

October 24, 2019

Abstract

1 Introduction

Here I will put the proposal with some adjustments to make it fit in the context of this document.

2 Preliminaries

This section serves as a concise introduction to the diagrammatic method for a reader who is familiar with quantum mechanics and Dirac notation. Appendix A contains all of the concepts discussed in this section as keywords with hyperrefs to the respective sections.

2.1 From Dirac to Diagrams

2.1.1 States, Effects, and Hermitian Operations

The **ket** is defined as a triangle with its sharp edge down in diagrammatic notation. It can be interpreted as the preparation of a state, in this case ψ . It is referred to as **state** throughout the thesis.

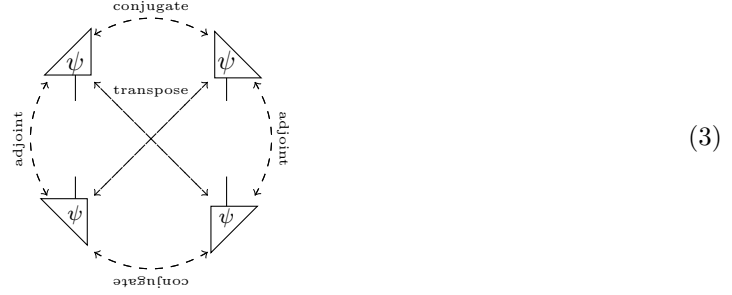
$$|\psi\rangle = \begin{array}{c} | \\ \psi \\ \triangle \end{array} \quad (1)$$

The **bra** in diagrammatic notation is the flipped state, and is referred to as **effect**.

$$\langle\psi| = \begin{array}{c} \triangle \\ \psi \\ | \end{array} \quad (2)$$

Triangles are the smallest building blocks in the diagrammatic notation. Most diagrams can be reduced to just triangles. This makes them a powerful tool for translating complicated diagrams to Dirac notation and vice versa.

From the fact that the **Hermitian adjoint** of a bra gives a ket and reversedly it follows that the operation of flipping a diagram around its horizontal axis corresponds to taking the Hermitian adjoint diagrammatically. Flipping a diagram around its vertical axis is also a legal operation and this corresponds to taking the **Hermitian conjugate**. Both of these operation applied together takes the **transpose**. All of these diagram operations can be summarized as follows:



Note that there are also triangles that are not on their side. These are representations of objects that are not affected by conjugate transformations, such as integers.

2.1.2 Wires

The identity map in the diagrammatic notation is given by the following diagram, referred to as a **wire**.



A wire can be reduced to triangles (and subsequently to a ket and a bra) as follows:

$$\begin{array}{c} | \\ \downarrow \\ \triangleleft i \\ \uparrow \\ \triangleright i \\ \downarrow \end{array} = \sum_i |i\rangle \langle i| = \sum_i |i\rangle \langle i|$$

(5)

Every wire has an associated **system type**, the space of the information that it carries. In the context of this report, the system types are Hilbert spaces or the tensor product of Hilbert Spaces.

2.1.3 Maps

A **linear map** is given by the following diagram:



We can find the equivalent form in Dirac notation as follows:

$$\begin{array}{c} \text{trapezoid } f \\ \downarrow \end{array} = \sum_{ij} r_{ij} \begin{array}{c} \triangleleft j \\ \uparrow \\ \triangleright i \end{array} = \sum_{ij} r_{ij} |i\rangle \langle j|$$

(7)

In the context of a bra and a ket, we can translate the diagrammatic linear map to Dirac notation as such:



$$= \langle \psi | f | \psi \rangle \quad (8)$$

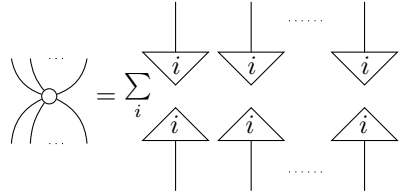
2.1.4 Spiders

A **spider** is a special map which functions as a Kronecker delta. It forces the inputs to be the same as the outputs. In the case where we have one input and output this gives a trivial result:



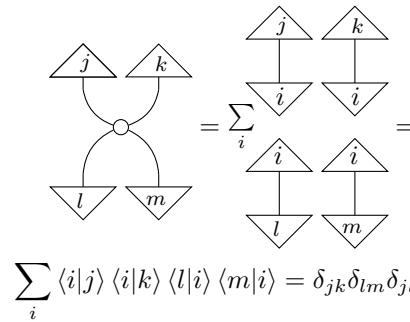
$$= \quad (9)$$

In the case where there are multiple outputs and inputs it forces all to be the same:



$$= \quad (10)$$

By applying arbitrary in- and outputs we can see how the **Kronecker delta** arises from Dirac notation. The following example is for two two inputs and two outputs but the same principle extends to an arbitrary amount of in- and outputs.



$$\sum_i \langle i | j \rangle \langle i | k \rangle \langle l | i \rangle \langle m | i \rangle = \delta_{jk} \delta_{lm} \delta_{jl} \quad (11)$$

