56

ENGINYERIES
DE LA
TELECOMUNICACIÓ

UNIVERSITAT POLITÈCNICA
DE CATALUNYA
BARCELONATECH

UPCGRAU

Quantum Computing
Problems and Exercises

Santiago Torres Gil
Pere Bruna Escuer
Pietro Massignan

56
ENGINYERIES
DE LA
TELECOMUNICACIÓ

UPCGRAU

Quantum Computing
Problems and Exercises

Santiago Torres Gil
Pere Bruna Escuer
Pietro Massignan

Primera edición: julio de 2020

© Iniciativa Digital Politècnica, 2020
Oficina de Publicacions Acadèmiques Digitals de la UPC
Jordi Girona 31,
Edifici Torre Girona, Plant 1, 08034 Barcelona
Tel.: 934 015 885
www.upc.edu/idp
E-mail: info.idp@upc.edu

DL: B13774-2020
ISBN:978-84-9880-843-8

Contents

Preface

Quantum technology is one of the most promising and challenging fields in contemporary science. Quantum computing, quantum cryptography, and more generally quantum information technologies claim that they, in the short term, will change our paradigm of classical computing and communications. In this regard, several news items filled headlines in the media while preparing this book: the first universal quantum computer was made available in the cloud by IBM; a Chinese quantum communication satellite provided secure quantum cryptography between continents; and Google announced that its quantum computer can solve a problem that classical computers cannot. Given these few examples, it is therefore not surprising to find these topics more and more frequently included in the current syllabuses of many technological undergraduate and postgraduate programs. However, unlike in other consolidated fields, it is essential to develop a body of syllabuses that adapt to the needs and characteristics of the studies carried out within the framework of the Universitat Politècnica de Catalunya (UPC).

This book draws on the experience of the authors during nearly ten years of work in this field. The course 'Quantum Information Technologies' began in 2012 as a mandatory course in the Bachelor Degree of Telecommunications Engineering at the Castelldefels School of Telecommunications and Aerospace Engineering (EETAC). Oriented toward telecom engineering students with a generic background in physics (not including quantum physics), the course aimed to introduce the basic concepts of quantum computing, the fundamentals of some quantum computer models and the means by which quantum key distribution protocols work. A few years later, in 2014, the Bachelor's Degree in Engineering Physics offered an elective course titled 'Quantum Optical Technologies', which also introduced quantum computing as part of the syllabus. On the other hand, engineering physics students happen to have the advantage of a solid education in quantum mechanics, which allows treating some quantum computation topics in greater depth. This is the case for quantum measurement and quantum algorithms, among others.

Regardless of the students' background, this field represents a challenging subject for educators and scientists. As once stated by Richard Feynman, winner of the 1965 Nobel Prize in Physics: *If you think you understand quantum mechanics, you don't understand quantum mechanics.* Quantum mechanics is a counterintuitive theory. Concepts such as

duality, *superposition*, *entanglement*, *teleportation* and many others seem to be closer to magic or science fiction than to everyday human experience. Yet, herein lies also the unlimited power of human thought, which mathematics and physics help us to go beyond our immediate experience of the world.

This book is oriented toward undergraduate students pursuing Bachelor's Degrees in Engineering. In particular, it is used as teaching material in the courses 'Quantum Information Technologies' within the Bachelor's Degree of Telecommunications Engineering at EETAC and in 'Quantum Optical Technologies' in the Bachelor's Degree in Engineering Physics. It is also recommended in the elective course 'Quantum Computing and Cryptography', which pertains to the Bachelor's Degree in Informatics Engineering at the Barcelona School of Informatics. Throughout this book, we have strived to maintain a balance between the rigorous mathematics needed for approaching quantum physics and the most qualitative and applied descriptions of phenomena. This book focuses mainly on resolving exercises, although basic compilations of theory are included at the beginning of each chapter. These summaries of theory are not intended to be exhaustive, let alone to serve as substitutes for formal theoretical explanations. They are proposed only as reminders of the basic concepts, formulas and definitions with which the student should be familiar.

The main body of the book consists of a comprehensive list of exercises with increasing degrees of dificulty (the hardest ones are marked with an asterisk). The solutions to most of them are provided at the end of the book. We can never emphasize enough how important it is for the students to try solving the diferent exercises and problems before checking the provided solutions. Additional exercises and examples are also included in each chapter. Some of these are to be solved with the aim of providing illustrative examples of how students are expected to reason and what they are expected to achieve. Each chapter introduces specific concepts with a focus on a few short true or false questions. Here, finding the right answer is as important to the student as correctly arguing and justifying the reason for it. Finally, throughout the book are included a few *boxes* with brief informative descriptions of some currently hot topics in quantum technologies. These *boxes* are intended for opening doors that will motivate students to continue delving into the field of quantum technologies, which has only just begun to be explored.

The authors.

Barcelona, 24th January 2020

→1

Fundamentals of Quantum Physics

1.1. Key Equations and Physical Constants

– A black body emits radiation, whose spectrum depends on the temperature of the body. In particular, the wavelength at which the spectrum has a maximum is described by Wien's law:

$$\lambda_{\text{peak}} = b/T,$$

where $b = 2.898 \times 10^{-3}$m K.

– Visible light is only a small portion of the whole electromagnetic spectrum, as shown in Fig. 1.1.

– A photon of frequency ν has energy $E = h\nu$, where h is Planck's constant.

– The frequency ν and wavelength λ of light are linked by the relationship $\lambda\nu = c$, where c is the speed of light.

– To a particle with momentum p, we may associate a quantum wave with wavelength λ through the de Broglie equation: $\lambda = h/p$. Quantum effects become important when λ becomes larger than the mean distance between particles.

– In an experiment on the photoelectric effect, the maximum kinetic energy of emitted photons is given by

$$E_{\text{kin,max}} = h\nu - W_0,$$

where ν is the frequency of incoming photons, $W_0 = h\nu_0$ is the work function of the material, and ν_0 is the corresponding threshold frequency.

– The Schrödinger equation for the wave function $\psi(\mathbf{r}, t)$ describing a quantum particle with mass m in an external potential $V(\mathbf{r}, t)$ reads:

$$i\hbar\frac{\partial\psi(\mathbf{r},t)}{\partial t} = \left[-\frac{\hbar^2\nabla^2}{2m} + V(\mathbf{r},t)\right]\psi(\mathbf{r},t),$$

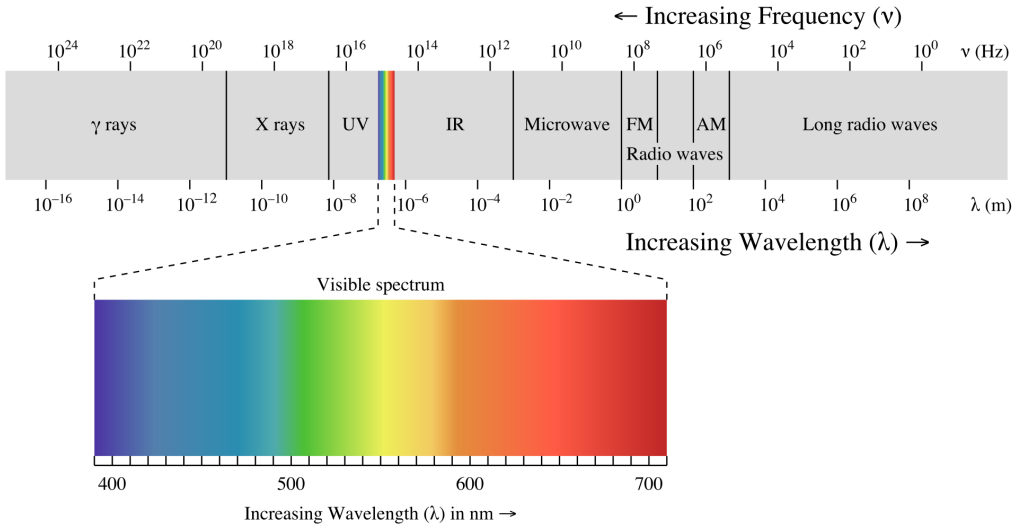


Fig. 1.1 Electromagnetic spectrum.

where $\hbar = h/(2\pi)$ is the *reduced* Planck constant.

– If the external potential is independent of time, it is easy to check that the wave function may be factorized as $\psi(\mathbf{r}, t) = e^{-iEt/\hbar}\psi(\mathbf{r})$, where $\psi(\mathbf{r})$ is the solution of the *time-independent* Schrödinger equation

$$E\psi(\mathbf{r}) = \left[-\frac{\hbar^2\nabla^2}{2m} + V(\mathbf{r})\right]\psi(\mathbf{r}),$$

where E is the energy.

