UNIVERZITET U BEOGRADU

MATEMATIČKI FAKULTET

Hana Almoner Louka

Kvantna teorija informacija i asimptotika kvantnog potpisivanja ugovora

DOKTORSKA DISERTACIJA

BEOGRAD, 2016

UNIVERSITY OF BELGRADE

FACULTY OF MATHEMATICS

Hana Almoner Louka

Quantum Information Theory and Asymptotics of Quantum Contract Signing

DOCTORAL DISSERTATION

BELGRADE, 2016

Abstract

This thesis has been written under the supervision of my mentor dr. Vladimir Božin at the University of Belgrade in the academic year 2016. The topic of this thesis is quantum information theory, with special attention to quantum contract signing protocols. The thesis is divided into four chapters. Chapter 1 gives introduction to Quantum mechanics and necessary mathematical background. Chapter 2 is about quantum information theory. Quantum algorithms, including Schor's and Grover's, are described. Chapter 3 deals with classical contract signing, and cryptography. Also discussed is the RSA algorithm and BB84 quantum key distribution. Chapter 4 describes quantum signing protocol, and proves, among other things, asymptotic behavior for probability of cheating.

Scientific field (naučna oblast): Mathematics (matematika)
Narrow scientific field (uža naučna oblast): Analysis (analiza)
UDC: 517.984+51-73/74+519.651

Abstrakt

Ova teza napisana je pod supervizijom mog mentora dr. Vladimir Božina na Univerzitetu u Beogradu 2016. akademske godine. Tema ove disertacije je kvantna teorija informacija, sa posebnim osvrtom na protokole kvantnog potpisivanja ugovora. Teza je podeljena u četiri poglavlja. Prvo poglavlje daje uvod u kvantnu mehaniku i relevantan matematički aparat. Drugo poglavlje je o kvantnoj teoriji informacija. Opisani su kvantni algoritmi, uključujući Šorov i Groverov. Treće poglavlje se bavi klasičnim potpisivanjem ugovora i kriptografijom. Govori se i o RSA algoritmu, kao i BB84 algoritmu kvantnog dodeljivanja ključeva. Četvrto poglavlje opisuje protokol kvantnog potpisivanja ugovora, i dokazuje se, izmedju ostalog, asimptotika za verovatnoću varanja.

Scientific field (naučna oblast): Mathematics (matematika)
Narrow scientific field (uža naučna oblast): Analysis (analiza)
UDC: 517.984+51-73/74+519.651

Podaci o mentoru i članovima komisije:

MENTOR:
docent dr Vladimir Božin
Matematički fakultet,
Univerzitet u Beogradu

ČLANOVI KOMISIJE :
redovni profesor dr Miloš Arsenović
Matematički fakultet,
Univerzitet u Beogradu

---

redovni profesor dr Aleksandar Lipkovski
Matematički fakultet,
Univerzitet u Beogradu

---

dr Nikola Paunković
Matematički departman,
Univerzitet u Lisabonu

Datum odbrane:

Acknowledgements

I would like to express my deepest gratitude to my advisor, dr Vladimir Božin. I am very grateful to the members of reading comitee, dr Nikola Paunković and Professors Miloš Arsenović and Aleksandar Lipkovski for their valuable time. I would also like to thank Prof. Žarko Mijajlović for his support and interest in my professional development and personal well-being. Finally, nothing would be possible without the support, encouragement and motivation from my parents, my husband and family, to whom I dedicate my work.

Hana LOUKA

Contents

Chapter 1

Introduction to Quantum Mechanics

Quantum Mechanics is a theory which describes nature most closely. For our work, we need to introduce some basic notions from this theory, and first we need to review the relevant part of mathematics, and introduce notation which is standard in this context, but is more used by physicists than mathematicians.
In quantum mechanics (QM) vector space plays an important role because QM is a linear theory.

1.1 Linear Algebra

In this section we review some basic concepts from linear algebra, related with quantum mechanics. The literature used is [36, pg. 62-65],[5],[7, pg. 21], [4, pg. 199-200],[18, pg.61],[30],[1],[32], [44],[3].
The standard notation which is used for concepts from linear algebra in the study of quantum mechanics is summarized in following table:

Symbol	Discribtion
z^*	Complex conjugate of the complex number z. $(1+i)^* = 1-i$
$\|\psi\rangle$	Vector. Also known as a *ket*.
$\langle\psi\|$	Vector dual to $\|\psi\rangle$. Also known as a *bra*.
$\langle\psi\|\varphi\rangle$	Inner product between the vectors $\|\varphi\rangle$ and $\|\psi\rangle$
$\|\psi\rangle \otimes \|\varphi\rangle, \|\psi\rangle\|\varphi\rangle, \|\psi\varphi\rangle$	Tensor product of $\|\psi\rangle$ and $\|\varphi\rangle$
$\|\psi\rangle\langle\varphi\|$	Outer product between $\|\psi\rangle$ and $\|\varphi\rangle$
$B^{\otimes n}$	n fold tensor product of B with itself
B^*	Complex conjugate of the B matrix.
B^T	Transpose of the B matrix.
$B^\dagger$	Hermitian conjugate or adjoint of the B matrix. $\begin{bmatrix} a & b \\ c & d \end{bmatrix}^\dagger = \begin{bmatrix} a^* & c^* \\ b^* & d^* \end{bmatrix}$
$\langle\psi\|B\|\varphi\rangle$	Inner product between $\|\psi\rangle$ and $B\|\varphi\rangle$. Equivalently, inner product between $B^\dagger\|\psi\rangle$ and $\|\varphi\rangle$.
$\|+\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$
$\|-\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle - \|1\rangle)$

1.1.1 Vector Space

Definition 1.1. *A vector space V* is a set of objects called vectors (denoted by $|\psi_1\rangle, |\psi_2\rangle, \dots$) and a set of numbers called scalars (denoted by $\alpha, \beta, \gamma, \dots$) with two operations, the operation "addition", denoted by " + ", and the operation "scalar multiplication", usually denoted by a dot ".". If the scalars are real numbers, we have a real vector space; if the scalars are complex numbers, we have a complex vector space. The set must be closed under vector addition and scalar multiplication.

Vector addition must have these properties:

- $|\psi_1\rangle + |\psi_2\rangle = |\psi_2\rangle + |\psi_1\rangle$;
- $|\psi_1\rangle + (|\psi_2\rangle + |\psi_3\rangle) = (|\psi_1\rangle + |\psi_2\rangle) + |\psi_3\rangle$;
- There exists a unique zero vector $|0\rangle$ such that: $|\psi_1\rangle + |0\rangle = |\psi_1\rangle$;
- For any vector $|\psi_1\rangle$ there exists a unique vector $|-\psi_1\rangle$ such that:

$$|\psi_1\rangle + |-\psi_1\rangle = |0\rangle$$

Scalar multiplication must have these properties:

- It is distributive with respect to vector addition and scalar addition: $\alpha(|\psi_1\rangle + |\psi_2\rangle) = \alpha|\psi_1\rangle + \alpha|\psi_2\rangle$ and $(\alpha + \beta)|\psi_1\rangle = \alpha|\psi_1\rangle + \beta|\psi_1\rangle$;
- It is associative with respect to ordinary scalar multiplication: $\alpha(\beta|\psi_1\rangle) = (\alpha\beta)|\psi_1\rangle$;
- Multiplication by the scalars 0 and 1 yields the expected: $0|\psi_1\rangle = |0\rangle$ and $1|\psi_1\rangle = |\psi_1\rangle$.

Usually, a vector space over $\mathbb{C}$ is called a complex vector space and a vector space over $\mathbb{R}$ is called a real vector space. We use complex vector space in quantum mechanics, and often call vectors "states".

Definition 1.2. *A linear combination of a set of vectors* $\{|\psi_i\rangle | 1 \leq i \leq n\}$ is given by

$$\alpha_1|\psi_1\rangle + \alpha_2|\psi_2\rangle + \alpha_3|\psi_3\rangle + \cdots + \alpha_n|\psi_n\rangle$$

where $\{\alpha_i | 1 \leq i \leq n\}$ is a set of complex coefficients .

Definition 1.3. *A set of vectors* $\{|\psi_i\rangle | 1 \leq i \leq n\}$ is linearly independent if no nontrivial linear combination (i.e. such that not all α_i are zero) is a zero vector, and we say that these vectors are *linearly independent.*

Definition 1.4. The *dimension* of a vector space is equal to the maximal number of linearly independent vectors.

Definition 1.5. *A subspace V_0* of a vector space V is a non-empty subset of V which satisfies the following two requirements:

- For any pair $|\phi_1\rangle, |\phi_2\rangle$ in V_0, $|\phi_1\rangle + |\phi_2\rangle$ is in V_0;
- For any $|\phi_1\rangle$ in V_0 and any scalar $\alpha, \alpha|\phi_1\rangle$ is in V_0.

Definition 1.6. *A spanning set for a vector space* is a set of vectors $\{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_n\rangle\}$ such that any vector $|\psi\rangle$ in the vector space can be written as a linear combination $|\psi\rangle = \sum_i \alpha_i |\psi_i\rangle$ of vectors in that set.

Definition 1.7. Let V denote a vector space and $S = \{|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_n\rangle\}$ a subset of V. S is called *a basis* for V if the following is true:

1. S spans V;
2. S is linearly independent.

1.1.2 Hilbert Space

Definition 1.8. The *inner product* (also called *scalar product* or *dot product*) of two vectors $|\psi\rangle$ and $|\phi\rangle$ is a complex number, written $\langle\psi|\phi\rangle$, assigned to each pair of vectors and with the following properties:

- $\langle\psi|\phi\rangle = \langle\phi|\psi\rangle^*$ (Hermitian symmetric);
- $\langle\psi|\psi\rangle \geq 0$ (nonnegative);
- $\langle\psi|\psi\rangle = 0 \leftrightarrow |\psi\rangle = |0\rangle$ (positive definite);
- $\langle\psi|(\alpha|\phi\rangle + \beta|\chi\rangle) = \alpha\langle\psi|\phi\rangle + \beta\langle\psi|\chi\rangle$.

Definition 1.9. The *length* of a vector $|\psi\rangle$ (also called the *norm* of $|\psi\rangle$) is equal the square root of $\langle\psi|\psi\rangle$ and is denoted by $|\psi|$.

In this way, given an inner product, the associated norm $|\cdot|$ on V is defined by

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

and also, an associated metric can be defined by

$$d(x, y) = |x - y|$$

Definition 1.10. A set of non-zero vectors $\{|v_1\rangle, |v_2\rangle, ..., |v_n\rangle\}$ is said to be *mutually orthogonal* if $\langle v_i|v_j\rangle = 0$ for all $i \neq j$.
Note that if $|0\rangle$ and $|1\rangle$ are orthogonal vectors (notation we will use for qubits), then $\langle 0|1\rangle = \langle 1|0\rangle = 0$.
The set is called *orthonormal* if additionally every vector in the set is a unit vector. Thus a set of vectors $\{|v_1\rangle, |v_2\rangle, ..., |v_n\rangle\}$ is orthonormal if and only if:

$$\langle v_i|v_j\rangle = \begin{cases} 0 & \text{if } i \neq j \\ 1 & \text{if } i = j \end{cases}$$

Definition 1.11. A vector space together with an inner product is called *an inner product space* or *a pre-Hilbert space.*

Proposition 1. *([25], Theorem 3 (Pythagorean Theorem)) If x and y are orthogonal vectors, then*

$$|x + y|^2 = |x|^2 + |y|^2$$

Proof.

$$\begin{aligned} |x+y|^2 &= \langle x+y|x+y\rangle \\ &= |x|^2 + 2\langle x|y\rangle + |y|^2 \\ &= |x|^2 + |y|^2 \end{aligned}$$

□

Definition 1.12. A sequence of elements x_n of an inner product space with associated norm and metric is called a *Cauchy sequence* if, for every $\epsilon > 0$, there exists an n_0 such that for all $k, m \geq n_0,\ |x_k - x_m| < \epsilon$.

Definition 1.13. *A Hilbert space* $\mathcal{H}$ is a vector space with an inner product and associated norm and metric such that every Cauchy sequence in $\mathcal{H}$ has a limit in $\mathcal{H}$.

A pre-Hilbert space is a Hilbert space if and only if it is a complete normed space (i.e. a Banach space) under the norm associated with the inner product[1].
A finite dimensional pre-Hilbert space is always a Hilbert space, and this is the case we will deal with mostly in this thesis.

1.1.3 Outer Product and Tensor Product

Definition 1.14. For a finite-dimensional vector space *outer product* between ket $|\psi\rangle$ and bra $\langle\phi|$ can be understood as:

$$|\psi\rangle\langle\phi| = \begin{bmatrix} \phi_0 \\ \phi_1 \\ \phi_2 \\ \vdots \\ \phi_n \end{bmatrix} \begin{bmatrix} \psi_0 & \psi_1 & \psi_2 & \cdots & \psi_n \end{bmatrix} = \begin{bmatrix} \psi_0\phi_0 & \psi_0\phi_1 & \psi_0\phi_2 & \cdots & \psi_0\phi_n \\ \psi_1\phi_0 & \psi_1\phi_1 & \psi_1\phi_2 & \cdots & \psi_1\phi_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \psi_n\phi_0 & \psi_n\phi_1 & \psi_n\phi_2 & \cdots & \psi_n\phi_n \end{bmatrix}$$

Below, we list a few examples (using qubit notation for the standard basis of a two dimensional space, $\{|0\rangle, |1\rangle\}$) :

$$|0\rangle\langle 0| = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

$$|0\rangle\langle 1| = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

$$|1\rangle\langle 0| = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$$

$$|1\rangle\langle 1| = \begin{bmatrix} 0 \\ 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

Definition 1.15. *Tensor product* $\mathcal{H}_1 \otimes \mathcal{H}_2$ of Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$ is a Hilbert space consisting of elements $|\psi\rangle \otimes |\phi\rangle$ (with $|\psi\rangle \in \mathcal{H}_1$ and $|\phi\rangle \in \mathcal{H}_2$) and their linear combinations. The operations in the space obey the following rules:

[1] a normed space is a Banach space if every Cauchy sequence in normed space converges

1. $\alpha(|\psi\rangle \otimes |\phi\rangle) = (\alpha|\psi\rangle) \otimes |\phi\rangle = |\psi\rangle(\alpha|\phi\rangle)$;
2. $(|\psi_1\rangle + |\psi_2\rangle) \otimes |\phi\rangle = |\psi_1\rangle \otimes |\phi\rangle + |\psi_2\rangle \otimes |\phi\rangle$;
3. $|\psi\rangle \otimes (|\phi_1\rangle + |\phi_2\rangle) = |\psi\rangle \otimes |\phi_1\rangle + |\psi\rangle \otimes |\phi_2\rangle$;
4. The inner product of two vectors $|\psi_1\rangle \otimes |\phi_1\rangle$ and $|\psi_2\rangle \otimes |\phi_2\rangle$ in $\mathcal{H}_1 \otimes \mathcal{H}_2$ is given by $\langle\psi_1\phi_1|\psi_2\phi_2\rangle = \langle\psi_1|\psi_2\rangle\langle\phi_1|\phi_2\rangle$.

Example 1.1. *Consider tensor product of two qubits (vectors from two dimensional space):*

$$|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|0\rangle \quad \textit{and} \quad |\psi_2\rangle = \alpha_2|0\rangle + \beta_2|0\rangle$$

Tensor product of $|\psi_1\rangle$ *and* $|\psi_2\rangle$ *is:*

$$\begin{aligned} |\psi_1\rangle \otimes |\psi_2\rangle &= (|\alpha_1|0\rangle + \beta_1|1\rangle) \otimes (\alpha_2|0\rangle + \beta_2|1\rangle) \\ &= \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle \end{aligned}$$

where

$$\begin{aligned} |00\rangle &= |0\rangle \otimes |0\rangle \\ |01\rangle &= |0\rangle \otimes |1\rangle \\ |10\rangle &= |1\rangle \otimes |0\rangle \\ |11\rangle &= |1\rangle \otimes |1\rangle. \end{aligned}$$

Tensor product is also defined for matrices. For example, tensor product of the following two matrices $X = \begin{bmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{bmatrix}$ and $Y = \begin{bmatrix} y_{11} & y_{12} \\ y_{21} & y_{22} \end{bmatrix}$ is given by

$$X \otimes Y = \begin{bmatrix} x_{11}Y & x_{12}Y \\ x_{21}Y & x_{22}Y \end{bmatrix} = \begin{bmatrix} x_{11}y_{11} & x_{11}y_{12} & x_{12}y_{11} & x_{12}y_{12} \\ x_{11}y_{21} & x_{11}y_{22} & x_{12}y_{21} & x_{12}y_{22} \\ x_{21}y_{11} & x_{21}y_{12} & x_{22}y_{11} & x_{22}y_{12} \\ x_{21}y_{21} & x_{21}y_{22} & x_{22}y_{21} & x_{22}y_{22} \end{bmatrix}$$

1.1.4 Linear Operators

In this chapter, we will sometimes refer to vectors as "states" (for convenience and because of a later use in quantum mechanic application).

Definition 1.16. If A is an operator mapping states to states, such that for arbitrary pair of states $|\psi_1\rangle$ and $|\psi_2\rangle$ and for any two complex numbers c_1 and c_2:

$$A(c_1|\psi_1\rangle + c_2|\psi_2\rangle) = c_1A|\psi_1\rangle + c_2A|\psi_2\rangle$$

then A is said to be a *a linear operator*. More generally, a linear operator A acts on a linear combination of states/vectors as follows:

$$A\Big(\sum_i c_i|\psi_i\rangle\Big) = \sum_i c_i A\big(|\psi_i\rangle\big)$$

Important linear operators on any vector space V are the corresponding unit or identity operator, $I = I_V$ and the zero operator 0. For the unit operator, $I_V|\psi\rangle = |\psi\rangle$ for all vectors $|\psi\rangle$, and for the zero operator, $0|\psi\rangle = 0$.

Definition 1.17. An operator A is *positive* if $\langle\psi|A|\psi\rangle$ is real and

$$\langle\psi|A|\psi\rangle \geq 0$$

for any vector $|\psi\rangle$.

Definition 1.18. The *Hermitian adjoint* of operator B is denoted by $B^\dagger$ and is defined by the following property:

$$\langle\phi|B^\dagger|\psi\rangle = \langle\psi|B|\phi\rangle^*.$$

To compute the Hermitian adjoint of any expression, we take the complex conjugate of all constants in the expression, replace all bras by kets and vice versa and replace operators by their adjoints. Also, just like transposition, Hermitian adjoint of a product reverses order, i.e. $(AB)^\dagger = B^\dagger A^\dagger$. For matrices, Hermitian adjoint of a matrix is the complex conjugate of the transpose matrix.

Definition 1.19. The operator B is *Hermitian* or *self adjoint* if it is equal to its Hermitian adjoint, i.e. if $B = B^\dagger$.

For example the Pauli operator $Y = -i|0\rangle\langle 1| + i|1\rangle\langle 0|$ is Hermitian, since $Y^\dagger = (-i|0\rangle\langle 1| + i|1\rangle\langle 0|) = -i|0\rangle\langle 1| + i|1\rangle\langle 0| = Y$.

Definition 1.20. The *inverse* of an operator B is denoted by B^{-1}. This operator satisfies $BB^{-1} = B^{-1}B = I$, where I is the identity operator.

Definition 1.21. An operator is said to be *unitary* if its adjoint is equal to its inverse. Unitary operators are often denoted using the symbol U. They satisfy

$$U^\dagger = U^{-1} \longleftrightarrow UU^\dagger = U^\dagger U = I$$

For example the Pauli operators are both Hermitian and unitary.
Unitary operators preserve the inner (scalar) product:

Proposition 2. *The inner product of $U|\phi\rangle$ and $U|\psi\rangle$ is the same as the inner product of $|\psi\rangle$ and $|\phi\rangle$.*

Proof. $(U|\psi\rangle, U|\phi\rangle) = \langle\psi|U^\dagger U|\phi\rangle = \langle\psi|I|\phi\rangle = \langle\psi|\phi\rangle$ □

Definition 1.22. An operator B is said to be *normal* if

$$B^\dagger B = BB^\dagger.$$

Unitary and Hermitian operators are examples of normal operators.

Example 1.2. *If A is Hermitian then the operator e^{iA} is unitary.*
Since:

$$e^{iA} = I + iA + \frac{i^2}{2!}A^2 + \cdots + \frac{i^n}{n!}A^n + \ldots$$
$$(e^{iA})^\dagger = I + (-i)A + \frac{(-i)^2}{2!}A^2 + \cdots + \frac{(-i)^n}{n!}A^n + \ldots = e^{-iA}$$

and

$$e^{-iA}e^{iA} = I.$$

Definition 1.23. An operator P is said to be *a projector* if

$$P^2 = P.$$

If P is also Hermitian, then it is called *an orthogonal projector.*

Projectors act as identity operator on some subspace of the vector space. Orthogonal projectors map vectors orthogonal to all vectors in that space to zero.

