UNIVERSITY OF TARTU

Institute of Computer Science
Software Engineering

Kristiina Rahkema

Quantum Position Verification in the Random Oracle Model

Master's Thesis (30 ECTS)

Supervisor: Dominique Unruh, PhD

Tartu 2016

Quantum Position Verification in the Random Oracle Model

Abstract:
Consider a situation where we wish to verify an entity solely by its location. This is called position verification. The simplest form of position verification is distance bounding where the verifier is located in the middle of the provers region, he sends information to the prover and checks how long it takes for the prover to respond. Since this is not always desirable one can place verifiers around the provers region forming a kind of triangulation. This thesis improves on the precision of the quantum position verification protocol form [Dominique Unruh, *Quantum position verification in the random oracle model*, CRYPTO 2014] i.e. presents a modification of the protocol that is sound for a smaller region. This is done by adding an additional receiving verifier. The previous result uses a two-player monogamy game. We define the three player monogamy game needed for the proof of the new protocol and explain our progress on the proof of this monogamy game. We also compare different three-player monogamy games and prove some results on their winning probabilities.

Keywords:
Quantum cryptography, monogamy of entanglement, quantum position verification, random oracle model

CERCS: P170 Computer science, numerical analysis, systems, control, P190 Mathematical and general theoretical physics, classical mechanics, quantum mechanics, relativity, gravitation, statistical physics, thermodynamics

Kvantkrüptograafiline positsiooni verifitseerimine juhusliku oraakli mudelis

Lühikokkuvõte:
Juhul kui kasutaja õigsuse kontrollimiseks on võimalik kasutada ainult tema asukohta, nimetatakse seda positsiooni verifitseerimiseks. Lihtsaim viis positsiooni verifitseerimisest on kasutaja kauguse mõõtmine keskpunktist (*distance bounding*). Verifitseerija paikneb kontrollitava ala keskel, saadab informatsiooni tõestajale ning kontrollib vastuse aega. Kuna selline ülesehitus ei ole alati soovitud, on võimalik kasutada ka teistsugust verifitseerijate asetust. Verifitseerijaid saab seada ümber tõestatava piirkonna, teatud liiki triangulatsioonis. Antud lõputöö muudab artiklis [Dominique Unruh, *Quantum position verification in the random oracle model*, CRYPTO 2014] esitatud positsiooni verifitseerimise protokolli, esitades uue versiooni protokollist, mis on turvaline väiksemal tõestataval piirkonnal. Algse protokolli turvalisuse tõestus kasutab kahe mängijaga põimunud kvantsüsteemide monogaamsuse mängu teoreemi. Lisades juurde ühe verifitseerija, defineerime uue kolme mängijaga põimunud kvantsüsteemide monogaamsuse mängu. Tõestame et muudetud protokolli turvalisus sõltub uue kolme mängijaga mängu võidu tõenäosusest. Selgitame probleeme ja edusamme antud monogaamsuse mängu tõestamisel. Võrdleme erinevaid kolme mängijaga monogaamsuse mänge ning tõestame mõned võidu tõenäosuste tulemused.

Võtmesõnad:
Kvantkrüptograafia, positisiooni verifitseerimine, põimumise monogaamsus, juhusliku oraakli mudel

CERCS: P170 Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine (automaatjuhtimisteooria), P190 Matemaatiline ja üldine teoreetiline füüsika, klassikaline mehaanika, kvantmehaanika, relatiivsus, gravitatsioon, statistiline füüsika, termodünaamika

Acknowledgements

I would like to thank first and foremost my supervisor Prof. Dominique Unruh who was always very supportive and helpful. I could always count on very informative and helpful discussions on any issues I faced. I would not have been able to finish this work without his help. I would also like to thank Prof. Marlon Dumas for giving me the idea of taking courses in cryptography. Thanks to this I found an area in computer science that I truly enjoy. I would also like to thank Ottar Tamm who has never failed to motivate me and support every choice I have made. Last but not least I would like to thank Skype and IT Academy for supporting me financially and therefore making my studies easier.

Contents

Introduction **7**

1 Mathematical preliminaries **13**
1.1 Vector space 13
1.2 Hilbert space 15
1.3 Operators 16
1.4 Norm 18

2 Quantum computing **19**
2.1 Background of quantum physics 19
2.1.1 Classical information 19
2.1.2 Probabilistic information 21
2.1.3 Quantum information 21
2.2 Quantum computing 22
2.2.1 Qubits 22
2.2.2 Measurements 24
2.2.3 Quantum circuits 26
2.3 Entanglement 26

3 Monogamy of entanglement games **28**
3.1 General setting 28
3.2 Original monogamy of entanglement game MG0 29
3.3 MG1 and MG2 games 30
3.4 MG3, MG4 and MG5 games 31
3.5 Concerns and assumptions for MG4 and MG5 33
3.5.1 First commutative property 33
3.5.2 Third commutative property 33
3.5.3 Second commutative property 34
3.6 MG6 and MG7 games 34
3.7 Progress on MG6 proof 36
3.7.1 Intuition 36

3.7.2 Steering game . . . 37
3.7.3 Application of steering game . . . 38
3.7.4 Implications . . . 40

4 Position verification **42**
4.1 Position verification . . . 42
4.1.1 Impossibility in classical setting . . . 42
4.1.2 Quantum setting . . . 43
4.2 Position verification with two receiving verifiers . . . 44
4.2.1 Proof sketch . . . 45
4.2.2 Size of the provers region . . . 48
4.3 Position verification with three receiving verifiers . . . 51
4.3.1 Proof sketch . . . 52

5 Full proof of position verification theorem with three receiving verifiers **58**
5.1 Definitions and Theorem statement . . . 58
5.2 Quantum circuit . . . 59
5.3 EPR pairs and reprogramming the random oracle . . . 61
5.4 Monogamy game . . . 64
5.5 Guessing x . . . 64

6 Conclusion **66**

Appendices **67**

A Proof of MG4 theorem **68**

B Another proof of MG7 theorem **73**

Bibliography **77**

Introduction

Position verification

Consider a situation where we wish to verify an entity solely by its location. This might be the case when we wish to provide services in a specific area, for example a sports stadium. Let us imagine that we have a sports stadium that wishes to stream replays of key moments of the game to spectators smartphones. Organisers are concerned that it is not possible to use passwords printed on the tickets as these might still be distributed outside of the stadium. Since it is crucial that no-one outside of the stadium is able to access this information they decided to verify the devices by their location.

The simplest way of achieving position verification is to place a device (the verifier) in the middle of the stadium. Let Victor take over the role of the verifier and let the time unit be such that light reaches the border of the stadium (i.e. the border of the provers region) at time $t = 1$. If Alice wishes to prove that she is indeed inside the stadium she starts the verification procedure. Victor sends a token x to Alice at time $t = 0$. Alice receives the token at time $t \leq 1$ and immediately sends the token back to Victor. Victor receives the token from Alice at time $t \leq 2$ and accepts. If Victor received the token back from Alice at time $t > 2$, then Victor would assume that Alice is too far away and would not accept.This kind of position verification is called distance bounding [1].

It is not always possible or desirable to have one verifier in the center of a spherical region. Another approach to position verification is to use multiple verifiers V_i $(i = 1, \ldots, r)$ that are placed around the provers region (i.e. the provers region is in the convex hull of the verifiers locations). Now let us consider the following protocol:

1. Let H be a function that takes r inputs. Verifiers V_i $(i = 1, \ldots, r)$ choose random bit-strings x_i.

2. At time $t = 0$ they send these bit-strings to the prover P°.

3. At time $t = 1$ prover receives all x_i and calculates $y = H(x_1, \ldots, x_r)$. He then sends y to all the verifiers.

4. At time $t = 2$ verifiers V_i each receive a bit-string y_i. They check if $y_i = H(x_i, \ldots, x_r)$ for all i. If this is true and the bit-strings indeed arrived on time they accept.

In a 2D world the position of the verifiers and the provers region might look as in Figure 1.

The most important property of a position verification protocol is soundness. We say that a protocol is sound for a region P if malicious provers outside of that region are not able to impersonate a honest prover inside the provers region. Unfortunately the protocol above cannot be secure in the classical setting. The impossibility of position verification in the classical setting was shown in [3].

The ability to keep a copy of the bit-string and forward copies of the bit-string to the other malicious provers is what makes it easy for multiple malicious provers to impersonate a honest prover. Since it is not possible to make copies of arbitrary quantum states there was hope that position verification might be possible in the quantum setting. It was shown in [2] that information-theoretically secure position verification protocols are not possible but it was shown in [2] and [3] that secure position verification protocols exist if we assume restrictions on the amount of allowed entanglement or provers storage capabilities. That secure position verification is possible in the random oracle model was shown in [9].

To show that position verification is possible in the random oracle model [9] introduced the following protocol

1. A random function $H : \{0,1\}^\ell \to \{0,1\}^n$ is chosen. Verifiers V_i pick random bit-strings x_i of length ℓ and a random bit-string $\hat{y}$ of length n.

2. Verifiers encode $\hat{y}$ in the basis $\theta = H(x_1 \oplus \cdots \oplus x_r)$ in the quantum state $|\Psi\rangle$. Verifiers V_1 sends $|\Psi\rangle$ to the prover.

3. At time $t = 0$ verifiers V_i send x_i to the prover P°.

4. At time $t = 1$ prover receives all x_i and calculates $\theta = H(x_1 \oplus \cdots \oplus x_r)$. He measures $|\Psi\rangle$ in the basis θ and gets the result y. He then sends y to verifiers V_1 and V_2.

5. At time $t = 2$ verifiers V_1 and V_2 receive y_1 and y_2. They check if $y_1 = y_2 = \hat{y}$. If yes, and y_1 and y_2 were indeed received on time they accept.

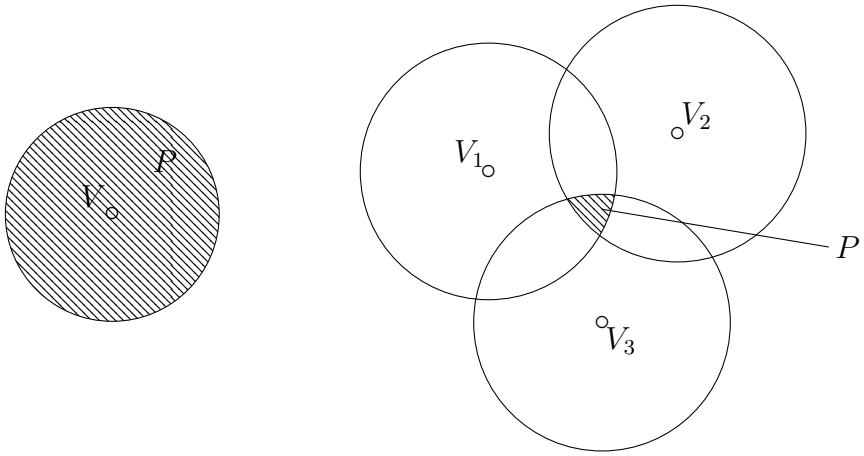


Figure 1: Location of verifiers and provers region for distance bounding vs. using multiple verifiers.

This protocol is sound for the region P, where all x_i are known and it is still possible for information to reach the verifiers V_1 and V_2. The region P is illustrated in Figure 2, where dotted lines show where x_i are known and solid lines show from where information can reach V_i.

Goal and contribution

A crucial point in the proof of the position verification theorem from [9] was taking advantage of the monogamy of quantum entanglement. Entanglement is a phenomenon where one quantum state cannot be described without describing another state that is entangled with it. As an important property entangled states influence each others measurements outcomes and can therefore be used to achieve the same measurement outcome on two systems without additional communication. Monogamy of entanglement means that if we have two parties Alice and Bob, that are fully entangled then Alice cannot be entangled with a third party Charlie. The monogamy game result form [6] stated that there is no strategy that lets Bob and Charlie always measure the same outcome as the referee Alice if the basis of Alice's measurement is revealed after Bob and Charlie agree on a common strategy.

Since the monogamy game theorem from [6] holds for two adversaries it could be used for the position verification theorem with two receiving verifiers. [9] listed it as an open problem if the result could be generalised to three receiving verifiers and if this could improve the precision of the protocol i.e. make the provers region smaller.

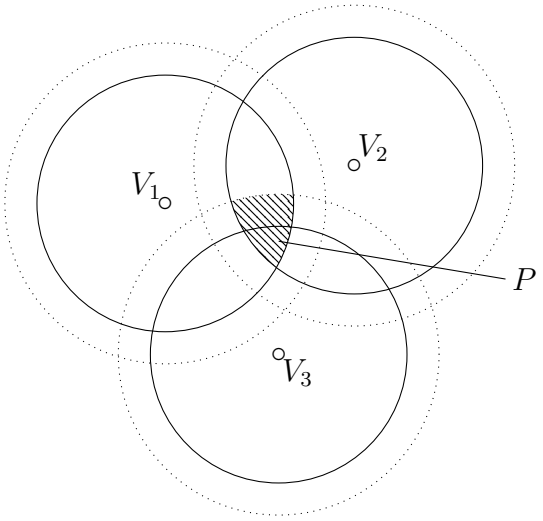


Figure 2: Provers region P. Intersection of spacetime at around time $t = 1$.

Goal of thesis

The goal of this thesis was to prove the soundness of the protocol with one added verifier and to define the monogamy game needed to prove the soundness of the new protocol. Under the assumption that the probability of winning this new monogamy game is indeed low we intended to give a proof for the soundness of the protocol and to show that it has indeed a higher precision.

Contribution

We investigate different three party monogamy games and prove that for multiple of these games the winning probability is negligible. We compare different 3 player games and discuss the different assumptions needed for the proofs.

We give a new protocol definition with an additional verifier, give a definition for the monogamy game needed so that the soundness of the protocol can be proven for a smaller provers region. We also give a formal proof for the position verification theorem with the new protocol that is dependent on the winning probability of the new monogamy game.

We also present our progress on the proof of the three-player monogamy game and explain the intuition behind the missing parts of the proof.

Open questions

We present current progress on the monogamy game theorem needed for the new position verification protocol. This proof is still an open problem. It is important to notice, that the current progress works in the one qubit case. We would like that the winning probability would decrease fast if the number of qubits grows, but it is not clear if this will be the case. If the probability will increase fast, then we can use the monogamy game theorem straight in the position verification proof. If the probability will not decrease fast with growing qubit numbers, then we would have to repeat the protocol itself. This would also result in the overall probability of malicious provers being able to impersonate a honest prover to be small, but the round complexity of the protocol would increase.

The position verification protocol in [9] allows an error rate. This is important as sending quantum states is not error free. For this the monogamy game has to be generalised to allow error rates as the monogamy game form [6] does.

We investigated the case where we added an additional receiving verifier to the protocol. It is important to notice, that three receiving verifiers is not the optimal case. In 3D four receiving verifiers will result in the highest precision. Adding an additional verifier should be possible in a similar manner as adding the third verifier. This means that the three party monogamy game has to be generalised to four parties. This was out of the scope of this thesis, but it seems that if the proof for the new monogamy game theorem works out as described it should be generalisable to four parties.

Thesis structure

The first chapter explains mathematical preliminaries. We present important well known definitions and some important known results without proof. This chapter is mainly meant for readers that lack mathematical background but would like to understand the proofs in detail.

Second chapter explains background in quantum information. We will discuss the differences of classical and quantum information. We will also briefly explain quantum states, measurements and entanglement. This chapter serves as mathematical background for readers who wish to look up mathematical definition used in other chapters.

Third chapter explains the monogamy game theorem from [6] and discusses different possibilities to generalise the monogamy game theorem to

more adversaries. We prove multiple versions of generalised monogamy theorems and explain the intuition behind the monogamy game theorem needed for the position verification proof. Unfortunately we were not yet able to prove this theorem.

In Chapter 4 we explain how position verification works. We also give a proof sketch for the position verification theorem from [9] and a proof sketch for a position verification theorem with 3 receiving verifiers. The proof sketches underline which parts of the proof had to be changed to accommodate an additional verifier and how we obtain a smaller provers region.

Chapter 5 gives a formal proof for the new position verification theorem and the last chapter gives a conclusion.

1. Mathematical preliminaries

Before introducing the quantum mechanical concepts used in this thesis we will will introduce some of the mathematical background needed. We will introduce frequently used definitions and some known results without proof.

1.1 Vector space

A nonempty set V with relations

$$+ : V \times V \to V$$

and

$$\cdot : \mathbb{C} \times V \to V$$

is called a complex vector space, if $\forall x, y, z \in V$ and $a, b \in \mathbb{C}$

$$\begin{aligned}
&x + (y + z) = (x + y) + z \\
&x + y = y + x \\
&\exists \mathbf{0} \in V : x + \mathbf{0} = x \\
&\exists - x \in V : x + (-x) = \mathbf{0} \\
&a \cdot (b \cdot x) = (ab) \cdot x \\
&1 \cdot x = x \\
&a \cdot (x + y) = a \cdot x + a \cdot y \\
&(a + b) \cdot x = a \cdot x + b \cdot x
\end{aligned}$$

In the following by ax we denote the scalar product $a \cdot x$. A basis of a vector space V is a set of elements $\{v_i\}$, $v_i \in V$ such that every element x of V can be represented as a combination of the basis elements i.e. there are elements $a_i \in \mathbb{C}$ such that

$$\sum_i a_i v_i = x.$$

We say that a vector space is n dimensional , if its basis has n elements. It is important to notice that a vector space can have multiple bases, but they all contain the same number of elements. It is also well known that every finite dimensional vector space has a basis. In the following we will only work with finite dimensional vector spaces.

Let x be an element of an n-dimensional vector space V and let $\{v_0, \ldots, v_n\}$ be a basis of V. This means, that there are elements $a_i \in \mathbb{C}$, such that $\sum_i a_i v_i = x$. Since a_i uniquely define x we can represent the vector space element (vector) x as

$$x = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_n \end{pmatrix}.$$

The conjugate transpose of the vector x is given by

$$x^\dagger = \begin{pmatrix} \overline{a_0} & \overline{a_1} & \cdots & \overline{a_n} \end{pmatrix},$$

where $\overline{x}$ denotes the complex conjugate of x. I.e. if $x = a+bi$, where $a, b \in \mathbb{R}$, then $\overline{x} = a - bi$. We can now define the inner product $\langle x, y \rangle$ of two vectors x and y by

$$\langle x, y \rangle = x^\dagger y,$$

Notice that the inner product of two vectors is not a vector, but a complex number.

In the following are some properties of the inner product. Let x, y, z be vectors and a, b complex numbers, then

$$\begin{aligned} &\langle x, y \rangle = \overline{\langle x, y \rangle} \\ &\langle ax + bz, y \rangle = a\langle x, y \rangle + b\langle z, y \rangle \\ &\langle x, x \rangle \geq 0. \end{aligned}$$

A norm $\|\cdot\|$ is a function on a vector space V

$$\|\cdot\| : V \to \mathbb{R},$$

with following properties. For every $x, y \in V$ and $a \in \mathbb{C}$

$$\begin{aligned} &\|ax\| = |a| \cdot \|x\| \\ &\|x + y\| \leq \|x\| + \|y\| \\ &\|x\| = 0 \Rightarrow x = \mathbf{0}. \end{aligned}$$

Notice that $\|x\| = \sqrt{\langle x, x\rangle}$ is a valid norm on any vector space with an inner product.

Using the norm we can also define a distance measure $d(x, y)$ as $d(x, y) = \|x - y\|$. We call a set M a metric space if we can calculate the distance $d(x, y)$ for every element $x, y \in M$. We say that a metric space is complete if every Cauchy sequence has a limit, that is also in M. This basically means, that if we have a sequence that converges, for example

$$1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \cdots, \frac{1}{n}$$

then the limit 0 also has to belong to the set. To complete the example, the set $(0, 1]$ is not complete, as the limit of the sequence given above is outside of the set.

1.2 Hilbert space

We are now able to define Hilbert spaces.

Definition 1.1. A vector space $\mathcal{H}$ with inner product $\langle \cdot, \cdot \rangle$ is called a Hilbert space if the norm induced by the inner product

$$\|x\| = \sqrt{\langle x, x\rangle}$$

turns the vector space into a complete metric space.

Let A and B be two matrices, such that

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ a_{21} & \cdots & a_{2n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}, B = \begin{pmatrix} b_{11} & \cdots & b_{1n} \\ b_{21} & \cdots & b_{2n} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix}.$$

Then the tensor product $A \otimes B$ of A and B is given as

$$A \otimes B = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ a_{21}B & \cdots & a_{2n}B \\ \vdots & & \vdots \\ a_{n1}B & \cdots & a_{nn}B \end{pmatrix}$$

This means, that if we have vectors x and y in a Hilbert space $\mathcal{H}$, such that

$$x = \begin{pmatrix} x_1 \\ x_2 \\ \cdots \\ x_n \end{pmatrix}, y = \begin{pmatrix} y_1 \\ y_2 \\ \cdots \\ y_n \end{pmatrix},$$

then the tensor product $x \otimes y$ is given by

$$x \otimes y = \begin{pmatrix} x_1 y_1 \\ x_1 y_2 \\ \vdots \\ x_1 y_n \\ x_2 y_1 \\ \vdots \\ x_2 y_n \\ \vdots \\ x_n y_n \end{pmatrix}$$

We can also calculate the tensor product of two Hilber spaces $\mathcal{H}_1$ and $\mathcal{H}_2$. The tensor product $\mathcal{H} = \mathcal{H}_1 \otimes \mathcal{H}_2$ is then equal to

$$\{x \otimes y | x \in \mathcal{H}_1 \text{ and } y \in \mathcal{H}_2\}.$$

Notice that $\mathcal{H}$ is again a Hilbert space. If $\{v_1, \ldots, v_n\}$ is the basis of the n-dimensional Hilbert space $\mathcal{H}_1$ and $\{u_1, \ldots, u_m\}$ is the basis of the m-dimensional Hilbert space $\mathcal{H}_2$, then the basis of H is

$$\{v_1 u_1, v_1 u_2, \ldots, v_1 u_m, v_2 u_1, \ldots, v_n u_m\}.$$

This means that $\mathcal{H}$ is nm-dimensional.