– The Heisenberg uncertainty principle imposes a lower bound on errors when measuring conjugate variables in the same physical state. For example, if one tries to measure the position x and the momentum p of a given state, the product of the uncertainties in the two measures will satisfy

$$\Delta x \Delta p \geq \hbar/2.$$

– The energy levels of Bohr's model of an atom are given by $E_n = -\frac{13.6}{n^2}$ eV, with integer $n \geq 1$. The energy of an electron at the most bound level (the "ground state") is therefore $E_1 = -13.6$ eV.

– When an electron in a quantum state i jumps to a less bound state f, the extra energy is carried away by a photon with energy

$$\Delta E = h\nu = E_i - E_f.$$

Constants

Quantity	Symbol	Value	Units
Planck's constant	h	6.626×10^{-34}	J s
reduced Planck's constant	$\hbar = h/(2\pi)$	1.054×10^{-34}	J s
electron's mass	m_e	9.109×10^{-31}	Kg
electron's charge	e	1.602×10^{-19}	C
speed of light	c	2.998×10^{8}	m/s
(a useful combination)	$h \cdot c$	1.24×10^{-6}	eV m
Boltzmann constant	k_B	1.381×10^{-23}	J/K
Bohr radius	a_0	5.292×10^{-11}	m

1.2. Solved Problems

1. Briefly explain why in our *macroscopic* world we usually do not see quantum effects. Provide a numerical example.

Solution

The wavelength involved in quantum effects is too short when compared with *macroscopic* scales. As an illustrative example, consider a soccer ball: typically mass and speed are typically 0.4 kg and 80 km/h, respectively. By means of the de Broglie equation, we can derive the wavelength associated to the ball:

$$\lambda = \frac{h}{p} = \frac{6.626 \times 10^{-34}\,\text{kg}\,\text{m}^2/\text{s}}{0.4\,\text{kg} \times 80\,\text{km/h} \times \dfrac{\text{m/s}}{3.6\,\text{km/h}}} = 7.5 \times 10^{-35}\,\text{m}.$$

This is an extremely short length, even shorter than the radius of an electron, which is $r_e \approx 10^{-15}$ m. The smallness of Planck's constant h makes quantum effects hardly detectable in our macroscopic world.

2. For a study of the photoelectric effect on a metal called Niobium (Nb), whose work function is $W_0 = 4.3$ eV:

a) What is the maximum kinetic energy of the electrons emitted when Nb is illuminated by photons with wavelength $\lambda = 200$ nm?

b) What is the Nb threshold frequency?

c) What happens when blue light ($\lambda \approx 480$ nm) hits Nb?

Solution

a) For incident photons with $\lambda = 200$ nm, we have

$$E_{kin,max} = hc/\lambda - W_0 = 1.9\,eV.$$

b) The Nb threshold frequency is $W_0/h = 1.04 \cdot 10^{15}$ Hz.

c) When blue light hits Niobium, the maximum kinetic energy would be negative, and thus no photoelectrons are emitted.

3. By illuminating an unknown material with ultra-violet (UV) light of wavelength 250 nm, we find that the corresponding stopping potential is 0.94 eV. A table of material properties tells us that the work functions of tin, titanium, and tungsten are, respectively, 4.38 eV, 4.06 eV, and 4.49 eV.

a) Which material are we investigating?

b) What happens if the same material is illuminated with green light? ($\lambda = 550$ nm)

Solution

a) The energy of incident photons:

$$h\nu = \frac{hc}{\lambda} = \frac{1.24 \cdot 10^{-6}\,\text{eV} \cdot \text{m}}{250 \cdot 10^{-9}\,\text{m}} = 4.96\,\text{eV}$$

Work function:

$$h\nu_0 = E_{\text{K,max}} - h\nu = (4.96 - 0.94)\,\text{eV} = 4.02\,\text{eV}$$

Given the result of the measurement, it is very likely that we are dealing with titanium.

b) The maximum kinetic energy of photoelectrons emitted using green light,

$$E_{\text{K,max}} = \frac{hc}{\lambda} - h\nu_0 = \left(\frac{1.24 \cdot 10^{-6}}{550 \cdot 10^{-9}} - 4.02\right)\text{eV} = -1.765\,\text{eV},$$

would be negative, meaning that light at this frequency hitting titanium will not produce the photoelectric effect.

4. Consider the 1D infinite square well defined by $V(|x| < 1) = 0$ and $V(|x| > 1) = +\infty$. The wave function for a particle in the second excited state for this potential is $\psi_2(x) = \cos(3\pi x/2)$ for $|x| < 1$, and zero otherwise.

a) Draw the corresponding probability density.

b) What is the probability of finding the particle in the region $-1/3 < x < 1/3$? And in the region $1/3 < x < 1$?

Solution

a) The corresponding density is shown in Fig. 1.2.

b) The probability of finding the particle in each of the two regions is 1/3.

5. A particle of mass m and frequency ω has the following wave function:

$$\psi(x) = C\, x\, e^{-m\omega x^2/(2\hbar)},$$

where $\hbar \equiv h/(2\pi)$, and C is a constant.

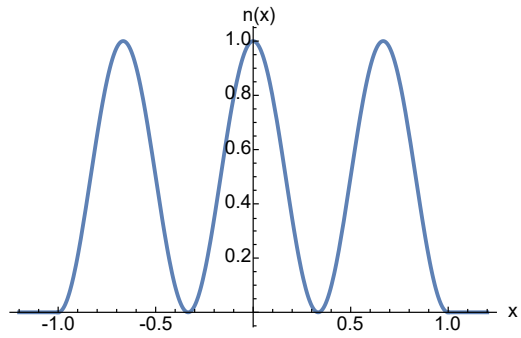


Fig. 1.2 Probability density for the second excited state of the square well of width $\Delta = 2$.

a) How should the constant C be determined?

b) What is the probability of finding the particle in $x = 0$?

c) Is it possible to find the particle in the region where $x < 0$? Justify the answer.

Solution

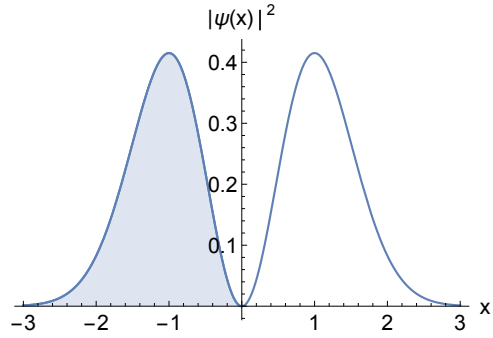


Fig. 1.3 Probability density for the wave function of the first excited state of the harmonic oscillator. The shaded area is the region $x < 0$.

a) The constant C should be determined by normalizing the wave function:

$$\int_{-\infty}^{\infty} \mathrm{d}x |\psi(x)|^2 = 1.$$

b) The probability of finding a particle in a certain region is proportional to the squared modulus of the wave function. In particular, $P(x = 0) = |\psi(x = 0)|^2 = 0$.

c) The probability of finding the particle in the negative half-plane is

$$P(-\infty < x < 0) = \int_{-\infty}^{0} \mathrm{d}x |\psi(x)|^2.$$

The integral yields a non-zero result. So it is possible to find the particle there. In particular, the integrand is symmetric around $x = 0$, and thus the probability of finding the particle in the region $x < 0$ is 1/2, as shown in Fig. 1.3.

1.3. Short Questions

Indicate if the following sentences are **TRUE** or **FALSE**, and **JUSTIFY** your answers:

1. Incident photons with wavelength λ_0 produce photoelectrons with kinetic energy E_K. If the incident photons now have half of the wavelength, $\lambda_1 = \lambda_0/2$, the kinetic energy of the electrons will double, $2E_K$.

2. The position of a particle with velocity $v = 10\,\text{m/s}$ and mass $m = 10^{-28}\,\text{kg}$ is measured with a precision of $\Delta x = 10^{-9}\,\text{m}$. The wavelength of the particle is $\lambda = 10^{-12}\,\text{m}$.

3. The work function for silver is $4.74\,\text{eV}$. The maximum wavelength of light that produces the photoelectric effect on this material is $262\,\text{nm}$.

4. The function $\Psi = Axe^{-i\omega t}$, where A and ω are constants and x is defined for $-\infty < x < \infty$, cannot be a solution of the Schrödinger equation.

5. The one-dimensional function $\Psi(x) = ax + b$ where a and b are positive constants and $x \in (-\infty, +\infty)$ is a valid wave function.

6. With the aid of an electron microscope, we want to observe details on the order of $\sim 10^{-10}\,\text{m}$. The electrons in the beam therefore must have a velocity $\sim 7.3 \cdot 10^6\,\text{m/s}$.

7. In the Bohr model of the hydrogen atom, the wavelength of a photon emitted during the jump of an electron from level $n = 3$ to $n = 1$ is shorter than the one emitted by an electron jumping from $n = 2$ to $n = 1$.

