



---

# Towards percolation-based quantum computing with a photonic machine gun

MASTER'S THESIS

Iñigo Lara Izcue

Supervised by  
Anders Søndberg Sørensen

May 20<sup>th</sup> 2021

# Abstract

For the last 40 years, the field of quantum technologies has expanded and incorporated fascinating approaches to overcome the difficulties regarding the operation and scalability of quantum operations. Among these ideas is *Measurement-Based Quantum Computing*, an alternative point of view in which a highly entangled resource state is grown at first, and the quantum computation is simulated by disentangling such state through single-qubit measurements. This approach suits perfectly optical systems, as these can provide thousands of entangled qubits encoded in photons. However, among the challenges, it is the initial creation of such highly-entangled resource in a scalable way.

In this thesis a theoretical overview of the different ingredients to implement *Measurement-based Quantum Computing* is presented: small entangled states such as GHZ states and linear clusters are created on-demand in a time-bin encoding using the spin dynamics and optical transitions of a solid state Quantum Dot (QD), that shall be called the *photonic machine gun*. These small entangled states, with less than tens of qubits, can then be entangled together probabilistically using *fusion gates*, that can be implemented with integrated linear-optics circuits. Under certain circumstances, it is possible that these probabilistic operations yield a scalable highly-entangled state through a percolation process.

This thesis studies and analyses entanglement percolation over a cubic lattice. It is determined that the protocol proposed can tolerate up to 10% photon loss, is ballistic and heralded. Furthermore, an improved version of a fusion gate called *Dynamic Type-II* which can be boosted to, e.g. 75% success while having a photon loss tolerance of 5%. The protocol for percolation-based quantum computing analyzed generates a graph state over the spin QD qubits, which means that the grown entangled state is stored in the solid-state QDs until the measurement-based computation is ready to start, therefore avoiding the need for quantum memories. Finally, it is shown a blueprint of a percolation-based quantum computer that puts together the different blocks discussed through the thesis.

In short, this thesis serves as a natural path towards implementing *Fusion-Based Quantum Computing* with the *photonic machine gun* system.

---

# Acknowledgements

I am one of those hectic paced minds that truly appreciate and value chaos; not for the chaos itself, but for the astonishing images that usually arise afterwards. After a cornerstone as important as the ending of a thesis, it's natural to sit down and look back at things you don't appreciate when you are immerse in the flow of things. First of all, I look back and I realise that I am were I wanted to be years in the past. And second of all, I look around and I see an eclectic set of people that are definitely the cause behind what I am at the moment. It's easy to forget how subtle is the equilibrium behind well-being, and that is why I want to thank all of them.

Thanks, first of all, to my parents. For all the background and the emotional and material support. But thanks over all for having faced me with myself and having unveiled my many contradictions. It is by contradictions that I believe we grow, so this is the most someone can do for someone else.

Thanks, second of all, to Anders. For his infinite patience and wise advice. You certainly helped me discover what I want, and brought back my illusion for research and physics. Of course, thanks to all the Hy-Q people and the Niels Bohr Institute environment for being such an empowering place.

Thanks, last but most, to all my friends and beloved ones around. It's endlessly enriching having all this German, Finnish, Danish, Norwegian, Serbian, Dutch, Luxemburgois, Italian and Spanish people minds by me. Thanks for all the questions, for all the talks, for all your fresh ideas and different of points of view, and for all the music and for all the slepless nights and days. Thanks for brightening me with your intelligence.

Once I heard that an artist is someone able to find inspiration, even at work. I am not an artist, so I can just thank you for inspiring me when I could not find inspiration at all. A main share of my results are also yours.

---

# Contents

<b>1</b>	<b>The circuit model and beyond</b>	<b>1</b>
1.1	Qubits in the circuit model . . . . .	1
1.1.1	The SWAP test . . . . .	3
1.1.2	Phase Kickback . . . . .	4
1.2	Deutsch algorithm . . . . .	5
1.2.1	Oracles & 1D binary Sudoku . . . . .	7
1.3	Beyond the circuit model . . . . .	8
1.3.1	The Stabilizer formalism . . . . .	8
1.3.2	Multi-particle entangled states . . . . .	9
<b>2</b>	<b>Linear Optics &amp; The Photonic Machine Gun</b>	<b>11</b>
2.1	Encoding qubits in light . . . . .	11
2.1.1	Overview of the different encodings . . . . .	11
2.2	Optical Quantum Gates . . . . .	13
2.2.1	N-mode Interferometer . . . . .	15
2.2.2	The KLM solution . . . . .	16
2.3	Working with other encodings . . . . .	16
2.3.1	Polarization encoding . . . . .	17
2.3.2	Time-bin encoding . . . . .	18
2.4	Integrated optics . . . . .	19
2.5	A Quantum Dot as a Photonic Machine Gun. . . . .	20
2.5.1	The physical system . . . . .	21
2.5.2	Electronic levels structure . . . . .	21
2.5.3	Spin dynamics . . . . .	22
2.5.4	Pulse sequences . . . . .	22
2.6	Concatenating pulse sequences . . . . .	26
<b>3</b>	<b>Measurement Based Quantum Computing</b>	<b>27</b>
3.1	From Gates to Measurements: Gate Teleportation . . . . .	27
3.1.1	Clifford Gates . . . . .	29
3.1.2	Limitations of Clifford Circuits: The Gottesman-Knill theorem . . . . .	31
3.1.3	Two-qubit gates in MBQC . . . . .	31
3.1.4	Building blocks for MBQC . . . . .	32
3.1.5	Graphical language . . . . .	35

<b>4</b>	<b>Merging clusters with Fusion Gates</b>	<b>37</b>
4.1	Merging clusters together . . . . .	37
4.1.1	Type-I fusion . . . . .	39
4.1.2	Type-II fusion . . . . .	41
4.1.3	Bell-State Measurement (BSM) . . . . .	42
4.2	Modified Type-II fusion gates . . . . .	44
4.2.1	Boosted Type-II fusion . . . . .	44
4.2.2	Rotated Type-II fusion gates . . . . .	45
<b>5</b>	<b>Towards Fusion-Based Quantum Computing</b>	<b>47</b>
5.1	Improved Type-II with no ancillary resources . . . . .	47
5.1.1	Photon losses for the Dynamic Type-II . . . . .	48
5.2	Percolation theory & how to use it . . . . .	49
5.3	Growing a percolating lattice . . . . .	50
5.3.1	The protocol . . . . .	51
5.3.2	The simulations . . . . .	51
5.3.3	Taking losses into account . . . . .	52
<b>6</b>	<b>Conclusion and outlook</b>	<b>55</b>
6.1	A blueprint for a percolation-based quantum computer . . . . .	55

# Chapter 1

## The circuit model and beyond

“And I am not happy with all the analyses that go with just the classical theory, because nature isn’t classical, dammit, and if you want to make a simulation of nature, you’d better make it quantum mechanical, ...”

---

R.P. Feynman, 1981, *Simulating Physics with computers* (Ref. [14]).

The aim of this chapter is to revisit the basics of quantum computing in the context of the circuit model in order to establish the notation and the theoretical tools that will be used later on in the thesis: the Bloch Sphere model is introduced as a way to reason about quantum operations, and two useful circuits are described. Deutsch algorithm for the 2-qubit case is explained, as this will serve to introduce some ideas and ways of reasoning about quantum circuits, useful for the incoming chapters.

### 1.1 Qubits in the circuit model

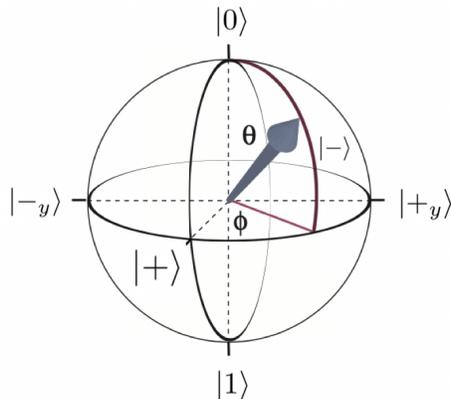
A Quantum Computer works by processing information stored in physical carriers with explicit quantum behaviour. These then undergo a series of unitary evolutions and measurements. The unit of quantum information is the *qubit*<sup>1</sup>. A Quantum algorithm is a recipe that describes how to apply transformations to a set of qubits in order to process the information in a meaningful way.

Qubits can take two perfectly distinguishable states that are usually called the logical states or the computational basis,  $\{|0\rangle, |1\rangle\}$ , like a classical bit. However, a qubit being the Quantum version of a bit means that it can also be in an arbitrary superposition of both computational states, denoted as  $\alpha|0\rangle + \beta|1\rangle$  (with  $|\alpha|^2 + |\beta|^2 = 1$ ). A visual representation of the states of a qubit is The Bloch Sphere, pictured in Figure 1.1.

Single-qubit states  $|\psi\rangle$  lie in the surface of the Bloch Sphere due to normalization ( $\langle\psi|\psi\rangle = 1$ ). Unitaries are transformations over states that conserve normalization ( $\langle\psi|U^\dagger U|\psi\rangle = \langle\psi|\psi\rangle = 1$ ). Therefore, they can be seen as movements over the surface of the Bloch Sphere. Indeed the transformations applied to single-qubit states are of a special type called  $SU(2)$ . Thanks to the connection  $SU(2) \leftrightarrow SO(3)$  [31], any  $SU(2)$  transformation can be seen as a rotation in a 3D space. Technically,

---

<sup>1</sup>Generalizations exist in the form of *qudits*, d-levels systems. For example, linear optics has been for arbitrary qudits (See S. Paesani *et al.* in Ref. [30])



**Figure 1.1** Bloch Sphere. Any general qubit state  $|\psi\rangle = \cos(\theta/2)|0\rangle + \sin(\theta/2)e^{i\phi}|1\rangle$  can be parametrized by two angles  $\{\theta, \phi\}$ . Orthogonal states like  $\langle 0|1\rangle = 0$  lie opposite to each other. The eigenstates along the directions  $X$ ,  $Y$  and  $Z$  are shown. These are  $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ , along the  $X$  axis; and  $|\pm_y\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm i|1\rangle)$ , along the  $Y$  direction.

the correspondence is not perfectly bijective but 2-to-1<sup>2</sup>. Therefore, any single qubit transformation (up to a global phase) can be visualized as a rotation with 3 parameters, like the 3 Euler angles, or alternatively as an axis of rotation and a rotation angle.

However, single-qubit states are of very few interest as they can be efficiently simulated in any computer. It is when we consider  $n$ -qubit states when non-classical properties such as entanglement arise. An evolution of a  $n$ -qubit state is described by a  $SU(n)$  matrix. A set of gates is said to be *universal* if any  $SU(n)$  can be boiled down to a series of these. For example, single qubit rotations plus an entangling gate such as CNOT are an universal set, as proven by Nielsen and Chuang section 4.5 (Ref. [25]).

The last ingredient to consider are measurements. In contraposition to quantum gates, measurements are just the opposite: irreversible, non-deterministic and discontinuous. Much more about measurement will be said in following chapters, so for now it is enough to take it as an irreversible step in the evolution of states in which part of the system collapses. For example, an state  $\alpha|0\rangle + \beta|1\rangle$  being measured in the computational basis collapses to the state  $|0\rangle$  with probability  $|\alpha|^2$ .

With all this formalism in hand, a definition of the circuit model can be shown: The circuit model pictures the time evolution of a quantum state as a sequence of unitary gates and measurements. An example is the SWAP test, shown in Figure 1.2 and to be discussed later.

The fact that the gates used in Quantum Circuit are unitaries ( $U^\dagger = U^{-1}$ ) means that every step is be reversible (except, of course, the measurement).

In the following two sections the circuit model is introduced through some examples. The first of all is the SWAP test, a circuit to compute the fidelity between two states; the second one is Phase Kickback, a way to reason about conditioned-unitaries that helps get a better insight on how Deutsch algorithm. They serve as a way to introduce notation and some basic ideas.

<sup>2</sup>This is the reason why angles in the Bloch Sphere are doubled: why opposite is orthogonal and why the identity operation is not a  $2\pi$  rotation but a  $4\pi$  one. Intuition over this effect can be gained with the Philippine wine dance video.

### 1.1.1 The SWAP test

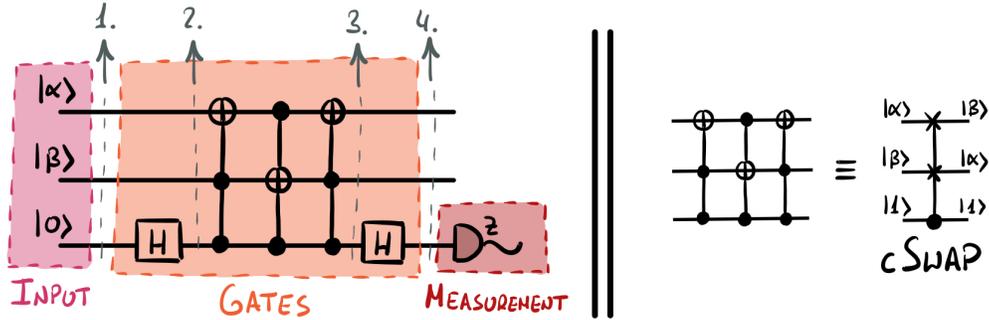
A Quantum Circuit important to measure the fidelity of quantum states is the SWAP test. Its circuit model representation is shown in Figure 1.2.

It is useful because it allows to compute the fidelity between the states  $|\alpha\rangle$  and  $|\beta\rangle$ , this is  $F = |\langle\alpha|\beta\rangle|^2$  by performing a single-qubit measurement over an ancilla qubit. As we will show, it happens that

$$\mathcal{P}(\text{ancilla} = 0) = \frac{1}{2} \left( 1 + |\langle\alpha|\beta\rangle|^2 \right)$$

But first things first, let's briefly discuss the circuit model: It is one of the many ways to picture the evolution of the wavefunction in a Quantum Computation. The order of events goes from left to right, and one can identify 3 stages in the evolution: Input of states into the circuit, the application of gates, which, as discussed earlier are a set of unitaries, and measurements in a certain basis at the end, which represent a non-unitary, and thus irreversible, process. Note that one can always respect this structure by shifting the measurements to the end<sup>3</sup>

When analysing quantum circuits it is useful to take a look at different moments of the evolution (1. 2. 3. and 4. in Figure 1.2).



**Figure 1.2** On the left, the SWAP test represented in the circuit model; on the right, a Controlled-SWAP operation is implemented with three CCNOT gates or *Toffoli* gates, applied upon the ancillary lower qubit.

1. The the input is:  $|\alpha\rangle |\beta\rangle |0\rangle$
2. After the first Hadamard gate, the state is  $\frac{1}{\sqrt{2}} \left( |\alpha\rangle |\beta\rangle |0\rangle + |\alpha\rangle |\beta\rangle |1\rangle \right)$
3. The three Controlled-Controlled-NOT Gates (or *Toffoli* Gates) constitute what is called c Controlled-SWAP operation. SWAP gates acts as  $\text{SWAP } |\alpha\rangle |\beta\rangle = |\beta\rangle |\alpha\rangle$ .

$$\frac{1}{\sqrt{2}} \left( |\beta\rangle |\alpha\rangle |0\rangle + |\beta\rangle |\alpha\rangle |1\rangle \right)$$

At this point, one might wonder how can the SWAP gate not contradict the No-Cloning theorem. Technically speaking, one can check that the SWAP operation is a valid gate because it is invertible ( $\text{SWAP} \cdot \text{SWAP } |\alpha\rangle |\beta\rangle = |\alpha\rangle |\beta\rangle$ ) and Hermitian ( $\text{SWAP} = \text{SWAP}^\dagger$ ), and therefore Unitary ( $\text{SWAP}^{-1} = \text{SWAP}^\dagger$ ). In loose words, one can understand this as there is no information gain in the application of the SWAP gate, allowing reversibility and therefore constituting a valid Quantum Gate. This way of reasoning works as well to disprove a *cloning*

<sup>3</sup>This is a result of the Deferred Measurement Principle, see Nielsen and Chuang (Ref. [25]).

operation, that should have the form, if existed, of  $\text{CLONE}|\alpha\rangle|\phi\rangle \stackrel{?}{=} |\alpha\rangle|\alpha\rangle$ . One can see that the information about the state  $|\phi\rangle$  is lost in the process. This avoids reversibility and disproves the cloning operation.

4. After the last Hadamard:

$$\frac{1}{2} \left( |\beta\rangle|\alpha\rangle|0\rangle + |\alpha\rangle|\beta\rangle|1\rangle + |\beta\rangle|\alpha\rangle|0\rangle - |\alpha\rangle|\beta\rangle|1\rangle \right) =$$

$$\frac{1}{\sqrt{2}} \left( |\beta\rangle|\alpha\rangle + |\alpha\rangle|\beta\rangle \right) |0\rangle + \frac{1}{\sqrt{2}} \left( |\beta\rangle|\alpha\rangle - |\alpha\rangle|\beta\rangle \right) |1\rangle$$

Finally, the measurement of the ancilla qubit in the computational basis projects the state onto the  $\{|0\rangle, |1\rangle\}$ . Taking the measurement outcome of  $|0\rangle$  one sees that:

$$\mathcal{P}(\text{ancilla} = 0) = \frac{1}{2} \left( \langle\beta|\langle\alpha| + \langle\alpha|\langle\beta| \right) \frac{1}{2} \left( |\beta\rangle|\alpha\rangle + |\alpha\rangle|\beta\rangle \right) = \frac{1}{2} \left( 1 + |\langle\alpha|\beta\rangle|^2 \right)$$

The SWAP test is generalizable to compute the fidelity between multi-qubit states. To do so, it is needed a Control-SWAP operation that swaps every pair of qubits as in  $|ijk\rangle \otimes |\alpha\beta\gamma\rangle \xrightarrow{\text{CSWAP}} |\alpha\beta\gamma\rangle \otimes |ijk\rangle$ , where  $|***\rangle = |*\rangle|*\rangle|*\rangle$  and  $|*\rangle$  take values in the computational  $\{|0\rangle, |1\rangle\}$  basis.

### 1.1.2 Phase Kickback

The global phase in a wavefunction is usually a disregarded quantity because it cannot be measured as it has no observable associated. However, under certain circumstances it becomes relevant and causes noticeable changes in the evolution of states<sup>4</sup>.

Phase Kickback is a technique in which the phase induced by a certain gate is transferred to another qubit, effectively changing the quantum state and becoming observable. It is said that the global phase is *kicked-back to another of the qubits*.

It is said that two wavefunctions are identical up to a global phase are equivalent, and we note this fact as  $|\psi\rangle \cong e^{i\phi} |\psi\rangle$ , where " $\cong$ " means that both lead to the same measurement results<sup>5</sup>. In terms of circuits, this means that applying local phases to different qubits just accumulates as a global phase that has no physical implications, and thus can be disregarded. A picture of this effect can be seen in Figure 1.3, where we have used unitaries and their corresponding eigenvectors, such that  $U_k |\psi_k\rangle = e^{i\phi_k} |\psi_k\rangle$

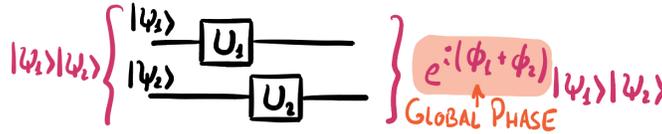


Figure 1.3 Global phases are factored and have no effect.

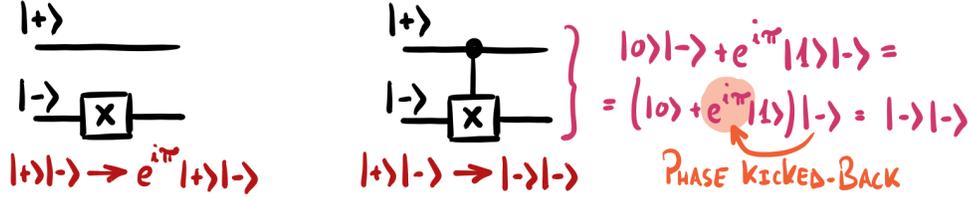
This might appear a bit strange at first sight: qubits are accumulating differences in phase one with respect to each other. Why would they dissolve into a global phase? Well, as there is no interaction between them, these transformations remain local and thus can be factored into a global phase.

An example of this behaviour can be seen with Pauli  $X$  gate when it operates over its eigenvector  $|-\rangle$ ; this is  $X|-\rangle = e^{i\pi} |-\rangle$ . In normal circumstances the  $e^{i\pi}$  phase gets factors as a global phase,

<sup>4</sup>An example of this is the Aharonov-Bohm effect.

<sup>5</sup>This fact is called  $\mathcal{U}(1)$  symmetry or global Gauge symmetry.

as in  $(\mathbb{1} \otimes X) |1\rangle |-\rangle = e^{i\pi} |+\rangle |-\rangle$ . However, if  $X$  is applied in a controlled manner (say, as a Controlled- $X$  gate), phase-kickback happens. This is shown in Figure 1.4.



**Figure 1.4** The phases added by  $X$  onto its eigenvector  $|-\rangle$  is *kicked-back* onto the top qubit through the controlled application of the gate.

The kickback refers to the fact that the eigenvalue added by a gate is kicked-back into a different qubit via a controlled operation. As a result, the eigenvalue has a measurable effect.

Another name for the Controlled- $X$  Gate is CNOT. What the circuit shown in Fig.1.4 means is:

$$\text{CNOT} |+\rangle |-\rangle = |-\rangle |-\rangle$$

In this example phase-kickback might seem something seem obvious and cumbersome, but it is a powerful tool to build more complex algorithms such as the Phase Estimation algorithm (Ref. [29]), Grover’s Search or Deutsch algorithm, the former to be discussed later in this chapter.

## 1.2 Deutsch algorithm

Around 1985 Quantum Computing was still in his early days when D. Deutsch proposed one of the first Quantum Algorithms. It exploits parallelism and superposition in QM to solve a *decidability* problem: given an function that can be of 2 definite types, identify it by analyzing the outcomes of its evaluations. If we define the complexity of an algorithm as the number of evaluations, or *queries* needed before a decision is made with certainty, Deutsch algorithm is better than any classical strategy.

The set functions considered are of a special type: they have to be binary functions with a binary output. Let

$$f : \{0, 1\} \longrightarrow \{0, 1\}$$

be a function that is either *constant* or *balanced*, meaning that that it either maps every input to the same output or half of the inputs to half to 0 and half to 1, respectively.

Classically the strategy involves evaluating 2 queries:  $f(0)$  and  $f(1)$ . Then, the decision can be made according to  $f(0) \oplus f(1) = 0$  in the constant case or  $f(0) \oplus f(1) = 1$  in the balanced case, where  $\oplus$  denotes addition modulo 2. The quantum strategy depicted by Deutsch just requires 1 query of  $f(x)$ .

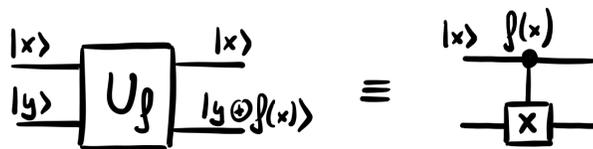
In order to use  $f(x)$  in a Quantum algorithm, it has to be embedded in a gate form. A convenient way is to insert it in a unitary  $U_f$  that behaves as:

$$U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$$

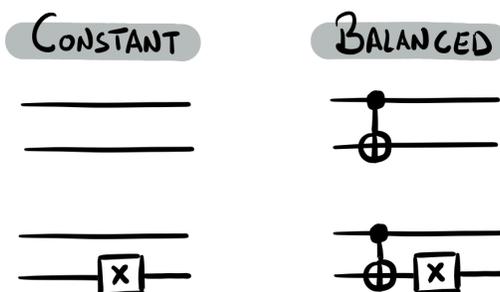
Defined in this way and setting  $|y\rangle = 0$   $U_f |x\rangle |0\rangle = |x\rangle |f(x)\rangle$  while remaining a valid hermitian unitary ( $U_f^{-1} = U_f$  as  $U_f \cdot U_f |x\rangle |y\rangle = |x\rangle |y \oplus f(x) \oplus f(x)\rangle = |x\rangle |y\rangle$ ).