Spiders with single in- or outputs also exist. A spider with a single input is the deletion of a classical variable and a spider with a single output is the creation of a random classical variable:

$$\text{circle with a vertical line} = \sum_i \text{triangle with a vertical line and index } i = \langle 0| + \langle 1| \quad (12)$$

An important property of spiders is that they fuse:

$$\begin{array}{c} n \text{ outputs} \\ \vdots \\ \vdots \\ \text{---} \circ \text{---} \\ \vdots \\ \vdots \\ m \text{ inputs} \end{array} = \begin{array}{c} n \text{ outputs} \\ \vdots \\ \vdots \\ \text{---} \circ \text{---} \\ \vdots \\ \vdots \\ m \text{ inputs} \end{array} \quad (13)$$

2.1.5 Colors and Bases

In the diagrammatic notation, the **color** of an object such as a spider or a triangle determines its basis. In the context of this paper it is sufficient to define two orthonormal **bases**, the Z and X bases. The Z basis has white diagrammatic elements, for the X basis they are gray. The following is an example of how to translate between bases in this notation:

$$\begin{array}{|c|} \hline \text{ } \\ \hline \text{0} \\ \hline \end{array} = \frac{1}{\sqrt{2}}(\text{white0} + \text{white1}) \quad (14)$$

This equation is of course entirely analogous to its Dirac notation counterpart, with $|-\rangle$ and $|+\rangle$ being the orthonormal basis states in the X basis and $|0\rangle$ and $|1\rangle$ the orthonormal basis states in the Z basis:

$$|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \quad (15)$$

Note that spiders of different colors do not fuse.

2.1.6 Doubling

Doubling is the operation of taking the **tensor product** of a diagram with itself. In the usual case, where the system type of a single wire is a Hilbert space (\mathcal{H}), the doubled wire has the set of density matrices on that Hilbert space as system type.:

$$\mathcal{H} \oplus \mathcal{H} = \mathcal{D}(\mathcal{H}) \quad (16)$$

Where $\mathcal{D}(\mathcal{H})$ is the set of density matrices on \mathcal{H} . \oplus is the tensor product.

Doubled maps and and states represent **pure** maps and states. Single maps and states represent their **mixed** counterparts. The most intuitive interpretation, and how it is mostly used in this report, is that the single wires represent classical data and thick wires represent data encoded into a quantum state.

Doubling in diagrammatic notation is nothing more than placing a second conjugate diagram next to the original diagram. In doubled diagrams lines are drawn thick, for example:

$$(17)$$

The notation of a map with a hat, such as \hat{f} , means that that map is pure.

2.1.7 Discarding

Discarding is the process of removing part of a diagram from the whole, or removing the whole diagram altogether. For doubled diagrams it is defined as follows:

$$(18)$$

It is trivial to see that applying discarding to any arbitrary (normalized) state always results in the number 1. In fact, discarding a state or map is equivalent to taking its **trace**. As an example, we discard an arbitrary normalized **density matrix**, ρ :

$$(19)$$

Discarding is not a pure map. It connects the two counterparts of a doubled state by a single wire. This allows discarding to be used to purify any arbitrary state or map. For the case of a map Φ , **purification** is as follows:

$$(20)$$

2.1.8 Phase Spiders

Phase spiders follow the same rules as normal spiders. However, perhaps unsurprisingly, they carry a **phase**. This phase is subject to a new set of rules which is evident from the definition of the phase spider.

$$(21)$$

An example of the principle that underlies these rules is given below, which shows how the phase gets eliminated in the process of **decoding** a quantum state to classical information.

$$\begin{array}{c} \circ \\ | \end{array} = \begin{array}{c} | \\ \circ \end{array} = \begin{array}{c} | \\ \circ \end{array} = \begin{array}{c} | \\ \circ \end{array} e^{i(\alpha-\alpha)} = \begin{array}{c} | \\ \circ \end{array} = \begin{array}{c} | \\ \circ \end{array} \quad (22)$$

Equation (22) exemplifies how phases behave when spiders fuse, they add. Furthermore, it shows how the phase gets eliminated when one tries to extract classical information, also known as measure, a quantum state.

2.1.9 Entanglement

Pure entangled states are those states that are not horizontally separable:

$$\begin{array}{c} | \\ | \end{array} \neq \begin{array}{c} | \\ \psi_1 \end{array} \begin{array}{c} | \\ \psi_2 \end{array} \quad (23)$$

Since horizontally composed states form the tensor product of those states diagrammatically, this definition is in line with theory, where entangled states are defined as those states that can not be written as the tensor product of two states [6].

An example of such a state is the following:

$$\begin{array}{c} \cup \end{array} = \sum_i \begin{array}{c} | \\ i \end{array} \begin{array}{c} | \\ i \end{array} = \langle 00| + \langle 11| \quad (24)$$

Which is up to a number the first Bell matrix, B_0 . Although it may seem like this state separates since it is made up of two triangles, it does not. Both triangles are correlated through the same index. Indeed, if the indices were different for each of the triangles this would not be an entangled state.