Definition 1.24. A *tensor product* of two linear operators, A acting on vector space V and B acting on vector space W, is the operator $A \otimes B$ acting on $V \otimes W$, so that

$$A \otimes B(|\phi\rangle \otimes |\psi\rangle) = (A|\phi\rangle) \otimes (B|\psi\rangle)$$

Definition 1.25. *The trace* of an operator A on an n-dimensional space $\mathcal{H}$ is the sum of the diagonal elements of an operator:

$$Tr(A) = \sum_{i}^{n} \langle\psi_i|A|\psi_i\rangle$$

for any orthonormal set of basis vectors $\{|\psi_i\rangle\}$

For any two operators A and B on a Hilbert space we have:

- $Tr(\alpha A) = \alpha Tr(A)$
- $Tr(A + B) = Tr(A) + Tr(B)$
- $Tr(AB) = Tr(BA)$

Example 1.3. *Lets compute trace of an operator expressed in the orthonormal basis* $\{|0\rangle, |1\rangle\}$ *as*

$$A = 2i|0\rangle\langle 0| + 3|0\rangle\langle 1| - 2|1\rangle\langle 0| + 4|1\rangle\langle 1|$$

We find the trace by computing

$$Tr(A) = \sum_{i} \langle\psi_i|A|\psi_i\rangle = \langle 0|A|0\rangle + \langle 1|A|1\rangle$$

$$\begin{aligned}\langle 0|A|0\rangle &= \langle 0|\big(2i|0\rangle\langle 0| + 3|0\rangle\langle 1| - 2|1\rangle\langle 0| + 4|1\rangle\langle 1|\big)|0\rangle \\ &= 2i\langle 0|0\rangle\langle 0|0\rangle + 3\langle 0|0\rangle\langle 1|0\rangle - 2\langle 0|1\rangle\langle 0|0\rangle + 4\langle 0|1\rangle\langle 1|0\rangle \\ &= 2i\langle 0|0\rangle\langle 0|0\rangle + 0 = 2i\end{aligned}$$

$$\begin{aligned}\langle 1|A|1\rangle &= \langle 1|\big(2i|0\rangle\langle 0| + 3|0\rangle\langle 1| - 2|1\rangle\langle 0| + 4|1\rangle\langle 1|\big)|1\rangle \\ &= 2i\langle 1|0\rangle\langle 0|1\rangle + 3\langle 1|0\rangle\langle 1|1\rangle - 2\langle 1|1\rangle\langle 0|1\rangle + 4\langle 1|1\rangle\langle 1|1\rangle \\ &= 4\langle 1|1\rangle\langle 1|1\rangle = 4\end{aligned}$$

Hence the trace is $\langle 0|A|0\rangle + \langle 1|A|1\rangle = 2i + 4$.

1.1.5 Eigenvalues and Eigenvectors

Definition 1.26. A state vector $|\psi\rangle$ is said to be an *eigenvector* (also called *an eigenket* or *eigenstate*) of an operator A if the application of A to $|\psi\rangle$ gives

$$A|\psi\rangle = \lambda|\psi\rangle$$

where λ is a complex number, called an *eigenvalue* of A. This equation is known as the eigenvalue equation, or eigenvalue problem, for the operator A (see [52]).

To find eigenvalues and eigenvectors for an operator A represented as an n by n matrix, the first step in this process is using what is known as the *characteristic equation*. The characteristic equation for an operator A is defined to be $det|A - \lambda I| = 0$ where λ is an unknown variable, I is the identity matrix and *det* denotes the determinant of the n by n matrix $A - \lambda I$.
The values λ_i of roots (solutions) of the characteristic equation are the eigenvalues of the operator A.
To find the associated eigenvectors, we solve the equation $(A - \lambda_i I)v = 0;$ for $i = 1, \ldots n$.
The set of all eigenvectors for given eigenvalue λ is called an *eigenspace*. When λ is a simple zero of characteristic equation, i.e. nondegenerate eigenvalue, the eigenspace for λ is one dimensional.
Eigenvalues of an operator are sometimes called *the spectrum* of that operator.
Now we give some proprieties of eigenvalues and eigenvectors for unitary and Hermitian operators (see [32]).
The eigenvalues and eigenvectors of a unitary operator satisfy the following:

- The eigenvalues of a unitary operator are complex numbers with modulus 1.
- A unitary operator with nondegenerate eigenvalues has mutually orthogonal eigenvectors.

The eigenvalues and eigenvectors of a Hermitian operator also satisfy the following important properties:

- The eigenvalues of a Hermitian operator are real.
- The eigenvectors of a Hermitian operator corresponding to different eigenvalues are orthogonal.

1.1.6 The Commutator and Anti-commutator

For litereature for this part, see for instance [24].

Definition 1.27. *The commutator of two operators* is $[A, B] = AB - BA$. Two operators commute/are *commutable* if $[A, B] = 0$.

Definition 1.28. *The anti-commutator of two operators A and B* is defined by

$$\{A, B\} = AB + BA.$$

We say that A anti-commutes with B if $\{A, B\} = 0$.

We have the following properties:

- Any operator commutes with itself:
  $[A, A] = 0$.
- The commutator of A, B is the negative of the commutator of B, A:
  $[A, B] = -[B, A]$.
- The commutator of two Hermitian operators is anti-Hermitian :
  $[A, B]^\dagger = (AB)^\dagger - (BA)^\dagger = B^\dagger A^\dagger - A^\dagger B^\dagger = -(AB - BA) = -[A, B]$.
- The anti-commutator of two Hermitian operators is Hermitian:
  $\{A, B\}^\dagger = (AB)^\dagger + (BA)^\dagger = B^\dagger A^\dagger + A^\dagger B^\dagger = BA + AB = \{A, B\}$.
- $\dfrac{[A, B]}{2} + \dfrac{\{A, B\}}{2} = \dfrac{AB - BA}{2} + \dfrac{AB + BA}{2} = AB$

Note that if A and B are Hermitian, and $|\psi\rangle$ is some state, then $\langle\psi|\{A, B\}|\psi\rangle$ is real and $\langle\psi|[A, B]|\psi\rangle$ is an imaginary number. So

$$|\langle\psi|\{A, B\}|\psi\rangle|^2 + |\langle\psi|[A, B]|\psi\rangle|^2 = 4|\langle\psi|AB|\psi\rangle|^2 \tag{1.1}$$

If two Hermitian operators acting on a finite dimensional Hilbert space commute, then there is a common orthonormal basis in which both are represented as diagonal matrices. This is not the case with the anticommuting operators.
In physics, non-commuting Hermitian operators are important, as they correspond to observables that cannot be measured at the same time. Note that since by the Cauchy-Schwartz inequality[2], for Hermitian operators $|\langle\psi|AB|\psi\rangle|^2 \leq \langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle$, we have from (1.1) the following bound for the commutator of Hermitian operators:

$$|\langle\psi|[A, B]|\psi\rangle|^2 \leq 4\langle\psi|A^2|\psi\rangle\langle\psi|B^2|\psi\rangle,$$

which is related with the so called uncertainty principle of quantum mechanics for non-commuting observables.

1.2 Quantum Mechanics and State Spaces

In this section we will give a general and quick introduction to quantum mechanics, which is basis for the sequel.

In the early 20th century a new science known as quantum mechanics appeared, see [16, pg. 188]. It is a mathematical theory that can describe the behavior of objects that are roughly 10,000,000,000 times smaller than a typical human being, typically of atomic size, describing for instance movement of electrons within atoms, see [39]. In this quantum world we need to forget everything we know about our daily experience: relation between action and reaction, reality, certainty and much more. Quantum mechanics is a separate science, it has its own rules and deals with physics which is impossible to explain in any classical way (for instance, the mentioned movement of electrons or photons within the atom).

[2] Cauchy-Schwartz inequality states that $|\langle x|y\rangle|^2 \leq |x|^2|y|^2$.

1.2.1 Postulates of Quantum Mechanics

In quantum mechanics *a state space* is a complex complete inner product space (i.e. Hillbert space that will be referred to as $\mathcal{H}$) corresponding to a physical system, and the following postulate holds (see[36, pp. 88-102],[35, pp. 80-83]):

Postulate 1: Associated to any isolated physical system is a complex Hilbert space known as the state space of the system. The system is completely described by its *state vector*, which is a unit vector in the system's state space.

For example an arbitrary state vector in a two dimensional state space can be written as $|\psi\rangle = a|0\rangle + b|1\rangle$ with $a, b \in \mathbb{C}$, and $|\psi\rangle$ must be a unit vector (i.e. $\langle\psi|\psi\rangle = 1$ or $|a|^2 + |b|^2 = 1$).
In general, a scalar multiple of a state vector by a number α with $|\alpha| = 1$ represents the same physical "state".

Postulate 2: The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\psi_1\rangle$ of the system at time t_1 is related to the state $|\psi_2\rangle$ of the system at time t_2 by a unitary operator U which depends only on the times t_1 and t_2,

$$|\psi_2\rangle = U|\psi_1\rangle$$

Example 1.4. *Let* $|\psi\rangle = 1|0\rangle + 0|1\rangle = \begin{bmatrix}1\\0\end{bmatrix}$, *where* $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$, $|1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$, $\langle 0| = \begin{bmatrix}1 & 0\end{bmatrix}$, $\langle 1| = \begin{bmatrix}0 & 1\end{bmatrix}$ *and* $U = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}$

We check that U is unitary, i.e. that $U^\dagger U = I$:

$$U^\dagger U = \frac{1}{\sqrt{2}}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} = \frac{1}{2}\begin{bmatrix}2 & 0\\0 & 2\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & 1\end{bmatrix} = I$$

$$|\psi_2\rangle = U|\psi_1\rangle = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \frac{1}{\sqrt{2}}\begin{bmatrix}1\\1\end{bmatrix} = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

Postulate 2′: The time evolution of a closed quantum system is described by Schrödinger equation:

$$i\hbar\frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

where $\hbar$ is Planck's constant, and H is a fixed Hermitian operator known as the Hamiltonian of the closed system.

Postulate 3: Quantum measurement is described by a set of operators $\{M_m\}$ acting on the state space of the system, where m refers to the measurement outcomes that may occur in the experiment.
If the state of the quantum system is $|\psi\rangle$ immediately before the measurement, then the probability p that result m occurs is given by:

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle$$

The state of the system after the measurement is:

$$|\psi'\rangle = \frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^* M_m|\psi\rangle}} = \frac{M_m|\psi\rangle}{\sqrt{p(m)}}$$

Furthermore the measurement operators satisfy the completeness equation:

$$\sum_m M_m^\dagger M_m = I,$$

where I is the identity operator on $\mathcal{H}$. The completeness equation expresses the fact that probabilities sum to 1:

$$\sum_m p(m) = \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle = \langle\psi|\psi\rangle = 1$$

Example 1.5. *Consider measuring a qubit basis* $\{|0\rangle, |1\rangle\}$*, and suppose that state before measurement is* $a|0\rangle\langle 0| + b|1\rangle\langle 1|$.
Measurement operators are:

$$\begin{aligned} M_0 = |0\rangle\langle 0| &= \begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} \\ &= \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} \\ M_1 = |1\rangle\langle 1| &= \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix} \\ &= \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix} \end{aligned}$$

Measurement probabilities are:

$$p(0) = \langle\psi|M_0^\dagger M_0|\psi\rangle = \langle\psi|M_0|\psi\rangle = \begin{bmatrix}a & b\end{bmatrix} \times \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} \times \begin{bmatrix}a\\b\end{bmatrix} = |a|^2$$

$$p(1) = \langle\psi|M_1^\dagger M_1|\psi\rangle = \langle\psi|M_1|\psi\rangle = \begin{bmatrix}a & b\end{bmatrix} \times \begin{bmatrix}0 & 0\\0 & 1\end{bmatrix} \times \begin{bmatrix}a\\b\end{bmatrix} = |b|^2$$

The possible states after measurement are:

$$\begin{aligned} \frac{M_0|\psi\rangle}{\sqrt{p(0)}} &= \frac{a|0\rangle}{\sqrt{|a|^2}} = \frac{a}{|a|}|0\rangle \\ \frac{M_1|\psi\rangle}{\sqrt{p(1)}} &= \frac{b|1\rangle}{\sqrt{|b|^2}} = \frac{b}{|b|}|1\rangle \end{aligned}$$

Postulate 4: The state space of a composite system consisting of n components is the tensor product of the state spaces of the components. If the component

system i has state $|\psi_i\rangle$ the composite system state is:

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes \cdots \otimes |\psi_n\rangle$$

1.2.2 Observables and Projective Measurements

In quantum mechanics, measurements are often expressed in terms of observables, which correspond to projective measurements.

Definition 1.29. *Projective measurement* is described by a Hermitian operator $\hat{A}$. It can be expressed as a sum

$$\hat{A} = \sum_m \lambda_m P_m,$$

where each λ_m is a real number, representing value of the observable corresponding to measurement outcome m, and each P_m is an orthogonal projector. The corresponding measurement has measurement operators $M_m = P_m$.

Not all measurements are projective. For example, measurement with two outcomes and measurement operators $M_1 = \frac{1}{\sqrt{2}}I$, $M_2 = \frac{1}{\sqrt{2}}I$ is not projective. However, every measurement can be expressed as a projective measurement in a composite system, after some unitary transformation (see [36, ch. 2.2.8]).

1.2.3 Density Operator Representation of Mixed and Pure States

This section is based on [32].
Suppose we have a situation, where a physical system is in state $|\psi_i\rangle$ with probability p_i. This is called a classical mixture of quantum states $|\psi_i\rangle$, each with corresponding probability p_i.
It is represented by a so called density matrix of a mixture, defined by:

$$\rho = \sum_{i=1}^{n} p_i |\psi_i\rangle\langle\psi_i|$$

such that $\sum_i p_i = 1$, where n is the (arbitrary) number of terms in the mixture.
We list several properties of the density operator:

- The density operator is Hermitian: $\rho = \rho^\dagger$;
- The density operator is positive: $\rho \geq 0$;
- The density operator is normalized: $Tr(\rho) = 1$.

Let's begin with the pure states, i.e. when there is only one state in the mixture. The density operator for pure state is $\rho = |\psi\rangle\langle\psi|$. A more general type of state is called mixed $\rho = \sum_i^n p_i |\psi_i\rangle\langle\psi_i|$, where $|\psi_i\rangle$ represent states as vectors, that are not necessarily orthogonal. The number n could be anything, and is not limited by the dimension of $\mathcal{H}$. The n numbers (or "weights") p_i are nonzero and satisfy the relations $p_i > 0$; $\sum p_i = 1$ and, when $n > 1$, $Tr(\rho^2) < 1$[3].
There are two simple tests to determine whether ρ describes a mixed state or not:

[3] mixed state is a so called statical ensemble $\{(|\psi_1\rangle, p_1), (|\psi_2\rangle, p_2), \ldots, (|\psi_n\rangle, p_n)\}$

- mixed state: $\rho^2 \neq \rho$; pure state: $\rho^2 = \rho$
- mixed state: $Tr(\rho^2) < 1$; pure state: $Tr(\rho^2) = 1$

Example 1.6. *A system is found to be in the state*

$$|\psi\rangle = \frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|0\rangle$$

The the density operator is

$$\begin{aligned}\rho = |\psi\rangle\langle\psi| &= \big(\frac{1}{\sqrt{5}}|0\rangle + \frac{2}{\sqrt{5}}|0\rangle\big)\big(\frac{1}{\sqrt{5}}\langle 0| + \frac{2}{\sqrt{5}}\langle 0|\big) \\ &= \frac{1}{5}|0\rangle\langle 0| + \frac{2}{5}|0\rangle\langle 1| + \frac{2}{5}|1\rangle\langle 0| + \frac{4}{5}|1\rangle\langle 1|\end{aligned}$$

In the $\{|0\rangle, |1\rangle\}$ basis the density matrix is

$$[\rho] = \begin{bmatrix}\langle 0|\rho|0\rangle & \langle 0|\rho|1\rangle \\ \langle 1|\rho|0\rangle & \langle 1|\rho|1\rangle\end{bmatrix} = \begin{bmatrix}\frac{1}{5} & \frac{2}{5} \\ \frac{2}{5} & \frac{4}{5}\end{bmatrix}$$

The trace is just the sum of the diagonal elements. In this case

$$Tr(\rho) = \frac{1}{5} + \frac{4}{5} = 1$$

Lets square the matrix:

$$\rho^2 = \begin{bmatrix}\frac{1}{5} & \frac{2}{5} \\ \frac{2}{5} & \frac{4}{5}\end{bmatrix}\begin{bmatrix}\frac{1}{5} & \frac{2}{5} \\ \frac{2}{5} & \frac{4}{5}\end{bmatrix} = \begin{bmatrix}\frac{1}{25} + \frac{4}{25} & \frac{2}{25} + \frac{8}{25} \\ \frac{2}{25} + \frac{8}{25} & \frac{4}{25} + \frac{12}{25}\end{bmatrix} = \begin{bmatrix}\frac{5}{25} & \frac{10}{25} \\ \frac{10}{25} & \frac{20}{25}\end{bmatrix} = \begin{bmatrix}\frac{1}{5} & \frac{2}{5} \\ \frac{2}{5} & \frac{4}{5}\end{bmatrix} = \rho$$

Since $\rho^2 = \rho$, it follows that $Tr(\rho^2) = 1$ and this is a pure state.

1.2.4 Separable States and Entangled States

Suppose we have a composite system which consists of two subsystems, $\mathcal{H}_1$ and $\mathcal{H}_2$ (see [34, pp. 61-86][40] and [17]). We can divide state vectors into two groups:

$$\text{Entangled States : There is no } |\psi_1\rangle \in \mathcal{H}_1, |\psi_2\rangle \in \mathcal{H}_2 \text{ such that } |\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$$

$$\text{Separable States : There exists } |\phi_1\rangle \in \mathcal{H}_1, |\phi_2\rangle \in \mathcal{H}_2 \text{ such that } |\phi\rangle = |\phi_1\rangle \otimes |\phi_2\rangle$$

So, a state vector $|\psi\rangle$ is called separable iff it can be written as $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, otherwise it is entangled.

- For example a pure separable state is

$$|\psi\rangle = \frac{|00\rangle + 2|01\rangle + |10\rangle + 2|11\rangle}{\sqrt{10}} = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \otimes \frac{|0\rangle + 2|1\rangle}{\sqrt{5}}$$

  .

- Examples of pure entangled states are $|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), |\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$, called "Bell states" or "EPR states".

A mixed state ρ is called separable (not entangled) iff it can be written as a convex combination of pure product states:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i| = \sum_i p_i \rho_i^{\psi} \otimes \rho_i^{\phi},$$

where $|\psi_i\rangle \in \mathcal{H}_1$ and $|\phi_i\rangle \in \mathcal{H}_2$ are state vectors of subsystems 1 and 2 respectively, and numbers $p_i > 0$ are such that $\sum_i p_i = 1$

1.2.5 EPR and Bell State

Suppose we have a pair of photons with their polarization states (vertical and horizontal) represented by vectors in two dimensional Hilbert spaces with basis vectors $\{|0\rangle_1, |1\rangle_1\}$ and $\{|0\rangle_2, |1\rangle_2\}$ respectively, which is generated by a physical process of annihilation of electron and positron. This process will give an entangled state known as an EPR pair (also called a Bell state), represented as

$$\begin{aligned} |\psi^-\rangle &= \frac{1}{\sqrt{2}}\big(|0\rangle_1 \otimes |1\rangle_2 - |1\rangle_1 \otimes |0\rangle_2\big) \\ &= \frac{1}{\sqrt{2}}\big(|-\rangle_1 \otimes |+\rangle_2 - |+\rangle_1 \otimes |-\rangle_2\big), \end{aligned}$$

where

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),\ |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \text{ and } |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}.$$

Of the two photons, one will be measured by Alice, and another by Bob, and they are in distant laboratories receiving one photon each. Both can choose what to measure on their photons. Suppose we have 4 observables, $\hat{A}_A, \hat{R}_A, \hat{A}_B, \hat{R}_B$, where the lower index denotes Alice or Bob, and for each there is the "accept" observable[4]

$$\hat{A} = 1.|1\rangle\langle 1| + 0.|0\rangle\langle 0|$$

and the "reject" observable

$$\hat{R} = 1.|+\rangle\langle +| + 0.|-\rangle\langle -|.$$

Here $\{|+\rangle, |-\rangle\}$ will be the the "reject basis", $\{|0\rangle, |1\rangle\}$ will be the the "accept basis" that is being measured.
If both measure the same basis, they will get the opposite results, for instance if they measure the "accept" observable, and the result is $|1\rangle$ for Bob, result will be $|0\rangle$ for Alice (also if Alice gets $|0\rangle$ Bob will get $|1\rangle$). At the same time if Alice measures the "reject" observable she will know what Bob would get if he measured the "reject" observable. Since photons are distant, measurements of Bob (or Alice) on one photon should not influence local properties of the other photon. But by quantum mechanics, no one, neither Alice nor Bob, can measure both $\hat{A}$ and $\hat{R}$ at

[4] our names of observables here used correspond to cryptography protocol we will discuss in the last chapter.

the same time on their photons. But if Alice measures $\hat{A}$ and Bob measures $\hat{R}$ it seems that they have measured both in $\hat{A}$ and $\hat{R}$ for one particle, which is called Einstein-Podolsky-Rosen (EPR) paradox, see [36].