1.3 Operators

Let $\mathcal{H}$ be a Hilbert space. A transformation $O : \mathcal{H} \to \mathcal{H}$ is called linear if it preserves both addition and scalar multiplication. This means that for every $x, y \in \mathcal{H}$ and $a \in \mathbb{C}$

$$\begin{aligned} O(x + y) &= O(x) + O(y) \\ O(ax) &= aO(x). \end{aligned}$$

We call these transformations operators on $\mathcal{H}$. It is important to notice that if we agree on a basis for the n-dimensional Hilbert space $\mathcal{H}$, then there is a one-to-one correspondence between operators on $\mathcal{H}$ and $n \times n$ matrixes. Therefore we will mostly use the matrix notation for operators if we have a fixed basis.

In the following we will recall some special types of operators. Let $\mathcal{H}$ be an n-dimensional Hilbert space and let the basis be fixed, such that all

operators can be represented by $n \times n$ matrices. We denote by $1_{\mathcal{H}}$ the identity operator on $\mathcal{H}$. This operator is such that for every vector $x \in \mathcal{H}$

$$1_{\mathcal{H}} x = x.$$

Definition 1.2. An operator P, that satisfies $PP = P$ is called a projector.

Definition 1.3. An operator P is called positive semi-definite, if for every vector x

$$x^\dagger P x \geq 0.$$

Lemma 1.1. *For any matrix C the matrix $C^\dagger C$ is positive semi-definite, where if $C = \{a_{ij}\}$, $C^\dagger = \{\overline{a_{ji}}\}$.*

Definition 1.4. We say that an operator H is hermitian if $H = H^\dagger$.

Definition 1.5. We say that an operator U is unitary if $UU^\dagger = 1_{\mathcal{H}}$, where $1_{\mathcal{H}}$ is the identity operator.

When we analyse operators then we often want to know which vectors they do not affect. These vectors are called eigenvectors. Let O be an operator. If

$$Ox = ax$$

for some vector $x \in \mathcal{H}$ and $a \in \mathbb{C}$, then x is called an eigenvector of O and a is called an eigenvalue of O.

Another important property of an operator is the trace. Let $O = \{o_{ij}\}$ be an operator, then

$$\mathrm{Tr}(O) = \sum_i o_{ii}.$$

The trace of an operator is cyclic. This means that if we have operators A, B and C, then $\mathrm{Tr}(ABC) = \mathrm{Tr}(CAB)$. Trace is also additive i.e. $\mathrm{Tr}(A + B) = \mathrm{Tr}(A) + \mathrm{Tr}(B)$ and preserves the scalar product: $\mathrm{Tr}(aA) = a\,\mathrm{Tr}(A)$, whrere $a \in \mathbb{C}$.

Definition 1.6. The Hadamard operator H is given by

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

1.4 Norm

In section 1.1 we encountered the vector norm induced by the inner product. We will now introduce a norm for operators. Let A be an operator on the Hilbert space $\mathcal{H}$ then the usual operator norm is given by

$$\|A\| = \inf\{c \geq 0 \quad | \quad \|Av\| \leq c\|v\| \text{ for all } v \in \mathcal{H}\}.$$

This norm is also called the Schatten ∞-norm.

We say that $A \geq B$ if $A - B$ is a positive semi-definite operator.

Lemma 1.2. *[6] Let A_1, A_2, ..., A_n be positive semi-definite projectors, and let $\{\pi^k\}_{k\in[n]}$ be a set of n mutually orthogonal permutations of $[n]$. Then*

$$\left|\left|\sum_{i\in[n]} A_i\right|\right| \leq \sum_{k\in[n]} \max \left|\left|A_i A_{\pi^k(i)}\right|\right|.$$

2. Quantum computing

In this chapter we will discuss what quantum information is and why we need it, what are the alternatives and what are the differences between quantum information and other types of information. A good introduction to quantum information is given in [8] another nice introduction in relation to quantum cryptography is given in [5].

2.1 Background of quantum physics

Let us consider an experiment given in [4]. The setting consists of a photon source, two beam splitters, two photon detectors and two mirrors. The photon source sends single photons onto the beam splitter. The beam splitter is located at such an angle that half of the photons are sent through the beam splitter and half of the photons are reflected upwards. In both directions photons hit a mirror and are reflected at 45 degrees. Both of the streams of photons now meet and hit a beam splitter at 45 degrees from opposite sides. Photon detectors are located so that they can register from which side of the beam splitter photons come from. See Figure 2.1 for a graphical description.

A beam splitter can be considered as flipping a coin and then reflecting or letting a photon through randomly. Measurement statistics for this experiment show that all photons arrive at photon detector B.

In the following we will discuss the result of the experience and see how it can be can be described in different models of information. The 0 and 1 paths are shown in Figure 2.2. The beam splitter can be seen as an operator that flips the bit with probability $\frac{1}{2}$. The starting state, as seen in Figure 2.2, is 0.

2.1.1 Classical information

Classical information is modelled as a bit. The value of a bit can be either 0 or 1. Almost everything that computers do today is translated into 0-s and 1-s.

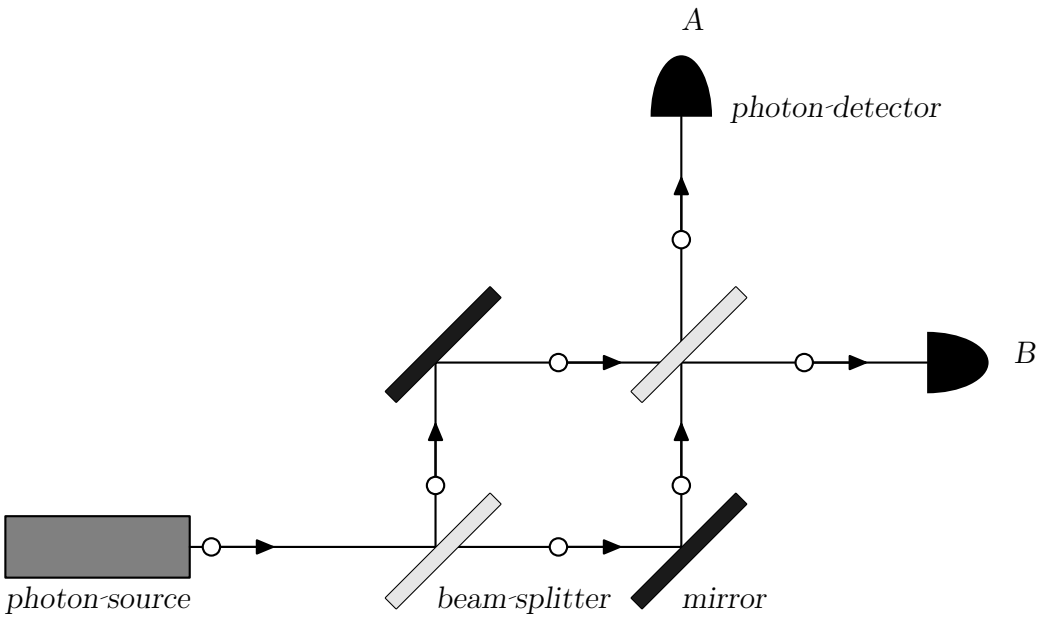
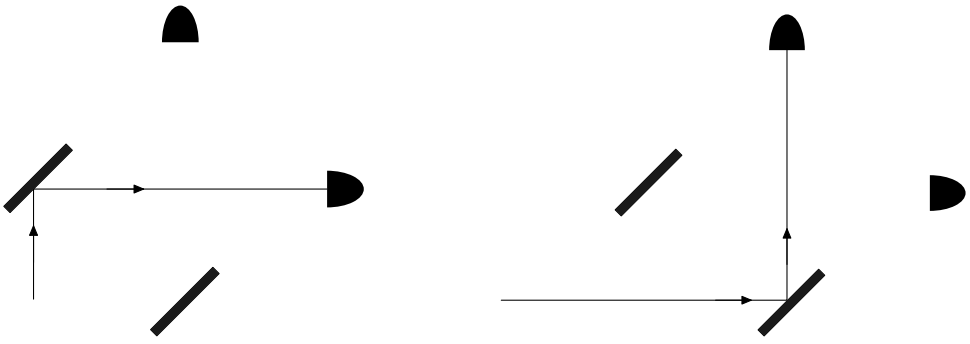


Figure 2.1: Setup of experiment. Figure reproduced from [4].



(a) The 1 path **(b)** The 0 path

Figure 2.2: Paths for 0 and 1. Figures reproduced from [4].

The starting state is 0. The beam splitter flips the bit with probability $\frac{1}{2}$, which means that with probability $\frac{1}{2}$ the state is equal to 0 and with probability $\frac{1}{2}$ equal to 1. We cannot represent this state with just 0 and 1. To include the probabilities we need a more complex state description than 0 and 1.

2.1.2 Probabilistic information

A probabilistic bit is given by $s = p_0 \cdot \mathbf{0} + p_1 \cdot \mathbf{1}$, where p_0 and p_1 are the probabilities of the value of s being 0 and 1 respectively. This means $p_0 + p_1 = 1$ and $p_0, p_1 \geq 0$. These probabilistic bits lie on the line between zero and one. This means that after the beam splitter the state is equal to $\frac{1}{2} \cdot \mathbf{0} + \frac{1}{2} \cdot \mathbf{1}$. Applying the second beamsplitter will result in

$$\frac{1}{2}\left(\frac{1}{2} \cdot \mathbf{0} + \frac{1}{2} \cdot \mathbf{1}\right) + \frac{1}{2}\left(\frac{1}{2} \cdot \mathbf{0} + \frac{1}{2} \cdot \mathbf{1}\right) = \frac{1}{2} \cdot \mathbf{0} + \frac{1}{2} \cdot \mathbf{1} \neq \mathbf{0}.$$

This means that the result does not coincide with the result of the experiment.

2.1.3 Quantum information

Quantum information is similar to probabilistic information, but the qubit (quantum bit) does not lie on the line between zero and one. It lies on the surface of the sphere, whose north pole lies on 1 and south pole on 0. In the following we will follow [4] to describe the experiment in the quantum information setting. Let $\begin{pmatrix}1\\0\end{pmatrix}$ be the $\mathbf{0}$ state and $\begin{pmatrix}0\\1\end{pmatrix}$ the $\mathbf{1}$ state. A quantum state is given by

$$\alpha \begin{pmatrix}1\\0\end{pmatrix} + \beta \begin{pmatrix}0\\1\end{pmatrix},$$

where α and β are complex numbers. The probability of measuring 0 is equal to $|\alpha|^2$ and the probability of measuring 1 is equal to $|\beta|^2$. Since these probabilities should add up to 1, we have $|\alpha|^2 + |\beta|^2 = 1$.

In this setting the beam splitter can be modelled by multiplying the quantum state with the matrix

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

The state is equal to **0** in the beginning. After passing the beam splitter the state is equal to

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\end{pmatrix} + \frac{i}{\sqrt{2}}\begin{pmatrix}0\\1\end{pmatrix}.$$

This means that the state is a superposition of **0** and **1**. If we were to measure the state after the beam splitter the result would be **0** with probability $|\frac{1}{\sqrt{2}}|^2 = \frac{1}{2}$ and the result would be **1** with probability $|\frac{i}{\sqrt{2}}|^2 = \frac{1}{2}$.

If we do not measure the state before the second beam spitter, the state after the second beam splitter would be

$$\frac{1}{\sqrt{2}}\begin{pmatrix}1 & i\\ i & 1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix} = \begin{pmatrix}0\\i\end{pmatrix} = 0\begin{pmatrix}1\\0\end{pmatrix} + i\begin{pmatrix}0\\1\end{pmatrix}.$$

Now the probability of measuring **0** is $|0|^2 = 0$ and the probability of measuring **1** is $|i|^2 = 1$. This corresponds with the experimental result that all photons are measured by the B photon detector.

In the given experiment information was "encoded" as paths of the photons, but there are other ways to encode quantum information as well. Quantum information can, for example, be encodes as the spin of an electron or polarisation of a photon. In the following we will not concern us with the exact physical representation, but will concentrate on the mathematical abstraction.

2.2 Quantum computing

In the following we will discuss the mathematics of quantum computing.

2.2.1 Qubits

As discussed in the previous section a qubit is represented as

$$\alpha\begin{pmatrix}1\\0\end{pmatrix} + \beta\begin{pmatrix}0\\1\end{pmatrix}.$$

In the following we will use a different notation, the Dirac or bra-ket notation, where

$$\begin{pmatrix}1\\0\end{pmatrix} =: |0\rangle \quad \text{and} \quad \begin{pmatrix}0\\1\end{pmatrix} =: |1\rangle.$$

This means that we can write any qubit as

$$\alpha|0\rangle + \beta|1\rangle,$$

where $|\alpha|^2 + |\beta|^2 = 1$.

In the bra-ket notation $|\cdot\rangle$ is called a ket, $\langle\cdot|$ is called a bra and $\langle\cdot|\cdot\rangle$ is called a bracket. Here $\langle s|$ denotes the conjugate transpose of quantum state $|s\rangle$. Hence $\langle s|t\rangle$ is the inner product of quantum states $|s\rangle$ and $|t\rangle$. Which means we can write the norm of the quantum state as $\||s\rangle\| = \sqrt{\langle s|s\rangle}$.

When we talk about quantum states we assume a Hilbert space $\mathcal{H}$, then a quantum state $|s\rangle$ is an element of $\mathcal{H}$. In the following we will always assume that Hilbert spaces are finite dimensional. This means that the given Hilbert space has a basis. Let us assume that the given Hilbert space is n dimensional, then one suitable basis is

$$n \left\{ \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \cdots, \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} . \right.$$

In the following we will see how this can be expressed in the bra-ket notation. For this we will calculate tensor products between $|0\rangle$ and $|1\rangle$

$$|00\rangle = |0\rangle \otimes |0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

$$|01\rangle = |0\rangle \otimes |1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}$$

$$|10\rangle = |1\rangle \otimes |0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

$$|11\rangle = |1\rangle \otimes |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \otimes \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}$$

This means that if we have a Hilbert space with dimension 2^n, then a basis of the Hilbert space is given by

$$|0\cdots000\rangle, |0\cdots001\rangle, |0\cdots010\rangle, |0\cdots011\rangle, \ldots, |1\cdots111\rangle$$

Definition 2.1. A density matrix ρ is an $n \times n$ matrix with unit trace that is Hermitian and positive semi-definite.

The density matrix of a quantum state $|s\rangle$ is $|s\rangle\langle s|$. It is important to notice that not all density matrices are of the form $|s\rangle\langle s|$. Quantum states whose density matrices are of the form $|s\rangle\langle s|$ are called pure states i.e. they can be written as $|s\rangle$.

There are also more general quantum states, whose density matrices cannot be written as the outer product of a pure state. These states are called mixed and they are a statical ensemble of different states. We can purify any mixed quantum state ρ in Hilbert space $\mathcal{H}$ by taking a big enough extension $\bar{\mathcal{H}}$ of the Hilbert space $\mathcal{H}$ [8]. Let $\bar{\mathcal{H}} = \mathcal{H} \otimes \mathcal{H}_{\mathcal{R}}$, then there is a pure state $|s\rangle$, such that

$$\mathrm{Tr}_R(|s\rangle\langle s|) = \rho.$$

Where Tr_R is the partial trace over $\mathcal{H}_{\mathcal{R}}$. This is also called tracing out the system $\mathcal{H}_R$.

2.2.2 Measurements

We will now explain the mathematics behind quantum measurements.

Definition 2.2. A projective measurement is a set of projectors $\{P_i\}$, where P_i are projectors that sum to the identity operator i.e. $\sum_i P_i = 1_{\mathcal{H}}$.

Let $\mathcal{H} = \mathbb{C}^2$ and let $|s\rangle \in \mathcal{H}$. The quantum state $|s\rangle$ can be written as $|s\rangle = \alpha|0\rangle + \beta|1\rangle$, where $|\alpha|^2 + |\beta|^2 = 1$. We want to measure if the sate $|s\rangle$ is $|0\rangle$ or $|1\rangle$. Such a measurement is given by $\{P_0, P_1\}$, where $P_0 = |0\rangle\langle 0|$ and $P_1 = |1\rangle\langle 1|$. We can calculate the probability of measuring $|0\rangle$ by

$$\begin{aligned}\langle s|P_0|s\rangle &= \left(\bar{\alpha}\langle 0| + \bar{\beta}\langle 1|\right)|0\rangle\langle 0|\left(\alpha|0\rangle + \beta|1\rangle\right) \\ &= \left(\bar{\alpha}\langle 0|0\rangle + \bar{\beta}\langle 1|0\rangle\right)\left(\alpha\langle 0|0\rangle + \beta\langle 0|1\rangle\right)\end{aligned}$$

Since $\langle 0|1\rangle = \langle 1|0\rangle = 0$ and $\langle 0|0\rangle = \langle 1|1\rangle = 1$ we have

$$\langle s|P_0|s\rangle = \bar{\alpha}\alpha = |\alpha|^2.$$

And analogously

$$\langle s|P_1|s\rangle = \bar{\beta}\beta = |\beta|^2.$$

We see that the outcomes are as expected.

In a general case, when we are given a measurement $\{P_i\}$, then the probability of measuring i on a quantum state $|s\rangle$ is

$$Pr[\text{"Measurement outcome is } i\text{"}] = \langle s|P_i|s\rangle.$$

Measurements on classical systems would be mere observations. Measurements on a quantum system on the other hand disturb states. If the measurement outcome is i, then $|s\rangle$ will be in state

$$\frac{P_i|s\rangle}{\sqrt{\langle s|P_i|s\rangle}}$$

after the measurement. This means that if we perform the $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ measurement on the state $|s\rangle = \alpha|0\rangle + \beta|1\rangle$ and the outcome is $|0\rangle$, then $|s\rangle$ will be in state $|0\rangle$ after the measurement. We say that the measurement collapses the state $|s\rangle$.

We can also perform projective measurements on mixed states. Let ρ be a mixed quantum state. In this case the probability of measuring i is

$$\mathrm{Tr}(P_i\rho).$$

One important property of projective measurements is that they are repeatable, since $P_iP_j = \delta_{ij}P_i$. More general measurements that are not repeatable exist as well.

Definition 2.3. Positive operator valued measure (POVM) is a measurement on an n dimensional Hilbert space is a set of k operators $\{E_k\}$ such that

$$\sum_i E_i = 1_{\mathcal{H}} \quad \text{and} \quad \forall i \quad E_i = E_i^\dagger, \quad E_i \geq 0.$$

Given a specific situation we sometimes like to measure a state in a certain basis for example in the computational or Hadamard basis. We say that we measure a qubit in the computational basis, if we perform the measurement $\{|0\rangle\langle 0|, |1\rangle\langle 1|\}$ and we say that we measure in the Hadamard basis if we perform the measurement $\{H^\dagger|0\rangle\langle 0|H, H^\dagger|1\rangle\langle 1|H\}$, where $H = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the Hadamard matrix. This means that for the Hadamard basis the basis vectors are $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

An interesting aspect about these bases is that if we measure $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ in the computational basis, the probability for both outcomes is $\frac{1}{2}$. And if we measure $|0\rangle$ and $|1\rangle$ in the Hadamard basis, the probability for both outcomes is again $\frac{1}{2}$. This means that if we do not know

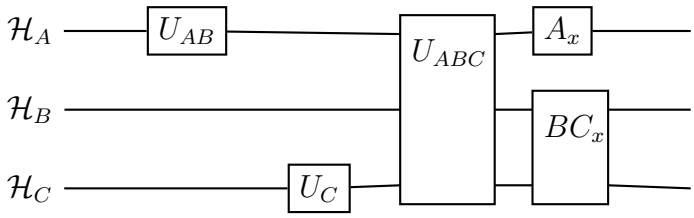


Figure 2.3: Example of a quantum circuit

in which of the two basis information is encoded, we cannot measure this information with certainty.

If we look at an 2^n-dimensional Hilbert space $\mathcal{H} = \underbrace{\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2}_{n}$ we can define what it means to measure in the basis $\theta \in \{0,1\}^n$.

Definition 2.4. We say that we measure in basis $\theta \in \{0,1\}^n$ if we perform the measurement $\{|x^\theta\rangle\langle x^\theta|\}_{x\in\{0,1\}^n}$, where

$$x^\theta = H^{\theta_1}x_1 \otimes H^{\theta_1}x_2 \otimes \cdots \otimes H^{\theta_n}x_n$$

2.2.3 Quantum circuits

In the following when we talk about measurements and other operators on quantum states we will often illustrate them with images that show quantum circuits. A quantum circuit consists of wires, quantum gates and measurements. Quantum gates are always reversible and therefore correspond to unitary operators. Quantum measurements are not reversible and they have two outputs, a classical output for the measurement outcome and a quantum output for the quantum state after the measurement.

Quantum wires can be seen as the tensor product presentation of a Hilbert space. This means that if we perform operations on a Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$ with unitary operators U_{AB}, U_C, U_{ABC} acting on $\mathcal{H}_A \otimes \mathcal{H}_B$, $\mathcal{H}_C$ and $\mathcal{H}$ respectively, and measurements $\{A_x\}$ and $\{BC_x\}$ acting on $\mathcal{H}_A$ and $\mathcal{H}_B \otimes \mathcal{H}_C$ respectively, we can represent this as a quantum circuit shown in Figure 2.3.

2.3 Entanglement

Entanglement is an interesting property of quantum states. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be Hilbert spaces.

Definition 2.5. We say that the quantum state $|s\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ is entangled, if it cannot be written as

$$|s\rangle = |s_a\rangle \otimes |s_b\rangle,$$

where $|s_a\rangle \in \mathcal{H}_A$ and $|s_b\rangle \in \mathcal{H}_B$.