1.4. Exercises

1.4.1. General Properties

1. Charcoal burns at temperatures of around $850\ K$. Compute the wavelength of the peak in the black body spectrum using Wien's law. To which region of the electromagnetic spectrum does this wavelength belong?

2. Which of the following experiments is suitable for revealing the particle-like behavior of electromagnetic waves?

a) Young's double-slit experiment

b) Diffraction through a small hole

c) Photoelectric effect

Argue why this experiment can only be explained by light being a particle.

3. Why are quantum effects difficult to see in our everyday lives?

4. Standard lasers used in telecommunications networks have wavelengths of around $2\,\mu\text{m}$. How many photons per second are transmitted by a laser with $5.5\,\text{mW}$ of power?

1.4.2. Photoelectric Effect

5. The work function of aluminum (Al) is $4.2\,\text{eV}$. If we use light with a wavelength of $1000\,\text{Å}$ on an Al surface:

a) What is the kinetic energy of the fastest photoelectron emitted?

b) What is the stopping potential?

c) What is the threshold frequency for aluminum?

d) If the light intensity is $4.0\,\text{W/m}^2$, what is the average number of photons per unit time and unit surface that hit the surface?

6. In a photoelectric experiment with monochromatic light and a platinum photocathode, the stopping potential is found to be $6.05\,\text{V}$ for $\lambda = 1000\,\text{Å}$ and $1.92\,\text{V}$ for $\lambda = 1500\,\text{Å}$. From these data, compute:

a) A value for the Planck's constant and its relative error.

b) The work function and the threshold wavelength for platinum.

7. The stopping potential for photoelectrons emitted from a surface illuminated by light of wavelength $\lambda = 4910\,\text{Å}$ is $0.71\,\text{V}$. When we change the wavelength of the light, the new stopping potential is found to be $1.43\,\text{V}$. What is this new wavelength?

8. An Argon laser has a power of $50\,\text{mW}$ and emits photons of $810\,\text{nm}$ wavelength. The laser beam illuminates a metal whose work function is $1.02\,\text{eV}$. Determine:

a) The number of electrons emitted by the photoelectric effect in $1\,\mu\text{s}$.

b) State if the following sentence is TRUE or FALSE and JUSTIFY your answer: *If we reduce the work function to half of its value, the number of emitted electrons doubles.*

1.4.3. Wave-Particle Duality

9. We are going to conduct a double-slit experiment with two types of sources: *a)* classical bullets and *b)* classical electromagnetic waves (see Fig.1.4).

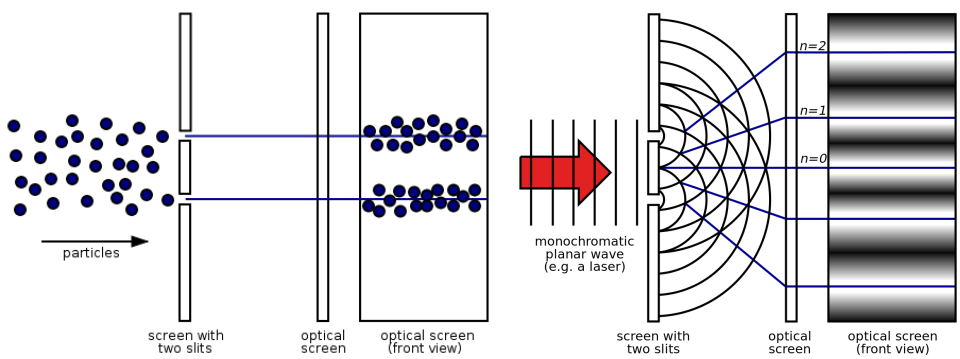


Fig. 1.4
Double-slit experiment with bullets and waves.

a) Assuming that the source (a) fires bullets at a very slow rate and that either nothing arrives at the detector or one and only one bullet arrives, what is the probability of a bullet's arrival as a function of x? Do not calculate anything, just describe the result qualitatively.

b) With source (b), what we detect is the interference of two spherical waves $E_i(\mathbf{r}, t) = A\sin(k|\mathbf{r} - \mathbf{r}_i| - \omega t)$, where $k = \frac{2\pi}{\lambda}$ is the wave number, ω is the angular frequency, and $\mathbf{r}_i$ is the center of the slit.

i. Write the wave equation of the resulting wave at the detector.

ii. Where do we obtain the maxima and minima of the interference pattern?

c) If we do the experiment with a source of electrons, what output would we expect by thinking classically? And by thinking quantum mechanically?

Hint: $\sin A + \sin B = 2\sin\left(\frac{A+B}{2}\right)\cos\left(\frac{A-B}{2}\right)$.

10. Compute the momentum and total energy of an electron and a photon with the same wavelength of $\lambda = 4.0$ Å. Compare their kinetic energies.

11. The finest detail that can be observed with a microscope is approximately equal to the wavelength of the probe used. If we want to "see" an atom with a diameter of 1 Å, we need to resolve details of about 0.1 Å.

a) If we use an electronic microscope, what is the minimum energy required for the electrons?

b) If we use a microscope with photons, what is the required energy for the photons? In which region of the electromagnetic spectrum are these photons found?

c) Which of the two microscopes is more useful for observing atoms?

1.4.4. Heisenberg's Uncertainty Principle

12. Is it important to know where the position of a particle is before making a measurement of its position?

13. In a given experiment, we measure a photon wavelength with a relative error of $\Delta\lambda/\lambda = 10^{-6}$. Which is the minimal uncertainty Δx that we may obtain for:

a) Gamma rays ($\lambda = 5.00 \times 10^{-4}$ Å)

b) X-rays ($\lambda = 5.00$ Å)

c) Visible light ($\lambda = 5000$ Å)

1.4.5. Schrödinger's Wave Equation

14. Solve the time-independent Schrödinger equation for a particle in an infinite square well potential of width L, *i.e.*:

$$V(x) = \begin{cases} 0 & \text{if } 0 \leq x \leq L, \\ \infty & \text{if } x < 0 \text{ or } x > L. \end{cases}$$

15. Consider a one-dimensional box of length 2 cm as an infinite square well potential. A particle with a mass of 2 μg is moving inside it with a velocity of 10 mm/s.

a) Calculate the approximate value of the quantum number *n* for the occupied state of the particle.

b) Determine Δx and Δp assuming that the uncertainties are: $\Delta x/L = 0.05\%$ and $\Delta p/p_x = 0.1\%$.

c) What is the value of $(\triangle x \triangle p_x/\hbar)$?

16. The wave functions for a particle of mass *m* in a one-dimensional box of length L centered in the origin are given by:

$$\psi(x) = \sqrt{\frac{2}{L}} \cos \frac{n\pi x}{L} \quad \text{when } n = 1, 3, 5, 7, ...$$

and

$$\psi(x) = \sqrt{\frac{2}{L}} \sin \frac{n\pi x}{L} \quad \text{when } n = 2, 4, 6, 8, ...$$

Calculate $\langle x \rangle$ and $\langle x^2 \rangle$ for the fundamental state ($n = 1$).

(Hint: $\int x \cos^2(ax)dx = \frac{x^2}{4} + \frac{x \sin(2ax)}{4a} + \frac{\cos(2ax)}{8a^2}$ and $\int x \sin(2ax)dx = \frac{\sin(2ax)}{4a^2} - \frac{x \cos(2ax)}{2a}$.)

17. Consider the wave function

$$\Psi(x,t) = Ce^{-\kappa|x|}e^{-i\omega t},$$

where C, κ, and ω are positive real constants.

a) Normalize Ψ.

b) Determine the expectation values of x and x^2.

c) Find the standard deviation of x. What is the probability that the particle would be found outside this range?

18. Let us consider a particle of mass m and energy $E < 0 < V_0$ exposed to the following potential:

$$V(x) = \begin{cases} 0, & \text{if } x < 0, \\ V_0, & \text{if } x > 0, \end{cases}$$

where V_0 is a positive constant. Define the wave function:

$$\psi(x) = \begin{cases} e^{+k_1 x}, & \text{if } x \leq 0 \\ e^{-k_2 x}, & \text{if } x \geq 0, \end{cases}$$

where k_1 and k_2 are constants defined as $k_1 = \dfrac{\sqrt{-2mE}}{\hbar}$ and $k_2 = \dfrac{\sqrt{2m(V_0 - E)}}{\hbar}$. Answer the following questions:

a) Does this wave function verify the time-independent Schrödinger equation? Check it in the two regions of the potential.

b) Is this wave function normalized? If not, find the normalization constant.

19. Solve the time-independent Schrödinger equation for a particle in a finite square well potential, *i.e.*:

$$V(x) = \begin{cases} -V_0, & \text{if } -a \leq x \leq a, \\ 0, & \text{for } |x| > a, \end{cases}$$

where V_0 is a positive constant.

