Mémoire pour une Habilitation à Diriger les Recherches de l'Université Grenoble Alpes
Discrete tools for understanding quantum information

Mehdi Mhalla
CRHC CNRS section 02
Laboratoire LIG équipe CAPP
Université Grenoble Alpes

Jury

Présidente	Prof.	Nadia Brauner	UGA, Laboratoire G-SCOP
Rapporteur	Prof.	Robert Raussendorf	Leibniz University Hannover, Allemagne
Rapporteur	DR	Frédéric Magniez	CNRS, IRIF
Rapporteur	DR	Omar Fawzi	Inria, LIP
Examinatrice	Prof.	Sophie Laplante	Université Paris Cité, IRIF

29/04/2025

Contents

Chapter 1

Introduction

At first glance, one might assume that since quantum information theory is formulated within the framework of complex Hilbert spaces, only tools from continuous mathematics can aid in understanding, manipulating, and controlling quantum systems. However, many tools from graph theory and discrete combinatorics offer significant insights into quantum information theory.

Here, we provide a brief overview of results we obtained[1], where discrete structures and graph-based descriptions have helped establish properties, reveal possibilities, or highlight limitations in quantum information theory.

First, we investigate quantum correlations in multipartite games and in measurement-based computation. Then we show an example where graphs help to prove properties about decoding information. Finally we give a brief overview of the different research directions taken, the various supervisions and the results obtained, to open the way to questions about other works that are not described here and to give a broader view of the different research results obtained and possible followups[2].

In Chapter 2 we discuss **quantumness by non-decomposability and multipartite correlations**.

Non-local games are a corner stone of quantum information theory. They describe settings where players not allowed to communicate try to correlate their answers and are the natural generalization of the experiments used to show that Einstein's hypothesis stating that quantum mechanics could be defined using local hidden variables was incorrect. This experiment earned Alain Aspect receiving the Nobel prize[3]. Non-local games have strong implications in different areas as can be seen in the famous result about complexity classes $MIP^* = RE$ [65]. The first chapter considers variations from these games:

- First, we try to capture, with combinatorial structures defined from graphs, the multipartiteness exhibited by correlations that can be obtained by quantum states. The starting point is the definition using graphs of families of games called pseudotelepathy games [20]. In these games, a set of players who are forbidden to communicate are asked to play a

[1] The proofs of the different results can be found in the corresponding papers in the arxiv version.

[2] We suppose that the reader has some basic notions of quantum information theory and refer to [92] as textbook.

[3] This prize was shared with John F. Clauser and Anton Zeilinger.

cooperative game such that it is impossible to win perfectly (with probability 1) with local strategies for classical players even when they have access to correlated randomness. However the players can achieve a pseudotelepathic behavior using quantum resources which means that they can win perfectly these games. We analyze the correlations within a general framework called contextuality [6]. This section presents results from [7, 8].

- Then we discuss multipartite correlations from graph states with classical communication. We consider here correlations that can be obtained in subsystems after local measurements and corrections on a disjoint subsystem. We present the results obtained in [30] and [29] in which we show that graph states described with projective planes and a family of reductions from them offer a very strong form of multipartite nonlocality in the sense that one can create using local operations and classical communication any graph state on any subset of $n^{1/4}$ qubits. We also show that one cannot hope to have any state with a bound better than $n^{1/2}$, and that the optimal bound is achieved with very high probability for a particular family of random bipartite graphs with explicitly chosen parameters.

- In the last section of this chapter we present our results from [1, 55] where we consider a setting much less studied in quantum information theory that is a central topic in classical game theory. In this setting different players have divergent interests and have access to different types of shared resources. We have shown that sharing quantum resources can give an exponential improvement and that surprisingly delegating the access to the quantum resources may help to achieve even better results than when each player has direct access to the resources.

In Chapter 3 we discuss **graph states for computation**. One of the many applications of graph states to quantum information theory is as a resource in the context of the one-way quantum computation [60] which consists in performing a quantum computation using single qubit measurements. We will explain in Chapter 3, how to characterize the possibility to use such graph states for a measurement based quantum computation assuming some restrictions called "robust determinism" which intuitively means that we want the way to implement an isometry by local measurements to be independent of the precise value of the non-Pauli angles. The results are from the publications [26, 42, 86–88]. We stay here in the combinatorial framework and try to understand as precisely as possible the time dependency in the transfer of information by measurement.

In Chapter 4 we use **graph as tools for analyzing message passing quantum decoders.** Error-correcting codes encode an information (a word in some finite alphabet) in codewords introducing substructures that put some distance between the codewords and that can be checked to ensure correctness offering the possibility of decoding *i.e.* removing the error.

The use of graphs is a cornerstone in coding theory and one very useful tool to represent codes is called the Tanner graph [111]. It is a bipartite graph with vertex sets representing check-nodes (allowing to get syndromes that check correctness of a codeword) and variable nodes (which contains the transmitted information and might have errors). In quantum information theory the most common codes are called stabilizer codes, and the graph states used in the previous chapters can be seen as stabilizer codes encoding one qubit. But they can also be used when considering more general codes. For instance [80] shows how by considering subsets of the vertices of graph state using a classical code one gets an interesting family of stabilizer

quantum codes from a graph state. In [81] it has even been proposed to use graphs as a universal encoding for stabilizer quantum codes. Poulin et al. [17] generalized the time slices to interpret consecutive syndrome measurement of a family of codes as a graph state in the analysis of decoding schemes for a family of codes and Raussendorf et al. [102] proposed the 3D lattice for fault tolerant measurement based quantum computing.

One very important decoding technique is Message passing (MP) decoding. MP decoding stands as both the fundamental theoretical reason behind the invention of classical Low-Density Parity-Check codes, and the key to their success and widespread application in real-world systems. However, quantum Low density Parity Check (LDPC) codes are known to be classically degenerate [98], thus the sparsity of their Tanner graph no longer fulfills its role of enabling efficient MP decoding, but merely acts as an enabler for fault-tolerance (*e.g.*, fault-tolerant syndrome extraction and fault-tolerant operations on logical qubits). Consequently, a significant effort has been devoted over the last few years to efficient decoding of quantum LDPC codes, by either combining the MP decoding with a post-processing step [38,39,94,105], and/or improving the MP decoding performance itself [75, 93, 104, 115, 117].

In Chapter 4 we show how classical tools to explore the message exchange using trees in classical codes can be adapted to show limitations for the message passing decoding of Kitaev's quantum toric code [73], which is the most commonly used code in practical implementations. The results are from [34] and were obtained during Julien Du Crest Ph.D.

Chapter 2

Quantumness by non-decomposability, correlations from graph states

What is quantumness? What is the phenomenon that makes quantum information theory go beyond classical information theory? Different directions could be taken to answer this question, e.g., considering superposition, entanglement, non clonability, or the fact that what can be seen is just a base of the space describing what can be. Any such angle offers a perspective on non classicality of quantum information theory. As the definition of quantum state is captured at the limit by local tomography it is natural to consider the correlations reachable by local measurements as capturing at the limit the essence of quantumness. Correlations are a description of randomness.

One main feature of quantum information theory is that measurement produces randomness. There are two sources of randomness within quantum information theory:

The first is by the choice of the interaction with a system. The classical outcome obtained by measuring a qubit depends not only on the state of the qubit, but also on the type of the measurement. A qubit u in the state $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ gives a perfect random bit when measured in the Z basis (we say that $t_u = 0$ for this choice of base) and always the bit 1 when measured in the X basis (i.e. when $t_u = 1$). Therefore, the conditional probability associated to its outcome a_u satisfies $P(a_u|t_u)$ is such that $p(1|0) = p(0|0) = 1/2$ and $p(0|1) = 1$, $p(1|1) = 0$. This probability can be understood under statement "it would have been deterministic if a measured according to an other measurement". The classical outcome of a measurement that projected the state onto a hyperplane (or a subspace) can be read as the state was perfectly defined in the available space and it was not orthogonal to its new state or subspace that is perfectly described by the measurement.

The second and more intricate source of randomness is by considering a part of an entangled system. The state of a system of two qubits $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ provides as marginals two random bits for each qubits in any basis but contains a correlation when both qubits are measured in the same basis whether it is in the X or in the Z basis. Quantum information theory shows that this correlation cannot be explained by shared random variables. To capture the state of the system one has to consider it as a bipartite system. In this case quantum information says

that "ìt would have been deterministic" only if it was defined in a larger subspace and cannot be deterministic when defined "locally".

Somehow by using Hilbert spaces quantum information theory allows to describes basic elements that are qubits which when viewed in the "good" space *i.e.* in a space large enough, allows to describe a system without loss of information "hiding" multipartite correlations to the most general definitions of its components.

In this section we will use graphs to describe the quantumness of multipartite states by investigating the correlations their local measurements allow to obtain.

2.1 Correlations in multipartite graph games

2.1.1 Cooperative multipartite graph games

We start with a simple combinatorial formalization for cooperative games where for simplicity we will restrict ourselves to the binary case unless specified otherwise.

Cooperative games: A multipartite cooperative game $\mathcal{G}$ for a set V of players is a combinatorial scenario characterized by a set $\mathcal{L} \subseteq \{0,1\}^V \times \{0,1\}^V$ of losing pairs (or a set $\mathcal{W}$ of winning pairs): each player u is asked a binary question (or have a local binary type) t_u and has to produce a binary answer a_u. The collaborative game is won by the players if for a given question $t \in \{0,1\}^V$ they produce an answer $a \in \{0,1\}^V$ such that the pair formed by a and t, denoted $(a|t)$, is not a losing pair, i.e. $(a|t) \notin \mathcal{L}$ (or equivalently $(a|t) \in \mathcal{W}$).

A combinatorial multipartite game cannot be perfectly won using classical strategies without communication (after the questions have been received) if every local deterministic strategies mapping t_u to a_u for each player u induce a set of possible pairs $(a|t)$ that intersects $\mathcal{L}$. Giving players access to extra shared random variables does not change this: a game that is not perfectly winnable classically without communication remains unwinnable even with shared randomness. Therefore, we use the term classical to refer to the case where the players have access only to shared randomness, which can be seen as agreeing beforehand on an infinite tape of random bits.

A game is called **pseudotelepathic** [20] if it is not perfectly winnable classically (without communication), but can be won perfectly using quantum resources, such as entangled states. It is possible for players sharing a quantum state to induce a set of possible pairs $(a|t)$ that is a subset of $\mathcal{W}$. This phenomenon gives the illusion of telepathy to a skeptic of quantum mechanics, as the only classical explanation for a perfect winning strategy would be communication between the players.

An n-player strategy here is viewed as a protocol without communication in which each player has access to some kind of resource.

Example 1: The losing set associated with the Mermin parity game [84] is $\mathcal{L}_{\mathbf{Mermin}} = \{(a|t) : \sum t_i = 0 \bmod 2 \text{ and } \sum a_i + (\sum t_i)/2 = 1 \bmod 2\}$. Notice that the losing set admits the following simpler description: $\mathcal{L}_{\mathbf{Mermin}} = \{(a|t) : 2|a| = |t| + 2 \bmod 4\}$, where $|t| = |\mathrm{supp}(t)|$ is the Hamming weight of t.

To explain the games that we introduced in [8] we first introduce some graph notations.

Graph notations. We consider finite simple undirected graphs. Let $G = (V, E)$ be a graph.

For any vertex $u \in V$, $N_G(u) = \{v \in V \mid (u, v) \in E\}$ is the neighborhood of u.

For any $D \subseteq V$, the odd neighborhood of D is the set of all vertices which are oddly connected to D in G: $\mathrm{Odd}(D) = \{v \in V : |D \cap N(v)| = 1 \bmod 2\}$ (See Figure 2.1).

$\mathrm{Even}(D) = V \setminus \mathrm{Odd}(D)$ is the even neighborhood of D, and $\mathrm{loc}(D) = D \cup \mathrm{Odd}(D)$ is the local set of D which consists of the vertices in D and those oddly connected to D.

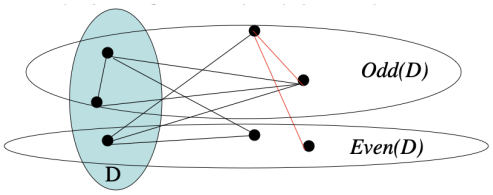

Figure 2.1: Even and odd neighborhoods.

For any $D \subseteq V$, $G[D] = (D, E \cap D \times D)$ is the subgraph induced by D, and $|G[D]|$ its size, *i.e.* the number of edges of $G[D]$.

Note that Odd can be realized as a linear map (where we consider subsets as binary vectors), which implies that for any two subset of vertices A, B, $\mathrm{Odd}(A \oplus B) = \mathrm{Odd}(A) \oplus \mathrm{Odd}(B)$ where $\oplus$ denotes the symmetric difference.

We introduce the notion of **involvement**: Given a graph $G = (V, E)$, a set $D \subseteq V$ of vertices is **involved** in a binary labelling $t \in \{0, 1\}^V$ of the vertices if $D \subseteq \mathrm{supp}(t) \subseteq \mathrm{Even}(D)$, where $\mathrm{supp}(t) = \{u \in V | \, t_u = 1\}$.

In other words, D is involved in the binary labelling t, if all the vertices in D are labelled with 1 and all the vertices in $\mathrm{Odd}(D)$ are labelled with 0. Notice that when $G[D]$ is not a union of Eulerian graphs[1], there is no binary labelling in which D is involved. On the other hand, if $G[D]$ is a union of Eulerian graphs, there are $2^{|\mathrm{Even}(D)|-|D|}$ binary labellings in which D is involved.

In [8] we defined games associated to graphs, to extend standard known pseudotelepathy games and propose a whole new family.

Cooperative graph games MCG(G): A multipartite cooperative game $\mathrm{MCG}(G)$ associated with a graph $G = (V, E)$, where V is a set of players, is the collaborative game where the set of losing pairs is $\mathcal{L}_G := \{(a|t) : \exists D$ involved in t s.t. $\sum_{u \in \mathrm{loc}(D)} a_u = |G[D]| + 1 \bmod 2\}$. In other words, the collaborative game is won by the players if for a given question $t \in \{0, 1\}^V$ they produce an answer $a \in \{0, 1\}^V$ such that for any non-empty D involved in t,

$$\sum_{u \in \mathrm{loc}(D)} a_u = |G[D]| \bmod 2$$

Example : Consider $\mathrm{MCG}(K_n)$ the collaborative game associated with the complete graph K_n of order n. When a question t contains an even number of 1s the players trivially win since

[1] The following three properties are equivalent: (i) $D \subseteq \mathrm{Even}(D)$; (ii) every vertex of $G[D]$ has an even degree; (iii) $G[D]$ is a union of Eulerian graphs. Notice that $D \subseteq \mathrm{Even}(D)$ does not imply that $G[D]$ is Eulerian as it may not be connected.

there is no non-empty subset of vertices involved in such a question. When t has an odd number of 1s, the set of players (vertices) involved in this question is $D = \text{supp}(t)$. In this case, all the players are either in D or $\text{Odd}(D)$ thus the sum of all the answers has to be equal to $|G[D]| = \frac{|D|(|D|-1)}{2} = \frac{|D|-1}{2} \bmod 2$. Thus for the complete graph K_n, $\mathcal{L}_{K_n} = \{(a|t) : |t| = 1 \bmod 2 \text{ and } |a| = \frac{|t|-1}{2} + 1 \bmod 2\} = \{(a|t) : 2|a| = |t| + 1 \bmod 4\}$.

Note that for this particular graph, the constraints are global in the sense that the sum of the answers of all the players is used for all the questions.

Notice also that the set of losing pairs $\mathcal{L}_{K_n} = \{(a|t) : 2|a| = |t| + 1 \bmod 4\}$ is similar to the one of the Mermin parity game, $\mathcal{L}_{\textbf{Mermin}} = \{(a|t) : 2|a| = |t| + 2 \bmod 4\}$.

To define a quantum strategy, in which the players have access to quantum resources, we use **graph states**. Given a graph G, the graph state $|G\rangle$ is defined as

$$|G\rangle = \frac{1}{\sqrt{2^{|V|}}} \sum_{y \in \{0,1\}^V} (-1)^{|G[\text{supp}(y)]|} |y\rangle$$

It has one qubit per vertex of the graph and is the fix point of the commuting Pauli operators $X_u Z_{N(u)}$ obtained by applying Pauli operator X on u and Z on all the vertices of $N_G(u)$.

It can be obtained from the pure quantum state $|+\rangle^V$ corresponding to the state such that each player have a qubit in the state $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ by applying CZ, the controlled Z unitary operator, on each pair $(u, v) \in E$.

The reference [60] provides a good introduction on these states.

