `10.1103/PhysRevA.88.022318`. arXiv: `0912.0195 [quant-ph]` (cit. on p. 10).

[74] G. Chiribella and H. Kristjánsson. 'Quantum Shannon theory with superpositions of trajectories'. In: *Proc. R. Soc. A* 475 (2019). DOI: `10.1098/rspa.2018.0903` (cit. on pp. 10, 11).

[75] G. Chiribella. 'Perfect discrimination of no-signalling channels via quantum superposition of causal structures'. In: *Phys. Rev. A* 86 (4 Oct. 2012), p. 040301. DOI: `10.1103/PhysRevA.86.040301`. arXiv: `1109.5154 [quant-ph]`. URL: `https://link.aps.org/doi/10.1103/PhysRevA.86.040301` (cit. on p. 10).

[76] M. Christandl and A. Müller-Hermes. 'Fault-Tolerant Coding for Quantum Communication'. In: *IEEE Transactions on Information Theory* 70.1 (2024), pp. 282–317 (cit. on p. 14).

[77] A. D'Aspremont, O. Banerjee and L. El Ghaoui. 'First-Order Methods for Sparse Covariance Selection'. In: *SIAM Journal on Matrix Analysis and Applications* 30.1 (Jan. 2008), pp. 56–66. DOI: `10.1137/060670985`. URL: `http://epubs.siam.org/doi/10.1137/060670985` (cit. on p. 4).

[78] G. De Palma, M. Marvian, D. Trevisan and S. Lloyd. 'The quantum Wasserstein distance of order 1'. In: *arXiv:2009.04469 [math-ph, physics:quant-ph]* (Sept. 2020). arXiv: 2009.04469. URL: `http://arxiv.org/abs/2009.04469` (visited on 29/06/2021) (cit. on p. 5).

[79] D. P. DiVincenzo, P. W. Shor and J. A. Smolin. 'Quantum-channel capacity of very noisy channels'. In: *pra* 57.2 (1998), p. 830. URL: `http://arxiv.org/abs/quant-ph/9706061` (cit. on p. 7).

[80] H. Dourdent, A. A. Abbott, N. Brunner, I. Šupić and C. Branciard. 'Semi-device-independent Certification of Causal Nonseparability with Trusted Quantum Inputs'. In: *Physical Review Letters* 129.9 (Aug. 2022). 5 + 17 pages, 1 figure, p. 090402. DOI: `10.1103/PhysRevLett.129.090402`. URL: `https://inria.hal.science/hal-03330393` (cit. on p. 16).

[81] F. Dupuis, O. Fawzi and R. Renner. 'Entropy accumulation'. In: *Communications in Mathematical Physics* 379.3 (2020). URL: `https://arxiv.org/abs/1607.01796` (cit. on p. 6).

[82] F. Dupuis, A. Goswami, M. Mhalla and V. Savin. 'Polarization of Quantum Channels using Clifford-based Channel Combining'. In: *IEEE Transactions on Information Theory* 67.5 (2021), pp. 2857–2877 (cit. on p. 8).

[83] B. Eastin and E. Knill. ‘Restrictions on Transversal Encoded Quantum Gate Sets’. In: *Phys. Rev. Lett.* 102 (11 Mar. 2009), p. 110502. DOI: `10.1103/PhysRevLett.102.110502`. URL: `https://link.aps.org/doi/10.1103/PhysRevLett.102.110502` (cit. on p. 9).

[84] D. Ebler, S. Salek and G. Chiribella. ‘Enhanced Communication with the Assistance of Indefinite Causal Order’. In: *Phys. Rev. Lett.* 120 (12 Mar. 2018), p. 120502. DOI: `10.1103/PhysRevLett.120.120502`. arXiv: `1711.10165 [quant-ph]` (cit. on pp. 10, 11).

[85] O. Fawzi, A. Grospellier and A. Leverrier. ‘Constant overhead quantum fault-tolerance with quantum expander codes’. In: *IEEE Symposium on Foundations of Computer Science (FOCS)*. 2018, pp. 743–754. URL: `http://arxiv.org/abs/1808.03821` (cit. on p. 8).

[86] D. S. Fran ça, S. Strelchuk and M. Studzi ński. ‘Efficient Classical Simulation and Benchmarking of Quantum Processes in the Weyl Basis’. In: *Phys. Rev. Lett.* 126 (21 May 2021), p. 210502. DOI: `10.1103/PhysRevLett.126.210502`. URL: `https://link.aps.org/doi/10.1103/PhysRevLett.126.210502` (cit. on p. 4).

