Leopold-Franzens-Universität Innsbruck

Master Thesis

Efficient Two Dimensional Quantum Repeater

Author:
Sonia López-Bravo

Supervisor:
Prof. Mag. Dr. Wolfgang Dür

A thesis submitted in partial fulfillment of the requirements for the degree of Master of Science

in the

Leopold-Franzens-Universität Innsbruck
at Institut für Theoretische Physik

May 23, 2019

Leopold-Franzens-Universität Innsbruck

Ich erkläre hiermit an Eides statt durch meine eigenhändige Unterschrift, dass ich die vorliegende Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe. Alle Stellen, die wörtlich oder inhaltlich den angegebenen Quellen entnommen wurden, sind als solche kenntlich gemacht.
Die vorliegende Arbeit wurde bisher in gleicher oder ähnlicher Form noch nicht als Magister-/Master-/Diplomarbeit/Dissertation eingereicht.

Unterschrift:

Datum:

I was within and without,
simultaneously enchanted and repelled by the inexhaustible variety of life.

Fitzgerald, F. Scott *The Great Gatsby*

Abstract

Long-distance quantum communication is one of the most appealing applications of quantum technology. It promises secure classical communication via quantum key distribution and is also essential for distributed quantum computation. High-rate quantum communication over long distances is possible using quantum repeaters, which either utilize quantum error correction or combine entanglement purification and entanglement swapping. In a real-world application of quantum communication one needs flexible multi-user structures that allow for quantum communication between arbitrary pairs of parties and facilitate also multi-user applications. Sharing of multi-partite entangled states between parties offers a solution, allowing for parallel quantum communication. To address this problem, a 2D quantum repeater architecture was proposed in [44] to establish long-distance entanglement shared between multiple partners. The scheme was based on the creation of self-similar multi-qubit entanglement structures at growing scale, where variants of entanglement swapping and multi-party entanglement purification are combined to create high fidelity entangled states. Here we propose an efficient 2D quantum repeater based on four-particle GHZ states, which allows quantum error correction against single qubit errors but also against multi-qubit errors.

Acknowledgements

These are the acknowledgements.

Contents

Chapter 1

Introduction

In the year 1935, Einstein, Podolsky and Rosen expressed their concerns about quantum mechanics as an incomplete theory [1]. They recognized a "spooky" feature which implied the existence of global states of a composite system which cannot be written as a product of the states of individual subsystems. They proposed a Gedanken experiment, known as EPR paradox, which should prove that description of quantum mechanics was incomplete and there were fixed values of physical quantities prior to measurement, known as hidden variables. This phenomenon, today known as "entanglement," was originally called by Schrödinger "Verschränkung" in the same year and he formulated some of the mathematical implications of entanglement on the statistics of measurement outcomes [2].

In 1964 Bell accepted the EPR conclusion - that quantum description of reality was not complete- as a working hypothesis and formalized the EPR idea of deterministic world in terms of local hidden variable model (LHVM) [3]. He assumes: (i) Realism, i.e. measurement results are determined by properties the particles carry prior to, and independent of, measurements; (ii) Locality, i.e. results obtained at one localition are independent of any action performed spacelike separated; and (iii) Freedom, i.e. the setting is independent of the hidden variables which determine the local results. Bell's theorem states that any physical theory that incorporates local realism impose constrains in the form of inequalities on statistical correlations in experiments involving bipartite systems. He showed that outcomes obtained from some entangled quantum state violate the Bell inequality, i.e local realism cannot reproduce all the predictions of quantum mechanics. It was not until 1981 when Aspect *et al* reproduced a convincing test of violation of Bell inequalities [4] using photons and demonstrated that predictions of quantum mechanics are correct, and since then many experiments have been tested LHVM leading to a evidence of violation of Bell's inequality. Nevertheless, Bell's theorem experiments rely on additional assumptions that open loopholes for local realism, and for that reason loophole-free Bell tests are performed [5], probably the most known is the recent Big Bell Test Collaboration [6].

Entanglement plays a central role in some key discoveries such as quantum cryptography [8], quantum dense coding [9] and quantum teleportation [10]. Quantum entanglement inspired the idea of quantum computation, and it plays a central role in one-way quantum computing, measurement-based schemes and linear optics quantum computing. Entanglement also leaded to a new domain called quantum information, which comprises quantum communication, quantum error correction, quantum key distribution or entanglement purification.

It is clear that entanglement is a valuable resource for tasks that cannot be performed by means of classical resources. It can be manipulated, broadcasted, controlled and distributed. It can help in tasks as reduction of classical communication complexity, clock synchronization, super-radiance, superconductivity or quantum phase transitions. Unfortunately, quantum entanglement has three disagreeable but interesting features: It has in general a very complex structure, it is fragile with respect to enviroment, and it cannot be increased on average when systems are not in direct contact but distributed in spatially separated regions.

In the context of applications in quantum information theory, we may choose multipartite entanglement states rather than bipartite. We could use only bipartite entanglement but in experiments the dimension of Hilbert spaces is finite because we cannot store infinite qubits. The dimension of Hilbert spaces is indeed restricted in quantum networks and quantum technologies. Graph states form a rich class of entangled states that exhibit key aspects of multipartite entanglement. The general form of graph states has been introduced by Raussendorf *et al* [12] as a generalization of cluster states [13]. They have a variety of applications, most prominently as algorithmic resources

of the one-way quantum computer, but also in other fields such as quantum error correction and multi-partite quantum communication.

1.1 Outline

This work is structured as follows. In chapter 2 we will introduce the concept of graph [14] and basic definitions regarding the features of graphs -most of them are intuitive- including how to manipulate graphs easily. We will see the notion of partitions and bipartite graphs which are crucial when modelling relations between two different classes of objects, as well as the notion of graph colouring. We will explain the operation of local complementation which is a very important graph operation in the context of equivalence classes of graphs and graph states, and the operation of vertex deletion which is related with the vertex-minor problem, with complexity $\mathbb{NP}$-complete. Finally, we will see how graphs are associated with quantum systems.

Once we are familiar with graphs and graph theory, we will see how they can be used in quantum theory of entanglement. In chapter 3 we will explain the concept of graph states giving two alternative definitions, in terms of the interaction pattern and in terms of stabilizer formalism, which will be explained in detail in section 3.3. We will study what we call equivalent graph states through the notion of Clifford and local Clifford operation, and, by the use of local complementation introduced previously in section 2.3, we will show that graph and graph state local operations are equivalent. Finally, since graph states are multipartite quantum systems we are interested in measurements of graph states, and for that reason we will see briefly the action of local Pauli measurements and Clifford operation, as well as the connection of two graph states.

In chapter 4 we start with a brief introduction to quantum entanglement. We will introduce the concept of quantum entangled state in the cases of pure and mixed states. In the context of quantum operations, we will define the most general way of describing the evolution of a quantum system, which is a quantum channel. We will talk about the separability problem, which is a $\mathbb{NP}$-hard problem, and necessary conditions for entanglement: PPT criterion and entanglement witnesses, in particular entanglement witnesses allow us to study the separability properties of density operators. We will see how we can characterize entanglement by means of non-increasing quantities under local operations and classical communications. Finally we review some of the first applications of quantum entanglement, such as quantum key distribution, quantum dense coding and teleportation.

In chapter 5 we focus on

Chapter 2

Graph Theory

2.1 Introduction

A graph is a collection of vertices and a description of which vertices are connected by an edge. The usual way to picture a graph is by drawing a dot for each vertex and joining two of these not necessarily distinct dots by a line if the corresponding two vertices form an edge. Graphs can be used to model many types of relations and processes in physical, biological, social and information systems. In the context of the present work, physical systems with Hilbertspace $\mathcal{H}^a$ will take the role of vertices, whereas edges represent an interaction. If not stated otherwise $\mathcal{H}^a \cong \mathbb{C}^2$ (qubit).

Formally, a graph [14] is a pair $G = (V, E)$ of sets such that $E \subseteq [V]^2$; thus, the elements of E are 2-element subsets of V. The elements $v \in V$ are called vertices (or nodes) of the graph G, the elements $e \in E$ are its edges. A graph with vertex set V is said to be a graph on V.

If the size of V is $|V| = N$, then the number of different possibilities for choosing set of edges E is $\binom{N}{2} = \frac{N(N-1)}{2}$. So, for a given set of vertices V there are $2^{\binom{N}{2}}$ distinct graphs. The vertex set of a graph G is referred to as $V(G)$, its edge set as $E(G)$. An edge $e \in E$ is written $e = \{a, b\}$, while for undirected graphs $\{a, b\} \equiv \{b, a\}$. A weighted graphs is a graph that has real numbers $P_{ab} \in \Re$ associated with edges $\{a, b\}$.

In the following we will only consider simple graphs, that is no edge connects a vertix with itself (no loops), $\{a, a\} \ni E$ and there is not multiples edges between the same pair of vertices.

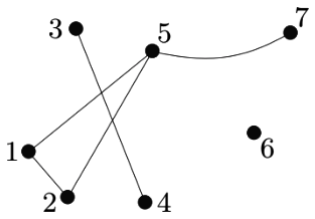

Figure 2.1: Example of a simple, undirected graph. In this case, $V = \{1, 2, 3, 4, 5, 6, 7\}$ and $E = \{\{1, 2\}, \{1, 5\}, \{2, 5\}, \{3, 4\}, \{5, 7\}\}$.

The number of vertices of a graph G is its order, written as $|G|$; its number of edges is denoted by $\|G\|$. Graphs are finite, infinite, countable and so on according to their order. An edge e is called incident with a vertix a if e contains a, i.e. $e = \{a, b\}$ with $b \in V$. When the vertices $a, b \in V$ are the endpoints of an edge, they are referred to as being adjacent.

Definition 2.1 **Paths and cycles** A $\{a, b\}$-path is an ordered list of vertices $a = a_1, a_2, \ldots, a_{n-1}, a_{n=b}$, such that for all i, vertices a_i and a_i+1 are adjacent. A cycle is a path wherein a vertex is reachable from itself. The number of vertices of a path is the lenght of the path.

Definition 2.2 **Connected graph** A connected graph is a graph that has a $\{a, b\}$-path for any two vertices $a, b \in V$. Otherwise we say it is a disconnected graph.

Definition 2.3 **Complete graph** A complete graph is a graph such that all vertices of G are pairwise adjacent, i.e. every pair of vertices is connected by an edge. For a given number of vertices, there is a unique complete graph which is written as K_N, where N is the number of vertices.

Note that every complete graph is necessarily connected, but connected graphs are not necessarily complete.

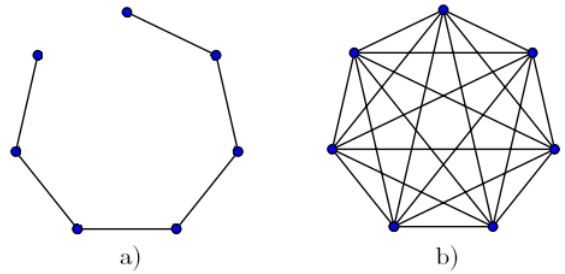

Figure 2.2: Two types of connected graphs for the case of seven vertices: (a) The linear graph and (b) the complete graph, i.e. fully connected.

Definition 2.4 **Adjacency matrix** The adjacency relation gives rise to an adjacency matrix Γ_G associated with a graph. If $V = \{a_1, \ldots, a_N\}$, then the adjacency matrix Γ_G is a symmetric matrix $N \times N$, with elements,

$$(\Gamma_G)_{ij} = \begin{cases} 1 & \{a_i, a_j\} \in E \\ 0 & \text{otherwise} \end{cases} \tag{2.1}$$

Remark For weighted graphs

$$(\Gamma_G)_{ij} = \{ \begin{matrix} \varphi_{a_i a_j} & , \{a_i, a_j\} \in E \\ 0 & , \text{otherwise} \end{matrix} \tag{2.2}$$

where $\varphi_{a_i a_j} \in \Re$.

Definition 2.5 **Neighborhood** The neighborhood of vertix a, written as N_a, is the set of vertices b connected with a with an edge.

$$N_a = \{b \in V | \{a, b\} \in E\} \tag{2.3}$$

In other words, the neighborhood is the set of vertices adjacent to a given vertex. The degree of vertix a is the size of its neighborhood, $d(a) = |N_a|$. A vertex $a \in V$ with an empty neighborhood will be called isolated vertex. In the study of graphs, we are mostly interested in problems that are invariant under permutations of the vertices when these permutations respect the neighborhood relation, i.e., map neighbored vertices onto neighbored vertices. Such permutations are called graph isomorphisms.

Definition 2.6 **Isomorphic graphs** Let consider two graphs $G = (V, E)$, $G' = (V', E')$ and $|V| = |V'|$. We say G and G' are isomorphic, $G \simeq G'$ if there exist a bijection $\phi : V \to V'$ such that

$$\{a, b\} \in E \Longleftrightarrow \{\phi(a), \phi(b)\} \in E' \tag{2.4}$$

for all $a, b \in V$. The map ϕ is called an isomorphism. We usually do not distinguish between isomorphic graphs. Note that the number of isomorphic graphs grows exponentially with the number N of vertices.

We set $G \cup G' := (V \cup V', E \cup E')$ and $G \cap G' := (V \cap V', E \cap E')$. If $G \cap G' = \varnothing$ then G and G' are disjoint. If $V' \subseteq V$ and $E' \subseteq E$ then G' is a subgraph of G, $G' \subseteq G$ (and G a supergraph of G'). Less formally, we say that G contains G'.

Consider a graph $G = (V, E)$, we can execute some manipulations and obtain new graphs from it. We will talk about the graph obtained from G by deleting vertix $a \in V$ and all edges incident with a, written$G \backslash a$; the graph obtained from G by deleting all $a \in A \subseteq V$ and all edges incident with a, $G \backslash A$ and the graph obtained from G by deleting all edges $e \in F \subseteq E$, $G \backslash F$.

Besides deleting vertices and edges, we can also join elements of graph G to other sets. For a set of edges $F \subseteq [V]^2$, we will write the graph obtained from G by cupping all edges $e \in F$, $G \cup F := (V, E \cup F)$ and the graph obtained from G by adding all edges $e \in F$, $G + F := (V, E + F)$, where

$$E + F = (E \cup F) \setminus (E \cap F) \tag{2.5}$$

is the symmetric difference of E and F.

Definition 2.7 **Complement graph** The complement $\overline{G}$ of graph G is the graph on V with edge set

$$\overline{E} = \{(a, b) \in [V]^2 : (a, b) \notin E \wedge a \neq b\} \tag{2.6}$$

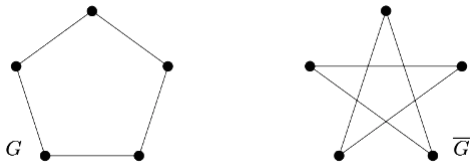

Figure 2.3: Example of a graph and its complement. In this particular case, G is isomorphic to $\overline{G}$.

2.1.1 Tree graphs

A tree is an undirected graph in which any two vertices are connected by exactly one path. Every graph that does not contain any cycle is a tree, and viceversa. A forest is a disjoint union of trees. Thus, a forest is a graph whose components are trees. The vertices of degree 1 in a tree are called leaves.

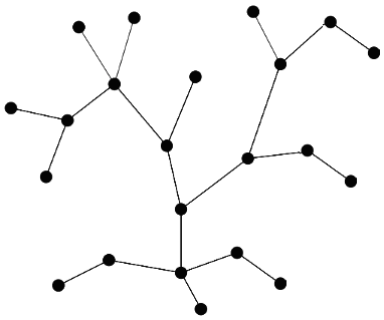

Figure 2.4: A tree

Proposition 2.1.1. *Consider a graph T, the following assertions are equivalent:*

(i) *T is a tree;*

(ii) *Any two vertices of T are linked by a unique path in T;*

(iii) *T is minimally connected, i.e. T is connected but $T \setminus e$ is disconnected for every edge $e \in T$;*

(iv) *T is maximally acyclic, i.e. T contains no cycle but $T + \{a, b\}$ does, for any two non-adjacent vertices $a, b \in T$.*

We will write $\{a, T, b\}$ for the unique path in a tree T between two vertices $a, b \in T$. Every connected graph G admits a spanning tree, which is a tree that contains every vertex of G and whose edges are edges of G. For any three vertices in a tree, the three paths between them have exactly one vertex in common.

Sometimes it is convenient to consider one vertex of a tree as special; such a vertex $r \in V$ is then called the root of this tree. A tree T with a fixed root is a rooted tree. The edges of a rooted tree can be assigned a natural orientation, either away from or towards the root, in which case the structure becomes a directed rooted tree. When a directed rooted tree has an orientation away from the root, it is called an arborescence, branching, or out-tree; when it has an orientation towards the root, it is called an anti-arborescence or in-tree. The tree-order is the partial ordering on the vertices of a tree, with $a <_T b$ for $a \in \{r, T, b\}$ if and only if the unique path from the root r to b passes through a. We say that a lies below b in T.

Theorem 2.1.1. *A connected graph with N vertices is a tree if and only if it has $N - 1$ edge.*

Proof. Induction on (i) shows that the subgraph spanned by the first i vertices has $i-1$ edges; for $i = N$ this proves the forward implication. Conversely, let G be any connected graph with N vertices and $N-1$ edges. Let G' be a spanning tree in G. Since G' has $N-1$ edges by the first implication, it follows that $G = G'$. □

2.1.2 Colouring

A vertex colouring of a graph $G = (V, E)$ is a map $c : V \to S$ such that $c(v) \neq c(w)$ for any adjacent vertices $v, w \in V$. The elements of the set S are called the available colours. We shall be asking for the smallest integer k such that G has a k-colouring, a vertex colouring $c : V \to \{1, \ldots, k\}$. This k is the vertex-chromatic number of G and it is denoted by $\chi(G)$. A graph G with $\chi(G) = k$ is called k-chromatic; if $\chi(G) \leq k$, the graph G is called k-colourable.

For $k = 2$, 2-colouring of a graph is a map $c : V \to \{1, 2\}$ such that all adjacent vertices are associated with a different element from $\{1, 2\}$, which can be identified with two colors. Note that a k-colouring is nothing but a vertex partition into k independent sets, now called colour classes. The non-trivial 2-colourable graphs are precisely the bipartite graphs.

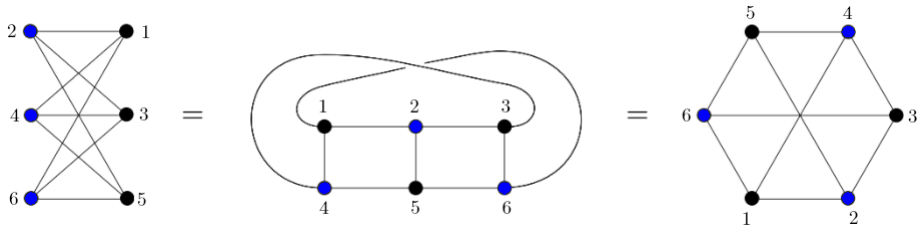

Figure 2.5: Three different representations of the same bipartite graph.

An edge colouring of $G = (V, E)$ is a map $c : E \to S$ such that $c(e) \neq c(f)$ for any adjacent edges $e, f \in E$. The smallest integer k for which a k-edge-colouring exists, i.e. an edge colouring $c : E \to \{1, \ldots, k\}$, is the edge-chromatic number of G and it is denoted by $\chi'(G)$.

2.1.3 Partitions

In the multi-partite case we can group vertices into different partitions and study different features as multipacks, entanglement between partitions, etc. A partition of V will be any tuple $(A_1, \ldots, A_N)$ where $A_i \subset V$ are disjoint sets with $\bigcup_{i=1}^{N} A_i = V$. We will write

$$(A_1, \ldots, A_N) \leqslant (B_1, \ldots, B_{N'}) \tag{2.7}$$

if $(A_1, \ldots, A_N)$ is finier than $(B_1, \ldots, B_{N'})$ meaning that for every A_i then is B_j with $A_i \subset B_j$. We say that B_j is a coarser partition.