2.1.2 Pseudotelepathy in combinatorial multipartite graph games

If players share a graph state $|G\rangle$, we defined a quantum strategy QSTRAT for $\text{MCG}(G)$:

Quantum strategy QSTRAT: Given a shared graph state $|G\rangle$, and a question t, every player u measures his qubit according to the Pauli observable X if $t_u = 1$ and according to the Pauli observable Z if $t_u = 0$. Every player answers the outcome $a_u \in \{0, 1\}$ of this measurement.

We have proven in [8] during the internship of Anurag Anshu that, not only for any graph G, players sharing $|G\rangle$, and applying QSTRAT, never lose at $\text{MCG}(G)$, but also that:

Theorem (1 of [8]) $\text{MCG}(G)$ is pseudotelepathic if and only if G is not bipartite.

The proof relies on the existence of a subset of vertices $D = v_1, \dots v_{2k+1}$ such that the subgraph $G[D]$ induced by the vertices is an odd cycle. It uses the fact that the stabilizer properties ensures that when applying QSTRAT for the odd cycle C_{2k+1}, the sum of the answers is always odd when the players have each $t_u = 1$ and that for any vertex u with $t_u = 1$ that has neighbors v, w with $t_v = t_w = 0$ the sum $a_u + a_v + a_w$ of their answers given by QSTRAT is 0.

Notice that extending $\mathcal{L}$ to a superset respecting the support of a quantum strategy preserves the property of being pseudotelepathic. In [55] we considered games with restricted set of questions while preserving the pseudotelepathic property. In Table 2.1.2, we give the winning conditions of a 5-player game defined in [55], that we will use in section 2.3. $\text{NC}_{01}(C_5)$ is a symmetrized version built from the multipartite game on a cycle $\text{MCG}(C_5)$ so that for each player there are as many questions where the associated type is 1 as ones where the associated type is 0.

Question $t_1t_2t_3t_4t_5$	Winning condition
10100	$a_5 \oplus a_1 \oplus a_2 = 0$
01010	$a_1 \oplus a_2 \oplus a_3 = 0$
00101	$a_2 \oplus a_3 \oplus a_4 = 0$
10010	$a_3 \oplus a_4 \oplus a_5 = 0$
01001	$a_4 \oplus a_5 \oplus a_1 = 0$
11111	$a_1 \oplus a_2 \oplus a_3 \oplus a_4 \oplus a_5 = 1$

Table 2.1: Winning conditions for the $\mathrm{NC}_{01}(C_5)$ family of games.

2.1.3 Pseudotelepathy in non-local games (with probability distributions)

In an analysis of the game, when repeated several times, one can define by counting the different occurrences of each pair $(a|t)$ a probability $P'(a,t)$ and decompose it as a prior probability $\Pi(t)$ and a conditional probability $P(a|t)$, where a and t are obtained by gluing answers and questions.

We suppose that the n players are in a setting in which they cannot communicate between the time they get their local question t_i and produced the answer a_i in any run. The games are called **non-local** as ensuring the non communication in an implementation of the game is often done by spatially separating the players and assuming the impossibility of faster than light communication.

This setting (with Π known to the players) is the one intensively studied in quantum information theory as it captures Bell inequalities which is the setting used to convince the scientific community if the validity of quantum physics as it shows how classical decomposition (in terms of events and preparations locally defined and having access to a common past fails to capture observable statistics correctly predicted by the quantum model.[2] It is a very rich topic in quantum of information and allowed to prove important results both in quantum and in classical complexity theory [21, 65], distributed computing [49] *e.t.c.*[3]

In [7] we have proven that :

Lemma (1 of [7]) The quantum strategy QSTRAT, not only produces correct answers, but provides all the good answers "uniformly".

It means that given a graph $G = (V, E)$ and question $t \in \{0,1\}^V$, the probability $P(a|t)$ to observe the outcome $a \in \{0,1\}^V$ when each qubit u of a graph state $|G\rangle$ is measured according to Z if $t_u = 0$ or according to X if $t_u = 1$ satisfies: The probability distribution obtained when each player u measures his qubit of the shared graph state according to X when $t_u = 1$ or according to Z when $t_u = 0$ satisfies:

$$P(a|t) = \begin{cases} 0 & \text{if } (a|t) \in \mathcal{L} \\ \frac{|\{D \text{ involved in } t\}|}{2^{|V|}} & \text{otherwise.} \end{cases}$$

[2] In [47] we have shown that the Bell inequalities separating the quantum correlations from the classical ones and the Tsirelson bounds showing the limitations of the quantum correlations without communication can have a formal proof.

[3] In some cases it is explicitly the setting used, in other it offers a way to view the results.

The probability distribution produced by QSTRAT depends on the number of sets D involved in a given question t. Notice that a set $D \subseteq \text{supp}(t)$ is involved in t if and only if $D \in \text{Ker}(L_t)$, where L_t linearly[4] maps $A \subseteq \text{supp}(t)$ to $\text{Odd}(A) \cap \text{supp}(t)$. Thus $|\{D \text{ involved in } t\}| = 2^{|t|-rk_G(t)}$, where $rk_G(t) = \log_2(|\{L_t(A) : A \subseteq \text{supp}(t))\}|)$ is the rank of $L_t = A \mapsto \text{Odd}(A) \cap \text{supp}(t)$.

It is very interesting to see that for these correlations, if the players have access to shared random variables, the quantum correlations of QSTRAT is equivalent to any strategy that gives only good answers for any question.

Lemma (4 of [7]) With shared random variables it is equivalent to give only good answers and to simulate the quantum strategy.

This shows that the combinatorial structure really captures the quantum behavior for this family of correlations.

As quantum theory is consistent with the impossibility of faster than light communication, the correlations obtained by local quantum strategies are *non-signalling*. It means that a set of players cannot acquire information about each other's input.

The strong (and most commonly used) version of non-signalling conditionnal probability distributions supposes that even if a given set of players knew each other's input and output, they cannot get information about the input of a player that is not in this set. This means that in the case where the inputs are in $\{0, 1\}$ the probability distribution satisfies: for any input $(t_1, t_2 \dots t_n)$, output $(a_1, a_2 \dots a_n)$ and any index $i \in [n]$,

$$\sum_{a_i} P(a_1, a_2 \dots a_n | t_1, \dots t_{i-1}, 0, t_{i+1} \dots x_n) = \sum_{a_i} P(a_1, a_2 \dots a_n | t_1, \dots t_{i-1}, 1, t_{i+1} \dots t_n)$$

This property can be viewed as a virtual type of ressource called multipartite nonlocal boxes. It refers to a virtual device that is shared between multiple parties $(1, 2 \dots n)$ and characterized by a joint probability distribution $P(a_1, a_2 \dots a_n | t_1, t_2 \dots t_n)$, where $(t_1, t_2 \dots t_n)$ is the 'input' to the box and $(a_1, a_2 \dots a_n)$ is the 'output'.

The term **nonlocal** implies that this probability cannot be written as $\sum_l p_l * P_l(a_1|t_1) * P_l(a_2|t_2) \dots P_l(a_n|t_n)$ $(p_l > 0, \sum_l p_l = 1)$, or equivalently that it cannot be simulated by a local classical protocol. It is a natural extension of the PR boxes [97] which is an important tool that played an important role in understanding quantum correlations and their usefulness in communication [69].

It has been observed that some multipartite correlations cannot be achieved with bipartite resources [14], and many notions were developed to characterize the correlations obtained for instance in [13] and such notions are still being developed [95].

We therefore introduced in [7] a measure of non classicality by obstruction to decomposability called multipartiteness width when using k-partite nonlocal boxes as extra resources for the players. It is defined in the setting of contextuality.

[4] L_t is linear for the symmetric difference: $L_t(D_1 \oplus D_2) = L_t(D_1) \oplus L_t(D_2)$

2.1.4 Contextuality with hypergraphs and multipartiteness width

A framework that has been broadly studied and that formalises possible sets of correlations strictly containing the ones observed used quantum resources is the framework of contextuality. There are many different models to describe contextuality [4,6,28,74]. The main general idea is that *a priori* the description of a system may depend on the context, wether it is its preparation or measurement or link with the environment.

We will follow a very general combinatorial setting that was proposed in [6]. One way to view this model is that one can consider that any repeatable experiment may have different "measurement settings" that allow to observe outcomes and that some outcomes may belong to different settings.

Formally a contextuality scenario is represented by a hypergraph whose hyperedges are the measurements and whose vertices or events are the outcomes measured in some setting. An interpretation of such scenario is mapping its vertices to positive real number that sum to one for all hyperedges that could be seen as (intrinsic) probabilities of outcomes viewed as events.

- Deterministic interpretations corresponds to probability distributions in $\{0,1\}$ that represent an independent set of vertices such that each hyperedge contains exactly a vertex.
- Classical interpretations can be seen as convex mixture of deterministic interpretations.
- Quantum interpretations are probability distributions that can be described by measurements of a shared quantum state.

With any multipartite collaborative game MCG(G), we associate a hypergraph which describes a contextuality scenario in the sense of the hypergraph approach to contextuality. The vertices are the pairs $(a|t)$ and each hyperedge corresponds, roughly speaking, to a constraint.

The hyperedges can be decomposed into two subsets: those (H_{Nsig_V}) which guarantee no-signaling and those (H_G), depending on the graph G, which avoid the losing pairs:

- H_{Nsig_V} is the hypergraph representing the no-signaling polytope. It corresponds [6] to the Bell scenario $B_{|V|,2,2}$ where $|V|$ parties have access to 2 local measurements each, each of which has 2 possible outcomes (see Figure 2.2), which is obtained as a product[5] of the elementary scenario $B_{1,2,2}$.
- The hypergraph H_G defined on the same vertex set, corresponds to the game constraints: for each question[6] $t \in \{0,1\}^V$ we associate an hyperedge e_t containing all the answers which make the players win on t *i.e.*, $e_t = \{(a|t) \in \{0,1\}^V \times \{0,1\}^V, (a|t) \notin \mathcal{L}\}$.

[5]The Foulis Randall product of scenarios [6] is the scenario $H_A \otimes H_B$ with vertices $V(H_A \otimes H_B) = V(H_A) \times V(H_B)$ and edges $E(H_A \otimes H_B) = E_{A\to B} \cup E_{A\leftarrow B}$ where $E_{A\to B} := \{\cup_{a\in e_A}\{a\} \times f(a) : e_a \in E_A, f : e_A \to E_B\}$ and $E_{A\leftarrow B} := \{\cup_{b\in e_A} f(b)\times\{b\} : e_b \in E_b, f : E_B \to E_A\}$. In the multipartite case there are several ways to define products, however they all correspond to the same non-locality constraints [6]. Therefore one can just consider the minimal product $^{\min}\otimes_{i=1}^n H_i$ which has vertices in the cartesian product $V = \Pi V_i$ and edges $\cup_{k\in[1,n]} E_k$ where $E_k = \{(v_1 \dots, v_n), v_i \in e_i \, \forall i \neq k, \, v_k \in f(\overrightarrow{v})\}$ for some edge $e_i \in E(H_i)$ for every party $i \neq k$ and a function $\overrightarrow{v} \mapsto f(\overrightarrow{v})$ which assigns to every joint outcome $\overrightarrow{v} = (v_1 \dots v_{k-1}, v_{k+1}, \dots v_n)$ an edge $f(\overrightarrow{v}) \in E(H_k)$ (the k^{th} vertex is replaced by a function of the others).

[6]Note that for the questions x for which there exists no D involved in x, all the answers are allowed thus the constraints represented by the associated edge is a hyperedge of no-signaling scenario H_{Nsig}.

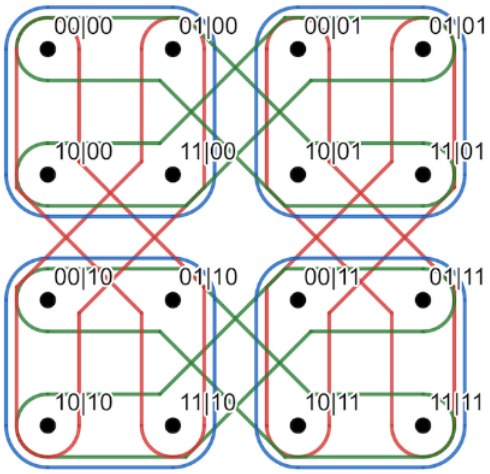

Figure 2.2: H_{Nsig_2}: hyperedges of the Bell scenario from [62]

Given a graph $G = (V, E)$, MCG(G) is a *pseudotelepathy* game if it admits a quantum model ($\mathcal{Q}(H_G \cup H_{\mathrm{Nsig}_V}) \neq \emptyset$) which means that players sharing a quantum states can win using their local measurement, but no classical model ($\mathcal{C}(H_G \cup H_{\mathrm{Nsig}_V}) = \emptyset$).

It is interesting to go back to the models of contextuality defined in [5] using sheaf theory as the probabilistic contextuality is what we considered in [8] as it corresponds to investigating the possibility of simulating a probability distribution of a quantum strategy playing with graph states. The two other levels of contextuality can gain some new perspectives when viewed as games: indeed the possibilistic contextuality is similar to the fact that the players cannot give all the good answers with non zero probability using classical local strategies, and strong contextuality is similar to the case where classical players cannot win the game (even by giving a strict subset of the good answers).

In [62], we have proven that as from a non-local game one has immediately a contextuality scenario on can also associate a nonlocal game by choosing the appropriate labeling to any contextuality scenario but one have to add extra events to have a product structure.

Within this framework we defined k-**multipartiteness** as :

An interpretation $P : \{0,1\}^V \times \{0,1\}^V \to [0,1]$ is k-**multipartite** if it can be obtained by a strategy without communication using nonlocal boxes that are at most k-partite: for any set $I \subset V$ with $|I| \leq k$, each player has access to one bit of a variable $\lambda_I(a_I|t_I)$ that has a no-signaling probability distribution.

In other words, a k-multipartite interpretation can be obtained with no-signaling correlations involving at most k players. For example the strategy to win the Mermin game proposed in [24] where each pair among n players share a (2-partite) non-localbox and each player outputs the sum of his boxes' ouputs is a 2-multipartite interpretation. Similarly, the result in [14] where they prove that a probability distribution that can be obtained by 5 players measuring a quantum state cannot be simulated without communication using any number of bi-partite non-local boxes shows that it is not a 2-multipartite interpretation.[7]

[7]The probability distribution described in [14] corresponds to the quantum winning strategy QSTRAT on the

A scenario has a **multipartiteness width** k if it admits a k-multipartite interpretation but no $(k-1)$-multipartite interpretation. It means that we introduced a hierarchy grading multipartiteness (which can be used as a measure of quantumness) as distance from classicality when assisted with non signaling locally bounded correlating ressouces and shared randomness.

In a contextual scenario, the more hyperedges one adds the less possible interpretations exist (the interpretations of a hypegraph with one extra hyperedge are a subset of the interpretations of the one with one less constraint). A scenario has a multipartiteness width k if its hyperedges already forbids all the interpretations of a product of Bell scenarios on less than k parties. For a scenario, having a classical interpretation means being decomposable : one can think of the probability distribution as local actors acting each on his bit and that's a classical interpretation. The multipartiteness width measure how non-decomposable a scenario is : it can not be decomposed with interpretations where each subspace has a small width. It can be therefore seen unformally as a "measure of non classicality" or as a "measure of quantumness" when it is within the quantum scenarios.

It implies that the players cannot perfectly win the game if they have only quantum systems on less than k qubits, this corresponds to using k separable states as resources as defined in [57].

We have shown in [7] with probabilistic arguments that:

Theorem (1 of [7]) There exists graph states on n qubits such that the correlations induced by QSTRAT have $0.11n$ mutipartiteness width

In terms of explicit family we know from [8] that the explicit family called Paley graphs have a logarithmic multipartiteness width. Indeed, in [7] the sufficient notion used to ensure multipartiteness width was k-**odd domination**, which was used to ensure a notion of k-way genuinely non signaling in [8] for the Paley graphs. This notion is defined as follows:

A graph $G = (V, E)$ is k-**odd dominated** (k-o.d.) if and only if for any $S \in \binom{V}{k}$, there exists a labelling of the vertices in $S = \{v_1, \dots, v_k\}$ and $C_1, \dots C_k$, s.t. $\forall i$, $C_i \subseteq V \setminus S$ and $\mathrm{Odd}(C_i) \cap \{v_i, \dots v_k\} = \{v_i\}$ and $C_i \subseteq \mathrm{Even}(C_i)$.

2.2 Vertex minor universality

Instead of just producing correlations without communicating one may consider producing using only Local Operations and Classical Communication (LOCC) the resources that allow to obtain these correlations.