2.2 Advanced diagrammatic concepts

2.2.1 Basis and phase translations on the Bloch sphere

*** Need more info here. ***

2.2.2 Encoding and Decoding

Diagrammatically, the encoding map is a single spider with one doubled wire as output and one single wire as input. The color of the spider is the basis in which the classical bit gets encoded into a quantum state. For example, encoding classical information on a density matrix ρ into a quantum state in the white basis with indices $i \in \{0, 1\}^n$:

$$\begin{array}{c} | \\ \rho \end{array} = \sum_i \begin{array}{c} | \\ i \end{array} \begin{array}{c} | \\ i \end{array} = \sum_i \langle \rho | i \rangle \begin{array}{c} | \\ i \end{array} = \begin{array}{c} | \\ \rho \end{array} \quad (25)$$

The decoding map is the adjoint of the encoding map. Its behavior follows directly from 25.

2.2.3 Fusion of single and double spiders

Single and double spiders fuse. The result is a single bastard spider. Bastard here refers to the fact it has both single and double outputs.

*** Need more info here. Section 8.3.3 in picturing quantum processes. ***

2.2.4 Complementary spiders

Alice encoding a classical state into a qubit in a certain basis and then Bob measuring that qubit in a complementary basis results in Bob receiving a random bit.

*** More info here ***




$$(26)$$

2.2.5 The xor gate

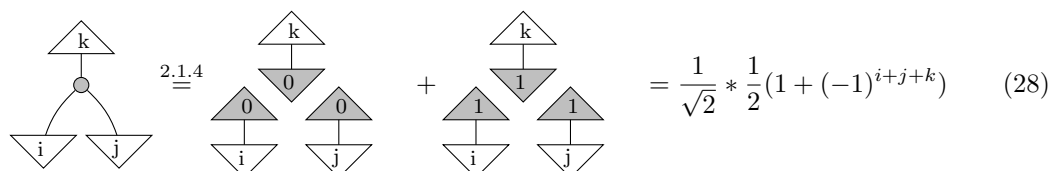
The Exclusive OR (xor) gate takes two inputs and gives an output of 0 when the inputs are the same and 1 when they are different. Mathematically, if we take $x, y \in \{0, 1\}$ as inputs the output of the xor gate is $(x + y) \bmod 2$. We could just define a diagrammatic map and give it this property. However, there is another way of creating the xor gate diagrammatically which only uses spiders. This has the advantage of allowing us to use spider rules to move xor gates around in diagrams.

If we enter two outputs of a certain basis into a spider that is of another basis orthonormal to the inputs this gives the xor gate. To see how this works, let's use a gray spider and apply white test in- and outputs. First, recall that:



$$(27)$$

Now applying the test in- and outputs to the proposed xor map [1]:



$$(28)$$

This equation results in 0 whenever the sum $i + j + k$ is uneven and $1/\sqrt{2}$ when it is even. Now $i + j + k$ is only even whenever $i \oplus j = k$. This thus, up to a factor of $\sqrt{2}$, gives the gate map.

3 Protocols

3.1 One Time Pad

The classical One Time Pad (OTP) is perhaps the oldest and most well known quantum cryptographic method. We will first discuss this protocol as a setup to the quantum version. Although originally proposed in 1884 [5], the OTP was first formalized and proven secure in 1949 [8]. Since

then, the scheme has essentially remained the same due to its simplicity. A typical OTP goes as follows:

Alice and Bob start with a uniformly random key $k \in \{0, 1\}^n$. Alice wants to send some message $m \in \{0, 1\}^n$ to Bob. She encrypts m using the key k by means of an xor gate, generating payload $x^n = m \oplus k$.¹ After this step, she sends x to Bob who applies k again to x to receive m since $k \oplus x = m^n$. The assumption on Eve in this scheme is that she doesn't know k and can intercept x . However, if k was truly uniformly random, x is so too, leaving Eve with a random variable even after a successful interception. The main drawback of this scheme is the fact that the key has to be the same size as the message and that this key can only safely be used once.

3.1.1 Diagrammatic Implementation

The OTP relies on classical communication channels and xor gates. Since we can represent both of these diagrammatically we can draw out the fully classical OTP protocol by means of diagrams. Recall from section 2.1.4 that the following state generates a random bit:

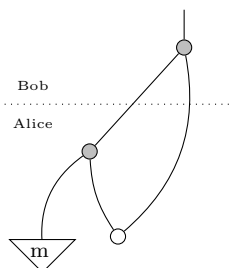
$$\begin{array}{c} | \\ \circ \end{array} \quad (29)$$