2.2 Bipartite graphs

Let $r \geq 2$ be an integer. A graph $G = (V, E)$ is called r-partite if the set of vertices V admits a partition into r classes such that every edge has its ends in different classes, i.e. vertices in the same partition class must not be adjacent. An r-partite graph in which every two vertices from different partition classes are adjacent is called complete and it is denoted by $K_{n_1,\ldots,n_r}$ where n_i is the number of vertices in partition i. If $n_1 = \ldots = n_r := s$, we simply write K_s^r. Thus, K_s^r is the complete r-partite graph in which every partition class contains exactly s vertices.

A bipartite graph is a 2-partite graph, i.e. its set of vertices can be partitioned into two disjoint sets, often called sinks or sources, such that no two vertices within the same set are adjacent.

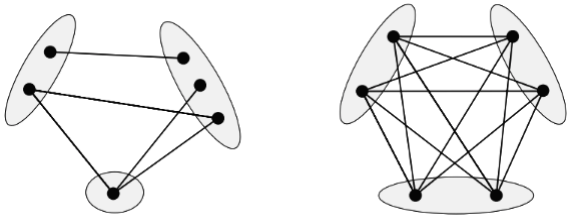

Figure 2.6: Example of two 3-partite graphs.

Theorem 2.2.1. *A graph is bipartite if and only if it contains no cycle of ood lenght.*

Proof. Consider a graph $G = (V, E)$ without odd cycles. A graph is bipartite if all its components are bipartite or trivial, so we may assume that G is connected. Since every connected graph admits a spanning tree, let T be a spanning tree in G, let $r \in T$ be its root, and denote the associated tree-order on V by $\leqslant_T$. For each $v \in V$, the unique path $\{r, T, v\}$ has odd or even length. This defines a bipartition of V; thus we show that G is bipartite with this partition.

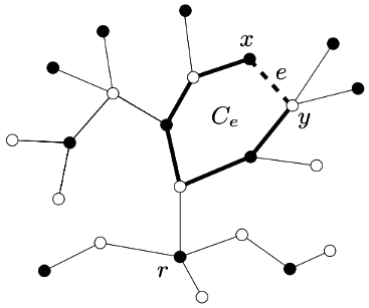

Figure 2.7: The cycle C_e in graph $T + e$.

Now let $e = \{a, b\}$ be an edge of a complete graph G. If $e \in T$, with $a <_T b$, then the unique path $\{r, T, b\} = \{r, T, a, b\}$ and so a and b lie in different partition classes and G is bipartite. If $e \notin T$ then $C_e := \{a, T, b\} + e$ is a cycle, and by the case treated already the vertices along $\{a, T, b\}$ alternate between the two classes and a and b again lie in different classes, and C_e is an even cycle. □

Corollary 1. *Every tree is a bipartite graph.*

Definition 2.8 **Star graph** A complete bipartite graph of the form $K_{1,N-1}$, i.e. a single vertex belongs to one set and all the remaining vertices belong to the other set, is called star graph and it is denoted by $S_{N,a}$ or $ST_{N,a}$ where $a \in V$ is the lone vertex.

Consider a bipartition (A, B) of the graph $G = (V, E)$. The subgraph $G_{AB} = (V, E_{AB})$ is induced by the edges $E_{AB} \equiv E(A, B)$ between A and B and Γ_{AB} will denote the $|A| \times |B|$-off-diagonal submatrix of adjacency matrix Γ_G:

$$\Gamma_G = \begin{pmatrix} \Gamma_A & \Gamma_{AB}^T \\ \Gamma_{AB} & \Gamma_B \end{pmatrix} \tag{2.8}$$

and similarly

$$\Gamma_{G_{AB}} = \begin{pmatrix} 0 & \Gamma_{AB}^T \\ \Gamma_{AB} & 0 \end{pmatrix} \tag{2.9}$$

2.3 Equivalent graphs

2.3.1 Local Complementation

Local complementation is a fundamental operation on graphs.

Proposition 2.3.1 (Local Complementation). *Local complementation τ_v (LC) is a graph operation specified by a vertex $v \in V$, transforming a graph $G = (V, E)$ into $\tau_v(G)$ by replacing the induced subgraph on the neighborhood of v, i.e. $G[N_v]$, by its complement. The neighborhood of any vertex u in the new graph $\tau_v(G)$ is therefore given by*

$$N_u^{\tau_v(G)} = \begin{cases} N_u \Delta (N_v \setminus \{u\}) & if\ (u,v) \in E \\ N_u & else \end{cases} \tag{2.10}$$

where Δ is the symmetric difference between two sets. Given a sequence of vertices $\boldsymbol{v} = \{v_1, \ldots, v_k\}$, we denote the induced sequence of local complementations, acting on a graph G, as

$$\tau_{\boldsymbol{v}}(G) = \tau_{v_k} \circ \cdots \circ \tau_{v_1}(G) \tag{2.11}$$

If two graphs G_1 and G_2 are related by a sequence of local complementations, i.e. $\exists \mathbf{v} : \tau_{\mathbf{v}}(G_1) = G_2$, we say the two graphs LC-equivalent and we write $G_1 \sim_{LC} G_2$. Starting with a graph, the complete orbit can be obtained by succesively applying local complementation to the vertices in the preceding graph.

Remark Consider a vertex set V. For a vertex $c \in V$ of the star graph $S_{|V|,c}$ we have that $\tau_c(S_{|V|,c}) = K_{|V|}$ and for any $v \in V$ we have $\tau_v(K_{|V|}) = S_{|V|,v}$. This means all star graphs on a vertex set V are equivalent to each other under local complementation and also to the complete graph on V . Moreover, no other graph is equivalent to the star or complete graph.

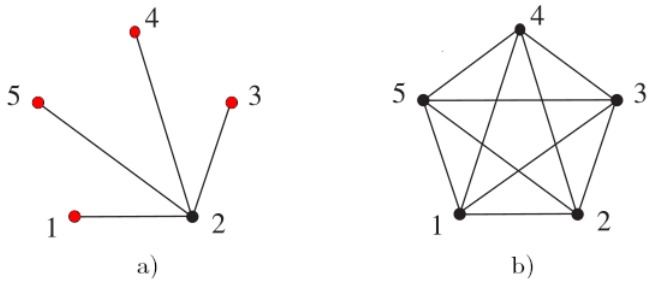

Figure 2.8: The star graph (a) and the complete graph (b) are related by a single local complementation operation. Red vertices represent the neighborhood of vertex 2.

2.3.2 Vertex-deletion

Another fundamental operation on a graph is that of vertex-deletion, which we will see it relates to measuring a qubit of a graph state in the standard basis.

Lemma 2.3.1 (Vertex-deletion). *Consider the graph $G = (V, E)$ and vertices $u, v \in V$ such that $u \neq v$, then*

$$\tau_v(G \setminus u) = \tau_v(G) \setminus u \tag{2.12}$$

This implies that on a graph $G = (V, E)$ local complementation and vertex-deletion are exchangeable.

Proof. We need to prove that graphs $G_1 = \tau_v(G \setminus u)$ and $G_2 = \tau_v(G) \setminus u$ are equal, and to do this we show that the neighborhoods of all vertex in the graphs are the same, i.e. $N_w^{G_1} = N_w^{G_2}$ for all $w \in V \setminus u$. We have seen that local complementation $\tau_v(G)$ only changes the neighborhoods for vertices which are adjacent to v, so for any vertex $w \neq u$ which is not adjacent to v, we have that

$$N_w^{G_1} = N_w^{G_2} = N_w^G \setminus \{u\} \tag{2.13}$$

If vertex w is adjacent to v its neighborhood becomes

$$N_w^{G_1} = (N_w^G \setminus \{u\}) \Delta \left((N_v^G \setminus \{u\}) \setminus \{w\} \right) = \left((N_w^G \Delta (N_v^G \setminus \{w\}) \setminus \{w\} \right) \setminus \{u\} = N_w^{G_2} \tag{2.14}$$

by the definition of a local complementation. □

Definition 2.9 **Vertex-minor** A graph G' is called a vertex-minor of G, i.e. $G' < G$ if and only if there exist a sequence of local complementations and vertex-deletions that takes G to G'. Since vertex-deletions can always be performed last in a sequence of local complementations (see Equation 2.3.1), an equivalent definition is the following:

$$G' < G \Longleftrightarrow \tau_{\mathbf{v}}(G)[V(G')] = G \tag{2.15}$$

where $\mathbf{v}$ is a sequence of local complementations.

Corollary 2. *If two graphs G_1, G_2 are LC-equivalent, then $G' < G_1$ if and only if $G' < G_2$.*

2.4 Quantum system

We can associate with each vertex $a \in V$ a two-level quantum system with Hilbertspace $\mathcal{H}^a \cong \mathbb{C}^2$ or qubit. The state vector of the single–qubit system $\mathcal{H}^a$ can be written as

$$|\psi\rangle^a = \alpha\,|0\rangle^a + \beta\,|1\rangle^a \tag{2.16}$$

with $|\alpha|^2 + |\beta|^2 = 1$. Consider the Pauli matrices of this two–level system $\sigma_i^a = \{\mathbb{I}^a, \sigma_x^a, \sigma_y^a, \sigma_z^a\}$ with $i = 0, 1, 2, 3$, where the upper index specifies the Hilbert space on which the operator acts.

$$\sigma_i^a = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\} \tag{2.17}$$

Note that these operators form an orthogonal basis of Hermitian operators with respect to the scalar product $\langle A, B\rangle := tr(A^\dagger B)$. The vectors $|0\rangle \equiv |+, z\rangle$ and $|1\rangle \equiv |-, z\rangle$ are the eigenvectors of the Pauli matrix σ_z with eigenvalues $+1$ and -1. Alternatively, we could use the vectors $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \equiv |+, x\rangle$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \equiv |-, x\rangle$, which are the eigenvectors of the Pauli matrix σ_x with eigenvalues $+1$ and -1.

$$\sigma_z\,|\pm, z\rangle = \pm\,|\pm, z\rangle \tag{2.18}$$
$$\sigma_x\,|\pm, x\rangle = \pm\,|\pm, x\rangle \tag{2.19}$$

In general $\overrightarrow{n} \cdot \overrightarrow{\sigma}\,|\pm, \overrightarrow{n}\rangle = \pm\,|\pm, \overrightarrow{n}\rangle$, where $\overrightarrow{n} = (n_x, n_y, n_z)$ and $\overrightarrow{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$.

The Pauli group $\mathcal{P} := \langle \{\pm 1, \pm i\} \times \{\sigma_0^a, \sigma_1^a, \sigma_2^a, \sigma_3^a\}\rangle$, is the set of all Pauli matrices up to phase factor $\pm 1, \pm i$. We will frequently use the projectors onto the eigenvectors of the Pauli operators. For example,

$$P_{z,\pm}^a = \frac{1 \pm \sigma_z^a}{2} = |\pm, z\rangle^a \langle \pm, z| \tag{2.20}$$

denotes the projector onto the eigenvector $|\pm, z\rangle$ of σ_z^a with eigenvalue ± 1, and similarly for σ_x^a and σ_y^a.

Consider the subset of vertices $A \subset V$, with aim to simplify notations we use sets and subsets as an upper index for states and operators. They denote the respective tensor product of a given state or sets, e.g. $|+\rangle^V = \bigotimes_{v\in V} |+\rangle^v$. Other examples are

$$\mathrm{H}^V = \bigotimes_{v\in V} \mathcal{H}^v \qquad \sigma_z^A = \bigotimes_{a\in A} \sigma_z^a$$
$$\mathrm{P}^V = \bigotimes_{v\in V} \mathcal{P}^v \quad \mathrm{P}_{x,+}^A = \bigotimes_{a\in A} \mathcal{P}_{x,+}^a \equiv |+\rangle^A \langle +|$$

2.4.1 Binary notation

We identify the subset $A \subset V$ with its corresponding binary vector, $A = (A_i)_{i\in V} \simeq (A_1, A_2, \ldots, A_N)$ over the binary field $\mathbb{F}_2^V$ (add multiples modulo 2).

Example: Consider the graph $G = (V, E)$, with set of vertices $V = \{1, 2, 3, 4, \}$. We can use set and binary notation in the same formula $A = \{1, 4\} \simeq (1, 0, 0, 1)$.

These notations allow us to use set and binary operations in the same formula. For example, for $A, B \in \mathcal{P}(V) \simeq \mathbb{F}_2^V$ we will simply write $A \cup B$, $A \cap B$ and $A \setminus B$ for the union, intersection and difference (complement) as well as $A + B$ and $\langle A, B\rangle$ for the addition and the scalar product modulo 2.

Chapter 3

Graph States

3.1 Introduction

A key concept in realizing quantum technologies is the preparation of specific resource states, which then will be used for quantum processing purposes. An important class of such resource states are graph states. These states can be described by a simple undirected and unweighted graph where the vertices correspond to the qubits of the state. Graph states can be regarded as the result of an interaction of particles initially prepared in some product state, however not all interaction patterns can be represented reasonably by a simple graph.

An important feature of graph states is that they can be efficiently described classically. To describe a graph state of n qubits, only $\frac{n(n-1)}{2}$ bits are needed in contrast to the 2^n complex numbers required to describe a general quantum state. It turns out that for graph states, their evolution under Clifford operations and Pauli measurement can be simulated efficiently on a classical computer [32],[17].

Graph states form a family of multiqubit states which includes many popular states such as the Greenberger-Horne-Zeilinger (GHZ) state and the cluster states.

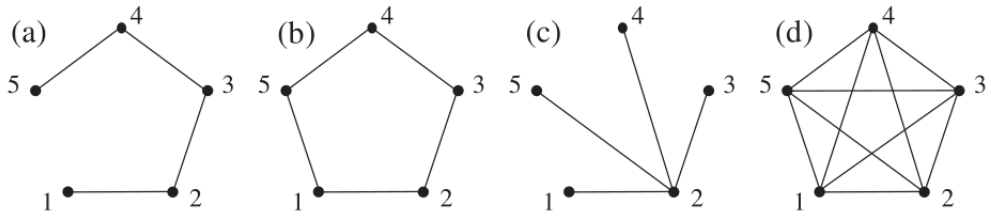

Figure 3.1: Types of graphs for the case of five vertices: (a) The linear cluster graph, (b) the ring cluster graph, (c) the star graph S_5, which describes a GHZ state, and (d) the complete graph K_5. Note that this graph can be obtained from S_5 by local complementation on the second qubit, so it also describes a GHZ state.

Graph states are useful for many applications: in characterization of computational resources in measurement based quantum computing models, in entanglement measurement and purification, in quantum error-correcting codes all codes correspond to graph states, the one-way quantum computation uses graph states as resources.

In the following sections we will see the concept of graph state from two perspectives. First, we will introduce the description of graph states in terms of the interaction pattern and show that such a definition is also meaningful if all particles interact with the same Ising-type interaction. Then, we will see a description in terms of the class of states that correspond to a simple graph and how these states can be described efficiently in terms of their stabilizer, which is a subgroup of the Pauli group. We will explain local unitary equivalence between graph states and discuss the relation to stabilizer states and illustrate an alternative representation of the stabilizer formalism in terms of its binary representation.

3.2 Interaction pattern

Consider a graph $G = (V, E)$ such that asociated with each vertex there is a two-level quantum system or qubit. The qubits are prepared in some initial state vector $|\psi\rangle$ and then they are coupled according to some interaction pattern. For each edge $\{a, b\} \in E$ the qubits of the two adjacent vertices a and b interact according to some (non-local) unitary $U_{ab} = e^{-i\varphi_{ab}H_{ab}}$, where H_{ab} is the interaction Hamiltonian and φ_{ab} is the coupling strength[1]. The most general of such interaction pattern has to be represented by the graph G. Under which conditions can this be completely specified by a simple graph G? For characterizing a large class of interaction patterns, the two–particle unitaries should fulfill the following:

(i) Since the graph G does not provide any ordering of the edges unitaries U_{ab} must commute:

$$[U_{ab}, U_{b,c}] = 0 \quad \forall a, b, c \in V \tag{3.1}$$

(ii) Since we are considering undirected graphs, unitaries U_{ab} must be symmetric:

$$U_{ab} = U_{ba} \quad \forall a, b \in V \tag{3.2}$$

(iii) Since we are considering unweighted graphs, all unitaries U_{ab} are the same for all qubits:

$$U_{ab} = U^{\{a,b\}} \quad \forall a, b \in V \tag{3.3}$$

Proposition 3.2.1 (Ising interactions)**.** *Any interaction pattern in which the qubits interact according to some two–particle unitaries chosen from a set of commuting interactions can alternatively be described by a pure Ising interaction according to the same graph and some local z-rotations*[2] *to be applied before or after the coupling operation.*

$$U^I_{ab}(\varphi_{ab}) := e^{-i\varphi_{ab}\sigma^a_z\sigma^b_z} \tag{3.4}$$

where the interaction Hamiltonian is $H^I_{ab} = \sigma^a_z\sigma^b_z$ and $\sigma^a_x, \sigma^a_y, \sigma^a_z$ are the Pauli matrices acting on qubit a..

Proof. Consider two different unitaries $U = e^{iH}$ and $\tilde{U} = e^{i\tilde{H}}$, where H and $\tilde{H}$ are hermitian operators and two setting of three vertices $a, b, c \in V$. We have that:

$$U_{ab} = U^{\{a,b\}} = \tilde{U}^{\{a,b\}} \text{ and } U_{bc} = U^{\{b,c\}} = \tilde{U}^{\{b,c\}}$$

$$\left[H^{\{a,b\}}, \tilde{H}^{\{b,c\}}\right] = 0 \text{ and } \left[\tilde{H}^{\{a,b\}}, H^{\{b,c\}}\right] = 0$$

We have used the fact that $[f(A), f(B)] = 0$ if and only if $[A, B] = 0$. Every hermitian operator allows for a real decomposition with respect to the basis of Pauli operators $\{\sigma_0, \sigma_x, \sigma_y, \sigma_z\}$, i.e., $H^{a,b} = \sum_{ij} A_{ij}\sigma^a_i\sigma^b_j$. By local unitaries we can diagonalize one of the Hamiltonians, $H^{a,b} = \sum_i A_i\sigma^a_i\sigma^b_i$ and represent the other one with respect to this basis, i.e., $\tilde{H}^{b,c} = \sum_{jk} B_{jk}\sigma^b_j\sigma^c_k$. Therefore we have

$$\sum_{ijk} A_i B_{jk} \sigma^a_i \otimes [\sigma_i, \sigma_j]^b \otimes \sigma^c_k = 0 \tag{3.5}$$

from which it follows:

$$\forall i, j = 1, 2, 3 \text{ with } i \neq j \; : \quad A_i = 0 \vee B_{jk} = 0 \, \forall k = 0, 1, 2, 3 \tag{3.6}$$

If H corresponds to a non-trivial two-body interaction up to a (local) change of basis we can assume that $A_3 \neq 0$. If another component, e.g. $A_2 \neq 0$, then all components in B except B_{00} vanish, and therefore $\tilde{H}$ is a trivial interaction. If instead $A_1 = A_2 = 0$, then at least all components in B apart from B_{00}, B_{03}, B_{30} and B_{33} have to vanish. Any terms due to B_{03} or B_{30} correspond to local z-rotations and all these rotations commute with the Ising interaction terms $H^I_{ab} = \sigma^a_z\sigma^b_z$.