It turns out that EPR paradox can be made more explicit.
Let us denote $|1\rangle_\phi = cos\,\phi\,|1\rangle + sin\,\phi\,|0\rangle$, $|0\rangle_\phi = -sin\,\phi\,|1\rangle + cos\,\phi\,|0\rangle$ and consider the observable

$$\hat{P}_\phi = 1.|1\rangle_\phi\langle 1|_\phi + 0.|0\rangle_\phi\langle 0|_\phi,$$

representing measurement of polarization for axes rotated by angle ϕ. Note that $\{|0\rangle_\phi, |1\rangle_\phi\}$ is a basis of our Hilbert space. For $\phi = 0$ we get $|0\rangle, |1\rangle$ respectively for $|0\rangle_\phi, |1\rangle_\phi$ and for $\phi = \pi/4$ we get $|-\rangle, |+\rangle$ respectively for $|0\rangle_\phi, |1\rangle_\phi$, so $\hat{P}_0 = \hat{A}$, $\hat{P}_{\pi/4} = \hat{R}$.

It can be checked that for all ϕ, $|\psi^-\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle_\phi \otimes |1\rangle_\phi - |1\rangle_\phi \otimes |0\rangle_\phi\big)$.
If Alice measures polarization angle α and Bob measures angle β on $|\psi^-\rangle$, and Alice gets i, $i \in \{0,1\}$ and Bob gets j, $j \in \{0,1\}$
probability of that event is

$$|\langle\psi^-|i\rangle_\alpha \otimes |j\rangle_\beta|^2.$$

But Alice's result for angle β would be opposite of Bob's. So for Alice's photon to have polarization 1 for angle α and 1 for angle β probability is $|\langle\psi^-(|1\rangle_\alpha \otimes |0\rangle_\beta)|^2$, and have polarization 1 for α and 0 for β probability is $|\langle\psi^-(|1\rangle_\alpha \otimes |1\rangle_\beta)|^2$.

$$|\langle\psi^-|(|1\rangle_\alpha \otimes |1\rangle_\beta)|^2 = \Big|\Big(\frac{\langle 0| \otimes \langle 1| - \langle 1| \otimes \langle 0|}{\sqrt{2}}\Big)\times \Big((cos\,\alpha\,|1\rangle + sin\,\alpha\,|0\rangle) \otimes (cos\,\beta\,|1\rangle + sin\,\beta\,|0\rangle)\Big)\Big|^2$$

Using notation $|0\rangle \otimes |1\rangle = |01\rangle$ etc, we have

$$\begin{aligned}
|\langle\psi^-|(|1\rangle_\alpha \otimes |1\rangle_\beta)|^2 &= \Big|\Big(\frac{\langle 01| - \langle 10|}{\sqrt{2}}\Big) \\
&\quad \times \Big(cos\,\alpha\,cos\,\beta\,|11\rangle + cos\,\alpha\,sin\,\beta\,|10\rangle \\
&\quad + sin\,\alpha\,cos\,\beta\,|01\rangle + sin\,\alpha\,sin\,\beta\,|00\rangle\Big)\Big|^2 \\
&= \Big|\Big(\frac{\langle 01| - \langle 10|}{\sqrt{2}}\Big)\,cos\,\alpha\,cos\,\beta\,|11\rangle + \Big(\frac{\langle 01| - \langle 10|}{\sqrt{2}}\Big)\,cos\,\alpha\,sin\,\beta\,|10\rangle \\
&\quad + \Big(\frac{\langle 01| - \langle 10|}{\sqrt{2}}\Big)\,sin\,\alpha\,cos\,\beta\,|01\rangle + \Big(\frac{\langle 01| - \langle 10|}{\sqrt{2}}\Big)\,sin\,\alpha\,sin\,\beta\,|00\rangle\Big|^2 \\
&= \Big|\frac{1}{\sqrt{2}}\big(cos\,\alpha\,cos\,\beta\,\langle 01|11\rangle - cos\,\alpha\,cos\,\beta\,\langle 10|11\rangle \\
&\quad + cos\,\alpha\,sin\,\beta\,\langle 01|10\rangle - cos\,\alpha\,sin\,\beta\,\langle 10|10\rangle \\
&\quad + sin\,\alpha\,cos\,\beta\,\langle 01|01\rangle - sin\,\alpha\,cos\,\beta\,\langle 10|01\rangle \\
&\quad + sin\,\alpha\,cos\,\beta\,\langle 01|00\rangle - sin\,\alpha\,cos\,\beta\,\langle 10|00\rangle\big)\Big|^2
\end{aligned}$$

Now we apply orthonomality of our basis to get:

$$\begin{aligned}|\langle\psi^-|(|1\rangle_\alpha \otimes |1\rangle_\beta)|^2 &= \Big|\frac{cos\,\alpha\, sin\,\beta - sin\,\alpha\, cos\,\beta}{\sqrt{2}}\Big|^2 \\ &= \Big|\frac{-\big(sin\,\alpha\, cos\,\beta - cos\,\alpha\, sin\,\beta\big)}{\sqrt{2}}\Big|^2 \\ &= \Big|\frac{-\big(sin(\alpha-\beta)\big)}{\sqrt{2}}\Big|^2 \\ &= \frac{sin^2(\alpha-\beta)}{2}\end{aligned}$$

Now we apply the same steps for $|\langle\psi^-|(|1\rangle_\alpha \otimes |0\rangle_\beta)|^2$:

$$\begin{aligned}|\langle\psi^-|(|1\rangle_\alpha \otimes |0\rangle_\beta)|^2 = \Big|\Big(&\frac{\langle 0|\otimes\langle 1| - \langle 1|\otimes\langle 0|}{\sqrt{2}}\Big)\times \\ &\Big((cos\,\alpha\,|1\rangle + sin\,\alpha\,|0\rangle)\otimes(-sin\,\beta\,|1\rangle + cos\,\beta\,|0\rangle)\Big)\Big|^2\end{aligned}$$

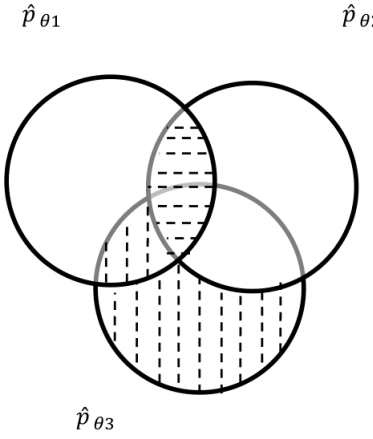
Using notation $|0\rangle\otimes|1\rangle = |01\rangle$ etc, we have

$$\begin{aligned}|\langle\psi^-|(|1\rangle_\alpha \otimes |0\rangle_\beta)|^2 = \Big|\Big(&\frac{\langle 01| - \langle 10|}{\sqrt{2}}\Big) \\ &\times\Big(- cos\,\alpha\, sin\,\beta\,|11\rangle + cos\,\alpha\, cos\,\beta\,|10\rangle \\ &- sin\ \alpha\ sin\,\beta\,|01\rangle + sin\,\alpha\, cos\ \beta\ |00\rangle\Big)\Big|^2 \\ = \Big| &- \Big(\frac{\langle 01| - \langle 10|}{\sqrt{2}}\Big)\ cos\,\alpha\, sin\,\beta\,|11\rangle + \Big(\frac{\langle 01| - \langle 10|}{\sqrt{2}}\Big)\ cos\,\alpha\, cos\,\beta\,|10\rangle \\ &- \Big(\frac{\langle 01| - \langle 10|}{\sqrt{2}}\Big)\ sin\ \alpha\ sin\,\beta\,|01\rangle + \Big(\frac{\langle 01| - \langle 10|}{\sqrt{2}}\Big)\ sin\,\alpha\, cos\ \beta\ |00\rangle\Big|^2 \\ = \Big|\frac{1}{\sqrt{2}}\Big(&- cos\ \alpha\ sin\ \beta\ \langle 01|11\rangle + cos\ \alpha\ sin\ \beta\ \langle 10|11\rangle \\ &+ cos\ \alpha\ cos\ \beta\ \langle 01|10\rangle - cos\ \alpha\ cos\ \beta\ \langle 10|10\rangle \\ &- sin\ \alpha\ sin\ \beta\ \langle 01|01\rangle + sin\ \alpha\ sin\ \beta\ \langle 10|01\rangle \\ &+ sin\ \alpha\ cos\ \beta\ \langle 01|00\rangle - sin\ \alpha\ cos\ \beta\ \langle 10|00\rangle\Big)\Big|^2\end{aligned}$$

Now we apply orthonomality of our basis to get:

$$\begin{aligned}|\langle\psi^-|(|1\rangle_\alpha \otimes |0\rangle_\beta)|^2 &= \Big|\frac{cos\,\alpha\, cos\,\beta + sin\,\alpha\, sin\,\beta}{\sqrt{2}}\Big|^2 \\ &= \Big|\frac{cos(\alpha-\beta)}{\sqrt{2}}\Big|^2 \\ &= \frac{cos^2(\alpha-\beta)}{2}\end{aligned}$$

FIGURE 1.1: Bell inequality for Alice's photon



From the figure (1.1) we see that the following formula (special case of *Bell inequalities*) should hold for Alice's photon ($\hat{p}_\theta$ denotes what would outcome be on Alice's photon if observable $\hat{P}_\theta$ were measured):

$$prob\,(\hat{p}_{\theta_1} = 1,\, \hat{p}_{\theta_2} = 1) + prob\,(\hat{p}_{\theta_2} = 0,\, \hat{p}_{\theta_3} = 1) \geq prob\,(\hat{p}_{\theta_1} = 1,\, \hat{p}_{\theta_3} = 1)$$

But setting $\theta_1 = 0$, $\theta_2 = \pi/3$ and $\theta_3 = \pi/4$ we get that it does not hold, since

$$prob\,(\hat{p}_0 = 1,\, \hat{p}_{\pi/3} = 1) + prob\,(\hat{p}_{\pi/3} = 0,\, \hat{p}_{\pi/4} = 1) = (cos^2(\pi/3) + sin^2(\pi/12))/2$$

$$prob\,(\hat{p}_0 = 1,\, \hat{p}_{\pi/4} = 1) = cos^2(\pi/4)/2$$

but $cos^2(\pi/4) > cos^2(\pi/3) + sin^2(\pi/12)$. In this way, we see that naive interpretation of photons having "local" properties does not hold in quantum mechanics, and this can be shown by a simple (in principle) experiment.

Chapter 2

Quantum Information Theory

Quantum information theory deals with specific aspects of quantum mechanics, and has played an important role in science in the last 20 years. There are practical applications in cryptography, and in theory, quantum computation is potentially much more powerful than classical.

2.1 Bit and quantum bit

In a classical computer, the value of a bit can be either 0 or 1. In a quantum computer, a quantum bit (or qubit for short) can exist in a superposition of states $|0\rangle$ and $|1\rangle$, and is described by:

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

where α and β are complex numbers satisfying the normalization condition: $|\alpha|^2 + |\beta|^2 = 1$, see [50, p. 208].
An n-qubit state is represented as a normalized vector in 2^n dimensional space, with basis vectors coressponding to all possible classical n-bit states,

$$|0\ldots00\rangle, |0\ldots01\rangle, \ldots, |1\ldots11\rangle.$$

2.2 Quantum Gates

Quantum gates are unitary transformations that act on one or several qubits, while leaving the rest of the qubits the same, i.e. acting as some unitary transformation tensored with identity operator on the rest of the qubit spaces.
Quantum gates are usually represented as matrices. A gate which acts on k qubits is represented by a $2^k \times 2^k$ unitary matrix (see [48, pg. 63-69],[38, pp. 138-147],[43] and [23]).

2.2.1 Single Qubit Gates

A single qubit gate is a unitary operator which transforms a single qubit state $|\psi\rangle_{in}$ to anther single qubit $|\psi_{out}\rangle = U|\psi_{in}\rangle$, where $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}$.

Examples of single qubit gates include Pauli gates, Hadamard gate, phase gate or phase shift gate, rotation gates and square root of-NOT.

1. Pauli Gates:

   - Pauli X-Gate or NOT Gate: is defined as

     $$X = \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

     It flips a bit from 0 to 1 and vice versa and is represented as

     $$X|0\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |1\rangle$$

     and

     $$X|1\rangle = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |0\rangle$$

   - Pauli Y-Gate is defined as:

     $$\sigma_Y = Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

     The Pauli-Y transformation is represented as

     $$Y|0\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = i \begin{bmatrix} 0 \\ 1 \end{bmatrix} = i|1\rangle$$

     and

     $$Y|1\rangle = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = -i \begin{bmatrix} 1 \\ 0 \end{bmatrix} = -i|0\rangle$$

   - Pauli Z-Gate, also known as Phase Flip is defined as:

     $$\sigma_z = Z = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$$

     The Pauli-Z transformation keeps $|0\rangle$ unchanged and changes $|1\rangle$ to $-|1\rangle$ and is represented as

     $$Z|0\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = |0\rangle$$

     and

     $$Z|1\rangle = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = |1\rangle$$

Note the following properties of Pauli matrices:

- $\mathrm{tr}(\sigma_x) = \mathrm{tr}(\sigma_y) = \mathrm{tr}(\sigma_z) = 0$
- $\det(\sigma_x) = \det(\sigma_y) = \det(\sigma_z) = -1$
- $\sigma_x^\dagger = \sigma_x$
- $\sigma_y^\dagger = \sigma_y$
- $\sigma_z^\dagger = \sigma_z$

The cyclic properties of Pauli matrices:

- $\sigma_x^2 = \sigma_y^2 = \sigma_z^2$
- $\sigma_x\sigma_y = -\sigma_y\sigma_x = i\sigma_z$
- $\sigma_y\sigma_z = -\sigma_z\sigma_y = i\sigma_x$
- $\sigma_z\sigma_x = -\sigma_x\sigma_z = i\sigma_y$
- $\sigma_x\sigma_y\sigma_z = iI$

we can use the Dirac notation $\sum_{ij} |i\rangle A_{ij}\langle j|$ for writing the Pauli matrices:

- $\sigma_x = |0\rangle\langle 1| + |1\rangle\langle 0| = \begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} = \begin{bmatrix}0 & 1\\0 & 0\end{bmatrix} + \begin{bmatrix}0 & 0\\1 & 0\end{bmatrix} = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$
- $\sigma_y = -i|1\rangle\langle 0| + i|0\rangle\langle 1| = -i\begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} + i\begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix} = \begin{bmatrix}0 & -i\\i & 0\end{bmatrix} + \begin{bmatrix}0 & 0\\1 & 0\end{bmatrix} = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix}$
- $\sigma_z = |0\rangle\langle 0| - |1\rangle\langle 1| = \begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} - \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix} = \begin{bmatrix}0 & 1\\0 & 0\end{bmatrix} - \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} = \begin{bmatrix}0 & -1\\1 & 0\end{bmatrix}$

2. Hadamard Gate: can be given as

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} = \frac{1}{\sqrt{2}}(X + Z)$$

The Hadamard transformation mathematically flips $|0\rangle$ to $|+\rangle$ and flips $|1\rangle$ to $|-\rangle$ and is represented as:

$$H|0\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle + |1\rangle\big) = |+\rangle$$

and

$$H|1\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle - |1\rangle\big) = |-\rangle$$

The matrix representation of H gate using Dirac notation:

$$\begin{aligned} H &= |0\rangle\frac{1}{\sqrt{2}}\big(\langle 0| + \langle 1|\big) + |1\rangle\frac{1}{\sqrt{2}}\big(\langle 0| - \langle 1|\big) \\ &= \frac{1}{\sqrt{2}}\big[|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| - |1\rangle\langle 0|\big] \\ &= \frac{1}{\sqrt{2}}\Big[\begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix} + \begin{bmatrix}1\\0\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix} + \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}1 & 0\end{bmatrix} - \begin{bmatrix}0\\1\end{bmatrix}\begin{bmatrix}0 & 1\end{bmatrix}\Big] \\ &= \frac{1}{\sqrt{2}}\Big[\begin{bmatrix}1 & 0\\0 & 0\end{bmatrix} + \begin{bmatrix}0 & 1\\0 & 0\end{bmatrix} + \begin{bmatrix}0 & 0\\0 & -1\end{bmatrix} - \begin{bmatrix}1 & 0\\0 & 0\end{bmatrix}\Big] \\ &= \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} \end{aligned}$$

The properties of Hadmard gate with respect to Pauli matrices:

- $H\sigma_x H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\begin{bmatrix}0 & 1\\1 & -0\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} = \begin{bmatrix}1 & 0\\0 & -1\end{bmatrix} = \sigma_z$
- $H\sigma_z H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} = \begin{bmatrix}0 & 1\\1 & 0\end{bmatrix} = \sigma_x$
- $H\sigma_y H = \frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix}\begin{bmatrix}0 & -i\\i & 0\end{bmatrix}\frac{1}{\sqrt{2}}\begin{bmatrix}1 & 1\\1 & -1\end{bmatrix} = \begin{bmatrix}0 & i\\-i & 0\end{bmatrix} = -\sigma_y$

3. Phase Gate or Phase shift Gate: The Phase Gate transformations keeps $|0\rangle$ unchanged and change the phase $|1\rangle$ by $e^{i\phi}$ and are represented as

$$p(\phi)|0\rangle = |0\rangle$$

and

$$p(\phi)|1\rangle = e^{i\phi}|1\rangle$$

Thus the unitary matrix corresponding to Phase Gate can be given as

$$p(\phi) = \begin{bmatrix}1 & 0\\0 & e^{i\phi}\end{bmatrix}$$

since ϕ can have infinity many values, we have infinity many gates, for example:
The $p(\frac{\pi}{4})$ Phase Gate is often denoted as T Gate:

$$T = p(\frac{\pi}{4}) = \begin{bmatrix}1 & 0\\0 & e^{i\frac{\pi}{4}}\end{bmatrix}$$

and

$$S = T^2 = p(\frac{\pi}{2}) = \begin{bmatrix}1 & 0\\0 & i\end{bmatrix}$$

is often called the "$\frac{\pi}{2}$" Phase Gate, also called the i Phase shift Gate, and we get the Pauli-Z gate when $\phi = \pi$. Note that $S^2 = T$.
The S transformation keeps $|0\rangle$ unchanged and changes $|1\rangle$ to $i|1\rangle$ and is

represented as:

$$S|0\rangle = \begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} = |0\rangle$$

$$S|1\rangle = \begin{bmatrix}1 & 0\\ 0 & i\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = i\begin{bmatrix}0\\1\end{bmatrix} = i|1\rangle$$

The T transformation keeps $|0\rangle$ unchanged and changes $|1\rangle$ to $e^{i\frac{\pi}{4}}|1\rangle$ and is represented as:

$$T|0\rangle = \begin{bmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{4}|1\rangle}\end{bmatrix}\begin{bmatrix}1\\0\end{bmatrix} = \begin{bmatrix}1\\0\end{bmatrix} = |0\rangle$$

$$T|1\rangle = \begin{bmatrix}1 & 0\\ 0 & e^{i\frac{\pi}{4}}\end{bmatrix}\begin{bmatrix}0\\1\end{bmatrix} = e^{i\frac{\pi}{4}}|1\rangle$$

4. Rotation Gates: are defined as follows:

$$R_x(\theta) = e^{-i\frac{\theta}{2}\sigma_x},$$
$$R_y(\theta) = e^{-i\frac{\theta}{2}\sigma_y},$$
$$R_z(\theta) = e^{-i\frac{\theta}{2}\sigma_z}.$$

Now to obtain the matrix forms of these single qubit gates we have to prove $e^{iAx} = Icos(x) + iAsin(x)$, when x is a real number and A is matrix such that $A^2 = I$.
Proof:

$$\begin{aligned}
e^{i\,A\theta} &= I + i\,Ax - \frac{A^2x^2}{2!} - i\frac{A^3x^3}{3!} + \frac{A^4x^4}{4!} + i\frac{A^5x^5}{5!} + \dots\\
&= I\big(1 - \frac{x^2}{2!} + \frac{x^4}{4!} + \dots\big) + iA\big(x - \frac{x^3}{3!} + \frac{x^5}{5!} + \dots\big)\\
&= I\sum_{n\ even}^{\infty}\frac{(x)^n}{n!} + i\,A\sum_{n\ odd}^{\infty}\frac{(x)^n}{n!}\\
&= I\,cos(x) + i\,Asin(x)
\end{aligned}$$

