Superdense Coding with GHZ and Quantum Key Distribution with W in the ZX-calculus

Anne Hillebrand

Oxford University Computing Laboratory
Oxford, UK

anne.hillebrand@maths.ox.ac.uk

Quantum entanglement is a key resource in many quantum protocols, such as quantum teleportation and quantum cryptography. Yet entanglement makes protocols presented in Dirac notation difficult to verify. This is why Coecke and Duncan have introduced a diagrammatic language for quantum protocols, called the ZX-calculus [11]. This diagrammatic notation is both intuitive and formally rigorous. It is a simple, graphical, high level language that emphasises the composition of systems and naturally captures the essentials of quantum mechanics. In the author's MSc thesis [18] it has been shown for over 25 quantum protocols that the ZX-calculus provides a relatively easy and more intuitive presentation. Moreover, the author embarked on the task to apply categorical quantum mechanics on quantum security; earlier works did not touch anything but Bennett and Brassard's quantum key distribution protocol, BB84. Two of the protocols in [18], namely superdense coding with the Greenberger-Horne-Zeilinger state and quantum key distribution with the W-state, will be presented in this paper.

1 Introduction

Quantum protocols are usually described in Dirac notation. Though such a presentation is adequate, it is low-level and therefore not a very intuitive formalism. The passage to a high level language was realized in [1], by relying on the compositional structure of monoidal categories. Corresponding presentations result in the form of quantum picturalism in [9, 10, 11, 13], which relies on the diagrammatic presentation of symmetric monoidal categories, tracing back to Penrose [27, 22, 29].

This diagrammatic notation is both intuitive and formally rigorous. It is a simple, graphical, high level language that emphasises the composition of systems and naturally captures the essentials of quantum mechanics. One crucial feature that will be exploited here is the encoding of complementary observables and corresponding phase shifts. Reasoning is done by rewriting diagrams, i.e. locally replacing some part of a diagram, according to a few simple rules. Diagrams are defined by their topology only; the number of inputs and outputs and the way they are connected. This exemplifies the 'flow' of information.

Entanglement, described by Einstein as "spooky action at a distance", is a key resource in many quantum protocols, like quantum teleportation and quantum cryptography. Yet entanglement makes protocols presented in Dirac notation difficult to verify. In the author's MSc thesis [18] an alternative presentation in the ZX-calculus of quantum protocols involving the GHZ or the W-state is considered. Over 25 different protocols are discussed, such as teleportation, superdense coding (SDC), quantum key distribution (QKD) and quantum direct communication. Moreover, the author has embarked on the task to apply quantum category theory on quantum security; earlier works did not touch anything but BB84 [3] in [1]. Two of the protocols in [18], SDC and QKD, will be discussed in this paper. SDC was first introduced by Bennett and Wiesner in [5]. In an SDC protocol a number of classical bits is transfered

Bart Jacobs, Peter Selinger, and Bas Spitters (Eds.):
8th International Workshop on Quantum Physics and Logic (QPL 2011)
EPTCS 95, 2012, pp. 103–121, doi:10.4204/EPTCS.95.10

by transferring fewer qubits. In this paper SDC with GHZ as described in [7, 17] will be presented in the ZX-calculus. Then a QKD protocol making use of the W-state will be presented. In QKD protocols a key is shared with two or more people in such a way that they can only retrieve the key if they work together. The first quantum key distribution protocol was proposed by Bennett and Brassard in [3] in 1984 and is generally referred to as the BB84 protocol. After that many other protocols have been proposed [16, 4, 2, 20, 25, 19, 26, 28, 8, 30]. In this paper QKD as described in [21] will be discussed.

To show that a protocol "works", the following definitions will be used.

Definition 1. *A quantum protocol consists of two parts, the* **set of instructions** *and the* **desired behaviour**. *The set of instructions are the things to be done to achieve the desired behaviour, i.e the goal of the protocol.*

Definition 2. *A quantum protocol is considered to be* **correct** *or* **valid** *if the set of instructions leads to the desired behaviour.*

This paper is organised as follows. First the ZX-calculus will be introduced in Sec. 2. Then SDC with GHZ will be presented in Sec. 3, after which QKD with W will be discussed in Sec. 4. Finally, some concluding remarks will be made in Sec. 5.

2 The Red/Green Calculus

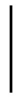
In this section the red/green calculus or the ZX-calculus is introduced. For a more thorough and complete presentation see [23, 12, 18] or [11][1].

2.1 Components of the ZX-calculus

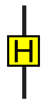
The ZX-calculus consists of components joined by wires, like an electrical circuit. Its components are the following:

1. Z-vertices (green dots), labeled by an angle $\alpha \in [0, 2\pi)$, called the phase, with any number of inputs and or outputs, zero included.
2. X-vertices (red dots), complementary to the Z-vertices, labeled by a phase, also with any number of inputs, including none.
3. H-vertices (yellow squares labeled with an H), which represent Hadamard gates. They have exactly one input and one output.
4. $\sqrt{D}$-vertices (black diamonds), which represent scalars. These generally don't have any inputs or outputs.

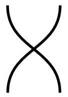
The Hilbert space interpretation of these components is as as follows:



$$= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$



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



$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

[1] Pictures from this paper are included with permission of the author.