We have shown that this Ising interaction $H^I_{ab} = \sigma^a_z\sigma^b_z$ fulfills conditions (i) and (ii) since it is symmetric. Condition (iii) implies that we have to fix the interaction strenght φ_{ab}. For simple graphs we will choose $\varphi = \frac{\pi}{4}$. □

[1] φ_{ab} can also be understood as the interaction time $\varphi_{ab} = \int_0^t d\tau g_{ab}(\tau)$ in the unitary time-evolution $U_{ab}(\varphi_{ab}) = e^{-\frac{i}{\hbar}\int_0^t d\tau H_{ab}(\tau)}$

[2] $V^\alpha = e^{i\beta_a\sigma^a_z}$

The unitary two-qubit operator U_{ab} is generated by an Ising-type interaction. Consider the interaction Hamiltonian:

$$\begin{aligned} H_{ab} &= \frac{\mathbb{I}-\sigma_z^a}{2} \otimes \frac{\mathbb{I}-\sigma_z^b}{2} = |1\rangle^a \langle 1| \otimes |1\rangle^b \langle 1| \\ &= P_{z,-}^a \otimes P_{z,-}^b = \frac{1}{4}\left(\mathbb{I} - \sigma_z^a - \sigma_z^b + H_{ab}^I\right) \end{aligned} \tag{3.7}$$

It generates the unitary transformation known as controlled phase gate:

$$U_{ab}\left(\varphi_{ab}\right) = e^{-i\varphi_{ab}H_{ab}} \tag{3.8}$$

We find

$$U_{ab}(\varphi_{ab}) = e^{-i\frac{\varphi_{ab}}{4}} e^{i\frac{\varphi_{ab}}{4}\sigma_z^a} e^{i\frac{\varphi_{ab}}{4}\sigma_z^b} e^{-i\frac{\varphi_{ab}}{4}\sigma_z^a\sigma_z^b} \tag{3.9}$$

$$= e^{-i\frac{\varphi_{ab}}{4}} e^{i\frac{\varphi_{ab}}{4}\sigma_z^a} e^{i\frac{\varphi_{ab}}{4}\sigma_z^b} U_{ab}^I\left(\frac{\varphi_{ab}}{4}\right) \tag{3.10}$$

Note that the phase gate corresponds to the Ising intercation up to some additional $\frac{\pi}{4}$-rotations around z-axes at each qubit, and the corresponding interaction strength now is $\varphi_{ab} = \pi$. Thus the control phase gate is generated by Ising interaction with phase $\varphi_{ab} = \pi$.

$$U_{ab}(\pi) = P_{z,+}^a \otimes \mathbb{I}^b + P_{z,-}^a \otimes \sigma_z^b = |0\rangle^a \langle 0| \otimes \mathbb{I}^b + |1\rangle^a \langle 1| \otimes \sigma_z^b \tag{3.11}$$

Proof.

$$\begin{aligned} e^{-i\pi P_{z,-}^a \otimes P_{z,-}^b} &= \sum_{k=0}^{\infty} \frac{(-i\pi)^k}{k!} \left(P_{z,-}^a \otimes P_{z,-}^b\right)^k \\ &= \mathbb{I} + \left(\sum_{k=1}^{\infty} \frac{(-i\pi)^k}{k!}\right) \left(P_{z,-}^a \otimes P_{z,-}^b\right)^k \\ &= \mathbb{I} + \left(e^{-i\pi} - 1\right)^k \left(P_{z,-}^a \otimes P_{z,-}^b\right)^k \\ &= \mathbb{I}^a \otimes \mathbb{I}^b - 2\left(P_{z,-}^a \otimes P_{z,-}^b\right) \\ &= \left(P_{z,+}^a + P_{z,-}^a\right) \otimes \left(P_{z,+}^b + P_{z,-}^b\right) - 2\left(P_{z,-}^a \otimes P_{z,-}^b\right) \\ &= \left(P_{z,+}^a \otimes P_{z,+}^b\right) + \left(P_{z,+}^a \otimes P_{z,-}^b\right) + \left(P_{z,-}^a \otimes P_{z,+}^b\right) - \left(P_{z,-}^a \otimes P_{z,-}^b\right) \\ &= P_{z,+}^a \left(P_{z,+}^b + P_{z,-}^b\right) + P_{z,-}^a \left(P_{z,+}^b - P_{z,-}^b\right) \\ &= P_{z,+}^a \otimes \mathbb{I}^b + P_{z,-}^a \otimes \sigma_z^b = U_{ab} \end{aligned}$$

□

This gate corresponds to a controlled σ_z on qubits a, b, i.e.

$$U_{ab} = |0\rangle \langle 0| \otimes \mathbb{I}^b + |1\rangle^a \langle 1| \otimes \sigma_z^b = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix} \tag{3.12}$$

Remark The phase gate U_{ab} creates and deletes the edge $\{a, b\}$ in a graph G depending on whether the edge is already existing.

Consider the state vector over all vertices $v \in V$:

$$|\psi\rangle = |+\rangle^V = |+\rangle^{v_1} \otimes |+\rangle^{v_2} \cdots \otimes |+\rangle^{v_n} \tag{3.13}$$

If we apply control phase gate U_{ab} on two qubits at vertices a, b with state $|+\rangle$ this ensures that the resulting state vector

$$U_{ab} |+\rangle^a |+\rangle^b = \frac{1}{\sqrt{2}} \left(|0\rangle^a |+\rangle^b + |1\rangle^a |-\rangle^b\right) \tag{3.14}$$

is maximally entangled, i.e. is a Bell state.

Proposition 3.2.2 (Graph States I)**.** *Let $G = (V, E)$ be a simple graph. The graph state $|G\rangle$ associated with G can be written as the pure state:*

$$|G\rangle = \prod_{\{a,b\}\in E} U_{ab} \, |+\rangle^V \tag{3.15}$$

Where U_{ab} is the control phase gate and $|+\rangle^V$ is the initial state. Note that $|+\rangle^V$ can be regarded as the graph state corresponding to the empty graph.

The preparation procedure is as follows:

1. Qubits at each vertex are prepared in the pure state with state vector $|+\rangle$
2. Phase gate U_{ab} is applied to every pair of vertices a, b such that $\{a, b\} \in E$.

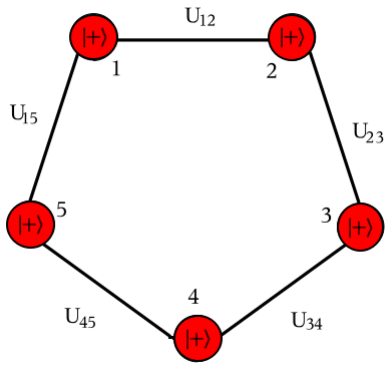

Figure 3.2: Preparation procedure to obtain a graph state that corresponds to a ring graph.

3.3 Stabilizer formalism

Apart from the interaction pattern, graph states can also be defined uniquely in terms of their stabilizer.

Definition 3.1 **Stabilizer subgroup** Consider a group H acting on a set X. For all $x \in X$ the stabilizer subgroup of H with respect to x is defined as the set of elements in H that leave x fixed:

$$\mathcal{S}_x = \{h \in H | h \cdot x = x\} \tag{3.16}$$

Consider two elements $x, y \in X$, and consider the group element h such that $y = h \cdot x$. Then the two stabilizer groups $\mathcal{S}_x$ and $\mathcal{S}_Y$ are related by $\mathcal{S}_y = h \cdot \mathcal{S}_x \cdot h^{-1}$, i.e. the stabilizers of elements in the same orbit are conjugate to each other.

Proof. By definition, $z \in \mathcal{S}_y$ if and only if $z \cdot (h \cdot x) = h \cdot x$. Applying h^{-1} to both sides of this equality yields $(h^{-1} z h) \cdot x = x$; that is, $h^{-1} \cdot z \cdot h \in \mathcal{S}_x$. An opposite inclusion follows similarly by taking $z \in \mathcal{S}_x$ and supposing $x = h^{-1} \cdot y$. □

A subgroup of Pauli matrices $\mathcal{S} \subset \mathcal{P}^V$ is a stabilizer on n qubits if and only if $\mathcal{S}$ is an abelian group which does not include $-\sigma_0^{\otimes n}$. The elements $M_i (i = 1, \ldots, l)$ are called generators of $\mathcal{S}$ if every element $M \in \mathcal{S}$ can be written as a product $M = M_1^{x_1} M_2^{x_2} \cdots M_l^{x_l}$ with $x_i \in \{0, 1\}$. If $l = n$, the elements in $\mathcal{S}$ will have only one common eigenvector with eigenvalue 1. We call this unique common eigenvector as stabilizer state.

Then, a stabilizer state $|S\rangle$ is the unique normalized state satisfying $M |S\rangle = |S\rangle$ for every $M \in \mathcal{S}$. It is easy to see that the density matrix of a stabilizer state $|S\rangle$ is

$$\rho_{\mathcal{S}} = |S\rangle \langle S| = \frac{1}{2^n} \sum_{M\in\mathcal{S}} M \tag{3.17}$$

Proposition 3.3.1 (Graph States II). *Let $G = (V, E)$ be a simple graph. The graph state $|G\rangle \in \mathcal{H}^V$ corresponding to G is the unique common eigenstate of a set of $N = |V|$ commuting observables*

$$K_a = \sigma_x^a \sigma_z^{N_a} = \sigma_x^a \prod_{b \in N_a} \sigma_z^b \quad a = 1, 2, \dots N \tag{3.18}$$

where $\sigma_x^a, \sigma_y^a, \sigma_z^a$ are the Pauli matrices acting on qubit a and N_a is the neighborhood of qubit a.

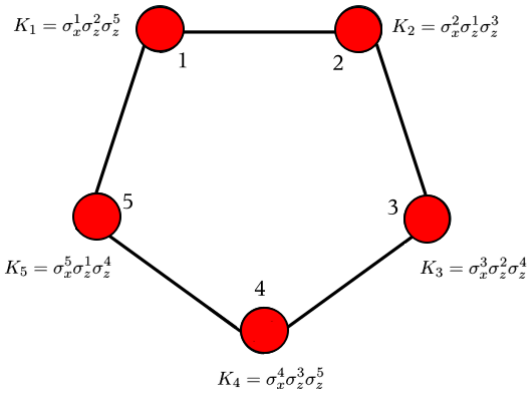

Figure 3.3: The stabilizing operator K_a for a ring graph state of 5 vertices.

The eigenvalues of the stabilizing operators K_a are $+1$ $\forall a \in V$, that is the graph state $|G\rangle$ associated with the graph G fulfills

$$K_a |G\rangle = |G\rangle, \forall a \in V \tag{3.19}$$

The stabilizer group of a graph state $|G\rangle$ is the abelian subgroup $\mathcal{S}$ of Pauli group $\mathcal{P}^V$ that is generated by the set $\{K_a | a \in V\}$.

Proof. Consider the initial state $|+\rangle^V$, with no correlations. The eigenvalues of $|+\rangle^V$ are $\sigma_x^a |+\rangle^V = |+\rangle^V, \forall a \in V$. We consider the vertix $a \in V$, choose $b \in N_a$ and compute theconjugation of σ_x^a with U_{ab}.

$$\begin{aligned} U_{ab} \sigma_x^a U_{ab}^\dagger &= \left(|0\rangle^a \langle 0| \otimes \mathbb{I}^b + |1\rangle^a \langle 1| \otimes \sigma_z^b\right) \sigma_x^a \left(|0\rangle^a \langle 0| \otimes \mathbb{I}^b + |1\rangle^a \langle 1| \otimes \sigma_z^b\right) && (3.20) \\ &= \sigma_x^a \left(|1\rangle^a \langle 1| \otimes \mathbb{I}^b + |0\rangle^a \langle 0| \otimes \sigma_z^b\right) \left(|1\rangle^a \langle 1| \otimes \mathbb{I}^b + |0\rangle^a \langle 0| \otimes \sigma_z^b\right) && (3.21) \\ &= \sigma_x^a \left(0 + |0\rangle^a \langle 0| \otimes \sigma_z^b + |1\rangle^a \langle 1| \otimes \sigma_z^b + 0\right) && (3.22) \\ &= \sigma_x^a \sigma_z^b && (3.23) \end{aligned}$$

If we iterate with all neighbors of a we get:

$$\left(\prod_{b \in N_a} U_{ab}\right) \sigma_x^a \left(\prod_{b \in N_a} U_{ab}^\dagger\right) = \sigma_x^a \prod_{b \in N_a} \sigma_z^b = \sigma_x^a \sigma_z^{N_a} = K_a \tag{3.24}$$

Now consider the eigenvalues equation $\sigma_x^a |+\rangle^V = |+\rangle^V, \forall a \in V$.

$$\left(\prod_{\{a,b\} \in E} U_{ab}\right) \sigma_x^a \left(\prod_{\{a,b\} \in E} U_{ab}^\dagger\right) \left(\prod_{\{a,b\} \in E} U_{ab}\right) |+\rangle^V = \left(\prod_{\{a,b\} \in E} U_{ab}\right) |+\rangle^V \tag{3.25}$$

Since $\left(\prod_{\{a,b\} \in E} U_{ab}\right) \sigma_x^a \left(\prod_{\{a,b\} \in E} U_{ab}^\dagger\right) = K_a$. If the edges are not in the neighborhood they are in different Hilbert spaces, other U_{cb} with $c \neq a$ can be pulled through σ_x^a.

$$K_a \left(\prod_{\{a,b\} \in E} U_{ab}\right) |+\rangle^V = \left(\prod_{\{a,b\} \in E} U_{ab}\right) |+\rangle^V, \forall a \in V \tag{3.26}$$

$$\left(\prod_{\{a,b\}\in E} U_{ab}\right)|+\rangle^V = |G\rangle \tag{3.27}$$

□

The stabilizing operator $K_a = \sigma_x^a \sigma_z^{N_a}$ gives rise to a measurement pattern of the vertices of the graph, the qubit at vertex a is measured in x-direction and the vertices b in N_b in z-direction. Physically, the generators K_a describe the perfect correlations in the state $|G\rangle$, since $\langle G|K_a|G\rangle = \langle \sigma_x^a \prod_{b\in N_a} \sigma_z^b\rangle = 1$. Then K_a provides constraints to the correlations between the measurement outcomes $m_x^a = \pm 1$ and $m_z^b = \pm 1$, namely

$$m_x^a \prod_{b\in N_a} m_z^b = 1 \tag{3.28}$$

3.3.1 Graph state basis

For each $|G\rangle$ associated with the graph G we have 2^{N-1} states with similar properties in $\mathcal{H}^V$. Consider the subset of vertices $W \subset V$ defined by:

$$|W\rangle = \sigma_z^W |G\rangle \equiv \prod_{\sigma_z^a} |G\rangle \tag{3.29}$$

The states $|W\rangle$ are eigenstates of the correlation operator K_a with different eigenvalues W_a and satisfy:

$$K_a |W\rangle = (-1)^{\delta_W(a)} |W\rangle \equiv (-1)^{W_a} |W\rangle \tag{3.30}$$

where $\delta_W(a) = \left\{ \begin{array}{cc} 1 & a \in W \\ 0 & otherwise \end{array} \right\} = W_a$ and that introduces the binary vector $w = (w_1, w_2 \dots w_N)$ associated with set W.

Proof.

$$K_a |W\rangle = K_a \prod_{b\in W} \sigma_z^b |G\rangle = (-1)^{\delta_w(a)} \prod_{b\in W} \sigma_z^b K_a |G\rangle$$

We know that $K_a |G\rangle = |G\rangle$ and $\prod_{b\in W} |G\rangle = |W\rangle$. Then,

$$K_a |W\rangle = (-1)^{\delta_w(a)} |W\rangle \ \ \forall a \in V \tag{3.31}$$

□

The set $\{|W\rangle = \sigma_z^W |G\rangle | w \subseteq V\}$ forms a basis of $\mathcal{H}^V = (\mathbb{C}^2)^V$ with completeness relation $\sum_{W\subset V} |W\rangle\langle W| = \mathbb{I}^V$.

For two different subsets $W, W' \subseteq V$ the states $|W\rangle$, $|W'\rangle$ have list of eigenvalues $(w_1, \dots, w_N)$ and $(w'_1, \dots, w'_N)$ which differ in at least one item, that is $\exists\ a \in V | w_a \neq w'_a$. This implies $\langle w|w'\rangle = \delta_{ww'}$, with $\{K_a | a \in V\}$ is a set of commuting observables. There are 2^N differents subsets $W \subseteq V$, therefore there exist 2^N pair-wise orthogonal eigenstates $|W\rangle$ and $\{|W\rangle | W \subseteq V\}$ form a basis of $\mathcal{H}^V$.

The proyector onto a graph state has a direct representation in terms of the corresponding stabilizer $\mathcal{S}$:

$$|G\rangle\langle G| = \frac{1}{2^N} \sum_{\sigma\in\mathcal{S}} \sigma \tag{3.32}$$

where

$$\{K_1^{s_1}, K_2^{s_2} \dots K_N^{s_N} | (s_1, \dots, s_N) \in \{0,1\}^N\} = \mathcal{S} \tag{3.33}$$

Proof. First, we consider the right-hand side of Equation 3.32.

$$\langle W|rhs|W'\rangle = \frac{1}{2^N} \sum_{\sigma\in S} \langle W|\sigma|W'\rangle = \frac{1}{2^N} \sum_{s_1,\dots,s_N=0}^{1} \langle W|K_1^{s_1}, K_2^{s_2} \dots K_N^{s_N}|W'\rangle \tag{3.34}$$

We know that $\langle W| = \langle G|\, \sigma_z^W$ and $|W'\rangle = \sigma_z^{W'}\, |G\rangle$. Besides, pulling the Ks through gets a sign ± 1.

$$\langle G|\sigma_z^W K_1^{s_1}, K_2^{s_2} \dots K_N^{s_N} \sigma_z^{W'}|G\rangle = (-1)^{\delta_w(1)s_1} \dots (-1)^{\delta_w(N)s_N} \langle G|\sigma_z^W \sigma_z^{W'}|G\rangle \tag{3.35}$$

$$= (-1)^{\delta_w(1)s_1} \dots (-1)^{\delta_w(N)s_N} \langle W|W'\rangle$$

$$= (-1)^{\sum_{a\in W} s_a} \delta_{WW'} \tag{3.36}$$

Therefore, for $|V| = N$ and $|W| = M$ $M \leq N$,

$$\langle W\,|G\rangle\, \langle G|\, W'\rangle = \frac{1}{2^N} \sum_{s_{M+1},\dots,s_N=0}^{1} \left(\sum_{s_1,\dots,s_M}^{1} (-1)^{\sum_{a\in W} s_a} \right) \delta_{WW'} \tag{3.37}$$

For $W \neq \emptyset$ there are $2^{|W|} - 1$ asignements for $\{s_a | a \in W\}$ with $\sum_{a\in W} s_a =$ even and same number with $\sum_{a\in W} s_a =$ odd. Then,

$$\sum_{s_1,\dots,s_M}^{1} (-1)^{\sum_{a\in W} s_a} = \begin{cases} 0 & W \neq \emptyset \\ 2^M & W = \emptyset \end{cases} \tag{3.38}$$

$$\frac{1}{2^N} 2^{N-M} 2^M \delta_{WW'} \delta_{W\emptyset} = \delta_{WW'} \delta_{W\emptyset} \;\forall W, W' \tag{3.39}$$

Now we consider the left-hand side of Equation 3.32.

$$\langle W|lhs|W'\rangle = \langle W|G\rangle\, \langle G|W'\rangle = \delta_{W\emptyset} \delta_{W'\emptyset} \;\forall W, W' \tag{3.40}$$

□

3.3.2 Binary representation

We now briefly review an alternative representation of the stabilizer formalism in terms of its binary representation, which allows one to treat the properties of the stabilizer in terms of a symplectic subspace of the vector space $\mathbb{F}_2^{2N}$. A more detailed description of binary representation can be found in [18],[16].

Every element of the Pauli group $U \in \mathcal{P}^V$ can be written uniquely, up to a phase factor, in form:

$$U = \sigma_x^{\mathbf{U}_x} \sigma_z^{\mathbf{U}_z} = \prod_{a\in V} \sigma_x^{U_x^a} \prod_{a\in V} \sigma_z^{U_z^a} \tag{3.41}$$

with $U_x^a, U_z^a \in \{0, 1\}$ for every $a \in V$

Therefore, we can introduce a mapping denoted by $\mathcal{B}$ which maps the elements of $\mathcal{P}^V$ to a $2N$-dimensional binary vectors as follows:

$$\mathcal{B} : U = \sigma_x^{U_x} \sigma_z^{U_z} \to (U_x|U_z) \in \mathbb{F}_2^{2N} \tag{3.42}$$

For single qubits this is

$$\sigma_0 \to (0|0) \quad \sigma_x \to (1|0)$$
$$\sigma_y \to (1|1) \quad \sigma_z \to (0|1)$$

and for example the correlation operator K_1 in Figure 3.3 has the binary representation

$$K_1 = \sigma_x^1 \sigma_z^2 \sigma_z^5 \to (10000|01001)$$

The binary representation has the following two important properties: letting $u, w, x \in \mathcal{P}^V$ with corresponding binary vectors $\mathbf{U}, \mathbf{V}, \mathbf{X} \in \mathbb{F}_2^{2N}$, one finds that:

(i) $u\ w \sim x \quad \longleftrightarrow \quad \mathbf{U} + \mathbf{W} = \mathbf{X} \pmod 2$

(ii) $[u, w] = 0 \quad \longleftrightarrow \quad \mathbf{U}^T \mathbf{P} \mathbf{W} = 0 \pmod 2$

where $\sim$ denotes equality up to a global phase factor and matrix $\mathbf{P}$ written

$$\mathbf{P} = \left(\begin{array}{c|c} 0 & 1 \\ \hline 1 & 0 \end{array}\right)$$

defines the symplectic inner profuct on the binary space $\mathbb{F}_2^{2N}$. From property (i) it follows that the mappin $\mathcal{B}$ is a homomorphism of groups and property (ii) shows that two Pauli operators commute if and only if the corresponding binary vectors are orthogonal with respect to the symplectic inner product.