Four famous entangled states are the EPR pairs:

$$\begin{aligned}
|\beta_{00}\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right), \\
|\beta_{01}\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right), \\
|\beta_{10}\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right), \\
|\beta_{01}\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right).
\end{aligned}$$

We will now see what happens if we measure the first qubit of the first EPR pair in the computational basis. This means that we will perform the measurement $\{|0\rangle\langle 0| \otimes 1, |1\rangle\langle 1| \otimes 1\}$. The probability of measuring $|0\rangle$ is

$$\begin{aligned}
\langle\beta_{00}| \left(|0\rangle\langle 0| \otimes 1\right) |\beta_{00}\rangle &= \left(\frac{1}{\sqrt{2}}\left(\langle 00| + \langle 11|\right)\right)\left(|0\rangle\langle 0| \otimes 1\right)\right)\left(\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)\right) \\
&= \frac{1}{2}\Big(\langle 0|0\rangle\langle 0| + \langle 1|0\rangle\langle 1|\Big)\Big(\langle 0|0\rangle|0\rangle + \langle 0|1\rangle|1\rangle\Big) \\
&= \frac{1}{2}\langle 0|0\rangle = \frac{1}{2}.
\end{aligned}$$

Since probabilities add up to 1, then the probability of measuring $|1\rangle$ on the first qubit is $\frac{1}{2}$ as well. The state of the EPR pair after measuring the first qubit, given that the measurment outcome was $|0\rangle$, is

$$\sqrt{2}\left(|0\rangle\langle 0| \otimes 1\right)\left(\frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)\right) = \left(|0\rangle\langle 0|0\rangle|0\rangle + |0\rangle\langle 0|1\rangle|1\rangle\right) = |00\rangle.$$

Now if we measure the second qubit in the computational basis the result is $|0\rangle$ with probability 1. We get the same result if we measure in the Hadamard basis. This means that the measurement on one half of the system determines the result on the other half of the system. The measurement outcomes on β_{00} and β_{10} are always correlated and the measurement outcomes on $\beta 01$ and β_{11} are always anticorrelated.

An important property about entanglement is that it is monogamous. If states ρ and ψ are fully entangled, then state ψ cannot be fully entangled with a third state ϕ. We discuss monogamy of entanglement in the next chapter.

3. Monogamy of entanglement games

In this chapter we introduce different three-player monogamy of entanglement games.

3.1 General setting

In the following we will always assume, that $\mathcal{H}_A$, $\mathcal{H}_B$, $\mathcal{H}_C$ and $\mathcal{H}_F$ are Hilbert spaces. Moreover Alice, Bob and Charlie are adversaries that have access to spaces $\mathcal{H}_A$, $\mathcal{H}_B$ and $\mathcal{H}_C$ respectively. The referee has access to the Hilbert space $\mathcal{H}_F$.

Monogamy of entanglement games will consist of a referee and adversaries. Before the game starts adversaries agree on a strategy of how to measure their spaces once the basis is revealed and choose a starting state of their liking that is then distributed to the referee and adversaries. Then the referee chooses a uniformly random basis and reveals it to the adversaries. Adversaries and referee perform measurements on their parts of the space and output values y_A, y_B (in case we have two adversaries A, B) and y_F. If $y_A = y_B = y_F$ adversaries win the game.

We will define game and strategy specifically in the following.

Definition 3.1. A monogamy of entanglement game $G = \{\mathcal{H}_F, \{F_x^\theta\}\}$ consists of a Hilbert space $\mathcal{H}_F$ and a set of projective measurements $\{F_x^\theta\}$ on this space.

In the following we will assume that $\{F_x^\theta\}$ is a measurement in basis θ. We will distinguish different monogamy of entanglement games by the strategies allowed by the game. In the following we will introduce the monogamy of entanglement game defined and analysed in [6].

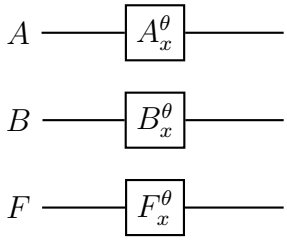


Figure 3.1: MG0

3.2 Original monogamy of entanglement game MG0

Definition 3.2. By MG0 we denote a monogamy of entanglement game where the allowed strategies are of the form $S = \{|s\rangle, \{A_x^\theta\}, \{B_x^\theta\}\}$, where $|s\rangle$ is the starting state and $\{A_x^\theta\}$ and $\{B_x^\theta\}$ are projective measurements on $\mathcal{H}_A$ and $\mathcal{H}_B$ respectively. By MG0^n we denote an MG0 game where $\{F_x^\theta\}$ is a measurement on an $n-$qubit state.

The quantum circuit corresponding to a MG0 strategy is shown in Figure 3.1.

Definition 3.3. By $P_{win}(G, S)$ we denote the probability that adversaries with strategy S win the game G.

Definition 3.4. The maximal winning probability of a monogamy of entanglement game is given by $P_{win}(G) = \sup_S(P_{win}(G, S))$, where supremum is taken over all allowed strategies S.

It is important to notice that although we consider projective measurements and pure starting states these results hold as well for more general measurements POVM-s and mixed states. Namely any POVM can be represented as a projective measurement if we consider Hilbert spaces with more dimensions. The same holds for pure and mixed quantum states. [6]

In [6] it was shown that $P_{win}(\text{MG0}^n) = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n$. Here the optimal strategy is that both Alice and Bob guess 0 independent of the basis and choose $|s\rangle = |s_0\rangle \otimes \ldots \otimes |s_n\rangle$, where $s_i = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$. It is easy to see

that then

$$\begin{aligned}
P_{win}(\mathrm{MG0}^n, S) &= \sum_{\theta\in\Theta} \frac{1}{|\Theta|}\langle s|F_0^\theta|s\rangle \\
&= \sum_{\theta\in\Theta} \frac{1}{|\Theta|}\langle s| \left(|0^{\theta_0}\rangle\langle 0^{\theta_0}| \otimes \ldots \otimes |0^{\theta_n}\rangle\langle 0^{\theta_n}|\right)|s\rangle \\
&= \sum_{\theta\in\Theta} \frac{1}{|\Theta|}\langle s_0|0^{\theta_0}\rangle\langle 0^{\theta_0}|s_0\rangle \otimes \ldots \otimes \langle s_n|0^{\theta_n}\rangle\langle 0^{\theta_n}|s_n\rangle \\
&= \sum_{\theta\in\Theta} \frac{1}{|\Theta|}\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n \\
&= \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n.
\end{aligned}$$

Here we use that

$$\langle s_i|0\rangle\langle 0|s_i\rangle = \left(\cos\frac{\pi}{8}\right)^2 = \frac{1}{2} + \frac{1}{2\sqrt{2}}$$

and

$$\begin{aligned}
\langle s_i|H|0\rangle\langle 0|H|s_i\rangle &= \frac{1}{2}\left(\cos^2\frac{\pi}{8} + \cos\frac{\pi}{8}\sin\frac{\pi}{8} + \cos\frac{\pi}{8}\sin\frac{\pi}{8} + \sin^2\frac{\pi}{8}\right) \\
&= \frac{1}{2} + \frac{1}{2\sqrt{2}}.
\end{aligned}$$

The monogamy game MG0 works with two adversaries. In the following sections we are analysing monogamy of entanglement games that allow more adversaries. We also consider games that allow unitary transformations on shared registers that are performed before the measurements and in some cases measurements that are performed on multiple registers at the same time.

3.3 MG1 and MG2 games

Definition 3.5. By MG1 we denote a monogamy of entanglement game that accepts strategies of the form $S = \{|s\rangle, \{A_x^\theta\}, \{B_x^\theta\}, \{C_x^\theta\}\}$, where $\{A_x^\theta\}$, $\{B_x^\theta\}$ and $\{C_x^\theta\}$ are projective measurements on $\mathcal{H}_A$, $\mathcal{H}_B$ and $\mathcal{H}_C$ respectively.

A diagram of MG1 is given in Figure 3.2.

It is evident that MG1 is a special case of MG0, therefore $P_{win}(\mathrm{MG1}) \leq P_{win}(\mathrm{MG0})$. Furthermore the optimal strategy given for MG0 in the beginning of this chapter is a valid strategy for MG1 as well. The third adversary will guess 0 as do the other adversaries. Therefore $P_{win}(\mathrm{MG1}) = P_{win}(\mathrm{MG0})$.

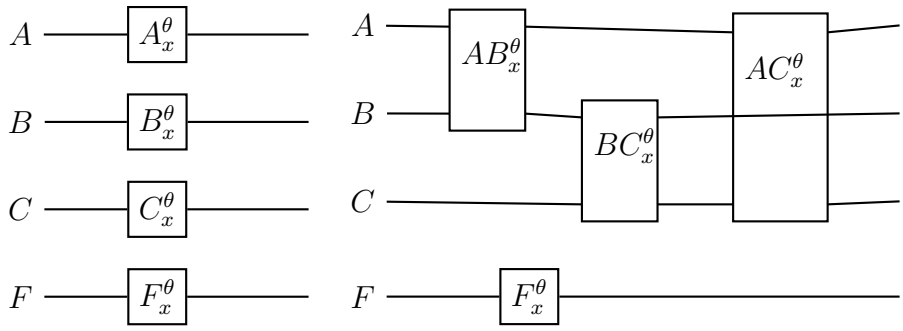


Figure 3.2: MG1 and MG2

We will now introduce another monogamy of entanglement game that allows measurements on overlapping spaces.

Definition 3.6. By MG2 we denote a monogamy of entanglement game that accepts strategies of the form $S = \{|s\rangle, \{AB_x^\theta\}, \{BC_x^\theta\}, \{AC_x^\theta\}\}$, where $\{AB_x^\theta\}$, $\{BC_x^\theta\}$ and $\{AC_x^\theta\}$ are projective measurements on $\mathcal{H}_A \otimes \mathcal{H}_B$, $\mathcal{H}_B \otimes \mathcal{H}_C$ and $\mathcal{H}_A \otimes \mathcal{H}_C$ respectively.

A diagram of MG2 is given in Figure 3.2.

Theorem 3.1. $P_{win}(MG2^n) = 1$.

Proof. Consider the strategy shown in Figure 3.3. Here one of the adversaries shares a fully entangled state with the referee and measures the state in the same basis as the referee does. This guarantees that the results of the adversary and the referee are identical. Now the first adversary can communicate the measurement outcome to the next adversary by preparing a state containing the same information in the given basis and outputting the state on the next wire. The second referee does the same. This guarantees a win. □

To prevent adversaries from communicating with each other directly, we can assume that for a given basis θ the measurements will have to commute.

In the following we will consider different restrictions on the measurements $\{AB_x^\theta\}$, $\{BC_x^\theta\}$ and $\{AC_x^\theta\}$.

3.4 MG3, MG4 and MG5 games

Definition 3.7. We say that the first commutative property holds for measurements $\{P_x^\theta\}$ and $\{Q_x^\theta\}$ if for every θ, x and y: $P_x^\theta Q_y^\theta = Q_y^\theta P_x^\theta$.

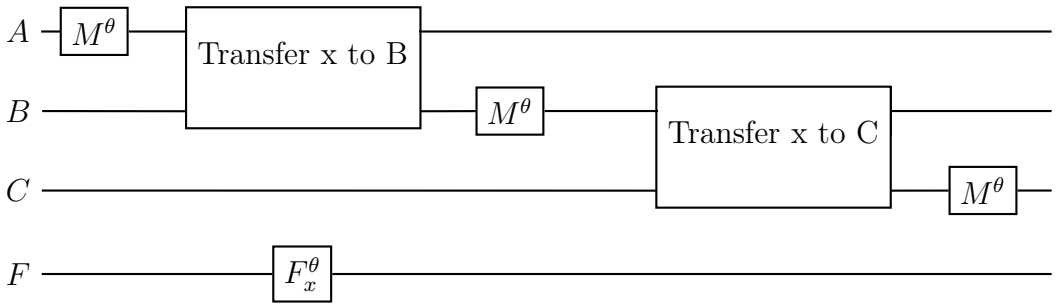


Figure 3.3: MG3 with no restrictions.

Definition 3.8. We say that the second commutative property holds for measurements $\{P_x^\theta\}$, $\{Q_x^\theta\}$ and $\{R_x^\theta\}$ if the first commutative property holds and for every x, y, θ and θ': $P_x^{\theta'}$ and $Q_y^\theta R_y^\theta$ commute.

Definition 3.9. We say that the third commutative property holds for measurements $\{P_x^\theta\}$ and $\{Q_x^\theta\}$ if for every x, y, θ, θ' we have that $P_x^\theta Q_y^{\theta'} = Q_y^{\theta'} P_x^\theta$.

It is easy to see that the 3rd commutative property implies the 2nd commutative property and the 2nd commutative property implies the 1st commutative property.

In the following we will define games based on these commutative properties.

Definition 3.10. Let MG3 be a monogamy game of type MG2, where the measurements fulfil the first commutative property.

Definition 3.11. Let MG4 be a monogamy game of type MG2, where the measurements fulfil the second commutative property.

Definition 3.12. Let MG5 be a monogamy game of type MG2, where the measurements fulfil the third commutative property.

Given the implications between the commutative properties and that the optimal strategy for MG1 can also be used for MG3, MG4 and MG5 the following lemma holds.

Lemma 3.2. *It holds that* $\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n \leq P_{win}(MG5^n) \leq P_{win}(MG4^n) \leq P_{win}(MG3^n) \leq P_{win}(MG2^n)$.

We phrase the monogamy game theorem for MG4.

Theorem 3.3. $P_{win}(MG4^n) = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n$.

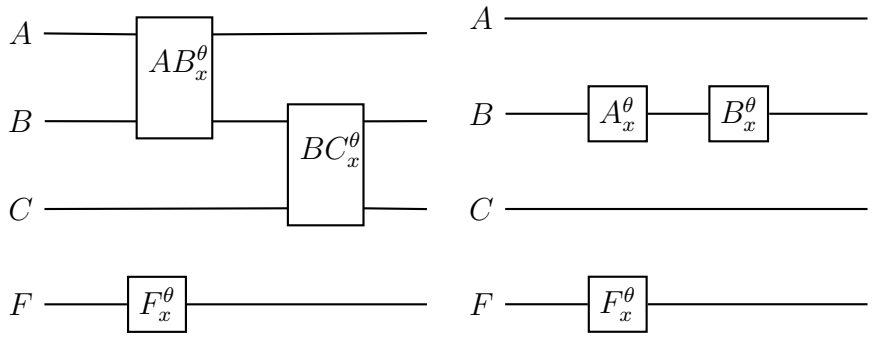


Figure 3.4: MG5' and winning strategy for MG5'

The proof of Theorem 3.3 is analogous to MG0 game theorem in [6] and is given in the Appendix A.

Based on Theorem 3.3 and Lemma 3.2 we have

Corollary 3.4. $P_{win}(MG5^n) = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n$.

3.5 Concerns and assumptions for MG4 and MG5

We proved that the winning probability for the monogamy games MG4 and MG5 is low, since we assume that the measurements fulfil the second commutative property. It is reasonable to question the choice of restriction on the measurements.

3.5.1 First commutative property

The first commutative property ensures that the adversaries are not allowed to communicate with each other directly. They may transfer and share information through entanglement though.

3.5.2 Third commutative property

In the following let us consider what assuming the 3rd commutative property for MG5 implies. For this let us look at a modified game MG5' (see figure 3.4), that accepts strategies of the form $S = \{|s\rangle, \{AB_x^\theta\}, \{BC_x^\theta\}\}$. It is basically a MG5 game where we drop the requirement of the third adversary outputting the correct value.

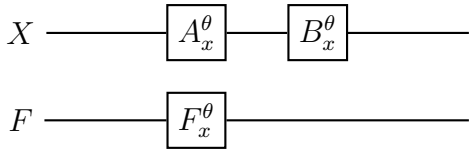


Figure 3.5: Alternative form of MG2, assuming the second commutative property

Looking at Figure 3.4 we see that it would be fairly easy to win the game MG5' without transferring any information between the wires. The adversary can simply create a set of EPR-paris, give the set of first qubits to the adversary and the other qubits to the B-wire. Both adversaries will measure the B-wire in basis θ. Unfortunately this simple strategy is not allowed, as the measurements do not fulfil the third commutative property. This suggest that the 3rd commutative property might be too strong for a reasonable game.

3.5.3 Second commutative property

The proof for Theorem 3.3 assumes that the second commutative property holds. Second commutative property is slightly weaker than the third property, but still stronger than the first commutative property, which rises the question if it is reasonable to assume.

Another concern regarding Theorem 3.3 is that the second commutative property implies that the game expects strategies of the form $S = \{|s\rangle, \{A_x^\theta\}, \{B_x^\theta\}\}$, where $\{A_x^\theta\}$ and $\{B_x^\theta\}$ are both measurements on a common space $\mathcal{H}_X$ and for every θ, θ', x and y we have that A_x^θ and $B_y^{\theta'}$ commute. An illustration is given in Figure 3.5. This is very similar to MG0 and the question arises if using measurements fulfilling the third commutative property is equivalent to using measurements that are carried out on separate wires.

3.6 MG6 and MG7 games

The following section will discuss a special case of MG2.

Definition 3.13. By MG6 we denote a monogamy game that allows strategies of the form $S = \{|s\rangle, \{AB^\theta\}, \{BC^\theta\}, \{AC^\theta\}, \{A_x^\theta\}, \{B_x^\theta\}, \{C_x^\theta\}\}$, where AB^θ, BC^θ and AC^θ are unitary transformations on $\mathcal{H}_A \otimes \mathcal{H}_B$, $\mathcal{H}_B \otimes \mathcal{H}_C$ and $\mathcal{H}_A \otimes \mathcal{H}_C$ respectively and $\{A_x^\theta\}$, $\{B_x^\theta\}$ and $\{C_x^\theta\}$ are projective measurements on $\mathcal{H}_A$, $\mathcal{H}_B$ and $\mathcal{H}_C$ respectively.

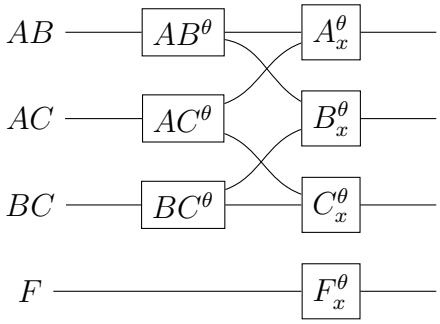


Figure 3.6: Game MG6

Monogamy game MG6 is illustrated in Figure 3.6. It is clear that independent from chosen unitary transformations and measurements the given unitary transformations commute and the measurements commute since they act on separate wires. For the same reason for every x, θ and θ' we have that AB^θ and $C_x^{\theta'}$ commute, BC^θ and $A_x^{\theta'}$ commute and AC^θ and $B_x^{\theta'}$ commute.

The winning probability for the game MG6 is given by

$$P_{win}(\text{MG6}, S) = \sum_{\theta\in\Theta} \frac{1}{|\Theta|} \sum_{x\in X} \langle s|(AB^\theta AC^\theta BC^\theta)^\dagger A_x^\theta B_x^\theta C_x^\theta (AB^\theta AC^\theta BC^\theta)|s\rangle.$$

It is easy to see that the optimal winning strategy from Section 3.3 is allowed for MG6 as well. We simply take AB^θ, AC^θ and BC^θ to be identities on the given Hilbert spaces. Therefore $P_{win}(\text{MG6}^n) \geq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n$.

Definition 3.14. By MG7 we denote a MG6 game, where one of the unitary transformations does not depend on the basis. I.e. an allowed strategy is of the form $S = \{|s\rangle, \{AB^\theta\}, \{BC^\theta\}, \{AC\}, \{A_x^\theta\}, \{B_x^\theta\}, \{C_x^\theta\}\}$.

Theorem 3.5. $P_{win}(MG7^n) = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n$

Proof. Let $S = \{|s\rangle, \{AB^\theta\}, \{BC^\theta\}, \{AC\}, \{A_x^\theta\}, \{B_x^\theta\}, \{C_x^\theta\}\}$ be the given strategy for MG7^n. Since AC does not depend on the basis we can assume, that the adversary has carried it out before supplying the state $|s\rangle$. Therefore we can assume, that it is part of the starting state and $AC = 1_{AC}$. See Figure 3.7. When we discard the B measurement, then the quantum circuits looks as in Figure 3.8. Since this game is now equivalent to MG0^n, we have $\text{MG7}^n \leq \text{MG0}^n = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n$. □

Theorem 3.5 can also be proven analogously to Theorem 3.3, this proof is given in Appendix B.

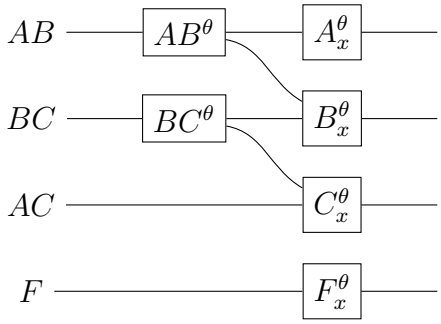


Figure 3.7: Game MG7

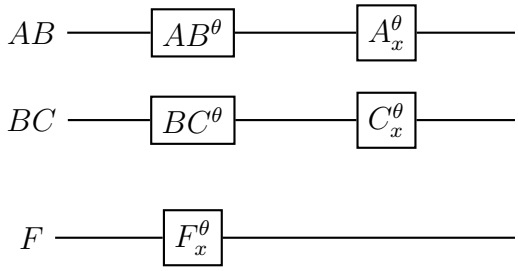


Figure 3.8: Game MG7 without B

3.7 Progress on MG6 proof

In this section we describe the progress on the proof of the MG6 game theorem and identify the gaps that need to be filled. We also explain our intuition behind the missing parts and where the difficulties lie in filling them.

3.7.1 Intuition

Proof. Given the referee F with measurements $\{F_x^\theta = |x^\theta\rangle\langle x^\theta|\}$ assume that $P_{win}(\text{MG6}) = 1$. This means that there exists a state $|\psi\rangle$ and adversaries A, B and C with measurements $\{\bar{A}_x^\theta\}$, $\{\bar{B}_x^\theta\}$ and $\{\bar{C}_x^\theta\}$ such that they guess the correct outcome with probability 1. Here

$$\bar{A}_x^\theta := (AB^\theta AC^\theta)^\dagger (A_x^\theta)(AB^\theta AC^\theta),$$
$$\bar{B}_x^\theta := (AB^\theta BC^\theta)^\dagger (B_x^\theta)(AB^\theta BC^\theta),$$
$$\bar{C}_x^\theta := (AC^\theta BC^\theta)^\dagger (C_x^\theta)(AC^\theta BC^\theta).$$

Our goal is to show that this leads to a contradiction.