In a graphical way,  $U_f$  can be represented as a conditioned Pauli  $X$  gate:

Deutsch algorithm uses the fact that in the quantum version of  $f(x)$ , which is  $U_f$ , a single query to the oracle is enough to determine  $f(0) \oplus f(1)$ .



**Figure 1.5** Deutsch function implemented as a gate  $U_f$  can be seen as a conditioned- $X$  that is applied if  $f(x) = 1$ . This is because the addition modulo 2 is equivalent to a flip  $|0\rangle \leftrightarrow |1\rangle$ . Note that  $|x\rangle$  and  $|y\rangle$  must be elements of the computational basis for the ket transformations to behave as shown in the figure above.

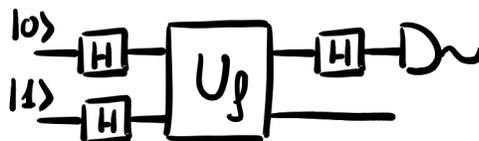


**Figure 1.6** Circuit model of the inside of the unitary  $U_f |x\rangle |0\rangle = |x\rangle |f(x)\rangle$  that implements the four possible  $f(x)$  for the single qubit Deutsch algorithm.

This can be understood using the idea of Phase-Kickback, introduced in the former section. In the lower qubit,  $|-\rangle$  which is the the eigenvector of Pauli  $X$  is used as input. In the upper qubit, an equal superposition of all the possible inputs is used. This is  $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) = |+\rangle$ . As the conditioning depends on  $f(x)$ , the  $(-1)$  phase added by  $X |-\rangle = (-1)|-\rangle$  is kicked-back onto  $|+\rangle$  in a form  $(-1)^{f(x)}$ .

$$|+\rangle |-\rangle \xrightarrow{U_f} \frac{1}{\sqrt{2}} \left( (-1)^{f(0)} |0\rangle + (-1)^{f(1)} |1\rangle \right) |-\rangle \sim \frac{1}{\sqrt{2}} \left( |0\rangle + (-1)^{f(0) \oplus f(1)} |1\rangle \right) |-\rangle$$

A measurement over the upper qubit yields the value of  $f(0) \oplus f(1)$ . In the *constant* case, it is  $|+\rangle$ , while in the *balanced* one is  $|-\rangle$ . These two states can be discriminated with unit probability<sup>6</sup>, because they are orthogonal.

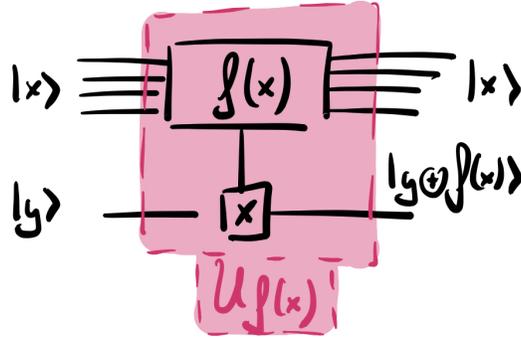


**Figure 1.7** The circuit of the Deutsch algorithm. The Hadamards on the left prepare an equal superposition of every input, on top, and the  $|-\rangle$  state. The Hadamard on the right changes the measurement basis to the  $\{|+\rangle, |-\rangle\}$  states. The bell-shaped symbol indicates a measurement in the  $Z$  basis.

There are other approaches to understand the functioning of Deutsch algorithm, one particularly

<sup>6</sup>The original algorithm by Deutsh allowed for a inconclusive outcome of the measurement. The strategy described in this chapter is due to Cleve, Ekert, Macchiavello and Mosca ([29]).

interesting one can be found in Nielsen and Chuang’s book. However, the one shown here can be easily generalized to the case of a multiple-inputs  $f(x)$ , such as  $f : \{0,1\}^* \rightarrow \{0,1\}$  where  $*$  is the *Kleene star* operator. The generalized version of the problem is solved by the Deutsch-Jozsa algorithm. However, for the purpose of this thesis only the restricted Deutsch algorithm is needed.



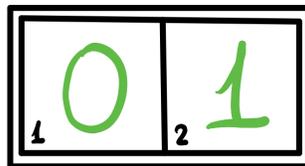
**Figure 1.8** Oracle for the general Deutsch-Jozsa algorithm: now  $f(x)$  takes several inputs and its output controls the application of an X gate.

At this point, it is normal to wonder about the internals of the gate  $U_f$ . Until now, it was just a black box, or an *oracle*. A device that upon certain inputs yields definite (but beforehand unknown) outputs. However, if such a device is to be built, it has to be known the way it transforms inputs to outputs, or in other words, the internal behaviour of  $f(x)$ . In that case, why bother running a complex algorithm such as Deutsch to gain some insight from the observation of the outputs, if we know beforehand how the inputs relate to the outputs?

This question is deeply connected to many topics in computer science, such as one-way functions and the P vs. NP problem. But this is better understood with an example, that is explained in the next section.

### 1.2.1 Oracles & 1D binary Sudoku

Say that a Japanese friend of yours proposed playing a binary version of Sudoku in the following board:



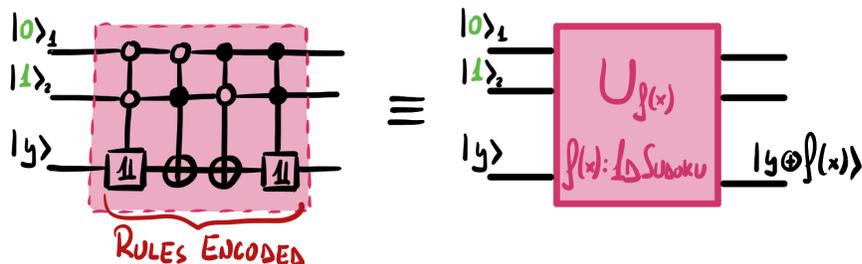
**Figure 1.9** Board for Binary Sudoku. Each box (1 and 2, in black) can take a binary digit (in green). A solution is a combination that does not repeat digits inside the grid.

It consists of a  $1 \times 2$  board that can be filled with binary digits (0 or 1). The rules are simple: you cannot repeat digits inside the board. The solution is pretty obvious and degenerate: both  $|0\rangle_1 |1\rangle_2$  or  $|1\rangle_1 |0\rangle_2$  are solutions. Moreover,  $|0\rangle_1 |0\rangle_2$  and  $|1\rangle_1 |1\rangle_2$  are wrong instances. This game is easy! Note that  $|0\rangle_i$  indicates a state 0 at cell  $i$ .

However, rather than solving the Sudoku with our (limited) intelligence, can we create an Oracle that checks for us whether a solution is valid. As we know what rules a valid solution has to satisfy,

the answer is yes. And we will do in the Quantum way, creating a suitable unitary  $U_{f(x)} |x\rangle |y\rangle = |x\rangle |y \oplus f(x)\rangle$  from these rules.

These rules can be encoded one by one as a table of truth just by using CNOT and  $\overline{\text{CNOT}}$  gates.  $\overline{\text{CNOT}} = X |0\rangle \langle 0| + \mathbb{1} |1\rangle \langle 1|$  is just a version in which the gate is applied if the first qubit is in the  $|0\rangle$  state. The Oracle is shown in Figure 1.10.



**Figure 1.10** Oracle for the 1D Sudoku encoded in a unitary gate.  $f(x) = 1$  if  $|x\rangle$  is a valid solution, encoded in the computational basis.

It is important to realise that when creating the Oracle, we are not encoding the solutions beforehand (how could we, if we don't know them?) but a set of rules to check if an input is a solution. The distinction between deciding if something is a solution and actually solving is paramount in Complexity Theory, and its study is one of the reasons why Alan Turing is so famous<sup>7</sup>.

This situation of an Oracle that can easily check solutions but that does not *know* the solutions relates how nature itself might work. All in all, nature could be seen as a computer following a complex algorithm encoded in the laws of physics, right? Therefore, there might be problems that not even nature could solve efficiently. Indeed, if  $P \stackrel{?}{\neq} NP$  (as it is believed), then there would exist experimental circumstances in which nature is not able to apply the laws of physics efficiently. In other words, the laws of physics, even if right, might not describe the gibberish behaviour of nature.

Scott Aaronson analyses this and other interesting problems regarding nature trying to solve NP-complete problems in Ref. [5].

### 1.3 Beyond the circuit model

The circuit model is a powerful tool to think over algorithms, gates and qubits. However, it is not the only one. Not aiming to get technical or detailed but to motivate alternative points of view, in this section I will highlight two other approaches to think about Quantum Computing.

#### 1.3.1 The Stabilizer formalism

Is a theoretical formalism based on group theory to describe entangled states. Its main results are the Gottesman-Knill theorem (explained later), a versatile tool to build error correction codes (see *toric codes*, e.g.) and a theoretical description of Cluster States.

Given a certain  $n$ -qubit state  $|\psi\rangle$ , a unitary  $g$  that belongs to the Pauli Group<sup>8</sup> is said to stabilize the state  $|\psi\rangle$  if  $g|\psi\rangle = |\psi\rangle$ . If  $|\psi\rangle$  can be stabilized, then it is a result from group theory that a

<sup>7</sup>Alan Turing studied the algorithmic limitations of computers. His results summarize in the Halting Problem, explained in this video.

<sup>8</sup>The  $n$ -Pauli Group  $G_n$  is defined as  $G_n \equiv \{\pm 1, \pm i\} \otimes \{1, X, Y, Z\}^{\otimes n}$ . Its elements are tensor products of  $n$  Pauli matrices. The phases  $\{\pm 1, \pm i\}$  are included to guarantee that the group is closed, as can be seen by the identity  $XYZ = i\mathbb{1}$

subgroup of  $2^n$  elements from the Pauli Group uniquely describes  $|\psi\rangle$ . Moreover, these  $2^n$  element subgroup is spanned from a smaller set of  $n$  generators. A complete descriptions and proof of this results can be found in Refs. [25] and [6].

It is convenient to restrict the unitary  $U$  to be a Clifford type. This means that  $U$  can be decomposed in terms of a series of Hadamard, Phase Gate and Controlled-NOT. In short,  $U$  being a Clifford Gate means that  $UgU^\dagger$  is also a member of the Pauli Group. This restriction comes at a price to pay, because the set  $\{H, S, CNOT\}$  is not universal. In return, this restriction makes the stabilizer formalism a perfect tool to *efficiently* simulate any quantum circuit composed of Clifford Gates.

An evolution of  $|\psi\rangle$  by a unitary Clifford transformation is described in the Circuit Model by  $|\psi\rangle \rightarrow U|\psi\rangle$ . Using stabilizers and the fact that  $U$  is unitary, it can be seen that

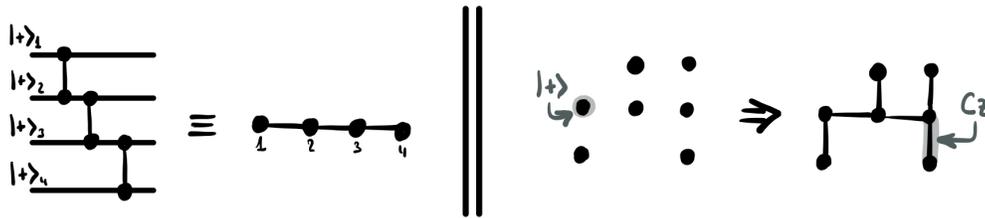
$$U|\psi\rangle = Ug|\psi\rangle = (UgU^\dagger)U|\psi\rangle$$

Which means that  $UgU^\dagger$  stabilizes  $U|\psi\rangle$ , the output state of the evolution. This point of view is similar to the Heisenberg equation of motion, in which it is not the states but the operators that are evolved in time.

### 1.3.2 Multi-particle entangled states

The rest of this thesis is going to build on top of the concept of multi-particle entangled states. Entanglement is a quantum property that describes non-local correlation between measurements over different systems, even if the are non-locally connected. There are many ways to establish entanglement between systems, but all of them require a local interaction. In the language of quantum information, a Controlled-Z gate entangles qubits that are initially in  $|+\rangle$  state. This can be seen in the case  $|+\rangle|+\rangle \xrightarrow{CZ} |0\rangle|+\rangle + |1\rangle|-\rangle$ , given that  $Z|+\rangle = |-\rangle$  is only applied when the first qubit is in  $|1\rangle$ . If the both qubits are now measured, the outcomes will always be either  $\{0, +\}$  or  $\{1, -\}$ .

Indeed, this process can be generalized to a set of qubits initially in  $|+\rangle$  state. A cZ operation may be applied between pairs that want to be entangled. The result is a highly entangled state called Graph State, as can be seen in Figure 1.11.



**Figure 1.11** Representation of a Graph States. On the left, equivalence between the circuit model and the graph state representation; On the right, the growth of a generic Graph State, where each node is a qubit initially in  $|+\rangle$  state, and each bond represents a CZ operation. The order of application is irrelevant, as these commute.

Graph States build a visual intuition over entanglement, which gets clumsy to work with in Dirac notation. The full power of this picture will be unveiled in Chapter 3, where graph states will be used for Measurement-Based quantum computing.

An interesting entangled state is the GHZ state:

## Greenberger–Horne–Zeilinger state (GHZ)

A GHZ state containing  $N$  particles takes the form:

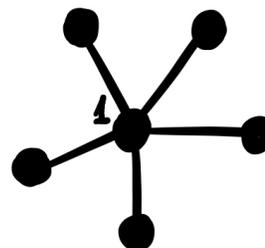
$$|\text{GHZ}^{(N)}\rangle = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N})$$

GHZ states can be seen as a generalization of the Bell States as they are maximally entangled. This is discussed as discussed in Ref. [18].

Moreover, GHZ states can be pictures as Graph States in a star-shape. The graph shown in Figure 1.12 represents a  $|\text{GHZ}^{(6)}\rangle$  state up to a local unitary  $H$  on every qubit except 1. This is:

$$\frac{1}{\sqrt{2}}(|0\rangle_1|+\rangle^{\otimes 5} + |1\rangle_1|-\rangle^{\otimes 5}) \sim |\text{GHZ}^{(6)}\rangle$$

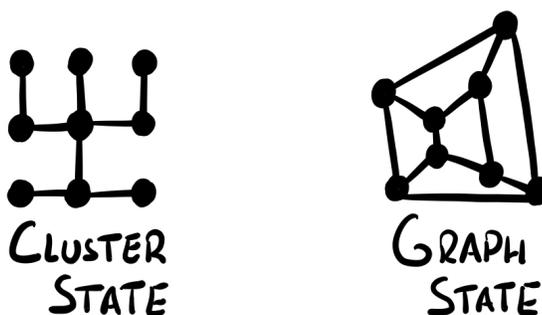
A graphical description of entanglement can be achieved through entanglement graphs. GHZ states have been proposed for Quantum Communication [37] and Quantum Metrology [3], and Cluster States for Measurement-Based Quantum Computing [28]. In this section GHZ and Linear-Cluster States are described.



**Figure 1.12** A 6-qubit GHZ state can be pictured as a star, where the central qubit has been applied a local Hadamard unitary.

## Cluster and Graph states

Both Cluster and Graph States refer to a set of qubits in  $|+\rangle$  entangled through Controlled-Z operations. The difference is in the topology of the lattices: In cluster states, the nodes take a square or cubic disposal, and the entanglement are between first order neighbours; Graph States are a generalization, taking any geometry. For example, see Figure 1.13.



**Figure 1.13** A cluster state is a graph state where the nodes follow a grid. Graph states can be effectively be multidimensional, or take fractal dimensions. For example, the Graph state depicted above on the right is effectively 3 dimensional, as it can be folded into a cube.

## Chapter 2

# Linear Optics & The Photonic Machine Gun

“My job as a physicist is to torture photons to pump out all the information that they carry.”

---

Y. Ascasibar, 2018, *during a lecture in Autonomous University of Madrid.*

This chapter is intended to present what a photonic qubit looks like in reality, and how are quantum gates applied to it. This is described for photonic qubits, whose operation depends on linear optics. A theoretical description of linear-optical devices for polarization, dual-rail and time-bin encoding is developed, and a motivation of the proof of universality of this system is presented using the KLM arguments. Lastly, the main ingredient is presented: the QD that generates entangled photons on demand. The pulse sequences leading to the creation of GHZ states and linear cluster are described.

### 2.1 Encoding qubits in light

Light can be described in terms of excitations of the EM field over different modes. A mode is a property of the excitation that remains constant during the evolution, unless it is externally forced to change. For example, horizontally polarized light is a mode of the EM field. In this sense, the modes of a certain state of light can be described in terms of creation and annihilation operators, and the changes between modes can be seen as transformations between these operators. This focus over the operators rather than the states follows a *Heisenberg Picture* and is handy to work with.

#### 2.1.1 Overview of the different encodings

Light has several degrees of freedom that constitute pairs of modes which can be exploited to encode qubits.

- **Dual-rail encoding:** Uses the propagation of single photons over two different spatial modes

$a$  and  $b$  (e.g., two separate waveguides) to encode the logical states of a qubit:

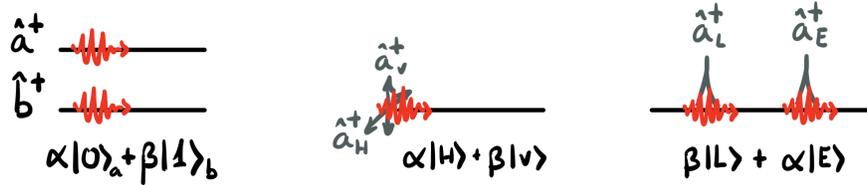
$$|0\rangle = a^\dagger |\emptyset\rangle \quad |1\rangle = b^\dagger |\emptyset\rangle$$

This encoding is the most intuitive one and manipulations are easy using regular Beam Splitters and waveplates, as will be shown a bit later. Moreover, photon loss is easily detected. However, spatial inhomogeneities in the transmission lines such as thermal fluctuations in the length of the waveguides or variations in physical properties might dirt the qubits.

- **Polarization encoding:** Photons can have two distinct polarizations<sup>1</sup>,  $|H\rangle$  or  $|V\rangle$ . The two states are encoded over the same spatial mode, say  $a$ :

$$|0\rangle = a_H^\dagger |\emptyset\rangle \equiv |H\rangle \quad |1\rangle = a_V^\dagger |\emptyset\rangle \equiv |V\rangle$$

This encoding is practical because polarization can be manipulated efficiently using experimental optical devices, such as birefringent materials or Polarization Beam Splitters. Again, inhomogeneities in the waveguides themselves to whom polarization is sensitive can break the qubits.



**Figure 2.1** Different encodings of qubits into photons. From left to right, dual-rail, polarization and time-bin encoding. Each spatial mode is represented by a letter. The process to set the parameters  $\alpha$  and  $\beta$  is explained later.

- **Time-bin encoding:** Encodes qubits in the arrival time of pulses of photons travelling along the same spatial mode. States can arrive either *Early* or *Late*:

$$|0\rangle = a_E^\dagger |\emptyset\rangle \equiv |E\rangle \quad |1\rangle = a_L^\dagger |\emptyset\rangle \equiv |L\rangle$$

In practice the photon wavepackets that conform the pulses can be 100 ps long and separated a few ns.

Time-bin encoding is safe against thermal fluctuations or inhomogeneities in the materials (given that these happen slower than the separation between pulses), as both pulses are affected in the same manner. This is the reason why it is a good choice to transmit quantum information over large distances. However, in terms of manipulations, it's difficult to operate, requiring fast switches or passive delays (all in all, the different states have to be treated differently but without gaining time information not to break the quantum superposition properties). These are typically inconvenient in the lab. Nevertheless, it can be transformed to dual-rail or polarization encodings to be operated and then reverted back to time-bin.

This encoding might seem too naive to actually be useful. However, it will be the cornerstone of the Photonic Machine Gun, to be introduced later. Of course, *Early* and *Late* are relative

<sup>1</sup>This is because photons are massless spin 1 bosons (hence, with 3 spin angular momentum states) that travel at the speed of light. As a consequence of Special Relativity the longitudinal polarization is suppressed, and just 2 polarizations remain.

concepts that only make sense one in relation to each other. Say that, by some means (for example, using the protocol described in ...), you got an spin-photon entangled state with the form  $|\psi\rangle = |+\rangle_s |E\rangle_\gamma + |-\rangle_s |L\rangle_\gamma$ . After several measurements over both the spin and the photon arrival time, you would notice that every time the spin happens to be in the "-" state, the photon arrives later than when it is in "+".

**Note:** The choice of the logical  $|0\rangle$  and  $|1\rangle$  may vary. For example, in some situations it might be useful to define  $|0\rangle = L$  or even  $|1\rangle = -|E\rangle$ .

Both dual-rail and polarization encodings can be used to apply quantum gates to the qubits encoded over them. Time-bin is handy for the generation of entangled states and the transmission of quantum information. In the following sections, a detailed analysis will explore how to apply qubit rotations over these encodings, and how to transform ones to the others.

## 2.2 Optical Quantum Gates

Every state of the EM field can be written in terms of the creation and annihilation operators. Therefore, the evolution of states under Quantum Gates can be described by changes over operators. This point of view, usually called the Heisenberg picture, is sometimes easier to work with. In this picture Hamiltonians  $H$  describe unitaries  $U = e^{iH}$  which are then applied following Heisenberg equation of motion  $\hat{a} \rightarrow U^\dagger \hat{a} U$ .

A powerful result of Linear Optics is that every single qubit unitary can be implemented using a combination of Beam Splitters and Phase Shifts:

- The **Phase Shift** operator introduces a phase into one mode of the EM field:

$$U \equiv R(\phi) = e^{i\phi \hat{a}^\dagger \hat{a}} \quad R(\phi)^\dagger \hat{a} R(\phi) = \hat{a} e^{i\phi}$$

Physically, a phase shift can be applied introducing an additional propagation length in one mode with respect to the other. This introduces a phase  $e^{ik\Delta L}$ . An alternative way is to place a material with a different refractive index in the propagation of one of the modes, yielding a phase shift of  $e^{ikL(n_2-n_1)}$ , where  $L$  is the width of the material.

In the language of Quantum Information, a Phase Shift applies a rotation around the Z-axis of the Bloch Sphere.