Consider the stabilizer state $|S\rangle$,i.e. $M|S\rangle = |S\rangle$, $\forall M \in \mathcal{S}$. The correlation operators can be written in binary representaion as follows:

$$S_1 = \sigma_x^{x_1}\sigma_z^{z_1} \to (x_1|z_1) \in \mathbb{F}_2^{2N} \tag{3.43}$$

$$\vdots$$

$$S_N = \sigma_x^{x_N}\sigma_z^{z_N} \to (x_N|z_N) \in \mathbb{F}_2^{2N} \tag{3.44}$$

We can summarize this in terms of a generator matrix $(\mathbf{X}|\mathbf{Z})$ where $\mathbf{X}$ and $\mathbf{Z}$ are $N \times N$ matrices, which is a full rank $2N \times N$. A generator matrix is obtained by assembling all binary representations of a set of independent stabilizer generators as the rows of the matrix.

$$\mathbf{X} = \begin{pmatrix} x_1 \\ \vdots \\ x_N \end{pmatrix} \quad \mathbf{Z} = \begin{pmatrix} z_1 \\ \vdots \\ z_N \end{pmatrix}$$

The generator matrix for graph state $|G\rangle$ has a normal form:

$$(\mathbf{X}|\mathbf{Z}) = (\mathbb{I} \mid \Gamma) \tag{3.45}$$

where Γ is the adjacent matrix of graph G.

Example: GHZ state for three particles $|\phi\rangle_{123} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$.

$$S_1 = x_1x_2x_3 \to (111|000)$$

$$S_2 = z_1z_2 \to (000|110)$$

$$S_3 = z_2z_3 \to (000|011)$$

So the generator matriz for GHZ state is

$$(\mathbf{X}|\mathbf{Z}) = \left(\begin{array}{ccc|ccc} 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right)$$

3.4 Equivalent graph states

Through definitions, each graph G uniquely specifies a graph state $|G\rangle$ and viceversa. In other words, two different graphs $G = (V, E)$ and $G' = (V, E')$ cannot describe the same graph state.

Proof. Suppose $\exists G = (V, E), G' = (V, E')$ with $E \neq E'$and $|G\rangle = |G'\rangle$.

$$|G\rangle = |G'\rangle \to \prod_{\{a,b\}\in E} U_{ab}|+\rangle^V = \prod_{\{a,b\}\in E'} U_{ab}|+\rangle^V \tag{3.46}$$

$$U_{ab} = U_{ab}^{-1} \to |+\rangle^V = \prod_{\{a,b\}\in E+E'} U_{ab} \tag{3.47}$$

Then $E + E' = \emptyset \to E = E' \to$ Contradicction □

On the other hand, two differents graphs $G = (V, E), G' = (V, E')$ can describe two graph states $|G\rangle \neq |G'\rangle$ that are identical up to same local unitary transformations $U = U_1, U_2, \ldots, U_N \in U^N(2)$. We say two graphs $G = (V, E), G' = (V, E')$ are LU-equivalent and we write $|G'\rangle \simeq_{LU} |G\rangle$ if there exists a local unitary $U \in \mathbf{U}(2)^V$ such that

$$|G'\rangle = U|G\rangle \tag{3.48}$$

Suppose that $\mathcal{S}$ is the stabilizer subgroup of $|G\rangle$, i.e. $s\,|G\rangle = |G\rangle\,\forall s \in \mathcal{S}$ and $|G'\rangle = U\,|G\rangle$. Then denoting,

$$\sum{}' = U\mathcal{S}U^\dagger = \{UsU^\dagger | s \in \mathcal{S}\} \tag{3.49}$$

we find that $s'\,|G'\rangle = |G'\rangle$ for all $s' \in \sum'$. In this sense the group $\sum'$ is a stabilizing subgroup of the state vector $|G'\rangle$, however in general (for general U) s' is not the tensor product of Pauli group, that is $\sum'$ is not a subgroup of Pauli group $\mathcal{P}^V$. But for certain U, $\sum' \in \mathcal{P}^V$.

3.4.1 Local Clifford operations

We now look for local unitaries $U \in \mathbf{U}^V(2)$, for which $U\mathcal{P}^V U^\dagger = \mathcal{P}^V$, meaning that U maps the whole Pauli group $\mathcal{P}^V$ onto itself under conjugation. The set of unitaries

$$\mathcal{C}_1^V := \{U \in \mathbf{U}^V(2) | U\mathcal{P}^V U^\dagger = \mathcal{P}^V\} \tag{3.50}$$

is a group and it is called local Clifford group of $N = |V|$ qubits. If $|G\rangle$ and $|G'\rangle$ are graph states and $|G'\rangle = U\,|G\rangle$ for $U \in \mathcal{C}_1^V$ then $\sum' = UsU^\dagger = s'$ is the stabilizer of $|G'\rangle$.

Therefore, local Clifford operations on graph states can entirely be described within the stabilizer formalism – and this is one of the main reasons why the local Clifford group is of central importance in the context of graph states. We will say two graph states $|G\rangle$ and $|G'\rangle$ are LC-equivalent, and we write $|G\rangle \simeq_{LC} |G'\rangle$, if and only if $\exists\, U \in \mathcal{C}_1^V$ such that $|G'\rangle = U\,|G\rangle$.

The Local Clifford group $\mathcal{C}_1^V := \mathcal{C}_1^{\otimes V}$ on N qubits is the N-fold tensor product of $\mathcal{C}_1$ with itself. The one-qubit Clifford group $\mathcal{C}_1$ is the normalizer of $\mathcal{P}_1$ in $\mathbf{U}(2)$, i.e. it is the subgroup of 2×2 unitary operators which map $\mathcal{P}_1$ to itself under conjugation. It is defined by

$$\mathcal{C}_1 = \{U \in U(2) | UPU^\dagger = P\} = \langle H, S\rangle \tag{3.51}$$

where the set of 2×2 unitary operators $\{H, S\}$ is the generator of the group, up to a global phase factor.

(i) H corresponds to Hadamard gate and generates rotations around 45° axis in xy, xz, yz plane with angle π.

$$H = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \tag{3.52}$$

(ii) S corresponds to single-qubit phase gate and generates rotations around x, y, z with angle $\frac{\pi}{2}$.

$$S = \sqrt{\sigma_z} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix} \tag{3.53}$$

We can see intuitively the action of the two single-qubit gates H and S looking at the Bloch sphere in Figure 3.4, where it is represented the pure state of a two-level quantum system $\rho = \frac{1}{2}(\mathbb{I} + \vec{s}\hat{\vec{\sigma}})$.

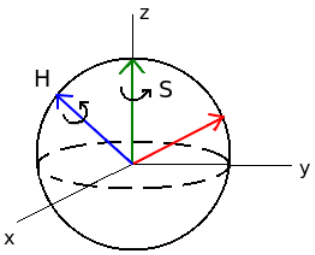

Figure 3.4: Bloch sphere and representation of H and S operators.

The action of the Clifford group $\mathcal{C}_1$ under conjugation permutes the Pauli matrices $\sigma_x, \sigma_y, \sigma_z$ up to a phase factor ± 1.

Examples: $H\sigma_z H^\dagger = \sigma_x$, $H\sigma_x H^\dagger = \sigma_z$, $S\sigma_x S^\dagger = \sigma_y$, $S\sigma_y S^\dagger = -\sigma_x$

Proof. First, note that matrices $\pm\sigma_0$ and $\pm i\sigma_0$ are left unchanged under conjugation. The set $\{\pm\sigma_x, \pm\sigma_y, \pm\sigma_z\}$ has to be mapped onto itself, since $U\sigma_i U^\dagger$ is herminitian if and only if σ_i is hermitian. Because the conjugation is invertible, it permutes the matrices $\sigma_x, \sigma_y, \sigma_z$ up to some sign $\pm$. □

Up to overall phase factors, the one-qubit Clifford group C_1 has finite cardinality $|C_1 \backslash \{e^{i\varphi} | \varphi \in [0, 2\pi]\}| = 24$. Ref. [18] presents all 24 single-qubit Clifford unitaries and their decomposition in terms of Pauli operators and $\frac{\pi}{2}$-rotations. Consider the $\frac{\pi}{2}$-rotation, i.e. rotation $e^{-i\frac{\alpha}{2}\vec{n}\vec{\sigma}}$ with rotation angle $\alpha = \frac{\pi}{2}$ around $\vec{n}$ axis.

$$\sqrt{\pm i\sigma_h} = e^{\pm i\frac{\pi}{4}\sigma_h} \ , h = 1, 2, 3 \tag{3.54}$$

These rotations lead to elementary permutations, i.e. permutations of only two indices:

$$\{1,2,3\} \xrightarrow{\sqrt{\pm i\sigma_1}} \{1,3,2\}$$

$$\{1,2,3\} \xrightarrow{\sqrt{\pm i\sigma_2}} \{3,2,1\}$$

$$\{1,2,3\} \xrightarrow{\sqrt{\pm i\sigma_3}} \{2,1,3\}$$

Instead of H and S any two of these elementary permutations can be used to generate the Clifford group $\mathcal{C}_1$.

Proof. We execute the explicit computation. For σ_z we have

$$\sqrt{\pm i\sigma_z} = e^{\pm i\frac{\pi}{4}\sigma_z} = \cos\frac{\pi}{4}\mathbb{I} \pm i\sin\frac{\pi}{4}\sigma_z = \frac{1}{\sqrt{2}}(\mathbb{I} \pm i\sigma_z) \tag{3.55}$$

And similar for σ_x and σ_y. Therefore, $\sqrt{\pm i\sigma_i}$ for $i = 1, 2, 3$ is equivalent to the $\pm\frac{\pi}{2}$-rotation around x, y, z axis. Now, we do the following calculations.

$$\sigma_z\sqrt{+\sigma_y} = \sigma_z\frac{1}{\sqrt{2}}(\mathbb{I} + i\sigma_y) = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) = H \equiv H_{xz} \tag{3.56}$$

$$\sigma_x\sqrt{+\sigma_z} = \sigma_x\frac{1}{\sqrt{2}}(\mathbb{I} + i\sigma_z) = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_y) = H_{xy} \tag{3.57}$$

$$\sigma_x\sqrt{-\sigma_y} = \sigma_x\frac{1}{\sqrt{2}}(\mathbb{I} - i\sigma_y) = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) = H_{xz} \tag{3.58}$$

$$\sigma_x\sqrt{+\sigma_y} = \sigma_x\frac{1}{\sqrt{2}}(\mathbb{I} + i\sigma_y) = \frac{1}{\sqrt{2}}(\sigma_x - \sigma_z) = \vec{H_{xz}} \tag{3.59}$$

So, these give rise to the rotations arround 45° axes. □

In conclusion, these operations generate all permutations and for that reason we can consider only operators H and $\sqrt{i\sigma_z}$ as generators of Clifford group.

$$\begin{aligned}
\sqrt{i\sigma_z}\sqrt{i\sigma_z} &= i\sigma_z \\
H\sigma_z H &= \sigma_x \\
H\sqrt{i\sigma_z}H &= \sqrt{i\sigma_x} \\
i\sigma_x\sigma_z &= \sigma_y \\
\sigma_z H = \sigma_z\frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) &= \frac{1}{\sqrt{2}}(\mathbb{I} + i\sigma_y) = \sqrt{i\sigma_y}
\end{aligned}$$

For a graph with $N = |V|$ vertices, we have 24^N different Clifford unitaries that generate its Clifford orbit. To decide whether two graph states are LC equivalent seem to be exponencially difficult, but there is in fact a polynomical method to calculate them.

Definition 3.2 **Clifford group** The Clifford group (on N qubits) is the group of all unitary operators that map the Pauli group to itself under conjugation.

$$\mathcal{C}_N := \{U \in \mathbf{U}(2^N) | U\mathcal{P}^V U^\dagger = \mathcal{P}^V\} \tag{3.60}$$

By definition, Clifford operations map stabilizer states to stabilizer states. Any Clifford operation U can be decomposed, up to a global phase factor, into a sequence of $\mathcal{O}(N^2)$ one- and two-qubit

gates in the set of generators $\langle H, S, CNOT\rangle$, where H and S are defined as before and $CNOT$ is the controlled-NOT gate

$$CNOT^{ab} = |0\rangle^a \langle 0| \otimes \mathbb{I}^b + |1\rangle^a \langle 1| \otimes \sigma_x^b = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

3.4.2 LC-Rule

As we have seen previuosly, local Clifford operations on graph states can entirely be described within the stabilizer formalism. Let us consider the following sequence of single-qubit Clifford operations:

$$U_a^\tau(G) = e^{-i\frac{\pi}{4}\sigma_x^a} \prod_{b\in N_a} e^{i\frac{\pi}{4}\sigma_z^b} \propto \sqrt{K_a} \tag{3.61}$$

The action of local Clifford operations on graph states can be described in terms of a simple graph transformation rule, called local complementation, defined in 2.3.1 in page 8.

Proposition 3.4.1 (LC-rule)**.** *By local complementation of a graph $|G\rangle$ at some vertex $a \in V$ one obtains a LC-equivalent graph state:*

$$|\tau_a(G)\rangle = U_a^\tau(G)\,|G\rangle \tag{3.62}$$

where τ_a is a local complementation on vertex a and $U_a^\tau(G)$ is a local Clifford unitary defined in Equation 3.61. Therefore, operation $U_a^\tau(G)$ on graph state $|G\rangle$ can be seen as an operation τ_a on the graph G.

Two graph states $|G\rangle$,$|G'\rangle$ are LC-equivalent if and only if the corresponding graph are related by a sequence of local complementation. That is

$$G' = \tau_{a_N} \cdot \tau_{a_{N-1}} \cdots \tau_{a_1}(G) \text{ with } \; a_1 \ldots a_N \in V \tag{3.63}$$

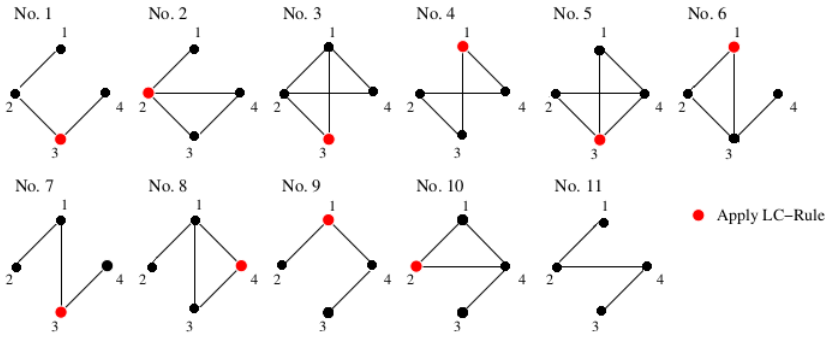

Figure 3.5: Example for a succesive application of LC-rule, which exhibits the whole equivalence class associated with graph No.1.

Proof. Consider a graph G, with the corresponding graph state $|G\rangle$ and correlation operator $K_b\,|G\rangle = |G\rangle \quad \forall b \in V$ and the graph obtained from local complementation at vertex a $G' := \tau_a(G)$ with correlation operator $K_b'\,|G'\rangle = |G'\rangle \quad \forall b \in V$. For $c \in V \backslash N_a$, we have that

$$U_a^\tau K_c (U_a^\tau)^\dagger = K_c = K_c^{'} \tag{3.64}$$

For $b \in N_a$ we find that

$$U_a^\tau K_b (U_a^\tau)^\dagger = \left(\sqrt{-i\sigma_x^a} \prod_{a'\in N_a} \sqrt{+i\sigma_z^{a'}}\right) \sigma_x^b \prod_{b'\in N_b} \sigma_z^{b'} \left(\sqrt{+i\sigma_x^a} \prod_{a'\in N_a} \sqrt{-i\sigma_z^{a'}}\right) \tag{3.65}$$

$$= \sqrt{-i\sigma_x^a}\sqrt{i\sigma_z^{N_a}}\sigma_x^b\sigma_z^{N_b}\sqrt{i\sigma_x^a}\sqrt{-i\sigma_z^{N_a}} \tag{3.66}$$

We can pull $\sqrt{i\sigma_x^a}$ in second place in the above equation and the only change could be just a phase ($\pm i$), but we have to be careful because a is in the neighborhood of b, so there is a σ_z which not commute. We can rewrite a few terms, $\sigma_z^{N_b} = \sigma_z^{N_b \setminus a}\sigma_z^a$ and $\sqrt{-i\sigma_z^{N_a}} = \sqrt{\sigma_z^{N_a \setminus b}}\sqrt{-i\sigma_z^b}$. Then, pulling $\sqrt{i\sigma_x^a}$ in second place changes $i \to -i$, and pulling $\sqrt{-i\sigma_z^b}$ in second place changes $-i \to i$. This gives us the following:

$$(-i\sigma_x^a)(i\sigma_z^b)(\sigma_x^b)(\sigma_z^{N_b}) = \sigma_x^a\sigma_z^b\sigma_x^b\sigma_z^{N_b} \tag{3.67}$$

We can rewrite the term $\sigma_z^b = \sigma_z^{N_a}\sigma_z^{N_a \setminus b}$.

$$\sigma_x^a\sigma_z^{N_a}\sigma_z^{N_a \setminus b}\sigma_x^b\sigma_z^{N_b} = \sigma_x^a\sigma_z^{N_a} \cdot \sigma_x^b(\sigma_z^{(N_b + N_a \setminus b)}) \tag{3.68}$$

$$\sigma_x^a\sigma_z^{N_a} \cdot \sigma_x^b\sigma_z^{b'} = K_a' \cdot K_b' \tag{3.69}$$

The stabilizer $U_a^\tau \mathcal{S}(U_a^\tau)^\dagger$ of the state $U_a^\tau |G\rangle$ is thus generated by:

$$\{K_c'\}_{c \in V \setminus N_a} \cup \{K_a'K_b'\}_{b \in N_a} \tag{3.70}$$

By multiplying $K_a'K_b'$ with K_a', one obtain a new generate set.

$$\{K_c'\}_{c \in V \setminus N_a} \cup \{K_b'\}_{b \in N_a} = \{K_a'\}_{a \in V} \tag{3.71}$$

$$\Rightarrow K_a' |G\rangle = |G'\rangle \quad \forall a \in V \tag{3.72}$$

This proves that by using the LC rule we obtain, standing from a given state, a sequence of Local Clifford equivalents graph states. □

Proposition 3.4.2 (Stabilizer states)**.** *Any stabilizer state vector $|S\rangle$ is LC-equivalent to some graph state vector $|G\rangle$, i.e., $|S\rangle = U|G\rangle$ for some LC-unitary $U \in \mathcal{C}^V$. This unitary can be calculated efficiently.*

The proof of 3.4.2 can be found in [16] in terms of binary description.

3.5 Measurements on graph states

3.5.1 Local Pauli measurements

The exact form of Local Pauli measurements can be found in [15] but we will only focus on the results of the measurements over graph state $|G\rangle$.