From the above simple identity and from identities $\sigma_x^2 = \sigma_y^2 = \sigma_z^2 = I$ it follows that:

$$\begin{aligned}
R_x(\theta) &= e^{-i\frac{\theta}{2}\sigma_x}\\
&= cos(\frac{\theta}{2})I - isin(\frac{\theta}{2})\sigma_x\\
&= cos(\frac{\theta}{2})\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} - isin(\frac{\theta}{2})\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}\\
&= \begin{bmatrix}cos(\frac{\theta}{2} & -isin(\frac{\theta}{2})\\ -isin(\frac{\theta}{2}) & cos(\frac{\theta}{2})\end{bmatrix}
\end{aligned}$$

$$\begin{aligned} R_y(\theta) &= e^{-i\frac{\theta}{2}\sigma_y} \\ &= cos(\frac{\theta}{2})I - isin(\frac{\theta}{2})\sigma_y \\ &= cos(\frac{\theta}{2})\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} - isin(\frac{\theta}{2})\begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} \\ &= \begin{bmatrix}cos(\frac{\theta}{2} & -sin(\frac{\theta}{2})\\ sin(\frac{\theta}{2}) & cos(\frac{\theta}{2})\end{bmatrix} \end{aligned}$$

$$\begin{aligned} R_z(\theta) &= e^{-i\frac{\theta}{2}\sigma_z} \\ &= cos(\frac{\theta}{2})I - isin(\frac{\theta}{2})\sigma_z \\ &= cos(\frac{\theta}{2})\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} - isin(\frac{\theta}{2})\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \\ &= \begin{bmatrix}e^{-i\frac{\theta}{2}} & 0\\ 0 & e^{i\frac{\theta}{2}}\end{bmatrix} \end{aligned}$$

5. Square root of-Not: One of the simplest non classical gates[1]

$$V = \sqrt{NOT} = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}^{\frac{1}{2}} = \frac{(1+i)}{2}\begin{bmatrix}1 & -i\\ -i & 1\end{bmatrix} = \begin{bmatrix}\frac{1+i}{2} & \frac{1-i}{2}\\ \frac{1-i}{2} & \frac{1+i}{2}\end{bmatrix}$$

it is very easy to check that $V.V = NOT$:

$$\begin{bmatrix}\frac{1+i}{2} & \frac{1-i}{2}\\ \frac{1-i}{2} & \frac{1+i}{2}\end{bmatrix}\begin{bmatrix}\frac{1+i}{2} & \frac{1-i}{2}\\ \frac{1-i}{2} & \frac{1+i}{2}\end{bmatrix} = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$

2.2.2 Two Qubit Gates

The general state of a two qubit system can be described as:

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{pmatrix}\alpha_{00}\\ \alpha_{01}\\ \alpha_{10}\\ \alpha_{11}\end{pmatrix}$$

The most important two qubit gates are the Controlled NOT gate or CNOT, Swap gate and Controlled-U gate

1. CNOT Gate: The first bit of a CNOT gate is called the control bit, and the second the target bit. The control bit does not change, while the target bit flips only when the control bit is 1, and it is works as following:

$$|00\rangle \rightarrow |00\rangle$$

[1] There are seven basic classical logic gates: AND, NOT, OR, XOR, NAND, NOR, and XNOR.

$$|01\rangle \to |01\rangle$$
$$|10\rangle \to |11\rangle$$
$$|11\rangle \to |10\rangle$$

it is represent in bra-ket notation as follows:

$$\text{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes \sigma_x$$

Thus the matrix representation for this gate is:

$$\text{CNOT} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

2. Controlled-U Gate: can be implemented using single qubit gates (e.g., U $= \sigma_x,\ \sigma_y,\ \sigma_z$, H, S, V ...) and CNOT, and it is works as follows:

$$|00\rangle \to |00\rangle$$
$$|01\rangle \to |01\rangle$$
$$|10\rangle \to |1\rangle \otimes U|0\rangle$$
$$|11\rangle \to |1\rangle \otimes U|1\rangle$$

and it is represnt by bra-ket as follows:

$$\text{Controlled-U Gate} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes U$$

Thus the matrix representation for this gate is:

$$\text{Controlled-U} = \begin{bmatrix} I & O \\ O & U \end{bmatrix},$$

where I is identity matrix, $O = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ and U is any quantum gate with 2×2 unitary matrix. For instance $(U = X, Y, Z, H, S, \cdots)$. We can see that CNOT gate is a special case of controlled U where $U = X$

3. Swap Gate: the swap gate swaps the state of two qubits; thus it maps $|mn\rangle \to |nm\rangle$ (i.,e.$|00\rangle \to |00\rangle, |01\rangle \to |10\rangle, |10\rangle \to |01\rangle$ and $|11\rangle \to |11\rangle$)
and it can represented by the matrix:

$$\text{SWAP} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

2.2.3 Three Qubit Gates

The Toffoli and Fredkin gates are an examples of three qubit gates

1. Toffoli gate (Controlled-Controlled-NOT): The Toffoli gate takes the state $|abc\rangle$ to the state $|abc'\rangle$ as follows:

$$|000\rangle \to |000\rangle;$$
$$|001\rangle \to |001\rangle;$$
$$|010\rangle \to |010\rangle;$$
$$|011\rangle \to |011\rangle;$$
$$|100\rangle \to |100\rangle;$$
$$|101\rangle \to |101\rangle;$$
$$|110\rangle \to |111\rangle;$$
$$|111\rangle \to |110\rangle.$$

   It can be understood as a gate that flips the third input bit if and only if the first two input bits are both 1.
   Now we can representing Toffoli gate as:

$$\text{Toffoli} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{bmatrix}$$

2. Fredkin gate: also known as Controlled-SWAP swaps the last two bits if and only if the first bit is $|1\rangle$, as follows:

$$|000\rangle \to |000\rangle;$$
$$|001\rangle \to |001\rangle;$$
$$|010\rangle \to |010\rangle;$$
$$|011\rangle \to |011\rangle;$$
$$|100\rangle \to |100\rangle;$$
$$|101\rangle \to |110\rangle;$$
$$|110\rangle \to |101\rangle;$$
$$|111\rangle \to |111\rangle.$$

and it can represented by the matrix:

$$\text{Fredkin} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

2.3 Universal Quantum Gates

We know in classical computers that, for instance, the gates NAND and NOR are universal, see [51, p. 57,p. 92], because we can build any logic gate using only NAND or NOR gates.

Example 2.1. *A NOT gate can be obtained using a NAND gate:*

$$[(A|A) \text{ has the same values as } \neg A]$$

TABLE 2.1: NOT in terms of NAND

A	A	$A\|A$	$\neg A$
0	0	1	1
1	1	0	0

Example 2.2. *An AND gate can be obtained using only NAND gate:*

$$[A \wedge B \equiv (A|B)|(A|B)]$$

TABLE 2.2: AND in terms of NAND

A	A	$A\|B$	$A\|B$	$(A\|B)\|(A\|B)$
0	0	1	0	0
0	1	1	0	0
1	1	1	0	0
1	0	0	1	1

In quantum computation, a similar situation occurs. The set of gates such that any unitary operator can be expressed by a quantum circuit using only the gates from that set is called a universal set of quantum gates. For example, one such universal set, as showed by Barenco, consists of the following two qubit gates, see [12, pp. 108-110],[31, pp. 67-71],[13]:

$$A(\phi, \alpha, \theta) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & e^{i\alpha}cos(\theta) & -ie^{(\alpha+\phi)}sin(\theta) \\ 0 & 0 & -ie^{(\alpha-\phi)}sin(\theta) & e^{i\alpha}cos(\theta) \end{pmatrix}$$

If we set $\theta = \pi/2, \phi = 0$ and $\alpha = \pi/2$ the Barence gate operates as a CNOT gate:

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

By setting $\theta = \pi/2, \phi = 3\pi/2$ and $\alpha = \pi/2$ the Barence gate operates as a controlled-Y gate$\big($in short C(Y)$\big)$:

$$C(Y) = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -i \\ 0 & 0 & i & 0 \end{bmatrix}$$

By setting $\alpha = \phi = 0$ and $\theta = \pi/2$ the Barence gate operates as an Identity matrix:

$$I = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

2.4 Quantum Algorithms

Quantum algorithms can be modelled by a unitary transformation of n-qubit state using quantum gates. Such transformation is always reversible, i.e. by playing steps of the algorithm in reverse, we get the original state.

However, the last step of a quantum algorithm is quantum measurement. This step is not reversible, and gives one state of the measured basis with corresponding probability.

Because of the measurement step, all quantum algorithms are in essence probabilistic. It is however possible to emulate any classical computation on a quantum computer.

In the following section we will explain structure of two of the most important quantum algorithms.

2.4.1 Shor's Algorithm

In 1994 Peter Shor published Shor's algorithm (see [45, pg. 105-110],[21, pg. 4-8]) for factoring big number N but the clasical part was known before. It takes polynomial time in $log\ N$, specifically $O\big((log\ N)^3\big)$. Classically, best known prime factorization algorithms take asymptically $Cexp[(log\ N)^{1/3}](log\ N)^{2/3}$ steps.

He shows (in principle), that quantum computer is capable of factoring very large number in polynomial time (polynomial in the number of digits of the number).

To understand the Shor's algorithm (and RSA algorithm in the next chapter), we shall need several mathematical ingredients from basic mathematics and number theory, see paper [37, pp. 159-186]:

Definition 2.1. (Division Algorithm for Integers). Let $a, b \in \mathbb{Z}$ with $b > 1$. Then there exist unique $q, r \in \mathbb{Z}$ such that $a = bq + r, 0 \leq r < b$. If $r = 0$, we say that b divides a and denote this by $b|a$.

Definition 2.2. (Greatest common divisor). Let $a, b \in \mathbb{Z}$. A positive integer d is the greatest common divisor of a and b if

1. $d|a$ and $d|b$,
2. if c is a positive integer satisfying $c|a$ and $c|b$, then $c|d$.

The greatest common divisor of a and b is denoted by $gcd(a, b)$.

Theorem 1. ***(Euclidean Algorithm)*** *To compute the greatest common divisor of two numbers a and b, let $r_{-1} = a$, let $r_0 = b$, and compute successive quotients and remainders:*

$$r_{i-1} = q_{i+1} \times r_i + r_{i+1}$$

for $i = 0, 1, 2, \ldots$ until some remainder r_{n+1} is 0. The last nonzero remainder r_n is then the greatest common divisor of a and b.

Primality and coprimality play a central role in the arithmetic of the RSA cryptosystem.

Definition 2.3. (Prime Integer) An integer $p \geq 2$ is said to be prime if its only positive divisors are 1 and p.

Definition 2.4. (Relatively Prime or Coprime Integers) Two integers a and b are said to be relatively prime or coprime if $gcd(a, b) = 1$.

Definition 2.5. (RSA Modulus) Let p and q be large prime numbers such that$p \neq q$. The product $N = pq$ is called an RSA modulus.

Definition 2.6. (Modular Arithmetic) $a \equiv b(mod c) \leftrightarrow a = b + kc$ for some integer k.

Example 2.3. $21 \equiv 1(mod\ 4)$ *because* $21 = 1 + 5(4)$
$5^2 \equiv 3(mod\ 11)$ *because* $25 = 3 + 2(11)$

2.4.1.1 General Steps of Shor's Algorithm

1. A reduction, which can be done on classical computer, of the factoring problem to the problem order finding.
2. A quantum algorithm to solve the problem order fining.

Classical Part : Reduction to Order Finding

1. scale integer a such that $1 < a < N$.
2. compute $z = \gcd(a, N)$. This may be done by Euclidean algorithm .

3. if $z = gcd(a, N) \neq 1$ then there is a nontrivial factor of N, so we are done.
4. otherwise, use the period-finding subroutine (below) to find r , the period of the following function:

$$f(x) = a^x mod N$$

   i.e. r is the smallest integare such that $a^r = 1 \, mod \, N$.
5. if r is odd go back to step 1.
6. otherwise, $z = max\{\gcd(N, a^r - 1), \gcd(N, a^r + 1)\}$.
7. if $z = 1$ go back to step 1.
8. The factors of N are $z = \gcd(N, a^{r/2} - 1)$ and $\gcd(N, a^{r/2} + 1)$. we are done.

Example 2.4. *Let us factor* $N = 15$ *using classical order finding.*

- *Choose* $a < 15$ *such that* $\gcd(a, 15) = 1 : a = 2$.
- *Calculate* $f(x) = a^x mod 15$ *and find order* r *of* $f(x)$

x	a^x	$2^x mod 15$
x	a^x	$2^x mod 15$
1	$2^1 = 2$	$2 mod 15 = 2$
2	$2^2 = 4$	$4 mod 15 = 4$
3	$2^3 = 8$	$8 mod 15 = 8$
2	$2^4 = 16$	$16 mod 15 = 1$

Therefore $r = 4$

- *Note here in this example* r *is even:*
- *The factors of 15 are* $z = \gcd(15, 2^2 - 1) = 3$ *and* $gcd(15, 2^2 + 1) = 5$

$$3 \times 5 = 15$$

Before we start with the Quantum part we will explain important things we need in order to understand this part:

Quantum Fourier Transform (QFT): This is the backbone of the Shor's algorithm.
In this section we will first explain what the (QFT) and discrete Fourier transform (DFT) mean. This part is based on the paper [32, pp. 211-212].
The (DFT) transforms an input vector of complex numbers $x_1, x_2, \ldots, x_{n-1}$ into an output vector of complex numbers $y_1, y_2, \ldots, y_{n-1}$ expressed as:

$$y_k = \frac{1}{\sqrt{q}} \sum_{j=0}^{q-1} x_j e^{2\pi i j k / q}$$

The QFT does the same transformation as the DFT, except it operates linearly on quantum states $|0\rangle, \ldots, |q-1\rangle$, which form an orthonormal basis.

The QFT is

$$j \longrightarrow \frac{1}{\sqrt{q}} \sum_{k=0}^{q-1} e^{2\pi ijk/q} |k\rangle$$

Assume that q is power of 2 $(q = 2^n)$ then:

$$j \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle$$

Binary expression:

$$j = j_0 2^0 + j_1 2^1 + j_2 2^2 + \cdots + j_{n-1} 2^{n-1}$$
$$k = k_0 2^0 + k_1 2^1 + k_2 2^2 + \cdots + k_{n-1} 2^{n-1}$$

The term $jk/2^n$ in (2) can be written as:

$$\begin{aligned}
\frac{jk}{2^n} &= \frac{1}{2^n}(j_0 2^0 + j_1 2^1 + j_2 2^2 + \cdots + j_{n-1} 2^{n-1}) \\
&\qquad \times (k_0 2^0 + k_1 2^1 + k_2 2^2 + \cdots + k_{n-1} 2^{n-1}) \\
&= \frac{1}{2^n}[k_0(j_0 2^0 + j_1 2^1 + j_2 2^2 + \cdots + j_{n-1} 2^{n-1}) \\
&\qquad + k_1 2^1 (j_0 2^0 + j_1 2^1 + j_2 2^2 + \cdots + j_{n-1} 2^{n-1}) \\
&\qquad + \cdots + k_{n-1} 2^{n-1} (j_0 2^0 + j_1 2^1 + j_2 2^2 + \cdots + j_{n-1} 2^{n-1})] \\
&= \frac{1}{2^n}[k_0(j_0 2^0 + j_1 2^1 + j_2 2^2 + \cdots + j_{n-1} 2^{n-1})] \\
&\qquad + k_1[j_0 2^1 + j_1 2^2 + j_2 2^3 + \cdots + j_{n-1} 2^n] \\
&\qquad + \cdots + k_{n-1}[j_0 2^{n-1}] \\
&= k_0\big(\frac{j_0}{2^n} + \frac{j_1}{2^{n-1}} + \cdots + \frac{j_{n-1}}{2}\big) + k_1\big(\frac{j_0}{2^{n-1}} + \frac{j_1}{2^{n-2}} \\
&\qquad + \cdots + \frac{j_{n-1}}{2}\big) + \cdots + k_{n-1}\frac{j_0}{2}
\end{aligned}$$

Any binary fraction j can be written as follows: $j = \frac{j_l}{2} + \frac{j_{l+1}}{4} + \cdots + \frac{j_m}{2^{m-l+1}}$ and we can use notation $[j_l j_{l+1} j_{l+2} \cdots j_m]$, for instance: $[0.j_0] \rightarrow \frac{j_0}{2}$, $[0.j_0 j_1] \rightarrow \frac{j_0}{4} + \frac{j_1}{2}$, with this notation, we can write $j \longrightarrow \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi ijk/2^n} |k\rangle$ as:

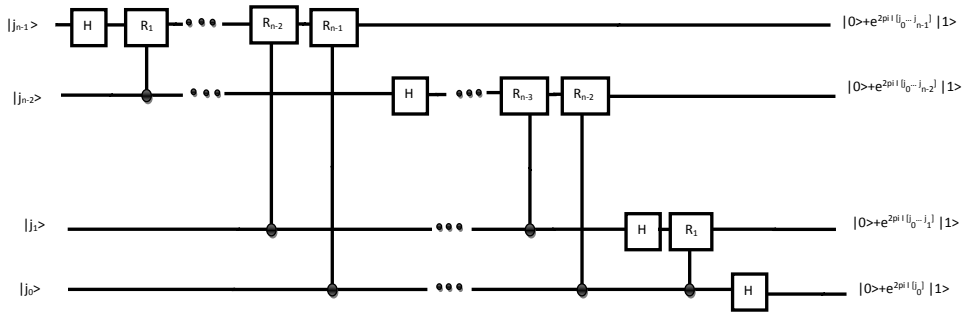
$$\frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} e^{2\pi[0.j_n]k_1} |k_1\rangle \otimes e^{2\pi[0.j_{n-1}j_n]k_2} |k_2\rangle \otimes \cdots \otimes e^{2\pi[0.j_1 j_2 \cdots j_n]k_n} |k_n\rangle$$

Where the state $|k\rangle : (k \in [0, 1])$, Then the last equation is equal to

$$\frac{1}{\sqrt{2^n}}\big(|0\rangle + e^{2\pi[0.j_n]}|1\rangle\big) \otimes \big(|0\rangle + e^{2\pi[0.j_{n-1}j_n]}|1\rangle\big) \otimes \cdots \otimes \big(|0\rangle + e^{2\pi[0.j_1 j_2 \cdots j_n]}|1\rangle$$

Quantum Part:

FIGURE 2.1: The QFT circuit consists of Hadamard gates and unitary Phase transform gates



I get this paragraph from paper [38, pg. 194-197]. To factor N, find $2\log_2 N < n < 2\log_2 \sqrt{2}N : q = 2^n$ and choose x such that $1 < x < N-1$, $\gcd(x, N) = 1$

Step 0: Initialize state.

$$|\psi_0\rangle = |00\ldots0\rangle^{\otimes n}|00\ldots0\rangle^{\otimes l}$$

Step 1: Application of $H^{\otimes n}$ on first register yielding

$$|\psi_1\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k\rangle|0\rangle$$

Step 2: Apply modular exponentiation: $f(k) = x^k mod\, N$ on second register yielding

$$|\psi_2\rangle = \frac{1}{\sqrt{2^n}}\sum_{k=0}^{2^n-1}|k, f(k)\rangle$$

Step 3: Measure the second register. Note that the second register will be in a base state where e is some power of $x\, mod\, N$ and all powers of $x\, mod\, N$ are equally likely to be observed

$$|\psi_3\rangle = \frac{1}{\sqrt{m}}\sum_{\acute{k}\in K}|\acute{k}, e\rangle,$$

$K = \{\acute{k} : x^{\acute{k}}\ mod\, N = e\}$ and $m = |K|$ is the number of elements in K

That is $K = \{\acute{k}_0, \acute{k}_0 + r, \acute{k}_0 + 2r, \ldots, \acute{k}_0 + (m-1)r\}$, $\acute{k}_0$ is first element in K.

$$|\psi_3\rangle = \frac{1}{\sqrt{m}}\sum_{j=0}^{m-1}|\acute{k}_0 + jr, e\rangle$$

Step 4: Apply the Quantum Fourier Transform (QFT) to the first register this transforms the state from

$$|\psi_3\rangle = \frac{1}{\sqrt{m}} \sum_{j=0}^{m-1} |\acute{k}_0 + jr, e\rangle \quad \text{to} \quad |\psi_4\rangle,$$

$$\begin{aligned} |\psi_4\rangle &= \frac{1}{\sqrt{qm}} \sum_{c=0}^{q-1} \sum_{j=0}^{m-1} e^{2\pi i c(\frac{\acute{k}_0 + jr}{q})} |k, e\rangle \\ &= \sum_{c=0}^{q-1} \frac{e^{\frac{2\pi i c\acute{k}_0}{q}}}{\sqrt{qm}} \sum_{j=0}^{m-1} e^{\frac{2\pi i cjr}{q}} |k, e\rangle \\ &= \sum_{c=0}^{q-1} \frac{e^{\frac{2\pi i c\acute{k}_0}{q}}}{\sqrt{qm}} \sum_{j=0}^{m-1} \zeta^j |k, e\rangle \text{ where } \zeta = e^{\frac{2\pi i cr}{q}} \end{aligned}$$

Step 5: Measure register 1. Note that register 1 has probability to be in state $|c\rangle$

$$pr(c) = \frac{1}{qm} \sum_{j=0}^{m-1} |\zeta^j|^2 \text{ where } \zeta = e^{\frac{2\pi i cr}{q}}$$

This is returns some numbers

▶ $\frac{\acute{c}}{q} \approx \frac{j}{r}$ such that $pr(\acute{c})$ is very high

But to determine the order r we need to estimate j, where is j equal to an integer number.