- A **Beam Splitter** (BS) typically consists of a semi-reflective mirror that splits the EM field. A quantum description of the effect requires conservation of energy and some additional constraints, such as preserving the bosonic commutation algebra between the creation-annihilation operators. A full description of these relations is done by C. Gerry & P.L. Knight in Ref. [11]. Let  $\hat{a}$  and  $\hat{b}$  be associated with the two spatial modes on either side of the BS:

$$U \equiv B(\theta, \phi) = e^{i\theta(e^{i\phi} \hat{a} \hat{b}^\dagger - e^{-i\phi} \hat{a}^\dagger \hat{b})}$$

The transformations  $\hat{a}_{out}^\dagger = B^\dagger \hat{a}_{in}^\dagger B$  and  $\hat{a}_{out} = B^\dagger \hat{a}_{in} B$  can be summarized as:

$$\begin{pmatrix} \hat{a}_{out}^\dagger \\ \hat{b}_{out}^\dagger \end{pmatrix} = \begin{pmatrix} \cos \theta & -e^{-i\phi} \sin \theta \\ e^{i\phi} \sin \theta & \cos \theta \end{pmatrix} \begin{pmatrix} \hat{a}_{in}^\dagger \\ \hat{b}_{in}^\dagger \end{pmatrix}$$

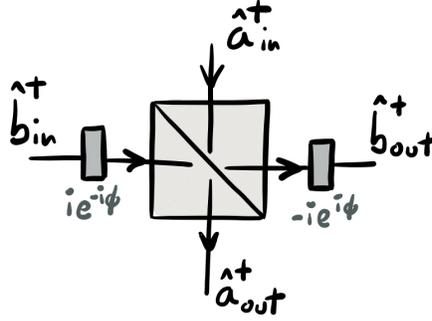
The BS matrix is represented as  $\begin{pmatrix} t & r^* \\ r & t^* \end{pmatrix}$  where  $t = \cos \theta$  and  $r = e^{i\phi} \sin \theta$ . In short,  $\theta$  is related to the transmittance/reflectance ratio, and  $\phi$  is related to the phase introduced by the coating of the mirror. For example, a so called 50-50 BS has  $\theta = \pi/4$ . Moreover, a symmetric BS (one

that applies the same phase shift to both reflected rays) is obtained setting  $\phi = \pi/2$ . This corresponds to a BS with a dielectric mirror, as these apply a  $\pi/2$  phase upon reflection. A dielectric 50-50 BS therefore takes the form:

$$\frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$$

Hopefully, one can combine dielectric a single BS with an arbitrary  $\theta$  parameter, with two phase shifters to obtain a general BS transformation:

$$\begin{pmatrix} \cos \theta & -e^{-i\phi} \sin \theta \\ e^{i\phi} \sin \theta & \cos \theta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & -ie^{i\phi} \end{pmatrix} \cdot \begin{pmatrix} \cos \theta & i \sin \theta \\ i \sin \theta & \cos \theta \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & ie^{-i\phi} \end{pmatrix}$$



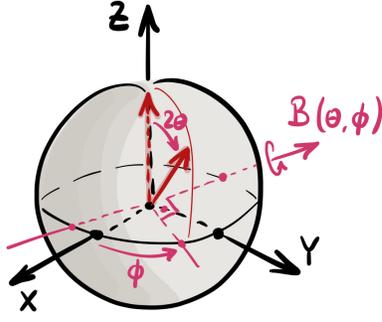
**Figure 2.2** A dielectric Beam Splitter with variable  $\theta$  applies the transformation  $\begin{pmatrix} \cos \theta & i \sin \theta \\ i \sin \theta & \cos \theta \end{pmatrix}$ . If combined with 2 phase shifters, represented as grey slabs and designed to introduce phase shifts indicated in the Figure above, the ensemble can be used to apply a general BS transformation  $\begin{pmatrix} \cos \theta & -e^{-i\phi} \sin \theta \\ e^{i\phi} \sin \theta & \cos \theta \end{pmatrix}$ .

The above matrix transformation applied by a BS can be connected to a rotation in the Bloch Sphere, as such a matrix is in  $SU(2)$  and can be connected to  $SO(3)$ . It is assumed that the algebraic basis is the computational basis  $\begin{pmatrix} \hat{a}_0 \\ \hat{a}_1 \end{pmatrix}$ , where  $\{|0\rangle, |1\rangle\}$  are the eigenstates of the Pauli Z operator. Fix  $\phi$  or  $\varphi$ . In short, the above BS transformation is a rotation around the equatorial axis  $|0\rangle + e^{i(\phi + \frac{\pi}{2})} |1\rangle$  of angle  $2\theta$ . This can be visualized in Figure 2.3. Proving this result is easy. It suffices to find its eigenvectors (fixed axis) and eigenvalues (rotated angle).

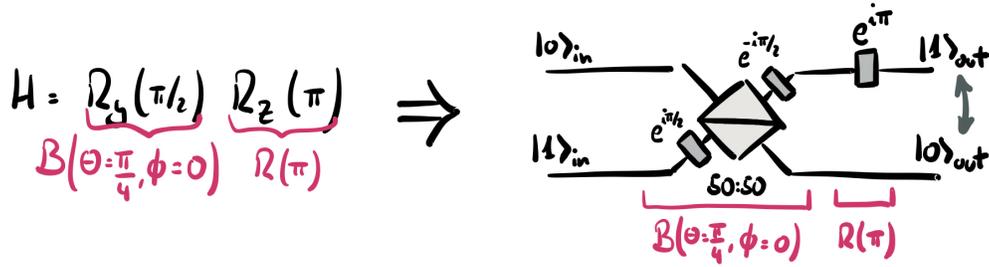
- A fixed vector of the above transformation  $B(\theta, \phi)$  is  $\begin{pmatrix} 1 \\ \pm e^{i(\phi + \pi/2)} \end{pmatrix}$ .
- The eigenvalues of the matrix  $B(\theta, \phi)$  are  $\lambda_{1,2} = \frac{\text{Tr}(B) \pm \sqrt{\text{Tr}(B)^2 - 4\text{Det}(B)}}{2} = \pm e^{i\theta}$ , which is a rotation of  $2\theta$  up to a global phase. This can also be checked by tracking the evolution of a point in the Bloch Sphere, such as  $|0\rangle$ .

By now it has been shown how rotations in the Bloch Sphere are related to physical operations over a dual-rail encoded qubit. Respectively, phase shifts and Beam Splitter operations. An immediate consequence of this is that now every single-qubit rotation can be implemented using a combination of this two elements. This is because any rotation in 3D can be implemented by a sequence of 3 rotations around two orthogonal axes. Many decompositions to accomplish this exists, but for example, the *Euler Angles* can be used.

**Example:** Application of a Hadamard gate in dual-rail encoding:



**Figure 2.3** Visualization of the action of a general Beam Splitter transformation  $B(\theta, \varphi)$ . It is a rotation of angle  $2\theta$  around an axis  $\phi + \frac{\pi}{2}$  away from the X axis.



**Figure 2.4** Linear Optics implementation of a Hadamard Gate. The BS depicted is a 50:50 dielectric Beam Splitter with parameters  $\theta = \pi/4$ ,  $\varphi = \pi/2$ . Note that the spatial order of the  $|0\rangle$  and  $|1\rangle$  modes are swapped after the BS.

## 2.2.1 N-mode Interferometer

The previous ideas can be generalized to the case in which we have  $N$  input modes  $\hat{a}_1^\dagger$  to  $\hat{a}_N^\dagger$  to build an  $N$ -mode Linear Interferometer<sup>2</sup>. We can express such unitary transformation in a matrix  $U$ . Specifically,  $U \in \text{SU}(N)$ :

$$\hat{\mathbf{a}}_{\text{out}}^\dagger = U \cdot \hat{\mathbf{a}}_{\text{in}}^\dagger \quad \text{or} \quad \hat{a}_{j\text{out}}^\dagger = \sum_k U_{jk} \hat{a}_{k\text{in}}^\dagger$$

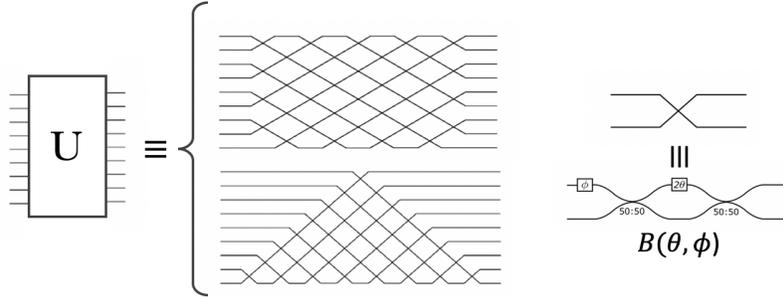
where  $\hat{\mathbf{a}}_{\text{out}}^\dagger = (\hat{a}_1^\dagger, \dots, \hat{a}_N^\dagger)^T$

It has been proven [34] [23] that any general  $U$  can be implemented by a convenient sequence of 2-mode interferometers, composed of Beam Splitters and Phase Shifts:

At this point, however, one should note a very important remark: even though every pair of modes serves to encode 1 qubit, the  $N$ -port interferometer cannot apply any Gate over  $N/2$  qubits. This is better understood with an example: Say we have a 4-mode interferometer, with modes  $\hat{a}_1^\dagger, \hat{a}_2^\dagger$  for qubit 1 and modes  $\hat{b}_1^\dagger, \hat{b}_2^\dagger$  for qubit 2. The Interferometer can implement gates in the base  $\{\hat{a}_1^\dagger, \hat{a}_2^\dagger, \hat{b}_1^\dagger, \hat{b}_2^\dagger\}$ . However, a general 2-qubit transformation requires to operate in the basis  $\{\hat{a}_1^\dagger \hat{b}_1^\dagger, \hat{a}_1^\dagger \hat{b}_2^\dagger, \hat{a}_2^\dagger \hat{b}_1^\dagger, \hat{a}_2^\dagger \hat{b}_2^\dagger\}$ .

In other terms, this means that Linear Interferometers are not enough to create entanglement. For example, lets take the transformation  $|H_a H_b\rangle \rightarrow \frac{1}{\sqrt{2}}(|H_c H_d\rangle + |V_c V_d\rangle)$ , where we use a single-rail polarization encoding over input modes  $a, b$  and output modes  $c, d$ . This is a common operation

<sup>2</sup>One can play with this type of interferometers and tune the parameters using e.g. Xanadu's hardware via *Strawberry Fields* [36]



**Figure 2.5** On the left, Decompositions of a N-port interferometer as suggested by *Reck et al.* [23] and *W.R. Clements et al.* [34]. Both use  $\mathcal{O}(N^2)$  generalized Beam Splitters; on the right Decomposition of a generalized BS in terms of PS and 50:50. The setup is a Mach-Zender interferometer.

that creates a maximally-entangled Bell Pair. In terms of operators, this transformation would mean  $\hat{a}_H^\dagger \hat{b}_H^\dagger \rightarrow \frac{1}{\sqrt{2}}(\hat{c}_H^\dagger \hat{d}_H^\dagger + \hat{c}_V^\dagger \hat{d}_V^\dagger)$ . However, Linear Interferometers just allow transformations such as:

$$\hat{a}_H^\dagger \hat{b}_H^\dagger = \left( \sum U_{Hj} \hat{c}_j^\dagger \right) \left( \sum \tilde{U}_{Vk} \hat{d}_k^\dagger \right)$$

Which is always a separable expression and therefore *not* entangled. Physically speaking, this makes sense because entanglement requires an interaction to take place. However, photons have a weak interaction even when they get close through the BS. The BS creates a superposition of the EM fields, which is different from an interaction. An interaction is understood as that the state of one photon actively determines what happens to the other.

In conclusion, Linear Interferometers alone cannot implement a Quantum Computer. However, they can implement *probabilistically* some useful operations, such as *fusion gates*, to be discussed in Chapter 4.

### 2.2.2 The KLM solution

E. Knill, R. Laflamme and G.J. Milburn developed a protocol (Ref. [12]) that permits the implementation of any gate using Linear Interferometers and Measurement. The idea is that by making measurement on part of the output we can reject certain states of the superposition and effectively create entanglement. Their solution, described originally in [12] is pretty intelligent and uses concepts such as the *teleportation trick* or post-selection, which means that their algorithm is probabilistic. To boost the probability of success they use  $2n$  extra photons and their are able to implement any 2-qubit gate with a success probability of  $(n/(n+1))^2$ .

Better proposals to boost further the success probability and reduce the number of extra resources needed have been proposed (a good summary is found in Ref. [15]).

The main victory of KLM, however, was to show that Linear Optics together with an Measurements serves as a full model for Quantum Computing and is usually referred as Linear Optical Quantum Computing.

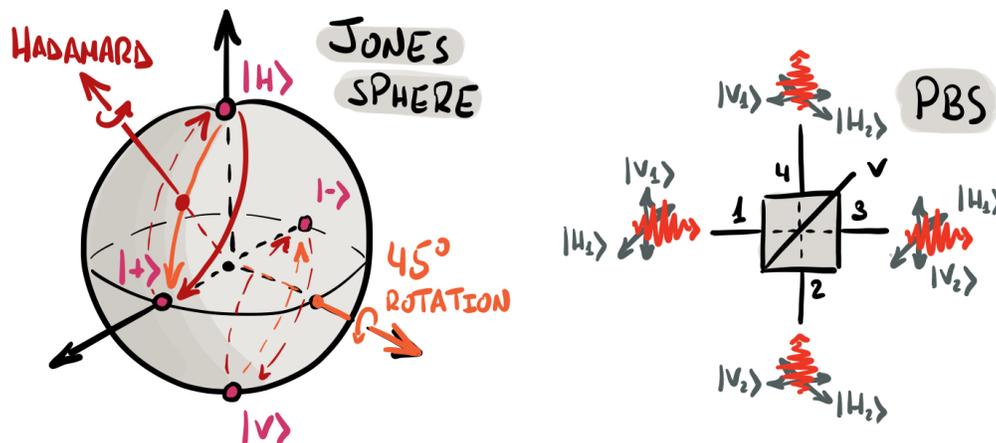
## 2.3 Working with other encodings

As mentioned before, other encodings than dual-rail propose certain advantages. For example, time-bin is useful for the long-distance transmission and the experimental generation of the qubits, while

polarization and dual-rail are handy to apply the transformations. There are several experimental tricks that allow to transform from one to another.

### 2.3.1 Polarization encoding

The polarization degree of freedom of photons is extremely handy to encode qubits. The  $|0\rangle$  and  $|1\rangle$  local states can be encoded in the horizontal ( $|H\rangle$ ) and vertical ( $|V\rangle$ ) polarizations. Superpositions of these two states give rise to other bases. For example, diagonally polarized light can be described by the combination  $\{|+\rangle, |-\rangle\} \sim \{|H\rangle + |V\rangle, |H\rangle - |V\rangle\}$  (up to normalization). Furthermore, circularly polarized light (right-handed and left-handed states) can be described by  $\{|R\rangle, |L\rangle\} \sim \{|H\rangle + i|V\rangle, |H\rangle - i|V\rangle\}$ . The similarities between these states and the usual one-qubit states, pictured in the Bloch Sphere, are not a coincidence. Indeed, it was around 1941, many years before the first apparition of the word qubit<sup>3</sup> in 1992, that R.C. Jones created a formalism to describe polarization calculus: The Jones Vectors and Jones Sphere:



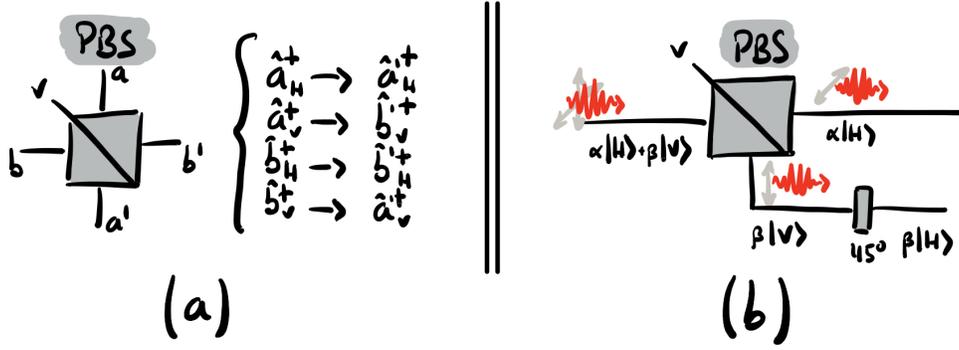
**Figure 2.6** A Hadamard operation and a  $45^\circ$  rotation operation depicted in the Jones Sphere as polarization rotations. They are similar upon acting on  $|0\rangle$  and  $|1\rangle$ , but not exactly the same, which is evident in the visual representation. The  $45^\circ$  rotation transforms  $|-\rangle \rightarrow -|1\rangle$  while Hadamard does  $|-\rangle \rightarrow |1\rangle$ . Experimental implementations of generic polarization rotations are shown in Ref. [17].

In the polarization encoding, single qubit rotations are understood as polarization rotations. In particular, simple  $45^\circ$  rotations, achieved by using birefringent materials are the analogous of rotations around the Y axis. However, more complex rotations such as Hadamard rotations can be achieved and implemented in integrated photonic circuits, as discussed in [17].

The other key ingredient in polarization encoding is the Polarization Beam Splitter (PBS). It splits horizontal and vertical polarization components of the input light. It is used to perform measurements in the  $\{H, V\}$  basis.

Now that many transformations of both dual-ray encoding and polarization encoding have been described, their similarities and differences become apparent: In dual ray encoding, a general single-

<sup>3</sup>The creation of the word qubit is attributed to Benjamin Schumacher and William Wootters who were discussing the necessity of a new word to measure the amount of quantum information in 1992. More like a joke, they proposed "qubit". They found it funny because it sounds like "cubit", unit of length in the Middle East that appears in the Bible: "And this is how you shall make it (the Ark of Noah): The length of the ark shall be three hundred cubits, its width fifty cubits, and its height thirty cubits." (Genesis 6:15 [1])



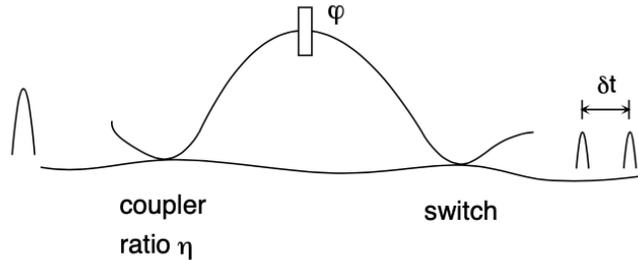
**Figure 2.7** The usual PBS transformations do not include any phases. In the picture, the diagonal line with a  $V$  indicates that it reflects the vertical component.

qubit rotation is achieved by a generalized BS; In polarization encoding, by a general polarization rotation. A PBS serves as a tool to convert between both encodings.

For simplicity in the equations, when talking about polarization rotation it will be implicit a Hadamard-like rotation, in which a repetition of the transformation comes back to the original state. As we do not have to fight with experimental implementations, we can assume this, and many of our equations will be greatly simplified in terms of signs.

### 2.3.2 Time-bin encoding

In the time-bin encoding, a superposition in time is used to store qubits. A general state can be expressed as  $|\psi\rangle = \eta|E\rangle + (1 - \eta)e^{i\varphi}|L\rangle$ . Such general state is easy to create using a circuit as the one in Figure 2.8.



**Figure 2.8** The creation of a general qubit state  $\eta|E\rangle + (1 - \eta)e^{i\varphi}|L\rangle$  just requires a regular light source (such a diode laser; no need for pulsed lasers or single photon sources), a tunable BS and an extra length of waveguide. If we look at the circuit from right to left, it constitutes a Time-Bin Measurement interferometer. Figure from [35].

Time bin can be converted to dual-rail encoding and polarization encoding using fast switches, as depicted in Figure 2.9

Time-Bin has, among its disadvantages, the technological difficulties that fast switching poses. As the time separation between pulses is in the order of a few ns, these devices have to switch at rates of GHZ. Moreover, a deterministic approach is difficult to create. This is because, if we gained time information to always send the  $|E\rangle$  pulse through the long path, we would destroy the



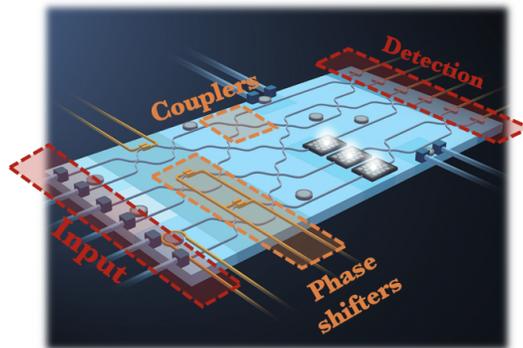
**Figure 2.9** (a) Time-Bin  $\rightarrow$  Polarization; (b) Polarization  $\rightarrow$  Time-Bin. The Polarization Controller (PC) rotates the polarization to match  $|H\rangle$  and  $|V\rangle$  states. The Switch (SW) flips the 2 paths periodically. An extra piece of wire delays the  $|E\rangle$  photon to match with the  $|L\rangle$  photon. Note that the circuit succeeds 50% of the time, just when the  $|E\rangle$  photon takes the long path.

superposition<sup>4</sup>.

## 2.4 Integrated optics

Experiments in optics typically operate using bulk devices in optical benches: mirrors, Beam Splitters and birefringent materials among others serve to affect the photons, which are usually transmitted through air. These systems are difficult to align and stabilize, take big spaces and are difficult to scale. However, the development of photonic waveguide technology, starting by silica waveguides in a Si chip in 2008 [8], has rapidly advanced. Nowadays experimentalists use the knowledge gained from lithography techniques used in electronic boards to etch on-chip photonic circuits. These allow miniaturization and need no further alignment once made.

An integrated photonic chip might look like the one in Figure 2.10.



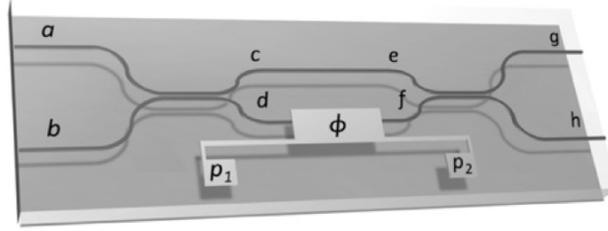
**Figure 2.10** Artistic image of an integrated photonic chip implementing a linear interferometer, as in the Reck model Ref. [23]. Apart from the elements indicated, one can see small loops called Ring Resonators that act as wavelength filters.

- **Beam Splitters** are implemented by directional couplers. These operate by bringing together waveguides so that the evanescent wave of one can couple and interfere with the other. By adjusting the separation and the length of the coupling area, one can tune the BS parameters.

<sup>4</sup>The same way a PBS reacts differently to  $|H\rangle$  and  $|V\rangle$ , an hypothetical material that would react differently to  $|E\rangle$  and  $|L\rangle$  would allow deterministic operation. However, such time-inhomogeneity is difficult to achieve.

- Tuneable **Phase Shifters** can be implemented through the thermo-optical effect: some materials change their refractive index when temperature changes (in the order of  $10^{-2}$  mK). These materials are slow. Newer technologies use the electro-optical or Pockels Effect to tune the refractive index. These have reconfiguration times of the order of ns.

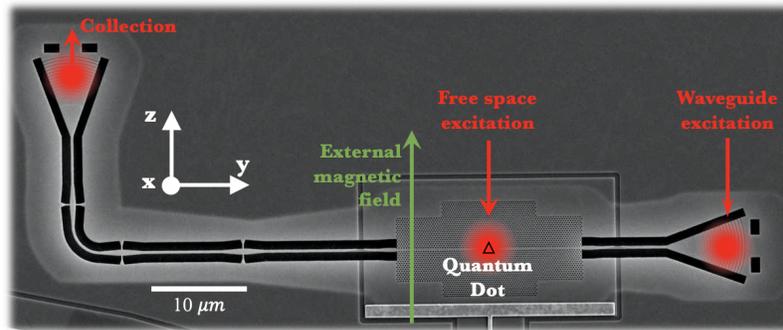
For example, an integrated Beam Splitter with variable reflectivity coefficient  $\theta$  can be implemented through a Mach-Zender Interferometer as the one in Figure 2.11



**Figure 2.11** Mach-Zender Interferometer that implements a Beam Splitter transformation  $\begin{pmatrix} \cos \theta & i \sin \theta \\ i \sin \theta & \cos \theta \end{pmatrix}$ . Device used by [22] to demonstrate Hong-Ou Mandel effect, among others.