In [30] then in [29] which was presented at ICALP 2024, with Maxime Cautrès (who was in Internship at the time and is now a Phd Student co-supervised with Valentin Savin), and other researchers from quantum and graph theory we investigated what quantum states exhibit the most uniform/anonymous/universal multipartite nonlocality, taking the perspective of pseudotelepathy games and viewing the indecomposable basic elements of the state (qubits) as players. We want the initial resource to be strong enough to ensure that if a referee chooses any subset of k players among n, and asks them to play any MCG pseudotelepathy graph game, they can win with probability 1. The uniformity/anonymity of multipartite nonlocality corresponds to the fact that any subset of k among n can win, and the universality by varying the set of possible games.

graph state $|C_5\rangle$ obtained from a cycle with 5 vertices.

The problem follows the idea presented in [22] about the problem of producing EPR pairs among any k pairs of parties among n using only LOCC. More precisely, we considered a more general formulation of the problem where the objective is to produce any stabilizer state and therefore any graph state, focusing on the fundamental case where each party has one qubit and we provided an exponential improvement with respect to [22] and a tight characterization. Beyond the fundamental aspect of characterizing the strength of correlations between elementary elements (qubits), the case of one qubit per party might have a practical relevance as it is much more likely in the future and much less costly to have many parties with possibility of acting on one qubit that they can receive.

A natural use of such state as a resource is in a setting where a source can distribute quantum states to parties that have one qubit quantum computers. For instance one can imagine a measurement based quantum computing model [102] (see Chapter 4), using a graph state as entangled initial resource and performing any computation by means of local measurements in a distributed scenario. Here we want the best resource to share so that any subset of the partners may be able to do the computation. A second possible use for the states we describe is that if a (possibly distributed) quantum computer on n qubits is wired in such a way that CZ operations are easy to implement for the pairs that are connected in the proposed graph family (can be prepared before the computation) and if each qubit can have a Bell measurement with an input qubit, then the notion of k stabilizer universal state ensures that for any input arriving on any k qubits, any set of two qubits CZ operations on the input state can be implemented with local Pauli measurements.

We introduced the notion of stabilizer universality: given an integer k we say that an n qubit quantum state is k-stabilizer universal when **any** stabilizer state on **any** k qubits among n can be induced by means of LOCC protocols. Notice that stabilizer universality is a generalization of the notion of pairability introduced in [22]. Our main objective is to design k-stabilizer universal states where the number n of qubits is as small as possible with respect to k. Our main tool is the graph state formalism and the ability to characterize properties of quantum states using tools from graph theory.

We call a graph k-vertex-minor universal if any graph defined on any k of its vertices can be obtained by means of local complementations[8] and vertex deletions. If a graph is k-vertex-minor universal, the corresponding graph state is k-stabilizer universal, hence we focus on the construction of vertex-minor universal graphs.

First, we studied what properties a graph must have in order to be k-vertex-minor universal. A crucial graph parameter, with regards to the entanglement properties of graph states, is the local minimum degree δ_{loc} – the minimum degree up to local complementation – which is closely related to the k-uniformity of the corresponding graph state [31]. We have shown that a graph needs to exhibit a rich entanglement structure in order to be k-vertex-minor universal.

Proposition (1 of [30]) If a graph of local minimum degree δ_{loc} is k-vertex-minor universal then $k < \delta_{\text{loc}} + 2$.

We also proved that the order n of a k-vertex-minor universal graph is least quadratic in k.

[8] Local complementation on a vertex u consists in complementing the subgraph induced by its neighbors.

Proposition (5 of [30]) If a graph of order n is k-vertex-minor universal then $k < \sqrt{2n\log_2(3)} + 2$.

Our first major contribution was to prove that there exist k-vertex-minor universal graphs of order quadratic in k. This is asymptotically optimal according to the bound above.

Theorem (8 of [29]) For any constant $\alpha > 2$, there exists k_0 s.t. for any $k > k_0$, there exists a k-vertex-minor universal graph G of order at most αk^2.

The construction of this k-vertex-minor universal graph is probabilistic as it implies a randomly generated bipartite graph. However, we have shown that the probability of creating a k-vertex-minor universal graph can be chosen to be arbitrarily close to 1, with a small overheard in the number of qubits.

Our second main contribution tackled the problem of constructing explicit families of k-vertex-minor universal graphs (in opposition to the probabilistic method).

We derive our constructions from the incidence graph $\mathbb{G}_q$ of the projective plane over the finite field $\mathbb{F}_q$, where q is a prime power. It is a bipartite graph of order $n = 2(q^2+q+1)$, with the same number $(n/2)$ of left and right vertices, corresponding respectively to points and lines of the projective plane (equivalently, 1-dimensional and 2-dimensional linear subspaces of $\mathbb{F}_q^3$). It satisfies the following properties:

- Any line contains exactly $q+1$ points, and any point is contained in exactly $q+1$ lines.
- Any two distinct lines intersect in one point, and for any two distinct points there is one unique line containing them.

We have shown that it satisfies the k-vertex-minor universality property, with $k = \Theta(n^{1/4})$.

Theorem (19 of [29]) Let k be such that $7k^2 - 16 \leqslant 4q$. Then $\mathbb{G}_q$ is k-vertex-minor universal.

Then we considered constructions obtained by building non bipartite graphs using reductions.

φ-reduction Let G be a bipartite graph and $\varphi : L(G) \to R(G)$ mapping left vertices to right vertices. The φ-reduction of G is the graph G_φ such that:

- The vertex set of G_φ is the left vertex set of G, that is $V(G_\varphi) = L(G)$,
- There is an edge between $a, b \in V(G_\varphi)$, if $a \neq b$ and either (a and $\varphi(b)$) or (b and $\varphi(a)$) are neighbors in G, that is,

$$E(G_\varphi) = \{(a,b) \,:\, a \neq b \text{ and } [\,(a,\varphi(b)) \in E(G) \text{ or } (b,\varphi(a)) \in E(G)\,]\,\}$$

The reduction is said to be **bijective** if φ is bijective. It is said to be **symmetric** if φ is such that $(a,\varphi(b)) \in E(G) \Leftrightarrow (b,\varphi(a)) \in E(G), \forall a, b \in L(G)$.

We enforce the condition $a \neq b$ in the definition of $E(G_\varphi)$, in order to avoid loops in case $(a,\varphi(a)) \in E(G)$ for some $a \in L(G)$.

Let G_φ be a bijective, symmetric reduction of G. For any vertex $a \in V(G_\varphi) = L(G)$, let $N_{G_\varphi}(a) \subseteq L(G)$ be the set of neighbors of a in G_φ, and $N_G(a) \subseteq R(G)$ be the set of neighbors

of a in G. By definition, if $b \in N_{G_\varphi}(a)$ then $\varphi(b) \in N_G(a)$. The converse is also true, except if $\varphi(a) \in N_G(a)$, or equivalently, $(a, \varphi(a)) \in E(G)$. Hence, $N_{G_\varphi}(a) = \{b : \varphi(b) \in N_G(a)\} \setminus \{a\}$, and therefore:

- If $(a, \varphi(a)) \notin E(G)$, the map φ induces a bijection between $N_{G_\varphi}(a)$ and $N_G(a)$. In particular, $|N_{G_\varphi}(a)| = |N_G(a)|$.
- If $(a, \varphi(a)) \in E(G)$, the map φ induces a bijection between $N_{G_\varphi}(a)$ and $N_G \setminus \{\varphi(a)\}$. In particular, $|N_{G_\varphi}(a)| = |N_G(a)| - 1$.

In $\mathbb{G}_q$, the bipartite incidence graph of the projective plane, a vertex $a \in L(\mathbb{G}_q)$ (that is, a point of the projective plane) corresponds to a 1-dimensional linear subspace of $\mathbb{F}_q^3$, while a vertex $\lambda \in R(\mathbb{G}_q)$ (that is, a line of the projective plane) corresponds to a 2-dimensional linear subspace of $\mathbb{F}_q^3$. Hence, for $a \in L(\mathbb{G}_q)$, we defined $\phi(a) \in R(\mathbb{G}_q)$ as the projective line corresponding to the 2-dimensional linear subspace orthogonal to a.

We denoted by $\mathbb{G}_{q|\phi}$ the reduction of $\mathbb{G}_q$ induced by ϕ. Note that $\mathbb{G}_{q|\phi}$ is a graph with q^2+q+1 vertices, and vertex degree equal to either q (vertices corresponding to self-orthogonal linear subspaces) or $q+1$ (other vertices). The diameter of $\mathbb{G}_{q|\phi}$ is equal to 2, and for any two non-adjacent vertices $a, b \in V(\mathbb{G}_{q|\phi})$, there is a unique path of length 2 connecting them.

Theorem (21 of [29]) Let k be such that $5k^2 - k - 10 \leqslant 2q$. Then $\mathbb{G}_{q|\phi}$ is k-vertex-minor universal.

It is interesting to see that we did not use the explicit definition of ϕ, but only the fact it is bijective and symmetric (therefore other families of graphs are also interesting in terms of vertex minor universality).

To the best of our knowledge, these are the first explicit constructions of k-vertex-minor universal graphs of order polynomial in k, significantly improving on the previous explicit construction of k-pairable states based on Reed-Muller codes from [22], with exponential overhead.

We also investigated the case where qubits are lost or of the presence of malicious parties. We prove a robustness property showing that any k' qubits can be discarded while preserving the $(k-k')$-vertex-minor universality of the remaining graph. We prove this result for pairability in [30] but can be easily extended for vertex-minor universality.

The explicit graph states we defined $|\mathbb{G}_q\rangle$ is also the "most quantum" known explicit state in terms of decomposability: it can produce a non-local correlation with multipartite width $\Omega(\sqrt{n})$ whereas the previous best known examples in [8] using Paley graphs had a logarithmic multipartiteness width.

Theorem 1 *The correlation obtained by* QSTRAT *on $MCG(\mathbb{G}_q)$ has multipartiteness width $\Omega(\sqrt{n})$*

Proof Sktech The key argument is the one used in the proof for the vertex minor universality. In the projective plane a point is incident to exactly $q+1$ lines and a line to $q+1$ points, so for any set K of k_1 points and k_2 lines one can take from outside this sets a disjoint set of points and lines each of them seeing exactly one element of K. Therefore taking one vertex as each C_i ensures the multipartiteness by $(q+1)$-odd domination. □

2.3 Quantum advantage in non-cooperative games with different types of quantum resources

An other interesting direction in understanding multipartite correlations is to consider the subfamily of correlations that are "locally meaningful" in the sense that they correspond to local behavior for which the interest of each player does not necessarily align but where each player is locally maximizing his interest.

In classical game theory, the most commonly studied setting is the one of non-cooperative games in which players have conflicting interests. The concept of *Nash equilibria* [90] is used to define stable solutions describing observable behavior in the situations modelised with these games. It has been extensively studied for its many applications, from economics [89] to the analysis of information warfare [66]. In these games, each player has an individual payoff function, rewarding them depending on their behaviour and that of the others. A Nash equilibrium is then a situation where no player has an incentive to deviate from their strategy and represent strategically stable behaviours [50]. One way to evaluate an equilibrium is to consider the mean (or total) payoff of the players, which is referred to as its *social welfare*.

The nonlocal games can be viewed as a subset of these games [27]. In such games, players sharing an entangled quantum state can achieve a higher winning probability than if they shared any classical random variable, showcasing the usefulness of quantum resources in decision making tasks, where they allow for better coordination without the need for a mediator, or for communication

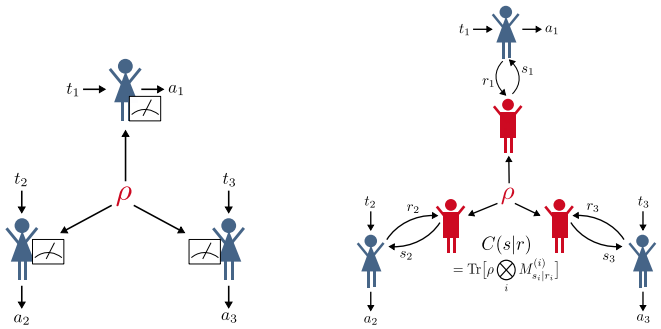

Figure 2.3: The two quantum scenarios we consider. (a) "Quantum advice": direct access to a shared quantum state. (b) "Quantum correlated advice": classical access to a quantum correlation $C(s|r)$ via several local mediators sharing an entangled quantum state ρ.

Shared quantum states can be seen as just one example of extra resource or *advice* that may be distributed amongst the players. Indeed, even in the classical study of such games, various works have looked at the capabilities afforded by providing correlated advice to the players, for instance in the form of shared random variables [10], or with the help of a trusted mediator, via belief-invariant (*i.e.*, non-signalling) advice [68, 82], or signaling advice [9].

The game's specification in this setting is completed by a payoff function (personal utility) u_i for each player, such that $u_i(a, t) \in \mathbb{R}$.

In particular, to build interesting non cooperative games from MCG, in [55], we considered

games where the payoff functions have the same form for all players and are defined from a set of "winning" input-output pairs $\mathcal{W} \subseteq A \times T$ as

$$u_i(a,t) = \begin{cases} 0 & \text{if } (a,t) \notin \mathcal{W}, \\ v_0 & \text{if } a_i = 0 \text{ and } (a,t) \in \mathcal{W}, \\ v_1 & \text{if } a_i = 1 \text{ and } (a,t) \in \mathcal{W}, \end{cases} \tag{2.1}$$

with $v_0, v_1 > 0$. Therefore, for a given question t, if two players output the same value they receive the same payoff. It is the ratio v_0/v_1 that may create conflicts of interest between the players: if the payoff is unbalanced, e.g., if $v_1 > v_0$, the players might have an interest in losing more often if it means answering 1 more often. The game thus becomes one of conflicting interests.

In a game, the strategy of a player influences their payoff but also that of other players. Naturally, each player seeks to maximise their own payoff. Some configurations of strategies are stable, meaning that no player can increase their payoff by unilaterally deviating from their strategy, and these configurations are called equilibria. Furthermore, when players are allowed to coordinate with some correlation or advice, they may reach different equilibria.

In [55] we answered a question of [9] showing that the quantum advantage is unbounded in terms of social welfare. Where social welfare is a measure of the quality of an equilibrium. More precisely we have shown using a form of parallel repetition on MCG that :

Theorem (3 of [55]) There exists games with bounded personal utilities on $\log(1/\epsilon)$ players were the classical social welfare is an epsilon fraction of the one achieved with a pseudotelepathic solution.

In [1], we continued further to investigate what quantum advantages can be obtained in multipartite non-cooperative games. We considered how different types of quantum resources can lead to new Nash equilibria and improve social welfare beyond the pseudotelepathy restriction.

Two different quantum settings have been considered: one in which players are given direct access to an entangled quantum state, and a second, which we introduced, in which they delegate their measurements and are only given classical advice obtained from quantum devices. For a given game G, these two settings give rise to different equilibria characterized by the sets of equilibrium correlations $Q(G)$ and $Q_{\text{corr}}(G)$, respectively. We have shown that $Q(G) \subseteq Q_{\text{corr}}(G)$, and by exploiting the self-testing property of some quantum correlations, that the inclusion is strict for some games G, thereby showing that delegating the quantum operations may give better equilibria. We made use of semidefinite programming (SDP) optimisation techniques to study how these quantum resources can improve social welfare, obtaining upper and lower bounds on the social welfare reachable in each setting. We investigated, for several games involving conflicting interests, how the social welfare depends on the bias of the game and improved upon a separation that was previously obtained using pseudotelepathic solutions using MCG.

We introduced in [1] a new type of quantum resource in the form of a *quantum correlated* advice, in which players have classical access to a quantum correlation via several local mediators who share parts of an entangled quantum state, as represented in Figure 2.3(b). This scenario arises rather naturally, as it is likely that in the near future access to quantum resources will be restricted to those with sufficient means, such as large corporations. Players may therefore

only have access to quantum states via local "quantum centres" (or mediators), which could share entangled states with other centres in a quantum network.

We have show in [1] that in conflicting-interest games, delegating quantum operations (which is easier to implement) can in fact be more powerful than the situation where players have full quantum access (as studied in [9]), as it leads to more and potentially better equilibria.

These results have a natural application in decision making situations where decisions have to be coordinated faster then the time needed for communication between the parties. They can also be relevant when the decisions have to be performed at a sufficiently high frequency relative to the speed of light, such that the players can be considered as spatially separated, something that is not uncommon in modern information processing tasks [35].

A new quantum resource by delegating quantum access

In scenarios with correlated advice, the players have access to some shared correlation $C \in \mathcal{C}$, with $\mathcal{C}$ characterizing their type. The literature has primarily considered shared randomness, belief-invariant (non-signalling), or signalling correlations, and while shared randomness is a local resource, belief-invariant and signalling correlations generally require a centralised and trusted mediator to be implemented. Here instead, we considered the intermediate set of quantum correlations $\mathcal{C}_Q$, which players can access via several local mediators; see Figure 2.3(b). Given access to such a correlation, the local strategies of the players define a *solution* that induces a probability distribution $P(a|t)$.