Proposition 3.5.1 (Local Pauli measurements)**.** *A projective measurement of $\sigma_x, \sigma_y, \sigma_z$ on qubit associated with a vertex $a \in G$ yields, up to local unitaries $U_{i,\pm}^a$ a new graph state $|G'\rangle$ on the remaining vertices. The resulting graph G' is*

$$P_{z,\pm}^a |G\rangle = \frac{1}{\sqrt{2}} |z, \pm\rangle^a \otimes U_{z,\pm}^a |G \setminus a\rangle \tag{3.73}$$

$$P_{y,\pm}^a |G\rangle = \frac{1}{\sqrt{2}} |y, \pm\rangle^a \otimes U_{y,\pm}^a |\tau_a(G) \setminus a\rangle \tag{3.74}$$

$$P_{x,\pm}^a |G\rangle = \frac{1}{\sqrt{2}} |x, \pm\rangle^a \otimes U_{x,\pm}^a |\tau_b(\tau_a \circ \tau_b(G) \setminus a)\rangle \tag{3.75}$$

for $b \in N_a$. The local unitaries $U_{i,\pm}^a$ are given by:

$$U_{z,+}^a = \mathbb{I}^a \qquad U_{z,-}^a = \sigma_z^{N_a}$$
$$U_{y,+}^a = \sqrt{-i\sigma_z^{N_a}} \qquad U_{y,-}^a = \sqrt{+i\sigma_z^{N_a}}$$
$$U_{x,+}^a = \sqrt{+i\sigma_y^b}\sigma_z^{N_a \setminus (b \cup N_b)} \qquad U_{x,-}^a = \sqrt{-i\sigma_y^b}\sigma_z^{N_b \setminus (a \cup N_a)}$$

For a sequence of local Pauli measurements, the local unitaries have to be taken into account if the graph state is unitarily transformed. A table with relevant commutation relations for Pauli projections and Clifford operations can be found in [15].

Consider a Pauli measurement $\sigma_x, \sigma_{y,z}$ at a single vertex a of a graph state $|G\rangle$. Notice that the resulting graph state $|G'\rangle$ can be obtained from the initial graph G: a σ_z-measurement is equivalent to deleting vertex a from G, a σ_y-measurement is equivalent to replacing the subgraph $G[N_a]$ by its complement and deleting vertex a, and a σ_x-measurement is equivalent to replacing the subgraph $G[N_b]$, for any $b \in N_a$, by its complement, applying the rule for σ_y and replacing $G[N_b]$ by its complement again.

3.5.2 Clifford operations

Clifford group are Clifford unitaries $U \in \mathcal{C}_N$ and Pauli measurements. Since it is possible to efficiently decompose an arbitrary Clifford unitary in terms of the one-qubit gates H, S and two-qubit gate $CNOT$ (see definition 10), any Clifford operation can be simulated by a sequence of at most $\mathcal{O}(N^2)$ of these gates together with one Pauli measurement at a single vertex. Therefore, any Clifford operation can be efficiently simulated on a classical computer on polynomial time [32].

Proposition 3.5.2 ((Gottesman–Knill theorem)**.** *Any stabilizer circuit on a quantum register of N qubits, which consists of M steps, can be simulated on a classical computer using at most $\mathcal{O}(N^3M)$ elementary classical operations.*

Indeed it has been shown that such classical simulator actually requires only $\mathcal{O}(N^2)$ elementary operations on classical computer. The Clifford group plays a crucial role in entanglement purification protocols and quantum error correcting codes, as many of them contain Clifford gates.

3.5.3 Connecting graph states

Two graph states can be connected by appling two different methods, one where the two connection qubits are merged into one, and one where they are both projected out. Consider two graphs states $|G\rangle, |G'\rangle$ with set of vertices V, V' respectively. Let $a \in V$ and $b \in V'$ be two qubits corresponding to vertices of the two graph states.

- *Connection 1.* We apply $CNOT$ operation between qubits a, b, $CNOT^{a\to b} = |0\rangle^a \langle 0| \otimes \mathbb{I}^b + |1\rangle^a \langle 1| \otimes \sigma_x^b$, followed by a σ_z-measurement on qubit b. The resulting state is a graph state (up to local Clifford unitaries) that corresponds to a graph without vertex b (since we measured in z-basis) and the neighborhood of a is given by $\tilde{N_a} = N_a \cup N_b - N_a \cap N_b$.

- *Connection 2.* We apply local complementation τ on both qubits a, b obtaining graphs $\tau_a(G)$ and $\tau_b(G')$. Then we apply $CNOT^{a\to b}$ followed by a σ_z-measurement on qubit b and σ_y-measurement on qubit a. he resulting state is a graph state (up to local Clifford unitaries) that corresponds to a graph without vertices a and b and edges according to $\tilde{N_i} = N_i \cup N_b - N_i \cap N_b$ for all $i \in N_a$ and $\tilde{N_j} = N_j \cup N_a - N_j \cap N_a$ for all $j \in N_b$.

Chapter 4

Quantum Entanglement

Formally, we say a quantum state is entangled if it is not classically correlated, and classically correlated means that it can be prepared using physical devices locally, where all correlations are due to shared classical randomness. In contrast entangled states cannot be prepared using local physical devices alone. Correlations in classical systems can always be described in terms of classical probabilities; this is not always true in quantum systems, entanglement is a unique phenomenon of quantum mechanics.

Composite quantum systems are systems that naturally decompose into two or more subsystems, where each subsystem itself is a proper quantum system. The Hilbert space associated with a composite, or multipartite system, is given by the tensor product $\mathcal{H} = \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_N$ of the spaces corresponding to each of the subsystems. In the following we shall focus on finite-dimensional bipartite quantum systems, i.e. systems composed of two distinct subsystems, described by the Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B = \mathbb{C}^2 \otimes \mathbb{C}^2$.

An entangled state of a bipartite system is a state that cannot be written as a product state of the component systems. Consider a two-qubit state

$$|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle_{AB} + |10\rangle_{AB}) \tag{4.1}$$

This state cannot be written as a product state of $|q\rangle_A |p\rangle_B$ for $q, p \in \{0, 1\}$. Quantum state $|\psi^+\rangle$ is maximally entangled, which means that when we trace over qubit B to find the reduced density operator ρ_A of qubit A we obtain a multiple of identity operator

$$\rho_A = tr_B(|\psi^+\rangle \langle\psi^+|) = \frac{1}{2}\mathbb{I}_A \tag{4.2}$$

(and similarly $\rho_B = \frac{1}{2}\mathbb{I}_B$). If we measure system A in any basis the result will be completely random ($|0\rangle$ or $|1\rangle$ with equal probability $\frac{1}{2}$). Therefore, if we perform any local measurement of A or B, we acquire no information about the preparation of the state, instead we merely generate a random bit. However, there is a perfect correlation: Whenever we measure $|1\rangle$ in system A then we will measure $|0\rangle$ in system B with certainty and viceversa. In fact, state $|\psi^+\rangle$ is one of a basis of four mutually orthogonal states that span the Hilbert space $\mathcal{H} = \mathbb{C}^2 \otimes \mathbb{C}^2$, the so-called four Bell states:

$$\begin{aligned} |\phi^\pm\rangle &= \frac{1}{\sqrt{2}}(|00\rangle_{AB} \pm |11\rangle_{AB}) \\ |\psi^\pm\rangle &= \frac{1}{\sqrt{2}}(|01\rangle_{AB} \pm |10\rangle_{AB}) \end{aligned} \tag{4.3}$$

The Bell states are special cases of bipartite maximally entangled states on the Hilbert space $\mathbb{C}^d \otimes \mathbb{C}^d$ given by

$$|\psi\rangle = U_A \otimes U_B |\phi_d^+\rangle_{AB} \tag{4.4}$$

with unitary transformations $U = \{\mathbb{I}, \sigma_x, \sigma_y, \sigma_z\}$ and where

$$|\phi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle |i\rangle \tag{4.5}$$

is the canonical maximally entangled state.

The definition of entanglement is operational motivated. Separability is defined via the existence of a decomposition of a state into product states in the case of pure states, or into a convex combination of tensor product for mixed states.

Definition 4.1 **Entanglement in pure states** A pure state $|\psi\rangle \in \mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ is separable if there are local states $|\varphi_A\rangle \in \mathcal{H}_A$ and $|\varphi_B\rangle \in \mathcal{H}_B$, such that the state of the system $|\psi\rangle$ can be written as a tensor product

$$|\psi\rangle = |\varphi_A\rangle \otimes |\varphi_B\rangle \tag{4.6}$$

If $|\varphi_A\rangle, |\varphi_B\rangle$ can be prepared via LOCC then $|\psi\rangle = |\varphi_A\rangle \otimes |\varphi_B\rangle$ is not entangled. A product state contains no correlations.

Definition 4.2 **Entanglement in mixed states** A mixed state ρ is separable if it can be written as a convex combination of projectors onto pure states

$$\rho = \sum_i p_i \left|e_i\right\rangle_A \left\langle e_i\right| \otimes \left|f_i\right\rangle_B \left\langle f_i\right| \tag{4.7}$$

with $p_i > 0$ and $\sum_i p_i = 1$, where $\{|e_i\rangle\}$ and $\{|f_i\rangle\}$ are basis, in general not orthogonal, of Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. Any state of this form can be prepare via LOCC, A prepares the state $|e_i\rangle$ with probability i and tell B to prepare $|f_i\rangle$.

Remark: ρ is separable if it can be written as $\rho = \sum p_i \rho_i^A \otimes \rho_i^B$. This definition is equivalent to $\rho = \sum_i p_i \left|e_i\right\rangle_A \left\langle e_i\right| \otimes \left|f_i\right\rangle_B \left\langle f_i\right|$.

$$\rho = \sum p_i \rho_i^A \otimes \rho_i^B \longleftrightarrow \rho = \sum_i p_i \left|e_i\right\rangle_A \left\langle e_i\right| \otimes \left|f_i\right\rangle_B \left\langle f_i\right| \tag{4.8}$$

Theorem 4.0.1 (Schmidt decomposition)**.** *Any pure state $|\psi\rangle$ can be expressed as*

$$|\psi\rangle = \sum_{k=1}^{r} \lambda_k |u_k\rangle \otimes |v_k\rangle \tag{4.9}$$

where $\lambda_k > 0$ are the Schmidt coefficients satisfying $\sum_k \lambda_k^2 = 1$ and $\{|u_k\rangle\}, \{|v_k\rangle\}$ are orthonormal basis of Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ respectevely. The value r is called the Schmidt rank.

Proof. Given two arbitrary local bases $\{|\varphi_i\rangle\}, \{|\phi_i\rangle\}$ in the spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ any pure state $|\psi\rangle$ can be expressed in terms of the corresponding product basis

$$|\psi\rangle = \sum_{ij}^{d} |\varphi_i\rangle |\phi_j\rangle \langle\varphi_i| \langle\phi_j| |\psi\rangle \tag{4.10}$$

$$= \sum_{ij} M_{ij} |\varphi_i\rangle \otimes |\phi_j\rangle \tag{4.11}$$

For every complex matrix M_{ij} there always exists a singular value decomposition given by $M = UDV$ where U, V are unitaries and D is a diagonal positive semidefinite matrix. Therefore coefficientes M_{ij} can be expressed as

$$M_{ij} = \sum_{k}^{r} U_{ik} \lambda_k V_{kj} \quad \text{with} \quad \lambda_k = D_{kk} \tag{4.12}$$

Finally, the state $|\psi\rangle$ expressed in the new basis has the form

$$|\psi\rangle = \sum_{k}^{r} \lambda_k \left(\sum_{i}^{d} U_{ik} |\varphi_i\rangle \right) \otimes \left(\sum_{j}^{d} V_{kj} |\phi_j\rangle \right) \tag{4.13}$$

$$= \sum_{k}^{r} \lambda_k |u_k\rangle \otimes |v_k\rangle \tag{4.14}$$

□

Like eigenvalues of a matrix, also the singular values λ_k are uniquely defined. Hence, for any state $|\psi\rangle$ the Schmidt coefficients are unique. If there is only one non-vanishing Schmidt coefficient, then $|\psi\rangle$ is separable. Otherwise, when at least two Schmidt coefficients are different from zero, it is not possible to express $|\psi\rangle$ as a product state. Consequently, we can conclude that a pure state $|\psi\rangle$ is separable if and only if the Schmidt rank $r = 1$.

4.1 Quantum channel

A basic issue in both quantum computation and quantum cryptography is that one needs to get information from one point to another in a reliable way. Even storing quantum information at one particular point is a nontrivial issue, since it might decay or degrade. Hence the study of quantum channels, used to transmit or store quantum information, is a very important topic.

We consider two spatially separated particles A(Alice) and B(Bob) and we want to transmit quantum information between them. They are connected via a (possibly noisy) quantum channel described by a completely positive map $\mathcal{E}$, and by a classical channel which either only allows for classical communication from $A \to B$ (one-way classical communication), or for classical communication between $A \to B$ and $B \to A$ (two-way classical communication). In addition, we assume that Alice and Bob can locally manipulate their quantum states and have access and control of auxiliary systems. This set of local operations and classical communication is denoted by LOCC.

A quantum channel is the most general way of describing th evolution of a quantum system, and it is mathematically described by a completely positive[1], trace-preserving linear map. A quantum channel is a superoperator, i.e. it maps density operators to density operators $\mathcal{E} : \mathcal{M}_d \longmapsto \mathcal{M}_d$ and it has the following properties:

(i) Linearity: $\mathcal{E}(\alpha\rho_1 + \beta\rho_2) = \alpha\mathcal{E}(\rho_1) + \beta\mathcal{E}(\rho_2) \quad \forall\alpha, \beta \in \mathbb{C}$

(ii) Hermicity: $\forall\rho : \rho = \rho^\dagger \longrightarrow \mathcal{E}(\rho) = \mathcal{E}^\dagger(\rho)$

(iii) Positivity: $\forall\rho : \rho \geq 0 \longrightarrow \mathcal{E}(\rho) \geq 0$

(iv) Trace-preserving: $tr(\rho) = tr(\mathcal{E}(\rho)) \quad \forall\rho$

Theorem 4.1.1 (Stinespring theorem)**.** *The evolution of a quantum system under a completely positive map can always be seen as the unitary evolution of a larger system, i.e. the composite system of the the quantum state and the environement $\varrho = \rho \otimes \rho_{\text{env}}$. Therefore, every quantum channel $\mathcal{E}$ can be written as*

$$\mathcal{E}(\rho) = tr_{\text{env}}\left(U(\rho \otimes \rho_{\text{env}})U^\dagger\right) \tag{4.15}$$

We can take without loss of generality $\rho_{\text{env}} = |0\rangle\langle 0|$.

$$\mathcal{E}(\rho) = \sum_k \left(\mathbb{I} \otimes \langle k|\right) U(\rho \otimes \rho_{\text{env}})U^\dagger \left(\mathbb{I} \otimes |k\rangle\right) \tag{4.16}$$

$$= \sum_k A_k \rho A_k^\dagger \tag{4.17}$$

We can conclude that $\mathcal{E}$ is a completeley positive map if and only if there exist known operators $\{A_k \in \mathcal{M}_d : \mathcal{E}(\rho) = \sum_k A_k \rho A_k^\dagger\}$ where $A_k = \left(\mathbb{I} \otimes \langle k|\right) U \left(\mathbb{I} \otimes |k\rangle\right)$ are known as Kraus operators. The decomposition of a quantum channel in Kraus operators is in general not unique, since we can perform the partial trace in any basis.

Remark: A quantum channel is trace-preserving, i.e. $tr(\rho) = tr(\mathcal{E}(\rho)) \quad \forall\rho$,

$$tr\left(\sum_k A_k \rho A_k^\dagger\right) = \sum_k tr(A_k \rho A_k^\dagger) \tag{4.18}$$

$$= \sum_k tr(A_k^\dagger A_k \rho) = tr\left(\sum_k A_k^\dagger A_k \rho\right) \tag{4.19}$$

Since $tr(\rho) = tr\left(\sum_k A_k^\dagger A_k \rho\right)$ this leads to the closure relation of Kraus operators $\sum_i A_i^\dagger A_i = \mathbb{I}$ for all ρ.

For qubits a general quantum channel $\mathcal{E}$ can be written as

$$\rho \longmapsto \mathcal{E}(\rho) = \sum_{k,l=0}^{3} p_{k,l} \sigma_k \rho \sigma_l \tag{4.20}$$

where σ_j denote Pauli operators. We consider often Pauli-diagonal channels $\mathcal{E}_\mathcal{P}$ which are of the form

$$\mathcal{E}_\mathcal{P}(\rho) = \sum_{k=0}^{3} p_k \sigma_k \rho \sigma_k \tag{4.21}$$

[1] A map Λ is completely positive if $\mathbb{I} \otimes \Lambda$ is positive.

Notice that any quantum channel $\mathcal{E}$ can be brought to Pauli–diagonal form by means of depolarization [53] in such a way that the diagonal elements are not altered, $p_k = p_{k,k}$. This often allows one to restrict considerations to Pauli–diagonal channels, and makes such channels particularly important. A special instance of a Pauli–diagonal channel is the depolarizing (or white noise) channel, where $p_1 = p_2 = p_3 = (1 - p_0)/3$, which is described by a single parameter $p = p_0$.

4.2 Separability criteria

Checking separability of a given state can turn out to be much more complicated, since in general there are infinetly many valid decompositions if ρ is not pure.

Theorem 4.2.1 (Uhlmann's theorem)**.** *A state ρ can be written as $\rho = \sum^I p_i |\psi_i\rangle \langle\psi_i| = \sum^J q_i |\phi_i\rangle \langle\phi_i|$ if and only if there exists an isometry U, not necessarly squared, such that $\sqrt{p_i}\,|\psi_i\rangle = \sum_j U_{ij}\sqrt{q_j}\,|\phi_j\rangle \quad \forall i$.*

For pure states, the Schmidt decomposition provides a necessary and sufficient criterion for separability but unfortunately for mixed states such decomposition does not exists. Futhermore, in general multipartite states cannot be written as a product of two states.

4.2.1 Peres-Horodecki criterion

Peres-Horodecki criterion [19][20] establishes a necessary condition for the density matrix ρ of a bipartite system to be separable. It is also called the PPT criterion, for positive[2] partial transpose. Consider a state $\rho \in \mathcal{H}_A \otimes \mathcal{H}_B$, then ρ is separable if and only if the new matrix ρ^{T_B} defined as

$$\rho^{T_B} = \sum_{ijkl} p_{kl}^{ij} |i\rangle \langle j| \otimes (|k\rangle \langle l|)^T = \sum_{ijkl} p_{kl}^{ij} |i\rangle \langle j| \otimes |l\rangle \langle k| \tag{4.22}$$

is a density operator, i.e. $\rho^{T_B} > 0$. The operation T_B, called partial transpose, corresponds to a transposition of indices corresponding to the second subsystem and has an interpretation as a partial time reversal. In other words, if the partial transpose ρ^{T_A} has a negative eigenvalue then ρ is guaranteed to be entangled. Notice that this result is independent of the transposed subsystem because $\rho^{T_A} = (\rho^{T_B})^T$. A fundamental fact is that in the cases $\rho \in \mathbb{C}^2 \otimes \mathbb{C}^2$ and $\rho \in \mathbb{C}^2 \otimes \mathbb{C}^3$ the PPT condition is also sufficient for separability.

It can be seen that PPT condition is equivalent to demanding the positivity of the operator $(\mathbb{I}_A \otimes T_B)(\rho)$. The partial transpose map T_B is a positive map but it is not completely positive, and so it is the map $(\mathbb{I}_A \otimes T_B)$.

Proposition 4.2.1. *Any positive but not completely positive map $\Lambda : \mathcal{M}_d \longmapsto \mathcal{M}_d$ provides a non-trivial necessary separability criterion in the form*

$$(\mathbb{I}_A \otimes \Lambda_B)(\rho) \geqslant 0 \tag{4.23}$$

As the partial transpose is a positive map, it turns out that positive maps can serve as good detectors of entanglement. However they cannot be implemented directly in the laboratory because they are unphysical.

4.2.2 Entanglement Witnesses

Entanglement witnesses are fundamental tools in quantum entanglement theory, they were introduced because we cannot directly detect entanglement. They are hermitian operators that completely characterize separable states and allow us to detect entanglement. An hermitian operator W is an entanglement witness if:

(i) $W \not\geqslant 0$, i.e. W has at least one negative eigenvalue.