If we were looking at a modified game MG6', that only required two adversaries A' and B' and the allowed strategies would be analogous, then it

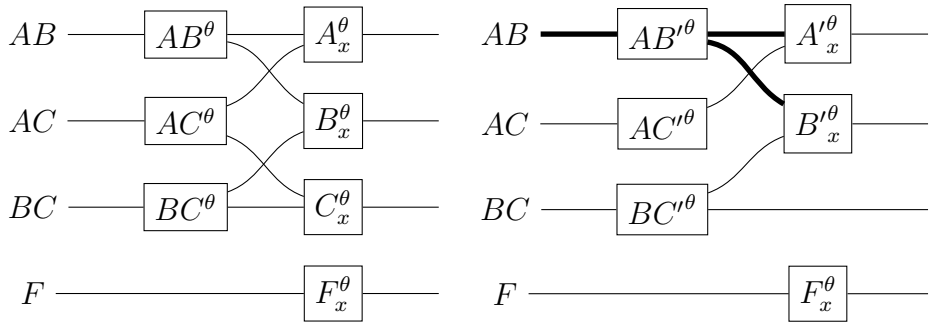


Figure 3.9: Game MG6 and modified game MG6'

would be easy to win the game. We would choose $|\psi\rangle$ as $|junk\rangle_{BC,AC}|\psi_+\rangle_{F,AB}$, where $|\psi_+\rangle = \frac{1}{2}(|00\rangle + |11\rangle)$. We would then use AB'^θ to measure $|\psi_x\rangle$ and forward the result encode in the basis θ to A' and B'. The comparison between games MG6 and MG6' is illustrated in Figure 3.9.

Intuition says that when A and B guess the correct answer in MG6 as well, then the input state $|\psi\rangle$ should be somehow related to $|junk\rangle_{AC,AB}|\psi_x\rangle$.

3.7.2 Steering game

This is indeed true. To show this we use Theorem 1 from [7], which sates that

Theorem 3.6. *[7] Suppose that from the observed correlations, one can deduce the existence of local observables $\{X'_F, Z'_F\}$ (functions of F), and $\{X'_A, Z'_A\}$ (functions of A) with eigenvalues ± 1, which act on the bipartite state $|\Psi\rangle$ such that*

$$\|(X'_F Z'_F + Z'_F X'_F)|\Psi\rangle\| \leq 2\gamma_1, \tag{3.1}$$
$$\|(X'_A Z'_A + Z'_A X'_A)|\Psi\rangle\| \leq 2\gamma_1, \tag{3.2}$$
$$\|(X'_A - X'_F)|\Psi\rangle\| \leq \gamma_2, \tag{3.3}$$
$$\|(Z'_A - Z'_F)|\Psi\rangle\| \leq \gamma_2. \tag{3.4}$$

Then there exists a local isometry $\Phi = \Phi_F \otimes \Phi_A$ and a state $|junk\rangle_{FA}$ such that

$$\|\Phi(M'N'|\Psi\rangle) - |junk\rangle MN|\psi_+\rangle\| \leq \varepsilon \tag{3.5}$$

for $M, N \in \{I, X, Z\}$ and $\varepsilon = (11\gamma_1 + 5\gamma_2)/2$.

We will first explain some of the notations in the above theorem in relation to MG6. The observable corresponding to measurements $\{\bar{A}_x^\theta\}$, $\{\bar{B}_x^\theta\}$ and $\{\bar{C}_x^\theta\}$ are

$$\begin{aligned} Z'_A &= \bar{A}_0^0 - \bar{A}_1^0, & X'_B &= \bar{B}_0^0 - \bar{B}_1^0, & X'_C &= \bar{C}_0^0 - \bar{C}_1^0, \\ X'_A &= \bar{A}_1^0 - \bar{A}_1^1, & Z'_B &= \bar{B}_1^0 - \bar{B}_1^1, & Z'_C &= \bar{C}_1^0 - \bar{C}_1^1 \end{aligned}$$

The observables for the referee are Pauli Z and X gates

$$\begin{aligned} Z_F = Z &= \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1| \\ X_F = X &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = H^\dagger|0\rangle\langle 0|H - H^\dagger|1\rangle\langle 1|H \end{aligned}$$

It is important to notice, that Z_F and X_F anticommute.

For all $P \in \{A, B, C, F\}$ the square of the observables X_P and Y_P is the identity:

$$\begin{aligned} Z_P Z_P &= (P_0^0 - P_1^0)(P_0^0 - P_1^0) \\ &= P_0^0 P_0^0 - P_0^0 P_1^0 - P_1^0 P_0^0 + P_1^0 P_1^0 \\ &= P_0^0 + P_1^0 \\ &= 1_P. \end{aligned} \tag{3.6}$$

Analogously this holds for X_P as well.

3.7.3 Application of steering game

We will now show that the assumptions of Theorem 3.6 hold. Let $|\psi\rangle$ be the input state and let the probability of the adversary A guessing correctly be $1 - \frac{1}{2}\varepsilon$ (for adversaries B and C the following holds analogously). This means

$$\begin{aligned} 2 - \varepsilon &\geq \langle\psi|(F_0^0\bar{A}_0^0 + F_1^0\bar{A}_1^0 + F_0^1\bar{A}_0^1 + F_1^1\bar{A}_1^1)|\psi\rangle \\ &\geq \langle\psi|(F_0^0\bar{A}_0^0 - F_0^0\bar{A}_1^0 - F_1^0\bar{A}_0^0 + F_1^0\bar{A}_1^0 + F_0^1\bar{A}_0^1 - F_0^1\bar{A}_1^1 - F_1^1\bar{A}_0^1 + F_1^1\bar{A}_1^1)|\psi\rangle \\ &= \langle\psi|((F_0^0 - F_1^0)(\bar{A}_0^0 - \bar{A}_0^1) + (F_0^1 - F_1^1)(\bar{A}_0^1 - \bar{A}_1^1))|\psi\rangle \\ &= \langle\psi|(Z_F Z_A + X_F X_A)|\psi\rangle. \end{aligned}$$

Since the value of $\langle\psi|Z_F Z_A|\psi\rangle$ and $\langle\psi|X_F X_A|\psi\rangle$ is between -1 and 1, we have

$$\langle\psi|Z_F Z_A|\psi\rangle \geq 1 - \varepsilon$$

and

$$\langle\psi|X_F X_A|\psi\rangle \geq 1-\varepsilon$$

We can now calculate the vector norm of the difference between the observables for inequality (3.3) and (3.4)

$$\begin{aligned}
\|(X_A - X_F)|\psi\rangle\|^2 &= \langle\psi|(X_A - X_F)^\dagger(X_A - X_F)|\psi\rangle \\
&= \langle\psi|(X_A - X_F)(X_A - X_F)|\psi\rangle \\
&= \langle\psi|(X_A X_A - X_A X_F - X_F X_A + X_F X_A)|\psi\rangle \\
&= 2\langle\psi|(1 - X_F X_A)|\psi\rangle \\
&= 2 - 2\langle\psi|X_F X_A|\psi\rangle \\
&\leq 2 - 2(1-\varepsilon) \\
&= 2\varepsilon.
\end{aligned}$$

Above we used that X_A and X_F commute, as they operate on separate wires. Analogously $\|(Z_A - Z_F)|\psi\rangle\|^2 \leq 2\varepsilon$, therefore

$$\begin{aligned}
\|(Z_A - Z_F)|\psi\rangle\| &\leq \sqrt{2\varepsilon}, \\
\|(X_A - X_F)|\psi\rangle\| &\leq \sqrt{2\varepsilon}.
\end{aligned} \tag{3.7}$$

Since X_F and Z_F anticommute we have $\|(X_F Z_F + Z_F X_F)|\psi\rangle\| = 0$. Using this and inequality 3.7 we can calculate the norm in equation (3.2)

$$\begin{aligned}
\|X_A Z_A + Z_A X_A\| &\leq 2\sqrt{2\varepsilon}\|X_A Z_F + Z_A X_F\| \\
&= 2\sqrt{2\varepsilon}\|Z_F X_A + X_F Z_A\| \\
&\leq 4\sqrt{2\varepsilon}\|Z_F X_F + X_F Z_F\| \\
&= 4\sqrt{2\varepsilon}.
\end{aligned}$$

This means that we have observables X_F, Z_F, X_A and Z_A with eigenvalues 1 and -1 such that

$$\begin{aligned}
\|(X_F Z_F + Z_F X_F)|\psi\rangle\| = 0 \leq 4\sqrt{2\varepsilon} &= 2\gamma_1, \\
\|(X'_A Z'_A + Z'_A X'_A)|\psi\rangle\| \leq 4\sqrt{2\varepsilon} &= 2\gamma_1 \\
\|(X'_A - X'_F)|\psi\rangle\| \leq \sqrt{2\varepsilon} &= \gamma_2 \\
\|(Z'_A - Z'_F)|\psi\rangle\| \leq \sqrt{2\varepsilon} &= \gamma_2
\end{aligned}$$

Therefore the assumptions of Theorem 3.6 hold and there exists a local isometry $\Phi = \Phi_F \otimes \Phi_A$ and a state $|junk\rangle_{AB}$ such that

$$\|\Phi(M_F N'_A|\psi\rangle) - |junk\rangle_{FA} M N|\phi_+\rangle\| \leq \gamma \tag{3.8}$$

for $M, N \in \{X, Z, 1\}$ and $\gamma = \frac{11}{2}\gamma_1 + \frac{5}{2}\gamma_2$. Using the equalities above we have $\gamma = 11\sqrt{2\varepsilon} + \frac{5}{2}\sqrt{2\varepsilon} = \frac{27}{2}\sqrt{2\varepsilon}$.

3.7.4 Implications

The isometry used in the proof of Theorem 3.6 in [7] is of the form

$$\begin{aligned}\Phi(|\psi\rangle) = &\frac{1}{4}(1+Z_F)(1+Z'_A)|\psi\rangle|00\rangle \\ &+\frac{1}{4}X'_A(1+Z_F)(1-Z'_A)|\psi\rangle|01\rangle \\ &+\frac{1}{4}X_F(1-Z_F)(1+Z'_A)|\psi\rangle|10\rangle \\ &+\frac{1}{4}X_FX'_A(1-Z_F)(1-Z'_A)|\psi\rangle|11\rangle.\end{aligned} \tag{3.9}$$

And the state $|junk\rangle_{FA}$ is close to (in case $\varepsilon = 0$ equal to) $\frac{(1+Z_F)(1+Z'_A)}{2\sqrt{2}}|\psi\rangle|\phi_+\rangle$. Note that $1+Z_F = F_0^1 + F_1^1 + F_0^1 - F_1^1 = 2F_0^1$, analogously $1+Z_A = 2\bar{A}_0^1$.

We see from (3.9) that Φ does not affect the BC wire. The preparation of $|junk\rangle$ and the quantum circuit are illustrated in Figure 3.10.

We see that the wires BC_B and BC_C cannot be entangled with the F wire. If we now work under the assumption, that adversary B guesses correctly then we end up with an analogous isometry Φ^B that does not affect the AC_A and AC_C wires showing that these wires cannot be entangled with the F wire. This follows the intuition that the entangled states comes through the AB_A and AB_B wires as shown in Figure 3.9.

The difficulty here is, that the BC_B and BC_C wires can still be entangled with AB_A, AB_B, AC_A and AC_C wires. If this was not the case we could simply leave away the BC_B and BC_C wires, which would result in MG7.

□

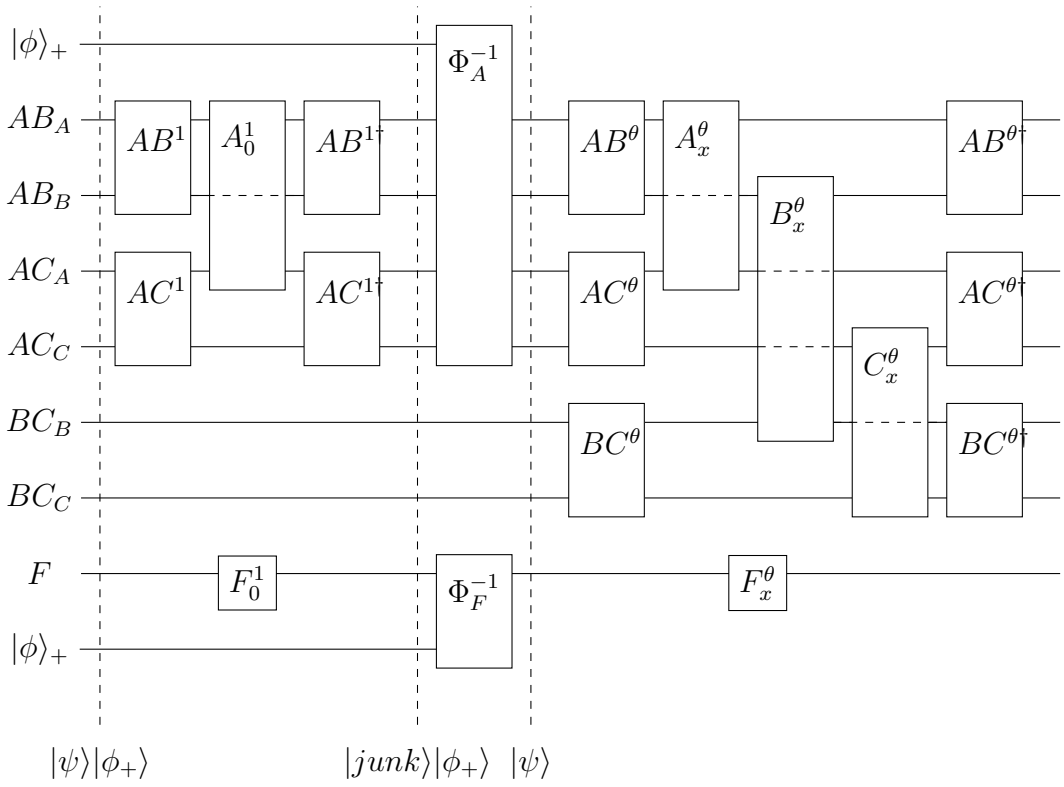


Figure 3.10: Circuit showing application of isometry Φ.

4. Position verification

The property that entanglement is monogamous can be used in situations where it is important to show that multiple parties, separated by space, cannot trivially impersonate a third person located at a specific place. This means that monogamy of entanglement is useful in quantum position verification.

4.1 Position verification

A position verification protocol is a protocol that verifies prover by its location only. It was shown that such a protocol can not be secure in the classical setting [3]. To demonstrate this we will use a simple protocol in the one dimensional case.

4.1.1 Impossibility in classical setting

Let there be two verifiers V_1 and V_2 that wish to verify that the location of a prover is exactly in the center of the line connecting these two verifiers. We assume that the verifiers have a secure communication channel so that they can agree on the starting information and verify the results. As a preparation they will randomly chooses bit-strings x_1 and x_2. Then at time $t = 0$ verifier V_1 sends x_1 to the prover and verifier V_2 sends x_2 to the prover. At time $t = 1$ prover receives both bit-strings. Prover then performs a calculation, say function F(a,b), on x_1 and x_2 resulting in $y_1 = y_2 = F(x_1, x_2)$. He then sends y_1 to the verifier V_1 and y_2 to the verifier V_2. At time $t = 2$ verifiers V_1 and V_2 receive the information y_1 and y_2 respectively. They then compare if $y_1 = y_2 = F(x_1, x_2)$ over a secure channel. The protocol is illustrated in Figure 4.1.

In the classical setting such a protocol is very insecure. To show that the protocol is insecure we have to show that an adversary, or a set of adversaries, would be able to convince the verifiers that he is located in the honest provers location, that is in the center of the line between the verifiers. Let there be

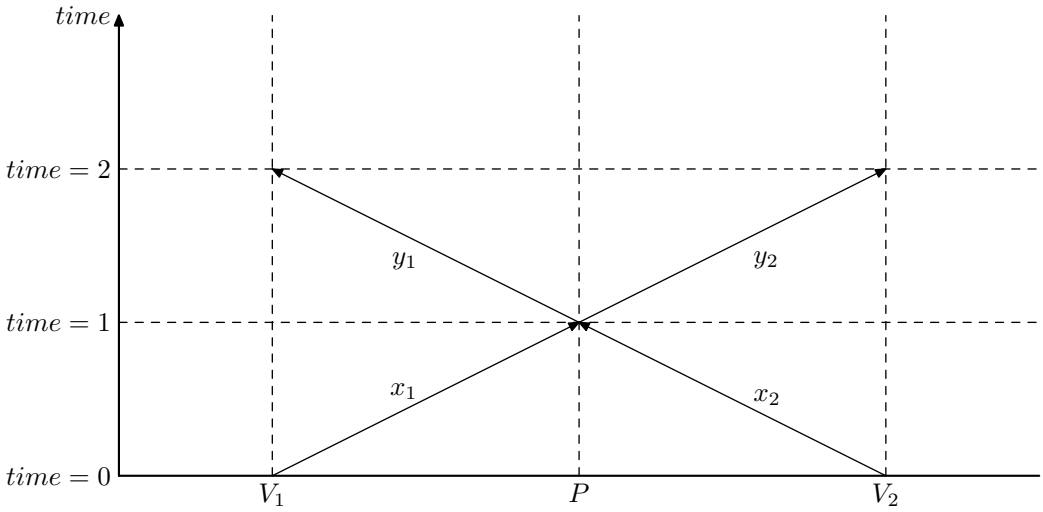


Figure 4.1: Position verification in one dimension

two adversaries A_1 and A_2. Let A_1 be located between verifier V_1 and the honest provers location and A_2 be located between V_2 and the honest provers location. Now at time t_0 both verifiers send out bit-strings x_1 and x_2. At time $t = \frac{1}{2}$ adversary A_1 receives x_1 and adversary A_2 receives x_2. Both adversaries will make a copy of this information and send the original to the other verifier. At time $t = \frac{3}{2}$ adversary A_1 receives x_2 and adversary A_2 receives x_1. They are now both able to calculate $F(x_1, x_2)$. Adversary A_1 sends $y_1 = F(x_1, x_2)$ to verifier V_1 and adversary A_2 sends $y_2 = F(x_1, x_2)$ to verifier V_2. At time $t = 2$, as expected, verifiers V_1 and V_2 receive y_1 and y_2 respectively. They then compare the results. But since $y_1 = F(x_1, x_2) = y_2$ they will accept.

In the classical setting it is easy for two adversaries, located at any point in the line, to trick the verifiers, as long as one adversary is at the right hand side of the honest provers location and the other on the left hand side of the honest provers location. The question arises if this is also the case in the quantum setting. The main reason why the adversaries were able to impersonate a honest prover that easily was that they could keep a copy of the information. This is not possible in the quantum setting due to the no-cloning theorem. Namely one cannot copy an unknown quantum state without disturbing the original state.

4.1.2 Quantum setting

Unfortunately it was shown in [2] that information-theoretically secure position verification is not possible in the quantum setting if adversaries are

allowed to share any amount of entangled states. It is shown in [2] that position verification is possible if no entanglement between adversaries is allowed and it was shown in [9] that position verification is possible in the random oracle model. Random oracle model is a model where we model hash functions as random oracles. When we model a hash function as a random oracle it means that we model it as a random function. We assume that the adversary has limited computational power and will query the random oracle a limited number of times. In such a setting the probability of guessing the hash value of x is close to guessing x itself.

The result in [9] uses the monogamy game MG0 to show that adversaries located outside the honest provers region can calculate the correct result and send it to the verifiers with negligible probability only. Since MG0 has two adversaries the number of receiving verifiers in [9] is limited to two verifiers as well. A monogamy game result with multiple adversaries and overlapping measurements can be used to prove a position verification result with more than two receiving verifiers and therefore tighten the honest provers region.

In the following section we will look at the position verification protocol introduced in [9].

4.2 Position verification with two receiving verifiers

In the following we will discuss the position verification protocol from [9] and sketch the proof given in [9]. The definitions given in this section are not precise but give an intuition for the protocol and the proof.

In the following we see all actions related to the protocol as spacetime circuits. Spacetime circuits can be seen as quantum circuits that are located at a specific place in spacetime. The location in spacetime specifies when and where the gate is executed. In a spacetime circuit there is a wire from gate A to gate B if information can travel from A to B without defying the laws of physics.

We say that a position verification protocol is sound for a region P in spacetime if the probability that the verifiers accept an adversary that has no gates in P is negligible.

Definition 4.1 (Position verification protocol)**.** [9] Let $V_1, \ldots, V_r$ be verifiers. Let n be the number of qubits and ℓ the length of classical challenges. Let $0 \leq \gamma \leq 1$ be the fraction of allowed errors. Let $H : \{0,1\}^\ell \to \{0,1\}^n$ be a hash function (we model it as a random oracle). Then the protocol execution is following:

1. Verifiers choose random bit-strings $x_1, \ldots, x_r$ of length ℓ. They also choose a random bit-string $\hat{y}$ of length n.

2. V_1 prepares the quantum state $|\Psi\rangle$ by encoding $\hat{y}$ in the basis $\theta = H(x_1 \oplus \cdots \oplus x_r)$. V_1 sends $|\Psi\rangle$ to the prover.

3. Each verifier V_i sends the bi-tstring x_i to the prover.

4. Prover receives all x_i and $|\Psi\rangle$. He calculates the basis $\theta = H(x_1 \oplus \cdots \oplus x_r)$ and uses it to measure $|\Psi\rangle$. He obtains the outcome y. He then sends y to verifiers V_1 and V_2.

5. Verifiers V_1 and V_2 receive y_1 and y_2 respectively. They check if $y_1 = y_2 = \hat{y}$ If this holds and both y_1 and y_2 were also received in time they accept.

Theorem 4.1 (Soundness of PV protocol)**.** *[9] There is no event in spacetime outside of P at which one can receive the messages x_i from all V_i, and send messages that will be received in time by V_1, V_2. (If the malicious prover is allowed to perform at most q queries, then the soundness error is at most $\nu := \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n + 2q2^{-\frac{\ell}{2}}$.)*

Here P is the region in spacetime where all x_i can be received from the verifiers and there is still enough time to send the result to verifiers V_1 and V_2. In any location in spacetime that is outside of P either one of x_i is not known or there is not enough time to send the result to one of the verifiers.

The definition of P may sound as if it is clear that malicious provers outside of this point cannot get the verifiers to accept (as they cannot at the same time receive all x_i and still have enough time to send the result to the verifiers). Yet when we look back at the previous section where we looked at position verification in the classical setting the region P would have been the point in spacetime located in the center of V_1 and V_2 at time 1. It was fairly simple to construct malicious provers that can send the correct y to the verifiers by simply copying and forwarding the classical challenges.

It is also important to notice that if we expect the prover to answer instantaneously then the region P becomes a single point in spacetime.