Step 6: We can calculate the order of N by computing the convergent of continuous fraction expansion of $\frac{\acute{c}}{q}$ and retuning the closest such fraction of $\frac{O}{r}$ where O is an integer

▶ continued fraction expansion:

$$\frac{\acute{c}}{q} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \ldots}}}}$$

▶ Convergent of Continued Fraction:
The n-th convergent of the sequence a_i is defined to be:

$$\frac{p_n}{q_n} = [a_0, a_1, a_2, \ldots, a_n]$$
$$\frac{p_0}{q_0} \approx \frac{a_0}{1} = a_0$$
$$\frac{p_1}{q_1} \approx a_0 + \frac{1}{a_1}$$
$$\frac{p_2}{q_2} \approx a_0 + \frac{1}{a_1 + \frac{1}{a_2}} = \frac{a_2 p_1 + p_0}{a_2 q_1 + q_0} = \frac{a_2(a_1 a_0 + 1)}{a_2 a_1 + 1}$$
$$\frac{p_3}{q_3} \approx a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3}}} = \frac{a_3 p_2 + p_1}{a_3 q_2 + q_1} = \frac{a_3(a_2(a_1 a_0 + 1)) + (a_1 a_0 + 1)}{a_3(a_2 a_1 + 1) + a_1}$$
$$\frac{p_n}{q_n} \approx a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots + \frac{1}{a_n}}}}} = \frac{a_n p_{n-1} + p_{n-1}}{a_n q_{n-1} + q_{n-1}}$$

Then one considers $\frac{p_n}{q_n} = [a_1, a_2, a_3, \ldots, a_n]$ converging to $\frac{\acute{c}}{q}$ ($\frac{p_n}{q_n}$ is a sequence of continued fractions of $\frac{\acute{c}}{q}$); we will use notation $\frac{j}{r_1}$ for values of continued fractions for $\frac{\acute{c}}{q}$. If $r_1 < N$ try small multiples of r_1 as possible values of r:

$$r_1, 2r_1, 3r_1, \ldots, \lfloor log\ (N^{1+\epsilon}) \rfloor\, r_1,$$

(this was suggested by Odlyzko), and check when $x^r\ mod\ N = 1$.
Finaly find $\gcd(y+1, N), \gcd(y-1, N)$ = factoring of N where $y = x^{r/2}\ mod\ N$.

Example 2.5. *Factoring $N = 21$ using Shor's algorithm.*

▶ *We have* $l = \log_2 N = 4.3 \approx 4,\ n = 2\log_2 N = 8.7 \approx 9,\ 2\log_2 \sqrt{2}N = 9.7$ *such that* $8.7 < 9 < 9.7$

▶ *Choose* $x = 8$ *such that* $1 < 8 < 21$ *and* $\gcd(8, 21) = 1$

Step 0: *Initialize state.*

$$|\psi_0\rangle = |00\ldots0\rangle^{\otimes n} |00\ldots0\rangle^{\otimes l} = |00\ldots0\rangle^{\otimes 9} |00\ldots0\rangle^{\otimes 4}$$

Step 1: *Application of $H^{\otimes n}$ on first register yielding*

$$|\psi_1\rangle = \frac{1}{\sqrt{512}} \sum_{k=0}^{511} |k, 0\rangle = \frac{1}{512}\big(|0,0\rangle + |1,0\rangle|2,0\rangle + |3,0\rangle + |4,0\rangle + \cdots + |511,0\rangle\big)$$

step 2: *Apply modular exponentiation: $f(k) = x^k\, mod\, N$*

$$|\psi_2\rangle = \frac{1}{\sqrt{512}} \sum_{k=0}^{511} |k, f(k)\rangle = \frac{1}{512}\big(|0,1\rangle + |1,8\rangle + |2,1\rangle + |3,8\rangle + \cdots + |511,8\rangle\big)$$

Step 3: *Observe register 2; Suppose we observe 8; as a power of* $x^k \bmod N$

$$|\psi_3\rangle = \frac{1}{\sqrt{256}}\big(|3,8\rangle + |5,8\rangle + |7,8\rangle + |9,8\rangle + |11,8\rangle + \cdots + |511,8\rangle\big)$$

Step 4: *Apply Quantum Fourier Transform on* $|\psi_3\rangle$ *to obtain*

$$|\psi_4\rangle = \frac{1}{131072}\sum_{c=0}^{511} e^{2\pi ic}\Big(\sum_{j=0}^{255}\zeta^j|c\rangle\Big) \text{ where } \zeta = e^{\frac{2\pi i.cr}{512}}$$

Step 5: *Measure register 1*

$$pr(c) = \frac{1}{131072}|\sum_{j=0}^{255}\zeta^j|^2 \quad \text{where } \zeta = e^{\frac{2\pi i.cr}{512}}, c \in [0,511] \text{ and } j \in [0,255]$$

Assume that we obtain $|256\rangle$

$$pr(256) = \frac{1}{131072}|\sum_{j=0}^{255} e^{2\pi ij}|^2 = 0.5$$

where $\frac{c}{2^n} = \frac{1}{2} = 0 + \frac{1}{2}$ *which can be written in continued fraction form as* $[0,2]$. *So* $r_1 = 2$. *Now we check* $x^{r_1} \bmod N$ *and we find that* $x^{r_1} \bmod N = 8^2 \bmod 21 = 1$. *Thus the required period is* 2 *where* $y = x^{\frac{r}{2}} \bmod N = 8 \bmod 21 = 8$.
Then the factor of $N = 21$ *are:* $\gcd(y \pm 1, 21) = \gcd(8 \pm 1, 21) = 3$ *and* 7.

2.4.2 Grover's Algorithm

Grover algorithm was invented by Lov Grover in 1996. The main goal for Grover's algorithm is to search an unsorted database more efficiently, with N entries requiring $O(\sqrt{N})$ time (the best classical algorithm can do this in time proportional to N).

A simple example is to find a desired file index among $N = 2^n$ files. The important things to understand for Grover algorithm are: Oracle function (black box) and quantum Oracle, see [49], [26] .

- Oracle (black box) that can recognize the solution, whose internal working is represented by a binary function

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

  Defined by:

  $$f(x) = \begin{cases} 1 & \text{if } x \text{ is a solution} \\ 0 & \text{otherwise} \end{cases}$$

- Quantum Oracle: in this case, we are given a unitary operation $|x\rangle \overset{U_w}{\to} (-1)^{f(x)}|x\rangle$ as a black box operation.

2.4.2.1 General Steps of Grovers Algorithm

Let us descibe the Grover's algorithm:
Input: A quantum Oracle U_w which performs operation $|x\rangle \stackrel{U_w}{\rightarrow} (-1)^{f(x)}|x\rangle$ where $f(x) = 0$ for all $0 \leq x \leq 2^n$ except x_0 for which $f(x_0) = 1$, n-qubits initialized to the state $|0\rangle$.

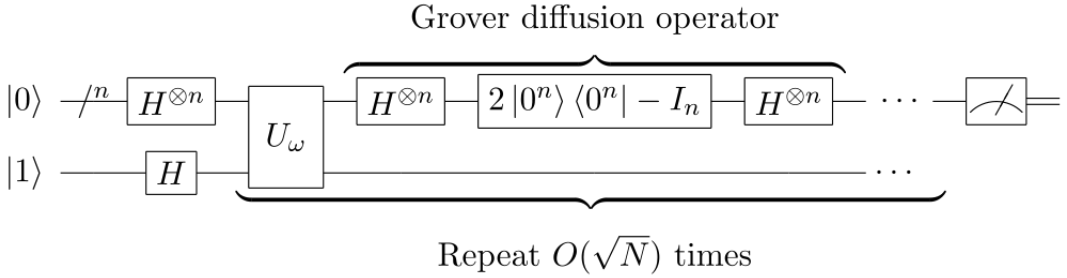
Output: x_0

Runtime: $O(\sqrt{2^n}\ )$ operations, with probability of success greater than some $q > 0$.

Procedure:

1. $\|0\rangle^{\otimes n}$	initial state
2. $H^{\otimes n}\|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} \|x\rangle = \|s\rangle$	apply the Hadmard transform to all qubits
3. $[\ 2(\|\psi\rangle\langle\psi\| - I)\ U_w]\ ^R\|\psi\rangle \approx \|w\rangle$	apply the Grover iteration $R \approx \frac{\pi}{4}\sqrt{2^n}$ times where $G = 2(\|\psi\rangle\langle\psi\| - I)\ U_w$
4. w	measure the register

FIGURE 2.2: Circuit diagram for Grover's algorithm, with a scratch qubit for the oracle



2.4.2.2 Grover iteration: How it works

Begin with: $|\psi\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$

Define $|\acute{\psi}\rangle$ as:

$$|\acute{\psi}\rangle = \frac{1}{\sqrt{N-1}} \sum_{\substack{x=0 \\ i \neq w}}^{N-1} |x\rangle$$

$$= \sqrt{\frac{N}{N-1}}|s\rangle - \frac{1}{\sqrt{N-1}}|w\rangle$$

From the first equation $\langle\acute{\psi}|w\rangle = 0$ *i.e*, $|\beta\rangle$ and $|\alpha\rangle$ are orthonormal. From the second equation we have:

$$|\psi\rangle = \sqrt{1 - \frac{1}{N}}|\acute{\psi}\rangle + \frac{1}{\sqrt{N}}|w\rangle$$

The state of the quantum computer at each step is:

$$G^k|\psi\rangle = \cos(\frac{2k+1}{2}\theta)|\acute{\psi}\rangle + \sin(\frac{2k+1}{2}\theta)|w\rangle$$

The value of θ is obtained substituting k for 0 in last equation ($G^k|s\rangle$) and comparing it with $|\psi\rangle$ equation:

$$\theta = 2\arccos\sqrt{1-\frac{1}{N}}$$

The number of times k_0 that G must be applied obeys the equation:

$$k_0\theta + \frac{\theta}{2} = \frac{\pi}{2}$$

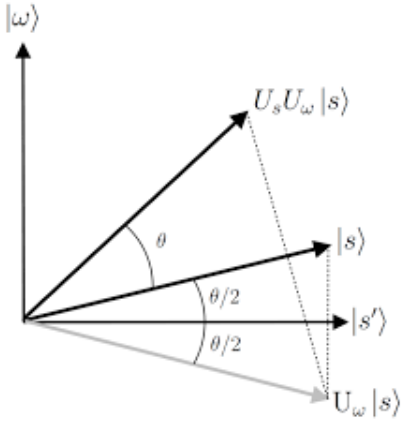
The number of steps required to find the desired element is:

$$k = round(\frac{\pi}{4}\sqrt{N}) \text{ times}$$

After applying G k times, the probability p of finding the desired element after a measurement is:

$$p = \sin^2(\frac{2k+1}{2}\theta)$$

FIGURE 2.3: Picture showing the geometric interpretation of the first iteration of Grover's algorithm. The state vector $|s\rangle$ is rotated towards the target vector $|w\rangle$ as shown



Example 2.6. *We consider a system consisting of* $N = 16 = 2^4$ *states, and the state we are searching for,* $i_0 = \beta$*, is represented by the bit string* $|1011\rangle$*.*
To describe this system, $n = 4$ *qubits are required, represented as:*
$|x\rangle = |0000\rangle + |0001\rangle + |0010\rangle + |0011\rangle + |0100\rangle + |0101\rangle + |0110\rangle + |0111\rangle + |1000\rangle + |1001\rangle + |1010\rangle + |1011\rangle + |1100\rangle + |1101\rangle + |1110\rangle + |1111\rangle$

Grover's algorithm begins with a system initialized to 0*:* $|0000\rangle$
and then apply the Hadamard transformation to obtain equal amplitudes associated with each state of $\frac{1}{\sqrt{N}} = \frac{1}{\sqrt{16}} = \frac{1}{4}$ *and thus also equal probability of being in any of*

the 16 *possible states:*

$$H^{\otimes 4}|0000\rangle = \frac{1}{4}\sum_{x=0}^{15}|x\rangle$$

The Grover iteration will be repeated $k = \frac{\pi}{4}\sqrt{N}$ *times. In our case* $k = \frac{\pi}{4}\sqrt{16} = 3.1415$ *which rounds to 3 iterations.*
Now, perform the diffusion transform $[2|s\rangle\langle s| - I]|x\rangle$

$$\begin{aligned}[2|\psi\rangle\langle\psi| - I]|x\rangle &= [2|\psi\rangle\langle\psi| - I][|\psi\rangle - \frac{2}{4}|1011\rangle \\ &= 2|\psi\rangle\langle\psi|\psi\rangle - |\psi\rangle - 2(\frac{2}{4})|\psi\rangle\langle\psi|1011\rangle + \frac{2}{4}|1011\rangle\end{aligned}$$

Note that $16 \times \frac{1}{4}\left(\frac{1}{4}\right)$. *Additionally, we can use* $\langle\psi|1011\rangle = \langle 1011|s\rangle = \frac{1}{4}$, *so*

$$\begin{aligned}&= |\psi\rangle - \frac{1}{4}|\psi\rangle + \frac{1}{2}|1011\rangle \\ &= \frac{3}{4}|\psi\rangle + \frac{1}{2}|1011\rangle\end{aligned}$$

Substituting $|\psi\rangle = \frac{1}{4}\sum_{x=0}^{15}|x\rangle$ *gives:*

$$\begin{aligned}&= \frac{3}{4}\Big[\frac{1}{4}\sum_{x=0}^{15}|x\rangle\Big] + \frac{1}{2}|1011\rangle \\ &= \frac{3}{16}\sum_{\substack{x=0\\x\neq 11}}^{15}|x\rangle + \Big[\frac{3}{16}|1011\rangle + \frac{1}{2}|1011\rangle\Big] \\ \implies |x_1\rangle &= \frac{3}{16}\sum_{\substack{x=0\\x\neq 11}}^{15}|x\rangle + \frac{11}{16}|1011\rangle\end{aligned}$$

This is completes the first iteration.

We apply the same two transformations in the second iteration (Oracle) in Grover algorithm, which gives:

$$\begin{aligned}|x_2\rangle &= \frac{3}{16}\sum_{\substack{x=0\\x\neq 11}}^{15}|x\rangle - \frac{11}{16}|1011\rangle \\ &= \frac{3}{16}\sum_{\substack{x=0\\x\neq 11}}^{15}|x\rangle + \Big[-\frac{11}{16}|1011\rangle - \frac{3}{16}|1011\rangle\Big]\end{aligned}$$

After the Oracle query, and after applying the diffusion transform:

$$\begin{aligned}[2|\psi\rangle\langle\psi| - I][\frac{3}{4}|\psi\rangle - \frac{7}{8}|1011\rangle] &= 2\Big(\frac{3}{4}\Big)|\psi\rangle\langle\psi|\psi\rangle - \frac{3}{4}|\psi\rangle - 2\Big(\frac{7}{8}\Big)|\psi\rangle\langle\psi|1011\rangle \\ &= \frac{3}{2}|\psi\rangle - \frac{3}{4}|\psi\rangle - \frac{7}{4}|\psi\rangle\Big(\frac{1}{4}\Big) + \frac{7}{8}|1011\rangle \\ &= \frac{5}{16}|\psi\rangle + \frac{7}{8}|1011\rangle \\ &= \frac{5}{16}\Big[\frac{1}{4}\sum_{\substack{x=0\\x\neq 11}}^{15}|x\rangle + \frac{1}{4}|1011\rangle\Big] + \frac{7}{8}|1011\rangle \\ \implies |x_3\rangle &= \frac{5}{64}\sum_{\substack{x=0\\x\neq 11}}^{15}|x\rangle + \frac{61}{64}|1011\rangle\end{aligned}$$

We apply the same two transformations in the third iteration:

$$|x_4\rangle = \frac{5}{64}\sum_{\substack{x=0\\x\neq 11}}^{15}|x\rangle - \frac{61}{64}|1011\rangle$$

After the oracle query, and after applying the diffusion transform:

$$\begin{aligned}[2|\psi\rangle\langle\psi| - I][\frac{5}{16}|\psi\rangle - \frac{33}{32}|1011\rangle] &= 2\Big(\frac{5}{16}\Big)|\psi\rangle\langle\psi|\psi\rangle - \frac{5}{16}|\psi\rangle \\ &\quad - 2\Big(\frac{33}{32}\Big)|\psi\rangle\langle\psi|1011\rangle + \frac{33}{32}|1011\rangle \\ &= \frac{5}{8}|\psi\rangle - \frac{5}{16}|\psi\rangle - \frac{33}{16}|\psi\rangle\Big(\frac{1}{4}\Big) + \frac{33}{32}|1011\rangle \\ &= \frac{13}{64}|\psi\rangle + \frac{33}{32}|1011\rangle \\ &= \frac{13}{256}\sum_{x=0}^{15}|x\rangle + \frac{33}{32}|1011\rangle \\ &= \frac{13}{256}\sum_{\substack{x=0\\x\neq 11}}^{15}|x\rangle + \Big[\frac{33}{32}|1011\rangle + \frac{13}{256}|1011\rangle\Big] \\ \implies |x_5\rangle &= \frac{13}{256}\sum_{\substack{x=0\\i\neq 11}}^{15}|x\rangle + \frac{251}{256}|1011\rangle\end{aligned}$$

Longer format:
$|x_5\rangle = \frac{13}{256}|0000\rangle + \frac{13}{256}|0001\rangle + \frac{13}{256}|0010\rangle + \frac{13}{256}|0011\rangle + \frac{13}{256}|0100\rangle + \frac{13}{256}|0101\rangle + \frac{13}{256}|0110\rangle + \frac{13}{256}|0111\rangle + \frac{13}{256}|1000\rangle + \frac{13}{256}|1001\rangle + \frac{13}{256}|1010\rangle + \frac{251}{6256}|1011\rangle + \frac{13}{256}|1100\rangle + \frac{13}{256}|1101\rangle + \frac{13}{256}|1110\rangle + \frac{13}{256}|1111\rangle$
Finally, to test Grover algorithm, we calculate the probability to find the state. We find :

$$p = \Big|\frac{251}{256}\Big|^2 = \Big|\frac{63001}{65536}\Big| = 96\%$$

The chance of getting the result $|1011\rangle$*, is around* 96%*. and we observe that success probability after each iteration four qubits is as follows:*
After the first iteration:

$$p = \left|\frac{11}{16}\right|^2 = \left|\frac{121}{256}\right| = 47\%$$

After the second iteration:

$$p = \left|\frac{61}{64}\right|^2 = \left|\frac{3721}{4096}\right| = 90\%$$

After the third iteration:

$$p = \left|\frac{251}{256}\right|^2 = \left|\frac{63001}{65536}\right| = 96\%$$

Chapter 3

Cryptography and Contract Signing

3.1 Cryptography in General

When we want to keep information secret, we have two possible strategies: hide the existence of the information, or make it unintelligible (cryptography), see [33, pg. 4] .

Definition 3.1. *Cryptography* is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication.

The term cryptography comes from the two Greek words *skrupto* and *graph*, which, when literally translated, means "secret writing". Cryptography is the process of disguising the messages (information security) so that it can only be read by sender and receiver, in other words enabling sender and receiver to mask confidential messages and to make tranmitted data illegible to any unauthorized third party, (see [42]).

The branch of mathematics encompassing both cryptography and cryptanalysis (decrypting of information or breaking the cryptographic designs) is cryptology .

$$\text{cryptology} = \text{cryptography} + \text{cryptanalysis}$$

A system to encrypt and decrypt information is known as cryptosystem.

Definition 3.2. *Cryptosystem* is a quintuple $(\mathcal{P};\mathcal{C};\mathcal{K};\mathcal{E};\mathcal{D})$ such that:

1. $\mathcal{P}$,$\mathcal{C}$, and $\mathcal{K}$ are finite sets, where
   - $\mathcal{P}$ is the plain text space or clear text space,
   - $\mathcal{C}$ is the cypher text space, and
   - $\mathcal{K}$ is the key space.

   Elements of $\mathcal{P}$ are referred to as plain text, and elements of $\mathcal{C}$ are referred to as cypher text. A message is a string of plain text symbols.
2. $\mathcal{E} = \{E_k | k \in \mathcal{K}\}$ is a family of functions $E_k : \mathcal{P} \to \mathcal{C}$ that are used for encryption, and $\mathcal{D} = \{D_k | k \in \mathcal{K}\}$ is a family of functions $D_k : \mathcal{C} \to \mathcal{P}$ that are used for decryption.

3. For each key $e \in \mathcal{K}$ there exists a key $d \in \mathcal{K}$ such that for each $p \in \mathcal{P}$:

$$D_d(E_e(p)) = p$$

A cryptosystem is called symmetric if $d = e$ (the same key is used to encrypt and decrypt information), or if d can at least be easily computed from e.
A cryptosystem is called asymmetric if $d \neq e$ (one key is used to encrypt and a different key to decrypt) and it is computationally infeasible in practice to compute d from e. Here, d is the private key and e is the public key. Public key is known both to the sender and to the adversary, but only the receiver can decrypt cipher because he or she knows the secret private key, and the steps as follows:

1. The sender converts the message into ciphertext using an encryption system.
   private key + plaintext $\longrightarrow$ ciphertext
2. The receiver converts the ciphertext back into plaintext using a corresponding system.
   private key + ciphertext $\longrightarrow$ plaintext

3.1.1 RSA Algorithm

The RSA algorithm was first published in 1977 by group of three scientists, namely Ron Rivest, Adi Shamir and Len Adleman. It is a form of asymmetric cryptography and is used to encrypt and decrypt in message communication for making the communication secure where one user (part) uses public key and other user uses secret (private key), see [2, pp. 48-50] .