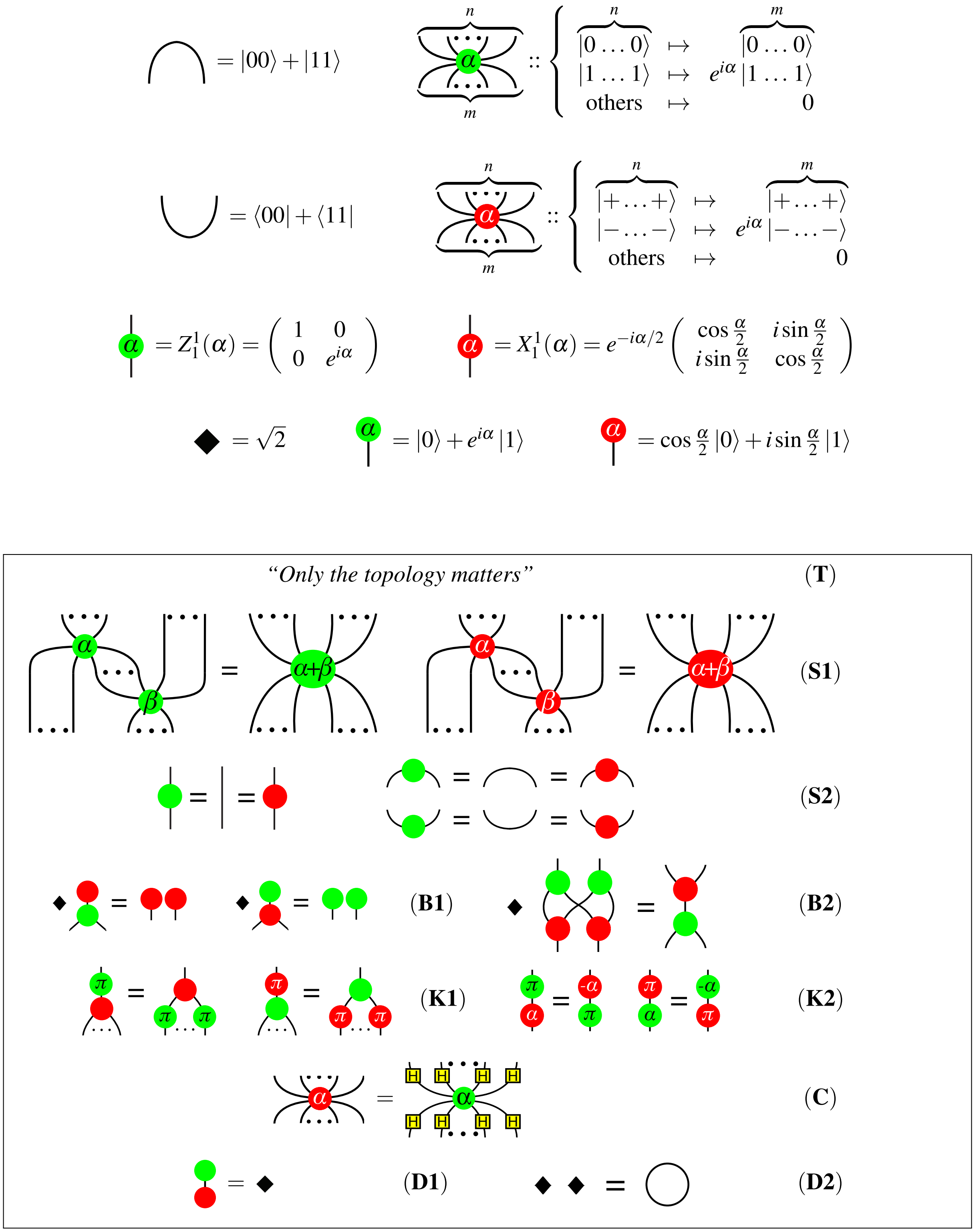

$= |00\rangle + |11\rangle$
n
m
α
$:: \begin{cases} \overbrace{|0\dots0\rangle}^{n} \mapsto \overbrace{|0\dots0\rangle}^{m} \\ |1\dots1\rangle \mapsto e^{i\alpha}|1\dots1\rangle \\ \text{others} \mapsto 0 \end{cases}$
$= \langle 00| + \langle 11|$
$:: \begin{cases} \overbrace{|+\dots+\rangle}^{n} \mapsto \overbrace{|+\dots+\rangle}^{m} \\ |-\dots-\rangle \mapsto e^{i\alpha}|-\dots-\rangle \\ \text{others} \mapsto 0 \end{cases}$
$= Z_1^1(\alpha) = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\alpha} \end{pmatrix}$
$= X_1^1(\alpha) = e^{-i\alpha/2}\begin{pmatrix} \cos\frac{\alpha}{2} & i\sin\frac{\alpha}{2} \\ i\sin\frac{\alpha}{2} & \cos\frac{\alpha}{2} \end{pmatrix}$
$= \sqrt{2}$
$= |0\rangle + e^{i\alpha}|1\rangle$
$= \cos\frac{\alpha}{2}|0\rangle + i\sin\frac{\alpha}{2}|1\rangle$
"Only the topology matters"
(T)
α
β
$\alpha+\beta$
(S1)
(S2)
(B1)
(B2)
π
(K1)
-α
(K2)
H
(C)
(D1)
(D2)

Figure 1: Basic Rules for the ZX-calculus

2.2 Quantomatic

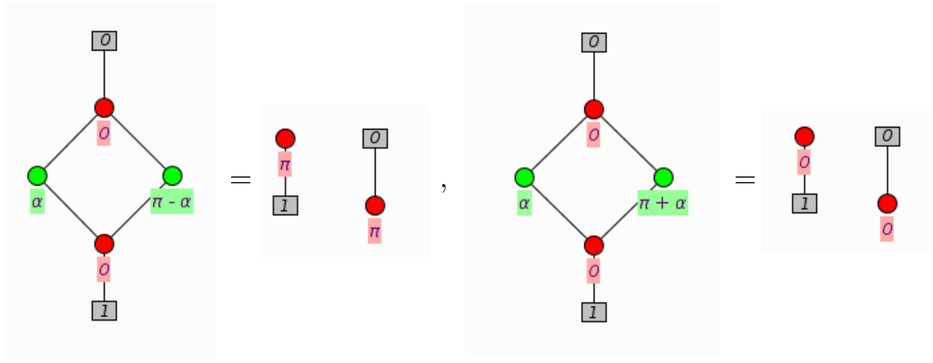
From now on all the pictures (except Fig. 1) are made with `quantomatic` [24], a software tool for reasoning with the ZX-calculus, developed jointly at Oxford, Cambridge, Google and Edinburgh. Different rule sets can be loaded into `quantomatic`. One can then input a graph and see what rewrites are possible within the loaded rules. Download and installation instructions can be found at `http://sites.google.com/site/quantomatic/home`. Using `quantomatic` to produce the pictures confirms that all the rewrites are valid, but `quantomatis` does not (yet) provide a way to determine the order in which these rewrites should be applied; `quantomatic`'s normalising tool often halts or gets into an infinite loop.

In `quantomatic` red and green dots are displayed as red and green dots, with their phase in a box of corresponding colour underneath the vertex. Hadamard gates are displayed as yellow boxes with an *H* in them. Finally, inputs and outputs are displayed as grey boxes with a number in it, called boundary vertices. `Quantomatic` does not distinguish between inputs and outputs, so they look the same and are numbered with the same counter. E.g. a diagram with one input and one output would have one boundary vertex with the number zero and one with the number one in it, as in the diagrammatic representation of the Hopf law in the next section. Which output or input gets which number is not important and depends solely on the order of input in `quantomatic`.

2.3 Basic Rules

Derivations in the Red/Green-calculus are done mostly by a few simple rules, outlined in Fig. 1. Note that rule **T** does not mean that the topology is always preserved; other rules might change this completely. Informally **T** can be seen as "yanking" the wires, making sure the number of inputs and outputs is preserved and the way they are connected.

An addition to these rules has been made by Kissinger in [23] and Coecke and Edwards in [12]. These two related rules that are called $|0\rangle$- and $|1\rangle$- supplementarity were found by solving a matrix equation in [23] and by means of the underlying algebraic structure in [12].

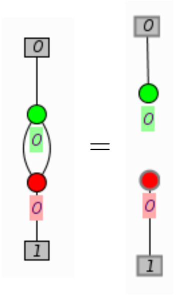


(**E**).

From now on scalars will be left out for sake of simplicity. Note also that `quantomatic` does not include scalars in the rewrites.