4.2.1 Proof sketch

Proof. In the following we will sketch the proof of Theorem 4.1. Assume that we have a malicious prover that is not located in the spacetime region P. This means that there will be no gates in P and there will be sub-circuits

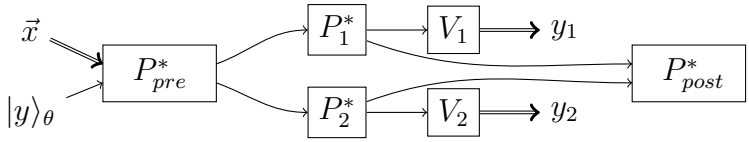


Figure 4.2: Circuit for position verification protocol. Figure reproduced from [9].

where the malicious prover calculates y_1 and y_2. We can therefore divide all gates between sub-circuits as follows.

Subcircuit	Intuition
P^*_{pre}	Pre-computation
P^*_P	Gates in P (empty)
P^*_1	Computing y_1
P^*_2	Computing y_2
P^*_{post}	After protocol end

Sub-circuit P^*_{pre} involves steps $1-3$ of the protocol. Sub-circuit P^*_P is empty. Sub-circuits P^*_1 and P^*_2 involve step 4 of the circuit and sub-circuit P^*_{post} is everything that is done after the protocol ends. Sub-circuits V_1 and V_2 are verifiers measuring the result sent by the prover. This circuit is illustrated in figure 4.2.

It is fairly clear the there are no wires coming into P^*_{pre} as everything in P^*_{pre} happens before the other circuits. It is also clear that there can be no wires leaving P^*_{post} as P^*_{post} is executed after protocol end. After the circuit P^*_{pre} all x_i are known. Therefore there are no wires between P^*_1 and P^*_2, as P^*_1 can only send information to V_1 and P^*_2 only to V_2. If this was not the case circuits P^*_1 and P^*_2 would be located in P.

We will now use games to estimate the probability of the verifiers accepting.

Game 1 (Protocol execution)**.** *Pick random bitstrings x_i of lenght ℓ and random bistring y of lenght n. Pick a random function $H : \{0,1\}^\ell \to \{0,1\}^n$. Execute circuit from figure 4.2 with output y_1 and y_2. Accept if $y_1 = y_2 = \hat{y}$.*

First we can get rid of P^*_{post}, as it has no effect on the results of V_1 and V_2. Our next goal is to delay the choice of the basis θ. Currently it is used before executing the protocol. To delay this we will use EPR pairs instead of preparing the state $|y\rangle_\theta$. An EPR pair is a fully entangled 2-qubit state that when measured on either qubit (either in the computational or diagonal basis) gives a uniformly random output 0 or 1. Furthermore when performing the same measurement on the other qubit, the results are the same. Therefore

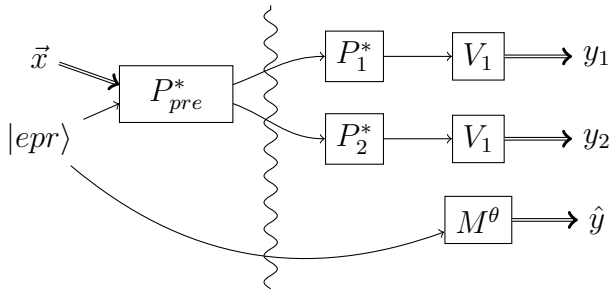


Figure 4.3: Circuit for protocol in Game 2. Figure reproduced form [9].

picking a random y and preparing the state $|y\rangle_\theta$ is equivalent to preparing EPR paris and measuring last half of the qubits in the basis θ to obtain y.

Game 2 (Using EPR paris)**.** *Pick random bitstrings x_i of lenght ℓ. Pick a random function $H : \{0,1\}^\ell \to \{0,1\}^n$. Prepare EPR pairs. Execute circuit form Figure 4.3 with outputs y_1, y_2 and $\hat{y}$. Accept if $y_1 = y_2 = \hat{y}$.*

We have

$$Pr[\text{accept} = 1 : \text{ Game 1 }] = Pr[\text{accept} = 1 : \text{ Game 2 }].$$

We have now delayed the use of basis θ but it is still chosen early. To fix this we will reprogram the random oracle H to be a completely random function in the beginning but from a given point in time to return θ on the input $x_1 \oplus \cdots \oplus x_r$. The prover will not notice this unless he queries $H(x_1 \oplus \cdots \oplus x_r)$ before the random oracle is reprogrammed. Results on the quantum random oracle (see [9]) show that the probability of this happening is equivalent to $2q$ times the square root of the probability of the prover guessing the value $x_1 \oplus \cdots \oplus x_r$ without knowing all x_i.

Game 3 (Reprogramming H)**.** *Pick random bitstring x_i of lenght ℓ. Pick a random function $H : \{0,1\}^\ell \to \{0,1\}^n$. Prepare EPR pairs. Execute circuit form Figure 4.3 until the wiggly line. Now reprogram H, so that $H(x_1 \oplus \cdots \oplus x_r) = \theta$. Run the circuit from Figure 4.3 after the wiggly line with outputs y_1, y_2 and $\hat{y}$. Accept if $y_1 = y_2 = \hat{y}$.*

Game 4 (Guessing $x_1 \oplus \cdots \oplus x_r$)**.** *Pick random bitstrings x_i of lenght ℓ. Pick a random function $H : \{0,1\}^\ell \to \{0,1\}^n$. Prepare EPR pairs. Execute P^*_{pre} until the j-th query to H. Measure the argument x' of that query.*

We have

$$\begin{aligned}|Pr[\text{accept} = 1 :\ \text{Game 2 }] - Pr[\text{accept} = 1 :\ \text{Game 3 }]| \\ &\leq 2q\sqrt{Pr[x_1 \oplus \cdots \oplus x_r = x' :\ \text{Game 4}]} \\ &\leq 2q\sqrt{2^{-\ell}} = 2q2^{-\ell/2}.\end{aligned}$$

We will now look at Game 3. Looking at Figure 4.3 we see that there are 3 separate registers at the wiggly line. Let the registers be called A, B and F. Let ψ be the quantum state at the wiggly line. Let A refer to the part of ψ on the wire entering P_1^*, let B refer to the part of ψ on the wire entering P_2^* and let F be the lowest wire containing qubits from the EPR paris. Let M_A^θ be the measurement consisting of P_1^* and V_1 and M_B^θ the measurement consisting of P_2^* and V_2. In general these measurements are POVM-s and ψ might be a mixed state, but without loss of generality we can assume that ψ is a pure state and the given measurements are projective as this can be done by increasing the underlying Hilbert spaces [6].

Game 5 (Monogamy game)**.** *Prepare* $|\psi\rangle$*. Pick random basis* θ*. Perform measurement* M_A^θ*,* M_B^θ *and* M_F^θ *resulting in* y_1*,* y_2 *and* $\hat{y}$*. Accept if* $y_1 = y_2 = \hat{y}$*.*

Then $Pr[\text{accept} = 1 :\ \text{Game 3}] = Pr[\text{accept} = 1 :\ \text{Game 5}]$. We see that Game 5 is an n-times parallelly repeated MG0 game. Therefore

$$Pr[\text{accept} = 1 :\ \text{Game 5}] \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n.$$

Combining all games we get

$$Pr[\text{accept} = 1 :\ \text{Game 1}] \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n + 2q2^{\ell/2}.$$

□

4.2.2 Size of the provers region

The provers region P is the region in spacetime where all x_i are known and there is still enough time for information to reach both verifiers. If we expect the prover to answer instantaneously then the region P becomes a single point in spacetime [9]. The region becomes larger when we give the prover more time for calculations. In the 1 dimensional case the provers region with additional time ε is illustrated in Figure 4.4.

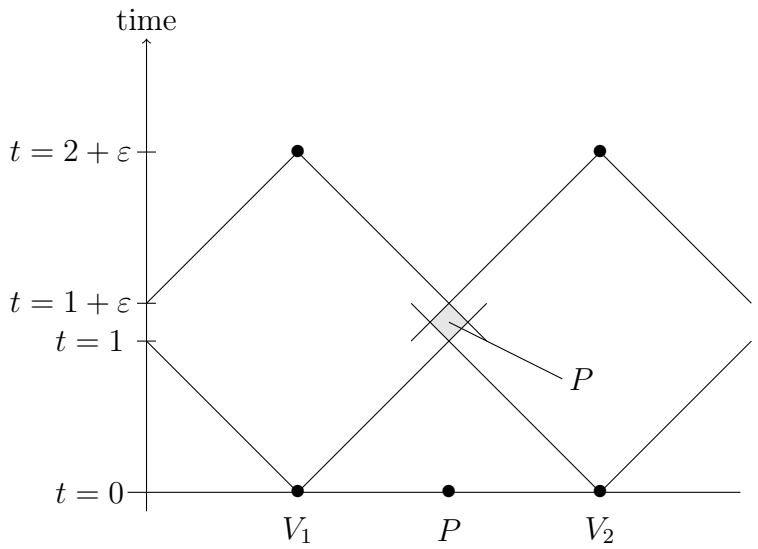
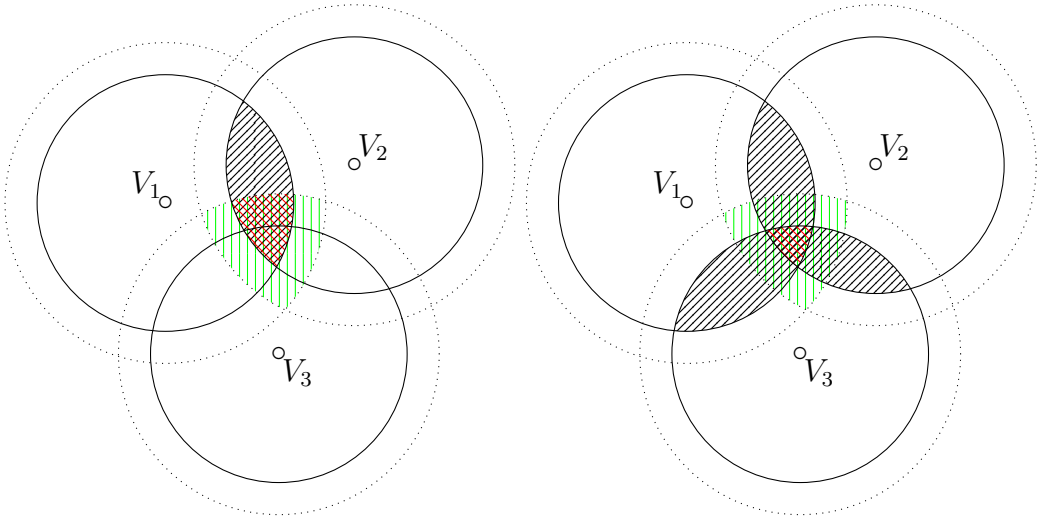


Figure 4.4: Size of the provers region in 1D. Figure reproduced from [9].

When we go into more dimensions the shape of the provers region becomes more complicated. As in 1D the region P is the intersection of light cones originating from V_i at time $t = 0$ showing where light can travel from the verifiers and light cones originating from V_1 and V_2 at time $t = 2 + \varepsilon$ showing from where information can reach the verifiers. For a better intuition Figure 4.5 (a) shows the intersection of spacetime at time $t = 1 + \frac{2}{3}\varepsilon$.

Now let us imagine what would happen if we were able to add a third receiving verifier. If the provers region in this setting would still be the intersection of the future light cones of sending verifiers and past light cones of receiving verifiers, then the provers region would become smaller. Looking at Figure 4.5 we can compare the two setting in (a) and (b). We see that there is a region between V_1 and V_2 where all x_i are known and both verifiers can be reached, but verifier V_3 would be out of reach.

Therefore the question arises if the position verification protocol would be sound for this smaller region if we add a third receiving verifier. We will look into this in the following section.



(a) 2 verifiers (b) 3 verifiers

Figure 4.5: Size of the provers region in 2D, intersection of spacetime at $t = 1+\frac{2}{3}\varepsilon$. Setting with 2 verifiers vs. 3 verifiers receiving.

4.3 Position verification with three receiving verifiers

In this section we define a new position verification protocol that uses three receiving verifiers instead of two. We state under which assumptions the protocol is sound and give a proof sketch. The definition in this section are again not precise but give a good intuition. Full proof with precise definitions is given in the next chapter.

Definition 4.2 (Position verification protocol)**.** Let $V_1, \ldots, V_r$ be verifiers. Let n be the number of qubits and ℓ the lenght of classical challenges. Let $0 \leq \gamma \leq 1$ be the fraction of allowed errors. Let $H : \{0,1\}^\ell \to \{0,1\}^n$ be a hash function (we model it as a random oracle). Then the protocol execution is following:

1. Verifiers choose random bitstrings $x_1, \ldots, x_r$ of length ℓ. They also choose a random bitstring $\hat{y}$ of length n.

2. V_1 prepares the quantum state $|\Psi\rangle$ by encoding $\hat{y}$ in the basis $\theta = H(x_1 \oplus \cdots \oplus x_r)$. V_1 sends $|\Psi\rangle$ to the prover.

3. Each verifier V_i sends the bitstring x_i to the prover.

4. Prover receives all x_i and $|\Psi\rangle$. He calculates the basis $\theta = H(x_1 \oplus \cdots \oplus x_r)$ and uses it to measure $|\Psi\rangle$. He obtains the outcome y. He then sends y to verifiers V_1 and V_2.

5. Verifiers V_1, V_2 and V_3 receive y_1, y_2 and y_3 respectively. They check if $y_1 = y_2 = y_3$ and if $y_1 = \hat{y}$ If this holds and both y_1, y_2 and y_3 were also received in time they accept.

Theorem 4.2 (Soundness of PV protocol)**.** *There is no event in spacetime outside of P at which one can receive the messages x_i from all V_i, and send messages that will be received in time by V_1, V_2 and V_3. (If the malicious prover is allowed to perform at most q queries, then the soundness error is at most $\nu := P_{win}(MG6^n) + 2q2^{-\frac{\ell}{2}}$.)*

Here P is the region in spacetime where all x_i can be received from the verifiers and there is still enough time to send the result to verifiers V_1, V_2 and V_3. In any location in spacetime that is outside of P either one of x_i is not known or there is not enough time to send the result to one of the verifiers.

As we discussed in the previous section the position verification protocol with 3 receiving verifiers has a higher precision than the protocol with 2

receiving verifiers that is the provers region for the 3 verifier protocol is smaller. See Figure 4.5.

4.3.1 Proof sketch

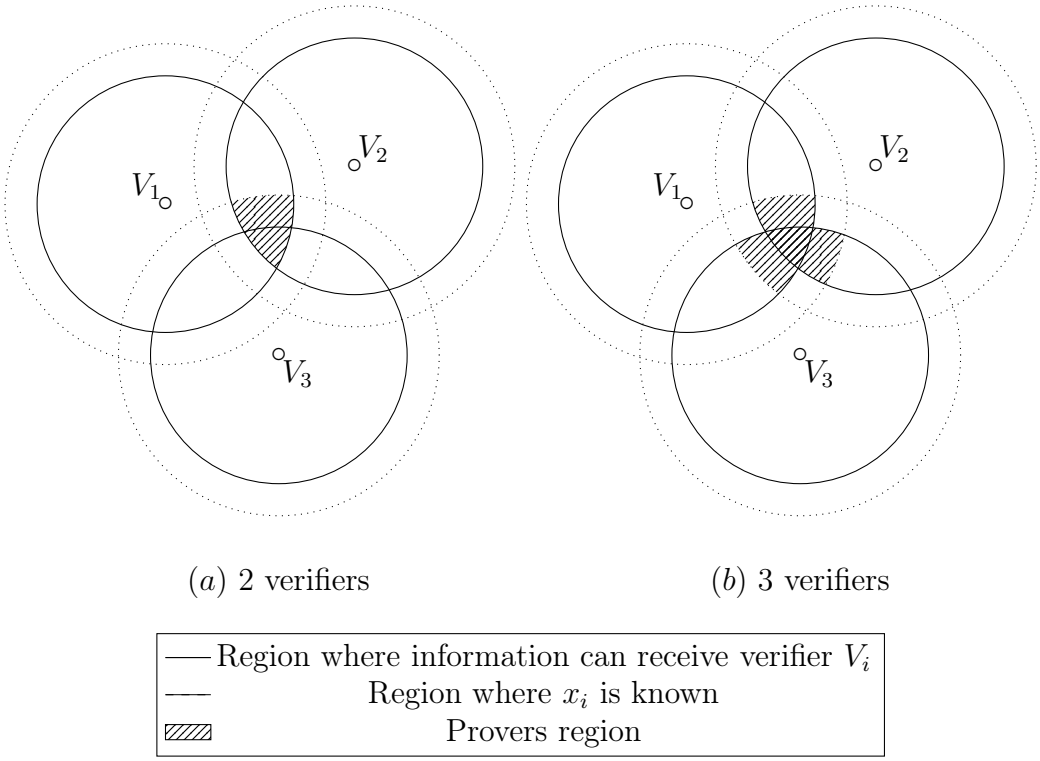
Proof. In the following we will sketch the proof of Theorem 4.2. The proof is very similar to the proof of Theorem 4.1 with a few key differences that we will emphasise.

Assume that we have a malicious prover that is not located in the space-time region P. This means that there will be no gates in P and there will be subcircuits where the malicious prover calculates y_1,y_2 and y_3. We would like to divide all gates between subcircuits as was done in the proof of Theorem 4.1. If we just added a gate P_3^* and used the division

Subcircuit	Intuition
P_{pre}^*	Precomputation
P_P^*	Gates in P (empty)
P_1^*	Computing y_1
P_2^*	Computing y_2
P_3^*	Computing y_3
P_{post}^*	After protocol end

we would end up with a larger provers region than we did with 2 receiving verifiers. Notice that for P_1^*, P_2^* and P_3^* to be separated subcircuits that have no wires between them we would have to include the spacetime region where all x_i are known and information can reach two verifiers in the region P. Figure 4.6 illustrates region P for 2 receiving verifiers and 3 receiving verifiers as an intersection at time $t = 1 + \frac{2}{3}\varepsilon$ in this setting.

This means that we will have subcircuits that have wires to two P_i^* and P_j^* each. We can interpret these subcircuits as preparing the quantum state before calculation of y_i and y_j. This way we can partition the quantum circuit into following subcircuits



(a) 2 verifiers (b) 3 verifiers

Figure 4.6: Size of the provers region in 2D, intersection of spacetime at $t = 1+\frac{2}{3}\varepsilon$. Setting with 2 verifiers vs. 3 verifiers receiving.

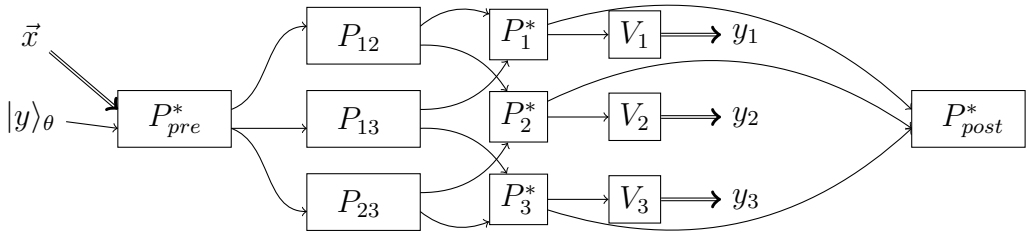


Figure 4.7: Circuit for protocol with 3 receiving verifiers.

Subcircuit	Intuition
P^*_{pre}	Precomputation
P^*_P	Gates in P (empty)
P_{12}	Preparing for y_1 and y_2 computation
P_{13}	Preparing for y_1 and y_3 computation
P_{23}	Preparing for y_2 and y_3 computation
P^*_1	Computing y_1
P^*_2	Computing y_2
P^*_3	Computing y_3
P^*_{post}	After protocol end

This circuit is illustrated in Figure 4.7.

It is fairly clear the there are no wires coming into P^*_{pre} as everything in P^*_{pre} happens before the other circuits. It is also clear that there can be no wires leaving P^*_{post} as P^*_{post} is executed after protocol end. After the circuit P^*_{pre} all x_i are known. There are no wires between P^*_1, P^*_2 and P^*_3, as P^*_1 can only send information to V_1, P^*_2 only to V_2 and P^*_3 only to V_3. If this was not the case and there was a wire for example form P^*_1 to P^*_2, then P^*_1 would be located in P_{12}. There are also no wires from P_{12} to P^*_3, from P_{13} to P_{23} to P_1 because otherwise they would be located in P.

We will now use games to estimate the probability of the verifiers accepting.

Game 1 (Protocol execution)**.** *Pick random bitstrings x_i of lenght ℓ and random bistring y of lenght n. Pick a random function $H : \{0,1\}^\ell \to \{0,1\}^n$. Execute circuit from figure 4.7 with output y_1, y_2 and y_3. Accept if $y_1 = y_2 = y_3 = \hat{y}$.*

First we can get rid of P^*_{post}, as it has no effect on the results of V_1, V_2 and V_3. Our next goal is to delay the choice of the basis θ. Currently it is used before executing the protocol. To delay this we will use EPR pairs instead

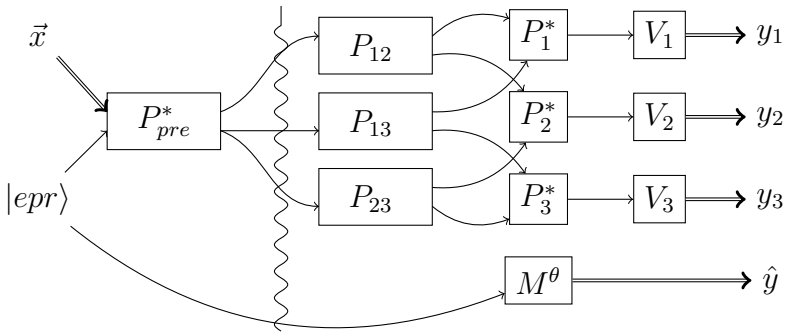


Figure 4.8: Circuit for protocol with 3 receiving verifiers for Game 2.

of preparing the state $|y\rangle_\theta$. Picking a random y and preparing the state $|y\rangle_\theta$ is equivalent to preparing EPR paris and measuring last half of the qubits in the basis θ to obtain y.