This new resource of *quantum correlated advice* that we introduced in the context of game theory, can be thought of as "classical" access to a quantum resource, and we compare it to the standard quantum advice, where the players directly share a quantum state upon which they make their own measurements [9]; see Figure 2.3(a). There, a quantum solution $(\mathcal{M}, \rho)$ is given by an n-partite quantum state ρ distributed among the players and two POVMs $\{M^{(i)}_{a_i|t_i}\}_{a_i}$ for each player. A quantum solution then induces a probability distribution $P(a|t)$ via the Born rule $P(a|t) = Tr((\bigotimes_i M^{(i)}_{a_i|t_i})\rho)$. While the two types of quantum resources seem at first sight equivalent, as they give rise to the same type of distribution on $P(a|t)$, we showed that they actually differ in non-cooperative games, where the notion of equilibrium matters.

Two notions of equilibria

In non-cooperative games, a solution is a Nash equilibrium if no player can improve their mean payoff by unilaterally deviating from their strategy. In scenarios with correlated advice, this property of a solution can be verified by checking a few inequalities on the induced correlation P – and we will speak thereof, with a slight abuse of language, of correlations P that are Nash equilibria. In particular, for quantum correlated advice the equilibria can be nicely characterized by noticing that an induced correlation P is in $\mathcal{C}_Q$ if and only if it is induced by a solution with players accessing a shared correlation $C \in \mathcal{C}_Q$. This allows us to characterize the equilibria accessible with quantum correlated advice with the set $\mathcal{Q}_{\text{corr}}(G) = \{P \in \mathcal{C}_Q \text{ such that } P \text{ is a Nash equilibrium for } G\}$.

In the other scenario, when the players directly access a shared quantum state, the equilibria conditions differ. Indeed, we say that a solution $(\rho, \mathcal{M})$ is a *quantum equilibrium*, if no player i can improve their payoff by choosing, for some type t_i, an alternative POVM $N^{(i)}_{t_i} = \{N^{(i)}_{a_i|t_i}\}_{a_i}$.

Whether a solution is an equilibrium or not can be checked using semi-definite programming. As in the former setting, we characterize the set of quantum equilibria by their induced correlations: $Q(G) = \{P \in \mathcal{C}_Q : \text{ there exists a quantum equilibrium } (\rho, \mathcal{M}) \text{ for } G \text{ that induces } P\}$.

The two sets of induced correlations thus defined, $Q_{\text{corr}}(G)$ and $Q(G)$, are both subsets of $\mathcal{C}_Q$, and by comparing them, we can compare the equilibria that are accessible with the two different types of quantum resources.

Results

In [1], during the Ph.D. of Pierre Pocreau, with Alastair Abbott, we have first shown that for any game G, the equilibria that can be reached when players share quantum advice (Fig. 2.3(a)), can also be accessed with quantum correlated advice (Fig. 2.3(b)).

Theorem (1 of [1]) For any game G, $Q(G) \subseteq Q_{\text{corr}}(G)$.
This inclusion follows by noticing that the condition for a solution with quantum advice $(\rho, \mathcal{M})$ to be a quantum equilibrium, encompasses the Nash equilibrium condition on its induced correlation P, so that P will be in $Q_{\text{corr}}(G)$. This result seems at first surprising, as restricting the power of the players does not limit their capability to reach an equilibrium. But another way of framing this is that, because the players are restricted to classical access to quantum states, they have less way of getting out of equilibrium, so the equilibria are more stable.

Then we have shown that this inclusion is in fact strict for some games G, meaning that delegating the quantum operations allows the players to reach more equilibria.

Theorem 2 ([1]) There exists a game G for which $Q(G) \subsetneq Q_{\text{corr}}(G)$.

Showing a strict inclusion was more difficult, and we built on recent results in the theory self-testing [109] to obtain this separation, in what is a novel application of such techniques. In particular, we studied a tripartite game G and a specific quantum solution parameterised by an angle θ, $(\rho_\theta, \mathcal{M}_\theta)$, that we call the tilted solution as it is based on a titled stabilizer construction of the GHZ state. This solution has the interesting property of inducing a correlation $P_\theta \in Q_{\text{corr}}(G)$ – *i.e.*, which defines a correlated quantum equilibrium – while *not* being a standard quantum equilibrium. To show that any alternative quantum solution $(\tilde{\rho}, \tilde{\mathcal{M}})$ inducing P_θ cannot be a quantum equilibrium either, we needed to map the action of any POVM on $\tilde{\rho}$ to one acting on ρ_θ. To that aim, we proved a slightly more general self-testing statement on P_θ and $(\rho_\theta, \mathcal{M}_\theta)$, showing the self-testing on a tomographically complete set of projectors. The proof is then obtained by tailoring a Bell inequality, inspired by the self-testing of a partially entangled GHZ state in [11]. This allows us to show that $P_\theta \in Q_{\text{corr}}(G)$ while $P_\theta \notin Q(G)$, proving that quantum correlated advice is strictly more powerful than quantum advice.

We then considered the best equilibria in terms of social welfare, and whether they differ under the two types of quantum resources. Because the sets $Q_{\text{corr}}(G)$ and $Q(G)$ are difficult to characterize directly, we instead relied on the NPA hierarchy [91] and an iterative "see-saw" optimisation method to compute both upper and lower bounds on the maximal social welfare for the two sets. Our numerical results for two families of three- and five-player games are summarised in Fig. 2.4. We found that the two types of quantum resource can provide better social welfare than pseudotelepathic solutions [55], despite these latter solutions winning all the time. We thus improved upon the known advantages of quantum resources in this game.

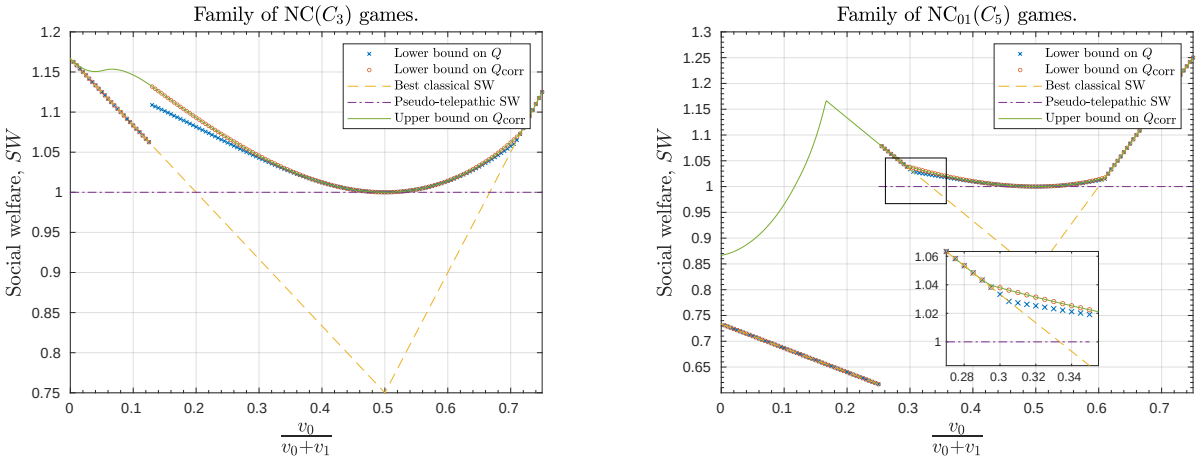

Figure 2.4: Numerical bounds on the social welfare of families of three and five players games, showing improvements over classical and pseudotelepathic quantum solutions.

Furthermore, when the game is not too biased, the bounds on $Q_{\text{corr}}(G)$ are tight and strictly higher than the best lower bounds we found for $Q(G)$, supporting the idea that not only are more equilibria reached in $Q_{\text{corr}}(G)$, but also better ones in term of social welfare.

Our numerical results also showed that these multipartite games exhibit several interesting phenomena, including families of solutions that are equilibria for the different types of quantum resource for differing ranges of bias in the game. Understanding the best equilibrium solutions remains an interesting and complex challenge.

More broadly, our results open interesting questions on the use of quantum resources in game theory and provide a new angle toward understanding the limits and advantages of delegated quantum measurements.

2.4 Conclusion

We see that graph states offer a very interesting and rich perspective to investigate quantum correlations and to understand the notion of multipartiteness. Even though these structures has been studied for a long time, they can still surprise us with new unexpected notions which could lead to potential application of quantum information theory.

Chapter 3

Graph states for computation

3.1 Determinism in Measurement Based Computation

Measurement-Based Quantum Computing (MBQC), also called one-way model, has been introduced by Briegel and Raussendorf in [23,56,99,101]. The key idea is to perform single-qubit measurements over a large resource (entangled) state. Its topological version that have shown very promising results for fault tolerant quantum computing using a 3D cluster state [103,113]. It is used in photonic quantum computing proposals [15] via a variant called FBQC. Another application of MBQC is to decrease the quantum depth: for instance the Quantum Fourier Transform can be approximated in constant quantum depth using MBQC [25] and thus provides a logarithmic speed-up compared to quantum circuits.

A fundamental property of MBQC is its probabilistic behavior: every measurement leads to two possible outcomes. In this context, performing an overall "deterministic" computation – e.g. for implementing a unitary evolution – requires a correction strategy, an adaptive computation which depends on the classical outcomes of the measured qubits, so that the output of the overall computation does not depend on the intermediate measurement outcomes. Some standard additional technical requirements, for instance that the computation remains deterministic under small variations of the measurement basis, or that partial computations are also deterministic, lead to the notion of robust determinism.

Robust determinism is in particular well-suited for variational quantum computing. Several recent works [48,106] points out the necessity of determinism in Measurement-based Variational Quantum Eigensolver. Measurement-based Variational Quantum Eigensolver is particularly promising in terms of physical implementation. Robust determinism guarantees the so-called *deterministic Ansätze*, indeed determinism is preserved when angles, *i.e.* the parameters, vary.

The existence of a correction strategy essentially depends on two parameters: the initial resource state and the performed measurements.

In MBQC, every measurement can be performed in three possible planes of the Bloch sphere (the so-called XY, YZ, and XZ-planes). The resource state and the measurements can be abstracted away into an **open graph**, i.e., a graph that describes the resource state together with a labelling of the vertices with the corresponding measurement plane (e.g. XZ).

3.2 Generalized Flow

In [26], we have shown that a robust deterministic computation is possible if and only if the corresponding open graph has a GFlow. Hence GFlow, an easy to compute graphical property, characterizes robust determinism in MBQC.

The correction strategy in MBQC fundamentally relies on some fixed-point properties of graph states: for any subset D of (non input) qubits, the Pauli operator $X_D Z_{\mathrm{Odd}D}$ is called a stabilizer, because it leaves the resource state invariant[1]. The local operation, on every qubit $v \in V$, of this stabilizer is called the *action of D on v*, denoted Act_v^D and thus defined as:

$$Act_v^D = \begin{cases} X \text{ if } v \in D \setminus \mathrm{Odd}D \\ Z \text{ if } v \in \mathrm{Odd}D \setminus D \\ Y \text{ if } v \in D \cap \mathrm{Odd}D \\ I \text{ Otherwise.} \end{cases}$$

The action on a vertex can be used to actually correct a measurement: when the action of D on a vertex u anti-commute with each element of λ_u according to which u is measured, the action of D turns one measurement projector into the other, performing the desired correction. Hence, we denote

$$\mathrm{cor}(D) = \{u, \forall P \in \lambda_u, [Act_u^D, P] \neq 0\}$$

GFlow is based on this idea and consists in finding for every measured qubit u a set D of correctors such that (i) $u \in \mathrm{cor}(D)$ and (ii) D acts trivially on all qubits measured before u to avoid uncontrolled side effects.

Proposition (4 of [88]) (Theorem of [26]) An MBQC is robustly deterministic if and only if its open graph has a GFlow.

The main idea is that using stabilizer properties one can use a set of non measured qubits which Odd neighborhood is the measured vertex to change the branch where the outcome of the measurement is 1 to the branch where it is 0. This somehow simulates the 'creation' of a Z operator correcting any measurement in the XY plane.

3.3 Pauli Flow and Shadow Pauli flow

Pauli measurements are ubiquitous in MBQC, for instance in the context of error correcting codes, or for implementing Clifford transformations. Some graphical transformations can be performed using Pauli measurements so that they can be used to locally transform a resource state into another one satisfying for instance some architecture constraints. More generally, it is reasonable to assume that a significant portion of the measurements of a practical MBQC are Pauli measurements. We have shown that this is for instance the case when using as a resource a constraint initial state like a cluster state or a triangular grid [87]. In terms of determinism, Pauli measurements satisfy some particular properties that are not captured by GFlow. For instance, an MBQC involving an X measurement can be deterministic, even though the corresponding open graph has no GFlow, regardless of whether the X measurement

[1] Up to a -1 global sign as discussed in previous chapter

is considered an XY or XZ measurement. Hence we have proposed a generalization of GFlow, called Pauli Flow in the original paper introducing GFlow [26]. Pauli Flow has been proved to be a sufficient condition for robust determinism, it is also a necessary condition for determinism when all measurements are real[2], but is not necessary in general [96].

The extension from GFlow to Pauli Flow is based on the following additional property: a correction can act on an already measured qubit as long as this qubit has been measured in the appropriate Pauli basis, in this case the qubit is not impacted by the action of a corrector. Hence, we say that the action of D *impacts* a vertex v if the action of D on v anticommutes with one Pauli element of λ_v and denote

$$\mathrm{imp}(D) = \{v, \exists P \in \lambda_v, [Act_v^D, P] \neq 0\}$$

An **open graph** (G, I, O, λ) is a graph G with two subset of vertices I and O corresponding to the inputs and outputs and measurement planes $\lambda_v \subsetneq \{X, Y, Z\}$ for $v \in O^c = V \setminus O$.

Pauli flow Given $p : O^c \to 2^{I^c}$ and $\prec$ a strict partial order over O^c,
$(p, \prec)$ is a Pauli Flow of (G, I, O, λ) iff

$$\forall u \in O^c,\ u \in \mathrm{cor}(p(u)) \text{ and } \mathrm{ana}_{p,\prec}(u) = \emptyset$$

where $\mathrm{ana}_{p,\prec}(u) := \{v \in O^c, \text{ s.t. } u \neq v,\ \neg(v \prec u) \text{ and } u \in \mathrm{imp}(p(v))\}$ is the set of vertices corrected after u which correction has an "anachronistic" impact on u.

We finally introduced in [88] an extension of the Pauli Flow called *Shadow Pauli Flow* that have proven to be a necessary and sufficient condition for robust determinism:

Shadow Pauli flow An open graph (G, I, O, λ) has a Shadow Pauli Flow $(p, \prec)$, where $p : O^c \to 2^{I^c}$ and $\prec$ partial order, if $\forall v \in O^c$,

- v is corrected by $p(v)$, i.e. $v \in \mathrm{cor}(p(v))$ and
- if v is anachronistically impacted ($\mathrm{ana}_{p,\prec}(v) \neq \emptyset$), then v is not a Pauli measurement ($|\lambda_v| = 2$), and it has a set of "shadow correctors" $D_v \subseteq I^c$ such that:

  $v \in \mathrm{cor}(D_v)$ and

  $\forall u \in \mathrm{ana}_{p,\prec}(v),\ \forall w \in (D_v \cup \mathrm{Odd}D_v) \setminus \{v\},\ w \notin \mathrm{imp}(D_v)$ and $w \preccurlyeq u$.

Theorem (1 of [88]) An MBQC is robustly deterministic if and only if it is consistent with a Shadow Pauli Flow on its open graph.

To prove this theorem, we first showed that when all Pauli measurements are performed at the beginning of the computation, the Pauli Flow is actually necessary and sufficient for robust determinism. The rest of the proof is obtained by showing how Pauli measurements can be moved forwards or backwards in an MBQC, and how such moves preserve robust determinism and/or Shadow Pauli Flow existence.

Notice that it implies that Pauli Flow actually also characterizes robust determinism but in a weaker way:

[2] i.e. measurements described by real observables: X, Z and any measurement in the XZ-plane.