## 2.5 A Quantum Dot as a Photonic Machine Gun.

Solid-state Quantum Dots (QD) serve as a promising source of on-demand single photons. Their electronic levels structure serve to encode a qubit in the spin degree of freedom of the QD. Moreover, driving transitions between these levels with excitation pulses in a correct way leads to the emission of single photons entangled in a time-bin encoding both with the QD spin state and between the photons themselves. Different pulse sequences generate different entangled resources such as Cluster States and GHZ States, and these can be used for Measurement-Based Quantum Computing.



**Figure 2.12** Scanning electron microscope image of the experimental system for the QD emitter, courtesy of Peter Lodahl's Hy-Q group at Niels Bohr Institute. The QD is not to scale. The metal strip on the bottom serves to apply an external bias voltage to charge the QD. The magnetic field of around 2 T defines a  $z$ -direction and fixes *Voigt geometry* regarding the transition selection rules ([27]).

### 2.5.1 The physical system

Many groups, including the Quantum Photonics research group at Niels Bohr Institute, are working on sources for on-demand photon generation. Indeed these can be engineered to be sources for *entangled* photon on-demand sources. A way to achieve this is to embed a QD into a photonic crystal waveguide. Quantum Dots consists on nanometric semiconductor structures in which several thousands of atoms are confined. They show an electronic levels structure similar to that of atoms. Therefore, these transitions that can be selected and used experimentally to emit light with certain well controlled properties.

In this thesis, a connection with the experiments at the Quantum Photonics lab at Niels Bohr Institute<sup>5</sup>.

These QD are self-assembled Indium Arsenide (InAs) Quantum Dots grown on top of a Gallium Arsenide (GaAs) substrate. They are grown through the Stranski-Krastanov method, where the difference in lattice constant between the GaAs substrate and layers of deposited InAs atoms creates a local strain that eventually breaks into tiny islands of InAs, which form the QD. They are pyramid-shaped with 1-10 nm in height and 10-70 nm in plane dimensions. InAs QD have direct bandgap transitions where the wavelength of the emission is around 850-1000 nm, depending on the specific geometry of the QD. This is infrared light which, as mentioned above, is well-shielded from ambient temperature noise.

Optical excitation of the QD creates an electron-hole pair (exciton) whose lifetime is approximately 1 ns. The recombination results in the emission of a photon. This process is called *Resonance Fluorescence*.

In normal circumstances, the QD is neutral, containing a fully occupied valence band and an empty conduction band. However, for this thesis positively charged QD are considered, which are referred to as  $X^+$ . In these systems, an electron is removed from the valence band by rising the valence band with respect to the Fermi level through an external bias voltage. If additionally another electron is excited to the conduction band, the resulting system consists of a pair of holes and an electron, just before recombination happens. This state is called *Positive Trion*.

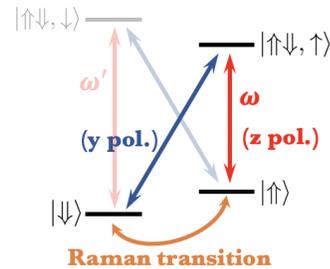
### 2.5.2 Electronic levels structure

The electronic levels of the  $X^+$  are depicted in Fig.2.13. It consists in a 4-level structure, even though only 3 of the levels will be used later on. An in-plane magnetic field of around 2 T introduces a Zeeman splitting that breaks down the degeneracy of the levels and sets the selection rules to be discussed below. This situation is frequently called *Voigt geometry*.

The four levels are:

- Two ground levels  $\{|\uparrow\rangle, |\downarrow\rangle\}$  that encode a qubit in the 1/2-spin Z- eigenstates of the hole.
- Two upper levels corresponding to the excitation of an electron to the conduction band, whose spin is denoted as  $\{|\uparrow\rangle, |\downarrow\rangle\}$ . Pauli exclusion applies to the pair of holes.

The magnetic field introduces selection rules regarding the polarization of the optical transitions. This way, controlling both the frequency and the polarization of the excitation each of the four transitions can be driven.



**Figure 2.13** Level structure of the  $X^+$   $\Lambda$ -system.

<sup>5</sup>A big thank you is dedicated to Peter Lodahl and Martin Hayhurst for showing what qubits *actually* look like and keeping my feet on earth.

### 2.5.3 Spin dynamics

A qubit can be encoded in the spin degree of freedom of a spin-1/2 particle, such as the Z-eigenstates  $\{|\uparrow\rangle, |\downarrow\rangle\}$  of the hole in the  $X^+$ . This conforms a *spin qubit* in a general state  $|\psi\rangle_s$ :

$$|\psi\rangle_s = \cos(\theta/2) |\downarrow\rangle + e^{i\phi} \sin(\theta/2) |\uparrow\rangle$$

The logical states can be chosen as  $\{|0\rangle, |1\rangle\} \leftrightarrow \{|\uparrow\rangle, |\downarrow\rangle\}$ , which are the two ground levels of the spin of the QD.

Decisive for every qubit is the ability to initialize the qubit, transform its state and measure it:

- **Initialization:** A pump laser z-polarized is set to drive resonantly the transition  $|\uparrow\rangle \rightarrow |\uparrow\downarrow, \uparrow\rangle$ , which decays most likely back to  $|\uparrow\rangle$ . However, there is a small probability for a decay to  $|\downarrow\rangle$ . Initialization consists in repeating this process until the state is  $|\downarrow\rangle$ . Once in  $|\downarrow\rangle$ , the system stays there, as the laser is non-resonant with any other transitions. This process is heralded by the observation of the wavelength of the light emitted by the QD.
- **Spin rotation:** The idea is to apply Raman transitions to drive coherent spin rotations between the states  $|\uparrow\rangle \leftrightarrow |\downarrow\rangle$ . These spin rotations can be experimentally tuned to implement rotations around an axis passing through the equator. For example, an  $X$  quantum gate can be implemented as a  $\pi$  rotation around the  $Y$  axis of the Bloch Sphere.
- **Optical transition:** A pump laser is set to resonantly drive the transition  $|\uparrow\rangle \rightarrow |\uparrow\downarrow, \uparrow\rangle$ , which results in the creation of an exciton which, upon recombination, emits a photon with a wavelength 850-1000 nm. The transition  $|\uparrow\rangle \rightarrow |\uparrow\downarrow, \downarrow\rangle$  is non-resonant and therefore effectively decoupled from the dynamics.
- **Readout:** Spin state readout can be achieved with microwave pulses.

The 3-level system resulting from the dynamics discussed above is called a  $\Lambda$  system. The system resulting from the dynamics of In conclusion, the system of interest is the set of the 3 levels that can be seen in Figure 2.13. The vertical transition is driven by a laser in resonance with the transition, and the rotations between the two ground levels  $|\uparrow\rangle \leftrightarrow |\downarrow\rangle$  are driven by Raman pulses.

### 2.5.4 Pulse sequences

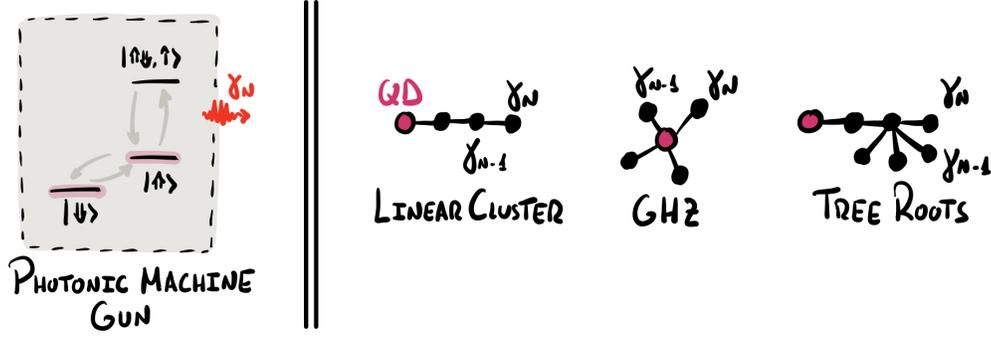
The 3 level system described above can be utilized to generate on-demand multi-photon entangled states such as linear clusters or GHZ states. A protocol similar to the one to be discussed was firstly proposed by Lindner and Rudolph in 2009 in Ref. [32]

The  $\Lambda$  system operates in cycles, each of them resulting in the emission of a photon entangled with the QD spin and other photons in a time-bin encoding. Two pulse sequences are to be described: The first of them grows a cluster state, while the second one creates a GHZ state. More complex entanglement graphs can be obtained by sandwiching the different pulse sequences.

The different atomic operations that constitute the pulse sequences are the following. The logical states have been encoded in the spin qubit as  $\{|0\rangle, |1\rangle\} \rightarrow \{|\downarrow\rangle, |\uparrow\rangle\}$ .

$$\begin{aligned} \hat{E} &= |0\rangle\langle 0| + |1\rangle\langle 1| \hat{a}_E^\dagger & \hat{L} &= |0\rangle\langle 0| + |1\rangle\langle 1| \hat{a}_L^\dagger \\ Y(\pi) &= |1\rangle\langle 0| - |0\rangle\langle 1| & Y(-\pi/2) &= |-\rangle\langle 0| + |+\rangle\langle 1| \end{aligned} \quad (2.1)$$

where  $|\pm\rangle = (|0\rangle \pm |1\rangle)$  (up to normalization) are the eigenstates in the  $X$  direction.  $Y(\phi)$  implements a right-handed rotation of  $\phi$  radians around the  $Y$  axis. The signs can be proven to be right noting that the  $Y$  operations keep its eigenstates  $|0\rangle + i|1\rangle$  fixed.



**Figure 2.14** On the left, the Quantum Dot photonic machine gun; on the right, example of three graph states that might be generated.

The entanglement protocol can split into 2 main parts: (i) Initialization of the QD; (ii) Pulse sequences, to be repeated on-demand. Can be chosen among 2 types, one to generate a linear-cluster type emission, and another to generate a GHZ- type emission. For a more detailed explanation, see [27].

The protocol to generate time-bin entangled photons is:

(i) **Spin initialization:**

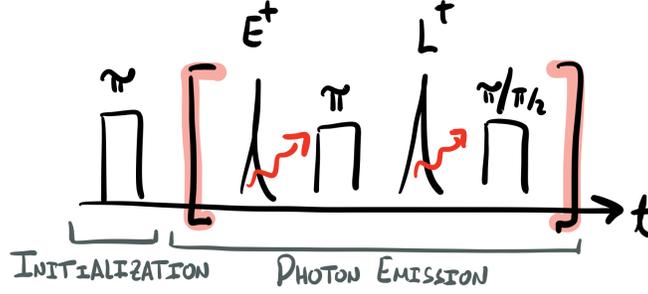
1. Initialize the QD in the  $|\downarrow\rangle$  state.
2. Rotate the spin ground state to an equal superposition:  $|\downarrow\rangle \rightarrow \frac{1}{\sqrt{2}}(|\downarrow\rangle + |\uparrow\rangle)$  using a  $\pi/2$  Raman pulse. This is achieved with a  $Y(\pi/2) = |+\rangle\langle 0| - |-\rangle\langle 1|$  Spin rotation pulse.

(ii) **Pulse sequence:**

3. Resonantly drive the  $|\uparrow\rangle \leftrightarrow |\uparrow\downarrow, \uparrow\rangle$  transition with an optical pulse, denoted  $\hat{E}$ : this results in the emission of an *early* photon  $|E\rangle = \hat{a}_E |\emptyset\rangle$ .
4. Apply a  $\pi$ -rotation to flip  $|\uparrow\rangle \leftrightarrow |\downarrow\rangle$  with a  $Y(\pi)$  Spin rotation pulse.
5. Resonantly drive again the  $|\uparrow\rangle \leftrightarrow |\uparrow\downarrow, \uparrow\rangle$  optical pulse, denoted  $\hat{L}$ : this results in the emission of an *late* photon, photon  $|L\rangle = \hat{a}_L |\emptyset\rangle$ .
6. (a) To grow entanglement for a Linear Cluster, apply a  $Y(-\pi/2)$  Spin rotation pulse.  
 (b) To entanglement as for a GHZ state, apply a  $Y(\pi)$  Spin rotation pulse to flip again  $|\uparrow\rangle \leftrightarrow |\downarrow\rangle$ .

A protocol may consist of one (i) Initialization and N repetitions of the (ii) Pulse sequence. This will generate an entangled state consisting of N-photons and the hole spin.

**Notation:** In general, the state of the hole-spin will be denoted as  $|*\rangle_s$  and the  $i$ -th photon as  $|*\rangle_i$ . However, a compact notation will be used when no confusion is possible. In this case, the first element in the ket will refer to the hole spin, and the rest to the emitted photons, time -ordered from left to right:  $|***\rangle \equiv |*\rangle_s |*\rangle_1 |*\rangle_2$



**Figure 2.15** Pulse sequences to excite the QD. On the last pulse,  $\pi$  grows a GHZ state, while  $\pi/2$  a Linear Cluster.

**Example:** Growth GHZ State

$$\begin{aligned}
 |\psi\rangle_s &\xrightarrow{1} |\downarrow, \emptyset\rangle \\
 &\xrightarrow{2} \frac{1}{\sqrt{2}} (|\uparrow, \emptyset\rangle + |\downarrow, \emptyset\rangle) \\
 &\xrightarrow{3} \frac{1}{\sqrt{2}} (|\uparrow, E\rangle + |\downarrow, \emptyset\rangle) \\
 &\xrightarrow{4} \frac{1}{\sqrt{2}} (|\downarrow, E\rangle - |\uparrow, \emptyset\rangle) \\
 &\xrightarrow{5} \frac{1}{\sqrt{2}} (|\downarrow, E\rangle - |\uparrow, L\rangle) \\
 &\xrightarrow{6} \frac{1}{\sqrt{2}} (|\uparrow, E\rangle + |\downarrow, L\rangle)
 \end{aligned} \tag{2.2}$$

Note that in  $\xrightarrow{4}$  a global  $(-1)$  phase has been taken out, for better organization. This global phase is, of course, unimportant.

**Note:** Rotations around X, Y, Z axis may be found defined in several different ways. However, they are all equivalent up to global phases. A quick way to check that a rotation is behaving as expected is to confirm that it transforms the basis vectors  $\{|\uparrow\rangle, |\downarrow\rangle\}$  as we want, and that it keeps invariant the axis of the rotation (e.g.,  $X(\pi)|+\rangle \rightarrow |+\rangle$ ).

The pulse sequences to generate GHZ and Linear Clusters look like this:

$$\hat{O}_{\text{GHZ}}^\dagger = Y(\pi)\hat{L}^\dagger Y(\pi)\hat{E}^\dagger \quad \hat{O}_{\text{Lin.Cluster}}^\dagger = Y(-\pi/2)\hat{L}^\dagger Y(\pi)\hat{E}^\dagger$$

which, when expanded, look like this:

$$\hat{O}_{\text{GHZ}}^\dagger = |0\rangle\langle 0| \hat{a}_0^\dagger + |1\rangle\langle 1| \hat{a}_1^\dagger \quad \hat{O}_{\text{Lin.Cluster}}^\dagger = |+\rangle\langle 0| \hat{a}_0^\dagger + |-\rangle\langle 1| \hat{a}_1^\dagger$$

where the time-bin creation operators have been identified with the logical creation operators in the following way: GHZ:  $\{\hat{a}_0^\dagger \equiv -\hat{a}_E^\dagger, \hat{a}_1^\dagger \equiv -\hat{a}_L^\dagger\}$ ; Linear Cluster:  $\{\hat{a}_0^\dagger \equiv -\hat{a}_L^\dagger, \hat{a}_1^\dagger \equiv -\hat{a}_E^\dagger\}$ . These operators act upon the spin qubit, initially in a state  $|+\rangle_s$  and a vacuum state  $|\emptyset\rangle$  before the photon is emitted. As these operators will be concatenated and repeated several times, it is a good idea to introduce a numbering in the photons emitted. This way, the  $i$ -th pulse sequence applied will emit the  $i$ -th photon. This can be denoted as  $\hat{O}_{\dots}^{\dagger(i)}$ , were the creation operators inherit this ordering  $\hat{a}^{(i)\dagger}$  and act upon  $|\emptyset\rangle_i$  such that  $\hat{a}^{(i)\dagger}|\emptyset\rangle_i = |1\rangle_i$ .

A single run of the pulse sequences creates a 2 qubit GHZ and Linear Cluster states respectively:

$$\hat{O}_{\text{GHZ}}^\dagger |+\rangle_s |\emptyset\rangle_1 = |0\rangle_s |0\rangle_1 + |1\rangle_s |1\rangle_1$$

$$\hat{O}_{\text{Lin.Cluster}}^\dagger |+\rangle_s |\emptyset\rangle_1 = |+\rangle_s |0\rangle_1 + |-\rangle_s |1\rangle_1$$

It is straightforward to see why  $N$  successive repetitions of  $\hat{O}_{\text{GHZ}}^\dagger$  grow an  $|\text{GHZ}^{(N)}\rangle$  state:

$$|\text{GHZ}^{(N)}\rangle = \hat{O}_{\text{GHZ}}^{\dagger(N)} \cdot \dots \cdot \hat{O}_{\text{GHZ}}^{\dagger(1)} |+\rangle_s |\emptyset\rangle_{N\dots 1} = \frac{1}{\sqrt{2}} \left( |0\rangle_s |0\dots 0\rangle_{1\dots N} + |1\rangle_s |1\dots 1\rangle_{1\dots N} \right)$$

Moreover, this idea also works if the QD spin qubit is initially entangled with an arbitrary state  $|\psi\rangle$  and  $\hat{O}_{\text{GHZ}}^\dagger$  is applied:

- Before:  $|0\rangle_s |\psi\rangle + |1\rangle_s \prod_{\text{ngs}(s)} |\psi\rangle$  ( $|\psi\rangle$  is the *support* of the QD qubit, as discussed in Chapter 3)
- After  $N$  GHZ pulse sequences:  $|0\rangle_s |0\dots 0\rangle_{1\dots N} |\psi\rangle + |1\rangle_s |1\dots 1\rangle_{1\dots N} \prod_{\text{ngs}} |\psi\rangle$ .

In sum, a GHZ star graph is being built around the QD spin qubit while keeping the previous entanglement with any other generic state  $|\psi\rangle$ .

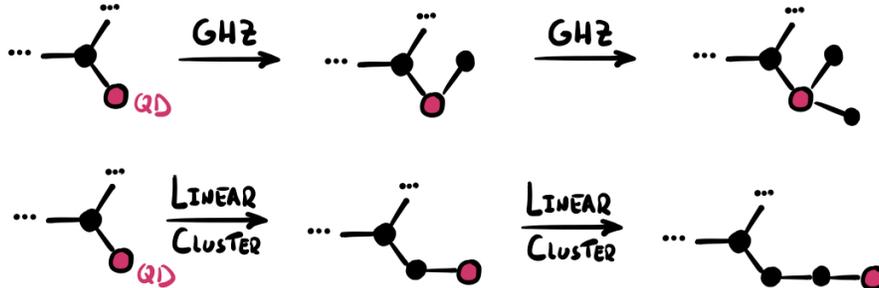
The same ideas work in the Linear Cluster case:

- Before:  $|0\rangle_s |\psi\rangle + |1\rangle_{s \text{ ngs}} |\psi\rangle$
- After a Linear Cluster pulse sequence emitting photon number  $i$ :  $|+\rangle_s |0\rangle_i |\psi\rangle + |-\rangle_s |1\rangle_i \prod_{\text{ngs}} |\psi\rangle$  which can be interpreted as if the entanglement that the spin qubit had with  $|\psi\rangle$  had been transferred to the photon  $i$ .

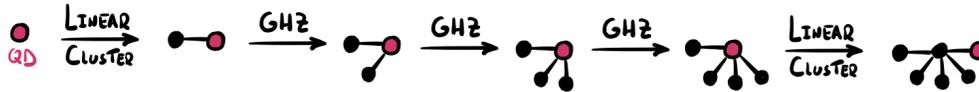
All this means that the pulse sequences can be combined in a sandwich-like fashion to create arbitrary entanglement patters.

## 2.6 Concatenating pulse sequences

The pulse sequences may be concatenated to generate more complex entangled states, as the ones shown below:



**Figure 2.16** Several repetitions of both the Linear Cluster and GHZ pulse sequences. The magenta dot represents the spin QD qubit.



**Figure 2.17** A sandwich of GHZ and Linear Cluster pulse sequences can grow a tree-root like pattern.

## Chapter 3

# Measurement Based Quantum Computing

“Everything we call real is made of things that cannot be regarded as real. Nothing exists until it is measured.”

---

Attributed to Niels Bohr.

Measurement Based Quantum Computing (MBQC) is an alternative approach to quantum computing. The idea is that single-qubit rotations and two-qubit entangling gates can be simulated by performing an adaptive set of *single-qubit measurements* over an entangled set of qubits called Cluster State. This state acts as a resource that is consumed as the computation advances. Thus the other name for MBQC as the One-Way model of QC.

This Chapter aims to build an intuition over MBQC. It begins explaining the core idea behind MBQC: Gate Teleportation; continues introducing the concept of *byproducts*, undesired results of the randomness of the measurement process; and finalizes presenting a set of basic building blocks that can be concatenated to create large and complex computations in a measurement-based fashion.

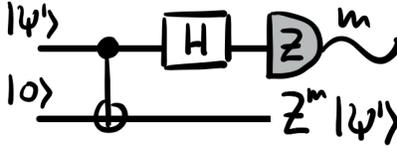
### 3.1 From Gates to Measurements: Gate Teleportation

In Gate Teleportation, a quantum gate is simulated in one part of an entangled state by collapsing the other part by a certain measurement. Described first in Ref. [25] by Nielsen & Chuang, it motivates the idea that Quantum gates can be implemented indirectly by performing *single-qubit measurements*. Of course, the precision of the applied gate is now determined by the measurement. Fortunately, single qubit measurements can be realized precisely in most quantum systems. Consider the circuit in Figure 3.1 that teleports the state  $|\psi'\rangle$ :

The measurement outcome can take values  $\{0, 1\}$ , and depending on it, a Z-Pauli is applied to the teleported state. So far, not much is happening. But we can redefine the input state as  $|\psi'\rangle = Z(\alpha)|\psi\rangle$ , where  $Z(\alpha) = e^{i\alpha Z/2}$  is an arbitrary rotation of angle  $\alpha$  around the Z axis.<sup>1</sup> Using

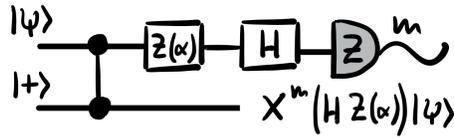
---

<sup>1</sup>The factor of 1/2 is there due to the fact that in SU(2) is a double cover of SO(3), so an angle of  $4\pi$  in the exponent effectively implements a  $\alpha = 2\pi$  rotation.



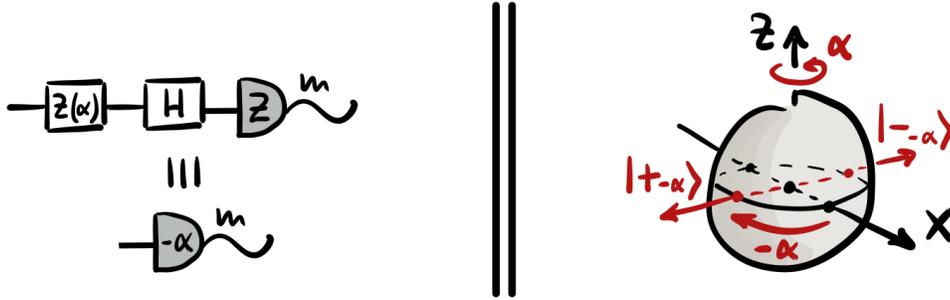
**Figure 3.1** State teleportation through entanglement. The bell-shape with a  $Z$  inside indicates a measurement in the computational basis with measurement outcome  $m \in \{0, 1\}$  for  $\{|0\rangle, |1\rangle\}$ , respectively.

the fact that  $\text{CNOT} = (\mathbb{1} \otimes H)\text{CZ}(\mathbb{1} \otimes H)$  and that  $\text{CZ}$  and  $Z(\alpha)$  commute, we can rewrite the circuit as:



**Figure 3.2** State and gate teleportation: the state  $|\psi\rangle$  is teleported and affected by a gate  $(HZ(\alpha))$ .