Game 2 (Using EPR pairs)**.** *Pick random bit-strings x_i of length ℓ. Pick a random function $H : \{0,1\}^\ell \to \{0,1\}^n$. Prepare EPR pairs. Execute circuit form Figure 4.8 with outputs y_1, y_2, y_3 and $\hat{y}$. Accept if $y_1 = y_2 = y_3 = \hat{y}$.*

We have

$$Pr[\text{accept} = 1 : \text{ Game 1 }] = Pr[\text{accept} = 1 : \text{ Game 2 }].$$

As in the proof sketch in the previous section we have now delayed the use of basis θ but it is still chosen early. To fix this we will reprogram the random oracle H to be a completely random function in the beginning but from a given point in time to return θ on the input $x_1 \oplus \cdots \oplus x_r$.

Game 3 (Reprogramming H)**.** *Pick random bit-string x_i of length ℓ. Pick a random function $H : \{0,1\}^\ell \to \{0,1\}^n$. Prepare EPR pairs. Execute circuit form Figure 4.8 until the wiggly line. Now reprogram H, so that $H(x_1 \oplus \cdots \oplus x_r) = \theta$. Run the circuit from Figure 4.3 after the wiggly line with outputs y_1, y_2, y_3 and $\hat{y}$. Accept if $y_1 = y_2 = y_3 = \hat{y}$.*

Game 4 (Guessing $x_1 \oplus \cdots \oplus x_r$)**.** *Pick random bit-strings x_i of length ℓ. Pick a random function $H : \{0,1\}^\ell \to \{0,1\}^n$. Prepare EPR pairs. Execute P^*_{pre} until the j-th query to H. Measure the argument x' of that query.*

We have

$$\begin{aligned}|Pr[\text{accept} = 1 :\ \text{Game 2 }] - Pr[\text{accept} = 1 :\ \text{Game 3 }]| \\ &\leq 2q\sqrt{Pr[x_1 \oplus \cdots \oplus x_r = x' :\ \text{Game 4}]} \\ &\leq 2q\sqrt{2^{-l}} = 2q2^{-l/2}.\end{aligned}$$

We will now look at Game 3. Sub-circuits P_{12}, P_{13} and P_{23} prepare the state for P_1^* and P_2^* for P_1^* and P_3^* and for P_2^* and P_3^* respectively. Let M_A^θ, M_B^θ and M_C^θ refer to the measurements consisting of P_1^* and V_1, of P_2^* and V_2 and of P_3^* and V_3 respectively. Then P_{12}, P_{13} and P_{23} can be modelled as unitary operators AB^θ, BC^θ and AC^θ. This way we get three measurements

$$(AB^\theta AC^\theta)^\dagger M_A^\theta (AB^\theta AC^\theta),$$
$$(AB^\theta BC^\theta)^\dagger M_B^\theta (AB^\theta BC^\theta)$$

and

$$(AC^\theta BC^\theta)^\dagger M_C^\theta (AC^\theta BC^\theta).$$

We somewhat abuse the notation here as for an operator A on space $\mathcal{H}_A$ we still write A if the underlying space becomes $\mathcal{H}_A \otimes \mathcal{H}_B$, although it would be correct to write $A \otimes 1_B$.

Notice that performing the conjugate transpose of the unitary operators after the measurement won't change the outcome, but will ensure that the measurements remain projective if M_i^θ is projective. Performing all the measurements is equivalent to

$$\begin{aligned}(AB^\theta AC^\theta)^\dagger M_A^\theta (AB^\theta AC^\theta)(AB^\theta BC^\theta)^\dagger M_B^\theta (AB^\theta BC^\theta)(AC^\theta BC^\theta)^\dagger M_C^\theta (AC^\theta BC^\theta) \\ = (AB^\theta AC^\theta BC^\theta)^\dagger (M_A^\theta M_B^\theta M_C^\theta)(AB^\theta AC^\theta BC^\theta).\end{aligned}$$

As in the previous section with 2 receiving verifiers we can assume that the measurements M_A^θ, M_B^θ and M_C^θ are projective.

Game 5 (Monogamy game)**.** *Prepare* $|\psi\rangle$*. Pick random basis* θ*. Perform measurement* $(AB^\theta AC^\theta)^\dagger M_A^\theta (AB^\theta AC^\theta)$*,* $(AB^\theta BC^\theta)^\dagger M_B^\theta (AB^\theta BC^\theta)$*,* $(AC^\theta BC^\theta)^\dagger M_C^\theta (AC^\theta BC^\theta)$ *and* M_F^θ *resulting in* y_1*,* y_2*,* y_3 *and* $\hat{y}$*. Accept if* $y_1 = y_2 = y_3 = \hat{y}$*.*

Then $Pr[\text{accept} = 1 :\ \text{Game 3}] = Pr[\text{accept} = 1 :\ \text{Game 5}]$. We see that Game 5 is an n-times parallelly repeated MG6 game. Therefore if we can show that

$$P_{win}(MG6^n) \leq \varepsilon$$

then we have

$$\begin{aligned} Pr[\text{accept} = 1 : \text{ Game 1}] &\leq Pr[\text{accept} = 1 : \text{ Game 5}] + 2q2^{l/2} \\ &\leq \varepsilon + 2q2^{l/2}. \end{aligned}$$

□

5. Full proof of position verification theorem with three receiving verifiers

In Chapter 4 we gave a proof sketch for the position verification protocol with 2 receiving verifiers from [9] and a proof sketch for the position verification theorem with 3 receiving verifiers. In this chapter we formalise the proof of the position verification theorem with 3 receiving verifiers.

5.1 Definitions and Theorem statement

We say that a protocol is sound for a region P in space time iff for any spacetime circuit P^* that has no gates in P, the following holds: In an interaction between the verifiers and P^*, the probability that the verifiers accept (the soundness error) is negligible [9]. We say that a protocol is more precise if the region P of the prover is smaller.

Definition 5.1. (Position verification protocol) Let P be a prover, and P° an event in spacetime (P° specifies where and when the honest prover performs its computation). Let $V_1, \dots, V_r$ be verifiers. Let $V_1^+, \dots, V_r^+$ be events in spacetime that causally precede P°. (V_i^+ specifies where and when the verifier V_i sends its challenge.) Let V_1^-, V_2^- and V_3^- be events in spacetime such that P° causally precedes V_1^-, V_2^- and V_3^-. (V_i^- specifies where and when V_i expects the prover's response.) Let n (number of qubits) and ℓ (bit length of classical challenges) be integers. Let $H : \{0,1\}^\ell \to \{0,1\}^n$ be a hash function (modeled as a quantum random oracle).

1. The verifiers choose uniform $x_1, \dots, x_r \in \{0,1\}^\ell, \hat{y} \in \{0,1\}^n$. (By communicating over secure channels.)

2. At some event that causally precedes P°, V_0 sends $|\Psi\rangle$ to P . Here $\theta := H(x_1 \otimes \cdots \otimes x_2)$, $|\Psi\rangle := |\hat{y}\rangle_\theta$.

3. For $i = 1, \ldots, r$: V_i sends x_i to P at event V_i^+.

4. At event P°,P will have $|\Psi\rangle, x_1, \ldots, x_r$. Then P computes $\theta := H(x_i \otimes \cdots \otimes x_r)$, measures $|\Psi\rangle$ in basis θ to obtain outcome y_1, and sends y_1 to V_1, $y_2 := y_1$ to V_2 and $y_3 := y_1$ to V_3.

5. At events V_1^-, V_2^-, V_3^- verifiers V_1, V_2 and V_3 receive y_1,y_2 and y_3. Using secure channels, the verifiers check whether $y_1 = y_2 = y_3 = \hat{y}$. If so (and y_1, y_2, y_3 indeed arrived at V_1^-, V_2^-, V_3^-), the verifiers accept.

In the following by $C^+(A)$ we denote the casual future of event A i.e. the light cone that shows where information can be sent from event A. By $C^-(A)$ we denote the casual past of event A i.e. the light cone that shows from where information can reach the event A.

Theorem 5.1. *The PV protocol from Definition 5.1 is sound for* $P := \cap_{i=1}^r C^+(V_i^+) \cap C^-(V_1^-) \cap C^-(V_2^-) \cap C^-(V_3^-)$. *(In words: There is no event in spacetime outside of* P *at which one can receive the messages* x_i *from all* V_i*, and send messages that will be received in time by* V_1, V_2 *and* V_3*.) Concretely, if the malicious prover performs at most* q *oracle queries, then the soundness error is at most* $\nu = P_{win}(MG6^n) + 2q2^{-\frac{\ell}{2}}$.

Proof. To shorten the notation we write C_i^+ for $C^+(V_i^+)$, C_i^- for $C^-(V_i^+)$, $\cup$ for $\cup_{i=1}^r$ and $\cap$ for $\cap_{i=1}^r$.

5.2 Quantum circuit

We divide all gates between sub-circuits as follows.

Subcircuit	Region in spacetime	Intuition
P^*_{pre}	$(C_1^- \cup C_2^- \cup C_3^-) \setminus \cap C_i^+$	Precomputation
P^*_P	$\cap C_i^+ \cap C_1^- \cap C_2^- \cap C_3^-$	Gates in P (empty)
P_{12}	$\cap C_i^+ \cap C_1^- \cap C_2^- \setminus C_3^-$	Preparing for y_1 and y_2 computation
P_{13}	$\cap C_i^+ \cap C_1^- \cap C_3^- \setminus C_2^-$	Preparing for y_1 and y_3 computation
P_{23}	$\cap C_i^+ \cap C_2^- \cap C_3^- \setminus C_1^-$	Preparing for y_2 and y_3 computation
P^*_1	$\cap C_i^+ \cap C_1^- \setminus (C_2^- \cup C_3^-)$	Computing y_1
P^*_2	$\cap C_i^+ \cap C_2^- \setminus (C_1^- \cup C_3^-)$	Computing y_2
P^*_3	$\cap C_i^+ \cap C_3^- \setminus (C_1^- \cup C_2^-)$	Computing y_3
P^*_{post}	$\Omega \setminus \cup C_i^- \setminus P^*_{pre}$	After protocol end

There can be a wire from one specetime circuit A to a specetime circuit B, if A and B are at events E_A and E_B respectively and E_A casually precedes

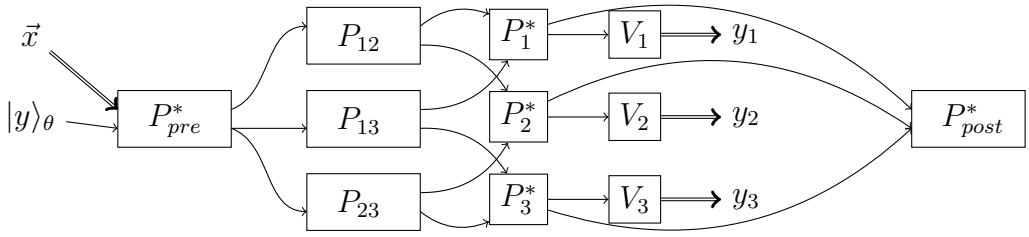


Figure 5.1: Circuit for protocol with 3 receiving verifiers.

E_B (denoted $E_A \prec E_B$). Note that $\prec$ is transitive. Therefore we have that there can be no wires leaving C_i^- and there are no wires entering C_i^+. Given these preconditions we would like, that all sub-circuits are disjoint and their union is Ω. We will show that the following equalities hold

$$P^*_{pre} \cap P^*_P = \emptyset \tag{5.1}$$
$$P^*_{pre} \cap P_{12} = \emptyset \tag{5.2}$$
$$P^*_{pre} \cap P^*_1 = \emptyset \tag{5.3}$$
$$P_{12} \cap P^*_1 = \emptyset \tag{5.4}$$
$$P_{12} \cap P^*_3 = \emptyset \tag{5.5}$$
$$P^*_{pre} \cap P^*_{post} = \emptyset \tag{5.6}$$
$$P_{12} \cap P^*_{post} = \emptyset \tag{5.7}$$
$$P^*_1 \cap P^*_{post} = \emptyset. \tag{5.8}$$

Equality (5.1) holds trivially as $P^*_P = \emptyset$ by assumption. Assume that $P^*_{pre} \cap P_{12} \neq \emptyset$, then $\exists x \in P^*_{pre} \cap P_{12}$, which means $x \notin \cap C_i^+$ and $x \in \cap C_i^+$, which is a contradiction. Therefore equality (5.2) holds. Equality (5.3) holds for the same reasoning. Assume $P_{12} \cap P^*_1 \neq \emptyset$, then $\exists x \in P_{12} \cap P^*_1$, which means $x \in C_2^-$ and $x \notin C_2^-$, which is a contradiction, therefore equality (5.4) holds. Assume $P_{12} \cap P^*_3 \neq \emptyset$, then $\exists x \in P_{12} \cap P^*_3$, which means $x \in C_1^-$ and $x \notin C_1^-$, which is a contradiction. Therefore equality (5.5) holds. Equality (5.6) holds by definition of P^*_{post}. Assume $P_{12} \cap P^*_{post} \neq \emptyset$, then $\exists x \in P_{12} \cap P^*_{post}$, which means $x \in C_1^-$ and $x \notin C_1^-$. Therefore equality (5.7) holds. Equality (5.8) holds for the same reasoning. All other equalities needed for the sub-circuits to be disjoint can be proven analogously.

We will now show that the union of the sub-circuits is Ω. The union of sub-circuits is trivially a subset of Ω. Therefore we have to show that Ω is also a subset of the union of sub-circuits. Assume that $\exists x \in \Omega$ such that x is not in the union of sub-circuits. This means $x \notin P_{pre}$, which means

$x \in \cap C_i^+$. Since $x \notin P_{post}$, we have $x \in \cup C_i^-$, which means that $\exists j$ such that $x \in C_j^-$. Without loss of generality we can assume that $j = 1$ (we can always simple rename the circuits). Since $x \notin P_1^*$ we have $x \in C_2^- \cup C_3^-$. If $x \in C_2^-$ and $x \notin C_3^-$ then $x \in P_{12}$, which is a contradiction. If $x \notin C_2^-$ and $x \in C_3^-$ then $x \in P_{12}$, which is again a contradiction. This means $x \in C_2^-$ and $x \in C_3^-$ which means $x \in \cap C_i^+ \cap C_1^- \cap C_2^- \cap C_3^-$, therefore $x \in P^*$. This is again a contradiction. This means that the union of sub-circuits is Ω.

The quantum circuits is shown in Figure 5.1. We will show that no other wires than the ones shown in Figure 5.1 exist. I.e. for every $i, j, k \in \{1, 2, 3\}$, $i \neq j$, $k \neq j$ the following holds

$$\begin{array}{lll} P_{ij} \nrightarrow P_{kj} \quad (\text{unless } k = i), & P_i^*, P_{ij}, P_{post}^* \nrightarrow P_{pre}^*, & P_i^* \nrightarrow P_j^* \\ P_{jk} \nrightarrow P_i^* \quad (\text{if } j \neq i \neq k), & P_{post}^* \nrightarrow P_i^*, P_{ij}, & P_i^* \nrightarrow P_{jk} \end{array} \tag{5.9}$$

Here $A \nrightarrow B$ denotes that there can be no wire going from A to B. Let A and B be two sub-circuits. $A \to B$ means that $\exists a \in A, b \in B$ such that $a \to b$ i.e. there are events a and b such that b follows a.

Assume $P_j^* \to P_{pre}^*$. This means that $\exists x \in P_j^* \subseteq \cap C_i^+$ and $y \in \Omega \setminus \cap C_i^+$ such that y follows x. This is a contradiction, since $x \in C_i^+, x \to y$ implies $y \in C_i^+$. With the same argument there is also no wire from P_{ij} to P_{pre}^*.

Assume there is a wire $P_{post}^* \to P_{pre}^*$. This means $\exists x \in P_{post} \subseteq \Omega \setminus \cup C_i^-$ and $\exists y \in P_{pre} \subseteq \cup C_i^-$ such that $x \to y$. This is a contradiction, since $y \in C_i^-$, $x \to y$ implies $x \in C_i^-$. This argument for all the other wires in equation (5.9).

In the following we can treat the spacetime circuit as a quantum circuit. If we perform permitted operations on the quantum circuit the result is again a quantum circuit but may not be a spacetime circuit anymore.

5.3 EPR pairs and reprogramming the random oracle

In the following we will analyse the execution of the protocol as a sequence of games. The games are analogous to the games in [9].

Game 1 (Protocol execution)**.** *Pick* $x_1, \ldots, x_r \xleftarrow{\$} \{0,1\}^\ell, \hat{y} \xleftarrow{\$} \{0,1\}^n, H \xleftarrow{\$}$ *Fun where Fun is the set of functions* $\{0,1\}^\ell \to \{0,1\}^n$*. Let* $\theta := H(x_1 \oplus \cdots \oplus x_r)$*. Execute circuit resulting in* y_1, y_2, y_3*. Let accept* $:= 1$ *iff* $y_1 = y_2 = y_3 = \hat{y}$*.*

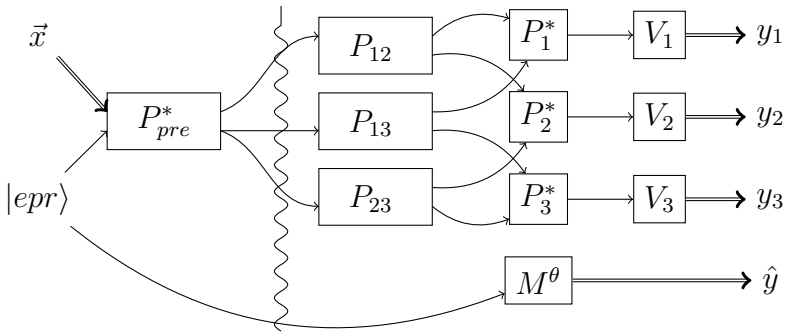


Figure 5.2: Circuit for protocol with 3 receiving verifiers for Game 2.

In the following we will show that $Pr[\text{accept} = 1 : \text{Game 1}] \leq \nu$. Game 2 will delay the choice of $\vec{x}$ by using EPR pairs. Verifiers send first qubits of the EPR paris to the prover and keep the second qubits of the pairs. It's also possible to remove the P^*_{post} circuit without affecting the outcomes y_1, y_2 and y_3.

Game 2 (Using EPR pairs)**.** *Pick* $x_1, \ldots, x_r \xleftarrow{\$} \{0,1\}^\ell, H \xleftarrow{\$} Fun$. *Let* $\theta := H(x_1 \oplus \cdots \oplus x_r)$. *Execute circuit in Figure 5.2 resulting in* y_1, y_2, y_3 *and* $\hat{y}$. *Let accept*$:= 1$ *iff* $y_1 = y_2 = y_3 = \hat{y}$.

In Figure 5.2 we have $|epr\rangle = 2^{-\frac{n}{2}} \sum_{x \in \{0,1\}^n} |x\rangle \otimes |x\rangle$. The upper wire from $|epr\rangle$ carries the first n qubits and the lower wire the last n qubits. The gate M^θ measures n qubits in bases $\theta \in \{0,1\}^n$.

We have $Pr[\text{accept} = 1 : \text{Game 1}] = Pr[\text{accept} = 1 : \text{Game 2}]$ since preparing $X = |y\rangle_\theta$ for a random $y \in \{0,1\}$ is perfectly indistinguishable from preparing an EPR pair XY and measuring Y in basis θ.

The next step is to reprogram the random oracle. This means that the basis θ will not be calculated as $H(x_1 \otimes \cdots \otimes x_r)$ but at some point in time H is reprogrammed to return $H(x_1 \otimes \cdots \otimes x_r) = \theta$. The idea behind this is that up to a certain point in time the probability that someone tries to query $H(x_1 \otimes \cdots \otimes x_r)$ is negligible. This means that with high probability the adversary won't notice that the random oracle has been reprogrammed, which makes it possible to delay the choice of the basis.

The random oracle will be reprogrammed just after P^*_{pre}. The time of reprogramming is illustrated in Figure 5.2 with a wiggly line. It makes sense to reprogram the oracle at this time, as all gates in P^*_{pre} are outside of $\cap C_i^+$, which means that there is no point in spacetime left of the wiggly line where all x_i are known. To show that this indeed holds Lemma 5.2 is used.

Lemma 5.2. *[9] Let $H : \{0,1\}^\ell \to \{0,1\}^n$ be a random oracle. Let (A_1, A_2) be oracle algorithms sharing state between invocations that perform at most q queries to H. Let C_1 be an oracle algorithm that on input (j, x) does the following: Run $A_1^H(x)$ till the j-th query to H, then measure the argument of that query in the computational basis, and output the measurement outcome. (Or $\perp$ if no j-th query occurs.) Let*

$$\begin{aligned}
P_A^1 &:= Pr[b' = 1 : H \xleftarrow{\$} (\{0,1\}^l \to \{0,1\}^n), x \leftarrow \{0,1\}^\ell, \\
&\qquad A_1^H(x), b' \leftarrow A_2^H(x, H(x))] \\
P_A^2 &:= Pr[b' = 1 : H \xleftarrow{\$} (\{0,1\}^l \to \{0,1\}^n), x \leftarrow \{0,1\}^\ell, \\
&\qquad B \xleftarrow{\$} \{0,1\}^n, A_1^H(x), H(x) := B, b \leftarrow A_2^H(x, B)] \\
P_C &:= Pr[x = x' : H \xleftarrow{\$} (\{0,1\}^l \to \{0,1\}^n), x \leftarrow \{0,1\}^\ell, \\
&\qquad j \xleftarrow{\$} \{1, \ldots, q\}, x' \leftarrow C_1 H(j, x)]
\end{aligned}$$

Then $|P_A^1 - P_A^2| \leq 2^q \sqrt{P_C}$.