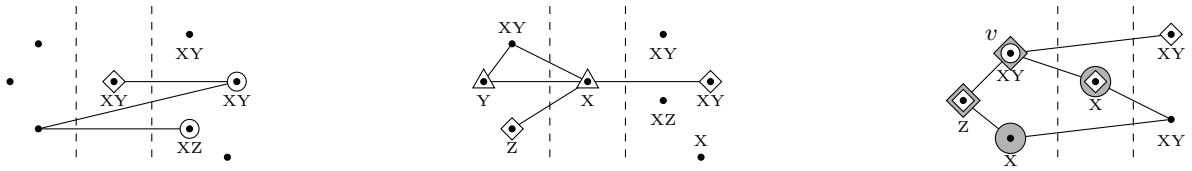

Figure 3.1: We illustrate the 3 kinds of flow : GFlow on the left, Pauli flow in the middle, and Shadow Pauli flow on the right. In each case, the correction required by the measurement of the central vertex involves the vertices with different Paulis represented with white shapes: triangle = $D \cap \mathrm{Odd}D$, diamond = $\mathrm{Odd}D \setminus D$ and circle= $D \setminus \mathrm{Odd}D$. A dependency on the past (vertex v) is allowed in the Shadow Pauli flow case when it is compensated by a D_v in the past represented by grey shapes.

Theorem (3 of [88]) A resource state, described as an open graph, can be used to perform a robustly deterministic MBQC if and only if it has a Pauli Flow.

The first theorem is stronger as, in particular, it relates the order in which the measurements are performed – and hence the depth of the MBQC – with the order of the corresponding flow.

It is common to discard the Pauli measurements in an analysis of MBQC considering that they can be moved first [99]. We strengthen this observation showing that moving the Pauli measurements first can be done in a way that preserves robust determinism. Furthermore, the robustness property applies for the original pattern of measurements which can be relevant in practice as it may be impossible to move some Pauli measurements in some implementations as one can reuse some qubits or have restrictions on the position of the qubits measured at some time step.

We showed that given a partial order on measured qubits and an open graph, a Shadow Pauli flow can be computed in polynomial time.

3.4 Conclusion

In conclusion we have investigated how an initial simple entanglement structure described by a graph, allows to push the information that could be inserted in some sites (input qubits) to others (output qubits) while preserving the determinism (applying a global isometry). First, when the only measurement constraints are being a plane of Pauli measurements with the notion of GFlow, which had many implications, for instance in ZX calculus [42] and for circuit optimisation [12, 41]. We refined the notion to consider cases where some vertices are Pauli Measured, this was consistent with the applications for efficient circuit optimisations [107] and rewrite rules for MBQC patterns preserving Pauli flow has been derived in [83]. We finally defined the Shadow Flow which allows to capture robust determinism as a necessary and sufficient condition giving a better understanding of the conditions for a deterministic pattern (which computes a unitary) to respect a temporality in the order in which the measurements have to be done.

Chapter 4

Graph tools for quantum codes

4.1 Message passing decoding on the toric code

In [34], we considered the Message Passing (MP) decoding of the Kitaev toric code [73], the planar version of which is currently the dominant error-correction solution to achieve fault-tolerance in large-scale quantum computers, especially for connectivity constrained technologies [52]. Among the large class of quantum Low Density Parity Check (LDPC) codes, the toric code is also known to be the less responsive to MP, due to the presence of weight-2 degenerate errors undecodable by vanilla MP decoders, such as belief-propagation (BP)[1] or min-sum (MS). Consequently, the logical error rate of these vanilla decoders scales as p^2, where p is the physical error rate, well behind the $p^{\lceil \frac{d}{2} \rceil}$ scaling of a minimum distance decoding (*i.e.*, correcting any error of weight $\leq \lfloor \frac{d-1}{2} \rfloor$), where d is the minimum distance of the code. A few approaches proposed in the literature, such as BP with memory [75], generalized BP [93], or neural-BP [79, 114], succeeded to improve the logical error rate performance for small distance toric codes ($d \leq 9$), but they all failed to scale to larger distance codes. Precisely, for $d \leq 9$, the above approaches may yield a logical error rate that scales as $p^{\lceil \frac{d}{2} \rceil}$, but this scaling no longer improves with increasing minimum distance, indicating the presence of undecodable errors of weight 5. In this work, we tried to understand if such difficulties come from an intrinsic limitation of the toric code itself, hindering further improvement of MP-based decoding for

[1] We use BP for the MP decoding using Bayesian rules to update the exchanged messages (also known as sum-product). It performs the exact Bayesian inference on trees, but may be used on more general graphical models. Note that BP is sometimes used (included in some of the papers cited here) with the generic meaning of MP.

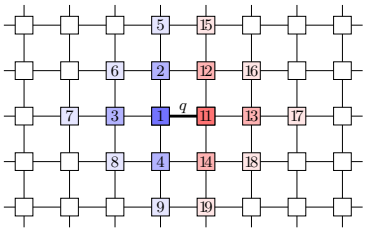

Figure 4.1: A qubit in the toric code

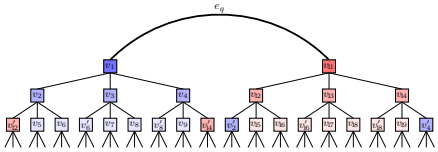

Figure 4.2: Decoding tree

$d > 9$.

We considered binary MP decoding, corresponding to separate decoding of X and Z-type errors. The input of the decoder consists of the error syndrome and the apriori *soft value* of each qubit (*e.g.*, error probabilities or log-likelihood ratio values). Decoding is carried out through an iterative exchange of extrinsic messages between qubits and checks they participate in, which is conveniently described via the Tanner graph representation of the code. In this representation, messages are exchanged between neighboring qubit and checks of the Tanner graph, and the iterative nature of the decoding process is aimed at spreading the information globally. At each decoding iteration, an aposteriori *soft value* is computed for each qubit, based on the collected messages, gradually improving the estimation of the error. For details on MP decoders, [116] provides a good introduction.

Our goal is to understand how the information is spreading on the toric code, and what is the maximum length it can travel. To provide a formal statement, we first introduce the notion of local blindness of an MP decoder. Informally, given an error syndrome $\mathbf{s}$ and an unsatisfied check c, *i.e.*, such that $\mathbf{s}(c) = 1$, we consider a fake syndrome $\mathbf{s}^c$, having c as the only unsatisfied check (note that $\mathbf{s}^c$ is not a valid error syndrome, since no error can generate it). We say that the MP decoding of $\mathbf{s}$ is *locally blind* in the neighborhood of c, if running the MP decoding on the error syndrome $\mathbf{s}$, or on the fake syndrome $\mathbf{s}^c$, yields the same aposteriori soft value for any qubit q neighboring c, and for any number of decoding iterations. Put differently, at no iteration are the qubits neighboring c aware that it is not the only unsatisfied check of the syndrome: the MP decoder fails to convey the information from the other unsatisfied checks. Intuitively, this may happen when c is too far away from the other unsatisfied checks of the syndrome.

4.2 Limitations of the Min-Sum decoding on the toric code

In [34] we focused on the MS decoding, with the conventional flooded scheduling which means that at each steps all the beliefs are updated synchronously. The reason is twofold. First, MS is an MP decoding algorithm that is aimed at solving the maximum likelihood (ML) decoding problem in a *localized* manner. It actually succeeds in doing so for codes defined by acyclic graphs. However, quantum LDPC codes (as well as good classical LDPC codes) are defined by graphs with cycles, preventing local information from being spread effectively, and causing a degradation of the error correction performance with respect to ML decoding. Second, MS presents a number of practical advantages, *e.g.*, low computational complexity (only requires additions and comparisons) and robustness to low precision arithmetic (*e.g.*, below 6-bit messages), being the *de facto* solution used in practical applications and hardware implementations [18]. Moreover, assuming a Pauli channel model for physical qubit errors, with X and Z errors decoded independently, MS does not need an apriori knowledge of the channel X, Y, Z error probabilities [39].

Our first result states that the **local** information exchange of the MS is not spreading **globally**:

Theorem (1 of [39]) MS Local Blindness Consider an error syndrome $\mathbf{s}$ on a toric code, such that all the unsatisfied checks are at distance at least 5 from each other. Then, under

the i.i.d. noise assumption, the MS decoding of $\mathbf{s}$ is locally blind in the neighborhood of any unsatisfied check.

In particular, it follows that such a syndrome is undecodable by MS. Further, we are interested in determining the smallest weight of an undecodable non-degenerate error. We say that an error $\mathbf{e}$ is **non-degenerate** if it generates a syndrome that cannot be generated by any other error $\mathbf{e}' \neq e$, such that $|e'| \leq |e|$. For instance, 1-dimensional errors $\mathbf{e}$ of weight $|e| \leq \left\lfloor \frac{d-1}{2} \right\rfloor$ and generating a syndrome of weight 2 are non-degenerate. But some 2-dimensional errors may also be non-degenerate.

We refined the classical notion of decoding radius (*i.e.*, the largest integer ω, such that any error of weight $\leq \omega$ is decoded correctly), by introducing the **non-degenerate decoding radius**, which only takes into account non-degenerate errors.

Theorem (2 of [39]) MS Non-Degenerate Decoding Radius For any toric code of distance ≥ 9, the non-degenerate decoding radius of the MS is 3.

The main tool used in the proof is the analysis of the tree describing the decision at each step by exhibiting a family of patterns allowing to have a formal proof of the decision for the message passing algorithm.

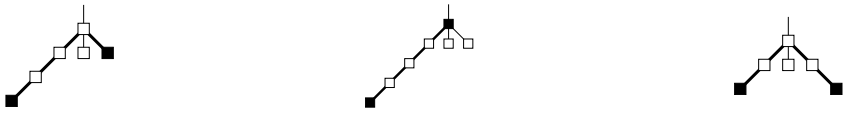

Figure 4.3: Patterns allowing to describe a family of configurations of minimal weight in the decoding tree

Although the toric code is know to be the hypergraph product code of two classical repetition codes [112], on which the MS decoding radius is equal to $\left\lfloor \frac{d-1}{2} \right\rfloor$, the decoding radius of the MS on the toric code is only equal to 1, and the essence of Theorem 2 is that even the **non-degenerate** decoding radius is no greater than 3.

4.3 Stabilizer blowup

Finally, we proposed a new pre-processing that runs in linear time and allows correcting all (degenerate) errors of weight up to 3 thus improving the decoding radius of the MS to 3. We refer to this pre-processing step as stabilizer-blowup (SB), and it amounts to applying a change of variable that locally removes the degeneracy to allow the decoder to converge. It uses a graph modification illustrated in Figure 4.4.

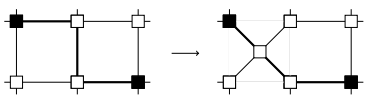

Figure 4.4: A stabilizer blowup for a degenerate error of weight 3

We proved that:

Theorem (3 of [39]) Stabilizer Blowup Pre-Processing SB+MS is able to correct all errors of weight up to 3 on a toric code of distance ≥ 7.

It follows that the SB+MS yields a quadratic improvement in the logical error rate performance, as compared to MS only. In particular, it can be applied to quadratically reduce the number of calls to a possible post-processing step, which remains a mustfor the MS-based decoding of toric codes of minimum distance $d \geq 9$.

4.4 Conclusion

Therefore, we see that a fine-grained analysis using graphs allows to prove the intrinsic limitations of the message passing decoding on the toric code and that a graph transformation allows to push this decoding to its limit. Note that even though the results are formulated for the toric code the notions introduced have been done so that it could be adapted for other codes.

Chapter 5

A broader overview of research activities and supervisions

During my Ph.D. I studied how quantum information helps solving some classical graph problems [44], providing almost tight upper and lower bounds. I was also already interested in understanding the combinatorial structures behind quantum entanglement and through the characterization of the positions of the zero amplitudes in pure tensor products [67].

The main center of interest for my research afterwards revolved around graph states and stabilizers. With collaborators and students, we considered the resources required to build graph states [61] describing how to prepare them with measurement only, and relations between the graph structure and the complexity of preparing these states. We also considered how to use them for computation using only one qubit measurements [86], and described which graph properties make the associated graph states powerful resources for quantum computation [85]. We defined a flow like property that is polynomially computable to find patterns composed of graph preparation measurement and simple one qubit correction allowing to compute with graph states improving on the literature. We also have shown for example how to use a triangular grid family of graphs to compute using only one plane for measurements [87]. More recently we gave necessary and sufficient conditions for the possibility of robust Measurement Base Quantum computation with a graph state when some qubits are measured with Pauli measurements [88] (as described in Chapter 3).

We also studied how we can use graph states in protocols, first to share classical and quantum secrets [63], and then more generally by trying to understand multipartite correlations and decomposing systems into subsystems in graph states as discussed in Chapter 2.

This contextual perspective led me to try to investigate the structure of quantum computing further. For instance one first work about extending the framework to allow the description of a more general way to apply quantum transformations was through investigating coherent control with polarized beam splitters during the Ph.D. of Julian Wechs. The first analysis, published in [3], was expanded in [19], were we used diagrams to represent Polarized beam splitters and investigated how much information can be hidden in the description of a quantum channel. We finally formalized properly for the query model a way to compare this more general way to process quantum information in [2] (during the Ph.D. of Pierre Pocreau). We have shown that the more natural extensions (those closer to physically possible implementations) do not help

for these problems but that when fixing the number of queries we can have a better probability of success for computing a boolean function in the more general model of general processes. Somehow we can see that relaxing the constraint of respecting a deterministic causal order in the process of computation can give a strict constant separation in the query model but that we don't know if it can be amplified by composition to have a proper complexity separation.

One of the most common use of stabilizers in quantum information theory is through error correction codes. I started investigating the field with Valentin Savin through the Ph.D. research of Ashutosh Goswami, and we proved that a classical phenomena that is very useful in classical codes occurs at the quantum level. The polarization is the fact that some generic encoding allows to encode the information using ancillas in such a way that some channels become perfect and some other becomes useless so that by iterating the construction one can reach the capacity of any channel with a generic construction. We proved that this phenomenon still holds in a quantum setting in [43], we further considered extension to qudits [53] and applications for fault tolerant computing [54] where we used techniques from measurement-based quantum computing to deal with the errors during the preparation of our states.

We also considered the decoding problem, proposing techniques for proving intrinsic limitations for one of the most efficient classical family of fast decoding technique [39] called message-passing decoders for the surface code which is the most commonly used quantum codes and have a grid as underlying graph as described in Chapter 4. We also proposed techniques for the color codes (based on the hexagonal grid) called trimming decoding [77].

Furthermore, we proposed very efficient preprocessing and post processing techniques compared to the state of the art by using stabilizers inactivation [33] (looking at smaller codes and solving a small system), layered decoding [37] to be compatible with hardware requirement we extended the partition of the decoding matrix to more general k coverings and used permutations to have efficient decoding by Message Passing without post-processing [38].

Recently and in view of the many mistakes appearing in quantum published results reused later [16], we tried to consider formal proofs for quantum information theory. Using a proof assistant, we introduced the proper notions to the formal proof archive to allow to write formally some quantum proofs with the idea of going towards that not only correlation can certify non classicality allowing to see that one does not need to rely on the person that made the device to certify the state of the system and the correlations but also that the proof of device independence can be formally established. With Mnacho Echenim [47], we proved Bell inequalities and the Tsirelson bound. We also considered superposition calculus with graphs in [45] using graph-based reasoning instead of term-based reasoning [46].

I also had some classical contributions about games based on graph decomposition and their complexity [40], graph properties related to quantum states [64], quantum inspired classical games [36] or about finding long paths with distinct colors in edge-colored graphs [58].

Most of the results were obtained with students in Master, pre-Master's internship or co-supervised Ph.D. The co-supervisions were with Simon Perdrix and Pablo Arrighi (for Jerome Javelle), with Cyril Branciard (for Julian Wechs), with Valentin Savin (for Ashutosh Goswami, Julien Du Crest and Maxime Cautres), and with Alastair Abbott (for Pierre Pocreau).

Chapter 6

Perspectives

The results presented here are just a small part of the different situations where results using discrete structures allow to exhibit and understand better complex phenomena. For instance, among the follow-ups that increases this motivation is the recent result in [32] which captures exactly the equivalence by general local unitary operators of graph states with a sequence of possibly infinite graph transformations that refines the standard local complementation allowing to consider multiple copies of the vertices. The importance of graphs can even be pushed further. For instance in a very recent Ph.D. thesis of Khesin [71] that just appeared on arxiv and that was directed by Peter Shor has as title *Quantum computation from graphs*.

The natural follow up of the results presented here is to use the cohomological framework used in [100], as it links contextuality with MBQC and error correction. This is even truer considering the huge impact of topology for recent development of codes like quantum Tanner codes [78] which, in some versions, have qubits on the faces, and lifts preserving the squares.

The fine grained interpretation that we have, taking into account the structure of the graphs might be a useful resource to insert back in building codes or MBQC resources or fault tolerance. This can be a possible use of the explicit families of graph states defined in Chapter 2.

It might be interesting to investigate the link with MBQC and Floquet codes [59], which have been recently widely discussed and for which the stabilizers change periodically in time.