We choose this as the uniformly random key k and give one end to Alice and one to Bob. Alice, who starts with message m , then applies the xor gate from section 2.2.5 to this message, generating payload x :



$$(30)$$

Everything Bob now has to do is to apply an xor gate to the payload x and the key k :



$$(31)$$

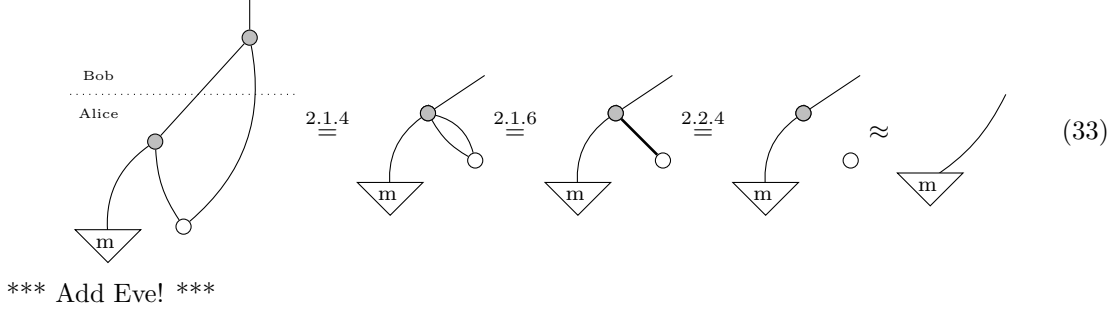
To check that this is indeed a viable communication protocol we want equation 31 to reduce to:



$$(32)$$

¹In different realizations of the OTP, Alice has different methods of encrypting her message. With that being said, applying an xor to the key and the message is one of the most common versions.

This happens up to a number:



3.2 Quantum One Time Pad

In the Quantum One Time Pad (QOTP) Alice and Bob again both share a uniformly random key $\alpha \in \{0, 1, 2, 3\}^n$ and want to communicate some quantum state, ρ . Alice first transforms ρ with a random Pauli map, σ_α . After she has prepared this state she sends it to Bob over a quantum channel. He can then apply the Hermitian adjoint of this random Pauli resulting in the original ρ sent by Alice. This step exploits the unitary property of the Pauli maps. Eve, who doesn't know α , can measure the state sent from Alice to Bob. However, from her perspective, this is the fully mixed state. Mathematically, this can be seen as follows:

$$\rho' = \sum_0^3 \frac{1}{4} \sigma_\alpha \rho \sigma_\alpha^\dagger = \frac{1}{2} \mathbb{I} \quad (34)$$

In principle, the QOTP is similar to the OTP. By means of encrypting a piece of information with a random key which is unknown to Eve but shared by Alice and Bob the latter can achieve secure communication. As a communication protocol, QOTP is not very efficient. Alice and Bob need use two bits as a key per bit of communicated information. However, as a scheme for the encryption of qubits it is actually applicable to various protocols as it allows for the eight-state encoding of qubits [2]. *** See if need some more information here ***

3.2.1 Diagrammatic Implementation

*** Look into removing ρ input state ***

In the diagrammatic formalism we can construct a set of maps that have the same property as the Pauli maps in equation 34, the Bell maps. These are defined in terms of the Pauli matrices as follows [1]:

$$\sigma_0 = B_0 \quad \sigma_1 = B_1 \quad \sigma_2 = iB_3 \quad \sigma_3 = B_2 \quad (35)$$

In order to form diagrams for these Bell maps we have to understand them a little bit better. One of their properties is that they can be constructed from rotations on the Bloch sphere around the z and x axes [3], also known as bitflips around these axes. For random $u, w \in \{0, 1\}^n$ and $\alpha \in \{0, 1, 2, 3\}^n$ we can write this mathematically as follows:

$$Z^u X^w = B_\alpha \quad (36)$$

Where Z^u and X^w denote the maps that do a bitflip in the z and x bases respectively.

Let's see if we can construct these smaller constituents, Z^u and X^w , diagrammatically. Starting with X^w , remember that a bitflip in the x basis corresponds to a rotation around the z axis on the Bloch sphere. Therefore we need to find a diagrammatic map that either rotates the Bloch sphere around its z axis by π radians (X^1) or not (X^0). Since a single spider without a phase is the identity 2.1.4 and the z basis is represented by the color white diagrammatically, we can use the white phaseless spider for the case where we don't flip the bit or rotate around the z axis. Let's send the 0 state through in the gray (x) basis to test if this map behaves as expected:

$$\begin{array}{c} \text{white spider} \\ \downarrow \\ \text{gray triangle with 0} \end{array} \stackrel{2.1.5}{=} \frac{1}{2} \begin{array}{c} \text{white spider} \\ \downarrow \\ \text{gray triangle with 0} \end{array} + \frac{1}{2} \begin{array}{c} \text{white spider} \\ \downarrow \\ \text{gray triangle with 1} \end{array} \stackrel{2.1.4}{=} \frac{1}{2} \begin{array}{c} \text{white spider} \\ \downarrow \\ \text{white circle} \end{array} \stackrel{2.1.8}{=} \frac{1}{2} \begin{array}{c} \text{white spider} \\ \downarrow \\ \text{white circle} \end{array} \stackrel{2.1.5}{=} \begin{array}{c} \text{white spider} \\ \downarrow \\ \text{gray triangle with 0} \end{array} \quad (37)$$