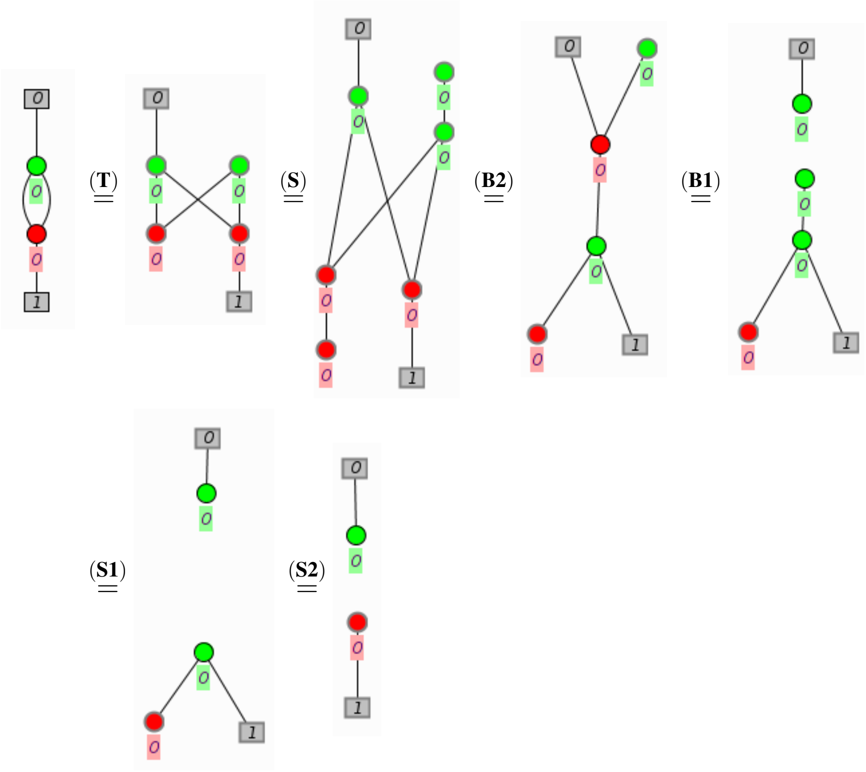
A useful derivation from the basic rules is the Hopf law:

Lemma 1 (Hopf law)**.**



(**B**′)

Proof.

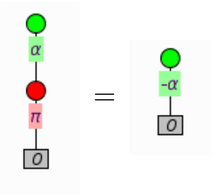


(1)

□

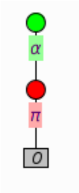
Another useful derivation, used later on is the following:

Lemma 2.

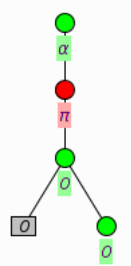


(**A**)

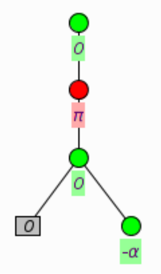
Proof.



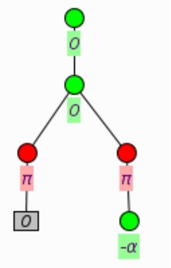
$\overset{(\mathbf{S})}{=}$



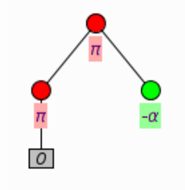
$\overset{(\mathbf{K2})}{=}$



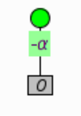
$\overset{(\mathbf{K1})}{=}$



$\overset{(\mathbf{S})}{=}$



$\overset{(\mathbf{S})}{=}$

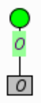


. (2)

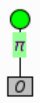
□

2.4 Measurements into the x- and z-basis

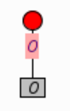
The graphical representation of measurements or "effects" into the x- and z-basis can be derived by the Hilbert space interpretation of points. $|+\rangle$ $(|x^+\rangle)$ and $|-\rangle$ $(|x^-\rangle)$ and $|0\rangle$ $(|z^+\rangle)$ and $|1\rangle(|z^-\rangle)$ are represented as



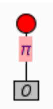
$= |+\rangle$



$= |-\rangle$



$= |0\rangle$



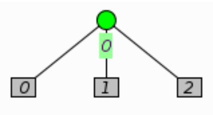
$= |1\rangle\,.$ (3)

2.5 The GHZ state

The GHZ state is one of the only two SLOCC-inequivalent classes of tripartite entanglement [15]. SLOCC-inequivalent means inequivalent under Stochastic Local Operations and Classical Communication, i.e. one cannot be turned into the other by means of stochastic local operations (unitaries and or measurements) and classical communication. GHZ is defined as $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, or as the map

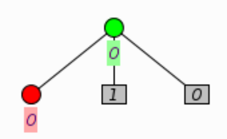
$$GHZ :: \begin{cases} |0\rangle \mapsto |00\rangle \\ |1\rangle \mapsto |11\rangle\,. \end{cases}$$

Graphically it is represented as [11]

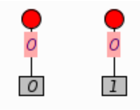


. (4)

Plugging $|0\rangle$ and $|1\rangle$ gives

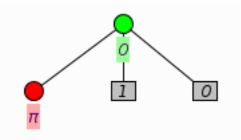


$\overset{(\mathbf{B1})}{=}$

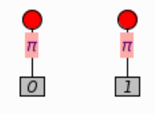


$= |00\rangle$ (5)

and



$\overset{(\mathbf{B1})/(\mathbf{K1})}{=}$



$= |11\rangle\,,$ (6)

as required.

2.6 The W-state

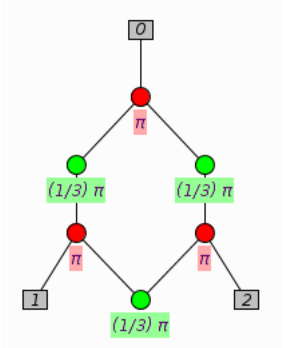
The class of W-states is SLOCC-inequivalent to the class of GHZ states [15]. The W-state is defined as

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle),$$

or as the map [23]

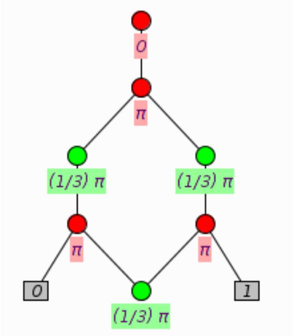
$$W :: \begin{cases} |0\rangle \mapsto |01\rangle + |10\rangle \\ |1\rangle \mapsto |00\rangle\,. \end{cases}$$

Considering this map, the W-state can be graphically represented as [23]

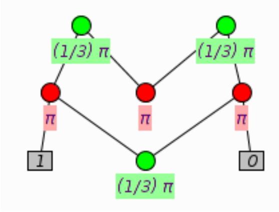


$$. \qquad (7)$$

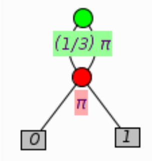
This graphical representation shows the robustness of the W-state; due to the pairwise entanglement, after tracing out one of the qubit, there is still the possibility of bipartite entanglement, as opposed to the GHZ state, which is fully separable when any of the qubits is traced out. Plugging $|0\rangle$ in Eq. 7 gives