The self-tested tilted solution used to prove the separation between the classes of equilibrium encourages further investigation of delegated MBQC which already allowed to provide interesting insights for blind quantum computing [70].

The multipartite structures defined in Chapter 2 may be interesting to consider in settings of distributed computing like the ones studied in [76] where quantumness offers an advantage.

An interesting direction is also the links with causality. Indeed when considering general processes there is a strong link between the non-signaling correlations and the conditions defining valid processes that prevents the future from signaling to the past. Furthermore, links between causality and contextuality have begun to be established with tools from algebraic geometry and topology [51].

A further-reaching perspective is to try to have a discrete combinatorial representation of quantum information that is not even relying on category theory. Can we capture logical properties of quantum information, such as reversibility and the fundamental distinction between what one can perceive and the concept used to describe it to build a sequence of discrete structures recovering the main properties of quantum information theory?

It might be less unlikely than it first seems, as for example in the theoretical model introduced in [110], one can see that describing combinatorial substructures of lattices without top element (that they call an "inaccessible statements") and relaxing probabilities to quasi probabilities one can recover qubits as the simplest model.

The motivation is not just foundational or at the level of finding an interpretation of quantum information theory. One relatively recent and important result in quantum information theory is the observation that the set of quantum correlations are not closed [108]: correlations obtained by taking the limit in increasing the dimension of complex Hilbert spaces (as traditionally considered in quantum information) are open, whereas the algebraic ones (where locality is defined by commutation) are closed. One question is whether this can help to define a complexity class between the problems that are polynomial in time corresponding to the complexity class P and the ones that require a polynomial space corresponding to the complexity class PSPACE.

I think that a possible program aiming at that direction could be through a proper discrete formalism that is more combinatorial than algebraic to describe an interesting formalizable language.

One hint on that this approach is plausible is the recent result of Kitaev et.al. [72] which shows that one can define a proper algebra of observables from an approximate C^*-algebra. Somehow, starting from a set of operators in a C^*-algebra allows to define "states" in a canonical way. So, as usual in mathematics, we start from regularity (algebra) to describe (a model of) reality. We can view the recent result as a hint that canonicity can be obtained even without structure by starting just from an ϵ (a distance from regularity). This could perhaps be used as a support for a transition to a discrete formalism.

Such a foundational program could provide a fresh perspective on well-studied concepts. For instance, we could define complexity depending not only on the size of the input but also on the time required to produce it, revisit the notion of online algorithms with adaptive constraints or consider a strong form of transcendence that arises from distinguishing numbers using a recursive construction of computation using positive integers.

At a time when humanism is losing its meaning, I think that it is important to try to understand *exprimable* things in the most general framework, learning from what we know and trying to infer to make expressible things as accessible as we can. I would therefore like to conclude with the main fundamental principles that in my sense capture the essence of quantum information theory and that I would like to keep in a long term attempt to formulate a more general framework for languages and processes.

- "We don't need to forget to understand". In quantum information theory every process is reversible when considered in the right space. Therefore it could be possible to have a language that "accompanies any abstraction with a correction" so that information is preserved.

- "Decomposition may require repeatability." If composing is simple, decomposing is not always just partitioning. Given a structure defining its components with some precision may require considering coarse graining of multiple copies of "instances" of it.

- "Concepts and percepts do not need to live in the same worlds". One cannot always identify the model that describes what we can see (exprimable percept) with the model

describing what can be or what we can act on (expressible concept). We just need a model where one can naturally transform the actions on operations into the actions on observations. Probabilities are born by the reduction from what can be imagined to what can be observed.

- "One can give a meaning to the difference of meanings". Either by purifying in larger spaces or by defining the measurement we can explain the probabilities observed and the different outcomes.

Bibliography

[1] Alastair A Abbott, Mehdi Mhalla, and Pierre Pocreau. Improving social welfare in non-cooperative games with different types of quantum resources. *Quantum*, 8:1376, 2024. arXiv:2211.01687, doi:10.22331/q-2024-06-17-1376.

[2] Alastair A Abbott, Mehdi Mhalla, and Pierre Pocreau. Quantum query complexity of boolean functions under indefinite causal order. *Physical Review Research*, 6(3):L032020, 2024. arXiv:2307.10285.

[3] Alastair A. Abbott, Julian Wechs, Dominic Horsman, Mehdi Mhalla, and Cyril Branciard. Communication through coherent control of quantum channels. *Quantum*, 4:333, 2020. arXiv:1810.09826, doi:10.22331/Q-2020-09-24-333.

[4] Samson Abramsky and Adam Brandenburger. The sheaf-theoretic structure of non-locality and contextuality. *New Journal of Physics*, 13(11):113036, 2011. arXiv:1102.0264.

[5] Samson Abramsky, Shane Mansfield, and Rui Soares Barbosa. The cohomology of non-locality and contextuality. In *Proceedings of the 8th International Workshop on Quantum Physics and Logic (QPL)*, pages 1–15, 2011. URL: https://arxiv.org/abs/1111.3620.

[6] Antonio Acín, Tobias Fritz, Anthony Leverrier, and Ana Belén Sainz. A combinatorial approach to nonlocality and contextuality. *Communications in Mathematical Physics*, 334(2):533–628, 2015. doi:10.1007/s00220-014-2260-1.

[7] Anurag Anshu, Peter Høyer, Mehdi Mhalla, and Simon Perdrix. Contextuality in multipartite pseudo-telepathy graph games. *Journal of Computer and System Sciences*, 107:156–165, 2020. arXiv:1609.09689, doi:10.1016/j.jcss.2019.06.005.

[8] Anurag Anshu and Mehdi Mhalla. Pseudotelepathy games and genuine NS k-way non-locality using graph states. *Quantum Information and Computation*, 13(9-10):833–845, 2013. arXiv:1207.2276.

[9] Vincenzo Auletta, Diodato Ferraioli, Ashutosh Rai, Giannicola Scarpa, and Andreas Winter. Belief-invariant and quantum equilibria in games of incomplete information. *Theoretical Computer Science*, 895:151–177, 2021. doi:10.1016/j.tcs.2021.09.041.

[10] Robert J. Aumann. Subjectivity and correlation in randomized strategies. *Journal of Mathematical Economics*, 1:67–96, 1974. URL: https://www.sciencedirect.com/science/article/pii/0304406874900378, doi:10.1016/0304-4068(74)90037-8.

[11] Flavio Baccari, Remigiusz Augusiak, Ivan Šupić, Jordi Tura, and Antonio Acín. Scalable Bell inequalities for qubit graph states and robust self-testing. *Physical Review Letters*, 124:020402, Jan 2020. URL: https://link.aps.org/doi/10.1103/PhysRevLett.124.020402, doi:10.1103/PhysRevLett.124.020402.

[12] Miriam Backens, Hector Miller-Bakewell, Giovanni de Felice, Leo Lobski, and John van de Wetering. There and back again: A circuit extraction tale. *Quantum*, 5:421, 2021. arXiv:2003.01664.

[13] Jean-Daniel Bancal, Jonathan Barrett, Nicolas Gisin, and Stefano Pironio. Definitions of multipartite nonlocality. *Physical Review A—Atomic, Molecular, and Optical Physics*, 88(1):014102, 2013. arXiv:1112.2626, doi:10.1103/PhysRevA.88.014102.

[14] Jonathan Barrett and Stefano Pironio. Popescu-rohrlich correlations as a unit of nonlocality. *Physical review letters*, 95(14):140401, 2005. arXiv:quant-ph/0506180, doi:10.1103/PhysRevLett.95.140401.

[15] Sara Bartolucci, Patrick Birchall, Hector Bombin, Hugo Cable, Chris Dawson, Mercedes Gimeno-Segovia, Eric Johnston, Konrad Kieling, Naomi Nickerson, Mihir Pant, et al. Fusion-based quantum computation. 2021. arXiv:2101.09310.

[16] Mario Berta, Fernando GSL Brandão, Gilad Gour, Ludovico Lami, Martin B Plenio, Bartosz Regula, and Marco Tomamichel. On a gap in the proof of the generalised quantum stein's lemma and its consequences for the reversibility of quantum resources. *Quantum*, 7:1103, 2023. arXiv:2205.02813.

[17] Andrew Bolt, David Poulin, and Thomas M. Stace. Decoding schemes for foliated sparse quantum error-correcting codes. *Physical Review A*, 98(6):062302, 2018. arXiv:1810.11572.

[18] Eric Boutillon and Guido Masera. Hardware design and realization for iteratively decodable codes. In David Declercq, Marc Fossorier, and Ezio Biglieri, editors, *Channel Coding: Theory, Algorithms, and Applications*, pages 583–642. Elsevier, 2014.

[19] Cyril Branciard, Alexandre Clément, Mehdi Mhalla, and Simon Perdrix. Coherent control and distinguishability of quantum channels via PBS-diagrams. In Filippo Bonchi and Simon J. Puglisi, editors, *46th International Symposium on Mathematical Foundations of Computer Science, MFCS 2021, August 23-27, 2021, Tallinn, Estonia*, volume 202 of *LIPIcs*, pages 22:1–22:20. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2021. URL: https://doi.org/10.4230/LIPIcs.MFCS.2021.22, doi:10.4230/LIPICS.MFCS.2021.22.

[20] Gilles Brassard, Anne Broadbent, and Alain Tapp. Quantum pseudo-telepathy. *Foundations of Physics*, 35(11):1877–1907, 2005. arXiv:quant-ph/0407221, doi:10.1007/s10701-005-7353-4.

[21] Sergey Bravyi, David Gosset, and Robert König. Quantum advantage with shallow circuits. *Science*, 362(6412):308–311, 2018. arXiv:2308.07915.

[22] Sergey Bravyi, Yash Sharma, Mario Szegedy, and Ronald de Wolf. Generating k epr-pairs from an n-party resource state. *Quantum*, 8:1348, 2024. arXiv:2211.06497, doi:10.22331/q-2024-05-14-1348.

[23] Hans J Briegel, David E Browne, Wolfgang Dür, Robert Raussendorf, and Maarten Van den Nest. Measurement-based quantum computation. *Nature Physics*, 5(1):19–26, 2009. doi:10.1038/nphys1157.

[24] Anne Broadbent and André Allan Méthot. On the power of non-local boxes. *Theoretical Computer Science*, 358(1):3–14, 2006. arXiv:0504136.

[25] Dan Browne, Elham Kashefi, and Simon Perdrix. Computational depth complexity of measurement-based quantum computation. In *Conference on Quantum Computation, Communication, and Cryptography*, pages 35–46. Springer, 2010. arXiv:0909.4673.

[26] Daniel E Browne, Elham Kashefi, Mehdi Mhalla, and Simon Perdrix. Generalized flow and determinism in measurement-based quantum computation. *New Journal of Physics*, 9(8):250, 2007. arXiv:0702212.

[27] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *Reviews of Modern Physics*, 86:419, 2014. URL: https://link.aps.org/doi/10.1103/RevModPhys.86.419, doi:10.1103/RevModPhys.86.419.

[28] Adán Cabello, Samson Abramsky, and Ehtibar N. Dzhafarov. Contextuality and probability in quantum mechanics and beyond. *Philosophical Transactions of the Royal Society A*, 377(2157):20190136, 2019. URL: https://doi.org/10.1098/rsta.2019.0136.

[29] Maxime Cautrès, Nathan Claudet, Mehdi Mhalla, Simon Perdrix, Valentin Savin, and Stéphan Thomassé. Vertex-Minor Universal Graphs for Generating Entangled Quantum Subsystems. In Karl Bringmann, Martin Grohe, Gabriele Puppis, and Ola Svensson, editors, *51st International Colloquium on Automata, Languages, and Programming (ICALP 2024)*, volume 297 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 36:1–36:18, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik. arXiv:2402.06260, doi:10.4230/LIPIcs.ICALP.2024.36.

[30] Nathan Claudet, Mehdi Mhalla, and Simon Perdrix. Small k-pairable states, 2023. arXiv:2309.09956.

[31] Nathan Claudet and Simon Perdrix. Covering a graph with minimal local sets, 2024. arXiv:2402.10678.

[32] Nathan Claudet and Simon Perdrix. Local equivalence of stabilizer states: a graphical characterisation. 2024. arXiv:2409.20183.

[33] Julien Du Crest, Mehdi Mhalla, and Valentin Savin. Stabilizer inactivation for message-passing decoding of quantum LDPC codes. In *IEEE Information Theory Workshop (ITW)*, pages 488–493. IEEE, 2022. arXiv:2205.06125.

[34] Julien du Crest, Mehdi Mhalla, and Valentin Savin. A blindness property of the min-sum decoding for the toric code. *arXiv preprint arXiv:2406.14968*, 2024. arXiv:2406.14968.

[35] Dawei Ding and Liang Jiang. Coordinating decisions via quantum telepathy, 2024. arXiv:2407.21723.

[36] Paul Dorbec and Mehdi Mhalla. Quantum combinatorial games. In Bob Coecke and Aleks Kissinger, editors, *Proceedings 14th International Conference on Quantum Physics and Logic, QPL 2017, Nijmegen, The Netherlands, 3-7 July 2017*, volume 266 of *EPTCS*, pages 237–248, 2017. arXiv:1701.02193, doi:10.4204/EPTCS.266.16.

[37] Julien du Crest, Francisco Garcia-Herrero, Mehdi Mhalla, Valentin Savin, and Javier Valls. Layered decoding of quantum LDPC codes. In *International Symposium on Topics in Coding*, 2023. arXiv:2308.13377.

[38] Julien du Crest, Francisco Garcia-Herrero, Mehdi Mhalla, Valentin Savin, and Javier Valls. Check-agnosia based post-processor for message-passing decoding of quantum LDPC codes. *Quantum*, 8:1334, 2024. arXiv:2310.15000.

[39] Julien du Crest, Mehdi Mhalla, and Valentin Savin. Stabilizer inactivation for message-passing decoding of quantum LDPC codes. In *IEEE Information Theory Workshop (ITW)*, pages 488–493. IEEE, 2022. arXiv:2205.06125.

[40] Éric Duchêne, Valentin Gledel, Sylvain Gravier, Fionn Mc Inerney, Mehdi Mhalla, and Aline Parreau. Smash and grab: The 0.6 scoring game on graphs. *Theor. Comput. Sci.*, 990:114417, 2024. URL: https://doi.org/10.1016/j.tcs.2024.114417, doi:10.1016/J.TCS.2024.114417.

[41] Ross Duncan, Aleks Kissinger, Simon Perdrix, and John Van De Wetering. Graph-theoretic simplification of quantum circuits with the ZX-calculus. *Quantum*, 4:279, 2020. arXiv:1902.03178.

[42] Ross Duncan and Simon Perdrix. Rewriting measurement-based quantum computations with generalised flow. In *International Colloquium on Automata, Languages, and Programming (ICALP)*, pages 285–296. Springer, 2010.

[43] Frédéric Dupuis, Ashutosh Goswami, Mehdi Mhalla, and Valentin Savin. Polarization of quantum channels using clifford-based channel combining. *IEEE Trans. Inf. Theory*, 67(5):2857–2877, 2021. doi:10.1109/TIT.2021.3063093.

[44] Christoph Dürr, Mark Heiligman, Peter Høyer, and Mehdi Mhalla. Quantum query complexity of some graph problems. *SIAM J. Comput.*, 35(6):1310–1328, 2006. doi:10.1137/050644719.

[45] Rachid Echahed, Mnacho Echenim, Mehdi Mhalla, and Nicolas Peltier. A superposition-based calculus for diagrammatic reasoning. In Niccolò Veltri, Nick Benton, and Silvia Ghilezan, editors, *PPDP 2021: 23rd International Symposium on Principles and Practice of Declarative Programming, Tallinn, Estonia, September 6-8, 2021*, pages 10:1–10:13. ACM, 2021. doi:10.1145/3479394.3479405.

[46] Rachid Echahed, Mnacho Echenim, Mehdi Mhalla, and Nicolas Peltier. A strict constrained superposition calculus for graphs. In Orna Kupferman and Pawel Sobocinski,

editors, *Foundations of Software Science and Computation Structures - 26th International Conference, FoSSaCS 2023, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2023, Paris, France, April 22-27, 2023, Proceedings*, volume 13992 of *Lecture Notes in Computer Science*, pages 135–155. Springer, 2023. doi:10.1007/978-3-031-30829-1_7.

[47] Mnacho Echenim and Mehdi Mhalla. A formalization of the CHSH inequality and tsirelson's upper-bound in isabelle/hol. *J. Autom. Reason.*, 68(1):2, 2024. URL: https://doi.org/10.1007/s10817-023-09689-9, doi:10.1007/S10817-023-09689-9.

[48] Ryan R Ferguson, Luca Dellantonio, A Al Balushi, Karl Jansen, Wolfgang Dür, and Christine A Muschik. Measurement-based variational quantum eigensolver. *Physical review letters*, 126(22):220501, 2021.