This map does seem to behave appropriately. We see that whenever we send a gray 0 through, we get a gray 0 as output. Following similar logic, we could also use the white spider with a π phase to make a rotation around the z axis, and thus a bitflip in the x basis. Let's test if this works too:

$$\begin{array}{c} \text{white spider with } \pi \\ \downarrow \\ \text{gray triangle with 0} \end{array} \stackrel{2.1.5}{=} \frac{1}{2} \begin{array}{c} \text{white spider with } \pi \\ \downarrow \\ \text{gray triangle with 0} \end{array} + \frac{1}{2} \begin{array}{c} \text{white spider with } \pi \\ \downarrow \\ \text{gray triangle with 1} \end{array} \stackrel{2.1.4}{=} \frac{1}{2} \begin{array}{c} \text{white spider with } \pi \\ \downarrow \\ \text{white circle} \end{array} \stackrel{2.1.8}{=} \frac{1}{2} \begin{array}{c} \text{white spider with } \pi \\ \downarrow \\ \text{white circle} \end{array} \stackrel{2.1.5}{=} \begin{array}{c} \text{white spider with } \pi \\ \downarrow \\ \text{gray triangle with 1} \end{array} \quad (38)$$

These maps do exhibit the correct properties. Indeed, whenever we send a gray 1 through we also get the expected results. It seems that we have formed the X^0 and X^1 maps. While we will not go through the full math here, the Z^0 and Z^1 maps follow very similar logic and also behave as expected. Perhaps unsurprisingly, the former is a gray phaseless spider whereas the latter is a gray spider with a phase π .

Now that we have created our four constituent maps we are in principle ready to make any Bell map of choice. However, we do not want to make a choice, we want to select a random Bell matrix. We still need to find a diagrammatic method to generate a random u and w on which our choice of Bell matrices depend. Recall that generating a random bit is the following diagram:

$$\begin{array}{c} \text{white circle} \\ \downarrow \\ \text{gray triangle with } i \end{array} \stackrel{2.1.4}{=} \sum_i \begin{array}{c} \text{white circle} \\ \downarrow \\ \text{gray triangle with } i \end{array} \quad (39)$$

We could encode this random classical bit into a qubit as follows:

$$\begin{array}{c} \text{white circle} \\ \downarrow \\ \text{white circle} \end{array} \stackrel{2.1.4}{=} \sum_i \begin{array}{c} \text{white circle} \\ \downarrow \\ \text{gray triangle with } i \end{array} \stackrel{2.2.2}{=} \sum_i \begin{array}{c} \text{white circle} \\ \downarrow \\ \text{gray triangle with } i \end{array} \quad (40)$$

The previous two equations are entirely analogous for the gray (x) basis.²

We now have the necessary ingredients to make a map that applies a random bitflip or not in x and another map that makes a random bitflip or not in z . The results are as follows:

²In fact, we can make an even stronger statement about the diagrams in equation 40: They are actually equal to the analogous diagrams in the gray basis. Note that the rightmost diagram is the adjoint of discarding, which can be interpreted as preparing the fully mixed state, up to a number. Since this state is independent of the basis, these diagrams of white basis are equal to the analogous diagrams in the gray basis.

$$\begin{array}{ccc}
X^w \Leftrightarrow & \begin{array}{c} \text{---} \circ \text{---} \\ | \\ \bullet \\ | \\ \bullet \end{array} & \\
Z^u \Leftrightarrow & \begin{array}{c} \text{---} \bullet \text{---} \\ | \\ \circ \\ | \\ \circ \end{array} & (41)
\end{array}$$

Let's confirm that the diagrammatic version of X^w does indeed behave as expected:

$$\begin{array}{c} \text{Diagram 1} \end{array} \stackrel{2.1,4}{=} \begin{array}{c} \text{Diagram 2} \end{array} + \begin{array}{c} \text{Diagram 3} \end{array} \stackrel{2.2,2}{=} \begin{array}{c} \text{Diagram 4} \end{array} + \begin{array}{c} \text{Diagram 5} \end{array} \stackrel{2.2,1}{=} \begin{array}{c} \text{Diagram 6} \end{array} + \begin{array}{c} \text{Diagram 7} \end{array} \stackrel{2.1,8}{=} \begin{array}{c} \text{Diagram 8} \end{array} + \begin{array}{c} \text{Diagram 9} \end{array} \quad (42)$$

So depending on whether the random bit was a 0 or a 1, we get the map from equation 37 (X^0) or the map from equation 38 (X^1). Again, this derivation is analogous for the map Z^u . We have thus successfully made the constituents to our Bell matrices. The random Bell map itself is then as follows:

$$B_\alpha = Z^u X^w \Leftrightarrow \text{diagram} \quad (43)$$

To make a diagrammatic version of QOTP without Eve we need to compose the Hermitian adjoint of this Bell map to its input. The bottom Bell map can then be seen as Alice encrypting her state and the top Bell map can be seen as Bob decrypting this state. We also need to make sure that Alice and Bob make the same choice in α and thus use the same Bell map. This can be done by connecting the outputs of the spiders that generate the random numbers to the Bell maps of both Alice and Bob. In all, this makes QOTP without Eve to be the following diagram:

(44)

For this protocol to be a good candidate for communication we need equation 44 to reduce to the following:



(45)

This simply states that Alice's qubit is sent to Bob through the identity map. We already know that this is true due to the unitarity of the Bell maps. Diagrammatically, the proof is as follows:

Now that we have diagrammatically shown that QOTP without Eve is indeed a communication protocol, we can start to introduce Eve. First of all, let's see what the result is of Alice encrypting her state by means of a Bell map. We will thus analyze QOTP purely as an encryption protocol. To understand what happens in this case diagrammatically we need to first extend equation 40. Note that RHS of this equation is actually the Hermitian adjoint of discarding as it is defined in 18, which is in turn the fully mixed state. Since this state is independent of the choice of basis we can construct the following equation:

Using equation 47 we can prove that whenever Alice encrypts a state with a Bell map and discards her classical u and w she prepares the fully mixed state:

This might give some intuition for what Eve would receive after Alice has encrypted her state. However, one major difference between QOTP as an encryption protocol and QOTP as a communication protocol is that in the latter case Alice can not discard her classical u and w . Somehow she

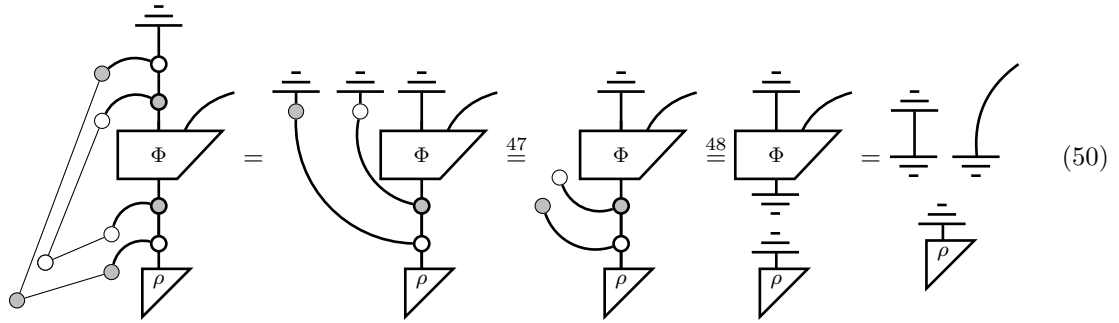
has to communicate them with Bob. The diagram of QOTP as a communication protocol and Eve with the ability to intercept the quantum state but not u or w is as follows:



Where Eve controls the map Φ and receives the rightmost output of this map.

Let's see what happens when we look at this situation from Eve's perspective and thus trace out (discard) Bob's channel.

*** Some info about causality here to show why do the trace maps behave as in the equation below ***



The third diagram in equation 50 is up until Eve's map Φ the same as equation 48. We therefore see that from Eve's perspective Alice gives her the fully mixed state due to the Bell map that she applies to her original state. So even as a communication protocol, the Bell map is responsible for encrypting the state such that Eve can extract no information from it.

3.3 Quantum Teleportation

In quantum teleportation, Alice and Bob want to communicate a qubit, ρ_1 , using the fact that they share an EPR pair, ρ_{23} , and a classical communication channel. Note that the subscripts in this paragraph help keep track of the different particles present. Subscript 1 refers to Alice's particle, 2 to her side of the EPR pair and 3 to Bob's side of the EPR pair. Alice measures ρ_1 together with ρ_2 in a Bell measurement, entangling these two states to give the total entangled state of ρ_{123} . This projects ρ_3 to one of four possible pure states dependent on the result of the Bell measurement done by Alice. Using the classical communication channel, Alice can send this measurement outcome to Bob in two classical bits. In order for Bob to extract ρ_1 from his part of the entangled state, ρ_3 , he needs to apply to it the Bell map that corresponds to the measurement outcome of Alice's Bell measurement.

The name of this protocol might lead one to think that it includes the teleportation of information. However, this is not the case. This protocol does not achieve faster than light communication. Although the projection of ρ_3 onto a pure state happens simultaneously with Alice making the Bell measurement, in order for Bob to receive any information on ρ_1 from ρ_3 he must apply the Bell map that corresponds to the measurement result of Alice's Bell measurement. Alice thus has to communicate classically to Bob the result of her Bell measurement.

Quantum teleportation carries some similarity to QOTP. In both protocols, Alice and Bob communicate two classical bits of information in order to communicate one qubit. Also, in both cases, Bob applies a Bell map. These similarities might give some intuition for the equivalence of these protocols. In section 4 we will see this equivalence diagrammatically.

3.3.1 Diagrammatic Implementation

The only component of this protocol that we have not worked out diagrammatically yet is the Bell measurement. We know that the Bell measurement is the adjoint of the Bell state. Therefore it suffices to create this Bell state and take its adjoint to make a Bell measurement.