In order to understand RSA encryption we need the Euclidean Algorithm (Theorem 1), the method of successive squaring, Fermat's Little Theorem and the Chinese Remainder Theorem, see [14].

Definition 3.3. *(Euler's Phi Function)* Let n be a positive integer. Eulers Phi Function, denoted $\phi(n)$, is the number of positive integers $\leq n$ which are relatively prime to n, computed as:

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$

For example $\phi(6) = 6 \times (1 - \frac{1}{2}) \times (1 - \frac{1}{3}) = 2$ because in the set $\{1, 2, 3, 4, 5, 6\}$ only two numbers 1 and 5 are coprime to 6.

Lemma 1. *If n is prime, then* $\phi(n) = n - 1$.

Proof. Let n be a prime number. Since n is prime, $1, 2, 3, 4, ..., n-1$ are relatively prime to n. Therefore, $\phi(n) = n - 1$. □

If p and q are prime, then $\phi(pq) = \phi(p)\phi(q) = (p-1)(q-1)$.

Theorem 2. ***(Euler's Theorem)*** *If a and n are two relatively prime positive integers, then*

$$a^{\phi(n)} \equiv 1 (mod\ n).$$

For instance, when $p = 3$ and $q = 5$ then

$$a^8 = 1(mod\ 15)$$

for any integer a that has no common divisior with pq; we verify that

$$2^8 = 1(mod\ 15)$$
$$4^8 = 1(mod\ 15)$$
$$7^8 = 1(mod\ 15)$$

The particular case in which n is a prime number p, Euler's theorem is called Fermat's Little Theorem.
We use the following Lemma to prove the Fermat's Little Theorem:

Lemma 2. *For any prime p, we have*

$$(x + y)^p = x^p + y^p\ mod(p).$$

Theorem 3. ***(Fermat's Little Theorem)*** *For any prime p and any positive integer a,*

$$a^p \equiv a(mod\ p)$$

Proof. There are several proofs using different techniques to prove the statement $a^p \equiv a(mod\ p)$ but the most straightforward way to prove this theorem is by applying the induction principle.
The proof is by induction on a. When $a = 1$ is obviously true. $a^p = 1^p = 1 = a$ so $1^p \equiv 1(mod\ p)$
Assume that $k^p \equiv k(mod\ p)$ (inductive hypothesis) and consider $(k + 1)^p$. By the previous lemma, we have $(k+1)^p \equiv k^p+1^p(mod\ p)$ and inductive hypothesis gives:

$$(k + 1)^p \equiv (k + 1)(mod\ p)$$

By the principle of induction, it follows that $a^p \equiv a(mod\ p)$, for every positive integer a. □

For instance, if $a = 2$ and $p = 7$, then we have, in fact, $2^{7-1} = 2^6 = 64 = 1+9\cdot 7 \equiv 1(mod\ 7)$.

Theorem 4. ***(Chinese Remainder Theorem)*** *(see [10][pp. 194–207] and [8][p .147])*
Let $m_1, m_2, \ldots, m_n$ be distinct positive integers such that $gcd(m_i, m_j) = 1$ if $i \neq j$.
Then, for any integers $a_1, a_2, \ldots, a_n$, consider the simultaneous congruences

$$x \equiv a_1(mod\ m_1)$$
$$x \equiv a_2(mod\ m_2)$$
$$x \equiv a_3(mod\ m_3)$$
$$\vdots$$
$$x \equiv a_n(mod\ m_n)$$

There exists an unique modulo solution of the system of simultaneous congruences above:

$$x = a_1M_1y_1 + a_2M_2y_2 + \cdots + a_nM_ny_n(mod\ M)$$

where $M = m_1 m_2 \dots m_n$, $M_1 = \dfrac{M}{m_1}, \dots, M_n = \dfrac{M}{m_n}$ *and* $M_1 y_1 \equiv 1(mod\ m_1)$, $\dots, M_n y_n \equiv 1(mod\ m_n)$

Example 3.1. *Find solutions to*

$$x \equiv 3(mod\ 5)$$
$$x \equiv 7(mod\ 8)$$
$$x \equiv 5(mod\ 7)$$

Solution:
We have $a_1 = 3,\ a_2 = 7,\ a_2 = 7,\ a_3 = 5,\ m_1 = 5,\ m_2 = 8,\ m_3 = 7$ and $M = 5 * 8 * 7 = 280$

$$M_1 = \frac{M}{m_1} = \frac{280}{5} = 56$$
$$M_2 = \frac{M}{m_2} = \frac{280}{8} = 35$$
$$M_3 = \frac{M}{m_3} = \frac{280}{7} = 40$$

we still need to find y_1, y_2 and y_3, so we need to solve the equation

$$56\, y_1 \equiv 1(mod\ 5)$$
$$56\, y_2 \equiv 1(mod\ 8)$$
$$40\, y_3 \equiv 1(mod\ 7)$$

Therefore $y_1 = 1, y_2 = 3$ and $y_3 = 3$
Then

$$x = \underbrace{\overbrace{(8*7)*1*3}^{\equiv 1\ mod\ 5}}_{\equiv 3\ mod\ 5} + \underbrace{\overbrace{(5*7)*3*7}^{\equiv 1\ mod\ 8}}_{\equiv 7\ mod\ 8} + \underbrace{\overbrace{(5*8)*3*5}^{\equiv 1\ mod\ 7}}_{\equiv 2\ mod\ 7}$$

The RSA algorithm involves three steps (see [2][pp. 15,16] and [41][pp. 165-168]): key generation, encryption and decryption:

3.1.1.1 Key Generation:

1. We begin by choosing two large prime numbers, p and q.
2. We compute $n = p \times q$.
3. We compute the Euler's function $\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1)$.
4. Next we choose a small number e such that $\gcd(e, \varphi(n)) = 1$ and find d such that $ed = 1\ mod\ \varphi(n)$, in other words $d = e^{-1}\ mod(\varphi(n))$.
5. We now have two key values:
   The public key: (n, e)
   The private key: (n, d)

3.1.1.2 Encryption and Decryption:

1. To encrypt a message m so it results in ciphertext c we use the following:

$$c = m^e mod\ n \quad \text{(remember encryption is done with the public key)}$$

2. To decrypt a message c so it results in plaintext c we use the following:

$$m = c^d mod\ n \quad \text{(remember decryption is done with private key)}$$

Theorem 5. ***(The correctness of the RSA algorithm).*** *(see [22])*
Let m, c, n, e, d be plaintext, ciphertext, encryption exponent and modules respectively, then

$$c = m^e mod\ n$$
$$m = c^d mod\ n$$

So

$$c^d = m\ mod\ n$$

Proof. Follows from Euler's theorem:

$$a^{\phi(n)} \equiv 1 (mod\ n)$$

since we have $ed = 1\ mod\, \phi(n) \implies ed = k\phi(n) + 1$ for some integer k, we can write

$$\begin{aligned} c^d &= (m^e)^d mod\ n \\ &= m^{ed} mod\ n \\ &= m^{k\phi(n)+1} mod\ n \\ &= m.(m^{\phi(n)})^k mod\ n \\ &= m.1^k mod\ n \\ &= m\ mod\ n \end{aligned}$$

□

So now that we know the theory behind how RSA encryption works, lets consider one example.

Example 3.2. *Take two large primes: p=37, q=23*
The product of p and q is n, in our case:

$$n = p \times q = 37 \times 23 = 851$$

The Euler's phi function, $\phi(n)$ is calculated below:

$$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1) = 36 \times 22 = 792$$

Now we have to choose $e = 5$ such that $e < n$ and $\gcd(e, \varphi(n)) = 1$. We can use 5, as $5 < 851$ and $\gcd(5, 792) = 1$. The pair (e, n) is our public key that is used

to encrypt messages, so the private key key: $(n, e) = (851, 5)$
We must find a number such that: $ed = 1 mod\ \varphi(n)$ *using Euclid's algorithm, we get* $d = 317$. *So the private key:* $(n, d) = (851, 317)$.
Suppose the plaintext value m *is 88 then,*
For encryption: sender wishes to send to receiver the message m, *sender computes ciphertext as* $c = m^e mod\ n$ *and sends it to receiver:*
Here we use the Chinese Remainder theorem, an easy way to solve $m^e mod\ n$ *(Ciphertext)*

$$\begin{aligned} c &= m^e mod\ n \\ &= 88^5 mod\ 851 \\ &= 103 \end{aligned}$$

For decryption:
receiver gets the ciphertext from sender:

$$\begin{aligned} m &= c^d mod\ n \\ &= 103^{317} mod\ 851 \\ &= 88 \end{aligned}$$

reciver knows the message is 88.

3.2 Digital Signatures

One way, in which RSA algorithm (or public key cryptography) is used, is for digital signatures. They provide an authentication mechanism that adds to a message a code, *a signature*, which corresponds to a message, but can be linked to the author.

In a way, it is public key cryptography in reverse - it uses private key for encryption, but public key for decryption.

Each digital signature requires three elements.

- Way to generate keys, at random. A private and a public key are generated.
- Way to sign a message, i.e. attach a small signature corresponding to each given message and private key.
- Way to verify the signature, i.e. using a public key and signed message, checks signature's authenticity.

Example 3.3. *Consider RSA protocol, but in reverse, i.e. such that key for encoding* e *is private, and key for decoding* d *is public. Then a signature would be computed as*

$$s = m^e\ (mod\ N),$$

and can be checked using d *by comparing* $s^d\ (mod\ N)$ *and* m.

The signer sends some message, M, and appends his signature s, using shortened version of message, $m = h(M)$, computed according to some publicly known function h, usually a function which is easy to compute but difficult to reverse, like so called hash functions.

3.3 Quantum Cryptography and Quantum Key Distribution

Quantum mechanics has some natural advantages for cryptography. For example, random numbers are generated by measurements, and there is no need for pseudorandom generators. This was noted in 1984. by Charles Bennett and Gilles Brassard (see [47]), who proposed the first quantum cryptography protocol, known as BB84.

This is a protocol for distribution of keys between two parties, Alice and Bob. The key is a n-bit sequence k. The message m is transformed to ciphertext c by bitwise addition, $c = m + k \ (mod\ 2)$, and then the plaintext is recovered as $m = p = c + k \ (mod\ 2)$ by bitwise addition of key bits.

To distribute the secret key between Alice and Bob, in BB84 EPR states are used. To protect against the third party eavesdropping, a N pairs of entangled qubits are used, where $N > n$. Each qubit is shared as an EPR state

$$\begin{aligned} |\psi^+\rangle &= \frac{1}{\sqrt{2}}\big(|0\rangle_1|1\rangle_2 + |1\rangle_1|0\rangle_2\big) \\ &= \frac{1}{\sqrt{2}}\big(|+\rangle_1|-\rangle_2 + |-\rangle_1|+\rangle_2\big) \end{aligned}$$

Where $\{|+\rangle, |-\rangle\}$ will be the the "reject basis", $\{|0\rangle, |1\rangle\}$ will be the the "accept basis"

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle),\ |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle),\ |0\rangle = \begin{bmatrix}1\\0\end{bmatrix} \text{ and } |1\rangle = \begin{bmatrix}0\\1\end{bmatrix}$$

The accept observable

$$\hat{A} = 1.|1\rangle\langle 1| + 0.|0\rangle\langle 0|$$

and the reject observable

$$\hat{R} = 1.|+\rangle\langle +| + 0.|-\rangle\langle -|$$

To generate a key, Alice chooses for each qubit either basis $\hat{A}$ or basis $\hat{R}$ to measure, and announces her choice publicly. Then Bob measures the same basis on his corresponding qubits, and gets to know results that Alice got. Out of the measured N qubits, randomly and publicly chosen n are used to get a secret shared key, and the remaining $N - n$ are compared, again publicly. If they do not match, that is used as evidence of eavesdropping, and in that case everything is repeated. The proof of security of BB84 was obtained much later, see for instance paper [47].

3.4 Contract Signing

Contract signing is a legal process, in which two parties (Alice and Bob) make a binding agreement. In law, it is defined in the following way:

Definition 3.4. Contract is a legally binding agreement made between two or more parties who intend it to have legal effect and for which the law will provide a remedy in the event of breach (see [19, pp. 3-16],[11, pp. 194-198]) .

The agreement can be formal, informal, written, oral or just plain understood. Some contracts are required to be in writing in order to be enforced. Legal terminology distinguishes offeror the party who makes an offer to enter in to a contract, and offeree the party to whom an offer to inter into a contract is made ,see [27, p. 375] .
The necessary essential elements to form a binding contract are usually described as:

1. An offer: is a proposal by one party (the offeror) to do or to give something and accepted by another party (the offeree).

2. An acceptance: To binding contract , there must be an acceptance of the offer and it is done by compliance with the terms of the offer by the party receiving the offer (offeree). Both of them (offer and acceptance) are called "mutual assent" means there must meeting of minds.

   The objective of the contract must be for a legal purpose. For example, a contract for illegal distribution of weapons is not a binding contract because the purpose for which it exists is not legal. if the parties violate the law.the contract will deemed to be "void" .

3. Consideration, i.e. something of value offered by offeror and accepted by offeree.

4. Competent Parties:
   meaning the parties who are legally qualified (that is, have the capacity) to make a binding contractual agreement, see [9, pp. 353-356] .

If the contract complies with all essential elements, it is *a valid contract*, if the has no legal effect at all then the contract is *a void*, see [15, p. 191].

Traditionally, paper-based contracts are signed by the transacting parties who need to be present at the same place and at the same time. Each party signs a copy of the contract and exchange signed papers, so that every party gets a copy of the signed contract.

When parties involved are physically far apart, alternative in this case signing an *electronic/digital signature* contract. However, that poses a problem: one party can get commitment from other party (a copy of the contract with her/his signature on it) without committing himself (Cheater). The solution to this problem is to get *a fair* and *viable* contract signing protocol by involving a trusted third party (TTP), which we will call Trent, to which both signers always send their signatures directly to it, see [29, p. 367].

Definition 3.5. *Fair protocol* means that either both parties get each others' commitment or none gets.

An unfair protocol is one in which one party has proof of commitment from the other, but does not commit itself. Thus, for instance in stock market, one party may want to buy futures or options, without commiting to the contract if the events on the maket do not go to its advantage. Naturally, this is a highly undesirable situation.

Definition 3.6. *Viable protocol* is one where, if both parties behave honestly, they will both get each others' commitments.

It can be shown that it is impossible to design a fair and viable contract signing protocol, without involving the trusted party (i.e. Alice and Bob have to rely on Trent).
However, it is desirable to involve Trent (i.e. a trusted third party) as little as possible.

Definition 3.7. *Optimistic protocols* are protocols in which the third trusted party in involved only when one party is cheating or the communication is interrupted.

In optimistic protocols, Alice and Bob *exchange* messages, so that in the end both parties will end up with signed contract. However, if there is a disruption or evidence of cheating, the parties have an option to invoke Trent, who would then *bind* the contract, assuring fairness.

Some protocols are only probabilisticaly fair, i.e. there is a small probability of advantage to one party. Such protocols have been designed using clasicall cryptography, which are both optimistic and probabilisticaly fair.

In classical cryptography, contract signing relies on digital signatures. However, using peculiarities of quantum mechanics, it is possible to design quantum contract signing protocols which do not rely on signed messages, see [39].

Chapter 4

Asymptotics of Quantum Contract Signing

4.1 Paunković-Bouda-Mateus Protocol

The idea of quantum contract signing is to use a pair of non-commuting observables (quantum complementarity), and inherent properties of quantum mechanics, to achieve a probabilistically fair, viable and optimistic protocol, without reliance on the digital signatures.

In [39], the following protocol is proposed for that purpose. Trent, a trusted third party, sends to Alice and Bob in *initialisation phase*, N qubits each, and classical data about the qubits received by the other party. In *exchange phase*, Alice and Bob make measurements of their choice on their qubits, and send the results to the other party in alternating turns. This phase does not involve Trent (protocol is optimistic). However, if the exchange is interrupted or there is evidence of cheating, they have an option to invoke Trent again. In this case *binding phase* occurs. They present to Trent their results of measurements and claims about which observables they measured. Trent then decides if the contract is a void, or if it is bound by the presented results. The idea is, that the party which was honest, has a way to enforce the contract (i.e. bind it) or reject it, the moment it notices a problem (i.e. evidence of cheating by the other party).
Let

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

and

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

Thus, $\{|+\rangle, |-\rangle\}$ is an alternative orthonormal qubit frame. We will call this frame the "reject basis", while $\{|0\rangle, |1\rangle\}$ will be the "accept basis". Define

$$\hat{A} = 1 \cdot |1\rangle\langle 1| + 0 \cdot |0\rangle\langle 0|$$
$$\hat{R} = 1 \cdot |+\rangle\langle +| + 0 \cdot |-\rangle\langle -|$$

to be the corresponding accept and reject observables.

- In the initialization phase, Trent chooses, at random, N qubits, out of the set $\{|+\rangle, |-\rangle, |0\rangle, |1\rangle\}$, to Alice, and similarly, randomly chosen N qubits from the same set to Bob. In addition, Trent lets Alice know which qubits are sent to Bob, and lets Bob know which qubits are sent to Alice. Thus, Alice has N qubits but does not know (without performing measurement) which ones she has, while Bob knows which qubits are sent to her, and vice versa.
- In the exchange phase, Trent is not involved. If Alice wants to accept the contract, she will measure her first qubit in the accept basis (i.e. measure obserable $\hat{A}$ on her first qubit), and send result to Bob. If she wants to reject the contract, she will measure $\hat{R}$ instead. Then Bob reciprociates, by measuring either accept or reject observable on his first qubit, and sends result to Alice. The process continues untill all N qubits are measured.
- Note that roughly half of the qubits sent to each Alice and Bob are in reject, and half in accept basis. Thus, parties can note what the other party is measuring, by comparing the results sent to them on the qubits which are in the corresponding basis, when there should be a perfect agreement with the classical information sent by Trent. Thus, if both parties are honest and want to accept the contract, they will note this and do not need to invoke Trent (i.e. protocol is viable). However, if they notice that there is evidence of cheating (for instance, change in basis being measured), they have an option to stop communication, and proceed to binding. In this case, they will have an option to try to bind contract, by measuring all the remaining qubits in the accept basis, or refuse the contract, by measuring all the remaining qubits in the reject basis. After that they send all of their results to Trent, together with information about which observables they measured.
- In the binding phase, when it occurs, Trent makes the ultimate decision if the contract is binding, or rejected/void. In order to do that, Trent will get results of the measurement on all of their qubits by both Alice and Bob. Then he choses, according to a pre-defined (by the protocol, this is something defined in advance) probability distribution a number α between $1/2$ and 1. The contract is binding to both parties, if at least a fraction α of Alice's qubits from accept basis are measured correctly, and also less that α fraction of Bob's reject qubits are measured correctly by Bob, or vice versa. If there is evidence that Alice cheated (did not measure the basis she reported she did), only Bob's results will count, and similarily if Bob cheated, only Alice will be taken into account. In all other cases, contract is declared invalid.

Paunković, Bouda and Mateus have shown that protocol is viable and proabilistically fair, and that probability of cheating can be made arbitrarily small. They have hypothesized that as N goes to infinity, probability of cheating goes to zero as $N^{-1/2}$, but have shown this only by numerical evidence.
The probability of cheating, computed in [39], depends on the strategy of the cheating party. Namely, out of N qubits, a number of them, say m, can be measured in the attempt to cheat, and thus strategies of cheating that they considered are indexed by a number m. For given m, and α chosen by Trent, probability of successful cheating is then given by:

$$P_{ch}(m;\alpha) = P_R(m;\alpha)(1 - P_R(m;\alpha)) \tag{4.1}$$

for a given m between 0 and N, and $\alpha \in (0.5, 1)$, where $P_R(m;\alpha)$, the expected probability to reject contract is:

$$P_R(m;\alpha) = \sum_{N_R=0}^{N} q(N_R) P_1(m;\alpha,N_R) \tag{4.2}$$

Here $q(N_R)$ is the probability to have exactly N_R states from the reject basis:

$$q(N_R) = 2^{-N}\binom{N}{N_R}, \sum_{N_R=0}^{N} q(N_R) = \sum_{N_R=0}^{N} 2^{-N}\binom{N}{N_R} = 1$$

and $P_1(m;\alpha,N_R)$ is the probability to (be able to) reject the contract.

$$P_1(m;\alpha,N_R) = \sum_{n=n'}^{m'} P_2(n;m,N_R) P_3(n;\alpha,N_R) \tag{4.3}$$

Here $n' = \begin{cases} m - N_R & \text{if } m \geq N_R \\ 0 & \text{otherwise} \end{cases}$, $m' = \begin{cases} N_R & \text{if } m \geq N_R \\ m & \text{otherwise} \end{cases}$

$$P_2(n;m,N_R) = \binom{m}{n}\binom{N-m}{N_R-n}\binom{N}{N_R}^{-1} \tag{4.4}$$

$$P_3(n;\alpha,N_R) = 2^{-n}\sum_{i=0}^{T}\binom{n}{i} \tag{4.5}$$

$T = \begin{cases} n & \text{if } n < (1-\alpha)N_R \\ (1-\alpha)N_R & \text{otherwise} \end{cases}$

Note that these values are of various probabilities, and between 0 and 1.
Finally, if $p(\alpha)$ is Trent's probability distribution for choosing α, probability of cheating for cheater strategy indexed by m is given by

$$P_{ch}(m) = \int p(\alpha) P_{ch}(m;\alpha) d\alpha$$

and one wants to estimate maximum of this over all m between 0 and N, which represents the maximal probability of cheating.