(ii) $\langle\psi| \langle\phi|W|\psi\rangle |\phi\rangle \geqslant 0 \quad \forall\, |\psi\rangle \in \mathcal{H}_\mathcal{A}, |\phi\rangle \in \mathcal{H}_\mathcal{B}$, i.e. W yields positive expectation values.

Since any separable mixed state ρ_{sep} can be expressed as the convex sum of projectors onto pure states (see Equation 4.7), the expectation value of an EW with respect to any separable mixed state is also non-negative

$$tr\,(W\rho_{sep}) \geqslant 0 \tag{4.24}$$

[2] A operator is positive if it is hermitian and has non-negative eigenvalues.

Theorem 4.2.2. *For any entangled state ρ_{ent} exists an entanglement witness W wich detects ρ_{ent}, i.e. $tr(W\rho_{ent}) < 0$.*

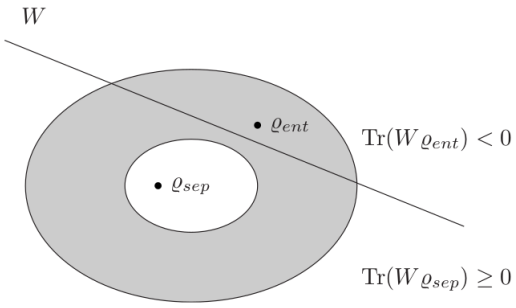

Figure 4.1: Geometric interpretation of entanglement witnesses. The line represents a hyperplane corresponding to the entanglement witness W. All states located to the left of the hyperplane or belonging to it (in particular, all separable states) provide non-negative expctation value of the witness, i.e. $tr(W\rho_{sep}) \geqslant 0$ while those located to the right are entangled states detected by the witness.

Proof. The proof of the above theorem goes through the Hahn-Banach theorem which states the following. Consider a sublinear function $\theta : V \longmapsto \Re$ and a linear function $\pi : U \longmapsto \Re$ on the subspace $U \subseteq V$ which is dominated by θ on U, i.e. $\pi(x) \leq \theta(x) \quad \forall x \in U$. There exists a linear extension $\Theta : V \longmapsto \Re$ of π to the whole space V such that

$$\Theta(x) = \pi(x) \quad \forall x \in U \tag{4.25}$$
$$\Theta(x) \leq \theta(x) \quad \forall x \in V \tag{4.26}$$

□

Choi-Jamiolkowski isomorphism

Entanglement witnesses and positive but not completely positive maps are related by the so-called Choi-Jamiolkowski isomorphism [21][22], given by

$$W_\Lambda = (\mathbb{I} \otimes \Lambda)\left(|\phi_d^+\rangle \langle\phi_d^+|\right) \tag{4.27}$$

where the maximally entangled state $|\phi_d^+\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ is defined as in Equation 4.5.

Proof. Let consider a positive map Λ such that $(\mathbb{I} \otimes \Lambda)(\rho)$ yields a non-positive operator, i.e. Λ is a not completely positive map. Then

$$(\mathbb{I} \otimes \Lambda)(\rho)\,|\chi\rangle = \lambda\,|\chi\rangle \tag{4.28}$$

where $\lambda < 0$ is a negative eigenvalue of eigenvector $|\chi\rangle$. We can show that observable $W = (\mathbb{I} \otimes \Lambda)(|\chi\rangle \langle\chi|)$ is an entanglement witness. For an arbitrary separable state $|\phi_{sep}\rangle$, we have

$$\langle\phi_{sep}|W|\phi_{sep}\rangle = tr\left[((\mathbb{I} \otimes \Lambda)(|\chi\rangle \langle\chi|))\,|\phi_{sep}\rangle \langle\phi_{sep}|\right] \tag{4.29}$$
$$= tr\left[|\chi\rangle \langle\chi|\,((\mathbb{I} \otimes \Lambda)(|\phi_{sep}\rangle \langle\phi_{sep}|))\right] \geqslant 0 \tag{4.30}$$

where the inequality is due to the positivity of Λ, such that $(\mathbb{I} \otimes \Lambda)(|\phi_{sep}\rangle \langle\phi_{sep}|)$ is a positive operator. □

Optimal entanglement witnesses

The method of entanglement witnesses is currently considered to be the most important and best method for detecting entanglement, unfortunately there are infinitely many of them and the determination of entanglement witnesses for all entangled states is a $\mathbb{NP}$-hard problem. Constructing entanglement witnesses in general, and finding the minimal set of them that allows for the detection of all entangled states is one of the most challenging open questions.

It is known that the set of quantum states (separable states and entangled states) is convex and compact. Hence, by Theorem 4.2.2 there is at least one "high-level" witness "witnessing" an entanglement witness [23]. For this high-level witness Π:

(i) $tr(\Pi\rho) \geq 0$ for all quantum (entangled or not) state ρ;

(ii) there exists an entanglement witness W such that $tr(\Pi W) < 0$.

Operators that satisfy the above two conditions are none other than entangled states. Entanglement witnesses "witness" entangled states and entangled states "witness" entanglement witnesses. Given a "high-level" witness, entangled state ρ, we can define $D_\rho = \{W | tr(W\rho) < 0\}$, that is the set of operators "witnessed" by ρ. Given two entangled states ρ_1 and ρ_2, we say that ρ_2 is finer than ρ_1 if $D_{\rho_1} \subseteq D_{\rho_2}$, that is if all the operators "witnessed" by ρ_1, are also "witnessed" by ρ_2. We say that an entangled state ρ is an optimal high-level witness if there exists no other high-level witness which is finer.

This leads to a hierarchy of entanglement witnesses. We need a criteria to determine when an EW is optimal [24].

Lemma 4.2.1. *Let W_2 be finer than W_1 and $\delta \equiv inf_{\rho_1 \in D_{W_1}} |\frac{tr(W_2\rho_1)}{tr(W_1\rho_1)}|$. Then we have:*

(i) If $tr(W_1\rho) = 0$ then $tr(W_2\rho) \leq 0$;

(ii) If $tr(W_1\rho) < 0$ then $tr(W_2\rho) \leq tr(W_1\rho)$;

(iii) If $tr(W_1\rho) > 0$ then $\delta tr(W_1\rho) \geq tr(W_2\rho)$;

(iv) $\delta \geq 1$, in particular $\delta = 1$ if and only if $W_1 = W_2$

Corollary 3. *$D_{W_1} = D_{W_2}$ if and only if $W_1 = W_2$.*

An entanglement witness is finer than another one if they differ by a positive operator. That is, if we have an EW and we want to find another one which is finer, we have to subtract a positive operator

Lemma 4.2.2. *An entanglement witness W_2 is finer than W_1 if and only if there exists a P and $1 > \epsilon \geq 0$ such that $W_1 = (1-\epsilon)W_2 + \epsilon P$*

By means of the two previuos lemmas we can fully characterize optimal entanglement witnesses.

Theorem 4.2.3. *An entanglement witness W is optimal if and only if for all $P > 0$ and $\epsilon > 0$, $W' = (1+\epsilon)W - \epsilon P$ is not an entanglement witness.*

Proof. On the one hand, according to 4.2.2 there is no EW which is finier than W and therefore W is optimal. On the other hand, if W' is an EW, then according to the same lemma W is not optimal. □

There exists a class of EW which is very simple to characterize, namely decomposable entanglement witnesses. An entanglement witness W is called decomposable if it can be written in the form

$$W_d = aP + (1-a)Q^T \tag{4.31}$$

where $a \in [0,1]$ and $P, Q \geq 0$. If it does not admit this form it is called non-decomposable. The set of decomposable EW is convex and compact.

Lemma 4.2.3. *A decomposable entanglement witness can only detect non-positive partial transpose entangled states.*

Proof. Consider an entanglement witness $W = P + Q^{T_A}$, then $tr(W\rho) = tr(P\rho) + tr(Q\rho^{T_A})$. Since $P, Q \geq 0$, if $tr(W\rho) < 0$ then $\rho^{T_A} \not\geq 0$. □

Theorem 4.2.4. *Given a decomposable entanglement witness W, if it is optimal then it can be written as $W = Q^T$, where $Q \geq 0$ contains no product vector in its range.*

4.3 Entanglement Measures

The distinction between separable and entangled states does not allow to compare the amount of entanglement of two different states. For such purpose, we need a quantitative description of entanglement. A way to do that is to consider the interconvertability between quantum states, this is: given two states $|\psi\rangle$ and $|\phi\rangle$, the question is whether or not $|\psi\rangle$ can be transformed into

$|\phi\rangle$ by local operations. Consider a bipartite state ρ, the most general local operation that acts non-trivially only on the first subsystem reads

$$\rho \longmapsto \sum_i (a_i \otimes \mathbb{I})\rho(a_i^\dagger \otimes \mathbb{I}), \quad \sum_i a_i^\dagger a_i = 1 \tag{4.32}$$

and analogously for operations on the second subsystem alone. Such operations do not induce any correlations: they map product states on product states,

$$\rho = \rho^A \otimes \rho^B \longmapsto \left(\sum_i a_i \rho^A a_i^\dagger\right) \otimes \rho^B \tag{4.33}$$

and separable states on separable states,

$$\rho = \sum_i p_i \rho_i^A \otimes \rho_i^B \longmapsto \sum_i p_i \left(\sum_j a_j \rho_j^A a_j^\dagger\right) \otimes \rho_i^B \tag{4.34}$$

The situation changes if one allows for a correlated application of such local operations, where the operation that is applied at a certain instance depends on the outcomes of previous operations. Such operations are called local operations and classical communication (LOCC). The idea is that Alice and Bob have access to the individual subsystems and they can apply their individual operations to their part of the compositve system. But in order to arrive at the above operation, they would need to communicate with each other, i.e. tell the other one their measurement results via a classical channel.

LOCC operations can take product states to states no more necessarily of product form. Thus, it is possible to create correlations with LOCC operations, but since these correlations are based on the classical exchange of information, they remain correlations of classical nature. Since LOCC operations are free, i.e. their implementation does not consume entanglement, a state $|\psi\rangle$ which can be mapped into $|\phi\rangle$ by LOCC is necessarily at least as entangled as $|\phi\rangle$. We can define some quantity E, called entanglement monotone [25], that does not increase under LOCC.

$$|\psi\rangle \xrightarrow{\text{LOCC}} |\phi\rangle \Longrightarrow E(|\psi\rangle) \geq E(|\phi\rangle)$$

Among all LOCC operations, we first consider local unitaries. Consider two bipartite states $|\psi\rangle$ and $|\phi\rangle$, they are LU-equivalent, written $|\psi\rangle \simeq_{LU} |\phi\rangle$, if there exist local unitary operators such that $|\psi\rangle = U_A \otimes U_B |\phi\rangle$. Note that if two states are LU-equivalent they have precisely the same amount of entanglement, and thus they can be usefull for the same applications.

$$E(\rho) \geq E\left((U_A \otimes U_B)\rho(U_A^\dagger \otimes U_B^\dagger)\right) \tag{4.35}$$

Because initial and final states are equal, so is their entanglement, and one necessarily concludes that any entanglement monotone is invariant under local unitaries.

Definition 4.3 **Entanglement Monotone (EnMon)** A function $E : \mathcal{H} \longmapsto \Re$ is an entanglement monotone if it is non-increasing on average under LOCC,

$$\forall \rho, \{p_i, \sigma_i\} : \rho \xrightarrow{\text{LOCC}} \{p_i, \sigma_i\} \Longrightarrow E(\rho) \geq \sum_i p_i E(\sigma_i) \tag{4.36}$$

Definition 4.4 **Entanglement Measure (EnMes)** A function $E : \mathcal{H} \longmapsto \Re$ is an entaglement measure if it is non-increasing under LOCC, i.e.

$$\forall \rho : \rho \xrightarrow{\text{LOCC}} \Lambda_{LOCC}(\rho) \Longrightarrow E(\rho) \geq E(\Lambda_{LOCC}(\rho)) \tag{4.37}$$

The difference between EnMes and EnMon is the final state after the LOCC protocol. In EnMes the final state is clear, is $\Lambda_{LOCC}(\rho)$, but in EnMon the final state is σ_i with probability p_i. In EnMon, the entanglement cannot increase in average. We see that mathematically there is a difference between entanglement measures and entanglement monotones, EnMon is a stronger condition.

Examples of entanglement measures are entanglement of formation, concurrence, negativity, Schmidt number, Renyi entropy and so on (see [26]). Almost all known criteria map an entangled state to a real number (sometimes between 0 and 1 for comparison). Generaly whether a state is regarded as being more entangled than another is dependent on the choice of criterion used. Therefore, there exists the possibility that two different entangled states obtain the same value with respect to some measure. There also exists the possibility that a criterion indicates $E_1(\rho_1) > E_1(\rho_2)$ but another criterion shows $E_2(\rho_1) < E_2(\rho_2)$.

Entanglement measures for pure bipartite states

Invariance under local unitary transformations is not only way to check entanglement monotones as non-monotonous under LOCC, but indeed it has much deeper implications. It implies that any entanglement monotone can be expressed as a function only of invariants under local unitaries.

Consider two pure states $|\psi\rangle, |\phi\rangle$. An entanglement measure E for pure states can be define as

$$\forall\, |\psi\rangle, |\phi\rangle : |\psi\rangle \xrightarrow{\text{LOCC}} |\phi\rangle \Longrightarrow E(|\psi\rangle) \geq E(|\phi\rangle) \tag{4.38}$$

The Schmidt coefficients introduced in Equation 4.0.1 provide a complete set of invariants, and all entanglement properties can be expressed in terms of them. Consider a pure bipartite state $|\phi\rangle$ such that it can be prepared by LOCC starting from another pure state $|\psi\rangle$. Then, their Schmidt coefficients, ordered decreasingly ($\lambda_1 \geq \lambda_2 \geq \ldots$), satisfy the following inequalities,

$$\begin{aligned}
\lambda_1^{(\phi)} &\geq \lambda_2^{(\psi)} \\
\sum_{i=1}^{2} \lambda_i^{(\phi)} &\geq \sum_{i=1}^{2} \lambda_i^{(\psi)} \\
\sum_{i=1}^{3} \lambda_i^{(\phi)} &\geq \sum_{i=1}^{3} \lambda_i^{(\psi)} \\
&\vdots
\end{aligned}$$

Theorem 4.3.1 (Majorization)**.** *A pure bipartite state $|\phi\rangle$ can be reached from $|\psi\rangle$ by means of LOCC if and only if the majorization condition is fulfilled.*

$$|\psi\rangle \xrightarrow{LOCC} |\phi\rangle \Longleftrightarrow \boldsymbol{\lambda}^{(\phi)} \succeq \boldsymbol{\lambda}^{(\psi)} \tag{4.39}$$

where the Schmidt vectors are $\boldsymbol{\lambda}^{(\phi)} = [\lambda_1^{(\phi)}, \lambda_2^{(\phi)}, \ldots]$ and similarly for $\boldsymbol{\lambda}^{(\psi)}$.

Entanglement monotones for pure states can be defined as

$$\forall\, |\psi\rangle, \{p_i, |\phi_i\rangle\} : |\psi\rangle \xrightarrow{\text{LOCC}} \{p_i, |\phi_i\rangle\} \Longrightarrow E(|\psi\rangle) \geq \sum_i p_i E(|\phi_i\rangle) \tag{4.40}$$

Therefore, E is an entanglement monotone for pure states if and only if E is not increasing on average under uni-local operations applied by A and B (we do not need to consider classical communication).

Notice that $|\psi\rangle \xrightarrow{\text{LOCC}} |\phi\rangle = |\psi\rangle \xrightarrow{\text{LOCC}} \{p_1 = 1, |\phi\rangle\}$, then we can conclude that if E is EnMon for pure states, it is also EnMes for pure states.

4.4 Some applications

4.4.1 Quantum cryptography

The aim of quantum cryptography is the secure transmission of secret messages from Alice to Bob. The most well known example of quantum cryptography is quantum key distribution, which was first developed by Bennet and Brassard in 1984 [7]. In this protocol, known as BB84, Alice want to establish a private key, a sequence of random bits that are only known to Alice and Bob, to transmit a message of the same length to Bob. Single qubits are prepared in non-orthogonal states and then transmitted from A to B and subsequently measured.

(i) Alice randomly selects a bit value $j \in \{0, 1\}$ and a basis $\alpha \in \{x, z\}$. She prepares the qubits in the states $|j_\alpha\rangle$, i.e. one of the four states $\{|0\rangle, |1\rangle, |0_x\rangle, |1_x\rangle\}$;

(ii) Alice sends the qubits to Bob;

(iii) Bob perfoms a measurement on the qubit in a random basis $\beta \in \{x, z\}$. If $\alpha = \beta$ Bob will obtain a deterministic outcome, otherwise the measurement result is random;

(iv) Alice and Bob reveal the used bases α and β for each qubit through a public channel. If $\alpha = \beta$ they know that they are sharing a random bit j;

(v) Alice and Bob select randomly M of the bits they share and compare the bit values over the public channel. If many of the bits do not coincide, they assume that an eavesdropper has interfered with the transmission. If all the M bits coincide, the remaining bits can be used as a random bit string, i.e. as a secret key.

The security of the BB84 protocol is based on the fact that any attempt to reveal information about the transmitted quantum system involves the measurement of some observable, it will change the transmitted state and this allows one to detect the presence of an eavesdropper. In addition, it is impossible to clone the state of a single qubit.

A QKD method based on entangled pairs and Bell's theorem was proposed by Ekert in 1991 [8]. The pairs of photons are created by Alice, by Bob, or by some source separated from both of them, and then distributed so that Alice and Bob each end up with one qubit from each pair. Similarly to BB84, the protocol involves a private measurement protocol, Alice measures randomly each photon she receives in some basis set and so does Bob. They keep their series of basis choices private until the measurements are completed. Two groups of qubits are made: the first consists of qubits measured using the same basis and the second contains the rest. To detect eavesdropping, they can compute the correlation coefficients according to Bell's inequalities and check whether Bell's theorem is violated or not. If the protocol is successful, the first group of qubits can be used to generate secure keys since they are completely anti-aligned between Alice and Bob.

The security of E91 relies on the so-called monogamy of entanglement: if two particles are entangled, they will not be entangled to any external system. In other words, no information about the system leaks to environement. If Eve tries to manipulate the qubits the entanglement will be lost.

An interesting fact is that Choi-Jamiolkowski isomorphism shows that prepare-and-measure protocols, such as BB84 and entanglement-based protocols, such as E91 are equivalent.

4.4.2 Quantum dense coding

Quantum dense coding, or superdense coding, was first proposed by Bennet and Weisner in 1992 [9] and it is a quantum communication protocol to transmit two classical bits of information (00, 01, 10, or 11) by first sharing an Bell state between Alice and Bob and then sending only one qubit. Superdense coding is the underlying principle of quantum secret coding since a third particle is unable to get any information without access to both qubits. Superdense conding protocol has the following steps:

(i) Alice and Bob share the Bell state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$;

(ii) Alice encodes the two classical bits she wants to share by applying a quantum gate to her qubit locally. The four quantum gates are Pauli-gates $\{\mathbb{I}, X, Y, Z\} = \{\mathbb{I}, \sigma_x, \sigma_y, \sigma_z\}$;

Classical bits	Quantum gate	Resulting Bell state
00	$\mathbb{I}_A$	$\|\phi^+\rangle$
01	Z_A	$\|\phi^-\rangle$
10	X_A	$\|\psi^+\rangle$
11	$Z_A X_A$	$\|\psi^-\rangle$

(iii) Alice sends her qubit to Bob, and he can make a measurement in the Bell basis and perfectly distinguish whether the state is $|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle$ or $|\psi^-\rangle$ since Bell states are orthogonal to each other, and hence retrieve Alice's message.

In the quantum circuit scheme, a Bell measurement can be seen as a unitary CNOT gate $CNOT^{A\to B} = |0\rangle^A \langle 0| \otimes \mathbb{I}^B + |1\rangle^A \langle 1| \otimes \sigma_x^B$ followed by a Hadamard gate $H_A \otimes \mathbb{I}_B = \frac{1}{\sqrt{2}}(\sigma_x + \sigma_z) \otimes \mathbb{I}$.