Let's see if we can take the Bell state apart and construct its smaller constituents diagrammatically. The Bell state is actually a composition of a Hadamard (H) and a CNOT gate. The Hadamard gate is applied first to one of the qubits. It transforms $|0\rangle$ to $(|0\rangle + |1\rangle)/\sqrt{2}$ and $|1\rangle$ to $(|0\rangle - |1\rangle)/\sqrt{2}$. These superposition states actually form the basis states in a different basis. Therefore, the Hadamard gate can be seen as a basis transformation. For example, a Hadamard gate applied to basis states in the z basis will transform those states to the x basis. The CNOT gate is then applied to the two qubits. In the CNOT gate, one input qubit controls whether or not the other is negated. If the former is $|0\rangle$ the latter undergoes the identity and if the former is $|1\rangle$ the latter is negated. The control qubit in the CNOT gate is in this case the output of the Hadamard gate. The result of these operations entangles the two input qubits and puts them in one of four possible Bell states. Let's test this construction on input state $|00\rangle$ to see if it indeed behaves as expected:

1. The Hadamard gate puts the first qubit in superposition: $|00\rangle \Rightarrow \frac{(|0\rangle + |1\rangle)|0\rangle}{\sqrt{2}}$
2. The CNOT negates the second qubit if the first is $|1\rangle$: $\frac{(|0\rangle + |1\rangle)|0\rangle}{\sqrt{2}} \Rightarrow \frac{(|00\rangle + |11\rangle)}{\sqrt{2}}$

The result is thus indeed one of the Bell states, namely B_0 .

Diagrammatically, we do not have to construct the whole Hadamard gate to put one of the qubits into the required superposition. In fact, all we have to do is encode one qubit into a different basis than the other and choose one of the two bases to read the results in. The first part of our diagrammatic version of the Bell state thus becomes:



Where i and j are test inputs.

The CNOT gate itself is composed by a copy map and an XOR map. The first qubit is copied after which the second is XOR'd with the copied qubit [7]. Diagrammatically:



Applying test states:

$$\begin{array}{c} \text{CNOT} \end{array} \stackrel{2.1.4}{=} \begin{array}{c} \text{CNOT} \end{array} \stackrel{2.2.5}{=} |i\rangle \otimes |i \oplus j\rangle \quad (53)$$

Which is indeed the behavior of the CNOT gate.

Composing equations 51 and 52 then gives the Bell state:

$$\begin{array}{c} \text{Bell State} \end{array} \quad (54)$$

Let's again apply the state $|00\rangle$ to test the functionality of this Bell state preparation map:

$$\begin{aligned}
 & \begin{array}{c} \text{CNOT} \end{array} \stackrel{2.2.2}{=} \begin{array}{c} \text{CNOT} \end{array} \stackrel{2.2.1}{=} \begin{array}{c} \text{CNOT} \end{array} \stackrel{2.1.4}{=} \frac{1}{2} \left(\begin{array}{c} \text{CNOT} \end{array} \right) + \frac{1}{2} \left(\begin{array}{c} \text{CNOT} \end{array} \right) \\
 & \stackrel{2.1.4}{=} \frac{1}{2} \left(\begin{array}{c} \text{CNOT} \end{array} \right) + \frac{1}{2} \left(\begin{array}{c} \text{CNOT} \end{array} \right) \stackrel{2.2.1}{=} \frac{1}{2} \left(\begin{array}{c} \text{CNOT} \end{array} \right) + \frac{1}{2} \left(\begin{array}{c} \text{CNOT} \end{array} \right) \\
 & \stackrel{2.1.8}{=} \frac{1}{2} \left(\begin{array}{c} \text{CNOT} \end{array} \right) + \frac{1}{2} \left(\begin{array}{c} \text{CNOT} \end{array} \right) \stackrel{2.2.1}{=} \frac{1}{2} \left(\begin{array}{c} \text{CNOT} \end{array} \right) + \frac{1}{2} \left(\begin{array}{c} \text{CNOT} \end{array} \right)
 \end{aligned} \quad (55)$$

The result is thus indeed the expected Bell state. Note that whereas usually the constants in the Bell states are $1/\sqrt{2}$ here they are $1/2$ since the final state is doubled.

Let's choose the entangled state of 2.1.9 for state ρ_{23} . We can then compose the Bell measurement that Alice applies on the left of this entangled state and the Bell map that Bob applies to the right. Alice also inputs ρ_1 to the Bell measurement. Finally, we need to make sure to connect the outputs of Alice's Bell measurement to Bob's Bell map. The protocol for teleportation then becomes:

$$\begin{array}{c} \text{Alice} \quad \text{Bob} \\ \text{Teleportation Protocol} \end{array} \quad (56)$$

It is redundant to see what happens to Eve or to show that this protocol allows for communication. In section 4 we will see that this protocol is equivalent to the OTP, for which we have shown these things already.

3.4 Quantum Key Distribution

QKD is the only protocol that has been diagrammatically (somewhat) thoroughly discussed in literature [4]. Therefore, we will not go over the full security proof here. This section is meant to get the reader to understand the diagrammatic version of QKD, such that we can use it later on in the context of equivalences.