4.2 Necessity of Parameter Randomization

It turns out that for probability of cheating to go to zero, Trent's random choice of α according to some non-singular probability distribution $p(\alpha)$ is essential. If α were known in advance, Alice (or Bob) could chose m accordingly, and make probability of cheating as much as 25%, no matter how large N is.

This illustrates why we have to assume that $p(\alpha)$ is a bounded probability density, or at least that no single value α is chosen with non-zero probability.
This is because of the following result (see [28]).

Theorem 6. *For any fixed $\alpha \in (0.5, 1)$ and $\varepsilon < 0.25$, maximum over all m between 0 and N of $P_{ch}(m;\alpha)$ will be greater than ε if N is large enough. Moreover, $P_{ch}(2(1-\alpha)N;\alpha)$ tends to $1/4$ as N goes to infinity.*

Proof. We will set $m = 2(1-\alpha)N$ in equation (4.1), or integer part of that (we shall omit the integer part according to our notation convention, for brevity). Subsequently the probability to cheat is given by:

$$P_{ch}(2(1-\alpha)N;\alpha) = P_R(2(1-\alpha)N;\alpha)(1 - P_R(2(1-\alpha)N;\alpha)) \tag{4.6}$$

We will show that $P_R(2(1-\alpha)N;\alpha)$ tends to $1/2$ as N goes to infinity, and this will prove our result, as the maximum of the function $x(1-x)$ is $1/4$, achieved at $x = 1/2$. For convenience of the estimates, we will introduce a number c, and assume $N \gg c^2$, and prove that the limit is $1/2$ when both c and N tend to infinity; we may think of this limit as a repeated limit of P_R, $\lim_{c\to\infty}\lim_{N\to\infty} P_R$, or of its estimates (which may in fact depend on c) .
The expected probability to reject contract $P_R(2(1-\alpha)N;\alpha)$ is:

$$P_R(2(1-\alpha)N;\alpha) = \sum_{\frac{N}{2}-c\sqrt{N}<N_R<\frac{N}{2}+c\sqrt{N}} q(N_R)P_1\big(2(1-\alpha)N;\alpha,N_R\big) \tag{4.7}$$

$$+ \sum_{N_R=0}^{\frac{N}{2}-c\sqrt{N}} q(N_R)P_1\big(2(1-\alpha)N;\alpha,N_R\big) \tag{4.8}$$

$$+ \sum_{N_R\geq\frac{N}{2}+c\sqrt{N}}^{N} q(N_R)P_1\big(2(1-\alpha)N;\alpha,N_R\big) \tag{4.9}$$

Here $0 \leq P_R(2(1-\alpha)N;\alpha) \leq 1$, $q(N_R)$ is the probability to have exactly N_R states from the reject basis: $q(N_R) = 2^{-N}\binom{N}{N_R}$, $\sum_{N_R=0}^{N} q(N_R) = \sum_{N_R=0}^{N} 2^{-N}\binom{N}{N_R} = 1$.
We can use Hoeffding's inequality, see [20], for binomial distribution

$$2^{-n}\sum_{i=0}^{n(1/2-\epsilon)}\binom{n}{i} \leq e^{-2\epsilon^2 n}, \quad 2^{-n}\sum_{i=0}^{n(1/2+\epsilon)}\binom{n}{i} \geq 1 - e^{-2\epsilon^2 n} \tag{4.10}$$

to estimate the last two sums:

$$\sum_{N_R=0}^{\frac{N}{2}-c\sqrt{N}} q(N_R)P_1\big(2(1-\alpha)N;\alpha,N_R\big) \leq \sum_{N_R=0}^{\frac{N}{2}-c\sqrt{N}} q(N_R)$$

$$\sum_{N_R=0}^{\frac{N}{2}-c\sqrt{N}} q(N_R) = 2^{-N}\sum_{N_R=0}^{N(\frac{1}{2}-\frac{c}{\sqrt{N}})}\binom{N}{N_R} \leq e^{-2\frac{c^2}{N}N} = e^{-2c^2}$$

$$\sum_{N_R \geq \frac{N}{2}+c\sqrt{N}}^{N} q(N_R) P_1\big(2(1-\alpha)N;\alpha,N_R\big) \leq \sum_{N_R \geq \frac{N}{2}+c\sqrt{N}}^{N} q(N_R)$$

$$\sum_{N_R \geq \frac{N}{2}+c\sqrt{N}}^{N} q(N_R) = 1 - \Big(\sum_{N_R=0}^{\frac{N}{2}+c\sqrt{N}} q(N_R)\Big)$$

$$\sum_{N_R=0}^{\frac{N}{2}+c\sqrt{N}} q(N_R) = 2^{-N} \sum_{N_R=0}^{\frac{N}{2}+c\sqrt{N}} \binom{N}{N_R}$$

$$= 2^{-N} \sum_{N_R=0}^{N(\frac{1}{2}+\frac{c}{\sqrt{N}})} \binom{N}{N_R} \geq 1 - e^{-2c^2}$$

Thus,

$$\sum_{N_R \geq \frac{N}{2}+c\sqrt{N}}^{N} q(N_R) \;=\; 1 - \Big(\sum_{N_R=0}^{\frac{N}{2}+c\sqrt{N}} q(N_R)\Big) \geq 1 - (1-e^{-2c^2}) = e^{-2c^2}$$

Then,

$$\sum_{N_R=0}^{\frac{N}{2}-c\sqrt{N}} q(N_R) P_1\big(2(1-\alpha)N;\alpha,N_R\big) + \sum_{N_R \geq \frac{N}{2}+c\sqrt{N}}^{N} q(N_R) P_1\big(2(1-\alpha)N;\alpha,N_R\big) \leq 2e^{-2c^2}$$

So, we can rewrite $P_R(2(1-\alpha)N;\alpha)$ using the last inequality to get, as c goes to infinity:

$$P_R(2(1-\alpha)N;\alpha) \;=\; \sum_{\frac{N}{2}-c\sqrt{N}<N_R<\frac{N}{2}+c\sqrt{N}} q(N_R) P_1\big(2(1-\alpha)N;\alpha,N_R\big) + o(1)$$

Note that in the formula (4.3), for our chosen value of $m = 2(1-\alpha)N$, value $m/2$ will be between n' and m', when $\frac{N}{2} - c\sqrt{N} < N_R < \frac{N}{2} + c\sqrt{N}$, for fixed c if N is large enough.
Note also that if $\frac{m}{2} - 3c\sqrt{N} < n < \frac{m}{2} + 3c\sqrt{N}$, we can substitute $\sqrt{N}$ with $\sqrt{\frac{m}{2(1-\alpha)}}$ to obtain $\frac{m}{2} - q\sqrt{m} < n < \frac{m}{2} + q\sqrt{m}$, where $q = 3c/\sqrt{2(1-\alpha)}$, and the whole interval will be between n' and m' for fixed c if N is large enough, so

$$P_1(m;\alpha,N_R) = \sum_{\frac{m}{2}-q\sqrt{m}<n<\frac{m}{2}+q\sqrt{m}} P_2(n;m,N_R) P_3(n;\alpha,N_R) \tag{4.11}$$

$$+ \sum_{n=n'}^{\frac{m}{2}-q\sqrt{m}} P_2(n;m,N_R) P_3(n;\alpha,N_R) \tag{4.12}$$

$$+ \sum_{n \geq \frac{m}{2}+q\sqrt{m}}^{m'} P_2(n;m,N_R) P_3(n;\alpha,N_R) \tag{4.13}$$

We will again prove that the last two sums are $o(1)$. Recall that

$$P_2(n;m,N_R) = \binom{m}{n}\binom{N-m}{N_R-n}\binom{N}{N_R}^{-1} \tag{4.14}$$

Hence, $\sum_{n=0}^{m} P_2(n;m,N_R) = 1$, as a probability distribution, corresponding to probabilities that among the N_R uniformly chosen different natural numbers from 1 to N there are exactly n no larger than m. Also P_3 is between 0 and 1, so we will estimate tails of the distribution P_2.
We will use the following version of normal approximation to the binomial distribution, see [46]:

$$\binom{k}{k/2-l}\frac{1}{2^{k+1}} = \frac{e^{-2l^2/k}}{\sqrt{2\pi k}} + O(\frac{1}{k^{3/2}}).$$

Note that in the last two sums of (4.13), $|n - m/2| \geq 3c\sqrt{N}$, and moreover, since other values of N_R are part of $o(1)$ terms in (4.9), $\frac{N}{2} - c\sqrt{N} < N_R < \frac{N}{2} + c\sqrt{N}$. From this follows that

$$\begin{aligned}\binom{m}{n}\binom{N}{N_R}^{-1} &\leq \binom{m}{m/2}\binom{N}{N/2-c\sqrt{N}}^{-1} = (2^m/\sqrt{m})/\big(2^N(e^{-2c^2}/\sqrt{N})\big)\big(1+O(\frac{1}{N})\big)\\ &= 2^{m-N}(e^{2c^2}\sqrt{\frac{N}{m}})\big(1+O(\frac{1}{N})\big) = 2^{m-N}e^{2c^2}/\sqrt{2(1-\alpha)}\big(1+O(\frac{1}{N})\big)\end{aligned}$$

Using this, we get

$$\begin{aligned}\sum_{\frac{m}{2}+q\sqrt{m}}^{m'} P_2(n;m,N_R)P_3(n;\alpha,N_R) &\leq \sum_{\frac{m}{2}+q\sqrt{m}}^{m'} P_2(n;m,N_R)\\ &\leq e^{2c^2}/\sqrt{2(1-\alpha)}(1+O(\frac{1}{N}))\cdot 2^{-(N-m)}\sum_{\frac{m}{2}+3c\sqrt{N}}^{m'}\binom{N-m}{N_R-n}\\ &\leq e^{2c^2}/\sqrt{2(1-\alpha)}\big(1+O(\frac{1}{N})\big)\cdot 2^{-(N-m)}\sum_{k=0}^{\frac{N-m}{2}-2c\sqrt{N}}\binom{N-m}{k}\\ \leq e^{2c^2}/\sqrt{2(1-\alpha)}\big(1+O(\frac{1}{N})\big)\cdot e^{-8c^2\frac{N}{N-m}} &\leq e^{-6c^2}/\sqrt{2(1-\alpha)}\big(1+O(\frac{1}{N})\big) = o(1)\end{aligned}$$

as c goes to infinity, where we applied the Hoeffding's inequality to get the last line.

Similarly, we get

$$\sum_{n=n'}^{\frac{m}{2}-q\sqrt{m}} P_2(n;m,N_R)P_3(n;\alpha,N_R) \leq \sum_{n=n'}^{\frac{m}{2}-q\sqrt{m}} P_2(n;m,N_R)$$

$$\leq e^{2c^2}/\sqrt{2(1-\alpha)}\big(1+O(\frac{1}{N})\big)\cdot 2^{-(N-m)} \sum_{n=n'}^{\frac{m}{2}-3c\sqrt{N}} \binom{N-m}{N_R-n}$$

$$\leq e^{2c^2}/\sqrt{2(1-\alpha)}\big(1+O(\frac{1}{N})\big)\cdot 2^{-(N-m)} \sum_{k\geq \frac{N-m}{2}+2c\sqrt{N}}^{N-m} \binom{N-m}{k}$$

$$\leq e^{2c^2}/\sqrt{2(1-\alpha)}\big(1+O(\frac{1}{N})\big)\cdot e^{-8c^2\frac{N}{N-m}} \leq e^{-6c^2}/\sqrt{2(1-\alpha)}\big(1+O(\frac{1}{N})\big) = o(1).$$

Moreover, from these calculations we see that

$$\sum_{\frac{m}{2}-q\sqrt{m}<n<\frac{m}{2}+q\sqrt{m}} P_2(n;m,N_R) = 1+o(1).$$

Note that $\binom{m}{n} = \binom{m}{m-n}$, $\binom{N-m}{N_R-n} = \binom{N-m}{(N-N_R)-(m-n)}$ and $\binom{N}{N_R}^{-1} = \binom{N}{N-N_R}^{-1}$ from symmetry of binomial coefficients, so

$$P_2(n;m,N_R) = P_2((m-n);m,N-N_R).$$

Similarly, $q(N_R) = q(N-N_R)$.
We want to show that $P_3(n;\alpha,N_R)+P_3((m-n);\alpha,N-N_R) = 1+o(1)$, for fixed c but as N goes to infinity, under restrictions on N_R and n, namely, $\frac{N}{2}-c\sqrt{N} < N_R < \frac{N}{2}+c\sqrt{N}$ and $\frac{m}{2}-q\sqrt{m} < n < \frac{m}{2}+q\sqrt{m}$, as we only consider first sums in (4.9) and (4.13). Such pairing will then help us prove that limit of P_R is indeed $1/2$.
We will again use normal approximation to binomial distribution, i.e. as N goes to infinity (c, on which restrictions depend, is fixed), we have:

$$P_3(n;m,N_R) = 2^{-n}\sum_{i=0}^{T_1}\binom{n}{i} = \frac{1}{2}\big(1+\mathrm{erf}(y_1)\big)+o(1),$$

$$P_3((m-n);m,(N-N_R)) = 2^{-(m-n)}\sum_{i=0}^{T_2}\binom{m-n}{i} = \frac{1}{2}\big(1+\mathrm{erf}(y_2)\big)+o(1)$$

where, under our restrictions on N_R and n, $T_1 = (1-\alpha)N_R$, $T_2 = (1-\alpha)(N-N_R)$, with the corresponding values $y_1 = \dfrac{\frac{T_1}{n}-\frac{1}{2}}{\frac{1}{2\sqrt{n}}\sqrt{2}}$ and $y_2 = \dfrac{\frac{T_2}{m-n}-\frac{1}{2}}{\frac{1}{2\sqrt{m-n}}\sqrt{2}}$.
Thus, to prove $P_3(n;\alpha,N_R)+P_3(n;\alpha,N-N_R) = 1+o(1)$ it is enough to show $y_1+y_2 = o(1)$ as N goes to infinity, as the function erf is odd and smooth with bounded derivative in $\mathbb{R}$.

$$y_1 + y_2 = \Big(\frac{\frac{T_1}{n} - \frac{1}{2}}{\frac{1}{2\sqrt{n}}\sqrt{2}}\Big) + \Big(\frac{\frac{T_2}{m-n} - \frac{1}{2}}{\frac{1}{2\sqrt{m-n}}\sqrt{2}}\Big)$$
$$= (\frac{T_1}{n} - \frac{1}{2})\sqrt{2}\sqrt{n} + (\frac{T_2}{m-n} - \frac{1}{2})\sqrt{2}\sqrt{m-n}$$

Set $n = \frac{m}{2} + k, \quad -q\sqrt{m} < k < q\sqrt{m}$ and $N_R = \frac{N}{2} + A, \quad -c\sqrt{N} < A < c\sqrt{N}$. After some algebraic manipulations, we get

$$\begin{aligned}
y_1 + y_2 &= \sqrt{2}\Big(\frac{(1-\alpha)(\frac{N}{2} + A) - \frac{1}{2}\big((1-\alpha)N + k\big)}{\sqrt{(1-\alpha)N + k}} \\
&\quad + \frac{(1-\alpha)(\frac{N}{2} - A) - \frac{1}{2}((1-\alpha)N - k)}{\sqrt{(1-\alpha)N - k}}\Big) \\
&= \sqrt{2}\Big(\frac{(1-\alpha)A - k}{\sqrt{(1-\alpha)N + k}} + \frac{-(1-\alpha)A + k}{\sqrt{(1-\alpha)N - k}}\Big) \\
&= \sqrt{2}\big((1-\alpha)A - k\big)\Big(\frac{1}{\sqrt{(1-\alpha)N + k}} - \frac{1}{\sqrt{(1-\alpha)N - k}}\Big) \\
&= \sqrt{2}\big((1-\alpha)A - k\big)\Big(\frac{\sqrt{(1-\alpha)N - k} - \sqrt{(1-\alpha)N + k}}{\sqrt{(1-\alpha)^2N^2 - k^2}}\Big) \\
&= \sqrt{2}\big((1-\alpha)A - k\big)\Big(\frac{\sqrt{(1-\alpha)N}\Big(\sqrt{1 - \frac{k}{(1-\alpha)N}} - \sqrt{1 + \frac{k}{(1-\alpha)N}}\Big)}{\sqrt{(1-\alpha)^2N^2 - k^2}}\Big)
\end{aligned}$$

Using Taylor series expansion for $\sqrt{1 - \frac{k}{(1-\alpha)N}}$ and $\sqrt{1 + \frac{k}{(1-\alpha)N}}$ we get

$$\begin{aligned}
y_1 + y_2 &= \sqrt{2}\sqrt{(1-\alpha)N}((1-\alpha)A - k)\times \\
&\qquad \Big(\frac{\big(1 - \frac{1}{2}\frac{k}{(1-\alpha)N} + O(\frac{k^2}{N^2})\big) - \big(1 + \frac{1}{2}\frac{k}{(1-\alpha)N} + O(\frac{k^2}{N^2})\big)}{\sqrt{(1-\alpha)^2N^2 - k^2}}\Big) \\
&= \sqrt{2}\sqrt{(1-\alpha)N}((1-\alpha)A - k)\Big(\frac{\frac{-k}{(1-\alpha)N}(1 + o(1))}{\sqrt{(1-\alpha)^2N^2 - k^2}}\Big).
\end{aligned}$$

Using that both A and k are $O(\sqrt{N})$, we finally get $y_1 + y_2 = O(1/\sqrt{N}) = o(1)$. So in this case we have $P_3(n; \alpha, N_R) + P_3((m-n); \alpha, N - N_R) = 1 + o(1)$, and for fixed c, convergence is uniform on the interval of restriction for N_R and n, as N goes to infinity.

Using our pairing, and considering the first, main sum of (4.9), and of (4.13), we see that indeed P_R is $1/2 + o(1)$ as both c and N tend to infinity.

□

4.3 Asymptotic behaviour

For large N, $q(N_R)$ will be approximated by the Gaussian distribution with mean $N/2$ and standard deviation proportional to $\sqrt{N}$. Thus, to value of probability $P_R(m;\alpha)$, only $P_R(m,\alpha;N_R)$ with N_R around $N/2$ will contribute, and with fixed weight on intervals of the form $(N/2 - c\sqrt{N}, N/2 + c\sqrt{N})$. Similar logic shows that if n not close to $m/2$, the probabilities will vanish. Also, if T is less than $n/2$ function P_3 will be close to 0, and if it is larger than $n/2$, it becomes close to 1. This gives that for a fixed α, function $P_R(m,\alpha)$ is close to 0, when m is greater than $2(1-\alpha)N$ and close to one when m is less than that, i.e. $2(1-\alpha)N$ is a treshold value for m with width of transition proportional, roughly speaking, to $\sqrt{N}$. In the previous chapter, when α is fixed, we have seen that taking value m to be $2(1-\alpha)N$, or close to it, will give a value of $P_R(m;\alpha)$ close to $1/2$. Away from $2(1-\alpha)N$, P_R becomes close to either 0 or 1, and $P_{ch} = P_R(1-P_R)$ is close to zero. In fact, have the following useful estimate (see [6]):

Theorem 7. *There is a constant C such that if $|m - 2(1-\alpha)N| > x\sqrt{N}$, then $P_{ch}(m,\alpha;N) < Ce^{-x^2/128}$, where $\alpha \in (1/2,1)$, $0 \le m \le N$.*

Proof. Note that when $|N_R - N/2| > x\sqrt{N}/16$, we have that by Hoeffding's inequality,

$$\sum_{N_R, |N_R - N/2| > x\sqrt{N}/16} 2^{-N} \binom{N}{N_R} < 2e^{-x^2/128} \tag{4.15}$$

and in particular, contribution of such N_R to $P_R(m,\alpha)$ in (4.2) is less than $2e^{-x^2/128}$.