Remark There is no contradiction with Holevo's theorem, which states that by using one two-level quantum system, we can only encode 1 bit of classical information. If we count step (i), Alice and Bob exchange 2 qubits in total. More precisely, Alice does not encode her message in an isolated particle, but in a non-locally entangled 2-particle system: not separable into two isolated particles.

4.4.3 Teleportation

As quantum dense coding, teleportation is a quantum communication protocol proposed by Bennet *et al* in 1993 [10], unless one qubit of information is transmitted instead of two classical bits. Alice

can transmit one unknown qubit $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$ to Bob by first sharing a Bell state, which is used as a perfect quantum channel, and then locally manipulating her qubit and sending classical information. Teleportation protocol has the following steps:

(i) Alice and Bob share the Bell state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$, Alice has an extra qubit to be teleported $|\varphi\rangle$, so the initial state is $|\varphi\rangle|\phi^+\rangle$;

(ii) Alice makes a local Bell measurement on her two qubits A', A, the resulting state is

$$\frac{1}{\sqrt{2}}\left(|00\rangle_{A'A}(\alpha|0\rangle_B + \beta|1\rangle_B) + |01\rangle_{A'A}(\alpha|1\rangle_B + \beta|0\rangle_B)\right.$$
$$\left. + |10\rangle_{A'A}(\alpha|0\rangle_B - \beta|1\rangle_B) + |11\rangle_{A'A}(\alpha|1\rangle_B - \beta|0\rangle_B)\right)$$

(iii) Alice makes a measurement in the computational basis on her two qubits and she tells Bob the resulting state using a classical channel;

(iv) According to Alice's message, Bob applies a correction operation on qubit B and he obtains the desired state $|\varphi\rangle$.

Alice's result	Correction
$\|00\rangle$	$\mathbb{I}_B$
$\|01\rangle$	X_B
$\|10\rangle$	Z_B
$\|11\rangle$	$Z_B X_B$

Notice that qubit B takes over completely the role of qubit A', in particular also its entanglement with additional particles. This property can be used for entanglement swapping, where entanglement between systems AC_1 and C_2B leads to an entanglement state between systems AB by teleporting C_1 to B. Teleportation has been experimentally demonstrated for single photons [27], light beams [28], atoms [29] and also between light and matter [30].

Chapter 5

Quantum Communication

Quantum communication is one of the most advanced applications of quantum information processing, and a basic tool for distributed quantum computation or quantum cryptography, where the transmission of quantum states allows one to establish a secret key between two communication partners, enabling secure communication. For all these applications of a quantum communication network, the term quantum internet has been suggested [31], in analogy with the classical internet. In classical communication, to send a message means to correlate the sender to the receiver. Thus the ability to faithfully transmit a bit is equivalent to the ability to faithfully share maximally correlated bits. In quantum communication theory it is entanglement which will play the role of correlations, and for this reason entanglement is the key tool of quantum communication theory. To send quantum information is equivalent to transmit an unknown entangled quantum state [10].

However, for quantum communication, teleportation alone is not sufficient. If we send maximally entangled states through a noisy quantum channel we end up with noisy, non-maximally entangled states, and although they can still be used for quantum teleportation, the fidelity of the teleported qubits is reduced. The generation and maintenance of high-fidelity entanglement is a central problem, noisy operations as well as interactions with the environement have the effect that the desired entangled states are produced only with a certain non–unit fidelity. In aim to solve the problem of quantum communication over noisy quantum channels several methods have been designed in last years.

Although classical communication theory inspires techniques for quantum communication, there are several issues that need to be considered. First, coding based on data-copying, which is used in classical error correction cannot be used due to the no-cloning theorem of quantum mechanics. This result implies that there exists no transformation resulting in the following mapping,

$$U(|\psi\rangle \otimes |e\rangle) = |\psi\rangle \otimes |\psi\rangle \quad \forall\, |\phi\rangle \tag{5.1}$$

i.e. it is impossible to perfectly copy an unknown quantum state.

Proof. Assume that such general transformation U exists. Take and arbitray state $|\chi\rangle$ and consider

$$(\langle\chi| \otimes \langle e|)(|\psi\rangle \otimes |e\rangle) = \langle\chi|\psi\rangle \langle e|e\rangle \tag{5.2}$$

$$(\langle\chi| \otimes \langle e|)U^\dagger U(|\psi\rangle \otimes |e\rangle) = (\langle\chi| \otimes \langle\chi|)(|\psi\rangle \otimes |\psi\rangle) \tag{5.3}$$

$$= |\langle\chi|\psi\rangle|^2 \tag{5.4}$$

So $\langle\chi|\psi\rangle = |\langle\chi|\psi\rangle|^2$, therefore they are either the same state or $\langle\chi|\psi\rangle = 0$ □

This means that quantum data cannot be protected from errors by simply making multiple copies. Secondly, direct measurement cannot be used to effectively protect against errors, since this will destroy any quantum superposition. Two solutions are proposed:

(i) quantum error correction: the information is encoded in a larger dimensional Hilbert space and it is protected from noise.

(ii) entanglement purification (combined with teleportation): the information is transmitted by means of teleportation, using a known entangled state with sufficiently high fidelity which is obtained by entanglement purification.

5.1 Quantum Error Correction

Quantum error correction codes utilizes the idea of redundant encoding. The total size of the Hilbert space is expanded beyond what is needed to store a single qubit of information, and in this way, errors on individual qubits are mapped to large set of mutually orthogonal subspaces, the size of which is determined by the number of qubits utilized in the code. In quantum error correction codes, quantum information is protected by encoding one logical qubit of information into several physical qubits, or more generally k logical qubits into n physical qubits. In the simplest case where one qubit is encoded into n qubits, we define the logical qubits $|0_L\rangle, |1_L\rangle$ as two orthogonal states in $\mathbb{C}^{2n}$. Any entangled state $\alpha|0\rangle + \beta|1\rangle$ is encoded via unitary encoding operation yielding an encoded state

$$(\alpha|0\rangle + \beta|1\rangle) \otimes |0\rangle^{\otimes n-1} \rightarrow \alpha|0_L\rangle + \beta|1_L\rangle \tag{5.5}$$

Logical qubits $|0_L\rangle, |1_L\rangle$ span a two-dimensional subspace which is mapped to orthogonal two-dimensional subspaces by error operators. Then by measuring appropriate two–dimensional projectors, one can distinguish between these subspaces and correct the errors. If all the subspaces are pairwise orthogonal then the corresponding code is able of an independent treatment of errors and of correcting all of them. Importantly, coherent superpositions within each of the subspaces are not altered and hence quantum information is preserved.

Finally, the error correction protocol cannot allow us to gain information regarding the coefficients, α and β of the encoded state since that would collapse the system.

Unlike classical information, qubits are susceptible to both bit-flip errors $|0\rangle \leftrightarrow |1\rangle$ and phase-flip errors $|0\rangle \leftrightarrow |0\rangle$, $|1\rangle \leftrightarrow -|1\rangle$. Hence, any error correction procedure needs to be able to simultaneosusly correct for both.

5.1.1 The 9-qubit code

The 9-qubit error correcting code was first developed by Shor in 1995 [34], demonstrating that QEC was possible. The Shor code is a degenerate single error correcting code, i.e. different types of errors have the same syndromes, and it is able to correct a logical qubit from one bit-flip, one phase-flip or one of each, on any of the nine physical qubits. This code is therefore sufficient to correct for an arbitrary single qubit error.

The two basis states for the code are,

$$|0_L\rangle = \frac{1}{\sqrt{8}}(|000\rangle + |111\rangle)(|000\rangle + |111\rangle)(|000\rangle + |111\rangle) \tag{5.6}$$

$$|1_L\rangle = \frac{1}{\sqrt{8}}(|000\rangle - |111\rangle)(|000\rangle - |111\rangle)(|000\rangle - |111\rangle) \tag{5.7}$$

and the circuit to perfom the encoding is shown in Figure 5.1.

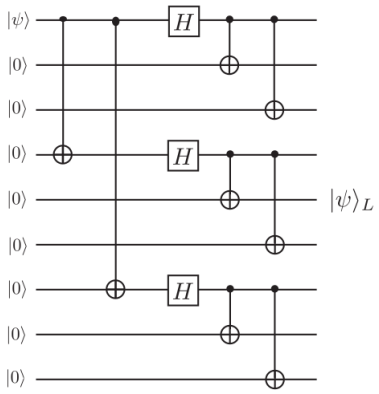

Figure 5.1: Circuit required to encode a single qubit with 9-qubit code.

For single bit-flip errors $\sigma_x \equiv X$ we consider blocks of three qubits, i.e. $|0_L\rangle = |000\rangle$ and

$|1_L\rangle = |111\rangle$ such that an arbitrary single qubit state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is mapped to

$$\begin{aligned}\alpha|0\rangle + \beta|1\rangle &\rightarrow \alpha|0_L\rangle + \beta|1_L\rangle \\ &= \alpha|000\rangle + \beta|111\rangle \\ &= |\psi_L\rangle\end{aligned}$$

For each block of three qubits encoded to $(|000\rangle + |111\rangle)/\sqrt{2}$ we perfom the correction circuit shown in Figure 5.2, we assume that all gate operations are perfect. Correction proceeds by introducing two ancilla qubits and performing a sequence of CNOT gates, which checks the parity of the three qubit data block. Using syndrome information, the X error can be corrected with a classically controlled σ_x gate. Phase-flip errors $\sigma_z \equiv Z$ can be corrected by checking the sign differences between the three blocks of qubits.

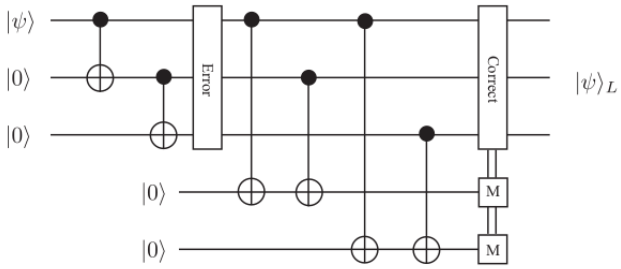

Figure 5.2: Circuit for encode and correct single X errors. After encoding a single logical qubit via two ancilla qubits and two CNOT gates, two extra ancilla qubits are coupled to the data block. These ancilla are measured and the measurement result indicates if an error has ocurred and where.

For each possible situation, either no error or a single bit-flip error, the ancilla qubits are flipped to a unique state based on the parity of the data block. These qubits are then measured to obtain the classical syndrome result and the result of the measurement will indicate if a correction is needed.

Ancilla measurement	Collapsed state	Error
00	$\alpha\|000\rangle + \beta\|111\rangle$	No error
01	$\alpha\|001\rangle + \beta\|110\rangle$	σ_x on qubit 3
10	$\alpha\|010\rangle + \beta\|101\rangle$	σ_x on qubit 2
11	$\alpha\|100\rangle + \beta\|011\rangle$	σ_x on qubit 1

Table 5.1: Ancilla measurements for single σ_x error for a block of three qubits. Each of the four possible results correspond to either no error or a bit flip on one of the three qubits.

The distance between two codeword states, d, defines the number of errors that can be corrected, t, as, $t = (d-1)/2$. In this case, for each block of three qubits we have $d = 3$, hence $t = 1$. This code will only work if a maximum of one error occurs per block.

Error	Final state: data, ancilla	Assumed error
Qubits 1,2	$\alpha\|110\rangle\|01\rangle + \beta\|001\rangle\|01\rangle$	σ_x on qubit 3
Qubits 2,3	$\alpha\|011\rangle\|11\rangle + \beta\|100\rangle\|11\rangle$	σ_x on qubit 1
Qubits 1,3	$\alpha\|101\rangle\|10\rangle + \beta\|010\rangle\|10\rangle$	σ_x on qubit 2
Qubits 1,2,3	$\alpha\|111\rangle\|00\rangle + \beta\|000\rangle\|00\rangle$	No error

Table 5.2: Error syndromes are not unique when multiple errors occur.

Notice that a phase-flip on any one qubit in a block of three has the same effect, this is why 9-qubit code is a degenerate code. In other error correcting codes, such as the 5- or 7-qubit codes ([35], [36]), there is a one-to-one mapping between errors and unique states. In degenerate codes such as the 9-qubit code, the mapping is not unique, we know in which block the error occurs and it does not matter which qubit we apply the correction operator to. As the 9-qubit code can correct for a single X error in any one block of three and a single phase-flip error on any of the nine qubits, this code is a full quantum error correcting code. However, in general, the 9-qubit code

is only a single error correcting code as it cannot handle multiple errors if they occur in certain locations.

5.1.2 QEC with stabilizer codes

The use of the stabilizer formalism introduced in the context of grah states in section 3.3 to describe quantum error correction codes is very useful since it allows easy generalised representation of correction circuits, regardless of the code used [33]. A state $|\psi\rangle$ is defined to be stabilized by operator K if it is an eigenstate of K with eigenvalue $+1$,

$$K|\psi\rangle = |\psi\rangle \tag{5.8}$$

For example, the single qubit state $|0\rangle$ is stabilized by operator $K = \sigma_x$, i.e. $\sigma_x|0\rangle = |0\rangle$.

The association between stabilizer codes and stabilizer states comes about by defining a coding subspace. Consider a bipartite state $|\psi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$, the Hilbert space has dimension four, however if we require that this two qubit state is stabilized by $\sigma_x \otimes \sigma_x \equiv XX$, then there are only two orthogonal basis states which satisfies that,

$$|0_L\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{5.9}$$

$$|1_L\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |11\rangle \tag{5.10}$$

Hence by using stabilizers we can reduce the size of the Hilbert space for a multi-qubit system to an effective single qubit system. For a n-qubit system the Hilbert space has dimensionality 2^n, if the stabilizer set of this system contains k elements then the dimension of the subspace is 2^{n-k}. A stabilizer code is therefore a subspace defined via stabilizer operators for a multi-qubit system containing $n-k$ logical qubits.

Consider the 9-qubit code, its stabilizer set is fully specified by the eight following operators

$$\begin{aligned} K^1 &= ZZIIIIIII & K^5 &= IIIIIIZZI \\ K^2 &= ZIZIIIIII & K^6 &= IIIIIIIZIZ \\ K^3 &= IIIZZIIII & K^7 &= XXXXXXIII \\ K^4 &= IIIZIZIII & K^8 &= XXXIIIXXX \end{aligned}$$

The dimensionality of a 9-qubit system is 2^9 and there are eight stabilizers, therefore the total dimension of this subspace defined by the stabilizer set is $2^{9-8} = 2$. The stabilizer set now defines an effective 2-dimensional subspace, and it encodes nine physical qubits into one logical qubit t correct for a single X, Z error. When we measure the eigenvalue of K^1, we determine if a bit-flip error has happened on qubit one or two, i.e. if $\sigma_x^{(1)}$ or $\sigma_x^{(2)}$ has happened. Note that both of these errors anticommute with K^1, while $\sigma_x^{(3)}$ through $\sigma_x^{(9)}$, which cannot be detected by just K^1, commute with it. Similarly, K^2 detects $\sigma_x^{(1)}$ or $\sigma_x^{(3)}$, which anticommute with it, and K^7detects $\sigma_z^{(1)}$ through $\sigma_z^{(6)}$.

5.1.3 Quantum error detection

We have focused on the requirement not only to detect errors but also correct them, however another approach is to not force the correcting ability. Post-selected quantum computation [37] demonstrated that large scale quantum computing could be achieved with higher noise rates when only error detection is used instead of more costly error correction codes. In general, error detection is faster and requires fewer qubits than performing active error correction, but on the other hand the resource requirements are much higher.

For error detection, it is only require that an error operator O_j maps states within subspace S to orthogonal subspace $S^{\perp}$, but it is not necessary that subspaces of different error operators are pairwise orthogonal. This implies that different error operators can lead to the same output state, and hence are indistinguishable.

The basic idea in post-selected schemes is to encode a large number of ancilla qubits with error detecting circuits, then sets of encoded qubits which pass error detection are selected and utilized as encoded ancillas for error correction. By producing and verifying large numbers of encoded

ancillas which are post-selected, error correction can be performed without data qubits waiting as long for appropriate ancilla to be prepared, decreasing the number of errors that need to be corrected.

5.2 Entanglement Purification

When distant parties share n copies of a mixed state ρ, which contains noisy entanglement, they can perform some LOCC, i.e. a sequence of local operations and one or two-way classical communication and obtain a reduced number of k pairs with increase fidelity. A sequence of LOCC operations achieving this task is called entanglement purification or entanglement distillation protocol. In entanglement purification, several copies of noisy, non–maximally entangled states are manipulated in such a way that a fewer number of copies with a reduced amount of noise are produced. This is possible since the desired state is known. The entanglement of the total ensemble is concentrated or distilled in a few copies, which hence contain a larger amount of entanglement and have higher fidelity, entanglement is purified at the cost of obtaining smaller number of copies. After purification protocol, the distilled states can be used to perfom quantum teleportation, quantum cryptography or other entanglement-based protocols.

Entanglement purification protocols were first introduced for bipartite states [38], and later for multipartite entangled states, in particular graph states or stabilizer states [39], [40], [41], [42]. In the multipartite case, there is no distinguished state like a singlet state that can be a universal target state in entanglement distillation procedures, however there are some classes of interesting target states, including the commonly studied GHZ state.

Purification protocols differ in the number of copies of the states they operate on and they can purify, the efficiency, and also whether they allow one-way or two-way classical communication. Consider a protocol that operates on N copies of noisy entangled states and produce $M \leq N$ purified copies. In case of one–way classical communication $A \to B$, we measure $N-M$ copies and use the obtained information to choose a proper correction operation on the remaining pairs. Notice that for the choice of these correction operations, Alice only has access to the local measurement outcomes in A, while Bob has access to outcomes of measurements in A and B. In particular, this implies that the particles cannot decide to discard certain pairs based on joint measures outcomes. To make this possible, two-way classical communication is needed. The purification protocols can be grouped into distillation protocols, where an ensembre of many copies is manipulated to get a few pairs with higher fidelity; and recurrence and pumping schemes, which are based on the iteration of a purification step several times, resulting in pairs with improved fidelity.

We define the yield of a EP protocol for quantitying how efficient a protocol is. Consider some $N \to M$ protocol, i.e. a protocol which starts with N copies of a mixed state, $\rho^{\otimes N}$ and after purification M copies of a maximaly entangled state are obtained. The yield of the protocol with respect to the state ρ is defined as

$$Y_\rho = \frac{M}{N} \tag{5.11}$$

We are interested in optimal entanglement purification protocols, i.e. those which result in a maximal ratio M/N. More precisely, we demand that for all $\epsilon > 0$, the fidelity of the resulting state after puritication protocol with respect to M copies of a maximally entangled state $|\Phi\rangle = |\phi^+\rangle^{\otimes M}$ must be $F \geq 1-\epsilon$. The yield is then determined by the ratio M/N of the maximum M for which this is the case in the asymptotic limit of $N \to \infty$. This optimal ratio is called distillable entanglement and denoted as E_D. Notice that such a strict definition of yield actually implies that many entanglement purification protocols have zero yield, although they can produce entangled states with arbitrary high fidelity.

The purification range of a protocol is defined as the set of all input states ρ that can be purified by the protocol, i.e. where maximally entangled states can be generated from N copies of ρ in the asymptotic limit of $N \to \infty$.

5.2.1 Basic purification protocols

5.2.2 Bound entanglement

The distillability problem, i.e. the question whether there exists a LOCC protocol that can generate maximally entangled states from (infinitely) many copies of a state, has been extensively studied in recent years, however a complete solution has not been obtained so far. What is, however, known

are necessary conditions for distillability (e.g. that the partial transposition of the density operator is non–positive), as well as sufficient criteria.