The QKD protocol BB84 was already described in the introduction. To write it out diagrammatically we need to generalize it to a protocol that is not dependent on the physical realization of the qubits. In the new protocol, we therefore say that Alice and Bob have the choice to encode their qubit in any two mutually unbiased bases, which we choose to be the z and x bases. Not considering Eve, if Alice and Bob then measure in the same basis, their quantum state is sent through just fine:

$$\begin{array}{c} \bullet \\ | \\ \bullet \end{array} \stackrel{2.1.4}{=} \begin{array}{c} \circ \\ | \\ \circ \end{array} \quad (57)$$

However, due to the fact that the bases are mutually unbiased we get the following situation when Alice and Bob's measurement bases do not agree:

$$\begin{array}{c} \circ \\ | \\ \bullet \end{array} \stackrel{2.2.4}{=} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \quad (58)$$

These are the cases that Alice and Bob decide to not use upon discussing their choice of bases later in the protocol.

Now if we limit Eve's interference to only a measurement in either the z or x bases she will have a 50% chance of measuring in the correct basis. In the case where Alice and Bob both use the x basis Eve can thus measure correctly:

$$\begin{array}{c} \bullet \\ | \\ \bullet \\ | \\ \bullet \end{array} \stackrel{2.1.4}{=} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \quad (59)$$

Or she measures in the wrong basis and both her and Bob receive a random bit:

$$\begin{array}{c} \bullet \\ | \\ \circ \\ | \\ \bullet \end{array} \stackrel{2.2.4}{=} \begin{array}{c} \bullet \\ | \\ \bullet \end{array} \quad (60)$$

This puts heavy constraints on Eve. Realistically, she could measure in different bases, or find even different ways to extract information from Alice's qubits. Therefore, it is more general to state that Eve can apply some map Φ , on which we can put constraints as needed:

$$\begin{array}{c} \text{Bob} \\ | \\ \boxed{\Phi} \\ | \\ \text{Alice} \end{array} \quad \begin{array}{c} \text{Eve} \\ | \end{array} \quad (61)$$

This is exactly how Kissinger et al. approach this problem in [4]. To prove security for noiseless communication they go on to claim that for Eve's intervention to be undetected whenever Alice and Bob's measurement results are the same, Eve's channel must exhibit the following property:

$$(62)$$

From here on Kissinger et al. in [4] include an extensive (fully diagrammatic) security proof which finally reaches the conclusion that for any Φ that satisfies 62 and orthonormal bases x and z we have:

$$(63)$$

In words: Eve's channel has no connection to Alice and Bob's and she thus learns nothing about the state Alice sent to Bob.

3.5 Quantum Key Recycling

4 Equivalences

The equivalence of QOTP and quantum teleportation is rather trivial. Simply putting them side by side and making a small adjustment to QOTP, drawing it a bit more suggestively, is enough to see the equivalence:

$$(64)$$

This is a strikingly simple equivalence. Bending the U-shaped curve in the quantum teleportation protocol such that it becomes a straight line already does the trick. In a sense, quantum teleportation could thus be seen as the EPR variant of the QOTP.

Due to their equivalence, whatever we can prove with the one diagram we can state as fact for the other without needing to prove it. This can be very convenient in security proofs.

References

- [1] Bob Coecke and Aleks Kissinger. *Picturing Quantum Processes*. Cambridge University Press, Cambridge, 2017.
- [2] Manon de Vries and Boris Skoric. Quantum Key Recycling with Eight-State Encoding. *Cryptography ePrint Archive*, 2016.
- [3] Ivan Djordjevic. Chapter 7 - quantum error correction. In Ivan Djordjevic, editor, *Quantum Information Processing and Quantum Error Correction*, pages 227 – 276. Academic Press, Oxford, 2012.
- [4] Aleks Kissinger, Sean Tull, and Bas Westerbaan. Picture-perfect Quantum Key Distribution. 2017.
- [5] John Markoff. Codebook Shows an Encryption Form Dates Back to Telegraphs, 2011.
- [6] Michael a. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. 2011.
- [7] Mehdi Saeedi and Igor Markov. Synthesis and optimization of reversible circuits - a survey. *ACM Computing Surveys*, 45, 10 2011.
- [8] C. E. Shannon. Communication Theory of Secrecy Systems. *Bell System Technical Journal*, 1949.

A Keywords

Base: E, page 2
Bra: A, page 1
Colour: E, page 2
Decoding: H, page 3
Density matrix: G, page 3
Discarding: G, page 3
Doubling: F, page 2
Effect: A, page 1
Hermitian Adjoint: A, page 1
Hermitian Conjugate: A, page 1
Identity: B, page 1
Ket: A, page 1
Kronecker delta: D, page 2
Linear map: C, page 1
Phase: H, page 3
Phase spider: H, page 3
Purity: F and G, pages 2 and 3
Spider: D, page 2
State: A, page 1
System type: B, page 1

Tensor product: F, page 3
Trace: G, page 3
Map: C, page 1
Mixed state: F, page 2
Transpose: A, page 1
Wire: B, page 1