[49] François Le Gall, Harumichi Nishimura, and Ansis Rosmanis. Quantum advantage for the local model in distributed computing. 2018. arXiv:1810.10838.

[50] Robert Gibbons. *Game Theory for Applied Economists*. Princeton University Press, 1992. doi:10.2307/j.ctvcmxrzd.

[51] Stefano Gogioso and Nicola Pinzani. The topology of causality. 2023. arXiv:2303.07148.

[52] Google Quantum AI. Suppressing quantum errors by scaling a surface code logical qubit. *Nature*, 614(7949):676–681, 2023. arXiv:2207.06431.

[53] Ashutosh Goswami, Mehdi Mhalla, and Valentin Savin. Quantum polarization of qudit channels. In *IEEE International Symposium on Information Theory, ISIT 2021, Melbourne, Australia, July 12-20, 2021*, pages 1487–1492. IEEE, 2021. doi:10.1109/ISIT45174.2021.9517845.

[54] Ashutosh Goswami, Mehdi Mhalla, and Valentin Savin. Improved rate fault-tolerant preparation of Q1 code-states. In *12th International Symposium on Topics in Coding, ISTC 2023, Brest, France, September 4-8, 2023*, pages 1–5. IEEE, 2023. doi:10.1109/ISTC57237.2023.10273493.

[55] Berry Groisman, Michael Mc Gettrick, Mehdi Mhalla, and Marcin Pawlowski. How quantum information can improve social welfare. *IEEE Journal on Selected Areas in Information Theory*, 1(2):445–453, 2020. URL: https://ieeexplore.ieee.org/document/9173538/, arXiv:1912.10967, doi:10.1109/JSAIT.2020.3012922.

[56] David Gross, Jens Eisert, Norbert Schuch, and David Perez-Garcia. Measurement-based quantum computation beyond the one-way model. *Physical Review A*, 76(5):052315, 2007. arXiv:0706.3401.

[57] Otfried Gühne, Géza Tóth, and Hans J Briegel. Multipartite entanglement in spin chains. *New Journal of Physics*, 7(1):229, 2005. arXiv:0502160.

[58] Andras Gyarfas and Mehdi Mhalla. Rainbow and orthogonal paths in factorizations of k_n. *Journal of Combinatorial Designs*, 18(3):167–176, 2010. URL: https://users.renyi.hu/~gyarfas/Cikkek/136_orthogonal.pdf.

[59] Matthew B Hastings and Jeongwan Haah. Dynamically generated logical qubits. *Quantum*, 5:564, 2021. arXiv:2107.02194.

[60] Marc Hein, Wolfgang Dür, Jens Eisert, Robert Raussendorf, Maarten Nest, and Hans J. Briegel. Entanglement in graph states and its applications. In *Quantum computers, algorithms and chaos*, pages 115–218. IOS Press, 2006. arXiv:0602096.

[61] Peter Høyer, Mehdi Mhalla, and Simon Perdrix. Resources required for preparing graph states. In Tetsuo Asano, editor, *Algorithms and Computation, 17th International Symposium, ISAAC 2006, Kolkata, India, December 18-20, 2006, Proceedings*, volume 4288 of *Lecture Notes in Computer Science*, pages 638–649. Springer, 2006. doi:10.1007/11940128_64.

[62] Sacha Huriot-Tattegrain and Mehdi Mhalla. Contextuality and expressivity of non-locality. In Benoît Valiron, Shane Mansfield, Pablo Arrighi, and Prakash Panangaden, editors, *Proceedings 17th International Conference on Quantum Physics and Logic, QPL 2020, Paris, France, June 2 - 6, 2020*, volume 340 of *EPTCS*, pages 160–173, 2020. arXiv:1912.11412, doi:10.4204/EPTCS.340.8.

[63] Jérôme Javelle, Mehdi Mhalla, and Simon Perdrix. New protocols and lower bounds for quantum secret sharing with graph states. In Kazuo Iwama, Yasuhito Kawano, and Mio Murao, editors, *Theory of Quantum Computation, Communication, and Cryptography, 7th Conference, TQC 2012, Tokyo, Japan, May 17-19, 2012, Revised Selected Papers*, volume 7582 of *Lecture Notes in Computer Science*, pages 1–12. Springer, 2012. doi:10.1007/978-3-642-35656-8_1.

[64] Jérôme Javelle, Mehdi Mhalla, and Simon Perdrix. On the minimum degree up to local complementation: Bounds and complexity. In Martin Charles Golumbic, Michal Stern, Avivit Levy, and Gila Morgenstern, editors, *Graph-Theoretic Concepts in Computer Science - 38th International Workshop, WG 2012, Jerusalem, Israel, June 26-28, 2012, Revised Selcted Papers*, volume 7551 of *Lecture Notes in Computer Science*, pages 138–147. Springer, 2012. doi:10.1007/978-3-642-34611-8_16.

[65] Zhengfeng Ji, Anand Natarajan, Thomas Vidick, John Wright, and Henry Yuen. MIP* =RE. *Communications of the ACM*, 64(11):131–138, 2021. arXiv:2001.04383.

[66] Jorma Jormakka and Jarmo V. E. Mölsä. Modelling information warfare as a game. *Journal of Information Warfare*, 4(2):12–25, 2005. URL: https://www.jstor.org/stable/26504060.

[67] Philippe Jorrand and Mehdi Mhalla. Separability of pure n-qubit states: Two characterizations. *Int. J. Found. Comput. Sci.*, 14(5):797–814, 2003. doi:10.1142/S0129054103002035.

[68] Yael Tauman Kalai, Ran Raz, and Ron D. Rothblum. How to delegate computations: the power of no-signaling proofs. In *Proceedings of the forty-sixth annual ACM symposium on Theory of computing*, pages 485–494, New York, NY, USA, 2014. Association for Computing Machinery. doi:10.1145/2591796.2591809.

[69] Marc Kaplan, Iordanis Kerenidis, Sophie Laplante, and Jérémie Roland. Non-local box complexity and secure function evaluation. *Quantum Information & Computation*, 11(1):40–69, 2011. arXiv:0903.2179.

[70] Elham Kashefi and Anna Pappa. Multiparty delegated quantum computing. *Cryptography*, 1(2):12, 2017. arXiv:1606.09200.

[71] Andrey Boris Khesin. *Quantum Computing from Graphs*. PhD thesis, Massachusetts Institute of Technology, Cambridge, MA, February 2025. arXiv:2501.17959. URL: https://arxiv.org/pdf/2501.17959.

[72] Alexei Kitaev. Almost-idempotent quantum channels and approximate c^*-algebras. 2024. arXiv:2405.02434.

[73] Alexei Yu Kitaev. Fault-tolerant quantum computation by anyons. *Annals of physics*, 303(1):2–30, 2003. arXiv:9707021.

[74] Simon Kochen and Ernst P Specker. The problem of hidden variables in quantum mechanics. *Ernst Specker Selecta*, pages 235–263, 1990.

[75] Kao-Yueh Kuo and Ching-Yi Lai. Exploiting degeneracy in belief propagation decoding of quantum codes. *npj Quantum Information*, 8(1):111, 2022. arXiv:2104.13659.

[76] François Le Gall and Frédéric Magniez. Sublinear-time quantum computation of the diameter in CONGEST networks. In *Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing*, pages 337–346, 2018. arXiv:1804.02917.

[77] Sangjun Lee, Mehdi Mhalla, and Valentin Savin. Trimming decoding of color codes over the quantum erasure channel. In *IEEE International Symposium on Information Theory, ISIT 2020, Los Angeles, CA, USA, June 21-26, 2020*, pages 1886–1890. IEEE, 2020. doi:10.1109/ISIT44484.2020.9174084.

[78] Anthony Leverrier and Gilles Zémor. Quantum tanner codes. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 872–883. IEEE, 2022. arXiv:2202.13641.

[79] Ye-Hua Liu and David Poulin. Neural belief-propagation decoders for quantum error-correcting codes. *Phys. Rev. Lett.*, 122:200501, May 2019. arXiv:1811.07835. doi:10.1103/PhysRevLett.122.200501.

[80] Seth Lloyd, Peter Shor, and Kevin Thompson. polylog-LDPC capacity achieving codes for the noisy quantum erasure channel. *IEEE Transactions on Information Theory*, 65(11):7584–7595, 2019. arXiv:1703.00382.

[81] Jonathan Z Lu, Andrey Boris Khesin, and Peter W Shor. Universal graph representation of stabilizer codes. 2024. arXiv:2411.14448.

[82] Lluis Masanes, Antonio Acín, and Nicolas Gisin. General properties of nonsignaling theories. *Physical Review A*, 73:012112, 2006. URL: https://link.aps.org/doi/10.1103/PhysRevA.73.012112, doi:10.1103/PhysRevA.73.012112.

[83] Tommy McElvanney and Miriam Backens. Complete flow-preserving rewrite rules for MBQC patterns with pauli measurements. *QPL 2022*, 2022. arXiv:2205.02009.

[84] N David Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Physical Review Letters*, 65(15):1838, 1990.

[85] Mehdi Mhalla, Mio Murao, Simon Perdrix, Masato Someya, and Peter S. Turner. Which graph states are useful for quantum information processing? In Dave Bacon, Miguel-Angel Martin-Delgado, and Martin Roetteler, editors, *Theory of Quantum Computation, Communication, and Cryptography - 6th Conference, TQC 2011, Madrid, Spain, May 24-26, 2011, Revised Selected Papers*, volume 6745 of *Lecture Notes in Computer Science*, pages 174–187. Springer, 2011. doi:10.1007/978-3-642-54429-3_12.

[86] Mehdi Mhalla and Simon Perdrix. Finding optimal flows efficiently. In Luca Aceto, Ivan Damgård, Leslie Ann Goldberg, Magnús M. Halldórsson, Anna Ingólfsdóttir, and Igor Walukiewicz, editors, *Automata, Languages and Programming, 35th International Colloquium, ICALP 2008, Reykjavik, Iceland, July 7-11, 2008, Proceedings, Part I: Tack A: Algorithms, Automata, Complexity, and Games*, volume 5125 of *Lecture Notes in Computer Science*, pages 857–868. Springer, 2008. doi:10.1007/978-3-540-70575-8_70.

[87] Mehdi Mhalla and Simon Perdrix. Graph states, pivot minor, and universality of (X,Z)-measurements. *Int. J. Unconv. Comput.*, 9(1-2):153–171, 2013. URL: http://www.oldcitypublishing.com/journals/ijuc-home/ijuc-issue-contents/ijuc-volume-9-number-1-2-2013/ijuc-9-1-2-p-153-171/.

[88] Mehdi Mhalla, Simon Perdrix, and Luc Sanselme. Characterising determinism in MBQCs involving pauli measurements. 2022. arXiv:2207.09368.

[89] Roger B. Myerson. Nash equilibrium and the history of economic theory. *Journal of Economic Literature*, 37:1067–1082, 1999. URL: https://pubs.aeaweb.org/doi/10.1257/jel.37.3.1067, doi:10.1257/jel.37.3.1067.

[90] John F. Nash. Equilibrium points in n-person games. *Proceedings of the National Academy of Sciences*, 36(1):48–49, 1950. doi:10.1073/pnas.36.1.48.

[91] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, July 2008. URL: https://iopscience.iop.org/article/10.1088/1367-2630/10/7/073013, doi:10.1088/1367-2630/10/7/073013.

[92] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press Cambridge, 2001.

[93] Josias Old and Manuel Rispler. Generalized belief propagation algorithms for decoding of surface codes. *Quantum*, 7:1037, 2023. arXiv:2212.03214 .

[94] Pavel Panteleev and Gleb Kalachev. Degenerate quantum LDPC codes with good finite length performance. *Quantum*, 5:585, 2021. arXiv:1904.02703.

[95] Jef Pauwels, Alejandro Pozas-Kerstjens, Flavio Del Santo, and Nicolas Gisin. Classification of joint quantum measurements based on entanglement cost of localization. 2024. arXiv:2408.00831.

[96] Simon Perdrix and Luc Sanselme. Determinism and computational power of real measurement-based quantum computation. In *International Symposium on Fundamentals of Computation Theory*, pages 395–408. Springer, 2017. arXiv:1610.02824.

[97] Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, March 1994. URL: http://link.springer.com/10.1007/BF02058098, doi:10.1007/BF02058098.

[98] David Poulin and Yeojin Chung. On the iterative decoding of sparse quantum codes. *Quantum Information and Computation*, 8(10):987–1000, 2008. arXiv:0801.1241.

[99] Robert Raussendorf. Measurement-based quantum computation with cluster states. *International Journal of Quantum Information*, 7(06):1053–1203, 2009. arXiv:0301052.

[100] Robert Raussendorf. Putting paradoxes to work: contextuality in measurement-based quantum computation. In *Samson Abramsky on Logic and Structure in Computer Science and Beyond*, pages 595–622. Springer, 2023. arXiv:2208.06624.

[101] Robert Raussendorf and Hans J Briegel. A one-way quantum computer. *Physical Review Letters*, 86(22):5188, 2001. arXiv:0108118.

[102] Robert Raussendorf, Jim Harrington, and Kovid Goyal. A fault-tolerant one-way quantum computer. *Annals of physics*, 321(9):2242–2270, 2006. arXiv:quant-ph/0510135, doi:10.1016/j.aop.2006.01.012.

[103] Robert Raussendorf, Jim Harrington, and Kovid Goyal. Topological fault-tolerance in cluster state quantum computation. *New Journal of Physics*, 9(6):199, 2007. arXiv:0703143.

[104] Alex Rigby, JC Olivier, and Peter Jarvis. Modified belief propagation decoders for quantum low-density parity-check codes. *Physical Review A*, 100(1):012330, 2019. arXiv:1903.07404.

[105] Joschka Roffe, David R White, Simon Burton, and Earl Campbell. Decoding across the quantum low-density parity-check code landscape. *Physical Review Research*, 2(4):043423, 2020. arXiv:2005.07016.

[106] Anna Schroeder, Matthias Heller, and Mariami Gachechiladze. Deterministic ansätze for the measurement-based variational quantum eigensolver. *New Journal of Physics*, 2023. arXiv:2312.13241.

[107] Will Simmons. Relating measurement patterns to circuits via pauli flow. *QPL2021*, 2021. arXiv:2109.05654.

[108] William Slofstra. The set of quantum correlations is not closed. In *Forum of Mathematics, Pi*, volume 7, page e1. Cambridge University Press, 2019. arXiv:1703.08618.

[109] Ivan Šupić and Joseph Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, September 2020. doi:10.22331/q-2020-09-30-337.

[110] Jacopo Surace. A theory of inaccessible information. *Quantum*, 8:1464, 2024. arXiv:2305.05734.

[111] Robert Michael Tanner. A recursive approach to low complexity codes. *IEEE Transactions on information theory*, 27(5):533–547, 1981.

[112] Jean-Pierre Tillich and Gilles Zémor. Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength. *IEEE Transactions on Information Theory*, 60(2):1193–1202, 2013. arXiv:0903.0566.

[113] Gabrielle Tournaire, Marvin Schwiering, Robert Raussendorf, and Sven Bachmann. A 3d lattice defect and efficient computations in topological MBQC. 2024. arXiv:2412.09781.

[114] Savvas Varsamopoulos, Koen Bertels, and Carmen Garcia Almudever. Comparing neural network based decoders for the surface code. *IEEE Transactions on Computers*, 69(2):300–311, 2019. arXiv:1811.12456.

[115] Yun-Jiang Wang, Barry C Sanders, Bao-Ming Bai, and Xin-Mei Wang. Enhanced feedback iterative decoding of sparse quantum codes. *IEEE Transactions on Information Theory*, 58(2):1231–1241, 2012. arXiv:0912.4546.

[116] Niclas Wiberg. Codes and decoding on general graphs, 1996. URL: https://api.semanticscholar.org/CorpusID:115168171.

[117] Hanwen Yao, Waleed Abu Laban, Christian Häger, Henry D Pfister, et al. Belief propagation decoding of quantum LDPC codes with guided decimation, 2023. preprint, arXiv:2312.10950.