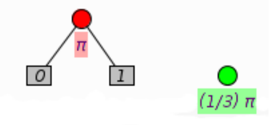
$$\overset{(\mathbf{S1})}{=}$$



$$\overset{(\mathbf{K2}),(\mathbf{S})}{=}$$

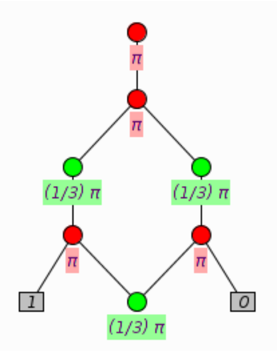


$$\overset{(\mathbf{B}')}{=}$$

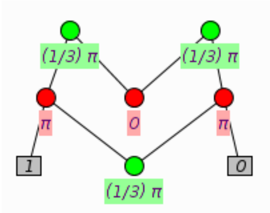


$$= |01\rangle + |10\rangle\,, \qquad (8)$$

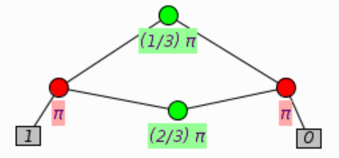
as expected. Plugging $|1\rangle$ in Eq. 7 gives



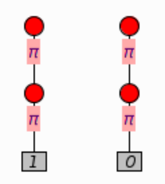
$\overset{(\mathbf{S1})}{=}$



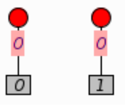
$\overset{(\mathbf{S})}{=}$



$\overset{(\mathbf{E})}{=}$



$\overset{(\mathbf{S1})}{=}$



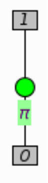
$= |00\rangle\,,$ (9)

as required.

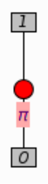
2.7 The Pauli Matrices

By the Hilbert space interpretation, one can obtain the representation of the Pauli-Z and Pauli-X matrices in ZX-calculus:

$\sigma_z =$



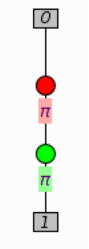
$= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \qquad \sigma_x =$



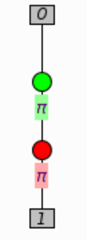
$= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} .$

Once the Pauli-X and Z matrices are known, it is easily deduced that $i\sigma_y = \sigma_z \times \sigma_x = \sigma_z \circ \sigma_x$ and $-i\sigma_y = \sigma_x \times \sigma_z = \sigma_x \circ \sigma_z$ are compositions of σ_x and σ_z.

$i\sigma_y =$



$= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad -i\sigma_y =$

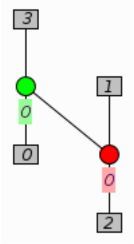


$= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} .$

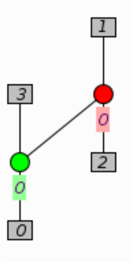
2.8 Controlled Not gate

Another useful tool is the Controlled Not gate. The Controlled Not gate is defined as follows:

CNOT =



=



$$= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}. \qquad (10)$$

3 Superdense Coding with GHZ

As with Bell states, it is possible to transfer an amount of classical bits by transferring fewer qubits by means of different states in the GHZ class. When states in the GHZ class are used for super dense coding, two qubits need to be transfered in order to transfer three classical bits [7]. This section is divided up in five subsections. First the steps of the protocol will be explained. Then the eight different states in the GHZ class will be presented. In the last three subsections it will be shown how, through measurement in the GHZ basis, these eight different states can be translated into three classical bits, proving the validity of the protocol.

3.1 Super Dense Coding with GHZ protocol

Provided Alice and Bob share $|GHZ\rangle$, such that the first qubit belongs to Bob and the other two qubits belong to Alice, the following protocol describes superdense coding with GHZ as in [7, 17]:

1. Alice applies a combination of $I, \sigma_x, i\sigma_y$ and σ_z on both her qubits, encoding one of eight distinguishable states in the GHZ class.
2. Alice transfers both her qubits to Bob.
3. Bob measures all three qubits in the GHZ basis, retrieving the state Alice encoded.
4. Bob translates the retrieved state to three classical bits.

3.2 Different GHZ states

There are eight different states in the GHZ class. One can go from one to the other by performing unitary single particle operations on two of the three particles. These unitary operations are $I, \sigma_x, i\sigma_y$ and σ_z. Though there are 16 different combinations of these operators on two qubits, only half of them generate distinguishable states [31] as can be seen by comparing the graphical representations in Table 1 and 2 in Appendix A. In this section we will work with states in the standard form

$$\left|GHZ_{+ij}\right\rangle = \frac{1}{\sqrt{2}}(|0ij\rangle + \left|1\bar{i}\bar{j}\right\rangle), \qquad (11)$$

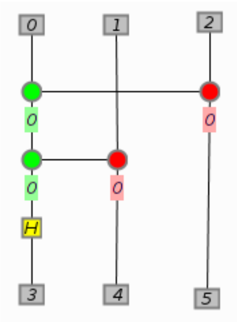
as in [14, 7], where $i, j \in \{0, 1\}$, $\bar{i} = 1 - i$ and $\bar{j} = 1 - j$.

3.3 Encoding a GHZ measurement outcome into classical bits

The encoding is as in [6]. After measurement, an output qubit is encoded as 0 if it is $|0\rangle$ and as 1 if it is$|1\rangle$. Every GHZ state gives three output bits. If the first output bit is 0, then there is an odd number of $|+\rangle$ in the basis, otherwise an even number. If the second output bit is 0, then the first two bits in the GHZ class state are the same, otherwise they are different. And finally, if the last output bit is 0, the last two bits in the GHZ class state are the same. This encoding is displayed in Table 1 in Appendix A.

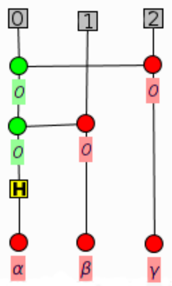
3.4 Measurement into the GHZ basis

The circuit to measure into the GHZ basis is [6]

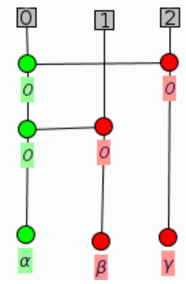


, (12)

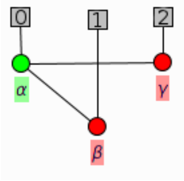
which gives three qubits in the z-basis. Plugging states in the z-basis, we obtain for $\alpha,\beta,\gamma \in \{0,\pi\}$



$\overset{(\mathbf{C})}{=}$



$\overset{(\mathbf{S})}{=}$



, (13)

which results in one of eight states in the GHZ class upside down by Table 1 and 2 in Appendix A if values for α, β and γ are set.

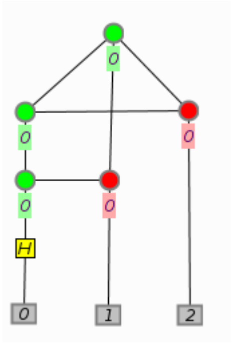
3.5 Validity of the protocol

Lemma 3. *The encoding in combination with the GHZ measurement circuit in [6] makes for a valid Superdense Coding protocol* [2].

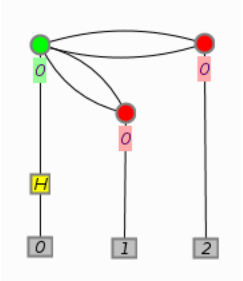
Proof. Let $|0\rangle = 0$ and $|1\rangle = 1$ in classical bits. What needs to be shown is that for all eight states in the

[2] Note that this encoding is different from [7, 17].