A question fundamental for quantum information processing then immediately arose: Can noisy entanglement always be purified? Bound entanglement vs free entanglement (can be distilled)

5.2.3 Error model

We consider entanglement purification protocols under non–idealized conditions, i.e. local operations are noisy. The main effect of noise is that no longer maximally entangled states can be produced, and the achievable fidelity is smaller than unity. Similarly, the required initial fidelity in the case of noisy local control operations is larger. We describe a noisy single-qubit operation by $\hat{U}\prod_k \varepsilon_q^{(k)}\rho$, i.e. single-qubit local noise with error parameter q, followed by the perfect unitary operation $\hat{U}$ with $\hat{U}\rho = U\rho U^\dagger$. We model local noise by

$$\varepsilon_q^{(k)}\rho = U_k[\mathcal{M}_k\mathcal{M}_k\rho]U_k^\dagger \tag{5.12}$$

where $\mathcal{M}_k$ is a local completely positive maps, which may denote white noise (depolarizing channels),

$$\mathcal{M}_k\rho = q\rho + (1-q)\frac{1}{4}\sum_{i=0}^{3}\sigma_i^{(k)}\rho\sigma_i^{(k)} \tag{5.13}$$

bit-flip channels,

$$\mathcal{M}_k^B\rho = q\rho + (1-q)\frac{1}{2}(\rho + \sigma_1^{(k)}\rho\sigma_1^{(k)}) \tag{5.14}$$

and phase-flip channels (dephasing channels),

$$\mathcal{M}_k^P\rho = q\rho + (1-q)\frac{1}{2}(\rho + \sigma_3^{(k)}\rho\sigma_3^{(k)}) \tag{5.15}$$

5.3 Quantum Repeater

For long-distance quantum communication, entanglement purification alone is not sufficient, losses and noise increase exponentially with the distance, thereby limiting the maximal distance to a few hundred kilometers when using photons transmitted through optical fibers. For this reason, in order to achieve the vision of secure quantum communication over arbitrary distances, several schemes have been proposed which either utilize quantum error correction or combine entanglement purification and entanglement swapping, thereby generating high fidelity entangled pairs that can then be used to teleport arbitrary quantum information. Similar to classical communication approach, such schemes can be seen as quantum repeaters.

The basic idea behind quantum repeaters is to split the long channel into smaller segments, and generate short-distance entangled pairs that are purified later to some fidelity F_0. These short-distance pairs are then connected via Bell measurements, which is equivalent to an entanglement swapping, to form an entangled pair of longer distance. For noisy operations, the fidelity of the resulting pairs is reduced, and only a few can be connected in this way. One then uses entanglement purification to re-purify these mid-distance pairs to the working fidelity F_0. When applied to all segments simultaneously, this leaves us with the same situation as initially, except that the distance of the pairs is enlarged. This procedure can than be applied in a nested way, thereby always at least doubling the distance. The required resources, i.e. the number of elementary pairs, increase only polynomial with the distance [46].

Quantum communication between distant parties is based on suitable instances of shared entanglement. For efficiency reasons, in an anticipated quantum network beyond point-to-point communication, it is preferable that many parties can communicate simultaneously over the underlying infrastructure. Sharing of multi-partite entangled states between parties offers a solution, allowing for parallel quantum communication. Specifically for the two-pair problem, the butterfly network provides the first instance of such an advantage in a bottleneck scenario. The underlying method differs from standard repeater network approaches in that it uses a graph state instead of maximally entangled pairs to achieve long-distance simultaneous communication.

As we have seen, the quantum repeater is a scheme that allows for efficient long-distance quantum communication. In a real-world application of quantum communication such as a quantum internet [31], one deals with a multi-user communication network. The network has to be able

to establish high-fidelity long-distance entangled pairs between the nodes but also it has to allow flexible communication between all the partners. Hence, to ensure multi-user communication, any given pair of particles has to be able to share entanglement and communicate to each other. For this purpose, 1D networks are not sufficient since they can only establish bipartite communication. In [44], Dür *et al* proposed a 2D quantum repeater

5.4 Two-dimensional quantum repeater

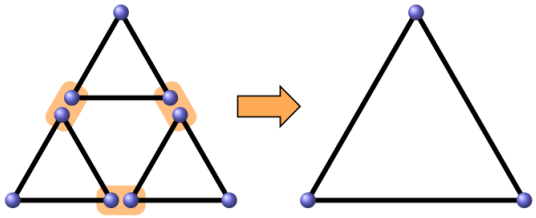

Figure 5.3: 2D repeater architecture based on three-particle GHZ states. Three short-distance GHZ states are connected to form one long-distance GHZ with reduced fidelity. Image taken from [44].

$$\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \otimes \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \otimes \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \tag{5.16}$$

The protocol can be summarized as follows:

1. Start with three copies of a (probably noisy) GHZ state.
2. Perfom Bell measurements on labeled qubits (2,6), (3,8), (5,9) (see Figure 5.4)
3. Depending on the outcomes of the Bell measurements, perform correction operations on remaining qubits 1,4 and 7.

The resulting state after performing Bell measurements I, II, III on qubits (2,6), (3,8) and (5,9), respectively is:

$$(|000\rangle + |111\rangle) \otimes |\phi^{\pm}\rangle \otimes |\phi^{\pm}\rangle \otimes |\phi^{\pm}\rangle \tag{5.17}$$
$$+(|001\rangle + |110\rangle) \otimes |\phi^{\pm}\rangle \otimes |\psi^{\pm}\rangle \otimes |\psi^{\pm}\rangle \tag{5.18}$$
$$+(|010\rangle + |101\rangle) \otimes |\psi^{\pm}\rangle \otimes |\phi^{\pm}\rangle \otimes |\psi^{\pm}\rangle \tag{5.19}$$
$$+(|100\rangle + |011\rangle) \otimes |\psi^{\pm}\rangle \otimes |\psi^{\pm}\rangle \otimes |\phi^{\pm}\rangle \tag{5.20}$$

Therefore,

Bell I	Bell II	Bell III	Correction
$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\mathbb{I}$
$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$X^{(1)}$
$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(4)}$
$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(7)}$

Table 5.3: Table of corrections for the four different measurements patterns.

Notice that we only need two of the three Bell measurements to connect the three GHZ states. The third measurement does not only make the protocol symmetric but can actually be used to detect some specific errors. As it will be described below, error syndromes are not unique and therefore it is not possible to correct the errors detected but it allows us to discard the cases with errors and obtain better error thresholds. However, this also means that the connection procedure only works probabilistically, and the whole procedure has to restart from the beginning if errors are detected.

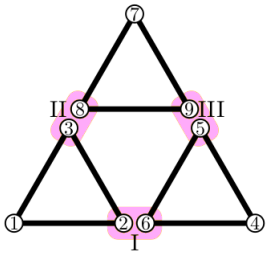

Figure 5.4: Repeater scheme connecting protocol based on Bell measurements.

We can distinguish two sets of qubits: qubits not involved in Bell measurements $\{1, 4, 7\}$, which remain in the next level of the quantum repeater and qubits involved in Bell measurements $\{2, 3, 5, 6, 8, 9\}$ which vanish. To carry out the error handling procedure we consider only single-qubit errors: bit-flip errors or error in x-basis, phase-flip errors or error in z-basis and combination of both.

Consider a bit-flip error in the set of qubits $\{1, 4, 7\}$.

Bell I	Bell II	Bell III	Error in 1	Error in 4	Error in 7
$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$X^{(1)}$	$X^{(4)}$	$X^{(7)}$
$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$X^{(1)}$	$X^{(4)}$	$X^{(7)}$
$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(1)}$	$X^{(4)}$	$X^{(7)}$
$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(1)}$	$X^{(4)}$	$X^{(7)}$

Table 5.4: Table of corrections for a bit-flip error in qubits located at 1,4 or 7.

Therefore, we see that not only the error syndromes are the same but they coincide with the measurement results with no error(see Table 5.3). We cannot distinguish between the Bell measurements pattern, either there is no error or one bit-flip error and if we apply one of the correction operations there is a probability of $\frac{1}{4}$ of success.

Now, we consider a bit-flip error in connection qubits. First, despite there are 6 remaining qubits, measurement patterns are the same for the two qubits involed in the same Bell measurement, then we only need to consider three different cases.

Bell I	Bell II	Bell III	Error BM I	Error BM II	Error BM III
$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\mathbb{I}$	$X^{(1)}$	$X^{(4)}$
$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$X^{(1)}$	$\mathbb{I}$	$X^{(7)}$
$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(4)}$	$X^{(7)}$	$\mathbb{I}$
$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(7)}$	$X^{(4)}$	$X^{(1)}$

Table 5.5: Table of corrections for a bit-flip error in qubits located at (2,6), (3,8) and (5,9).

Error syndromes are the same, for each measurement outcome there is a set of three correction operations, therefore if we apply one of the correction operations there is a probability of $\frac{1}{3}$ of success.

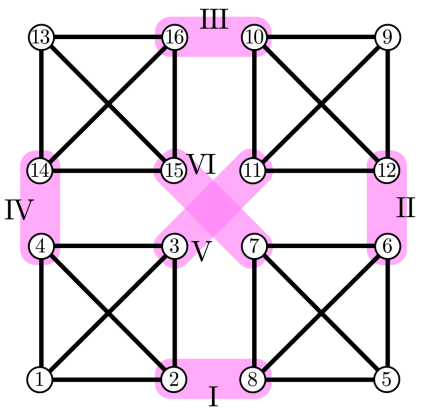

Figure 5.5: Repeater scheme using four GHZ states of four particles.

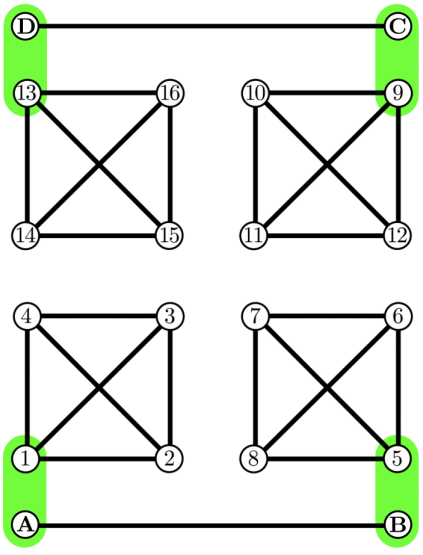

Figure 5.6: .

Appendix A

Tables GHZ4

Bell I	Bell II	Bell III	Bell IV	Bell V	Bell VI	Correction
$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\mathbb{I}$
$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(13)}$
$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$X^{(9)}$
$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(9)}X^{(13)}$
$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(5)}$
$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$X^{(5)}X^{(13)}$
$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(5)}X^{(9)}$
$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$X^{(1)}$

Table A.1: Table of corrections for no error.

Bell I	Bell II	Bell III	Bell IV	Bell V	Bell VI	Error in 1	Error in 5	Error in 9	Error in 13
$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$X^{(1)}$	$X^{(5)}$	$X^{(9)}$	$X^{(13)}$
$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(1)}X^{(13)}$	$X^{(5)}X^{(13)}$	$X^{(9)}X^{(13)}$	$\mathbb{I}$
$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$X^{(1)}X^{(9)}$	$X^{(5)}X^{(9)}$	$\mathbb{I}$	$X^{(9)}X^{(13)}$
$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(5)}$	$X^{(1)}$	$X^{(13)}$	$X^{(9)}$
$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(1)}X^{(5)}$	$\mathbb{I}$	$X^{(5)X^{(9)}}$	$X^{(5)X^{(13)}}$
$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$X^{(9)}$	$X^{(13)}$	$X^{(1)}$	$X^{(5)}$
$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(13)}$	$X^{(9)}$	$X^{(5)}$	$X^{(1)}$
$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\mathbb{I}$	$X^{(1)}X^{(5)}$	$X^{(1)}X^{(9)}$	$X^{(1)}X^{(13)}$

Table A.2: Table of corrections for a bit-flip error in qubits 1,5,9 and 13.

Bell I	Bell II	Bell III	Bell IV	Bell V	Bell VI	Correction
$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\mathbb{I}$
$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(13)}$
$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$X^{(9)}$
$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(9)}X^{(13)}$
$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(5)}$
$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$X^{(5)}X^{(13)}$
$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(5)}X^{(9)}$
$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$X^{(1)}$

Table A.3: Table of corrections for a bit-flip error in qubits involved in Bell measurement I, (2,8).

Bell I	Bell II	Bell III	Bell IV	Bell V	Bell VI	Correction
$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\mathbb{I}$
$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(13)}$
$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$X^{(9)}$
$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(9)}X^{(13)}$
$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(5)}$
$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$X^{(5)}X^{(13)}$
$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(5)}X^{(9)}$
$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$X^{(1)}$

Table A.4: Table of corrections for a bit-flip error in qubits involved in Bell measurement II, (6,12).

Bell I	Bell II	Bell III	Bell IV	Bell V	Bell VI	Correction
$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\mathbb{I}$
$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(13)}$
$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$X^{(9)}$
$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(9)}X^{(13)}$
$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(5)}$
$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$X^{(5)}X^{(13)}$
$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(5)}X^{(9)}$
$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$X^{(1)}$

Table A.5: Table of corrections for a bit-flip error in qubits involved in Bell measurement III, (10,16).

Bell I	Bell II	Bell III	Bell IV	Bell V	Bell VI	Correction
$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\mathbb{I}$
$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(13)}$
$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$X^{(9)}$
$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(9)}X^{(13)}$
$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(5)}$
$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$X^{(5)}X^{(13)}$
$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(5)}X^{(9)}$
$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$X^{(1)}$

Table A.6: Table of corrections for a bit-flip error in qubits involved in Bell measurement IV, (4,14).

Bell I	Bell II	Bell III	Bell IV	Bell V	Bell VI	Correction
$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\mathbb{I}$
$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(13)}$
$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$X^{(9)}$
$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(9)}X^{(13)}$
$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(5)}$
$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$X^{(5)}X^{(13)}$
$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(5)}X^{(9)}$
$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$X^{(1)}$

Table A.7: Table of corrections for a bit-flip error in qubits involved in Bell measurement V, (3,11).

Bell I	Bell II	Bell III	Bell IV	Bell V	Bell VI	Correction
$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\mathbb{I}$
$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$X^{(13)}$
$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(9)}$
$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$X^{(9)}X^{(13)}$
$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$X^{(5)}$
$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$X^{(5)}X^{(13)}$
$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\phi^{\pm}$	$X^{(5)}X^{(9)}$
$\psi^{\pm}$	$\phi^{\pm}$	$\phi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$\psi^{\pm}$	$X^{(1)}$

Table A.8: Table of corrections for a bit-flip error in qubits involved in Bell measurement VI, (7,15).

Bibliography

[1] A. Einstein, B. Podolsky and N. Rosen, Phys. Rev. **47** 777 (1935).

[2] E. Schrödinger, Naturwissenschaften **23** 807, 823, 844 (1935).

[3] J.S. Bell, Physics **1** 195 (1964).

[4] A. Aspect, P. Grangier and G. Roger, Phys. Rev. Lett. **47** 460 (1981).

[5] B. Hensen *et al*, Nature **526** 682-686 (2015).

[6] The BIG Bell Test Collaboration, *Challenging local realism with human choices*, Nature **557** 212-216 (2018).

[7] C.H. Bennet and G. Brassard, International Conference on Computers, Systems and Signal proccesing, **175** 8 (1984).

[8] A.K. Ekert, Phys. Rev. Lett **67** 661 (1991).

[9] C.H. Bennet and S.J. Wiesner, Phys. Rev. Lett **69** 2881 (1992).

[10] C.H. Bennet *et al*, Phys. Rev. Lett. **70** 1895 (1993).

[11] H. Singh, D.L. Gupta and A.K. Singh, IOSR Journal of Computer Engineering Volume 16, Issue 2, Ver. XI (2014).

[12] R. Raussendorf, D. E. Browne, and H. J. Briegel, Phys. Rev. A **68** 022312 (2003).

[13] H. J. Briegel and R. Raussendorf, Phys. Rev. Lett. **86** 910 (2001).

[14] R. Diestel, *Graph Theory*, Springer, Heidelberg, (2000).

[15] M. Hein, J. Eisert and H.J. Briegel, Phys. Rev. A **69** 062311 (2004).

[16] M. Van den Nest, J. Dehaene and B. De Moor, Phys. Rev. A **69** 022316 (2004).

[17] G. Vidal, Phys. Rev. Lett. **91** 147902 (2003).

[18] M. Hein, W. Dür, J. Eisert, R. Raussendorf, M. Van den Nest and H.J. Briegel arXiv:quant-ph/0602096v1 (2006).

[19] A. Peres, Phys. Rev. Lett. **77** 1413–1415 (1996).

[20] M. Horodecki, P. Horodecki and R. Horodecki, Phys. Lett. A **223** 1-8 (1996).

[21] M.D. Choi, Can. J. Math **3** 520 (1972).

[22] A. Jamiołkowski, Rep. Math. Phys. **3** 275 (1972).

[23] D. Bruß, J.I. Cirac, P. Horodecki, F. Hulpke, B. Kraus, M. Lewenstein, and A. Sanpera, Journal of Modern Optics **49** 1399 (2002).

[24] M. Lewenstein, B. Kraus, J. I. Cirac and P. Horodecki, Phys. Rev. A **62** 052310 (2000).

[25] G. Vidal, arXiv:quant-ph/9807077v2 (1999).

[26] M.B. Plenio and S. Virmani, arXiv:quant-ph/0504163v3 (2006).

[27] D. Bouwmeester *et al*, Nature **390** 575 (1997).

[28] A. Furusawa *et al*, Science **282** 706 (1998).

[29] M.D. Barrett *et al*, Nature **429** 737 (2004).

[30] J.F. Sherson *et al*, Nature **443** 557 (2006).

[31] H.J. Kimble, Nature **453** 1023 (2008).

[32] M.A. Nielsen and I.L. Chuang, *Quantum computation and information*, Cambridge University Press, Cambridge (2000).

[33] D. Gottesman, *Stabilizer codes and quantum error correction*, PhD thesis, Caltech, (1997).

[34] P.W. Shor, Phys. Rev. A **52** R2493 (1995).

[35] A.M. Steane, Phys. Rev. Lett. **77** 793 (1996).

[36] R. Laflamme, C. Miquel, J.P. Paz, and W.H. Zurek, Phys. Rev. Lett. **77** 198 (1996).

[37] E. Knill, Nature **434** 39 (2005).

[38] C.H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin and W. K. Wootters, Phys. Rev. Lett. **76** 722 (1996).

[39] D. Deutsch, A. Ekert, R. Josza, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77** 2818 (1996).

[40] W. Dür and H. J. Briegel, Rep. Prog. Phys. **70** 1381 (2007).

[41] W. Dür, H. Aschauer, H.-J. Briegel, Phys. Rev. Lett. **91** 1079031 (2003).

[42] H. Aschauer, W. Dür, H.-J. Briegel, Phys. Rev. A **71** 012319 (2005).

[43] R.F. Werner, Phys. Rev. A **40** 4277 (1989).

[44] J. Wallnöfer, M. Zwerger, C. Muschik, N. Sangouard and W. Dür, arXiv:1604.05352 [quant-ph] (2016).

[45] J.C. Garcia-Escartin and P. Chamorro-Posada, arXiv:1110.2998v1 [quant-ph] (2011).

[46] H.J. Briegel, W. Dür, J.I. Cirac, and P. Zoller, Phys. Rev. Lett. **81** 5932 (1998).

[47] W. Dür, H.J. Briegel, J.I. Cirac and P. Zoller, Phys. Rev. A **60** 725 (1999).

[48] G. Uchida, R.A. Bertlmann and B.C. Hiesmayr, arXiv:1410.7145 [quant-ph] (2014).

[49] M. Zwerger, W. Dür and H.J. Briegel, arXiv:1204.2178 [quant-ph] (2012).

[50] M. Zwerger, H.J. Briegel and W. Dür, arXiv:1506.00985v1 [quant-ph] (2015).

[51] J. Wallnöfer, A. Pirker, M. Zwerger and W. Dür, arXiv:1806.11562v1 [quant-ph] (2018).

[52] A. Dahlberg and S. Wehner, Phil. Trans. R. Soc. A **376** 0325 (2018).

[53] W. Dür, M. Hein, J.I. Cirac and H.J. Briegel, Phys. Rev. A **72** 052326 (2005).