1.4.6. Bohr's Atom and Quantum Numbers

20. Consider the Bohr model for the hydrogen atom:

a) Find the photon's energy and wavelength corresponding to the limit (shortest wavelength) of the Pfund series ($n = 5$) for hydrogen.

b) Calculate the three larger wavelengths of the Lyman series ($n = 1$).

21. The energy levels for the hydrogen atom within the Bohr model are given by the expression $E_n = -13.6\,\text{e}V/n^2$, where $n = 1, 2, 3\ldots$ is the principal quantum number. Determine:

a) The wavelength of a photon emitted when an electron jumps from $n = 4$ to $n = 2$.

b) The largest wavelength of photons emitted when the final state of the electron is characterized by $n = 2$.

22. Consider the infinite square potential and 5 particles. Evaluate the total energy of the system if the particles are: a) identical bosons, b) identical fermions, c) spin-1/2 fermions.

23. Consider a quantum system with a principal quantum number $n = 3$ and an orbital quantum number $l = 2$. Determine: a) the possible values of the magnetic quantum number m, and b) all possible quantum states.

→ 2

Quantum Computing: Gates and Circuits

2.1. Definitions

- A quantum system is described by a state vector $|\psi\rangle$. Given a collection of vectors $\{|i\rangle\}$ which form a complete and orthonormal basis of the space, every state may be written as a linear superposition $|\psi\rangle = \sum_i c_i|i\rangle$, where $\{c_i\}$ are complex coefficients.
- The probability $P(i)$ of finding the quantum system in state $|i\rangle$ is given by $P(i) = |c_i|^2$. If the state vector is correctly normalized, then $\sum_i P(i) = 1$.
- For example, a qubit can be defined as the superposition of two states $\{|0\rangle, |1\rangle\} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$, named "computational basis", as $|q\rangle = c_0|0\rangle + c_1|1\rangle$, and the normalization condition is simply $|c_0|^2 + |c_1|^2 = 1$.
- A qubit can also be represented as a point on the Bloch sphere given two angles (θ, ϕ) such as:
$$|q\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\phi}\sin\frac{\theta}{2}|1\rangle$$
- A 1-qubit quantum gate is represented by a 2×2 matrix. In turn, every such matrix may be expressed as a linear combination of 4 basis matrices: the identity $\mathbb{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, and the three Pauli matrices
$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & \text{-1} \end{pmatrix}.$$
- For example, the Hadamard matrix $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & \text{-1} \end{pmatrix} = \frac{1}{\sqrt{2}}(X + Z)$. Its eigenstates give the Hadamard basis
$$\{|+\rangle, |-\rangle\} = \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}.$$

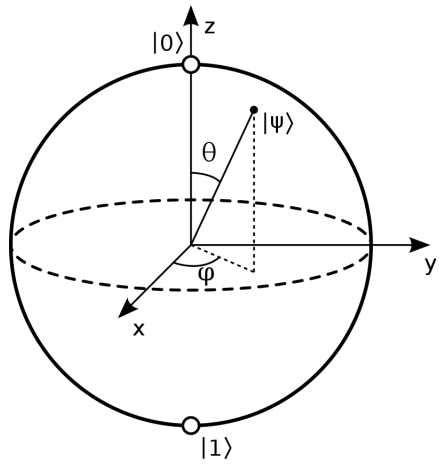


Fig. 2.1
Qubit representation within the Bloch sphere.

– The Hadamard quantum gate acts as a change basis matrix between the computational basis, $\{|0\rangle, |1\rangle\}$, and the Hadamard basis, $\{|+\rangle, |-\rangle\}$:

$$H|0\rangle = |+\rangle, \quad H|1\rangle = |-\rangle and H|+\rangle = |0\rangle, \quad H|-\rangle = |1\rangle.$$

– The four Bell states (also named as EPR[1] pairs) are defined as:

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}} \quad |\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}} \quad |\beta_{11}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

– The GHZ[2] state of an n-qubit state is defined as

$$|GHZ\rangle = \frac{|00\ldots\rangle + |11\ldots\rangle}{\sqrt{2}}.$$

For example, when $n = 4$, one has $|GHZ\rangle = \dfrac{|0000\rangle + |1111\rangle}{\sqrt{2}}$.

2.2. Solved problems

1. Consider the two-qubit state

$$|q\rangle = c\left(|00\rangle + 2|01\rangle + 3i|11\rangle\right).$$

Determine:

a) the constant c.

[1] Einstein-Podolsky-Rosen.
[2] Greenberger-Horne-Zeilinger.

Then, compute what is the probability of finding:

b) the first qubit in state $|0\rangle$?

c) the second qubit in state $|1\rangle$, provided that the first qubit was found in state $|0\rangle$?

d) both first and second qubits in state $|1\rangle$? Does the result depend on which qubit is first measured?

Solution

a) Normalization of the vector implies that $|c| = 1/\sqrt{14}$.

b) $P(1^{\text{st}}$ qubit in $|0\rangle) = 5/14$. The post-measurement state is $|q_0\rangle = (|00\rangle + 2|01\rangle)/\sqrt{5}$.

c) $P(2^{\text{nd}}$ qubit in $|1\rangle \,|\, 1^{\text{st}}$ qubit in $|0\rangle) = 4/5$.

d) If we measure the 1^{st} qubit first, the probability is $9/14$. If we measure first the 2^{nd} qubit, the joint probability is $(13/14) \times (9/13) = 9/14$. In this case, the result therefore does not depend on which qubit we measure first.

2. Consider a quantum gate U that transforms the qubit $|+\rangle$ into $|0\rangle$ and the qubit $|-\rangle$ into $-|1\rangle$.

a) Write down the matrix associated to this quantum gate. Justify your answer.

b) Determine the resulting qubits if we first apply the quantum gate U and then the quantum gate H to the computational basis.

c) To which matrix is equivalent the previous operation?

Solution

a) One has to find the matrix $U = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $U|+\rangle = |0\rangle$, and $U|-\rangle = -|1\rangle$. These conditions lead to a system of four linear-equations,

$$\begin{cases} a+b &= \sqrt{2} \\ c+d &= 0 \\ a-b &= 0 \\ c-d &= -\sqrt{2} \end{cases}$$

whose solution is: $a = b = d = -c = 1/\sqrt{2}$. As such,

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

b) The matrix associated to first applying U and then H is

$$H \cdot U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \cdot \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Its action on the vectors of the computational basis is therefore:

$$(H \cdot U)|0\rangle = |1\rangle,$$

and

$$(H \cdot U)|1\rangle = |0\rangle.$$

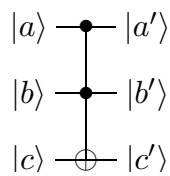
c) We clearly see that the effect on the computational basis of U and H is exactly the same as the Pauli matrix X. We can also see that the matrix form of $H \cdot U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ is exactly the X matrix.

3. Write the matrix U of the previous exercise in the Hadamard basis $\{|+\rangle, |-\rangle\}$.

Solution

To build the matrix associated to U in the Hadamard basis $\{|+\rangle, |-\rangle\}$, $U_{\{|+\rangle,|-\rangle\}}$, one computes $U_{\{|+\rangle,|-\rangle\}}|+\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$ and $U_{\{|+\rangle,|-\rangle\}}|-\rangle = \begin{pmatrix} c \\ d \end{pmatrix}$, and the matrix will be $U_{\{|+\rangle,|-\rangle\}} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, where all the qubits must be expressed in the Hadamard basis. That is, $|+\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|-\rangle = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, hence $|0\rangle = \frac{1}{\sqrt{2}}(|+\rangle + |-\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $|1\rangle = \frac{1}{\sqrt{2}}(|+\rangle - |-\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$. The action of the quantum gate U is then $U_{\{|+\rangle,|-\rangle\}}|+\rangle = |0\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $U_{\{|+\rangle,|-\rangle\}}|-\rangle = -|1\rangle = \frac{-1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$. Finally, we obtain the matrix expressed in the Hadamard basis: $U_{\{|+\rangle,|-\rangle\}} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$.

4. Consider the quantum Toffoli gate as shown in the figure below.



a) Write down the matrix and the truth table of the Toffoli gate.

b) Specify which inputs and outputs should be used in order to implement the NAND gate.

Solution

a) The truth-table of the CC-NOT (Toffoli) gate and the corresponding matrix are:

a	b	c	a'	b'	c'
0	0	0	0	0	0
0	0	1	0	0	1
0	1	0	0	1	0
0	1	1	0	1	1
1	0	0	1	0	0
1	0	1	1	0	1
1	1	0	1	1	1
1	1	1	1	1	0

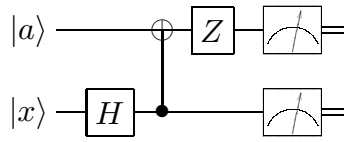
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

b) The truth table of the gate $z = \texttt{NAND}(x, y)$ is:

x	y	z
0	0	1
0	1	1
1	0	1
1	1	0

By looking at the truth table of the Toffoli gate we can obtain the NAND by fixing $c = 1$, and taking $x = a$, $y = b$ and $z = c'$. That is: $c' = \texttt{NAND}(a, b, c = 1)$.