[87] D. S. Franca and R. Garcia-Patron. ‘Limitations of optimization algorithms on noisy quantum devices’. In: *arXiv:2009.05532 [quant-ph]* (Sept. 2020). arXiv: 2009.05532. URL: `http://arxiv.org/abs/2009.05532` (visited on 29/06/2021) (cit. on p. 4).

[88] D. S. França and A. K. Hashagen. ‘Approximate randomized benchmarking for finite groups’. In: *Journal of Physics A: Mathematical and Theoretical* 51.39 (Sept. 2018), p. 395302. DOI: `10.1088/1751-8121/aad6fa`. URL: `https://iopscience.iop.org/article/10.1088/1751-8121/aad6fa` (cit. on p. 4).

[89] D. Gottesman. ‘Fault-tolerant quantum computation with constant overhead’. In: *Quantum Information and Computation* 14.15-16 (Nov. 2014), pp. 1338–1372 (cit. on p. 14).

[90] B. Groisman, M. Mc Gettrick, M. Mhalla and M. Pawłowski. ‘How quantum information can improve social welfare’. In: *IEEE Journal on Selected Areas in Information Theory* 1.2 (2020), pp. 445–453 (cit. on p. 11).

[91] P. A. Guérin, A. Feix, M. Araújo and Č. Brukner. ‘Exponential Communication Complexity Advantage from Quantum Superposition of the Direction of Communication’. In: *Phys. Rev. Lett.* 117 (Sept. 2016), p. 100502. DOI: `10.1103/PhysRevLett.117.100502`. arXiv: `1605.07372 [quant-ph]` (cit. on pp. 10, 11).

[92] R. Harper, S. T. Flammia and J. J. Wallman. ‘Efficient learning of quantum noise’. In: *Nature Physics* 16.12 (Aug. 2020), pp. 1184–1188. DOI: `10.1038/s41567-020-0992-8`. URL: `https://doi.org/10.1038%5C%2Fs41567-020-0992-8` (cit. on p. 4).

[93] M. . Hastings. ‘Superadditivity of communication capacity using entangled inputs’. In: *natphys* 5.4 (2009), pp. 255–257. URL: `http://arxiv.org/abs/0809.3972` (cit. on p. 7).

[94] A. Holevo. ‘Bounds for the quantity of information transmitted by a quantum communication channel’. In: *Problemy Peredachi Informatsii* 9.3 (1973), pp. 3–11 (cit. on p. 7).

[95] A. Holevo. ‘The additivity problem in quantum information theory’. In: *Proc. ICM.* Vol. 3. 2006, pp. 999–1018 (cit. on p. 7).

[96] A. Y. Kitaev. ‘Quantum computations: algorithms and error correction’. In: *Russian Mathematical Surveys* 52 (1997), p. 1191. DOI: `10.1070/RM1997v052n06ABEH002155` (cit. on p. 14).

[97] M. Kliesch, R. Kueng, J. Eisert and D. Gross. ‘Guaranteed recovery of quantum processes from few measurements’. In: *Quantum* 3 (Aug. 2019), p. 171. DOI: `10.22331/q-2019-08-12-171`. URL: `https://quantum-journal.org/papers/q-2019-08-12-171/` (cit. on p. 4).

[98] L. Kong and Z.-W. Liu. *Charge-conserving unitaries typically generate optimal covariant quantum error-correcting codes*. 2021. eprint: `arXiv:2102.11835` (cit. on p. 9).

[99] A. Kubica and R. Demkowicz-Dobrza ński. ‘Using Quantum Metrological Bounds in Quantum Error Correction: A Simple Proof of the Approximate Eastin-Knill Theorem’. In: *Phys. Rev. Lett.* 126 (15 Apr. 2021), p. 150503. DOI: `10.1103/PhysRevLett.126.150503`. URL: `https://link.aps.org/doi/10.1103/PhysRevLett.126.150503` (cit. on p. 9).

[100] F. Leditzky, M. A. Alhejji, J. Levin and G. Smith. 'Playing games with multiple access channels'. In: *Nature communications* 11.1 (2020), pp. 1–5 (cit. on p. 11).

[101] O. Oreshkov, F. Costa and Č. Brukner. 'Quantum correlations with no causal order'. In: *Nat. Commun.* 3 (2012), p. 1092. DOI: `10.1038/ncomms2076`. arXiv: `1105.4464 [quant-ph]` (cit. on p. 10).

[102] C. Rouzé and N. Datta. 'Concentration of quantum states from quantum functional and transportation cost inequalities'. en. In: *Journal of Mathematical Physics* 60.1 (Jan. 2019), p. 012202. DOI: `10.1063/1.5023210`. URL: `http://aip.scitation.org/doi/10.1063/1.5023210` (visited on 29/06/2021) (cit. on p. 5).