Where we have used that  $H|0\rangle = |+\rangle$  and  $HZ^m = X^m H$ . It is useful to define the states  $|\pm\rangle_\alpha \equiv |0\rangle + e^{i\alpha}|1\rangle$ , which lie in the equator of the Bloch Sphere. The combination  $Z(\alpha)H$  followed by a measurement in the computational basis can be understood as a measurement in the basis  $\{|+\rangle_{-\alpha}, |-\rangle_{-\alpha}\}$ .



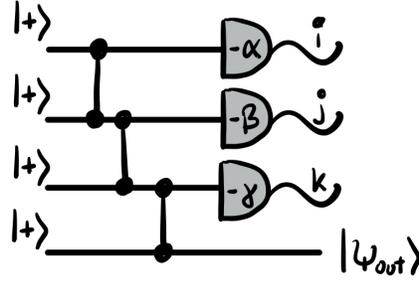
**Figure 3.3** The block  $(HZ(\alpha))$  followed by a measurement in the computational basis is equivalent to measurement in the equatorial basis  $\{|+\rangle_{-\alpha}, |-\rangle_{-\alpha}\}$ , where  $|\pm\rangle_\alpha = |0\rangle + e^{-i\alpha}|1\rangle$ . Measurement in such base is indicated by a bell-like shape with an angle  $-\alpha$  inside.

Any rotation in the Bloch Sphere  $U(\theta)$  can be described in terms of three Euler angles  $\alpha, \beta, \gamma$  that characterize rotations around 2 orthogonal axis, such as X and Z:

$$U(\theta) = Z(\gamma)X(\beta)Z(\alpha) = H(HZ(\gamma))(HZ(\beta))(HZ(\alpha))$$

where we have used the fact that  $H^2 = \mathbb{1}$  and  $HXH = Z$ . Therefore, we can implement any arbitrary single-qubit rotation concatenating the Gate Teleportation protocol 3 times:

$$\text{with } |\psi_{\text{out}}\rangle = (X^k HZ(\gamma))(X^j HZ(\beta))(X^i HZ(\alpha)) |\psi_{\text{in}}\rangle.$$



**Figure 3.4** Any arbitrary rotation in 3D can be decomposed into 3 rotations, described for example by the 3 Euler angles. In MBQC, this is equivalent to 3 measurements.

Having non-deterministic gates (or gates that are applied depend on the randomness of the former measurement outcomes) on the middle of the computation is inconvenient. One way to solve this is to commute them so that they are the last gates applied<sup>2</sup>. In this case, that can be done using the relation  $XZ(\alpha) = Z(-\alpha)X$ . Therefore  $|\psi_{\text{out}}\rangle = X^k Z^j X^i \left( HZ((-1)^j \gamma) \right) \left( HZ((-1)^i \beta) \right) \left( HZ(\alpha) \right)$

At this point we appreciate the main features of a measurement-based approach to apply gates:

1. The computation starts from an entangle set of 4 entangled qubits, that we consume (disentangle) during the computation. That is why this model is also called *one-way*.
2. The gates applied are non-deterministic, as they depend on the particular outcomes.
3. The measurement bases have to be readjusted with the outcome results as the computation executes. This is called *feedforward* in the context of MBQC and defines a temporal direction of the computation.

With a proper readjustment of the sign of the angles, one can implement the desired  $U(\theta)$ .

### 3.1.1 Clifford Gates

Measurements in quantum mechanics are non-deterministic. Moreover, measurements are projections into a subspace that changes depending on the measurement outcome  $s$ . Therefore, each individual measurement  $g$  in a Measurement-Based QC approach over a cluster state effectively simulates the action of a gate  $U_g$  plus an undesired operator  $\Sigma_g$ , which is called the *by-product*.  $\Sigma_g$  consists on local operations on the  $n - 1$  non-measured qubits:

$$\Sigma_g = \bigotimes_j^{n-1} X^{f_j(s)} Y^{g_j(s)}$$

Where  $f(s), g(s) \in \{0, 1\}$  control whether the Pauli operators are applied or not based on the measurement outcome  $s$ . The former formula just emphasizes that  $\Sigma_g$  may consist of  $X, Y$  or  $Z$  Pauli operators applied locally. However, the particular form of  $\Sigma_g$ , described by  $f_j(s)$  and  $g_j(s)$  is established by the particular cluster architecture and measurements scheme.

$|\psi_{\text{out}}\rangle = \Sigma_g U_g |\psi_{\text{in}}\rangle$ . For example, (in the Gate Teleportation described above) the undesired effect is the Pauli  $X^m$ , so  $U_g = HZ(\alpha)$  and  $\Sigma_g = X^m$ .

<sup>2</sup>This is always possible because Pauli operators and Hadamard gates of a type called Clifford gates. This means that they are part of a group closed under commutation operations.

As discussed in [21], the concatenation of two measurements  $g_1$  and  $g_2$  behaves as expected and simply concatenates the gates and by-products of both measurements:  $|\psi_{\text{out}}\rangle = \Sigma_{g_2} U_{g_2} \Sigma_{g_1} U_{g_1} |\psi_{\text{in}}\rangle$ . Having these by-products applied in the middle of the state is inconvenient. Alternatively, if the state had the form  $|\psi_{\text{out}}\rangle = \tilde{\Sigma}_{g_2} \tilde{\Sigma}_{g_1} \tilde{U}_{g_2} \tilde{U}_{g_1} |\psi_{\text{in}}\rangle$  the accumulated byproduct could be undone with a *decoding* operator  $\tilde{\Sigma}_g^\dagger$ , where  $\tilde{\Sigma}_g^\dagger = \prod_i \tilde{\Sigma}_{g_i}^\dagger$  for all measurements  $g_i$ . In some simple cases, where the gate applied  $U_{g_i}$  is off a type called *Clifford Gates*, the commutation of  $U_{g_i}$  and  $\Sigma_{g_j}$  takes the form  $U_{g_i} \Sigma_{g_j} = \tilde{\Sigma}_{g_j} U_{g_i}$  with  $\tilde{\Sigma}_{g_j} = U_{g_i} \Sigma_{g_j} U_{g_i}^\dagger$ .  $\tilde{\Sigma}_{g_j}$  remains a product of local Pauli operators, thanks to the Clifford Group:

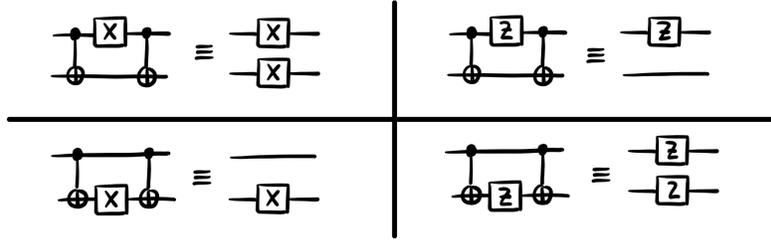
The Clifford Group is a group in the mathematical sense (closed, etc.) consisting of unitaries  $U$  that transform Pauli operators into Pauli operators. Formally,  $\text{CLIFFORD}_n \equiv \{U U P_n U^\dagger \in P_n \forall P_n\}$ .  $P_n$  is any tensor product of  $n$  Pauli operators over  $n$  qubits:  $P_n = \{1, i\} \cdot \{\mathbb{1}, X, Y, Z\}^{\otimes n}$  (technically, there is no need to keep track of  $Y$  as its behaviour is totally fixed by  $X$  and  $Z$  because  $Y = -iXZ$ . Indeed, any combination of  $\{\mathbb{1}, X, Y, Z\}$  can be decomposed into  $X$  and  $Z$ . Neither is needed to track the phases  $\{1, i\}$ .)

Therefore, to show that for some  $U$  it holds  $U \in P_n$  it suffices to show  $U X U^\dagger \in P_n$  and  $U Z U^\dagger \in P_n$ .

**Example:**  $H \in \text{CLIFFORD}_n$  because  $H X H = Z$  and  $H Z H = X$ .

**Example:** The Phase Shift gate  $S = \sqrt{Z} = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$  is also a Clifford Gate:  $S Z S^\dagger = Z$  and  $S X S^\dagger = iY$ .  $S$  gate swaps the  $X$  and  $Y$  axes.

**Example:**  $\text{CNOT} \in \text{CLIFFORD}_n$  as it behaves in the following way:



**Figure 3.5** CNOT Gate Clifford equivalences for  $X_1, X_2, Z_1, Z_2$ . Technically, the remaining cases like  $X_1 X_2$  should also be considered, but as  $\text{CNOT}^\dagger = \text{CNOT}$ , these hold automatically from the single-qubit ones.

A powerful result of the Clifford group is that  $\text{CLIFFORD}_n = \langle H_i, S, \text{CNOT}_{ij} \rangle$ , where the  $\langle \dots \rangle$  notation indicates *the generators of the group*.

In practical terms, this means that any gate that can be decomposed into a combination of  $\langle H_i, S, \text{CNOT}_{ij} \rangle$  is a member of the Clifford group (Example: SWAP gate can be decomposed into 3 CNOTs. Indeed  $\text{SWAP}_{ij} X_i = X_j$  and  $\text{SWAP}_{ij} Z_i = Z_j$ ).

The previous discussion shows that any single qubit rotation can be implemented given a certain entangled state and 3 adaptive measurements. Without loss of generality, we can use a  $|+\rangle$  state as input and transform it to any  $|\psi_{\text{out}}\rangle = U |+\rangle$ .

Another powerful characteristic of Clifford Gates is that they offer simple commutation rules: Being  $U$  a Clifford Unitary and  $Q_n$  and  $R_n$  combinations of Pauli operators over  $n$  qubits, if  $U Q_n U^\dagger = R_n \implies U Q_n = R_n U$ .

In the process of commuting the byproducts  $\Sigma_{g_j}$  to the left in expressions of the form  $U_{g_i} \Sigma_{g_j}$ , two different things can happen:

- If  $U_{g_i}$  is a Clifford Gate, as the byproducts are elements off the Pauli Group  $\Sigma_{g_i} \in P_n$ , it holds  $U_{g_i} \Sigma_{g_j} = \tilde{\Sigma}_{g_j} U_{g_i}$ , where  $\tilde{\Sigma}_{g_j} \in P_n$  is still a product of local Pauli operators. The important point to notice is that  $U_{g_i}$  is unaffected, which means no adaptive measurements are needed.

- If  $U_{g_i}$  is not a Clifford Gate, the byproduct can still be commuted, but now  $U_{g_i}\Sigma_{g_j} = \Sigma_{g_j}\tilde{U}_{g_i}$  where  $\tilde{U}_{g_i} \equiv \Sigma_{g_j}^\dagger U_{g_i} \Sigma_{g_j}$ . This means that the gate applied will vary depending on the measurement outcome  $s$ . Or in other words, that the measurement pattern has to be adapted to counteract the propagation effect ([21], [28]). For example this can be seen in the example above, where the commutation of the byproduct  $X^m$  affects the applied gate  $Z(\alpha)$  such that  $Z(\alpha)X^s = X^s Z((-1)^s \alpha)$ .

### 3.1.2 Limitations of Clifford Circuits: The Gottesman-Knill theorem

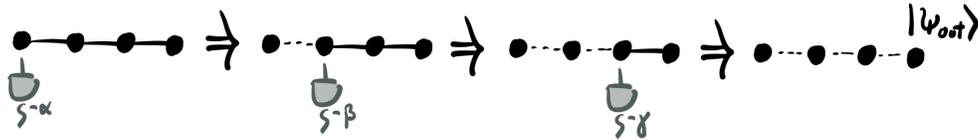
The fact that a Measurement-Based scheme to simulate a circuit consisting merely of Clifford Gates needs no feedforward has some deep consequences in the computational power of such circuits. First of all, in theory all the measurements could be done at the same time, which in theory would mean that the computation runs instantaneously (of course, a final correction of the byproducts should still be carried away). This sounds powerful! However, it is not as good as it seems. In 1998 Daniel Gottesman and Emanuel Knill showed that circuits composed of Clifford Gates can be simulated in polynomial time in a classical probabilistic computer<sup>3</sup> ([16]).

### 3.1.3 Two-qubit gates in MBQC

The central ingredient in Measurement-Based Quantum Computing is an entangled set of qubits called *Graph State* (or *Cluster State*, if the nodes are distributed following a grid). It consists of a bunch of qubits initialized in the  $|+\rangle$  state that are connected following a graph by using CZ operations<sup>4</sup>.

Single qubit evolution can be performed by a linear cluster (as shown in the previous section), while multi-qubit evolution requires 2D clusters<sup>5</sup>. A measurement over a qubit applies a certain gate and moves the quantum state to the neighbouring qubits. It also disentangles the qubit under consideration. This dynamic process can be seen as measurements transforming the quantum state and moving the information through the nodes of the graph.

The power of Cluster States is that, given enough entanglement, any quantum circuit can be implemented solely by adaptive single-qubit measurements. Quantifying *how much* entanglement is needed for a cluster to be *universal* will be discussed later.



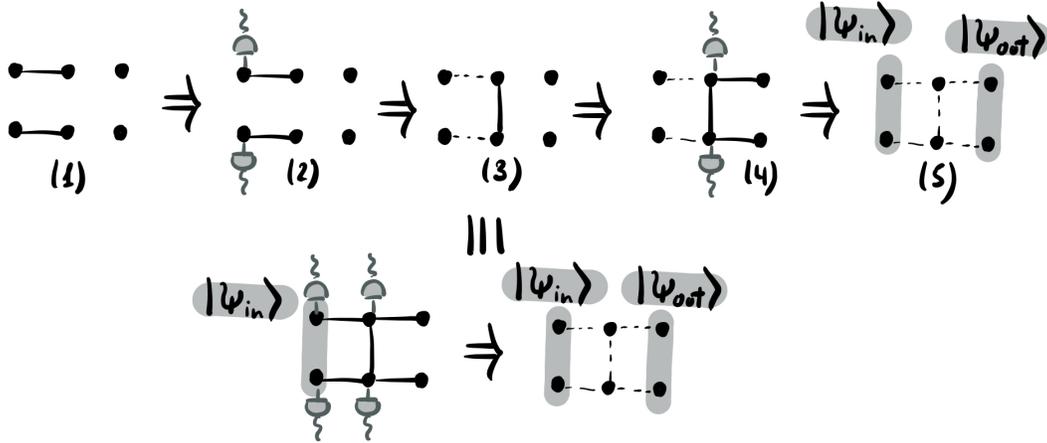
**Figure 3.6** MBQC implementation of an arbitrary single-qubit rotation as the concatenation of 3 rotations. Evolution of a cluster state as measurements are applied to implement a single-qubit rotation. A grey bell-like shape with a  $\theta$  angle inside represents a measurement in a basis  $|0\rangle \pm e^{i\theta} |1\rangle$ . The measurement bases should be adapted based on the previous measurement outcomes.

To show how 2D clusters can implement for example a CZ operation lets consider the following sequence of measurements and entangling operations, shown in Fig. 3.7.

<sup>3</sup>Indeed, Scott Aaronson and Daniel Gottesman implemented the simulation of Clifford circuits into a simple computer program called CHP ([7], [4])

<sup>4</sup>The choice of  $|+\rangle$  state and CZ operation gets inspired from the fact that an Ising interaction between graph neighbours is described in that way.

<sup>5</sup>3D clusters serve as a model for Fault-tolerant QC.



**Figure 3.7** MBQC implementation of a CZ gate. Top: Intuitive application of a CZ gate. Bottom: Measurement-Base approach to apply a CZ, up to local unitaries; the 4 single-qubit measurements over the shown cluster implement a CZ gate:  $|\psi_{out}\rangle = CZ |\psi_{in}\rangle$ .

In Fig. 3.7, it is shown the logic behind. In (1), two entangling operations are created. These vertices will transport the quantum states when, in (2), the first column of qubits are measured. Of course, depending on the measurement bases, a rotation will also be applied to both qubits. In (3) an entanglement in the form of a CZ gate is applied. In (4), two more entanglements are created, and the central column is measured. This effectively disentangles all the qubits and teleports the state to the two qubits on the right. In (5),  $\psi_{out}$  takes all the operations applied previously:  $|\psi_{out}\rangle = R_1 R_2 CZ R_3 R_4 |+\rangle |+\rangle$ .

However, the measurements can always be performed at the end. We could have therefore established all the entanglement at the beginning and just performed the measurements. This is the approach taken in MBQC.

Having shown that a Measurement-Based protocol over a 2D cluster permits to implement any single-qubit rotation and the CZ gate<sup>6</sup>, concludes that the Cluster State is a *universal* resource for Quantum Computation.

### 3.1.4 Building blocks for MBQC

Research carried on by M. S. Tame *et al* in [21] presents a graphical viewpoint to create complex MBQC protocols by concatenating smaller ones. These are referred to as Building Blocks, and can be used as Lego<sup>7</sup> pieces: several can be stacked together and the result is the concatenated effect of them all. A formal justification of why combining them works can be found in [21], but in short it is due to the fact that CZ entangling gates commute with each other. This, combined with the fact that each block is shown to work for arbitrary input states, makes it possible to understand the evolution when measurements are applied to a big cluster as the evolution of the two smaller ones separately, that are afterwards entangled together.

The graphical language to be explained contains information about the qubits, the entanglement connections between them and the measurements performed over some of them. **Note** that the measurements commute with each other, so in principle there is no predetermined order. However, in practice some will be performed before, and their outcomes must be accounted to adapt the future

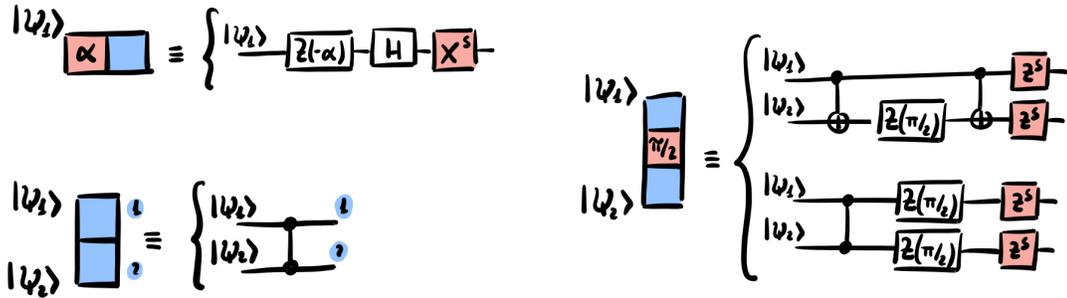
<sup>6</sup>These form a Universal Set of Gates.

<sup>7</sup>Lego, coming from the Danish *Leg-Godt* that means *play well*.

measurements so that the final result is the desired one.

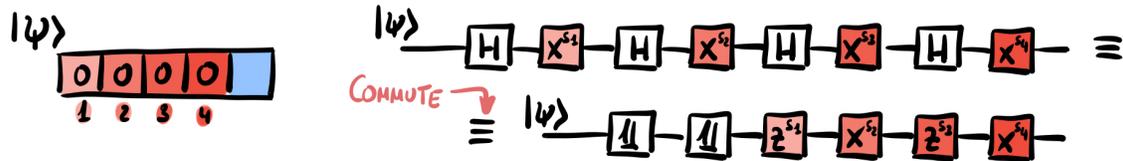
In the graphical notation, the Cluster State is depicted as a set of boxes, such that touching edges represent CZ gates. Measured qubits are drawn red, and the measurement basis is indicated by an angle  $\alpha$ , that this defines a measurement in the basis  $B_\alpha = \{|+\alpha\rangle, |-\alpha\rangle\}$  where  $|\pm\alpha\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm e^{i\alpha}|1\rangle)$ , and  $s$  the measurement outcome ( $s \in \{0, 1\}$ ) Blue boxes indicate the input and output states. When a certain input  $|\psi\rangle$  is shown close to a blue box, this should be understood as the state of such qubit before the CZ are applied to grow the graph state. Each measurement performed may have a side effect in the form of a local unitary Pauli Gate that is applied if the measurement outcome is  $s = 1$ .

The three basic building blocks can be seen in Figure 3.8.



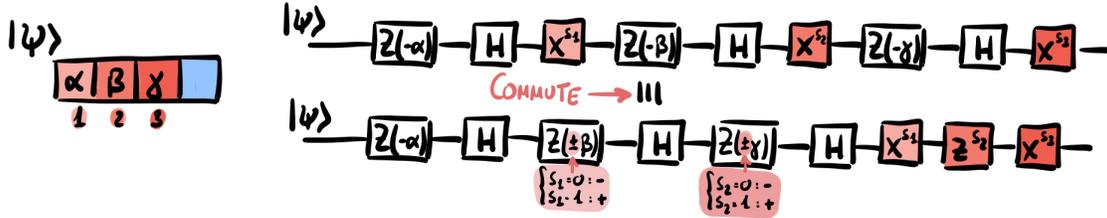
**Figure 3.8** Basic building blocks for MBQC schemes. They can be combined and concatenated on demand. On the left, the measurement scheme; on the right, the equivalent circuit simulated. Taken from Ref. [21].

**Example: Information flow** The most simple example applies measurements in the X eigenstates ( $\alpha = 0$ ) over a linear cluster. Using the blocks, it can be seen that this applies a Hadamard and the corresponding byproduct. An even number of repetitions erases the Hadamards (because its idempotent, say  $H^2 = 1$ ) and simply move the quantum information encoded in the state  $\psi$  around the cluster.



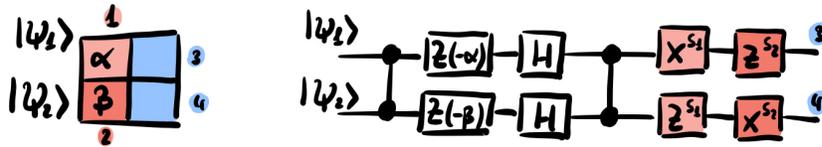
**Figure 3.9** Measurements in the X eigenbasis ( $\alpha = 0$ ) move the state around. The Pauli gates are commuted to the end using  $HZ = XH$ .

**Example: Arbitrary single-qubit unitary** Following the ideas described above, three measurements are enough to implement any arbitrary single-qubit unitary. The gates  $Z(-\alpha)$  are not Clifford gates, which means that commuting the Pauli Gates to the end introduces changes in the measurement bases during the computation that have to be addressed as feedforward.



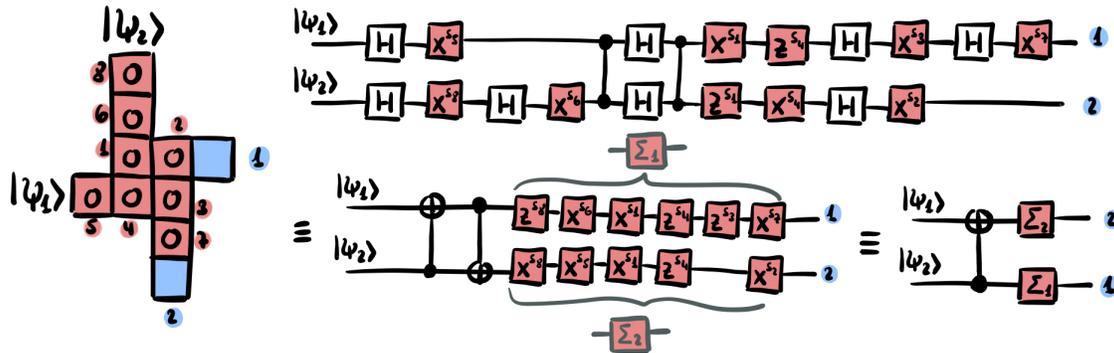
**Figure 3.10** MBQC simulation of single-qubit rotations plus feedforward. The Pauli Gates are commuted to the end using the identity  $XZ(\alpha) = Z(-\alpha)X$ . The angles applied depend on previous measurement outcomes.