5. Consider the quantum circuit of the figure below.



a) Determine the matrix associate to it.

b) If the input state is $|a\rangle \otimes |x\rangle = \frac{1}{2}|00\rangle - \frac{1}{2}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$, determine the pre-measurement state.

Solution

a) Firstly, we evaluate the output for each of the elements of the computational basis. That is:

$$|00\rangle \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \mapsto \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$$

$$|01\rangle \mapsto \frac{1}{\sqrt{2}}(|00\rangle - |01\rangle) \mapsto \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \mapsto \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

$$|10\rangle \mapsto \frac{1}{\sqrt{2}}(|10\rangle + |11\rangle) \mapsto \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) \mapsto \frac{1}{\sqrt{2}}(-|10\rangle + |01\rangle)$$

$$|11\rangle \mapsto \frac{1}{\sqrt{2}}(|10\rangle - |11\rangle) \mapsto \frac{1}{\sqrt{2}}(|10\rangle - |01\rangle) \mapsto \frac{1}{\sqrt{2}}(-|10\rangle - |01\rangle).$$

Then, we build the column matrix for each of the outputs obtained:

$$\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ -1 \end{pmatrix}; \quad \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \end{pmatrix};$$

$$\frac{1}{\sqrt{2}}(-|10\rangle + |01\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix}; \quad \frac{1}{\sqrt{2}}(-|10\rangle - |01\rangle) = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 \\ -1 \\ -1 \\ 0 \end{pmatrix}.$$

Finally, the matrix of the circuit, C, is easily built:

$$C = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & -1 \\ -1 & 1 & 0 & 0 \end{pmatrix}.$$

b) The pre-measurament state $|\Psi\rangle$ is obtained as $|\Psi\rangle = C(|a\rangle \otimes |x\rangle)$. Using matrix notation, we have

$$|\Psi\rangle = C(|a\rangle \otimes |x\rangle) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & -1 \\ 0 & 0 & -1 & -1 \\ -1 & 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1/2 \\ -1/2 \\ -1/\sqrt{2} \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ -1/2 \\ +1/2 \\ -1/\sqrt{2} \end{pmatrix}.$$

Consequently, the pre-measurement state is $|\Psi\rangle = -\frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle - \frac{1}{\sqrt{2}}|11\rangle$.

2.3. Short questions

Indicate if the following sentences are **TRUE** or **FALSE**, and **JUSTIFY** your answers:

1. The qubits $|q_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ and $|q_2\rangle = \frac{1}{\sqrt{2}}(i|0\rangle - |1\rangle)$ represent the same physical state.

2. The qubit defined in the Bloch sphere by the angles $\theta = \phi = \frac{\pi}{2}$ is $|q\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

3. The angles in the Bloch sphere corresponding to the qubit $|q\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ are $\theta = \pi/2$ and $\phi = \pi$.

4. Consider the following two-qubit: $|q\rangle = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$. The probability to obtain a 0 in the first qubit as a first measurement is 0.

5. We have a 2-qubit $|\Psi\rangle$ where the probability to obtain a 0 in the first qubit as first measure is $1/2$, and the probability to obtain a 0 in the second qubit also as a first measure is $3/8$. The 2-qubit is: $|\Psi\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2\sqrt{2}}|10\rangle + \frac{\sqrt{3}}{2\sqrt{2}}|11\rangle$.

6. The 3-qubit GHZ state is defined as: $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$. After crossing the controlled-swap gate (Fredkin's gate), this state remains unchanged.

7. The EPR-Bell state $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$ can also be written as $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|+-\rangle + |-+\rangle)$.

2.4. Exercises

2.4.1. 1-qubit operations

1. For each of the following qubits, if a measurement is made, what is the probability that we find the qubit in state $|0\rangle$? And in the state $|1\rangle$?

a) $|\psi\rangle = \sqrt{\frac{2}{3}}|0\rangle + \sqrt{\frac{1}{3}}|1\rangle$

b) $|\phi\rangle = \frac{1}{2}|0\rangle + \frac{i\sqrt{3}}{2}|1\rangle$

c) $|\chi\rangle = \frac{i}{\sqrt{3}}|0\rangle - \frac{1-i}{\sqrt{3}}|1\rangle$

2. Find the set of all values of θ for which the following qubits are equivalent:

a) $|1\rangle$ and $\frac{1}{\sqrt{2}}\left(|+\rangle + e^{i\theta}|-\rangle\right)$.

b) $\frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\theta}|1\rangle\right)$ and $\frac{1}{\sqrt{2}}\left(|1\rangle + e^{-i\theta}|0\rangle\right)$

c) $\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$ and $e^{i\theta}\left(\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle\right)$

3. Let $|A\rangle, |B\rangle$ be a basis for representing qubits, the *NOT operation* is defined as

$$|A\rangle \to |B\rangle, \qquad |B\rangle \to |A\rangle.$$

Find the matrix representation of U_{NOT} for the following basis:

a) the computational basis

$$|A\rangle = \begin{pmatrix}1\\0\end{pmatrix}, \quad |B\rangle = \begin{pmatrix}0\\1\end{pmatrix}.$$

b) the Hadamard basis

$$|A\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \quad |B\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}$$

4. Find the eigenvalues and eigenvectors of the gate with the following matrix representation:

$$M = \begin{pmatrix}1 & 0\\0 & e^{i\pi/4}\end{pmatrix}$$

5. Write the matrix S ($\pi/2$ phase gate) as a function of the Pauli matrices and the identity. The S matrix is defined as:

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

6. Show the action of the following 2×2 quantum gates on a qubit expressed in the computational basis $|q\rangle = \alpha|0\rangle + \beta|1\rangle$. X, Y, Z are the Pauli matrices and H is the Hadamard matrix.

a) $U = YXY$

b) $U = HZ$

7. Prove the following three indentities

$$HXH = Z, \qquad HYH = -Y, \qquad HZH = -X.$$

2.4.2. Rotation matrices and the Bloch sphere

8. Locate on the Bloch sphere the following qubits: $|0\rangle$, $|1\rangle$, $|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, $|-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, $|R\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ and $|L\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$.

9. Describe the effect in the Bloch sphere of the Pauli matrices acting on a general qubit expressed in the computational basis.

10. Find the points on the Bloch sphere which correspond to the eigenvectors of the three Pauli matrices.

11. Demonstrate that two orthonormal qubits are represented by antipodal points within the Bloch sphere.

12. If x is a real number and A a matrix that verifies that $A^2 = \mathbb{I}$, show that:

$$\exp(iAx) = \cos(x)\mathbb{I} + i\sin(x)A$$

13. Demonstrate that, except for a global phase, $T = R_z(\pi/4)$. The gate T, also called $\pi/8$ gate, is defined as:

$$T = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{pmatrix}$$

14. Write the Hadamard gate H as a product of R_x and R_z rotations and $e^{i\theta}$ for some θ.

15. Demonstrate that $(\hat{n}\cdot\vec{\sigma})^2 = I$ and use this equivalence to check the following equation:

$$R_{\hat{n}}(\theta) \equiv \exp(-i\theta\hat{n}\cdot\vec{\sigma}/2) = \cos\left(\frac{\theta}{2}\right) I - i\sin\left(\frac{\theta}{2}\right)(n_x X + n_y Y + n_z Z)$$

where $\vec{\sigma}$ denotes the three component vector (X, Y, Z) of Pauli matrices and $\hat{n} = (n_x, n_y, n_z)$ is a real unit vector in three dimensions.

16. Show that ± 1 are the eigenvalues of $\hat{n}\cdot\vec{\sigma}$, and that the projectors onto the corresponding eigenvectors are given by $P_\pm \equiv (I \pm \hat{n}\cdot\vec{\sigma})/2$.

17. Which is the probability of obtaining $+1$ as the result of a measurement of $\hat{n}\cdot\vec{\sigma}$, given that the state prior to measurement is $|0\rangle$. What is the state of the system after the measurement if $+1$ is obtained?

18. Demonstrate that an arbitrary single qubit unitary operator can be written in the form

$$U = \exp(i\alpha) R_{\hat{n}}(\theta)$$

for some real numbers α and θ, and a real three-dimensional unit vector $\hat{n}$. Also find values for α, θ and $\hat{n}$ giving the Hadamard gate H and the phase gate S.