Now, assume

$$N/2 - x\sqrt{N}/16 < N_R < N/2 + x\sqrt{N}/16. \tag{4.16}$$

Let us estimate in this case the sum $\sum_{n,|n-m/2|\ge x\sqrt{N}/4} P_2(n;m,N_R)$.
Recall that

$$P_2(n;m,N_R) = \binom{m}{n}\binom{N-m}{N_R-n}\binom{N}{N_R}^{-1}.$$

Using (4.16) it follows that when $|n - m/2| \ge x\sqrt{N}/4$, we have

$$\begin{aligned} |(N/2 - m/2) - (N_R - n)| &= |(N/2 - N_R) - (m/2 - n)| \\ &\ge |(m/2 - n)| - |(N_R - N/2)| \ge (1/4 - 1/16)x\sqrt{N}. \end{aligned}$$

$$|(N/2 - m/2) - (N_R - n)| \ge 3x\sqrt{N}/16 \tag{4.17}$$

Using normal approximation to binomial distribution,

$$\binom{k}{k/2-l}\frac{1}{2^{k+1}} = \frac{e^{-2l^2/k}}{\sqrt{2\pi k}} + O(\frac{1}{k^{3/2}})$$

we get

$$\begin{aligned}\binom{N-m}{N_R-n}\binom{N}{N_R}^{-1} &\leq \binom{N-m}{(N-m)/2}\binom{N}{N/2-x\sqrt{N}/16}^{-1}\\ &= (2^{N-m}/\sqrt{N-N_R})/\big(2^N(e^{-x^2/128}/\sqrt{N})\big)\big(1+O(\frac{1}{N})\big)\\ &= 2^{-m}(e^{x^2/128}\sqrt{\frac{N}{N-m}})\big(1+O(\frac{1}{N})\big)\end{aligned}$$

and

$$\begin{aligned}\binom{m}{n}\binom{N}{N_R}^{-1} &\leq \binom{m}{m/2}\binom{N}{N/2-x\sqrt{N}/16}^{-1}\\ &= (2^m/\sqrt{m})/\big(2^N(e^{-x^2/128}/\sqrt{N})\big)\big(1+O(\frac{1}{N})\big)\\ &= 2^{m-N}(e^{x^2/128}\sqrt{\frac{N}{m}})\big(1+O(\frac{1}{N})\big).\end{aligned}$$

Note that, by Hoeffding's inequality, and using $m \leq N$,

$$\sum_{n,|n-m/2|\geq x\sqrt{N}/4}\binom{m}{n} \leq \sum_{n,|n-m/2|\geq x\sqrt{m}/4}\binom{m}{n} \leq 2e^{-x^2/8}2^m$$

and, using (4.17)

$$\begin{aligned}\sum_{n,|n-m/2|\geq x\sqrt{N}/4}\binom{N-m}{N_R-n} &\leq \sum_{n,|(N/2-m/2)-(N_R-n)|\geq 3x\sqrt{N}/16}\binom{N-m}{N_R-n}\\ &\leq \sum_{n,|(N/2-m/2)-(N_R-n)|\geq 3x\sqrt{N-m}/16}\binom{N-m}{N_R-n} \leq 2e^{-9x^2/128}2^{N-m}.\end{aligned}$$

Now, either $m \leq N/2$, when $N/(N-m) \leq 2$, in which case we use the first of each pair of the inequalities above, to get

$$\sum_{n,|n-m/2|\geq x\sqrt{N}/4} P_2(n;m,N_R) \leq 2\sqrt{2}e^{-15x^2/128}(1+O(1/N)) < 2\sqrt{2}e^{-x^2/128}(1+O(1/N)),$$

or when $m > N/2$, so $N/m \leq 2$, when we get from the second inequalities

$$\sum_{n,|n-m/2|\geq x\sqrt{N}/4} P_2(n;m,N_R) \leq 2\sqrt{2}e^{-8x^2/128}(1+O(1/N)) < 2\sqrt{2}e^{-x^2/128}(1+O(1/N)).$$

So, when (4.16) holds, we have

$$\sum_{n,|n-m/2|\geq x\sqrt{N}/4} P_2(n;m,N_R) = O(e^{-x^2/128}). \tag{4.18}$$

Now assume that that $m - 2(1-\alpha)N > x\sqrt{N}$, or

$$m > 2(1-\alpha)N + x\sqrt{N}.$$

Suppose that (4.16) holds and that

$$m/2 - x\sqrt{N}/4 < n < m/2 + x\sqrt{N}/4 \tag{4.19}$$

and also $n, m \leq N$. We have then

$$(1-\alpha)N + x\sqrt{N}/4 < n \tag{4.20}$$

and from (4.16) it follows $n > N_R(1-\alpha)$. So we have that, in formula (4.5), $T = N_R(1-\alpha)$. However, we have then that

$$T < (1-\alpha)N/2 + x\sqrt{N}(1-\alpha)/16 < n/2 - x\sqrt{N}/16 \leq n/2 - x\sqrt{n}/16. \tag{4.21}$$

So, by Hoeffding's inequality, we have that, in this case $P_3(n, \alpha; N_R) < e^{-x^2/128}$.

Now we can estimate $P_R(m, \alpha)$. The contribution to the sum when $|N_R - N/2| > x\sqrt{N}/16$, is bounded by $2e^{-x^2/128}$ by (4.15). When (4.16) holds, using that $q(N_R)$ is probability distribution, we can estimate P_1. Again, we have two cases. In the first case, when $|n - m/2| \geq x\sqrt{N}/4$, we see that contribution of such n to P_1 is $O(e^{-x^2/128})$ by (4.18). Finally, using that P_2 is a probability distribution in n (probability that out of N_R chosen elements out of N, specified n chosen elements will be among the first m), when (4.19) holds, it is enough to bound P_3. But we have demonstrated that in that case $P_3(n, \alpha; N_R) < e^{-x^2/128}$. Thus,

$$P_R(m, \alpha) < 2e^{-x^2/128} + O(e^{-x^2/128}) + e^{-x^2/128} = O(e^{-x^2/128}),$$

and consequently,

$$P_{ch}(m; \alpha, N) < O(e^{-x^2/128}).$$

The case $m < 2(1-\alpha)N - x\sqrt{N}$ is analogous.
Namely, from

$$N/2 - x\sqrt{N}/16 < N_R < N/2 + x\sqrt{N}/16$$

and

$$m/2 - x\sqrt{N}/4 < n < m/2 + x\sqrt{N}/4$$

follows

$$n < (1-\alpha)N - x\sqrt{N}/4.$$

When in (4.5), $T = n$, $P_3 = 1$, otherwise $T = N_R(1-\alpha)$ and

$$T > (1-\alpha)N/2 - x\sqrt{N}(1-\alpha)/16 > n/2 + x\sqrt{N}/16 \geq n/2 + x\sqrt{n}/16, \tag{4.22}$$

So, by Hoeffding's inequality, we have that $P_3(n, \alpha; N_R) > 1 - e^{-x^2/128}$.

Now we can estimate $P_R(m,\alpha)$. Recall that P_R, P_1, P_2 and P_3 take values between 0 and 1, and that P_2 is probability distribution in n and $q(N_R) = 2^{-N}\binom{N}{N_R}$ is probability distribution in N_R. Note that from (4.15) follows

$$\sum_{N_R,|N_R-N/2|\leq x\sqrt{N}/16} 2^{-N}\binom{N}{N_R} \geq 1 - 2e^{-x^2/128},$$

and that from (4.18) follows that, when $|N_R - N/2| \leq x\sqrt{N}/16$,

$$\sum_{n,|n-m/2|\leq x\sqrt{N}/4} P_2(n;m,N_R) = 1 - O(e^{-x^2/128}).$$

Now summing just contributions from N_R with $|N_R - N/2| \leq x\sqrt{N}/16$ to P_R, and from n with $|n - m/2| \leq x\sqrt{N}/4$ to P_1, and using $P_3(n,\alpha;N_R) > 1 - e^{-x^2/128}$, we get

$$P_R(m,\alpha) \geq (1 - 2e^{-x^2/128})(1 - O(e^{-x^2/128}))(1 - e^{-x^2/128}),$$
$$P_R(m,\alpha) > 1 - 2e^{-x^2/128} - O(e^{-x^2/128}) - e^{-x^2/128},$$
$$P_R(m,\alpha) = 1 - O(e^{-x^2/128}),$$

and consequently, in the case $m < 2(1-\alpha)N - x\sqrt{N}$, we also get

$$P_{ch}(m;\alpha,N) < O(e^{-x^2/128}).$$

□

From Theorem 7 we get

Theorem 8. *If the probability density $p(\alpha) < B$, then there is a constant A such that $P_{ch}(m;N) \leq A/\sqrt{N}$, where $P_{ch}(m;N) = \int_{1/2}^{1} p(\alpha)P_{ch}(m,\alpha;N)d\alpha$.*

Proof. Note that $\alpha = 1 - m/2N + c/\sqrt{N}$ is relationship between c and α, then $d\alpha = dc/\sqrt{N}$ and hence assuming $p(\alpha) < B$, we get

$$P_{ch}(m;N) = \int_{1/2}^{1} p(\alpha)P_{ch}(m,\alpha;N)d\alpha \leq \int_{1-m/2N-1/\sqrt{N}}^{1-m/2N+1/\sqrt{N}} BP_{ch}(m,\alpha;N)d\alpha$$
$$+ \int_{1}^{\infty} 2BCe^{-c^2/128}dc/\sqrt{N} \leq 2BC/\sqrt{N} + 2BC/\sqrt{N}\int_{0}^{\infty} e^{-c^2/128}dc$$
$$\leq 2BC/\sqrt{N}(1 + \sqrt{32\pi}).$$

□

A consequence of this result is the following theorem.

Theorem 9. *Functions $f_N : [0,1] \to \mathbb{R}$,*

$$f_N(x) = P_{ch}([xN],N)\sqrt{N},$$

where $P_{ch}(m,N) = \int p(\alpha)P_{ch}(m;\alpha,N)d\alpha$ is described in the previous chapter (N is number of qubits, not explicitly used as parameter in notation from [39]), and $[xN]$ is closest integer to xN, are uniformly bounded .

A more precise computation shows that, in fact, sequence $\{f_N\}$ converges to a bounded limit function $f : [0, 1] \to \mathbb{R}$. Note that in the above argument, key point was that $p(\alpha)$ was indeed a bounded function.
Note that, as a consequence of this result, we get that maximum over all m of $P_{ch}(m)$ goes to zero as $\frac{1}{\sqrt{N}}$, as was noticed in numerical simulations in [39] and conjectured in that paper.

Finally, note that for Paunković-Bouda-Mateus protocol, we have only considered cheating strategies that measured either accept or reject basis, and did not allow for some other observables. However, the same result holds if we use any entangled basis instead, which was noted in the Paunković-Bouda-Mateus paper, using security of BB84 protocol.

Bibliography

[1] D. Z. Albert and D. Z. Albert, *Quantum mechanics and experience*, Harvard University Press, 2009.

[2] I. D. V. Bagad, *Data Communication*, Technical Publications, 2007.

[3] S. Banerjee and A. Roy, *Linear algebra and matrix analysis for statistics*, CRC Press, 2014.

[4] H. J. Bierens, *Introduction to the mathematical and statistical foundations of econometrics*, Cambridge University Press, 2004.

[5] ——, *Hilbert space theory and its applications to semi-nonparametric modeling and inference*, 2012.

[6] V. Božin and H. Louka, *Asymptotics of quantum contract signing*, Publications de l'Institut Mathmatique, (to appear).

[7] I. N. Bronštejn and K. A. Semendjaev, *Handbook of mathematics*, Springer, 2013.

[8] M. J. Campagna and A. Sethi, *Key recovery method for crt implementation of rsa.*, IACR Cryptology ePrint Archive, 2004 (2004), p. 147.

[9] D. Carper and J. McKinsey, *Understanding the law*, Cengage Learning, 2011.

[10] L. N. Childs, *The chinese remainder theorem*, in A Concrete Introduction to Higher Algebra, Springer, 1995, pp. 194–207.

[11] F. Cross and R. Miller, *The Legal Environment of Business: Text and Cases–Ethical, Regulatory, Global, and E-Commerce Issues*, Cengage Learning, 2008.

[12] I. Djordjevic, *Quantum information processing and quantum error correction: an engineering approach*, Academic press, 2012.

[13] I. B. Djordjevic, *On the photonic implementation of universal quantum gates, bell states preparation circuit, quantum relay and quantum ldpc encoders and decoders*, Photonics Journal, IEEE, 2 (2010), pp. 81–91.

[14] M. Evans, *RSA encryption*, The University of Melbourne on behalf of the Australian Mathematical Sciences Institute (AMSI), 2013.

[15] F. W. Galaty, W. J. Allaway, and R. C. Kyle, *Modern Real Estate Practice in Ohio*, Dearborn Real Estate, 2001.

[16] J. W. Haag, G. R. Peterson, and M. L. Spezio, *The Routledge companion to religion and science*, Routledge, 2012.

[17] A. Harrow and A. Montanaro, *An efficient test for product states*, arXiv preprint arXiv:1001.0017, (2010).

[18] D. A. Harville, *Matrix algebra from a statistician's perspective*, vol. 1, Springer, 1997.

[19] J. A. Helewitz, *Basic contract law for paralegals*, Aspen Publishers Online, 2010.

[20] W. Hoeffding, *Probability inequalities for sums of bounded random variables*, Journal of the American statistical association, 58 (1963), pp. 13–30.

[21] L. Kauffman and S. J. Lomonaco, *Mathematics of quantum computation and quantum technology*, CRC Press, 2007.

[22] C. K. Koc, *High-speed rsa implementation*, tech. report, Technical Report, RSA Laboratories, 1994.

[23] A. Kumar, *PHY 301: Mathematical Methods I 2x2 Complex (Real) Matrices.*

[24] P. Langacker, *The standard model and beyond*, CRC press, 2009.

[25] I. Lankham, B. Nachtergaele, and A. Schilling, *Inner product spaces*, (2007).

[26] C. Lavor, L. Manssur, and R. Portugal, *Grover's algorithm: quantum database search*, arXiv preprint quant-ph/0301079, (2003).

[27] J. Long, *Office procedures for the legal professional*, Cengage Learning, 2004.

[28] H. Louka, *Necessity of parameter randomization in quantum contract signing*, Matematički Vesnik, (to appear).

[29] D. Lugiez, *CONCUR 2003-Concurrency Theory: 14th International Conference, Marseille, France, September 3-5, 2003, Proceedings*, vol. 2761, Springer Science & Business Media, 2003.

[30] E. Manousakis, *Practical Quantum Mechanics: Modern Tools and Applications*, Oxford University Press, 2015.

[31] D. C. Marinescu, *Classical and quantum information*, Academic Press, 2011.

[32] D. McMahon, *Quantum computing explained*, John Wiley & Sons, 2007.

[33] A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook of applied cryptography*, CRC press, 1996.

[34] F. Mintert, C. Viviescas, and A. Buchleitner, *Basic concepts of entangled states*, in Entanglement and Decoherence, Springer, 2009, pp. 61–86.

[35] N. Nedjah, L. dos Santos Coelho, and L. de Macedo Mourelle, *Quantum inspired intelligent systems*, vol. 121, Springer Science & Business Media, 2008.

[36] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, Cambridge university press, 2010.

[37] A. Nitaj, *The mathematical cryptography of the rsa cryptosystem*.

[38] A. Pathak, *Elements of quantum computation and quantum communication*, Taylor & Francis, 2013.

[39] N. Paunković, J. Bouda, and P. Mateus, *Fair and optimistic quantum contract signing*, Physical Review A, 84 (2011).

[40] T. Placek and J. Butterfield, *Non-locality and Modality*, vol. 64, Springer Science & Business Media, 2012.

[41] M. Y. Rhee, *Internet security: cryptographic principles, algorithms and protocols*, John Wiley & Sons, 2003.

[42] J. Rothe, *Some facets of complexity theory and cryptography: A five-lecture tutorial*, ACM Computing Surveys (CSUR), 34 (2002), pp. 504–549.

[43] S. Roy, S. Nag, I. K. Maitra, and S. K. Bandyopadhyay, *International journal of advanced research in computer science and software engineering*, International Journal, 3 (2013).

[44] G. S. Rule and T. K. Hitchens, *Fundamentals of protein NMR spectroscopy*, vol. 5, Springer Science & Business Media, 2006.

[45] J. Schiller, *Quantum Computers*, CreateSpace, 2009.

[46] R. Sedgewick and P. Flajolet, *An introduction to the analysis of algorithms*, Addison-Wesley, 2013.

[47] P. W. Shor and J. Preskill, *Simple proof of security of the bb84 quantum key distribution protocol*, arXiv preprint quant-ph/0003004.

[48] J. Stolze and D. Suter, *Quantum computing: a short course from theory to experiment*, John Wiley & Sons, 2008.

[49] E. Strubell, *An introduction to quantum algorithms*, COS498 Chawathe Spring, (2011).

[50] G. Werth, V. N. Gheorghe, and F. G. Major, *Charged Particle Traps II: Applications*, vol. 54, Springer Science & Business Media, 2009.

[51] C. P. Williams and S. H. Clearwater, *Explorations in quantum computing*, 1998.

[52] N. Zettili, *Quantum mechanics: concepts and applications*, John Wiley & Sons, 2009.

Prilog 1.

Izjava o autorstvu

Potpisana Hana Almoner Louka
broj indeksa 2020/2010

Izjavljujem

da je doktorska disertacija pod naslovom

"Quantum Information Theory and Asymptotics of Quantum Contract Signing"

- rezultat sopstvenog istraživačkog rada,
- da predložena disertacija u celini ni u delovima nije bila predložena za dobijanje bilo koje diplome prema studijskim programima drugih visokoškolskih ustanova,
- da su rezultati korektno navedeni i
- da nisam kršio autorska prava i koristio intelektualnu svojinu drugih lica.

Potpis doktoranda

U Beogradu, _____

_____

Prilog 2.

Izjava o istovetnosti štampane i elektronske verzije doktorskog rada

Ime i prezime autora: *Hana Almoner Louka*
Broj indeksa: 2020/2010
Studijski program: _____
Naslov rada: *"Quantum Information Theory and Asymptotics of Quantum Contract Signing"*
Mentor: *docent dr. Vladimir Božin*

Potpisana *Hana Almoner Louka*

Izjavljujem da je štampana verzija mog doktorskog rada istovetna elektronskoj verziji koju sam predao za objavljivanje na portalu **Digitalnog repozitorijuma Univerziteta u Beogradu**.

Dozvoljavam da se objave moji lični podaci vezani za dobijanje akademskog zvanja doktora nauka, kao što su ime i prezime, godina i mesto rodjenja i datum odbrane rada.

Ovi lični podaci mogu se objaviti na mrežnim stranicama digitalne biblioteke, u elektronskom katalogu i u publikacijama Univerziteta u Beogradu.

Potpis doktoranda

U Beogradu, _____

_____

Prilog 3.

Izjava o korišćenju

Ovlašćujem Univerzitetsku biblioteku "Svetozar Marković" da u Digitalni repozitorijum Univerziteta u Beogradu unese moju doktorsku disertaciju pod naslovom:

"Quantum Information Theory and Asymptotics of Quantum Contract Signing"

koja je moje autorsko delo.

Disertaciju sa svim prilozima predao sam u elektronskom formatu pogodnom za trajno arhiviranje.

Moju doktorsku disertaciju pohranjenu u Digitalni repozitorijum Univerziteta u Beogradu mogu da koriste svi koji poštuju odredbe sadržane u odabranom tipu licence Kreativne zajednice (Creative Commons) za koju sam se odlučio.

1. Autorstvo
2. Autorstvo - nekomercijalno
3. Autorstvo - nekomercijalno - bez prerade
4. Autorstvo - nekomercijalno - deliti pod istim uslovima
5. Autorstvo - bez prerade
6. Autorstvo - deliti pod istim uslovima

(Molimo da zaokružite samo jednu od šest ponudjenih licenci, kratak opis licenci dat je na poledjini lista).

Potpis doktoranda

U Beogradu, _____

_____

1. Autorstvo - Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način odredjen od strane autora ili davaoca licence, čak i u komercijalne svrhe. Ovo je najslobodnija od svih licenci.

2. Autorstvo - nekomercijalno. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način odredjen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela.

3. Autorstvo - nekomercijalno - bez prerade. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način odredjen od strane autora ili davaoca licence. Ova licenca ne dozvoljava komercijalnu upotrebu dela. U odnosu na sve ostale licence, ovom licencom se ograničava najveći obim prava korišćenja dela.

4. Autorstvo - nekomercijalno - deliti pod istim uslovima. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način odredjen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca ne dozvoljava komercijalnu upotrebu dela i prerada.

5. Autorstvo - bez prerade. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, bez promena, preoblikovanja ili upotrebe dela u svom delu, ako se navede ime autora na način odredjen od strane autora ili davaoca licence. Ova licenca dozvoljava komercijalnu upotrebu dela.

6. Autorstvo - deliti pod istim uslovima. Dozvoljavate umnožavanje, distribuciju i javno saopštavanje dela, i prerade, ako se navede ime autora na način odredjen od strane autora ili davaoca licence i ako se prerada distribuira pod istom ili sličnom licencom. Ova licenca dozvoljava komercijalnu upotrebu dela i prerada. Slična je softverskim licencama, odnosno licencama otvorenog koda.