We now take $A_1^H(x)$ to be the machine that executes the circuit in Figure 4.3 until the wiggly line. Let B be θ. And let $A_2^H(x, B)$ be the oracle machine, that takes in the oracle state from A_1^H and executes the part of the circuit left of the wiggly line with the reprogrammed oracle. A_2^H returns 1 if $y_1 = y_2 = y_3 = \hat{y}$. By construction we have $P_A^1 = Pr[\text{accept} = 1 : \text{ Game 2}]$ and $P_A^2 = Pr[\text{accept} = 1 : \text{ Game 3}]$ for the following game

Game 3 (Reprogramming H)**.** *Pick $x_1, \ldots, x_r \xleftarrow{\$} \{0,1\}^\ell, H \xleftarrow{\$} Fun$. Execute circuit from Figure 5.2 until the wiggly line (with oracle access to H). Pick $\theta \xleftarrow{\$} \{0,1\}^n$. Execute the circuit after the wiggly line (with oracle access to modified H with $H(x) := \theta$) resulting in $y_1, y_2, y_3, \hat{y}$. Let accept:= 1 iff $y_1 = y_2 = y_3 = \hat{y}$.*

P_C from lemma 5.2 can be expressed as $P_C = Pr[x' = x_1 \oplus \cdots \oplus x_r : \text{ Game 4}]$ for game

Game 4 (Guessing $x = x_1 \oplus \cdots \oplus x_r$)**.** *Pick $x_1, \ldots, x_r \xleftarrow{\$} \{0,1\}^\ell, H \xleftarrow{\$} Fun, j \xleftarrow{\$} \{1, \ldots, q\}$. Prepare $|epr\rangle$ and execute circuit P_{pre}^* until the j-th query to H. Measure the argument x' of that query.*

Lemma 5.2 then says $|P_A^1 - P_A^2| \leq 2q\sqrt{P_C}$, wich means

$$\begin{aligned}
&|Pr[\text{accept} = 1 : \text{ Game 2}] - Pr[\text{accept} = 1 : \text{ Game 3}]| \\
&\leq 2q\sqrt{Pr[x' = x_1 \oplus \cdots \oplus x_r : \text{ Game 4}]}
\end{aligned}$$

5.4 Monogamy game

We will now look at Game 3. Sub-circuits P_{12}, P_{13} and P_{23} prepare the state for P_1^* and P_2^* for P_1^* and P_3^* and for P_2^* and P_3^* respectively. Let M_A^θ, M_B^θ and M_C^θ refer to the measurements consisting of P_1^* and V_1, of P_2^* and V_2 and of P_3^* and V_3 respectively. Then P_{12}, P_{13} and P_{23} can be modelled as unitary operators AB^θ, BC^θ and AC^θ. This way we get three measurements

$$(AB^\theta AC^\theta)^\dagger M_A^\theta (AB^\theta AC^\theta),$$
$$(AB^\theta BC^\theta)^\dagger M_B^\theta (AB^\theta BC^\theta)$$

and

$$(AC^\theta BC^\theta)^\dagger M_C^\theta (AC^\theta BC^\theta).$$

We again somewhat abuse the notation here as for an operator A on space $\mathcal{H}_A$ we still write A if the underlying space becomes $\mathcal{H}_A \otimes \mathcal{H}_B$, although it would be correct to write $A \otimes 1_B$.

Performing the conjugate transpose of the unitary operators after the measurement won't change the outcome, but will ensure that the measurements remain projective if M_i^θ is projective. Performing all the measurements is equivalent to

$$\begin{aligned}(AB^\theta AC^\theta)^\dagger M_A^\theta (AB^\theta AC^\theta)(AB^\theta BC^\theta)^\dagger M_B^\theta (AB^\theta BC^\theta)(AC^\theta BC^\theta)^\dagger M_C^\theta (AC^\theta BC^\theta) \\ = (AB^\theta AC^\theta BC^\theta)^\dagger (M_A^\theta M_B^\theta M_C^\theta)(AB^\theta AC^\theta BC^\theta).\end{aligned}$$

Without loss of generality we can assume that M_A^θ, M_B^θ and M_C^θ are projective and ψ is a pure state [6].

Game 5 (Monogamy game)**.** *Prepare state* $|\psi\rangle$*. Pick* $\theta \xleftarrow{\$} \{1, \ldots, n\}$*. Perform measurements* $(AB^\theta AC^\theta)^\dagger M_A^\theta (AB^\theta AC^\theta)$*,* $(AB^\theta BC^\theta)^\dagger M_B^\theta (AB^\theta BC^\theta)$*,* $(AC^\theta BC^\theta)^\dagger M_C^\theta (AC^\theta BC^\theta)$ *and* M_F^θ *resulting in* y_1, y_2, y_3 *and* $\hat{y}$*. Accept if* $y_1 = y_2 = y_3 = \hat{y}$*.*

As we see Game 5 is a n times parallelly repeated MG6 game. Therefore

$$Pr[\text{accept} := 1 : \text{ Game 3}] \leq P_{win}(MG6^n).$$

5.5 Guessing x

We will now define what it means to guess x in Game 4. Execution of Game 4 will perform $j \in \{1, \ldots, q\}$ queries to the oracle. We want to show that

the probability of one of these queries being $H(x_1 \oplus \cdots \oplus x_r)$ is low. We can look at every query as a separate gate in P^*_{pre}. Let E_i be the event at which the gate of performing the i-th query is located. Since $P^*_{pre} \subset \Omega \setminus (\cap C^+_i)$ we have that for every E_i there is a $k \in \{1, \ldots, r\}$ such that $E_i \notin C^+_k$. This means that x_k is not known to E_i. We can now partition the set $\{1, \ldots, q\}$ into disjoint subsets J_k, $k \in \{1, \ldots, q\}$ such that for every $i \in J_k$ we have $E_i \notin C^+_k$.

Let Game 4_i be like Game 4, which the only difference that j is not chosen form $\{1, \ldots, q\}$ but from J_i. We can then express Game 4 as follows

$$Pr[x' = x_1 \oplus \cdots \oplus x_r : \text{ Game 4}] = \sum_{i=1}^{r} \frac{|J_i|}{q} Pr[x' = x_1 \oplus \cdots \oplus x_r : \text{ Game } 4_i].$$

For every $i \in \{1, \ldots, q\}$ we not divide P^*_{pre} into two subcircuits P^i_{low} and P^i_{high}. Let P^i_{low} be the subcircuit that has no access to x_i and P^i_{high} the subcircuit that has access to x_i. Executing circuit P^*_{pre} is equivalent to first executing circuit P^i_{low} and then executing circuit P^i_{high}. Notice that for every $j \in J_i$ measuring the j-th query of P^*_{pre} is equivalent to measuring the j-th query of P^i_{low}, since E_j is outside of C^+_i. Therefore Game 4_i is equivalent to the following Game 6_i

Game 6_i (Executing P^i_{low} only)**.** *Pick* $x_1, \ldots, x_r \xleftarrow{\$} \{0,1\}^\ell, H \xleftarrow{\$} Fun, j \xleftarrow{\$} J_i$. *Prepare* $|epr\rangle$ *and execute circuit* P^i_{low} *until the* j*-th query to* H. *Measure the argument* x' *of that query.*

We have $Pr[x' = x_1 \oplus \cdots \oplus x_r : \text{ Game } 4_i] = Pr[x' = x_1 \oplus \cdots \oplus x_r : \text{ Game } 6_i]$. Since x_i cannot be accessed in P^i_{low} we have that in Game 6_i x_i is randomly chosen and never accessed. This leads to $Pr[x' = x_1 \oplus \cdots \oplus x_r : \text{ Game } 6_i] \leq 2^{-\ell}$. Therefore

$$\begin{aligned} Pr[x' = x_1 \oplus \cdots \oplus x_r : \text{ Game 4}] &= \sum_{i=1}^{r} \frac{|J_i|}{q} Pr[x' = x_1 \oplus \cdots \oplus x_r : \text{ Game } 4_i] \\ &\leq \sum_{i=1}^{r} \frac{|J_i|}{q} 2^{-\ell} = 2^{-\ell}. \end{aligned}$$

This means

$$Pr[\text{accept} = 1 : \text{ Game 1}] \leq P_{win}(MG6^n) + 2q2^{-l/2} = \nu.$$

□

6. Conclusion

With the intention to increase the precision of the position verification protocol form [9] we defined a modified position verification protocol and showed that it is sound for a smaller region than the original protocol if the winning probability $P_{win}(MG6^n)$ is small. We were not able to prove the monogamy game theorem for MG6, but described our progress and the intuitive idea behind the proof attempt. This means that proving the MG6 theorem remains an open question. We also compared different three player monogamy games and gave some results about their winning probabilities.

If the proof of MG6 works out using [7] then the next step would be to generalise Theorem 1 in [7] to $n \geq 1$. If this would not give a probability that declines fast with growing n, then one would have to use the 1 qubit monogamy game and repeat the position verification protocol. This way we get a small bound for the soundness but also increase the round complexity of the protocol.

The position verification theorem from [9] includes a possible error rate as well. This is something we haven't considered in the monogamy games presented in Chapter 3. It is also not very clear how this can be done using Theorem 1 form [7] since this theorem is only usable if the probability of the adversary guessing the correct result is rather high.

Currently we looked into three-player monogamy games. To achieve the highest precision in 3D we would need four-player monogamy games and a protocol with four receiving verifiers. This was out of the scope of this theses. If the proof for MG6 works out as intended, then it should be possible to generalise it to four adversaries.

In [9] it was shown that the proof of the position verification theorem introduced in [2] does not hold in higher dimensions than 1D. Proof of this theorem for 2D was shown in personal communication between Dominique Unruh and Serge Fehr [10]. The generalised monogamy game MG6 might be useful in the 3D case.

Appendices

A. Proof of MG4 theorem

Proof. Let y_x be the measurement outcome on $\mathcal{H}_x$. Then $P_{win}(G,S) = Pr(y_F = y_{AB} = y_{BC} = y_{AC})$. We can calculate

$$
\begin{aligned}
&Pr(y_F = y_{AB} = y_{BC} = y_{AC}) = \\
&\quad = \sum_\theta \frac{1}{|\Theta|} Pr(y_F = y_{AB} = y_{BC} = y_{AC}|\theta) \\
&\quad = \sum_\theta \frac{1}{|\Theta|} \sum_x Pr(y_F = x \wedge y_{AB} = x \wedge y_{BC} = x \wedge y_{AC} = x|\theta) \\
&\quad = \sum_\theta \frac{1}{|\Theta|} \sum_x Pr(y_F = x|y_{AB} = x \wedge y_{BC} = x \wedge y_{AC} = x \wedge \theta) \\
&\qquad\qquad Pr(y_{AB} = x \wedge y_{BC} = x \wedge y_{AC} = x|\theta) \\
&\quad = \sum_\theta \frac{1}{|\Theta|} \sum_x Pr(y_F = x|y_{AB} = x \wedge y_{BC} = x \wedge y_{AC} = x \wedge \theta) \\
&\qquad\qquad Pr(y_{AB} = x|y_{BC} = x \wedge y_{AC} = x \wedge \theta) Pr(y_{BC} = x \wedge y_{AC} = x|\theta) \\
&\quad = \sum_\theta \frac{1}{|\Theta|} \sum_x Pr(y_F = x|y_{AB} = x \wedge y_{BC} = x \wedge y_{AC} = x \wedge \theta) \\
&\qquad\qquad Pr(y_{AB} = x|y_{BC} = x \wedge y_{AC} = x \wedge \theta) Pr(y_{BC} = x|y_{AC} = x \wedge \theta) Pr(y_{AC} = x|\theta).
\end{aligned}
$$

For fixed x and θ let us define

$$
\begin{aligned}
P_F &= Pr(y_F|y_{AB} = x \wedge y_{BC} = x \wedge y_{AC} = x \wedge \theta) \\
P_{AB} &= Pr(y_{AB} = x|y_{BC} = x \wedge y_{AC} = x \wedge \theta) \\
P_{BC} &= Pr(y_{BC} = x|y_{AC} = x \wedge \theta) \\
P_{AC} &= Pr(y_{AC} = x|\theta)
\end{aligned}
$$

And let $|s_{AB}\rangle$ be the quantum state after measurement AB, $|s_{BC}\rangle$ the quantum state after the measurement BC and $|s_{AC}\rangle$ the quantum state after the

measurement AC. Then we have

$$|s_{AC}\rangle = \frac{(1_F \otimes AC_x^\theta \otimes 1_B)|\rho\rangle}{\sqrt{\langle\rho|1_F \otimes AC_x^\theta \otimes 1_B|\rho\rangle}} = \frac{1}{\sqrt{P_{AC}}}(1_F \otimes AC_x^\theta \otimes 1_B)|\rho\rangle$$

$$|s_{BC}\rangle = \frac{(1_F \otimes 1_A \otimes BC_x^\theta)|s_{AC}\rangle}{\sqrt{\langle s_{AC}|1_F \otimes 1_A \otimes BC_x^\theta|s_{AC}\rangle}} = \frac{1}{\sqrt{P_{BC}}}(1_F \otimes 1_A \otimes BC_x^\theta)|s_{AC}\rangle$$

$$|s_{AB}\rangle = \frac{(1_F \otimes AB_x^\theta \otimes 1_C)|s_{BC}\rangle}{\sqrt{\langle s_{BC}|1_F \otimes AB\theta_x \otimes 1_C|s_{BC}\rangle}} = \frac{1}{\sqrt{P_{AB}}}(1_F \otimes AB_x^\theta \otimes 1_C)|s_{BC}\rangle$$

$$= \frac{1}{\sqrt{P_{AB}P_{BC}}}(1_F \otimes (AB_x^\theta \otimes 1_C)(1_A \otimes BC_x^\theta))|s_{AC}\rangle$$

$$= \frac{1}{\sqrt{P_{AB}P_{BC}P_{AC}}}(1_F \otimes (AB_x^\theta \otimes 1_C)(1_A \otimes BC_x^\theta)(AC_x^\theta \otimes 1_B))|\rho\rangle$$

Using this we get

$$P_F = \langle s_{AC}|F_x^\theta \oplus 1_{ABC}|s_{AC}\rangle$$

$$= \frac{1}{P_{AB}P_{BC}P_{AC}}\langle\rho|(1_F \otimes ((AB_x^\theta \otimes 1_C)(AC_x^\theta \otimes 1_B)(1_A \otimes BC_x^\theta)))^\dagger F_x^\theta \otimes 1_{ABC}$$
$$(1_F \otimes ((AB_x^\theta \otimes 1_C)(AC_x^\theta \otimes 1_B)(1_A \otimes BC_x^\theta))|\rho\rangle$$

$$= \frac{1}{P_{AB}P_{BC}P_{AC}}\langle\rho|(1_F \otimes (1_A \otimes BC_x^\theta)(AC_x^\theta \otimes 1_B)(AB_x^\theta \otimes 1_C))(F_x^\theta \otimes 1_{ABC})$$
$$(1_F \otimes (AB_x^\theta \otimes 1_C)(AC_x^\theta \otimes 1_B)(1_A \otimes BC_x^\theta))|\rho\rangle$$

Using the third commutative property we get

$$P_F = \frac{1}{P_{AB}P_{BC}P_{AC}}\langle\rho|1_F \otimes (AB_x^\theta \otimes 1_C)(AC_x^\theta \otimes 1_B)(1_A \otimes BC_x^\theta)|\rho\rangle$$

Therefore

$$P_F P_{AB}P_{BC}P_{AC} = \langle\rho|1_F \otimes (AB_x^\theta \otimes 1_C)(AC_x^\theta \otimes 1_B)(1_A \otimes BC_x^\theta)|\rho\rangle$$

And we have

$$Pr(y_F = y_{AB} = y_{BC} = y_{AC}) =$$
$$= \sum_\theta \frac{1}{|\Theta|}\sum_x \langle\rho|F_x^\theta \otimes (AB_x^\theta \otimes 1_C)(AC_x^\theta \otimes 1_B)(1_A \otimes BC_x^\theta)|\rho\rangle$$

Now following the proof of theorem 3 in [6] let us denote $\Pi^\theta = \sum_x 1_F \otimes (AB_x^\theta \otimes 1_C)(AC_x^\theta \otimes 1_B)(1_A \otimes BC_x^\theta)$. Then $p_{win}(G,S) = \sum_\theta \frac{1}{|\Theta|}\langle\rho|\Pi^\theta|\rho\rangle =$

$\sum_\theta \frac{1}{|\Theta|} tr(\Pi^\theta|\rho\rangle\langle\rho|)$. From the definition of the norm we have $tr(\Pi^\theta|\rho\rangle\langle\rho|) \leq \|\Pi^\theta\|$. Using Lemma 2 from [6] we have

$$p_{win}(G,S) = \sum_\theta \frac{1}{2^n} tr(\Pi^\theta|\rho\rangle\langle\rho|) \leq \frac{1}{2^n}\|\sum_\theta \Pi^\theta\| \leq \frac{1}{2^n}\sum_k \max_\theta \|\Pi^\theta \Pi^{\pi^k(\theta)}\|.$$

Optimal permutations π^k are determined later. We will now bound the norm $\|\Pi^\theta \Pi^{\theta'}\|$, where $\theta' = \pi^k(\theta)$. For fixed θ and k, we denote by τ the set of indices where θ and θ' differ. By τ^c we denote its complement and by t the Hamming distance between θ and θ', which means $|\tau| = t$. Now we define the following projectors:

$$\bar{P} = \sum_x |x_\tau^\theta\rangle\langle x_\tau^\theta| \otimes 1_{\tau^c} \otimes (AC_x^\theta \otimes 1_B)(1_A \otimes BC_x^\theta)$$

and

$$\bar{Q} = \sum_x |x_\tau^{\theta'}\rangle\langle x_\tau^{\theta'}| \otimes 1_{\tau^c} \otimes AB_x^{\theta'} \otimes 1_C$$

Now we will show that $\Pi^\theta \leq \bar{P}$ and $\Pi^{\theta'} \leq \bar{Q}$. Recall that $A \leq B$ if $B - A$ is positive semi-definite. We know that for any matrix C, $C^\dagger C$ is positive semi-definite. Therefore we will show that $(\bar{P} - \Pi^\theta)(\bar{P} - \Pi^\theta) = (\bar{P} - \Pi^\theta)$ and $(\bar{Q} - \Pi^{\theta'})(\bar{Q} - \Pi^{\theta'}) = (\bar{Q} - \Pi^{\theta'})$.

$$\begin{aligned}
\bar{Q} - \Pi^{\theta'} &= \sum_x |x_\tau^{\theta'}\rangle\langle c_\tau^{\theta'}| \otimes 1_{\tau^c} \otimes AB_x^{\theta'} \otimes 1_C \\
&\quad - \sum_x |x^{\theta'}\rangle\langle x^{\theta'}| \otimes (AB_x^{\theta'} \otimes 1_C)(AC_x^{\theta'} \otimes 1_B)(1_A \otimes BC_x^{\theta'}) \\
&= \sum_x |x_\tau^{\theta'}\rangle\langle x_\tau^{\theta'}| \otimes \Big[\Big((1_{\tau^c} \otimes (AB_x^{\theta'} \otimes 1_C)\Big) \\
&\quad - \Big(|x_{\tau^c}^{\theta'}\rangle\langle x_{\tau^c}^{\theta'}| \otimes (AB_x^{\theta'} \otimes 1_C)(AC_x^{\theta'} \otimes 1_B)(1_A \otimes BC_x^{\theta'}))\Big)\Big] \\
&= \sum_x |x_\tau^{\theta'}\rangle\langle x_\tau^{\theta'}| \otimes \Big[\Big(1_{\tau^c} \otimes (AB_x^{\theta'} \otimes 1_C)\Big) \\
&\quad - \Big(1_{\tau^c} \otimes (AB_x^{\theta'} \otimes 1_C)\Big)\Big(|x_{\tau^c}^{\theta'}\rangle\langle x_{\tau^c}^{\theta'}| \otimes (AC_x^{\theta'} \otimes 1_B)(1_A \otimes BC_x^{\theta'})\Big)\Big] \\
&= \sum_x |x_\tau^{\theta'}\rangle\langle x_\tau^{\theta'}| \otimes \Big(1_{\tau^c} \otimes (AB_x^{\theta'} \otimes 1_C)\Big) \\
&\quad \Big(1_{\tau^c} \otimes 1_{ABC} - |x_{\tau^c}^{\theta'}\rangle\langle x_{\tau^c}^{\theta'}| \otimes (AC_x^{\theta'} \otimes 1_B)(1_A \otimes BC_x^{\theta'})\Big)
\end{aligned}$$

Now let us calculate the product:

$$
\begin{aligned}
&(\bar{Q}-\Pi^{\theta'})(\bar{Q}-\Pi^{\theta'}) = \\
&\quad = \sum_x |x_\tau^{\theta'}\rangle\langle x_\tau^{\theta'}| \otimes \Big(1_{\tau^c} \otimes (AB_x^{\theta'} \otimes 1_C)\Big) \\
&\qquad \Big(1_{\tau^c} \otimes 1_{ABC} - |x_{\tau^c}^{\theta'}\rangle\langle x_{\tau^c}^{\theta'}| \otimes (AC_x^{\theta'} \otimes 1_B)(1_A \otimes BC_x^{\theta'})\Big) \\
&\quad \sum_y |y_\tau^{\theta'}\rangle\langle y_\tau^{\theta'}| \otimes \Big(1_{\tau^c} \otimes (AB_y^{\theta'} \otimes 1_C)\Big) \\
&\qquad \Big(1_{\tau^c} \otimes 1_{ABC} - |y_{\tau^c}^{\theta'}\rangle\langle y_{\tau^c}^{\theta'}| \otimes (AC_y^{\theta'} \otimes 1_B)(1_A \otimes BC_y^{\theta'})\Big) \\
&\quad = \sum_{xy} |x_\tau^{\theta'}\rangle\langle x_\tau^{\theta'}|y_\tau^{\theta'}\rangle\langle y_\tau^{\theta'}| \otimes \Big(\\
&\qquad (1_{\tau^c} \otimes AB_x^{\theta'} \otimes 1_C)(1_{\tau^c} \otimes 1_{ABC} - |x_{\tau^c}^{\theta'}\rangle\langle x_{\tau^c}^{\theta'}| \otimes (AC_x^{\theta'} \otimes 1_B)(1_A \otimes BC_x^{\theta'})) \\
&\qquad (1_{\tau^c} \otimes AB_y^{\theta'} \otimes 1_C)(1_{\tau^c} \otimes 1_{ABC} - |y_{\tau^c}^{\theta'}\rangle\langle y_{\tau^c}^{\theta'}| \otimes (AC_y^{\theta'} \otimes 1_B)(1_A \otimes BC_y^{\theta'})\Big) \\
&\quad = \sum_x |x_\tau^{\theta'}\rangle\langle x_\tau^{\theta'}| \ \otimes \Big(\\
&\qquad (1_{\tau^c} \otimes AB_x^{\theta'} \otimes 1_C)(1_{\tau^c} \otimes 1_{ABC} - |x_{\tau^c}^{\theta'}\rangle\langle x_{\tau^c}^{\theta'}| \otimes (AC_x^{\theta'} \otimes 1_B)(1_A \otimes BC_x^{\theta'})) \\
&\qquad (1_{\tau^c} \otimes AB_x^{\theta'} \otimes 1_C)(1_{\tau^c} \otimes 1_{ABC} - |x_{\tau^c}^{\theta'}\rangle\langle x_{\tau^c}^{\theta'}| \otimes (AC_x^{\theta'} \otimes 1_B)(1_A \otimes BC_x^{\theta'})\Big)
\end{aligned}
$$