2.4.3. N-qubit operations

19. Consider the following 2-qubit states:

$$|\alpha\rangle = 3|00\rangle - 2|01\rangle + |10\rangle - 5|11\rangle$$

a) Normalize the state

b) Write it in terms of the two 2-qubits $|q_0\rangle$ (a 2-qubit with the first bit 0) and $|q_1\rangle$ (a 2-qubit with the first bit 1)

c) If we attempt to measure only the first bit, with which probability the state will collapse into $|q_0\rangle$? And into $|q_1\rangle$?

d) If the state collapses into $|q_0\rangle$, with which probability we will obtain a 0 in the second bit after a second measurement?

20. A quantum state is described by the following 2-qubit:

$$|\Psi\rangle = 0.5|0\,0\rangle + 0.3e^{i\pi}|0\,1\rangle + b|1\,0\rangle - 0.1e^{-i\pi/2}|1\,1\rangle$$

Determine

a) The value b that normalize $|\Psi\rangle$.

b) The probability to obtain a 0 value in the second qubit as a first measurement.

c) If the first qubit results to be a 0, evaluate the post-measurement probability that the second qubit is also a 0.

d) Are the probabilities of questions b) and c) equal? Reason the answer.

e Write the post-measurement state $|\Psi'\rangle$ of question c).

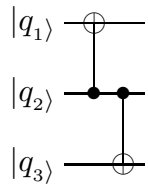
21. For which combinations of input qubits $|a\rangle$ $|x\rangle$, the $CNOT$ gate can generate any of the four *Bell States*?

22. For the matrix represented by:

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

Demonstrate that two applications of it on the same state, namely $B(B|\psi\rangle)$ has the same effect that the NOT gate, giving the same probabilities of finding $|0\rangle$ and $|1\rangle$.

23. Consider the following quantum gate.



a) Write down the matrix associated to this gate.

b) Using matrix notation, determine the output qubit if the input qubit is:

$$|\Psi\rangle = \frac{1}{\sqrt{3}}|000\rangle + \frac{1}{\sqrt{2}}|010\rangle + \frac{1}{\sqrt{6}}|110\rangle.$$

24. Recall that the Fredkin gate performs the following transformation:

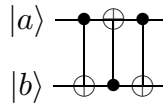
$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

a) Give a quantum circuit which uses three Toffoli gates to construct the Fredkin gate (Hint: the control qubits of the Toffoli gates can be different for each Toffoli gate).

b) Show that the first and last Toffoli gates can be replaced by $CNOT$ gates

2.4.4. Quantum circuits

25. In the figure below, the first gate corresponds to the CNOT gate whereas the second is a reversed CNOT gate.

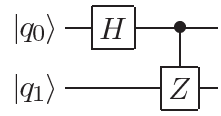


a) Find the matrix representation of the reversed CNOT gate in the computational basis $\{|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle\}$.

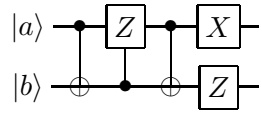
b) Compute the matrix of the total circuit.

26. Find the matrix associated to the following quantum circuits

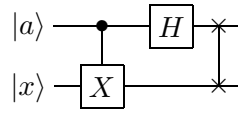
a)



b)

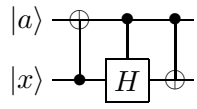


c)



27. Build a 4-qubit circuit that from the input $|0000\rangle$ produces the 4-qubit GHZ state, that is $\frac{1}{\sqrt{2}}(|0000\rangle + |1111\rangle)$.

28. Consider the following quantum circuit

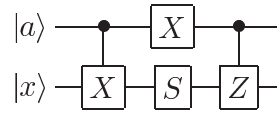


Determine:

a) The matrix of the circuit.

b) If $|a\rangle = |+\rangle$ and $|x\rangle = |-\rangle$, build the two-qubit $|q\rangle = |a\rangle \otimes |x\rangle$ and, using matrix notation, determine the pre-measurement state.

29. Assuming separately $|a\rangle = |0\rangle$ and $|a\rangle = |1\rangle$ compute the action of the following quantum circuit and find the matrix representation in the computational basis.



30. Consider the following two qubits transformations:

$$|00\rangle \rightarrow \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$$
$$|11\rangle \rightarrow \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

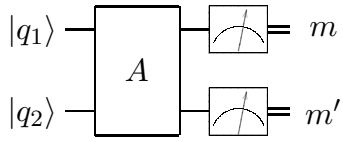
a) Using one-qubit gates and CNOT gates, draw the quantum circuit needed to perform the previous transformation simultaneously.

b) What will be the result if we apply the same circuit to the two states $|01\rangle$ and $|10\rangle$?

31. We have the qubit $|q_1\rangle = \frac{\sqrt{3}}{2}|0\rangle + \mathrm{i}\frac{1}{2}|1\rangle$ and the qubit $|q_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

a) Build the two-qubit $|q\rangle = |q_1\rangle \otimes |q_2\rangle$ and normalize it (if necessary).

Consider now that the two-qubit $|q\rangle$ crosses a quantum circuit, as shown in the figure below,



where the matrix A that represents the circuit is given by

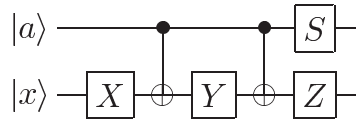
$$A = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -i & 0 \\ 1 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \end{pmatrix}.$$

Determine

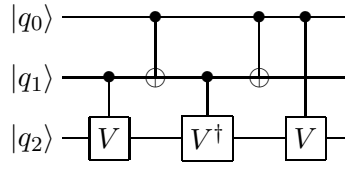
b) The pre-measurement state.

c) The probability to obtain $m' = 1$ if we know that $m = 0$.

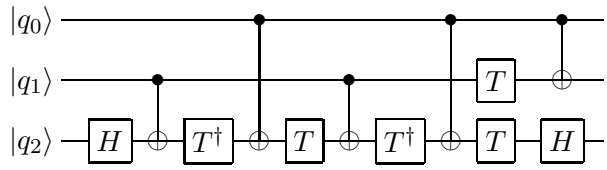
32. Compute the action of the following quantum circuit:



33. Show that if $V = (1-i)\dfrac{I+iX}{2}$, then the three-qubit Toffoli gate can be replaced by the following circuit containing only two-qubit gates:



34. Prove that the quantum circuit:



which includes Hadamard gates (H) and $\pi/4-$phase gate $T = \begin{pmatrix} 1 & 0 \\ 0 & \exp(i\pi/4) \end{pmatrix}$ is an equivalent realization of a $CCNOT$ or Toffoli gate.

35. Using Toffoli gates a binary adder can be constructed accepting two bits X and Y, and at the output, there is a carry bit as well as $(X + Y \ mod \ 2)$. Show the circuit of this binary adder.

36. * The Walsh-Hadamard transform of $n-$qubits, WHT, is defined as $WHT|x\rangle = H^{\otimes n}|x\rangle$. Demonstrate:

a) That

$$H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^{n-1}} |x\rangle$$

b) In the general case we have

$$H^{\otimes n}|x\rangle = \frac{1}{\sqrt{2^n}} \sum_z (-1)^{xz}|z\rangle$$

where $xz = x_1z_1 + x_2z_2 + \ldots + x_nz_n$ is the bitwise inner product modulo 2.

37. * Design a quantum circuit that constructs the Hardy state[3] $\frac{1}{\sqrt{12}}(3|00\rangle + |01\rangle + |10\rangle + |11\rangle$ starting from the two-qubit state $|00\rangle$.

[3]For a general technique to construct arbitrary quantum states we refer the reader to the papers `arxiv.org/abs/quant-ph/0104030` and `arxiv.org/abs/quant-ph/0406176`

The IBM Quantum Experience

The IBM Quantum Experience is an online platform that allows, for the first time in history, the general public to execute quantum codes on real quantum computers. Since 2018 IBM makes available through the cloud three quantum processors: two 5-qubit processors, called Essex and Yorktown, and a 16-qubit processor, named Melbourne. IBM prototype processors rely on transmon superconducting qubits at cryogenic temperatures as low as 15 mK.

In order to use these quantum computers, IBM developed two interfaces: the Circuit Composer and the Quantum Information Software Kit or Qiskit. The Circuit Composer is an intuitive and simple drag and play quantum circuit builder. On the other hand, Qiskit is a more suitable tool which permits, among other features, high performance simulation of a quantum circuit, even introducing noise as it can appear in a real device. Both interfaces permit to run quantum circuits and algorithms through the cloud and compare theoretical results with experimental results based in real quantum computers.

Exercises:

a) Sign up for an account on the IBM Quantum Experience website (`https://quantum-computing.ibm.com/`). Beware that IBM uses the reverse notation for qubits, that is, the qubit $|001\rangle$ is expressed by IBM as $|100\rangle$.

b) Get familiar with Qiskit Aqua. This platform uses Python to create quantum programs based on QASM (Open Quantum Assembly Language), a quantum programming language to specify instructions into a quantum computer.

c) Run with Qiskit some of the quantum circuits proposed in this Chapter. Compare the results obtained from Qiskit simulations with those you would obtain on a real quantum computer. Do the results match?

d) Build a $CNOT$-gate between the 1st and 3rd qubit using the Essex and the Yorktown processors (see Figure 2.2). Given that their architecture is different you will have to implement different quantum circuits. After executing both circuits, does the result depend on the architecture? Does the number of gates influence the results?