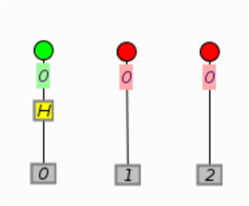
GHZ class, their measurement outcome is equal to their binary representation in Table 1 in Appendix A.



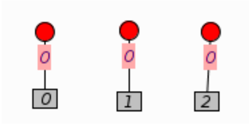
$\overset{(\mathbf{S})}{=}$



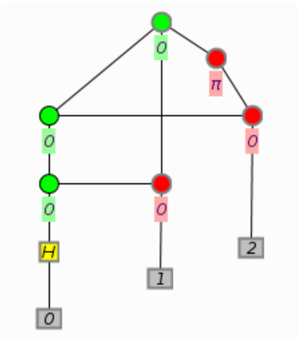
$\overset{(\mathbf{B}')}{=}$



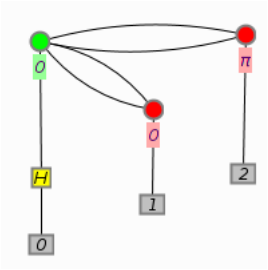
$\overset{(\mathbf{C})}{=}$



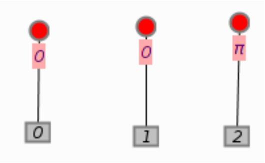
$$= |000\rangle = 000 = 0 \tag{14}$$



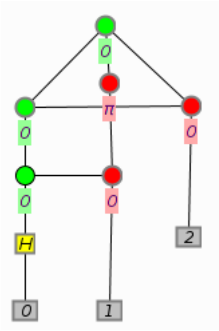
$\overset{(\mathbf{S})}{=}$



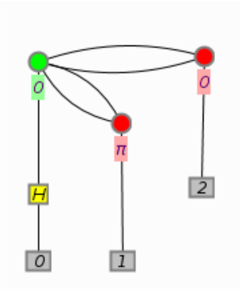
$\overset{(\mathbf{B}')/(\mathbf{C})}{=}$



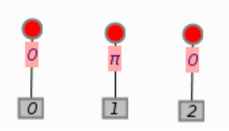
$$= |001\rangle = 001 = 1 \tag{15}$$



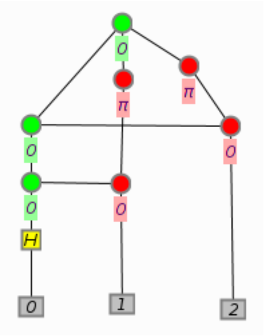
$\overset{(\mathbf{S})}{=}$



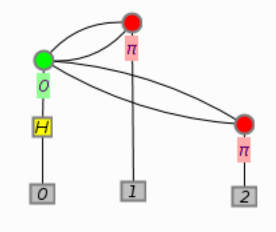
$\overset{(\mathbf{B}')/(\mathbf{C})}{=}$



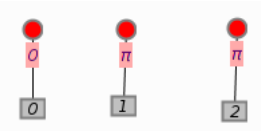
$$= |010\rangle = 010 = 2 \tag{16}$$



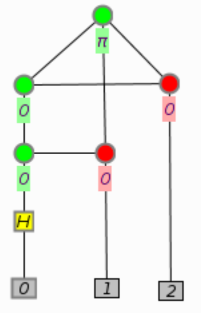
$\underline{\underline{(\mathbf{S})}}$



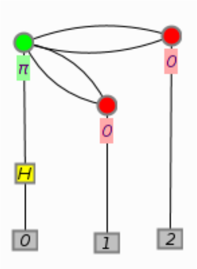
$\underline{\underline{(\mathbf{B}')/(\mathbf{C})}}$



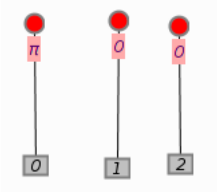
$$= |011\rangle = 011 = 3 \tag{17}$$



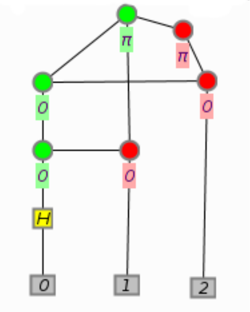
$\underline{\underline{(\mathbf{S})}}$



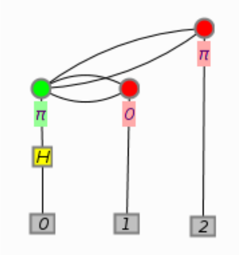
$\underline{\underline{(\mathbf{B}')/(\mathbf{C})}}$



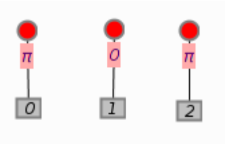
$$= |100\rangle = 100 = 4 \tag{18}$$



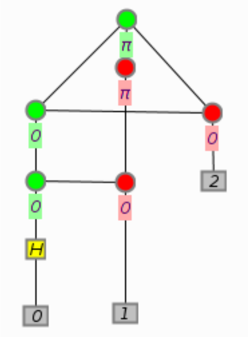
$\underline{\underline{(\mathbf{S})}}$



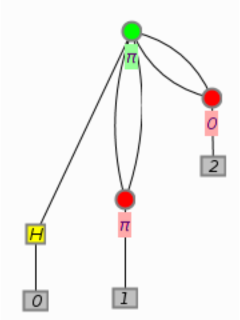
$\underline{\underline{(\mathbf{B}')/(\mathbf{C})}}$



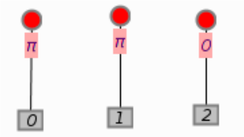
$$= |101\rangle = 101 = 5 \tag{19}$$



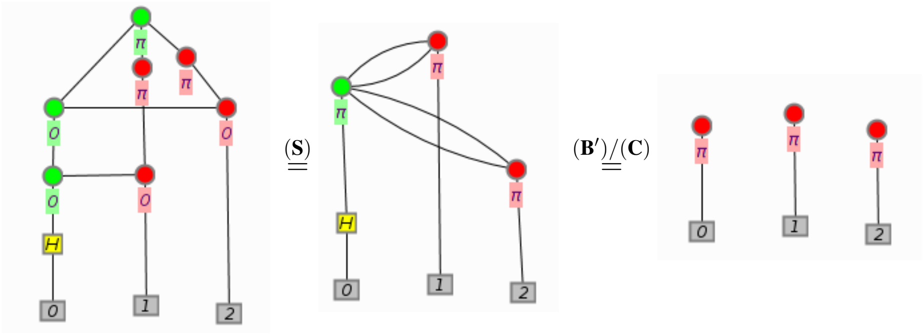
$\underline{\underline{(\mathbf{S})}}$



$\underline{\underline{(\mathbf{B}')/(\mathbf{C})}}$



$$= |110\rangle = 110 = 6 \tag{20}$$



$$= |111\rangle = 111 = 7. \tag{21}$$

Eq. 14-21 imply the validity of the protocol. □

3.6 Superdense coding with N-GHZ

In a similar way superdense coding for N-GHZ states can be constructed. One of $\{I, \sigma_x, i\sigma_y, \sigma_z\}$ can be applied on the N^{th} qubit and one of $\{I, \sigma_x\}$ on qubit $2-(N-1)$ to encode 2^N different states. They can be distinguished with a measurement like the GHZ basis measurement [6].