Using the third commutative property we have

$$
\begin{aligned}
&(\bar{Q}-\Pi^{\theta'})(\bar{Q}-\Pi^{\theta'}) = \\
&\quad = \sum_x |x_\tau^{\theta'}\rangle\langle x_\tau^{\theta'}| \ \otimes \Big((1_{\tau^c} \otimes AB_x^{\theta'} \otimes 1_C)(1_{\tau^c} \otimes AB_x^{\theta'} \otimes 1_C) \\
&\qquad (1_{\tau^c} \otimes 1_{ABC} - |x_{\tau^c}^{\theta'}\rangle\langle x_{\tau^c}^{\theta'}| \otimes (AC_x^{\theta'} \otimes 1_B)(1_A \otimes BC_x^{\theta'})) \\
&\qquad (1_{\tau^c} \otimes 1_{ABC} - |x_{\tau^c}^{\theta'}\rangle\langle x_{\tau^c}^{\theta'}| \otimes (AC_x^{\theta'} \otimes 1_B)(1_A \otimes BC_x^{\theta'})\Big) \\
&\quad = \sum_x |x_\tau^{\theta'}\rangle\langle x_\tau^{\theta'}| \ \otimes \Big((1_{\tau^c} \otimes AB_x^{\theta'} \otimes 1_C) \\
&\qquad (1_{\tau^c} \otimes 1_{ABC} - |x_{\tau^c}^{\theta'}\rangle\langle x_{\tau^c}^{\theta'}| \otimes (AC_x^{\theta'} \otimes 1_B)(1_A \otimes BC_x^{\theta'})) \\
&\qquad (1_{\tau^c} \otimes 1_{ABC} - |x_{\tau^c}^{\theta'}\rangle\langle x_{\tau^c}^{\theta'}| \otimes (AC_x^{\theta'} \otimes 1_B)(1_A \otimes BC_x^{\theta'})\Big)
\end{aligned}
$$

Now notice that if we have two operators 1 and A, where 1 is the identity operator and A is a projector. Then

$$(1-A)(1-A) = 1 - A - A + A = 1 - A$$

Using this property we have that

$$\begin{aligned}(\bar{Q}-\Pi^{\theta'})(\bar{Q}-\Pi^{\theta'}) &= \sum_x |x_\tau^{\theta'}\rangle\langle x_\tau^{\theta'}| \otimes \Big((1_{\tau^c}\otimes AB_x^{\theta'}\otimes 1_C) \\ &\qquad (1_{\tau^c}\otimes 1_{ABC} - |x_{\tau^c}^{\theta'}\rangle\langle x_{\tau^c}^{\theta'}|\otimes (AC_x^{\theta'}\otimes 1_B)(1_A\otimes BC_x^{\theta'}))\Big) \\ &= \bar{Q}-\Pi^{\theta'}.\end{aligned}$$

Therefore $\bar{Q}-\Pi^{\theta'}$ is positive semi-definite, which gives us $\Pi^{\theta'}\leq\bar{Q}$. Analogously we also have $\Pi^{\theta}\leq\bar{P}$.

Now since $\Pi^{\theta}\leq\bar{P}$ and $\Pi^{\theta'}\leq\bar{Q}$ we can bound $\|\Pi^{\theta}\Pi^{\theta'}\|^2\leq\|\bar{P}\bar{Q}\|^2 = \|\bar{P}\bar{Q}\bar{P}\|$ using Lemma 1.2. We now bound the norm $\|\bar{P}\bar{Q}\bar{P}\|$.

$$\begin{aligned}\bar{P}\bar{Q}\bar{P} &= \sum_{xyz}|x_\tau^\theta\rangle\langle x_\tau^\theta|y_\tau^{\theta'}\rangle\langle y_\tau^{\theta'}|z_\tau^\theta\rangle\langle z_\tau^\theta|\otimes 1_{\tau^c}\otimes(AC_x^\theta\otimes 1_B)(1_A\otimes BC_x^\theta)(AB_y^{\theta'}\otimes 1_C) \\ &\qquad (AC_z^\theta\otimes 1_B)(1_A\otimes BC_z^\theta) \\ &= \sum_{xyz}|x_\tau^\theta\rangle\langle x_\tau^\theta|y_\tau^{\theta'}\rangle\langle y_\tau^{\theta'}|z_\tau^\theta\rangle\langle z_\tau^\theta|\otimes 1_{\tau^c}\otimes(AB_y^{\theta'}\otimes 1_C)(AC_x^\theta\otimes 1_B)(1_A\otimes BC_x^\theta) \\ &\qquad (AC_z^\theta\otimes 1_B)(1_A\otimes BC_z^\theta) \\ &= \sum_{xy}|x_\tau^\theta\rangle\langle x_\tau^\theta|y_\tau^{\theta'}\rangle\langle y_\tau^{\theta'}|x_\tau^\theta\rangle\langle x_\tau^\theta|\otimes 1_{\tau^c}\otimes(AB_y^{\theta'}\otimes 1_C)(AC_x^\theta\otimes 1_B)(1_A\otimes BC_x^\theta) \\ &= \sum_{xy}|\langle x_\tau^\theta|y_\tau^{\theta'}\rangle|^2|x_\tau^\theta\rangle\langle x_\tau^\theta|\otimes 1_{\tau^c}\otimes(AB_y^{\theta'}\otimes 1_C)(AC_x^\theta\otimes 1_B)(1_A\otimes BC_x^\theta) \\ &= 2^{-t}\sum_x|x_\tau^\theta\rangle\langle x_\tau^\theta|\otimes 1_{\tau^c}\otimes(AC_x^\theta\otimes 1_B)(1_A\otimes BC_x^\theta).\end{aligned}$$

Here we used that the operators fulfil the third commutative property, $AC_x^\theta AC_z^\theta=\delta_{xz}AC_x^\theta$ and $|\langle x_\tau^\theta|y_\tau^{\theta'}\rangle|^2=2^{-t}$. This means that $\|\bar{P}\bar{Q}\bar{P}\|\leq 2^{-t}$. When choosing the permutations the same way as in [6] we get

$$p_{win}(G,S)\leq\frac{1}{2^n}\sum_k\max_\theta\|\Pi^\theta\Pi^{\pi^k(\theta)}\|\leq\frac{1}{2^n}\sum_{t=0}^n\binom{n}{t}\left(\frac{1}{\sqrt{2}}\right)^t=\left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right)^n.$$

□

B. Another proof of MG7 theorem

For the proof we will again follow the proof of Theorem 3 in [6]. Where useful for a transformation X on $\mathcal{H}_X$ we will use the same name X if the transformation is carried out on $\mathcal{H}_X \otimes \mathcal{H}_Y$ instead of $X \otimes 1_Y$, if the affected space is clear from the context.

Let us denote

$$\Pi^\theta = \sum_x 1_F \otimes \left((AB^\theta \otimes AC^\theta \otimes BC^\theta)^\dagger A_x^\theta \otimes B_x^\theta \otimes C_x^\theta (AB^\theta \otimes AC^\theta \otimes BC^\theta) \right).$$

Then

$$P_{win}(G,S) = \sum_\theta \frac{1}{|\Theta|} \langle s|\Pi^\theta|s\rangle = \sum_\theta \frac{1}{|\Theta|} tr(\Pi^\theta |s\rangle\langle s|).$$

From the definition of the norm we have $tr(\Pi^\theta |s\rangle\langle s|) \leq \|\Pi^\theta\|$. Using Lemma 2 from the article we have

$$P_{win}(G,S) = \sum_\theta \frac{1}{2^n} tr(\Pi^\theta |s\rangle\langle s|) \leq \frac{1}{2^n} \|\sum_\theta \Pi^\theta\| \leq \frac{1}{2^n} \sum_k \max_\theta \|\Pi^\theta \Pi^{\pi^k(\theta)}\|.$$

Optimal permutations π^k are determined later. We will now bound the norm $\|\Pi^\theta \Pi^{\theta'}\|$, where $\theta' = \pi^k(\theta)$. For fixed θ and k, we denote by τ the set of indices where θ and θ' differ. By τ^c we denote its complement and by t the Hamming distance between θ and θ', which means $|\tau| = t$. Now we define the following projectors:

$$P = \sum_x |x_\tau^\theta\rangle\langle x_\tau^\theta| \otimes 1_{\tau^C} \otimes (AC^\theta \otimes BC^\theta)^\dagger C_x^\theta (AC^\theta \otimes BC^\theta)$$

$$Q = \sum_x |x_\tau^{\theta'}\rangle\langle x_\tau^{\theta'}| \otimes 1_{\tau^C} \otimes (AB^{\theta'} \otimes AC^{\theta'})^\dagger A_x^{\theta'} (AB^{\theta'} \otimes AC^{\theta'})$$

$$R = \sum_x |x_\tau^\theta\rangle\langle x_\tau^\theta| \otimes 1_{\tau^C} \otimes (AB^\theta \otimes BC^\theta)^\dagger B_x^\theta (AB^\theta \otimes BC^\theta).$$

In the following we will show that $\Pi < P$, for this we show that $P - \Pi$ is positive semi definite. First we calculate $P - \Pi$.

$$\begin{aligned}
P - \Pi = \sum_x |x_\tau\rangle\langle x_\tau| \otimes \big[&(1_{\tau^C} \otimes (AC^\theta \otimes BC^\theta)^\dagger C_x^\theta (AC^\theta \otimes BC^\theta)) \\
&-|x_{\tau^C}\rangle\langle x_{\tau^C}| \otimes (AB^\theta \otimes BC^\theta \otimes AC^\theta)^\dagger (A_x^\theta \otimes B_x^\theta \otimes C_x^\theta)(AB^\theta \otimes BC^\theta \otimes AC^\theta)\big] \\
= \sum_x |x_\tau\rangle\langle x_\tau| \otimes &(1_{\tau^C} \otimes AC^{\theta\dagger} \otimes BC^{\theta\dagger}) \Big(1_{\tau^C} \otimes C_x^\theta \\
&-|x_{\tau^C}\rangle\langle x_{\tau^C}| \otimes (AB^{\theta\dagger})(A_x^\theta \otimes B_x^\theta \otimes C_x^\theta)(AB^\theta)\Big) (1_{\tau^C} \otimes AC^\theta \otimes BC^\theta)
\end{aligned}$$

In the following we will calculate $(P - \Pi)(P - \Pi)$ if the product is equal to $P - \Pi$ then Lemma 1.1 says that $P - \Pi$ is positive semi-definite.

$$\begin{aligned}
&(P - \Pi)(P - \Pi) = \\
&= \Bigg[\sum_x |x_\tau\rangle\langle x_\tau| \otimes (1_{\tau^C} \otimes AC^{\theta\dagger} \otimes BC^{\theta\dagger}) \Big(1_{\tau^C} \otimes C_x^\theta \\
&\qquad -|x_{\tau^C}\rangle\langle x_{\tau^C}| \otimes (AB^{\theta\dagger})(A_x^\theta \otimes B_x^\theta \otimes C_x^\theta)(AB^\theta)\Big) (1_{\tau^C} \otimes AC^\theta \otimes BC^\theta)\Bigg] \\
&\quad \cdot \Bigg[\sum_y |y_\tau\rangle\langle y_\tau| \otimes (1_{\tau^C} \otimes AC^{\theta\dagger} \otimes BC^{\theta\dagger}) \Big(1_{\tau^C} \otimes C_y^\theta \\
&\qquad -|y_{\tau^C}\rangle\langle y_{\tau^C}| \otimes (AB^{\theta\dagger})(A_y^\theta \otimes B_y^\theta \otimes C_y^\theta)(AB^\theta)\Big) (1_{\tau^C} \otimes AC^\theta \otimes BC^\theta)\Bigg] \\
&= \sum_x \sum_y |x_\tau\rangle\langle x_\tau|y_\tau\rangle\langle y_\tau| \otimes \Bigg[(1_{\tau^C} \otimes AC^{\theta\dagger} \otimes BC^{\theta\dagger}) \Big(1_{\tau^C} \otimes C_x^\theta
\end{aligned}$$

$$
\begin{aligned}
&\quad -|x_{\tau^C}\rangle\langle x_{\tau^C}| \otimes (AB^{\theta^\dagger})(A_x^\theta \otimes B_x^\theta \otimes C_x^\theta)(AB^\theta)\Big)\,(1_{\tau^C} \otimes AC^\theta \otimes BC^\theta)\Big] \\
&\cdot \Big[(1_{\tau^C} \otimes AC^{\theta^\dagger} \otimes BC^{\theta^\dagger})\,\Big(1_{\tau^C} \otimes C_y^\theta - |y_{\tau^C}\rangle\langle y_{\tau^C}| \otimes (AB^{\theta^\dagger})(A_y^\theta \otimes B_y^\theta \otimes C_y^\theta)(AB^\theta)\Big) \\
&\quad (1_{\tau^C} \otimes AC^\theta \otimes BC^\theta)\Big] \\
&= \sum_x |x_\tau\rangle\langle x_\tau| \otimes \Big[(1_{\tau^C} \otimes AC^{\theta^\dagger} \otimes BC^{\theta^\dagger}) \\
&\quad \Big(1_{\tau^C} \otimes C_x^\theta - |x_{\tau^C}\rangle\langle x_{\tau^C}| \otimes (AB^{\theta^\dagger})(A_x^\theta \otimes B_x^\theta \otimes C_x^\theta)(AB^\theta)\Big) \\
&\quad \Big(1_{\tau^C} \otimes C_x^\theta - |x_{\tau^C}\rangle\langle x_{\tau^C}| \otimes (AB^{\theta^\dagger})(A_x^\theta \otimes B_x^\theta \otimes C_x^\theta)(AB^\theta)\Big)\,(1_{\tau^C} \otimes AC^\theta \otimes BC^\theta)\Big]
\end{aligned}
$$

Now notice that if we have two operators A and B, where A and B are projectors and $AB = BA = B$, then

$$(A - B)(A - B) = A - B - B + B = A - B$$

Using this property we have that

$$
\begin{aligned}
&(P - \Pi)(P - \Pi) = \\
&\quad = \sum_x |x_\tau\rangle\langle x_\tau| \otimes \Big[(1_{\tau^C} \otimes AC^{\theta^\dagger} \otimes BC^{\theta^\dagger}) \\
&\quad \Big(1_{\tau^C} \otimes C_x^\theta - |x_{\tau^C}\rangle\langle x_{\tau^C}| \otimes (AB^{\theta^\dagger})(A_x^\theta \otimes B_x^\theta \otimes C_x^\theta)(AB^\theta)\Big)\,(1_{\tau^C} \otimes AC^\theta \otimes BC^\theta)\Big] \\
&\quad = P - \Pi.
\end{aligned}
$$

Therefore we have that $P - \Pi$ is positive semi-definite, which means that $P \geq \Pi$. Analogously we have $Q \geq \Pi$ and $R \geq \Pi$.

In the following we will estimate $\|PQRQP\|$. We have

$$PQP = \sum_{xyz} |x_\tau^\theta\rangle\langle x_\tau^\theta|y_\tau^{\theta'}\rangle\langle y_\tau^{\theta'}|z_\tau^\theta\rangle\langle z_\tau^\theta| \otimes 1_{\tau^C} \otimes (AC^\theta \otimes BC^\theta)^\dagger C_x^\theta (AC^\theta \otimes BC^\theta)$$
$$(AB^{\theta'} \otimes AC^{\theta'})^\dagger A_y^{\theta'} (AB^{\theta'} \otimes AC^{\theta'})(AC^\theta \otimes BC^\theta)^\dagger C_z^\theta (AC^\theta \otimes BC^\theta)$$
$$= \sum_{xyz} |x_\tau^\theta\rangle\langle x_\tau^\theta|y_\tau^{\theta'}\rangle\langle y_\tau^{\theta'}|z_\tau^\theta\rangle\langle z_\tau^\theta| \otimes 1_{\tau^C} \otimes (AB^{\theta'} \otimes AC^\theta \otimes BC^\theta)^\dagger C_x^\theta (AC^\theta AC^{\theta'\dagger})$$
$$A_y^{\theta'} (AC^{\theta'} \otimes AC^{\theta\dagger}) C_z^\theta (AB^{\theta'} \otimes AC^\theta \otimes BC^\theta)$$

Since $AC^\theta = AC^{\theta'}$ we have

$$PQP = \sum_{xyz} |x_\tau^\theta\rangle\langle x_\tau^\theta|y_\tau^{\theta'}\rangle\langle y_\tau^{\theta'}|z_\tau^\theta\rangle\langle z_\tau^\theta| \otimes 1_{\tau^C} \otimes (AB^{\theta'} \otimes AC^\theta \otimes BC^\theta)^\dagger C_x^\theta$$
$$A_y^{\theta'} C_z^\theta (AB^{\theta'} \otimes AC^\theta \otimes BC^\theta)$$

Now since $C_x^\theta C_z^\theta = \delta_{xz} C^\theta$ we get

$$PQP = \sum_{xy} |x_\tau^\theta\rangle\langle x_\tau^\theta|y_\tau^{\theta'}\rangle\langle y_\tau^{\theta'}|x_\tau^\theta\rangle\langle x_\tau^\theta| \otimes 1_{\tau^C} \otimes (AB^{\theta'} \otimes AC^\theta \otimes BC^\theta)^\dagger C_x^\theta$$
$$A_y^{\theta'} (AB^{\theta'} \otimes AC^\theta \otimes BC^\theta)$$
$$= \sum_{xy} |\langle x_\tau^\theta|y_\tau^{\theta'}\rangle|^2 |x_\tau^\theta\rangle\langle x_\tau^\theta| \otimes 1_{\tau^C} \otimes (AB^{\theta'} \otimes AC^\theta \otimes BC^\theta)^\dagger C_x^\theta$$
$$A_y^{\theta'} (AB^{\theta'} \otimes AC^\theta \otimes BC^\theta)$$
$$= 2^{-t} \sum_{xy} |x_\tau^\theta\rangle\langle x_\tau^\theta| \otimes 1_{\tau^C} \otimes (AB^{\theta'} \otimes AC^\theta \otimes BC^\theta)^\dagger C_x^\theta A_y^{\theta'} (AB^{\theta'} \otimes AC^\theta \otimes BC^\theta)$$

Now since $\Pi^\theta \leq P$ and $\Pi^{\theta'} \leq Q$ we can bound $\|\Pi^\theta \Pi^{\theta'}\|^2 \leq \|\bar{P}\bar{Q}\|^2 = \|\bar{P}\bar{Q}\bar{P}\|$ using Lemma 1.2. We now bound the norm $\|\bar{P}\bar{Q}\bar{P}\|$.

Bibliography

[1] Stefan Brands and David Chaum, *Distance-bounding protocols*, Advances in Cryptology — EUROCRYPT '93: Workshop on the Theory and Application of Cryptographic Techniques Lofthus, Norway, May 23–27, 1993 Proceedings (Berlin, Heidelberg), Springer, 1994, pp. 344–359.

[2] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner, *Position-based quantum cryptography: Impossibility and constructions*, SIAM Journal on Computing **43** (2014), no. 1, 150–178.

[3] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky, *Position based cryptography*, Cryptology ePrint Archive, Report 2009/364, 2009.

[4] Phillip Kaye, Raymond Laflamme, and Michela Mosca, *An introduction to quantum computing*, Oxford University Press, Great Clarendon Street, Oxford 0x2 6DP, 2007.

[5] Susan Loepp and William K. Wootters, *Protecting information : from classical error correction to quantum cryptography*, Cambridge University Press, Cambridge, 2006.

[6] Tomamichel Marco, Fehr Serge, Kaniewski Jądrzej, and Wehner Stephanie, *A monogamy-of-entanglement game with applications to device-independent quantum cryptography*, New J. Phys. 15, 103002 (2013).

[7] Matthew McKague, Tzyh Haur Yang, and Valerio Scarani, *Robust self-testing of the singlet*, Journal of Physics A: Mathematical and Theoretical **45** (2012), no. 45, 455304.

[8] Michael A. Nielsen and Isaac L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, The Edinburgh Building, Cambridge CB2 8RU, UK, 2010.

[9] Dominique Unruh, *Quantum position verification in the random oracle model*, Advances in Cryptology – CRYPTO 2014: 34th Annual Cryptology Conference, Proceedings, Part II (Berlin, Heidelberg), Springer, 2014, pp. 1–18.

[10] Dominique Unruh and Serge Fehr, personal communication.

Index

basis, 13

commutative property
    first, 31
    second, 32
    third, 32
complete, 15

density matrix, 24

eigenvalue, 17
eigenvector, 17
entangled, 27
EPR pair, 27

Hilbert space, 15

inner product, 14

measurement, 24
    in Hadamard basis, 25
    in basis, 26
    in computational basis, 25
    outcome, 25
    POVM, 25
    probability, 25
    projective, 24
metric space, 15
monogamy of entanglement game, 28
    maximal winning probability, 29
    MG0, 29
    MG1, 30
    MG2, 31
    MG3, 32
    MG4, 32
    MG5, 32
    MG6, 34
    MG7, 35
    parallel repetition, 29

norm, 14

operator, 16
    Hadamard, 17
    hermitian, 17
    identity, 17
    positive semi-definite, 17
    projection, 17
    trace, 17
    unitary, 17
operator norm, 18

projector, 17

quantum circuit, 26
    quantum gates, 26
    wires, 26
quantum state, 23
    mixed, 24
    norm, 23
    pure, 24
qubit, 22

tensor product, 15
trace, 17

vector, 14
vector space, 13
    n-dimensional, 14

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, _____Kristiina Rahkema_____,
(*autori nimi*)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose
_____ "Quantum position verification in the random oracle model" _____,
(*lõputöö pealkiri*)

mille juhendaja on _____Prof. Dominique Unruh_____,
(*juhendaja nimi*)

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus/~~Tallinnas/Narvas/Pärnus/Viljandis~~, **17.05.2016**

K. Rahkema