**Example: 2D circuit** Combining Blocks it can be obtained what is called the *box cluster*. It is the key ingredient in one of the first experimental implementations of MBQC to show a 2 qubit Grover's algorithm ([26]).



**Figure 3.11** MBQC simulation of a 2D circuit. The Pauli Gates are commuted to the end using the identity  $(X_1 \otimes \mathbb{1})CZ = CZ(X_1 \otimes Z_2)$

**Example: CNOT:** This is an approach that uses 10 qubits in a helix-like entangled state to apply a CNOT gate. An alternative version uses 15 qubits and two linear clusters linked in the middle, as can be seen in Ref. [21].



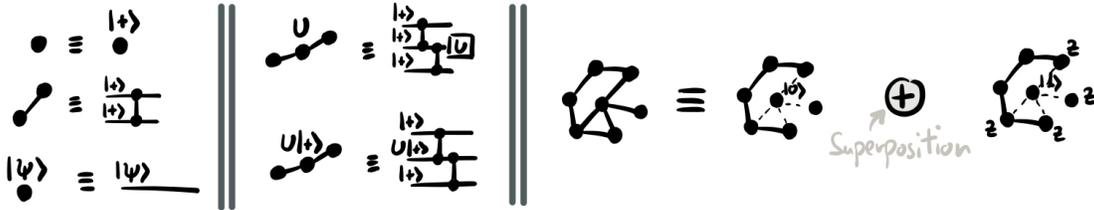
**Figure 3.12** MBQC simulation of a CNOT gate in a helix pattern. In the last step, one of the CNOTs has been merged into a SWAP gate.

### 3.1.5 Graphical language

Cluster States are a powerful tool because they offer a way to picture entanglement avoiding the kets of Dirac notation, which get particularly clumsy as entangled states grow.

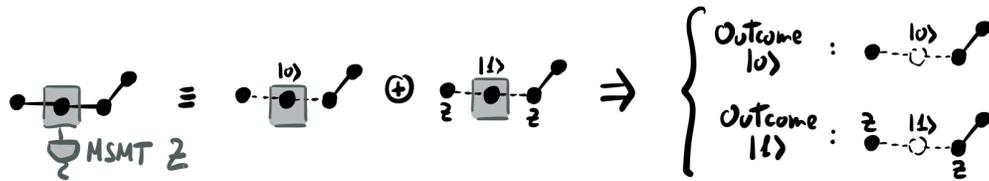
Moreover, the fact that CZ gates commute with each other permits to reorganize the growth of entanglement through the graph. Particularly, this serves to understand why, if a particular qubit in the cluster goes under a certain operation, just its nearest neighbours are affected, leaving the rest of the cluster unaffected. This picture of information flowing through the entanglement nodes is powerful. This picture of clusters can be used to gain a deeper insight on how operations affect the cluster, and to prove some results in a rather visual and intuitive way.

First of all, there has to be a way to picture some basic operations, such as the initialization of a node in a state different than  $|+\rangle$  or the application of local unitaries to particular nodes of the cluster. A visual representations is shown in Fig. 3.13. Secondly, it will be useful to decompose clusters around a particular qubit  $q$  according to the definition  $|0\rangle_q |\psi\rangle + |1\rangle_q \prod_{i \in \text{ng}(q)} Z_i |\psi\rangle$ , where  $\text{ng}(q)$  stands for the first order neighbours of qubit  $q$ .

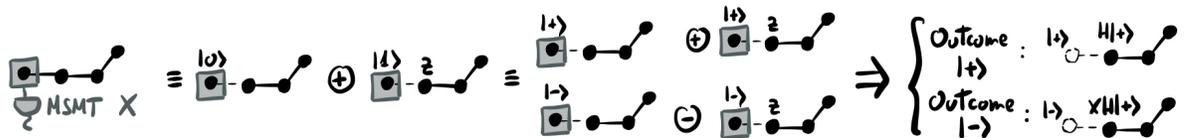


**Figure 3.13** By default, a black dot, or a node, represents a qubit initialized in the  $|+\rangle$  state, unless a different state is indicated, either as  $|\psi\rangle$  or as  $U|+\rangle$ . If a unitary  $U$  is drawn next to a node, this means a local unitary operation. On the right, a cluster is graphically expanded using local unitaries.

With this language, the fact that a measuring a qubit in the Z basis disentangles it from the cluster is straightforward to prove:



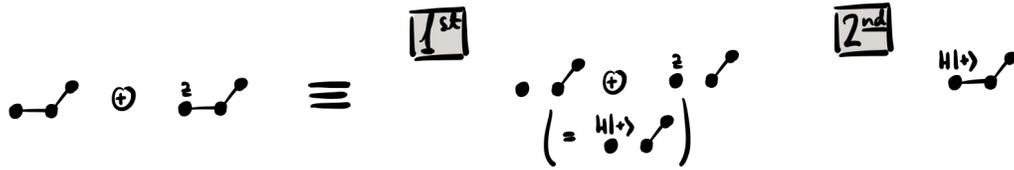
**Figure 3.14** Measuring a qubit in the Z basis effectively disentangles that qubit and cuts the cluster. It also applies a Pauli Z on its neighbours depending on the measurement outcome.



**Figure 3.15** Gate Teleportation upon measurement in X basis, proven graphically. It is shown expanding the cluster as a superposition and changing the basis to  $\{|+\rangle, |-\rangle\}$ :

In the Fig. 3.15, it has been used the fact that the creation of the entanglement with non-direct

neighbours can be postponed after the measurement, as shown in Fig. 3.16.



**Figure 3.16** The superposition of graphs on the left can be understood as a two-step process: First, a superposition of graphs in which the entanglement in the middle is not setup yet is equivalent to the left qubit being initialized in  $H|+\rangle$ . Second, the missing entanglement is finally setup. This works before the  $CZ$  commute with the  $Z$  local unitary.

# Chapter 4

## Merging clusters with Fusion Gates

“Everything is artifice and mere appearance”

---

Miguel de Cervantes, *Don Quixote*.

Measurement-Based Quantum Computing (QC) is a powerful approach that solves the problem of noisy gates by not applying gates at all. Instead, measurements, which can be performed with high accuracy, are used to emulate gates over quantum circuits. However, MBQC requires a graph state big enough that will be consumed as the computation advances<sup>1</sup> In this chapter *fusion gates* will be presented as a tool to merge small clusters into larger ones. Type-I and Type-II will be discussed, and modifications to the Type-II will lead to the Rotated Type-II, and a proposed fusion gate called *Dynamic Type-II*. These can be used for Percolation-Based QC, to be introduced in Chapter 5. Moreover fusion gates will be related to linear optics as Bell State Measurements. This allows implementing them as integrated photonic circuits.

### 4.1 Merging clusters together

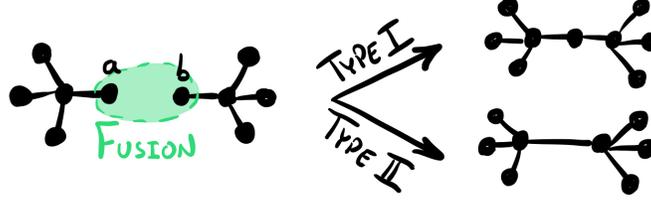
The idea behind a fusion mechanisms is an operation that takes two clusters and entangles them together.

In global terms, two types of fusion operations can be performed: Type-I and Type-II.

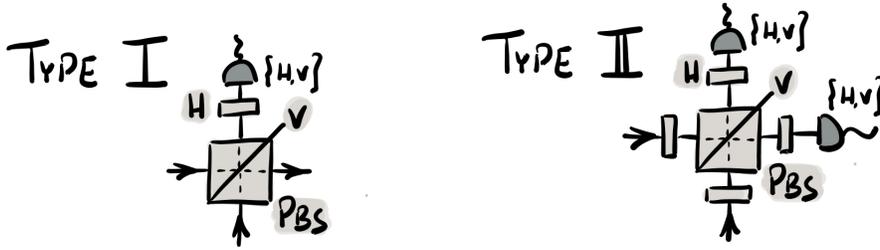
In a really high level, fusion gates work by performing polarization rotations with PBS and measurements in the  $\{H, V\}$  basis. The core idea is to delete polarization information before the measurement, so that when this is performed, the resulting state is in an entangled superposition state. Both fusion gates are performed by Bell State Measurements, which makes them suitable for interferometers and integrated optics circuits. Upon success, they entangle the clusters together. However, as they depend on measurement outcomes, their success rate is probabilistic. As a summary of the properties that will be discussed below, both Type-I and Type-II have a success rate of 50% (even though this can be boosted, as will be discussed later). Type-I consumes one qubit of the cluster, while Type-II consumes two. However, Type-II is heralded, which means that photon losses

---

<sup>1</sup>State of the art cluster state research has created cluster states with thousands of qubits encoded in continuous variables of photons. This approach is called Continuous Variables Quantum Information Process. See Ulrik L. Andersen *et al* in Ref. [24].



**Figure 4.1** Type-I and Type-II fusion gates results upon success. This picture shows a motivation of the idea of fusion. The full details, such as local unitaries resulting from the operation, are not displayed. Precisely the bottom picture represents a *Rotated* Type-II, that is discussed later in this chapter.



**Figure 4.2** Type-I and Type-II fusion gates implemented with optical devices. Both of them employ a PBS that reflects one of the modes at each input (in this case, the vertical one, indicated by a line with a V letter) and polarization rotations (gray slabs) that perform a Hadamard-like operation between  $\{|H\rangle, |V\rangle\}$  and  $\{|H\rangle \pm |V\rangle\}$ . In Type-II, preceding the inputs and outputs of the PBS by polarization rotators has the effect of a PBS acting in the rotated  $\{|H\rangle \pm |V\rangle\}$ . This is said to be a PBS *cut to diagonal polarization*.

can be detected. In both cases detectors have to be photon-number resolving<sup>2</sup>. All this makes Type-II more appealing for Fusion-Based Quantum Computing, to be discussed in Chapter 5.

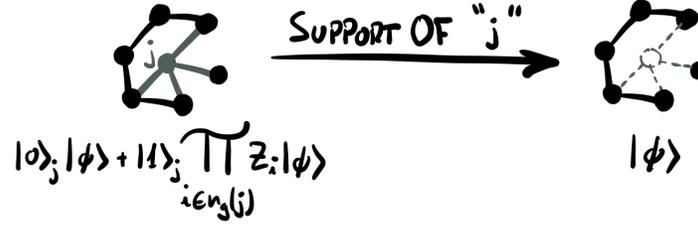
In the rest of the chapter a polarization encoding for qubits will be used, as it is more enlightening to describe fusion gates.

In order to develop a formalism to describe the action of fusion gates, first the CZ operation must be made explicit. Given a certain cluster state  $|\psi\rangle$  composed of nodes initialized in the state  $|+\rangle_i$  that are linked using CZ operations, we define a subcluster (called *support of a qubit  $j$*  and denoted as  $|\phi\rangle$ ) as the cluster resulting from disentangling qubit  $j$  from the initial cluster. This can be achieved applying CZ to the neighbours of  $j$ , denoted  $\text{ng}(j)$ :

$$|\psi\rangle = |0\rangle_j |\phi\rangle + |1\rangle_j \prod_{i \in \text{ng}(j)} Z_i |\phi\rangle \xrightarrow{\text{disentangle } j} |+\rangle_j |\phi\rangle = \prod_{i \in \text{ng}(j)} CZ_{ij} |\psi\rangle$$

Disentangling is easy to achieve because CZ is its own inverse.

<sup>2</sup>Current photon number resolving detectors need to be cooled down, while the rest of the integrated photonics chip can operate at room temperature. This is one advantage of photonics based quantum computers.



**Figure 4.3** The *support* of a qubit  $j$  is defined as the cluster resulting from disentangling  $j$  from the graph.

### 4.1.1 Type-I fusion

Consider the case in which 2 clusters are to be fused through qubits  $a$  and  $b$  (see Fig. 4.3). As always, each of these clusters are defined by initializing all the qubits in the  $|+\rangle$  state and applying CZ operations where links want to be established. Before the fusion operation, both clusters can be described as:

$$\left( |0\rangle_a |\psi\rangle + |1\rangle_a \prod_{i \in \text{ng}(a)} Z_i |\psi\rangle \right) \otimes \left( |0\rangle_b |\phi\rangle + |1\rangle_b \prod_{i \in \text{ng}(b)} Z_i |\phi\rangle \right)$$

where  $|\psi\rangle$  and  $|\phi\rangle$  represent the subclusters entangled to qubits  $a$  and  $b$  respectively. The notation  $\text{ng}(a)$  refers to the set of qubits having links with  $a$ .



**Figure 4.4** Type-I successful result. Alternatively, it can also yield the same cluster but with some local unitary gates, as will be shown later.

The idea of the Type-I fusion is to create an operation such that, upon success, switches qubit labels  $a$  and  $b$  for a new label  $c$  and outputs a state with the form:

$$\left( |0\rangle_c |\psi\rangle + |1\rangle_c \prod_{i \in \text{ng}(a)} Z_i \prod_{j \in \text{ng}(b)} Z_j |\phi\rangle \right)$$

A convenient way to realize a Type-I fusion gate employs a PBS where one output mode is rotated and then measured in the  $\{H, V\}$  basis:

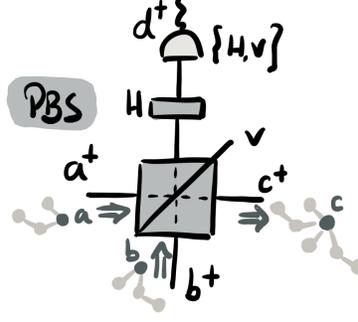
To see why this works, let's work in a polarization encoding where the logic states are encoded as  $\{|0\rangle, |1\rangle\} \rightarrow \{|H\rangle, |V\rangle\}$ . As defined before, let's denote  $|\psi_a\rangle$  and  $|\psi_b\rangle$  to the support of qubits  $a$  and  $b$  respectively.

With all this notation, the initial clusters can be written as:

$$\left( |H\rangle_a |\psi_a\rangle + |V\rangle_a \prod_{i \in \text{ng}(a)} Z_i |\psi_a\rangle \right) \otimes \left( |H\rangle_b |\psi_b\rangle + |V\rangle_b \prod_{i \in \text{ng}(b)} Z_i |\psi_b\rangle \right)$$

The former expression can be read as input modes  $a$  and  $b$  being entangled with some other modes in the polarization encoding.

To prove the effect of Type-I fusion it is easier to switch to the Heisenberg picture and work with the transformations of operators under linear optics. Initially, the two input clusters can be



**Figure 4.5** Detection in the  $\{H, V\}$  basis with photon number discrimination. The polarization rotation, depicted by a grey slab, is like a Hadamard transformation, in which  $|H\rangle \rightarrow \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ .

described as:

$$(f_1 \hat{a}_H^\dagger + f_2 \hat{a}_V^\dagger) \otimes (g_1 \hat{b}_H^\dagger + g_2 \hat{b}_V^\dagger) |\emptyset\rangle$$

where  $f_1, f_2$  and  $g_1, g_2$  are arbitrary functions of the creation operators that describe the states  $|\psi_a\rangle$ ,  $\prod_{i \in \text{ng}(a)} Z_i |\psi_a\rangle$  and  $|\psi_b\rangle$ ,  $\prod_{i \in \text{ng}(b)} Z_i |\psi_b\rangle$  respectively. These are the supports of  $a$  and  $b$ , and the same supports but with some local  $Z$  gates acting upon the neighbours of  $a$  and  $b$ . Even though the polarization encoding is being used here, the idea is easily adapted to other encodings and modes.

Substituting the transformation of the PBS and the polarization rotation, the following expression is obtained (see the Appendix for the full calculation):

$$\hat{d}_H^\dagger (f_1 g_1 \hat{c}_H^\dagger + f_2 g_2 \hat{c}_V^\dagger) + \hat{d}_V^\dagger (f_1 g_1 \hat{c}_H^\dagger - f_2 g_2 \hat{c}_V^\dagger) + \frac{1}{\sqrt{2}} (\hat{d}_H^{\dagger 2} - \hat{d}_V^{\dagger 2}) f_2 g_1 + \hat{c}_H^\dagger \hat{c}_V^\dagger f_1 g_2$$

Note that the previous expression is not normalized. However, it is the relative weights that are important.

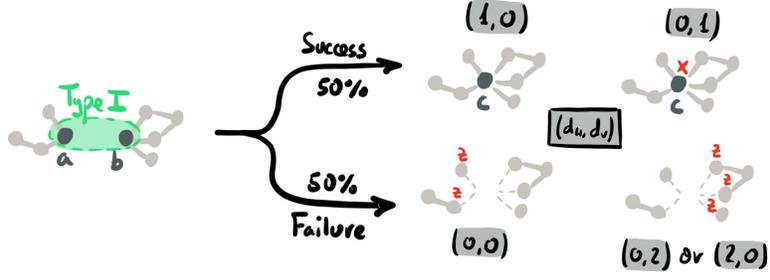
Upon detection in mode  $d$ , with outcomes denoted as  $(d_H, d_V)$ , four scenarios can arise:

$$\begin{aligned} (1, 0) : & \quad \frac{1}{\sqrt{2}} (f_1 g_1 \hat{c}_H^\dagger + f_2 g_2 \hat{c}_V^\dagger) |\emptyset\rangle \\ (0, 1) : & \quad \frac{1}{\sqrt{2}} (f_1 g_1 \hat{c}_H^\dagger - f_2 g_2 \hat{c}_V^\dagger) |\emptyset\rangle \\ (0, 0) : & \quad f_1 g_2 \hat{c}_H^\dagger \hat{c}_V^\dagger |\emptyset\rangle \\ (2, 0) \text{ or } (0, 2) : & \quad f_2 g_1 |\emptyset\rangle \end{aligned}$$

In the cases where a single photon is detected in one of the modes, entanglement is created between the two input clusters. In the other cases, the output is a product state, therefore not entangled. The four scenarios are equiprobable which means a successful Type-I fusion happens with a 50% probability.

Using the graphical language introduced at the end of Chapter 3, the four outcome scenarios are depicted in Figure 4.6

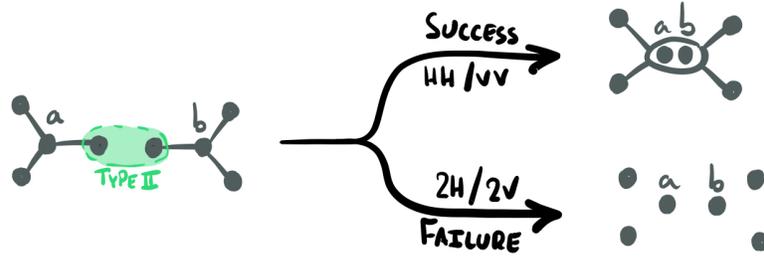
One of the problems of Type-I gates is that a failure combined with a lost photon has the same signature as a success. This can lead to misimplementation of the MBQC protocol.



**Figure 4.6** Type-I possible scenarios upon detection outcomes on mode  $d$ . In some cases, local Pauli operations are applied (depicted in red). Note that failure erases some entanglements. The way this graphs are depicted is through the *graphical language*, introduced at the end of Chapter 3

### 4.1.2 Type-II fusion

The Type-II fusion works similarly to Type-I, but now the two output modes of the Polarization Beam Splitter are measured in the  $\{H, V\}$  basis. This is shown in Figure 4.3. Moreover, the PBS used now is built to split the diagonal polarizations  $|H\rangle \pm |V\rangle$ . This transformation equivalent to rotating the inputs and outputs to a regular  $\{H, V\}$  PBS by  $45^\circ$ .



**Figure 4.7** Graphical representation of the outcomes of a successful and failed Type-II fusion. This figure will be discussed again later, but its worth mentioning that upon failure lots of entanglement is lost.

Substituting the transformations of the operators in Figure 4.3, the transformation takes the form (for the full details, see Ref. [20]):

$$\begin{aligned} & (f_1 + f_2)(f_3 - f_4)(\hat{c}_H^{\dagger 2} - \hat{c}_V^{\dagger 2}) + (f_1 - f_2)(f_3 + f_4)(\hat{d}_H^{\dagger 2} - \hat{d}_V^{\dagger 2}) + 2(f_1 f_3 + f_2 f_4)\hat{c}_H^{\dagger}\hat{d}_H^{\dagger} \\ & + 2(f_1 f_4 + f_2 f_3)\hat{c}_H^{\dagger}\hat{d}_V^{\dagger} + 2(f_1 f_4 + f_2 f_3)\hat{c}_V^{\dagger}\hat{d}_H^{\dagger} + 2(f_1 f_3 + f_2 f_4)\hat{c}_V^{\dagger}\hat{d}_V^{\dagger} \end{aligned}$$

Detection is performed in the modes  $c$  and  $d$  with photon number discrimination. Depending on the detection pattern  $(c, d)$ , the output state might look like the following:

$$\begin{aligned}
 (H, H) \text{ or } (V, V) &: (f_1 g_1 + f_2 g_2) |\emptyset\rangle \\
 (H, V) \text{ or } (V, H) &: (f_1 g_2 + f_2 g_1) |\emptyset\rangle \\
 (2H, 0) \text{ or } (2V, 0) &: (f_1 + f_2)(g_1 - g_2) |\emptyset\rangle \\
 (0, 2H) \text{ or } (0, 2V) &: (f_1 - f_2)(g_1 + g_2) |\emptyset\rangle
 \end{aligned}$$

When one photon is found in each mode, entanglement is preserved; however, in those cases where photons are bunched in the same mode, the two clusters remain as a product state and therefore disentangled. All the possibilities have the same probability. Hence, we say that Type-II is a fusion gate with a 50% success probability. It is heralded, meaning that the detection of one photon in each mode guarantees success.

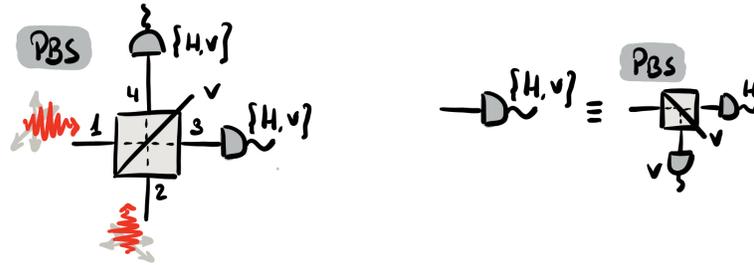
Fusion gates are not regular quantum gates (they consume resources). However, they can be used to create big entangled states such as graph states. The first of these proposals is due to Brown and Rudolph [10].

### 4.1.3 Bell-State Measurement (BSM)

An alternative way to understand the operation of Type-II fusion gates is as a Bell-State Measurement (BSM). A BSM is intended to distinguish between the maximally-entangled Bell states  $\{|\psi^\pm\rangle \sim (|01\rangle \pm |10\rangle), |\phi^\pm\rangle \sim (|00\rangle \pm |11\rangle)\}$ . Therefore, a BSM is a projection onto these states.

Following the original ideas by Braunstein and Mann in 1995 in [9], a PBS can be used to implement an optical version of a BSM. However, as it will be discussed, it is not possible to implement the full BSM in linear optics, which means that not all the 4 Bell-States can be discriminated deterministically. As a consequence, Type-II fusion gates have to be probabilistic entangling gates.