Chapter 7

Curriculum Vitae

Experience

- 2023 CRHC (Full-Time Researcher) CNRS, LIG section 02
- 2021-2023 40% M.A.D. ANR Responsible Actions Quantum Technologies
- 2006 CRCN CNRS, LIG section 06
- 2005 Post-doc University of Calgary, Canada Department of Computer Science
- 2004 ATER University Joseph Fourier, Grenoble.
- 2001-2004 PhD Computer Science at Institut National Polytechnique de Grenoble, "Informatique quantique: algorithmes et complexité" under the supervision of Philippe Jorrand (Scholarship BDI -CNRS)

Awards

- EATCS Best Paper Award at ICALP 2004 joint with C. Dürr (LRI, Orsay), P. Hoyer (U. of Calgary, Canada) et M. Heiligmann (NSA, Fort Mead, MD, USA): Quantum query complexity of some graph problems.
- Ph.D. Award 2005 from the Institut National Polytechnique de Grenoble (INPG)

Teaching

- 2010-present, ENSIMAG Cybersecurity Master Cours en Information Quantique
- 2004-2005, Université Joseph Fourrier,Valence ATER en Informatique
- 2001-2004 Université Joseph Fourrier,Grenoble, Monitorat

Phd and Master Supervision

- 2024, Ph.D. Maxime Cautrès (with Valentin Savin) 50 %
- 2024, Internship post Master Maxime Cautrès (with Valentin Savin)
- 2022, Ph.D. Pierre Pocreau (with Alastair Abbott) 30 %
- 2022, Internship Caroline Mori (with Mnacho Echenim) 30%
- 2021, Ph.D. Julien Du Crest (with Valentin Savin) 50%
- 2021-2022 PFE of Pierre Pocreau
- 2018-2021 Phd Ashutosh Goswami (with Valentin Savin) 50 % (Now Post doc University of Copenhagen)
- 2018 Master de Louis Mathieu
- 2017-2020 Ph.D. Julian Wechs (avec Cyril Branciard) 30% (Now Post Doc Universite libre de Bruxelles)
- 2012 Internship Anurag Anshu (Assistant Professor Harvard)
- 2010-2014 Ph.D. Jérome Javelle (avec Simon Perdrix et Pablo Arrighi) 50% (Now Quantum Software Engineer UK)

Recent Grants

- 2024 Member of PraQV ANR JCJC
- 2023 Member of Scientific Board of QuantAlps
- 2022 Member of Quantera EQUIP
- 2017-2021 Responsible WP Computer science in ANR Idex QuEnG (Quantum Engineering Grenoble)
- 2015 Member of FeDMaM Maths à modeler (representing LIG)
- 2015-2019 Member of ANR GAG (Graphs and Games)

Chapter 8

List of publications

- **Peer-Reviewed International Journals**
  - **J.du Crest, M. Mhalla and V. Savin** A Blindness Property of the Min-Sum Decoding for the Toric Code. *IEEE Journal on Selected Areas in Information Theory.* 2025 (To appear) 10.48550/arXiv.2406.14968 `arXiv::2406.14968`,
  - **A. A. Abbott, M. Mhalla, and P. Pocreau.** Quantum query complexity of Boolean functions under indefinite causal order. *Phys. Rev. Research*, 6, L032020 (2024). DOI: 10.1103/PhysRevResearch.6.L032020.
  - **A. A. Abbott, M. Mhalla, and P. Pocreau.** Improving social welfare in non-cooperative games with different types of quantum resources. *Quantum*, 8, 1376 (2024). DOI: 10.22331/q-2024-06-17-1376.
  - **J. du Crest, F. Garcia-Herrero, M. Mhalla, V. Savin, and J. Valls.** Check-Agnosia based Post-Processor for Message-Passing Decoding of Quantum LDPC Codes. *Quantum*, 8, 1334 (2024). DOI: 10.22331/q-2024-05-02-1334.
  - **E. Duchene, V. Gledel, S. Gravier, F. Mc Inerney, M. Mhalla, and A. Parreau.** Smash and grab: The 0.6 scoring game on graphs. *Theoretical Computer Science*, 990 (2024). PDF.
  - **M. Echenim and M. Mhalla.** A Formalization of the CHSH Inequality and Tsirelson's Upper-bound in Isabelle/HOL. *J. Autom. Reason.*, 68(1): 2 (2024). URL: `https://doi.org/10.1007/s10817-023-09689-9`, `doi:10.1007/S10817-023-09689-9`.
  - **A. Goswami, M. Mhalla, and V. Savin.** Fault-tolerant preparation of quantum polar codes encoding one logical qubit. *Phys. Rev. A*, 108, 042605 (2023). `doi:10.1109/ISTC57237.2023.10273493`.
  - **M. Echenim, M. Mhalla, and C. Mori.** The CHSH inequality: Tsirelson's upper-bound and other results. *Arch. Formal Proofs*, 2023.
  - **A. Goswami, M. Mhalla, and V. Savin.** Multilevel polarization for quantum channels. *Quantum Inf. Comput.*, 21(7-8): 577-606 (2021). 10.48550/arXiv.2006.12652

– **F. Dupuis, A. Goswami, M. Mhalla, and V. Savin.** Polarization of Quantum Channels Using Clifford-Based Channel Combining. *IEEE Trans. Inf. Theory*, 67(5): 2857-2877 (2021). doi.org/10.1109/TIT.2021.3063093

– **A. A. Abbott, J. Wechs, D. Horsman, M. Mhalla, and C. Branciard.** Communication through coherent control of quantum channels. *Quantum*, 4: 333 (2020). arXiv:1810.09826, doi:10.22331/Q-2020-09-24-333.

– **B. Groisman, M. Mc Gettrick, M. Mhalla, and M. Pawlowski.** How Quantum Information can improve Social Welfare. *IEEE Journal on Selected Areas in Information Theory*, 2020. URL: https://ieeexplore.ieee.org/document/9173538/, arXiv:1912.10967, doi:10.1109/JSAIT.2020.3012922.

– **A. Anshu, P. Høyer, M. Mhalla, and S. Perdrix.** Contextuality in multipartite pseudo-telepathy graph games. *J. Comput. Syst. Sci.*, 107: 156-165 (2020). arXiv:1609.09689, doi:10.1016/j.jcss.2019.06.005.

– **J. Javelle, M. Mhalla, and S. Perdrix.** On weak odd domination and graph-based quantum secret sharing. *Theor. Comput. Sci.*, 598: 129-139 (2015). 10.1016/j.tcs.2015.05.038.

– **M. Mhalla and F. Prost.** Gardner's Minichess variant is solved. *ICGA Journal*, Vol. 36, No. 4, December 2013. 10.48550/arXiv.1307.711.

– **A. Anshu and M. Mhalla.** Pseudotelepathy games and genuine NS k-way non-locality using graph states. *Quantum Information and Computation*, 13(9-10): 833-845, 2013. arXiv:1207.2276.

– **M. Mhalla and S. Perdrix.** Graph States, Pivot Minor, and universality of (X-Z) Measurements. *IJUC*, 9(1-2): 153-171, 2013. URL: http://www.oldcitypublishing.com/journals/ijuc-home/ijuc-issue-contents/ijuc-volume-9-number-1-2-2013/ijuc-9-1-2-p-153-171/.

– **A. Gyarfas and M. Mhalla.** Rainbow and Orthogonal Paths in Factorizations of K_n. *Journal of Combinatorial Designs*, 18(3): 167-176, 2010. URL: https://users.renyi.hu/~gyarfas/Cikkek/136_orthogonal.pdf.

– **E. Duchene, S. Gravier, and M. Mhalla.** Combinatorial graph games. *Ars Combinatoria*, Vol. XC, pp. 33-44, 2009. URL:https://perso.liris.cnrs.fr/eric.duchene/articles/graphgames.pdf.

– **D. E. Browne, E. Kashefi, M. Mhalla, and S. Perdrix.** Generalized Flow and Determinism in Measurement-based Quantum Computation. *New J. Phys.*, 9: 250, 2007. arXiv:0702212.

– **S. Gravier, P. Jorrand, M. Mhalla, and C. Payan.** Quantum octal games. *International Journal of Foundations of Computer Science (IJFCS)*, 17(4): 919-932, 2006. https://arxiv.org/pdf/quant-ph/0311018.

– **C. Dürr, P. Høyer, M. Heiligmann, and M. Mhalla.** Quantum query complexity of some graph problems. *SIAM Journal on Computing*, 35(6): 131-132, 2006. doi:10.1137/050644719.

– **P. Jorrand and M. Mhalla.** Separability of pure N-qubit states: two characterizations. *International Journal of Foundations of Computer Science (IJFCS)*, 14(5): 797-814, October 2003. doi:10.1142/S0129054103002035.

- **S. Gravier, M. Mhalla, and E. Tannier.** On a modular domination game. *Theoretical Computer Science A*, 306(1-3): 291-303, September 2003. https://www.sciencedirect.com/science/article/pii/S0304397503002858.

- **Peer-Reviewed International Conferences with Proceedings**
  - **M. Cautrès, N. Claudet, M. Mhalla, S. Perdrix, V. Savin, and S. Thomassé.** Vertex-Minor Universal Graphs for Generating Entangled Quantum Subsystems. *ICALP 2024*, July 8-12, 2024, Tallinn, Estonia. arXiv:2402.06260, doi:10.4230/LIPIcs.ICALP.2024.36.
  - **M. Mhalla, S. Perdrix and L. Sanselme** Shadow Pauli Flow: Characterising Determinism in MBQCs involving Pauli Measurements *QPL 2025* arXiv::2207.09368,
  - **A. Abbott, M. Mhalla and P. Pocreau** Classical and quantum query complexity of Boolean functions under indefinite causal order *QPL 2025*
  - **A. Goswami, M. Mhalla, and V. Savin.** Improved Rate Fault-Tolerant Preparation of Q1 Code-States. *ISTC 2023*, Brest, France. doi:10.1109/ISTC57237.2023.10273493.
  - **J. du Crest, F. Garcia Herrero, M. Mhalla, V. Savin, and J. Valls.** Layered Decoding of Quantum LDPC Codes. *ISTC 2023*, Brest, France. arXiv:2308.13377.
  - **R. Echahed, M. Echenim, M. Mhalla, and N. Peltier.** A Strict Constrained Superposition Calculus for Graphs. *FoSSaCS 2023*, pp. 135-155. doi:10.1007/978-3-031-30829-1_7.
  - **J. Du Crest, M. Mhalla, and V. Savin.** Stabilizer Inactivation for Message-Passing Decoding of Quantum LDPC Codes. *2022 IEEE Information Theory Workshop (ITW)*, pp. 488-493, 2022. arXiv:2205.06125.
  - **N. Peltier, M. Echenim, R. Echahed, and M. Mhalla.** A Superposition-Based Calculus for Diagrammatic Reasoning. *PPDP 2021: 23rd International Symposium on Principles and Practice of Declarative Programming*, Tallinn, Estonia, 2021. doi:10.1145/3479394.3479405.
  - **C. Branciard, A. Clement, M. Mhalla, and S. Perdrix.** Coherent Control and Distinguishability of Quantum Channels via PBS-Diagrams. *MFCS 2021*, pp. 22:1-22:20. URL: https://doi.org/10.4230/LIPIcs.MFCS.2021.22, doi:10.4230/LIPICS.MFCS.2021.22.
  - **S. Lee, M. Mhalla, and V. Savin.** Trimming Decoding of Color Codes over the Quantum Erasure Channel. *2020 IEEE International Symposium on Information Theory (ISIT)*, pp. 1886-1890, IEEE, 2020. doi:10.1109/ISIT44484.2020.9174084.
  - **S. Huriot-Tattegrain and M. Mhalla.** Contextuality and Expressivity of Non-locality. *QPL 2020*, arXiv preprint arXiv:1912.11412. arXiv:1912.11412, doi:10.4204/EPTCS.340.8.
  - **F. Dupuis, A. Goswami, M. Mhalla, and V. Savin.** Purely Quantum Polar Codes. *ITW 2019*, Gotland, Sweden. doi: 10.1109/ITW44776.2019.8989387. https://ieeexplore.ieee.org/document/8989387.

– **A. Anshu, P. Høyer, M. Mhalla, and S. Perdrix.** Contextuality in Multipartite Pseudo-Telepathy Graph Games. *FCT 2017*, pp. 41-55. arXiv:1609.09689.

– **P. Dorbec and M. Mhalla.** Toward Quantum Combinatorial Games. *QPL 2017*. doi:10.48550/arXiv.1701.02193.

– **S. Gravier, J. Javelle, M. Mhalla, and S. Perdrix.** Quantum Secret Sharing with Graph States. *MEMICS*, 2012. https://hal.science/hal-00933722/document

– **J. Javelle, M. Mhalla, and S. Perdrix.** On the Minimum Degree by Local Complementation. *WG*, 2012. doi:10.1007/978-3-642-34611-8_16.

– **J. Javelle, M. Mhalla, and S. Perdrix.** New Protocols and Lower Bounds for Quantum Secret Sharing. *TQC*, 2012. doi:10.1007/978-3-642-35656-8_1.

– **M.Mhalla, M. Murao, S. Perdrix, M. Someya and P.S. Turner** Which graph states are useful for quantum information processing? *TQC 2011* In Theory of Quantum Computation, Communication, and Cryptography: 6th Conference Madrid, Spain, May 24-26, 2011, Revised Selected Papers 6 (pp. 174-187). Springer Berlin Heidelberg, 2014. doi:10.1007/978-3-642-54429-3_12.

– **J. Degorre and M. Mhalla.** A Combinatorial Approach of Non-Locality. *Recent Progress in the Theoretical and Experimental Foundations of Quantum Technology*, Quantum Africa, Durban, 2010.

– **E. Kashefi, D. Markham, M. Mhalla, and S. Perdrix.** Information Flow in Secret Sharing Protocols. *Developments in Computational Models*, EPTCS, Volume 9, pp. 87-97, 2009. https://arxiv.org/abs/0909.4479.

– **M. Mhalla and S. Perdrix.** Finding Optimal Flows Efficiently. *ICALP (1)*, pp. 857-868, 2008. doi:10.1007/978-3-540-70575-8_70.

– **P. Høyer, M. Mhalla, and S. Perdrix.** Resources Required for Preparing Graph States. *ISAAC*, pp. 638-649, 2006. doi:10.1007/11940128_64.

– **E. Duchene, S. Gravier, and M. Mhalla.** Around Wythoff's Game. *Proceedings of the 7th International Colloquium on Graph Theory*, September 2005. https://www.sciencedirect.com/science/article/abs/pii/S1571065305051991.

– **C. Dürr, P. Høyer, M. Heiligmann, and M. Mhalla.** Quantum Query Complexity of Some Graph Problems. *ICALP 2004*, Turku, Finland, July 2004, Automata, Language and Programming, pp. 481-493.

– **P. Jorrand and M. Mhalla.** Minimal Sets of Bi-Product Equalities Characterize Separable Pure Quantum States. *SIAM Conference on Applied Linear Algebra*, Williamsburg, VA, USA, July 2003, SPIE proceedings. Une version pour des mathématiciens a été publiée dans *IJFCS*, 14(5), October 2003.

– **P. Jorrand and M. Mhalla.** Minimal Sets of Conditions for Distinguishing Among Separable and Entangled States of Multi-Qubit Systems. *International Symposium on Quantum Informatics (QI'2002)*, pp. 157-163, Moscow, Russia, October 2002, SPIE proceedings. Une version générale incluant les preuves a été publiée dans *IJFCS*, 14(5), October 2003.

- **P. Jorrand and M. Mhalla.** On the Distinction Between Entangled and Separable States of Quantum Registers. *Second IEEE Conference on Nanotechnology (IEEE-NANO'2002)*, pp. 301-304, Washington DC, USA, August 2002. Une version générale incluant les preuves a été publiée dans *IJFCS*, 14(5), October 2003.
- **P. Jorrand and M. Mhalla.** Characterizing Separable Pure States of Multi-Qubit Systems. *Sixth International Conference on Quantum Communication, Measurement and Computing (QCMC'02)*, pp. 29-32, MIT, Cambridge MA, USA, July 2002, Rinton Press proceedings. simplified version for physicists from *IJFCS*, 14(5), October 2003.

• **Peer-Reviewed International Conferences**

- **A. Abbott, M. Mhalla, and P. Pocreau.** Query Complexity of Boolean Functions under Indefinite Causal Order. *QPL 2023*
- **A. Abbott, M. Mhalla, and P. Pocreau.** Improving social welfare in non-cooperative games with different types of quantum resources. *CEQIP 2023*, arXiv preprint arXiv:2211.01687, 2023.
- **F. Dupuis, A. Goswami, M. Mhalla, and V. Savin.** Purely Quantum Polar Codes. *QIP 2020*, China.
- **A.A. Abbott, J. Wechs, D. Horsman, M. Mhalla, and C. Branciard.** Communication through coherent control of quantum channels. *AQIS 2019*, Seoul.
- **J. Degorre and M. Mhalla.** A combinatorial approach of non-locality. *Quantum Africa 2010*, Durban.
- **C. Dürr, P. Høyer, M. Heiligmann, and M. Mhalla.** Quantum query complexity of some graph problems (Single Source Shortest Paths). In *QIP 2004*, Waterloo, Canada, January 2004. Part of arXiv preprint quant-ph/041091.