[103] G. Rubino, L. A. Rozema, D. Ebler, H. Kristjánsson, S. Salek, P. A. Guérin, A. A. Abbott, C. Branciard, Č. Brukner, G. Chiribella and P. Walther. 'Experimental Quantum Communication Enhancement by Superposing Trajectories'. In: *Phys. Rev. Research* 3 (2021), p. 013093. DOI: `10.1103/PhysRevResearch.3.013093` (cit. on p. 11).

[104] C. Shannon. 'A mathematical theory of communications'. In: *Bell System Technical Journal* 27 (4 1948), pp. 379–423 (cit. on p. 7).

[105] G. Smith and J. Yard. 'Quantum communication with zero-capacity channels'. In: *Science* 321.5897 (2008), pp. 1812–1815. URL: `http://arxiv.org/abs/0807.4935` (cit. on p. 7).

[106] A. Steane. 'Multiple-particle interference and quantum error correction'. In: *Proc. R. Soc. Lond. A* 452.1954 (1996), pp. 2551–2577 (cit. on p. 8).

[107] V. Vilasini and R. Colbeck. 'General framework for cyclic and fine-tuned causal models and their compatibility with space-time'. In: *Physical Review A* 106.3 (Sept. 2022). DOI: `10.1103/physreva.106.032204`. URL: `http://dx.doi.org/10.1103/PhysRevA.106.032204` (cit. on p. 15).

[108] C. Villani. *Optimal Transport*. Ed. by M. Berger, B. Eckmann, P. de la Harpe, F. Hirzebruch, N. Hitchin, L. Hörmander, A. Kupiainen, G. Lebeau, M. Ratner, D. Serre, Y. G. Sinai, N. J. A. Sloane, A. M. Vershik and M. Waldschmidt. Vol. 338. Grundlehren der mathematischen Wissenschaften. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. DOI: `10.1007/978-3-540-71050-9`. URL: `http://link.springer.com/10.1007/978-3-540-71050-9` (visited on 01/03/2021) (cit. on p. 5).

[109] D.-S. Wang, G. Zhu, C. Okay and R. Laflamme. 'Quasi-exact quantum computation'. In: *Phys. Rev. Research* 2 (3 July 2020), p. 033116. DOI: `10.1103/PhysRevResearch.2.033116`. URL: `https://link.aps.org/doi/10.1103/PhysRevResearch.2.033116` (cit. on p. 9).

[110] J. Wechs, A. A. Abbott and C. Branciard. 'On the definition and characterisation of multipartite causal (non)separability'. In: *New J. Phys.* 21 (2019), p. 013027. DOI: `10.1088/1367-2630/aaf352`. arXiv: `1807.10557 [quant-ph]` (cit. on p. 10).

[111] J. Wechs, H. Dourdent, A. A. Abbott and C. Branciard. 'Quantum Circuits with Classical Versus Quantum Control of Causal Order'. In: *PRX Quantum* 2 (2021), p. 030335. DOI: `10.1103/PRXQuantum.2.030335` (cit. on p. 11).

[112] M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2014. URL: `http://www.arxiv.org/abs/1106.1445` (cit. on p. 7).

[113] D. P. Woodruff. 'Sketching as a Tool for Numerical Linear Algebra'. en. In: *Foundations and Trends® in Theoretical Computer Science* 10.1-2 (2014), pp. 1–157. DOI: `10.1561/0400000060`. URL: `http://www.nowpublishers.com/articles/foundations-and-trends-in-theoretical-computer-science/TCS-060` (visited on 29/06/2021) (cit. on p. 6).

[114] M. P. Woods and Á. M. Alhambra. 'Continuous groups of transversal gates for quantum error correcting codes from finite clock reference frames'. In: *Quantum* 4 (Mar. 2020), p. 245. DOI: `10.22331/q-2020-03-23-245`. URL: `https://doi.org/10.22331/q-2020-03-23-245` (cit. on p. 9).

[115] M. P. Woods, R. Silva and J. Oppenheim. 'Autonomous Quantum Machines and Finite-Sized Clocks'. In: *Annales Henri Poincaré* 20.1 (Oct. 2018), pp. 125–218. DOI: `10.1007/s00023-018-0736-9`. URL: `https://doi.org/10.1007/s00023-018-0736-9` (cit. on pp. 4, 11).

[116] Y. Yang, Y. Mo, J. M. Renes, G. Chiribella and M. P. Woods. *Covariant Quantum Error Correcting Codes via Reference Frames*. 2020. eprint: `arXiv:2007.09154` (cit. on p. 9).

[117] S. Zhou, Z.-W. Liu and L. Jiang. *New perspectives on covariant quantum error correction*. 2020. eprint: `arXiv:2005.11918` (cit. on p. 9).