4 Pairwise Quantum Key Distribution with W_3

In this section the Quantum Key Distribution protocol with W_3 from [21] will be explained. It will moreover be shown by means of the ZX-calculus that this protocol works.

4.1 Pairwise Quantum Key Distribution with W_3 protocol

Alice, Bob and Charlie share a series of W_3-states in the Pairwise Quantum Key Distribution with W_3 protocol and perform measurements on their qubits in such way that two of them will share a common (classical) key. Assuming they share a series of W_3-states, the protocol can be established as follows:

1. All choose at random the x- or the z-basis to measure their qubit in.
2. Each announces publicly his or her measurement direction.
3. For security reasons, they randomly choose to announce their measurement outcomes, to check for eavesdropping. If they do, the protocol is restarted.
4. If the overall measurement basis is $z-x-x$, $x-z-x$ or $x-x-z$, they continue with the protocol. Otherwise they start over and discard these measurement outcomes.
5. The one who measured along the z-axis is the decider. S/he tells the others whether the outcome is $\langle z^+|$. Otherwise they restart the protocol.
6. The other two now know that they have the same outcome, i.e. they share a bit now.
7. Repeat the protocol until the desired amount of key bits are obtained.
8. Use the information from step 3 to check for eavesdropping. If eavesdropping is detected, discard the obtained key bits and start a new quantum channel to repeat the protocol.

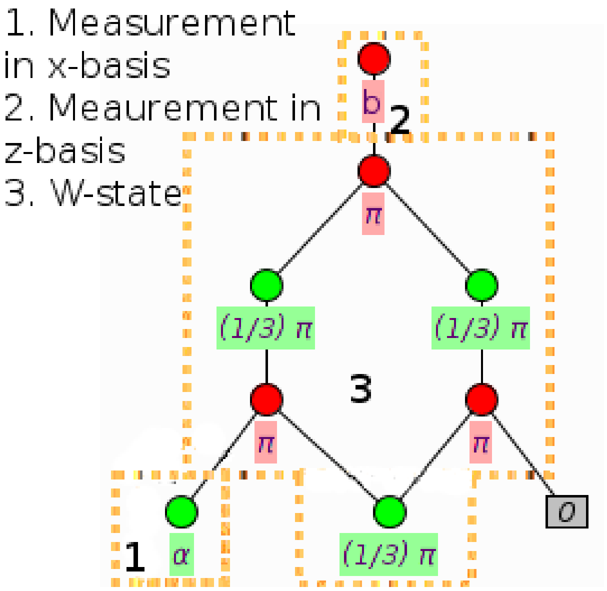


Figure 2: Graphical representation of the set of instructions of the Pairwise Quantum Key Distribution with W_3 protocol. $\alpha, b \in 0, \pi$

Lemma 4. *Fig. 2 is the graphical representation of the set of the instructions of the Pairwise Quantum Key Distribution with W_3 protocol, when the first two measurements are in the z- and x-basis.*

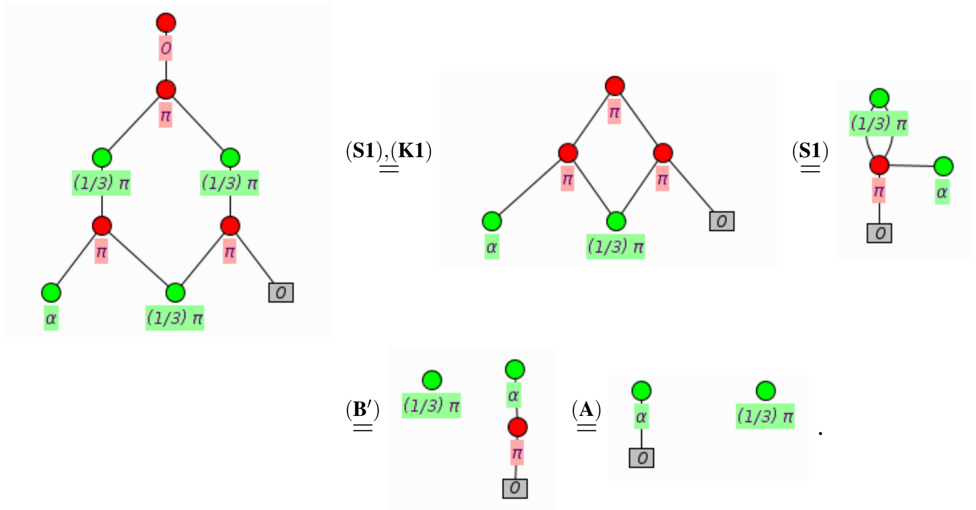
Proof. Box 1 is a measurement in the x-basis, box 2 is a measurement into the z-basis. Box 3 is the W_3-state. □

Lemma 5. *If any one of them gets the outcome $\langle z^- |$ the entanglement will be broken and the outcomes for the other two will be $\langle z^+ |$.*

Proof. Setting $b = \pi$, then by Eq 9. □

Lemma 6. *When there is a proper overall measuring basis and the decider has the outcome $\langle z^+ |$, the other two always have the same result.*

Proof. Let $\alpha \in \{0, \pi\}$ and set $b = 0$, then



. (22)

□

Corollary 7. *The Pairwise Quantum Key Distribution with W_3 protocol is correct.*

5 Conclusions

In this paper two of the 25 plus quantum protocols in [18] have been presented in the ZX-calculus. It has been shown that they are both valid protocols, by means of easy manipulations of their diagrammatic representation. Producing the diagrammatic representation of a protocol is a matter of “gluing” together basic constructions, such as CNOT gates, Bell states and measurements. The more of these basic constructions are known, the easier this becomes. Many of these basic constructions can be found in the author’s MSc thesis, along with examples in which they are used [18]. After this representation has been found, the correctness of a protocol can be shown by a few simple manipulations of the diagrams. From this it can be concluded that the red/green calculus provides a clear and intuitive way to represent and check quantum protocols.

Though not explicitily discussed here, it turns out that it is difficult to check the security of many protocols by means of the ZX-calculus. This is because detection of eavesdropping or disturbance often depends on the probability of obtaining illegal measurement outcomes after the quantum channel is interfered with. Although it is easy to plug different measurement outcomes in the diagrammatic notation, it is not always possible to calculate what combinations of measurement outcomes are possible. Moreover one cannot calculate the probability of different combinations of measurement outcomes from the diagrammatic notation, because in the implementation of the the ZX-calculus, `quantomatic` [24], scalars are ignored.

One can conclude from this, that a presentation in either Dirac notation or the ZX-calculus is not optimal. Instead, a combined approach should be taken. The ZX-calculus provides a simple and intuitive way to understand the workings of the protocol and Dirac notation is helpful to check the security of protocols.