A regular PBS is considered upon two input spatial modes 1 and 2, each of them implementing a qubit in the polarization encoding. As always, the logical  $\{|0\rangle_i, |1\rangle_i\}$  in spatial mode  $i$  are encoded by  $\{|H\rangle_i, |V\rangle_i\}$ . (**Notation:**  $|H_i V_j\rangle \equiv |H\rangle_i |V\rangle_j$ ). The setup requires of a regular PBS and two detectors able to distinguish polarization, as in Figure 4.8.



**Figure 4.8** On the left, setup to discriminate the Bell States  $|\psi^\pm\rangle$  vs  $|\phi^\pm\rangle$ . The PBS reflects the vertical component; On the right, the practical implementation of a measurement in the  $\{H, V\}$  polarization basis.

The PBS applies the following transformation to the Bell-States:

$$\begin{aligned}
 |\psi^\pm\rangle &\sim (|H_1 V_2\rangle \pm |V_1 H_2\rangle) \xrightarrow{\text{PBS}} (|H_3 V_3\rangle \pm |H_4 V_4\rangle) \\
 |\phi^\pm\rangle &\sim (|H_1 H_2\rangle \pm |V_1 V_2\rangle) \xrightarrow{\text{PBS}} (|H_3 H_4\rangle \pm |V_3 V_4\rangle)
 \end{aligned}$$

It is straightforward to check that the detection signature in detectors 3 and 4 allow to distinguish  $|\psi^\pm\rangle$  versus  $|\psi^\pm\rangle$ , but do not serve to distinguish neither  $|\psi^+\rangle$  versus  $|\phi^+\rangle$  nor  $|\phi^+\rangle$  versus  $|\phi^+\rangle$ .

It is possible to decide which 2 Bell-States we want to be able to discriminate, as linear optics permits to transform between Bell-States.

A fully deterministic BSM that only uses linear optics and vacuum ancillary vacuum states has been proven impossible (Ref. [33]). However, there are other types of methods that boost the success probability as close to unity as desired, at the cost of using and increasing number of entangled ancillary states and single photons. These ideas are motivated on the original KLM scheme [12], even though modern versions are much simpler and will be discussed down below.

It has been shown that the effect of a PBS is to implement a probabilistic BSM. The scheme used to do so is the same used for Type-II fusion except that there the PBS is cut to split  $\{|H\rangle \pm |V\rangle\}$ . These two situations are equivalent. Hence, a Type-II fusion is effectively a BSM in some slightly modified Bell-States. A powerful consequence of this result is that the same methods that boost BSM can be used to boost the success probability of Type-II fusion. This is an advantage in comparison to Type-I, for which no boosting method has neither been found nor proven impossible.

With the previous results in mind, the operation of Type-II gates can be better understood as a projection off the input states onto the Bell States. This result, taken from Ref. [15], is briefly reproduced here for clarity. In short, we want to show that certain detection signatures effectively project the inputs into certain Bell States. These are those cases:

Successful fusion (one photon per output):

$$h_3 h_4 \text{ and } v_3 v_4 \iff \frac{1}{\sqrt{2}} (|++\rangle_{1,2} + |--\rangle_{1,2}) \quad (4.1)$$

$$h_3 v_4 \text{ and } v_3 h_4 \iff \frac{1}{\sqrt{2}} (|++\rangle_{1,2} - |--\rangle_{1,2}) \quad (4.2)$$

Failed fusion:

$$h_3^2 \text{ and } v_3^2 \iff |+-\rangle_{1,2} \quad (4.3)$$

$$h_4^2 \text{ and } v_4^2 \iff |-+\rangle_{1,2} \quad (4.4)$$

To check these results, the idea is to run the Type-II fusion gate backwards and see that the detection signature corresponds to the indicated Bell-State. A complete discussion is found in [15], but for the shake of completeness, let's show one case of success and failure:

$$h_3 h_4 \xrightarrow{\text{Final Pol. Rot.}} p_3 p_4 = h_3 h_4 + h_3 v_4 + v_3 h_4 + v_3 v_4 \xrightarrow{\text{PBS}} h_1 h_2 + h_1 v_1 + v_2 h_2 + v_2 v_1 \xrightarrow{\text{Initial Pol. Rot.}} p_1 p_2 + p_1 m_1 + m_2 p_2 + m_2 m_1$$

However, we assume implicitly when operating a fusion that there is just one input photon per mode. This reduces the number of terms in the superposition to:

$$h_3 h_4 \iff p_1 p_2 + m_1 m_2$$

being this last input the Bell State  $|++\rangle_{1,2} + |--\rangle_{1,2}$ .

In one of the cases of failure:

$$h_4^2 \xrightarrow{\text{Final Pol. Rot.}} p_4^2 = h_4^2 + v_4^2 + 2h_4 v_4 \xrightarrow{\text{PBS}} h_2^2 + v_1^2 + 2h_2 v_1 \xrightarrow{\text{Initial Pol. Rot.}} p_2^2 + m_2^2 + 2p_2 m_1$$

Again, considering only one photon per input:

$$h_4^2 \iff m_1 p_2$$

being this last input the Bell State  $|-\rangle_{1,2}$ .

This formalism is useful because it serves as a tool to analyze the evolution of the states in Dirac formalism under Type-II fusion.

**For example**, let's analyze the fusion of two 4-qubits GHZ states under Type-II gate:

$$|\text{GHZ}\rangle_{1,2,3,4} \otimes |\text{GHZ}\rangle_{5,6,7,8} = \frac{1}{2} (|0+++ \rangle_{1,2,3,4} + |1--- \rangle_{1,2,3,4}) \otimes (|0+++ \rangle_{5,6,7,8} + |1--- \rangle_{5,6,7,8})$$

A Type-II fusion is performed on qubits 2 and 6 (two of the arms). If successful with signature  $hh$  or  $vv$ , the resulting state is:

$$\left( \frac{\langle ++|_{2,6} + \langle --|_{2,6}}{\sqrt{2}} \right) |\text{GHZ}\rangle_{1,2,3,4} \otimes |\text{GHZ}\rangle_{5,6,7,8} = \frac{1}{\sqrt{2}} (|0++0++ \rangle_{1,3,4,5,7,8} + |1--1-- \rangle_{1,3,4,5,7,8})$$

which is similar to a 4-legged GHZ state in which qubits 1 and 4 both act as a single center. This is called redundant encoding, because even if one of both is lost, the cluster structure remains unaffected.

Upon failure with signature  $h^2$  or  $v^2$ :

$$\langle +-|_{2,6} |\text{GHZ}\rangle_{1,2,3,4} \otimes |\text{GHZ}\rangle_{5,6,7,8} = |0++1-- \rangle_{1,3,4,5,7,8}$$

which is a totally disconnected graph with some local unitaries over some of the qubits. Of course, other success/failure signatures would produce different results but with the same entanglement properties.

The outcome from the former sample case is that, even when the Type-II fusion succeeds, the outcome entanglement is what one would expect. The redundantly encoded qubit breaks the symmetric appearance of the cluster state. A modified version of Type-II fusion in which an entanglement link is established between qubits 1 and 5, as one would desire Type-II to behave, can be accomplished by introducing some variations to the fusion gate. This, and other possible variations, will be studied in the next section.

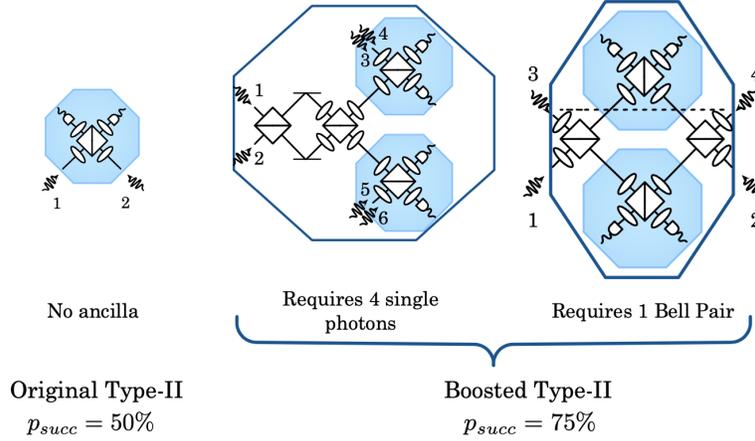
## 4.2 Modified Type-II fusion gates

### 4.2.1 Boosted Type-II fusion

The success rate of Type-II fusion gates can be improved by using extra resources such as single photons ([13]) or Bell Pairs ([17]). The boosted strategy is inspired by the one followed by Knill, Milburn and Laflamme in Ref. [12]. Based on these results and the work done in Ref. [15], an improved version of Type-II fusion with  $p_{\text{success}} = 75\%$  can be built, as shown in Fig. 4.9.

These variants implement the same Type-II transformation as the simple Type-II fusion. Therefore, the measurement signature heralds success and failure of the fusion. Moreover, they inherit the same loss tolerance as the simple Type-II.

As a short discussion, note that the one requiring single photons needs a total of 4 extra photons, while the one using an ancillary bell pair just 2. Even though a Bell pair is more sophisticated in terms of entanglement, both are equivalent as there are procedures to (deterministically) obtain a Bell pair from 4 single photons.



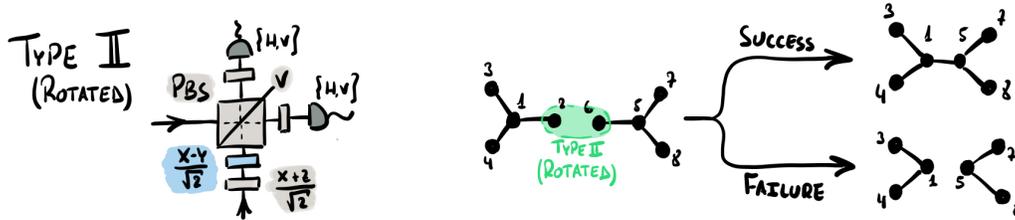
**Figure 4.9** A boosted version off the Type-II fusion. Image from Ref. [15].

There is nevertheless a small difference between both procedures that arises when considering loss of photons: the more photons involved in the operation, the higher chance we might lose one.

The loss of a photon is a severe problem in an entangled graph. This is because an lost photon will eventually interact with the environment and collapse, leaving an unknown side-effect in the rest of the cluster.

### 4.2.2 Rotated Type-II fusion gates

Changing the polarization of the photons before they interfere in the PBS gives raise to different projection operations when the measurements are performed. This results in different entanglement dynamics when the fusion is performed. It is of particular interest the modification of the Type-II fusion shown in Figure 4.10, described in Ref. [15].



**Figure 4.10** The rotated fusion keeps more entanglement than the normal fusion upon failure. It is discussed in Ref. [15].

This gate behaves in a much more interestingly way: upon success, entangles the neighbouring qubits; and in case of failure, just avoids the entanglement, but does not disentangle the rest of the cluster. A complete and formal description of the transformations implemented by the gate can be found in [15], but for the purpose of this thesis, this qualitative analysis of the behaviour is enough. There is a point to note however, and it is that, if studied carefully, some unitaries are applied to certain qubits. However, these can be known beforehand and taken into account to adjust the measurement pattern accordingly.



## Chapter 5

# Towards Fusion-Based Quantum Computing

“La biblioteca es ilimitada y periódica. Si un eterno viajero la atravesara en cualquier dirección, comprobaría al cabo de los siglos que los mismos volúmenes se repiten en el mismo desorden (que, repetido, sería un orden: el Orden). Mi soledad se alegra con esa elegante esperanza.”

---

Jorge Luis Borges, *La biblioteca de Babel*.

This chapter is aimed to propose some ideas to put together the different components explained in the previous chapters to create a resource for MBQC that can be escalated to create a fault-tolerant universal quantum computer.

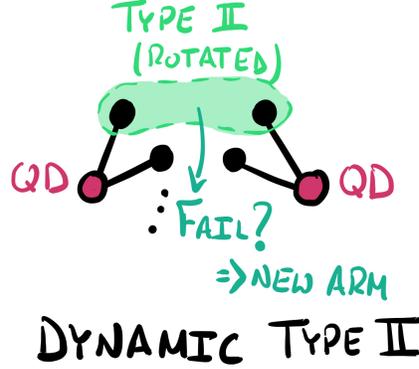
First of all, a dynamic version of the Type-II fusion gate is proposed to boost the overall success probability without external resources. Second of all, a percolation based approach to grow scalable cluster states is discussed

### 5.1 Improved Type-II with no ancillary resources

The Rotated Type-II fusion gate as depicted in 4.10 is an interesting tool: it succeeds with 50% probability and it is heralded upon photon loss. If successful, it entangles links the clusters and if not, at least it keeps the rest of entanglement. However, for some situations, a 50% success probability might not be enough; an alternative proposal, in the Boosted Type-II can achieve 75% with the addition of external resources. Type-II gate can be boosted even higher at the cost of adding an exponential number of external resources.

An alternative approach uses the Photonic Machine Gun discussed before to boost the success probability with a try-until-succeed approach. The idea is to produce a new pair of photons if the previous Type-II fusion fails. It will be referred to as *Dynamic Type-II*. This procedure can be seen in Figure 5.2.

Intuitively, as many repetitions as necessary until a successful fusion happen will lead to both QDs being fused sooner or later. However, things change when we consider photon losses:



**Figure 5.1** GHZ states are grown around the Spin QD qubit sequentially if the previous fusions failed. The black dots, which are photonic qubits, are referred to as *arms*

### 5.1.1 Photon losses for the Dynamic Type-II

In the event of photon being lost, all the qubits entangled with the lost photon become meaningless. Therefore they must be cut and discarded (for example, through a Z-basis measurement). This is because a lost photon will eventually collapse the cluster in an unknown state, and this collapse might transfer in the worst scenario to every qubit entangled with the affected one. Therefore, photon loss is an incorporated challenge that reduces the success probability of fusion gates, independently from the fusion process itself:

Now, the probability of the two QD being fused together depends on

- One fusion eventually succeeds, with probability  $p$ .
- None of the previous photons emitted is lost. A photon loss happens with probability  $\eta$ .

Therefore, the probability of success after  $M$  trials of the previous protocol is:

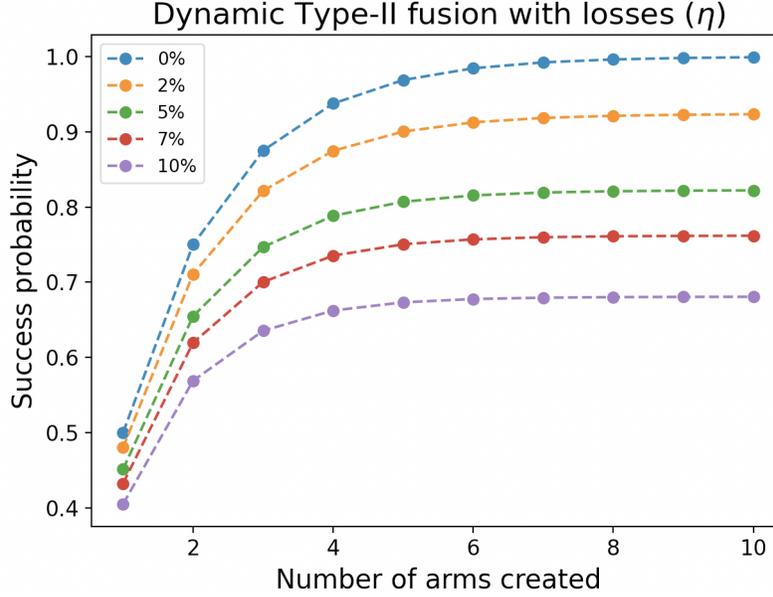
$$\mathcal{P}(\text{QDs are fused}) = \sum_i^{M-1} p(1-p)^i \eta^{2(i+1)}$$

where the factor of 2 account for the fact that each fusion trial involves a pair of photons. This is a geometric series that can be added up.

Figure 5.2 gathers the results of evaluating the previous expression considering several loss probabilities.

Several things can be noted from Figure 5.2: first of all, the success probability saturates no matter how many repetitions of the protocol are considered. This is because sooner or later a photon will be lost, and this will destroy the whole process; second of all, this saturation value depends on  $\eta$ ; in third place, it should be noted that for  $\eta = 5\%$ , the saturation line is above 75% even for  $M=3$  (6 photons involved in the whole process). This is an improvement over the normal Type-II fusion gate, as that gate, involving 6 photons as well and a complex array of linear optical elements, achieves 75% assuming no losses.

It is worth considering that the process discussed is sequential and ballistic: the optical circuit implementing the fusion operations can be reused for the new trials; moreover, as the QD can be excited to emit a pair of photons when needed there is no need for external memories. Moreover, no fast-switching is needed.

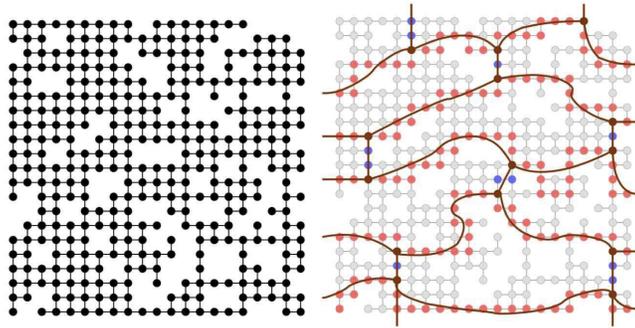


**Figure 5.2** Probability of success of the Dynamic Type-II protocol described above for several values of  $\eta$ . Note that with just 3 arms are needed to get a probability a success above 75% and tolerate a photon loss probability of 5%.

## 5.2 Percolation theory & how to use it

As outlined in Chapter 3, and proven in [28], a 2D cluster state is a universal resource for quantum computing using MBQC. Moreover, it has been shown that a 3D lattice can serve to implement fault-tolerant quantum computing. Therefore it is desirable to have a reliable procedure to grow 3D clusters scalably.

The difficulty lies however in combining small clusters ( $<10$  qubits) available experimentally into big graphs. Fusion gates seem to fill the gap: they offer a probabilistic operation that binds together clusters. The question is how to get a probabilistic operation to behave deterministically. And the answer is in percolation theory.

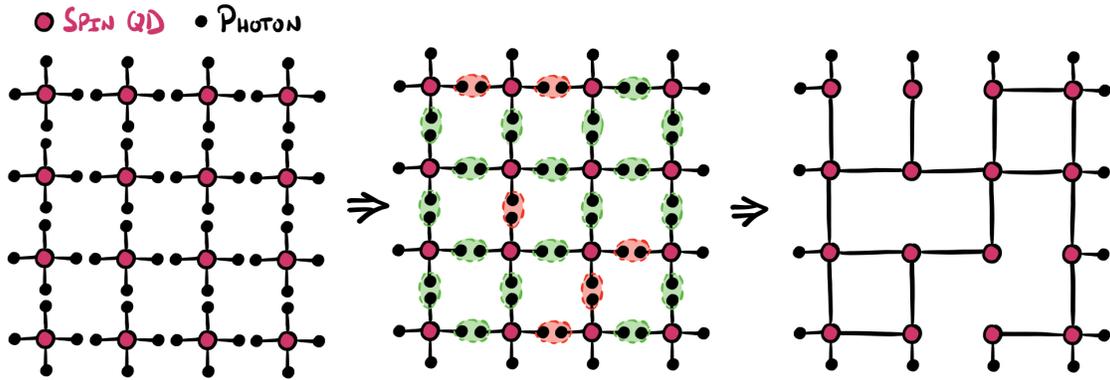


**Figure 5.3** A percolating cluster can be reduced and transformed deterministically into a graph state. Leftover qubits can be disentangled through Z-measurements, and where to cut is a classical algorithm solvable in polynomial time (Ref. [19]). Image courtesy of [19].

The phenomenon of percolation is of paramount importance in classical and statistical mechanics.

In few words, it studies the process through which a set of nodes that are connected with a certain probability  $p$  can give rise to a connected graph that spans through the whole lattice. This is controlled by the *percolation threshold*  $p_c$ , a quantity characteristic of a certain topology. If  $p > p_c$  the systems is in the *super-critical* regime and a percolating cluster appears. If the linear size of the lattice is  $L$ , the percolating cluster has a size that escalates as  $\mathcal{O}(L)$ ; if  $p < p_c$ , called *sub-critical regime*, the biggest cluster spans as  $\mathcal{O}(\log L)$ , which means that it eventually stops spanning and does not percolate over the whole lattice. This can serve as a signature of percolation behaviour. However, the percolation threshold might be defined from a graph representing the percolation phase transition by plotting the probability of percolation as a function of the probability of bonds  $p$ . An image like that is shown in Figure 5.6.

In this thesis it will be used the model of *bond-percolation*, as the Cluster State will consist on a set of nodes (qubits) that will be connected with bonds with a probability  $p$ .



**Figure 5.4** Bond percolation establishment in a 2D square lattice. On the left, the resources are 5-GHZ states grown around the spin QD qubit; on the middle, fusion gates are performed over the photons; on the right, the final cluster is established over the spin QD qubits.

To our interest, it is easy to convince oneself that a percolated lattice is a Universal resource for MBQC. By definition, a percolated network is such that there can be found a connected set of nodes that spans through the whole network, no matter how big it is.

It is easy to see why a percolated network is at least as computationally powerful as a regular 2D or 3D grid: this is because one can find a subset of the percolated grid that is actually such 2D or 3D grid, as shown in Figure 5.3. A systematic approach to convert a percolated lattice into a regular square or cubic grid is shown in Ref. [19].

The main takeaway is that an intelligent use of the fusion gates that produces a percolating network is a universal resource for MBQC.

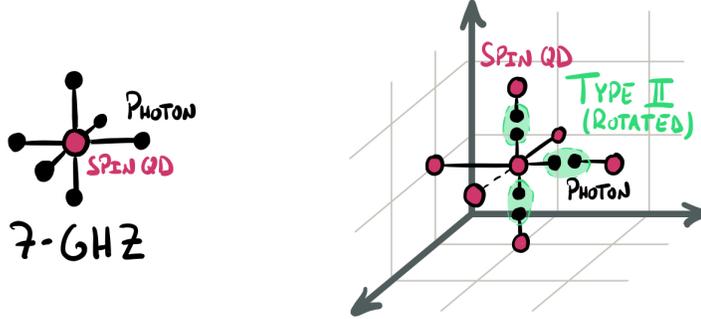
### 5.3 Growing a percolating lattice

The gap between small graph states and a full 3D cluster state is to be filled by fusion gates. In particular, the Rotated Type-II fusion gate is to be used, as it is heralded, has a success probability of 50% and keeps most entanglement upon failure (see Figure 4.10).

At this point, there are two questions to approach: What is the best protocol to use the previous ingredients to build a 3D cluster? And how is this protocol affected upon photon losses?

### 5.3.1 The protocol

The most naïf approach to grow a percolating 3D lattice is to use a *cubic* topology in which each node is populated by a spin QD qubit entangled with 6 photons. The Rotated Type-II Fusion Gate is performed to entangle neighbouring qubits. A representation of this process can be seen in Figure 5.5.



**Figure 5.5** The percolated lattice is built from a cubic grid. On the left, the small resource state, grown from the QD with 6 repetitions of the GHZ pulse sequence; on the right, the entangling operation: some of the fusions have succeeded, represented as continuous lines, and some failed, pictured as discontinuous lines.

The regular bond percolation over a cubic lattice has a percolation threshold  $p_c = 24.8\%$  (Ref. [2]). Therefore the Type-II fusion should be enough to enter in the super-critical regime and therefore achieve a percolating cluster.

Given that the Photonic Machine Gun described in Chapter 2 can generate GHZ states on demand by subsequently repeating the pulse sequences, it is assumed that it can produce a  $|\text{GHZ}^{(7)}\rangle$  cluster.