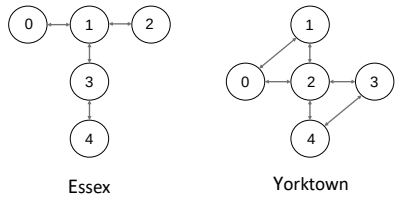


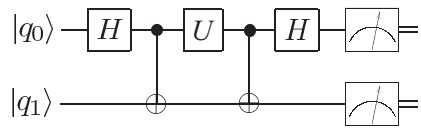
Fig. 2.2 Topological configuration of the 5-qubit IBM processors Essex and Yorktown.

→ 3

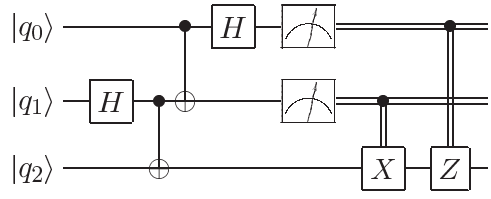
Quantum Computing: Applications

3.1. Definitions

– Quantum circuit for superdense coding:



– Standard quantum teleportation circuit with $|q_0\rangle$ (the teleported qubit) and $|q_1\rangle$ and $|q_2\rangle$ (ancilla qubits).



3.2. Solved Problems

1. Consider a standard quantum teleportation circuit between Alice and Bob. They think that they share the entangled Bell state $|\beta_{00}\rangle$, but an error has occurred in the production of the entangled state and they actually share the state $|q_1 q_2\rangle = \frac{1}{2}(|00\rangle + |11\rangle) + \frac{1}{\sqrt{2}}|01\rangle$.

Determine:

a) The probability of Alice measuring (m, m').

b) If Alice wants to teleport the qubit $|q_0\rangle = |+\rangle$ and she measures $(m, m') = (0, 1)$, what is the probability that the qubit was correctly teleported to Bob?

Solution

a) We are considering a general qubit, $|q_0\rangle = \alpha|0\rangle + \beta|1\rangle$; so the initial state is:

$$|q_0\rangle \otimes |q_{12}\rangle = (\alpha|0\rangle + \beta|1\rangle) \otimes (\frac{1}{2}(|00\rangle + |11\rangle) + \frac{1}{\sqrt{2}}|01\rangle) =$$
$$= \frac{1}{2}\left[\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle\right] + \frac{1}{\sqrt{2}}[\alpha|001\rangle + \beta|101\rangle].$$

Then we cross the CNOT and the Hadamard gates to obtain the following pre-measurement state:

$$\mapsto \frac{1}{2}\left[\alpha|000\rangle + \alpha|011\rangle + \beta|110\rangle + \beta|101\rangle\right] + \frac{1}{\sqrt{2}}[\alpha|001\rangle + \beta|111\rangle] \mapsto$$
$$\frac{1}{2\sqrt{2}}[\alpha|000\rangle + \alpha|100\rangle + \alpha|011\rangle + \alpha|111\rangle + \beta|010\rangle - \beta|110\rangle +$$
$$+ \beta|001\rangle - \beta|101\rangle] + \frac{1}{2}[\alpha|001\rangle + \alpha|101\rangle + \beta|011\rangle - \beta|111\rangle].$$

Finally, we arrange the first two qubits that Alice can measure for the different values (m, m'):

$$= |00\rangle \frac{1}{2}\left[\frac{1}{\sqrt{2}}\alpha|0\rangle + \left(\frac{1}{\sqrt{2}}\beta + \alpha\right)|1\rangle\right] +$$
$$|01\rangle \frac{1}{2}\left[\frac{1}{\sqrt{2}}\beta|0\rangle + \left(\frac{1}{\sqrt{2}}\alpha + \beta\right)|1\rangle\right] +$$
$$|10\rangle \frac{1}{2}\left[\frac{1}{\sqrt{2}}\alpha|0\rangle - \left(\frac{1}{\sqrt{2}}\beta - \alpha\right)|1\rangle\right] +$$
$$|11\rangle \frac{1}{2}\left[\frac{-1}{\sqrt{2}}\beta|0\rangle + \left(\frac{1}{\sqrt{2}}\alpha - \beta\right)|1\rangle\right]$$

Then, the probabilities of measuring (m, m') will be

$$P(0,0) = \left(\frac{1}{2\sqrt{2}}\alpha\right)^2 + \frac{1}{2}\left(\frac{1}{\sqrt{2}}\beta + \alpha\right)^2 = \frac{1}{8} + \frac{\alpha\beta}{2\sqrt{2}} + \frac{1}{4}\alpha^2,$$

given that $|q_0\rangle$ is normalized (i.e., $\alpha^2 + \beta^2 = 1$). The first two terms in the brackets will give the same results; so we easily obtain the remaining probabilities:

m	m'	$P(m, m')$
0	0	$\frac{1}{8} + \frac{\alpha\beta}{2\sqrt{2}} + \frac{1}{4}\alpha^2$
0	1	$\frac{1}{8} + \frac{\alpha\beta}{2\sqrt{2}} + \frac{1}{4}\beta^2$
1	0	$\frac{1}{8} - \frac{\alpha\beta}{2\sqrt{2}} + \frac{1}{4}\alpha^2$
1	1	$\frac{1}{8} - \frac{\alpha\beta}{2\sqrt{2}} + \frac{1}{4}\beta^2$

We can easily check that $\sum_{m,m'} P(m,m') = 1$.

b) If Alice measures $(m,m') = (0,1)$, Bob's qubit collapses into:

$$|q_2\rangle = \frac{1}{2}\left[\frac{1}{\sqrt{2}}\beta|0\rangle + \left(\frac{1}{\sqrt{2}}\alpha + \beta\right)|1\rangle\right].$$

After applying $Z^m X^{m'} = Z^0 X^1$, we will obtain:

$$|q_2\rangle = \frac{1}{2}\left[\left(\frac{1}{\sqrt{2}}\alpha + \beta\right)|0\rangle + \frac{1}{\sqrt{2}}\beta|1\rangle\right].$$

Given that the teleported qubit is $|q_0\rangle = |+\rangle \Rightarrow \alpha = \beta = \frac{1}{\sqrt{2}}$

$$|q_2\rangle = \frac{1}{4}\left(1+\sqrt{2}\right)|0\rangle + \frac{1}{2}|1\rangle \approx 0.604|0\rangle + 0.5|1\rangle;$$

and after renormalizing, the final qubit that Bob has is:

$$|q_2\rangle = 0.924|0\rangle + 0.382|1\rangle.$$

The probability that the qubit $|q_0\rangle$ was correctly teleported is obtained by projecting $|q_2\rangle$ onto the $|+\rangle$ state

$$P = |\langle +|q_2\rangle|^2 = \left(\frac{0.924}{\sqrt{2}} + \frac{0.382}{\sqrt{2}}\right)^2 = 0.853.$$

3.3. Short Questions

Indicate if the following sentences are **TRUE** or **FALSE**, and **JUSTIFY** your answers:

1. No quantum circuit exists that can make copies of the qubits $|+\rangle$ or $|-\rangle$.

2. No quantum circuit exists that can make copies of the computational basis $\{|0\rangle, |1\rangle\}$ and also of the Hadamard basis $\{|+\rangle, |-\rangle\}$.

3. In a communication through a superdense coding, Alice and Bob are sharing the EPR-Bell state $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$. If Alice wants to send the classical bits 10 to Bob, she should apply the matrix $U = ZX$.

4. In a superdense coding experiment, Alice sends 3 classical bits to Bob using only 1 qubit.

5. In a typical teleportation process of a qubit $|q\rangle = \alpha|0\rangle + \beta|1\rangle$, the probability that Alice measures $(m,m') = (0,0)$ depends on the values of α and β.

6. Alice and Bob are sharing the Bell state $|\beta_{10}\rangle$ within a teleportation circuit. Alice wants to teleport the qubit $|+\rangle$ and, after measuring, the outcome she obtains is $(m,m') = (0,0)$, which is sent to Bob. Bob needs to apply a Z gate to its qubit for correct teleportation.

3.4. Exercises

3.4.1. No-cloning Theorem and Quantum Parallelism

1. The CNOT gate performs the following operation in which a and b could be 0 or 1

$$|a\rangle \otimes |b\rangle \rightarrow |a\rangle \otimes |a \oplus b\rangle,$$

where $\oplus$ is the XOR operation. Demonstrate that the CNOT gate can be used to clone a bit.