References

[1] S. Abramsky & B. Coecke (2004): *A categorical semantics of quantum protocols*. In: Logic in Computer Science, 2004. Proceedings of the 19th Annual IEEE Symposium on, pp. 415 – 425, doi:10.1109/LICS.2004.1319636.

[2] C. Bennett (1992): *Quantum cryptography using any two nonorthogonal states*. Physical Review Letters 68(21), pp. 3121–3124, doi:10.1103/PhysRevLett.68.3121.

[3] C. Bennett & G. Brassard (1984): *Quantum cryptography: Public key distribution and coin tossing*, pp. 175–179. 175, Bangalore, India, doi:10.1016/j.tcs.2011.08.039. Available at `http://www.cs.ucsb.edu/~chong/290N-W06/BB84.pdf`.

[4] C. Bennett, G. Brassard & N. Mermin (1992): *Quantum cryptography without Bell's theorem*. Physical Review Letters 68(5), pp. 557–559, doi:10.1103/PhysRevLett.68.557.

[5] C. Bennett & S. Wiesner (1992): *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*. Phys. Rev. Lett. 69(20), pp. 2881–2884, doi:10.1103/PhysRevLett.69.2881.

[6] D. Bruss, A. Ekert, S. F. Huelga, J.-W. Pan & A. Zeilinger (1997): *Quantum Computing with Controlled-Not and Few Qubits*. 355, The Royal Society, doi:10.1098/rsta.1997.0124. Available at `http://www.jstor.org/stable/54931`.

[7] J. L. Cereceda (2001): *Quantum Dense coding using three qubits*. ArXiv Quantum Physics e-prints Available at `http://arxiv.org/abs/quant-ph/0105096`.

[8] R. Cleve, D. Gottesman & H.-K. Lo (1999): *How to share a quantum secret*. Physical Review Letters 83, pp. 648–651, doi:10.1103/PhysRevLett.83.648. Available at `http://link.aps.org/doi/10.1103/PhysRevLett.83.648`.

[9] B. Coecke (2006): *Kindergarten Quantum Mechanics: Lecture Notes*. AIP Conference Proceedings 810(1), pp. 81–98, doi:10.1063/1.2158713. Available at `http://link.aip.org/link/?APC/810/81/1`.

[10] B. Coecke (2010): *Quantum Picturalism*. Contemporary Physics 51, pp. 59–83. Available at `http://arxiv.org/abs/0908.1787`.

[11] B. Coecke & R. Duncan (2011): *Interacting quantum observables: categorical algebra and diagrammatics*. New Journal of Physics 13(4), p. 043016, doi:10.1088/1367-2630/13/4/043016. Available at `http://stacks.iop.org/1367-2630/13/i=4/a=043016`.

[12] B. Coecke & B. Edwards (2010): *Three qubit entanglement within graphical Z/X-calculus*. In: HPC, pp. 22–33. Available at `http://arxiv.org/abs/1103.2811`.

[13] B. Coecke & S. Perdrix (2010): *Environment and classical channels in categorical quantum mechanics*. In: Proceedings of the 24th international conference/19th annual conference on Computer science logic, CSL'10/EACSL'10, Springer-Verlag, pp. 230–240, doi:10.1007/978-3-642-15205-4_20. Available at `http://arxiv.org/abs/1004.1598`.

[14] F.-G. Deng, X.-H. Li, C.-Y. Li, P. Zhou & H.-Y. Zhou (2005): *Multiparty quantum-state sharing of an arbitrary two-particle state with Einstein-Podolsky-Rosen pairs*. Physical Review A 72(4), p. 044301, doi:10.1103/PhysRevA.72.044301.

[15] W. Dür, G. Vidal & J. I. Cirac (2000): *Three qubits can be entangled in two inequivalent ways*. Physical Review A 62(6), p. 062314, doi:10.1103/PhysRevA.62.062314.

[16] A. Ekert (1991): *Quantum cryptography based on Bell's theorem*. Physical Review Letters 67(6), pp. 661–663, doi:10.1103/PhysRevLett.67.661.

[17] V. N. Gorbachev, A. I. Trubilko, A. I. Zhiliba & E. S. Yakovleva (2000): *Teleportation of entangled states and dense coding using a multiparticle quantum channel*. Technical Report. Available at `http://arxiv.org/abs/quant-ph/0011124`.

[18] A. M. Hillebrand (2011): *Quantum Protocols involving Multiparticle Entanglement and their Representations*

in the ZX-calculus. Master's thesis, University of Oxford. Available at http://www.cs.ox.ac.uk/people/bob.coecke/Anne.pdf.

[19] H. Imai, J. Mueller-Quade, A. C. A. Nascimento, P. Tuyls & A. Winter (2003): *A Quantum Information Theoretical Model for Quantum Secret Sharing Schemes*. *ArXiv Quantum Physics e-prints* Available at http://arxiv.org/abs/quant-ph/0311136.

[20] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter & A. Zeilinger (2000): *Quantum Cryptography with Entangled Photons*. *Physical Review Letters* 84(20), pp. 4729–4732, doi:10.1103/PhysRevLett.84.4729.

[21] J. Joo, J. Lee, J. Jang & Y.-J. Park (2002): *Quantum secure Communication via W states*. *ArXiv Quantum Physics e-prints* Available at http://arxiv.org/abs/quant-ph/0204003.

[22] A. Joyal & R. Street (1991): *The geometry of tensor calculus, I*. *Advances in Mathematics* 88(1), pp. 55 – 112, doi:10.1016/0001-8708(91)90003-P. Available at http://www.sciencedirect.com/science/article/pii/000187089190003P.

[23] A. Kissinger (2009): *Exploring a Quantum Theory with Graph Rewriting and Computer Algebra*. In J. Carette, L. Dixon, C. Coen & S. Watt, editors: *Intelligent Computer Mathematics*, *Lecture Notes in Computer Science* 5625, Springer Berlin / Heidelberg, pp. 90–105, doi:10.1007/978-3-642-02614-0_12.

[24] A. Kissinger, A. Merry, B. Frot, L. Dixon, M. Soloviev & R. Duncan (2008-present): *Quantomatic*. Available at http://sites.google.com/site/quantomatic/home.

[25] H.-K. Lo, X. Ma & K. Chen (2005): *Decoy State Quantum Key Distribution*. *Physical Review Letters* 94(23), doi:10.1103/PhysRevLett.94.230504.

[26] A. Nascimento, J. Mueller-Quade & H. Ima (2001): *Improving quantum secret-sharing schemes*. *Physical Review A* 64, doi:10.1103/PhysRevA.64.042311.

[27] R. Penrose (1971): *Application of negative dimensional tensors*. *Combinatorial Mathematics and its Applications* , pp. 221–244. Available at http://www.math.uic.edu/~kauffman/Penrose.pdf.

[28] K. Rietjens (2004): *Quantum Secret Sharing Schemes*. Master's thesis, Technische Universiteit Eindhoven. Available at www.win.tue.nl/~henkvt/images/VerslagKarinRietjens.pdf.

[29] P. Selinger (2007): *Dagger Compact Closed Categories and Completely Positive Maps*. *Electronic Notes in Theoretical Computer Science (ENTCS)* 170, pp. 139–163, doi:10.1016/j.entcs.2006.12.018. Available at http://portal.acm.org/citation.cfm?id=1229185.1229207.