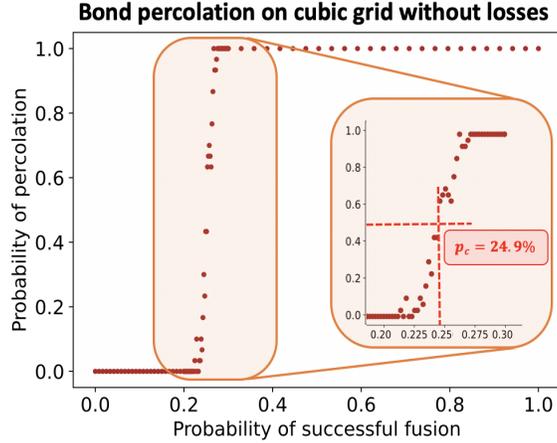
Other approaches use different topologies. For example, in Ref. [15] a diamond lattice is used, as it is the lattice with the smallest coordination number (4) able to percolate in 3D. This means that  $|\text{GHZ}^{(5)}\rangle$  are enough. This comes at the price of a bigger percolation threshold  $p_c^{(\text{diamond})} = 38.9\%$  (Ref. [2]), which means that there is less room for photon losses (In Ref. [15] a 2% photon loss can be tolerated).

Therefore, in order to choose the topology of the grid to place the nodes, a balance must be found between the percolation threshold, the fusion gates to be used and the small resource clusters to be used.

### 5.3.2 The simulations

The dynamics of bond-percolation establishment has been simulated in Python over a finite  $20 \times 20 \times 20$  cubic lattice. This is rather small, but the results are good enough (taking, as a proof of concept the comparison between the percolation threshold for the simulated case  $p_c^{(\text{cubic})} = 24.9\%$  against the tabulated one of 24.8%). In each trial of the simulation, bonds are established with a certain probability, and the existence of a percolating cluster is decided whether there is a connected path from one corner of the grid to the other, or not. For each probability, 30 trials have been performed to get statistics.

In Figure 5.6 the typical graph of a percolation process can be seen. It is computed for the no-losses case. Therefore, the percolation threshold observed is the one for a regular cubic lattice:



**Figure 5.6** Percolation phase transition for the no-losses case.  $p_c = 24.9\%$ , as expected for a regular cubic lattice in bond-percolation.

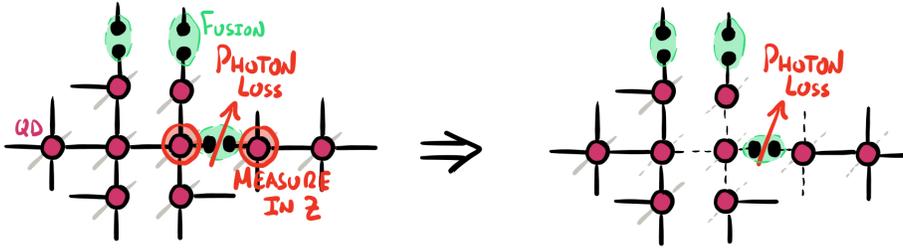
24.9%. It is defined as the point in which the step of the phase transition is halfway. This is, the value at which the percolation probability is 50%.

### 5.3.3 Taking losses into account

In the real world photons might be lost during fusion operation. And as these are entangled with other parts of the network, a detailed analysis has to be done in order not to break the cluster state.

In the event of photon loss, this might collapse randomly, and its collapse might be transferred to those particles entangled with it. An approach to avoid undesired behaviours is to cut around the qubits that might be compromised by the photon lost. Cutting can be performed through Z-measurements.

An scheme of how to proceed upon photon lost can be seen in Figure 5.8.



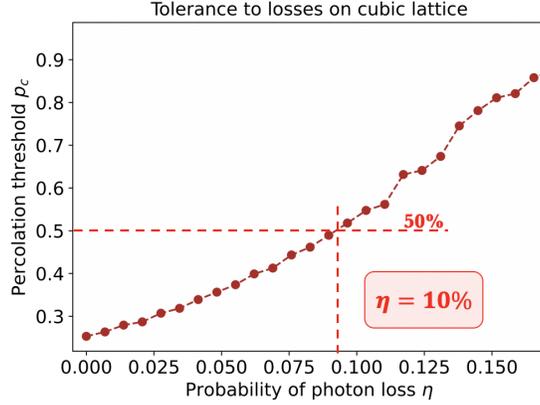
**Figure 5.7** When a photon is lost, any qubit entangled with it must be cut by performing Z-measurements over its neighbours.

As can be seen, a lost photon is pretty destructive with respect to entanglement. Simulations have been performed taking into account this model.

The simulations for photon losses first grow a network and then choose nodes to disentangle by emulating a photon loss on them.

Two situations have been studied: First of all, the evolution of the percolation threshold with respect to the probability of losses. This is shown in Figure 5.8.

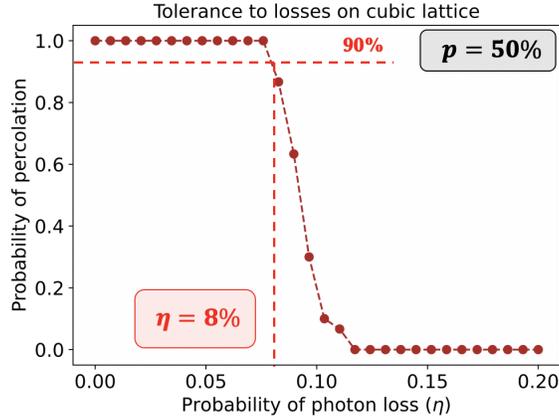
As the loss probability increases, the percolation threshold does as well. At some point it surpasses 50%, which means that Type-II fusion is no longer able to percolate in the network. At this



**Figure 5.8** Evolution of the percolation threshold as a function of the photon loss probability. At  $\eta = 10\%$ ,  $p_c = 50\%$ . Therefore, Type-II fusions serve no more to percolate.

point, the dynamic Type-II or the Boosted Type-II might be good resources.

In Figure 5.9, a Type-II fusion gate with 50% success is assumed, and the evolution of the probability of percolation against photon loss probability is studied. The probability of percolation is how likely percolation is established assuming  $p = 50\%$ . For the case  $\eta = 0\%$  this is 1, but this shifts down as  $\eta$  increases. Indeed, it can be seen that until  $\eta = 8\%$  percolation is likely to happen. However, from there it quickly drops.



**Figure 5.9** Evolution of the percolation probability as a function of the photon loss probability. a fusion success probability of 50% is kept fixed.

In conclusion, the percolation method to grow cluster states over cubic lattices using Rotated Type-II fusion gates is robust to build a percolating cluster up to an 8% of photon loss probability. From that point, the 50% success probability of Type-II fusion is not well-above the percolation threshold and the systems swifts to a sub-critical regime in which the percolating cluster is not able to grow. An alternative fusion gate with higher success probability (e.g., Boosted Type-II or Dynamic Type-II) could still be used.



# Chapter 6

## Conclusion and outlook

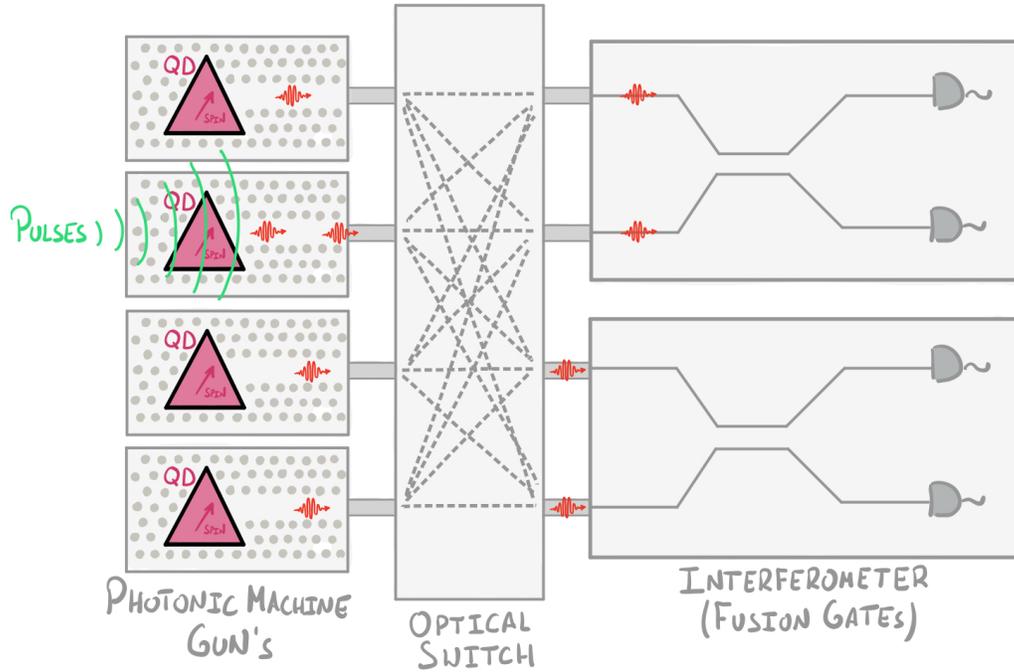
This work has served to understand the many ingredients, techniques and theoretical background involved in percolation-based schemes for quantum computing.

- The photonic machine gun is a flexible tool to generate small but customized entanglement patterns. At the moment, its main limitation is decoherence time. However, as long as the spin qubit is coherent, it serves as a solid-state memory for the graph state. This is a critical point, because in MBQC protocols one has to have a map of the entanglement before starting the measurements, and the graph has to be stored somewhere on the meantime. To give some numbers, the QD system available at Niels Bohr Institute is characterized by  $T_1 \sim 20 \mu\text{s}$ ,  $T_2 \sim 450 \text{ ns}$ ,  $T_2^* \sim 16 \text{ ns}$ , so it might produce  $\sim 10$  time-bin photons, given the time-bin separation is of  $\sim 10 \text{ ns}$ , and different emissions can be put apart up to  $\sim 45 \text{ ns}$ . This should be enough time to wait until the entangled graph is set up, to (classically) have an algorithm design the measurement pattern based on the entanglement map, and to perform the adaptive measurements. However, technology changes fast so all this should be taken with a grain of salt.
- Integrated photonic circuits are interesting because they operate at room temperature (except the photon number detectors). It is true that they cannot perform *universal deterministic* computations, but they can implement the probabilistic fusion gates. Moreover, they can be built over Si chips and therefore escalated using the currently-available semiconductor technologies mastery.
- Different variants of fusion gates have been discussed. After all it is desired to have one heralded, ballistic and that keeps as much entanglement as possible upon failure. The rotated Type-II is a great candidate when  $p = 50\%$  is needed, and the Dynamic Type-II when higher probabilities are required. The latter one is resilient up to a 5% photon loss with  $p = 75\%$ .
- Measurement-based quantum computing is a paradigm well studied that, if provided with a 2D can implement any universal quantum computation. And a 3D graph incorporates fault-tolerance.

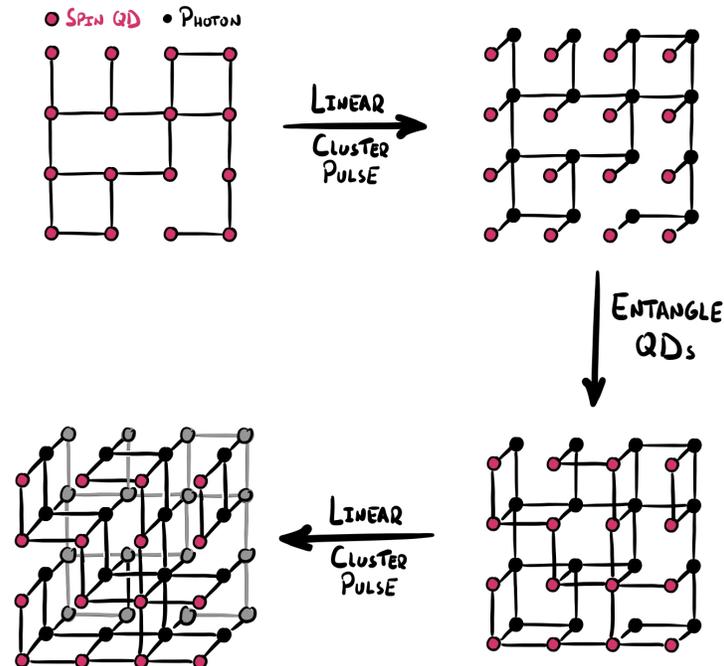
### 6.1 A blueprint for a percolation-based quantum computer

But what might a system combining all these ingredients look like? Maybe it would be something like in Figure 6.1.

Many QD can be integrated into waveguides so that they can be locally activated by sequences of pulses. These represent many spin qubits. Indeed, which QD to activate and drive could be selected



**Figure 6.1** The emission from a set of photonic machine gun's can be entangled using integrated fusion gates. To do so, an optical switch must lay in the middle and redirect the light to where it should be used.



**Figure 6.2** Once the graph is created over the spin QD qubits, it can be transferred to a photonic cluster by linear-cluster pulse sequences, as discussed in Chapter 2.

through selection rules by applying a local magnetic fields. Otherwise, just sending localized pulses is also an option. The fusion operations might be engraved into integrated photonic circuits. These will be used on demand by sending pairs of photons to be fused. Therefore, in the middle there has to be some device playing the role of an active switch. It's mission is to redirect the emissions of pairs of QD that have to get fused together. This active switch has to be software controlled to reproduce the lattice structure underlying the graph that is being built.

When the percolation process has taken place the resulting state will be a graph state around the QD spin qubits. The graph state will remain stored on them as long as they are maintain coherence.

It should be noted that the approach discussed is ballistic: photons are created on-demand when they are needed just before they are sent for a fusion operation. Moreover, the architecture is flexible: regular Type-II fusion might be changed with Dynamic Type-II fusions just by trying again with a new pair of photons. Lastly, the fact that the graph state is stored on the QDs is extremely convenient: it avoids the need for quantum memories.

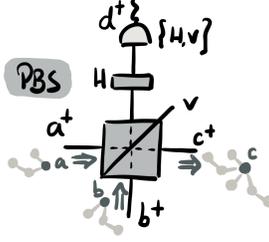
The final step of the protocol is performing the actual measurement pattern. This has to be designed by a classical algorithm based on the particular entanglement topology resulting from the percolation. Therefore, storing the graph over the QDs can provide this waiting time. The measurements can be performed directly over the QDs. Otherwise, if linear-cluster pulse sequences are applied to every QD, the entangled graph is emitted as a set of photons. This is shown in Figure 6.2. The remaining QDs are still linearly entangled to the photons, so if more photons are emitted from each QD and the percolation process is repeated again, a 3D cluster can be grown in layers, as if it were a sandwich. This process can be repeated over and over, cyclically, in an endless fashion (only constrained by the coherence time of the QD), creating the cluster as it is being consumed for the computation.



# Appendix and calculations

## Type-I Fusion

Working in a polarization encoding where the PBS in Fig...., that reflects the vertical component, implements the transformations  $\{\hat{a}_H^\dagger \rightarrow \hat{c}_H^\dagger, \hat{a}_V^\dagger \rightarrow \hat{d}_V^\dagger, \hat{b}_H^\dagger \rightarrow \hat{d}_H^\dagger, \hat{b}_V^\dagger \rightarrow \hat{c}_V^\dagger\}$  and the polarization rotation implements a Hadamard-like rotation of the form  $\{\hat{d}_H^\dagger \rightarrow \hat{d}_+^\dagger \equiv \frac{1}{\sqrt{2}}(\hat{d}_H^\dagger + \hat{d}_V^\dagger), \hat{d}_V^\dagger \rightarrow \hat{d}_-^\dagger \equiv \frac{1}{\sqrt{2}}(\hat{d}_H^\dagger - \hat{d}_V^\dagger)\}$



**Figure 6.3** Type-I possible scenarios upon detection outcomes on mode  $d$ . In some cases, local Pauli operations are applied. Note that failure erases some entanglements.

The two input cluster have the form:

$$(f_1 \hat{a}_H^\dagger + f_2 \hat{a}_V^\dagger) \otimes (f_3 \hat{b}_H^\dagger + f_4 \hat{b}_V^\dagger) |\emptyset\rangle$$

Expanded:

$$f_1 f_3 \hat{a}_H^\dagger \hat{b}_H^\dagger + f_1 f_4 \hat{a}_H^\dagger \hat{b}_V^\dagger + f_2 f_3 \hat{a}_V^\dagger \hat{b}_H^\dagger + f_2 f_4 \hat{a}_V^\dagger \hat{b}_V^\dagger$$

After the PBS:

$$f_1 f_3 \hat{c}_H^\dagger \hat{d}_H^\dagger + f_1 f_4 \hat{c}_H^\dagger \hat{c}_V^\dagger + f_2 f_3 \hat{d}_V^\dagger \hat{d}_H^\dagger + f_2 f_4 \hat{d}_V^\dagger \hat{c}_V^\dagger$$

Upon the polarization rotation:

$$\begin{aligned} & f_1 f_3 \hat{c}_H^\dagger \hat{d}_+^\dagger + f_1 f_4 \hat{c}_H^\dagger \hat{c}_V^\dagger + f_2 f_3 \hat{d}_-^\dagger \hat{d}_+^\dagger + f_2 f_4 \hat{d}_-^\dagger \hat{c}_V^\dagger = \\ & \frac{f_1 f_3}{\sqrt{2}} \hat{c}_H^\dagger (\hat{d}_H^\dagger + \hat{d}_V^\dagger) + f_1 f_4 \hat{c}_H^\dagger \hat{c}_V^\dagger + \frac{f_2 f_3}{2} (\hat{d}_H^{\dagger 2} - \hat{d}_V^{\dagger 2}) + \frac{f_2 f_4}{\sqrt{2}} \hat{c}_V^\dagger (\hat{d}_H^\dagger - \hat{d}_V^\dagger) \end{aligned}$$

Reorganizing terms based on the possible results in mode  $d$ :

$$f_1 f_4 \hat{c}_H^\dagger \hat{c}_V^\dagger + \frac{f_2 f_3}{2} (\hat{d}_H^{\dagger 2} - \hat{d}_V^{\dagger 2}) + \frac{\hat{d}_H^\dagger}{\sqrt{2}} (f_1 f_3 \hat{c}_H^\dagger + f_2 f_4 \hat{c}_V^\dagger) + \frac{\hat{d}_V^\dagger}{\sqrt{2}} (f_1 f_3 \hat{c}_H^\dagger - f_2 f_4 \hat{c}_V^\dagger)$$



# Bibliography

- [1] *Bible*, chapter Genesis 6:15.
- [2] Percolation thresholds. Wikipedia. [https://en.wikipedia.org/wiki/Percolation\\_threshold#Thresholds\\_on\\_3D\\_latticesr](https://en.wikipedia.org/wiki/Percolation_threshold#Thresholds_on_3D_latticesr).
- [3] Precision limits in quantum metrology with open quantum systems. *Quantum journal*.
- [4] S. Aaronson. Chp code. <https://www.scottaaronson.com/chp/r>.
- [5] S. Aaronson. Np-complete problems and physical reality. *arXiv:quant-ph/0502072*, 2005.
- [6] S. Aaronson. *Introduction to Quantum Information Science Lecture Notes*, chapter 28. 2018.
- [7] S. Aaronson and D. Gottesman. Improved simulation of stabilizer circuits. *Phys. Rev. A Journal*, 2004.
- [8] John G. Rarity Siyuan Yu Jeremy L. O'Brien Alberto Politi, Martin J. Cryan. Silica-on-silicon waveguide quantum circuits. *Science*, 2008.
- [9] Samuel L. Braunstein and A. Mann. Measurement of the bell operator and quantum teleportation. *Phys. Rev. A*, 1996.
- [10] D. E. Browne and T. Rudolph. Resource-efficient linear optical quantum computation. *Daniel E. Browne and Terry Rudolph*, 2005.
- [11] P. Knight C. Gerry. *Introductory Quantum Optics*. 2004.
- [12] R. Laflamme G. J. Milburn E. Knill. A scheme for efficient quantum computation with linear optics. *Nature*, 2001.
- [13] Fabian Ewert and Peter van Loock. Efficient bell measurement with passive linear optics and unentangled ancillae. *Phys. Rev. Lett.*, 2014.
- [14] R.P. Feynman. Simulating physics with computers. *International Journal of Theoretical Physics*, 1982.
- [15] M. Gimeno-Segovia. *Towards practical linear optical quantum computing*. PhD thesis, Imperial College London, 2016.
- [16] D. Gottesman. The heisenberg representation of quantum computers. *arXiv:quant-ph/9807006*, 1998.
- [17] W.P. Grice. Arbitrarily complete bell-state measurement using only linear optical elements. *Physical Review A*, 2011.
- [18] Otfried Guhne. *Detecting Quantum Entanglement: Entanglement Witnesses and Uncertainty Relations*. PhD thesis, Universitat Hannover, 2004.

- 
- [19] J. Eisert K. Kieling. Percolation in quantum computation and communication. *arXiv:0712.1836*, 2007.
- [20] Pieter Kok. *Five Lectures on Optical Quantum Computing*. 2007.
- [21] M. S. Kim M. S. Tame, M. Paternostro and V. Vedral. Quantum-information processing with noisy cluster states. *Phys. Rev. A*.
- [22] J.C.F. Matthews J.L. O'Brien M.G. Thompson, A. Politi. Integrated waveguide circuits for optical quantum computing. *G-Animal's Journal*, 2011.
- [23] Herbert J. Bernstein Michael Reck, Anton Zeilinger and Philip Bertani. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.*, 1994.
- [24] Casper R. Breum Jonas S. Neergaard-Nielsen Ulrik L. Andersen Mikkel V. Larsen, Xueshi Guo. Deterministic generation of a two-dimensional cluster state. *Science*, 2019.
- [25] Michael A. Nielsen and Isaac L. Chuang. Quantum computation and quantum information. 2010.
- [26] T. Rudolph E. Schenck H. Weinfurter V. Vedral M. Aspelmeyer A. Zeilinger P. Walther, K.J. Resch. Experimental one-way quantum computing. *Nature*, 2005.
- [27] Simon Refshauge Pabst. *Towards Spin-Multiphoton Entanglement from a Quantum Dot*. PhD thesis, University of Copenhagen, 2021.
- [28] D.E. Browne R. Raussendorf and H.J. Briegel. Measurement-based quantum computation on cluster states. 2003.
- [29] Chiara Macchiavello Michele Mosca Richard Cleve, Artur Ekert. Quantum algorithms revisited. *arXiv:quant-ph/9708016*, 1997.
- [30] Alex E. Jones Raffaele Santagati Anthony Laing Stefano Paesani, Jacob F. F. Bulmer. A scheme for universal high-dimensional quantum computation with linear optics. *arXiv:2105.02748v1*, 2021.
- [31] Robert J. Sternberg. *Group Theory In Physics*. 1994.
- [32] Sophia Economou Terry Rudolph, Netanel Lindner. A photonic cluster state machine gun. *APS Physics*.
- [33] L. Vaidman and N. Yoran. Methods for reliable teleportation. *Phys. Rev. A*.
- [34] Benjamin J. Metcalf W. Steven Kolthammer William R. Clements, Peter C. Humphreys and Ian A. Walmsley. An optimal design for universal multipoint interferometers. *OSA*, 2016.
- [35] Gregor Weihs Wolfgang Tittel. Photonic entanglement for fundamental tests and quantum communications. *Quantum Information Computation*, 2001.
- [36] Xanadu. Strawberry fields. <https://strawberryfields.ai/photronics/hardware/details.html>.
- [37] Y. Yeo and W.K. Chua. Teleportation and dense coding with genuine multipartite entanglement. *Phys. Rev. Lett.*, 2006.