[30] S. Singh & R. Srikanth (2005): *Generalized quantum secret sharing*. *Phys. Rev. A* 71, doi:10.1103/PhysRevA.71.012328. Available at http://link.aps.org/doi/10.1103/PhysRevA.71.012328.

[31] C. Wang, F. Deng & G. Long (2005): *Multi-step quantum secure direct communication using multi-particle Green-Horne-Zeilinger state*. *Optics Communications* 253(1-3), pp. 15 – 20, doi:10.1016/j.optcom.2005.04.048. Available at http://www.sciencedirect.com/science/article/pii/S0030401805003949.

A The Graphical representation of GHZ class States

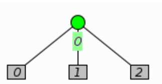
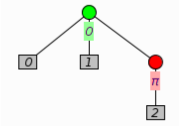
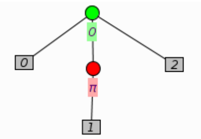
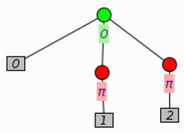
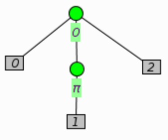
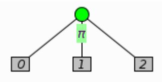
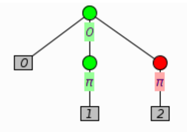
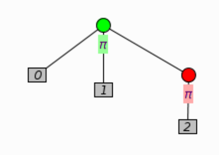
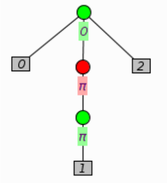
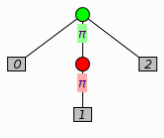
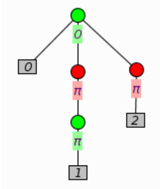
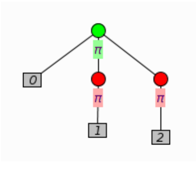
#	Binary	Standard Form (SF)	Unitaries	Graphical Representation
0	000	$\frac{1}{\sqrt{2}}(\|000\rangle+\|111\rangle)$	$I\otimes I$	
1	001	$\frac{1}{\sqrt{2}}(\|001\rangle+\|110\rangle)$	$I\otimes\sigma_x$	
2	010	$\frac{1}{\sqrt{2}}(\|010\rangle+\|101\rangle)$	$\sigma_x\otimes I$	
3	011	$\frac{1}{\sqrt{2}}(\|011\rangle+\|100\rangle)$	$\sigma_x\otimes\sigma_x$	
4	100	$\frac{1}{\sqrt{2}}(\|000\rangle-\|111\rangle)$	$\sigma_z\otimes I$	 $\overset{(\mathbf{S})}{=}$ 
5	101	$\frac{1}{\sqrt{2}}(\|001\rangle-\|110\rangle)$	$\sigma_z\otimes\sigma_x$	 $\overset{(\mathbf{S})}{=}$ 
6	110	$\frac{1}{\sqrt{2}}(\|010\rangle-\|101\rangle)$	$i\sigma_y\otimes I$	 $\overset{(\mathbf{K2})}{=}$ 
7	111	$\frac{1}{\sqrt{2}}(\|011\rangle-\|100\rangle)$	$i\sigma_y\otimes\sigma_x$	 $\overset{(\mathbf{S})}{=}$ 

Table 1: This table shows the eight different states in the GHZ class, their binary presentation, the unitaries that should be applied to the second and the third qubit to obtain this state from $|GHZ\rangle$ and finally their graphical representation.

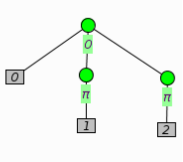
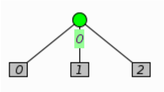
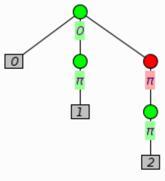
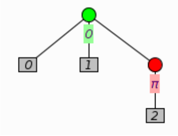
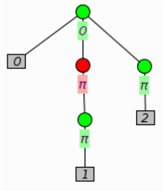
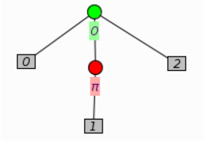
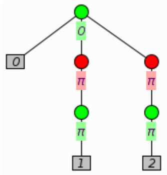
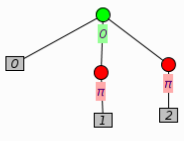
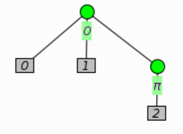
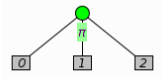
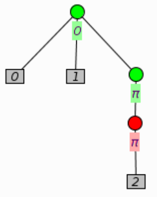
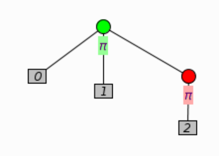
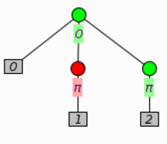
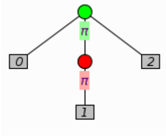
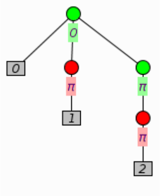
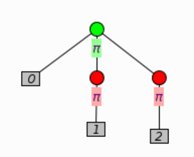
#	Binary	Alternative Form (AF)	Unitaries	Graphical Representation
0	000	$\frac{1}{\sqrt{2}}(\|111\rangle + \|000\rangle)$	$\sigma_z \otimes \sigma_z$	 $\overset{\textbf{(S)}}{=}$ 
1	001	$\frac{1}{\sqrt{2}}(\|110\rangle + \|001\rangle)$	$\sigma_z \otimes i\sigma_y$	 $\overset{\textbf{(S)},\textbf{(K2)}}{=}$ 
2	010	$\frac{1}{\sqrt{2}}(\|101\rangle + \|010\rangle)$	$i\sigma_y \otimes \sigma_z$	 $\overset{\textbf{(S)},\textbf{(K2)}}{=}$ 
3	011	$\frac{1}{\sqrt{2}}(\|100\rangle + \|011\rangle)$	$i\sigma_y \otimes i\sigma_y$	 $\overset{\textbf{(S)},\textbf{(K2)}}{=}$ 
4	100	$\frac{1}{\sqrt{2}}(\|111\rangle - \|000\rangle)$	$I \otimes \sigma_z$	 $\overset{\textbf{(S)}}{=}$ 
5	101	$\frac{1}{\sqrt{2}}(\|100\rangle - \|001\rangle)$	$I \otimes i\sigma_y$	 $\overset{\textbf{(S)},\textbf{(K2)}}{=}$ 
6	110	$\frac{1}{\sqrt{2}}(\|101\rangle - \|010\rangle)$	$\sigma_x \otimes \sigma_z$	 $\overset{\textbf{(S)}}{=}$ 
7	111	$\frac{1}{\sqrt{2}}(\|100\rangle - \|011\rangle)$	$\sigma_x \otimes i\sigma_y$	 $\overset{\textbf{(S)},\textbf{(K2)}}{=}$ 

Table 2: This table shows the remaining states in the GHZ class, their binary presentation, the unitaries that should be applied to the second and the third qubit to obtain this state from $|GHZ\rangle$ and finally their graphical representation.