2. Suppose we have a 2-qubit system in which the first qubit is in the state $|\psi\rangle$, which we know to be either $|+\rangle$ or $|-\rangle$, and the second qubit is $|0\rangle$. We wish to make a copy of the first qubit, i.e., we want to end up in the state $|\psi\rangle|\psi\rangle$. Design a quantum circuit with three Hadamard gates and one CNOT capable of making this copy.

3. * Consider a unitary transformation U_f that implements $\mod 4$ calculations. Let $a = (a_1, a_0)$ and $b = (b_1, b_0)$ represent two numbers $\in \mathbb{Z}_4$, such that $a = 2a_1 + a_0$ and $b = 2b_1 + b_0$. By using as many standard gates as you need, build a small 6-qubit circuit that implements:

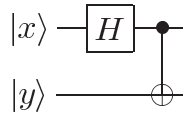
a) The addition transformation $|a, b, 0\rangle \mapsto |a, b, a + b \mod 4\rangle$.

b) The multiplication transformation $|a, b, 0\rangle \mapsto |a, b, ab \mod 4\rangle$.

c) Is it possible to generalize the previous operations to n-bits numbers $a, b \in \mathbb{Z}_{2n}$?

3.4.2. EPR-Bell State Generators and Measurement

4. Compute the action of the following circuit when applied to the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Do you know any other circuit capable of producing the same result?

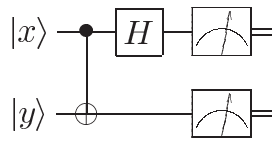


5. Consider the four possible Bell states $|\beta_{xy}\rangle$.

a) Calculate the following four probabilities: (i) of finding 0 in the first qubit; (ii) of finding 1 in the first qubit; (iii) of finding 0 in the second qubit; and (iv) of finding 1 in the second qubit.

b) If we make a measurement E_{im} of the Bell states, which is the final state after the measurement? Write down the 16 possible results (remember that E_{im} stands for the measurement in the i^{th} position of the qubit m).

6. The following circuit includes 2-qubit state measurements. If the measurements are made on the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, which one is the classical bit m, m' output if the input to this gate circuit are any of the four Bell states $|\beta_{m,m'}\rangle$? This procedure is called a *Bell measurement*.



7. Consider the EPR-Bell state measurement of the previous question. When the input state $|\beta_{00}\rangle$ is introduced in the circuit, this obtains the two classical bits $m = 0$ and $m' = 0$, as expected. But, eventually, a noisy quantum state is introduced into the system $|\Psi\rangle = \frac{\sqrt{3}}{2\sqrt{2}}(|00\rangle + |11\rangle) + \frac{1}{2}|10\rangle$. Evaluate:

a) If the input state is $|\Psi\rangle$, which classical bits are obtained) At what probability?

b) What is the probability that we make a wrong measurement? (In other words, that we obtain something different than $(m, m') = (0, 0)$?)

c) If the probabilities of obtaining m and m', $P(m, m')$, are $P(0, 0) = P(0, 1) = \frac{1}{4}$, $P(1, 0) = 0$ and $P(1, 1) = \frac{1}{2}$, what is the input state?

3.4.3. Superdense Coding

8. Let us assume that Alice and Bob share the entangled Bell state $|\beta_{00}\rangle$. Alice wants to send two classical bits to Bob using only one qubit (*superdense coding*). In order to send the four possible pairs of classical bits (00, 01, 10 and 11), she switches the U gate into $\mathbb{I}$, Z, X and ZX; applies it to $|\beta_{00}\rangle$; and sends her part of the qubit to Bob, who performs a Bell measurement on the resulting entangled qubit. Show which classical bits Bob measured after each change of gate performed by Alice.

9. Consider the standard quantum circuit used for superdense coding. Alice and Bob share the EPR-Bell state $|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$.

a) Which Pauli matrices should Alice use for gate U in order to transform $|\beta_{10}\rangle$ into any of the EPR-Bell states?

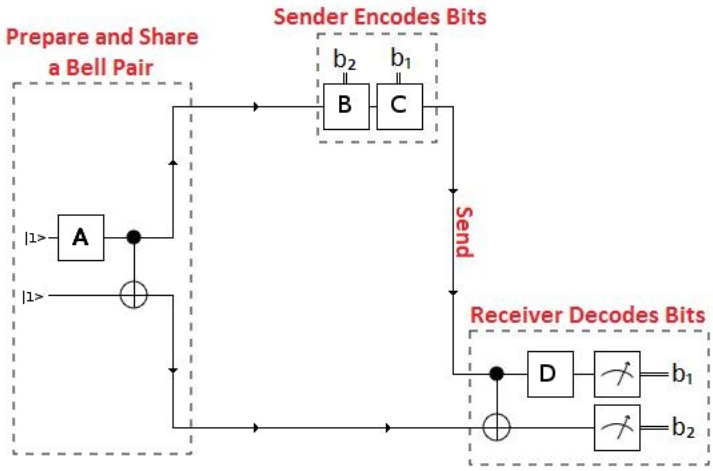
b) What are the pre-measurement states?

c) Write out the classical bits m and m' as a function of the matrix U.

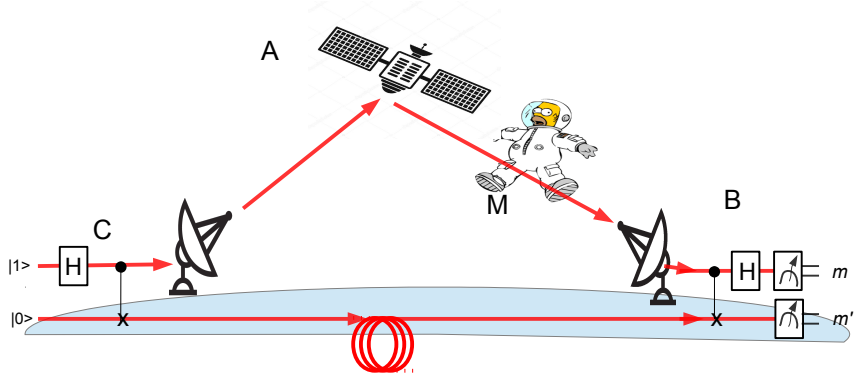
10. From the figure below, consider the quantum circuit designed for superdense coding communication. If the circuit is initialized with the qubit $|11\rangle$, determine:

a) Which of the matrices A, B, C and D Alice (the sender) should use if she wants to send to Bob (the receiver) the bits $(b_1, b_2) = (0, 0)$. Justify your answer.

b) Imagine now that there is an error in the system. Specifically, the circuit is not initialized by the qubit $|11\rangle$ but is instead initialized by a different qubit $|ab\rangle$. Knowing this, the receiver now obtains $(b_1, b_2) = (0, 1)$. Determine which qubit will be $|ab\rangle$.



11. Consider the quantum superdense coding that is implemented in the figure below. Charlie (C) initializes the system with the 2-qubit $|10\rangle$. Then, after crossing the corresponding quantum gates, the first qubit (photon) is sent to the satellite (Alice) and the other one is transmitted along an optical fiber to Bob (B).



a) Determine the matrix or matrices that Alice should apply if she wants to send to Bob the bits $(m, m') = (0, 1)$.

b) A man-in-the-middle (M) interferes with the photon sent by Alice. M measures the photon (collapsing the qubit) and resends it to Bob. Determine the values that Bob can now obtain, as well as their probabilities.

c) Considering the previous question's results, would Bob be able to guess that M exists?

3.4.4. Teleportation

12. Alice and Bob share a state $a|+-\rangle + b|-+\rangle$, where the first qubit is Alice's and the second qubit is Bob's.

a) Write the shared state so that Alice's qubit is expressed in the $\{|0\rangle, |1\rangle\}$ basis and Bob's qubit is expressed in the $\{|+\rangle, |-\rangle\}$ basis.

b) Alice measures her qubit in the standard basis $\{|0\rangle, |1\rangle\}$ and sends the measurement outcome to Bob. Using only X, Z and H gates (or combinations of them), what does Bob have to do to transform his qubit into the $a|0\rangle + b|1\rangle$?

13. Alice and Bob share a state $a|++\rangle + b|--\rangle$, where the first qubit is Alice's and the second qubit is Bob's. Alice measures her qubit in the standard basis and sends the measurement outcome to Bob. What does Bob have to do to transform his qubit into $a|0\rangle + b|1\rangle$?

14. Show tha, when appropriately choosing $|q_1\rangle$ and $|q_2\rangle$ to create the different Bell states, quantum teleportation of qubit $|q_0\rangle$ is possible within the standard teleportation quantum circuit.

15. Beginning with the right-hand expression and going backwards, show that:

$$|\psi\rangle|\beta_{00}\rangle = \frac{1}{2}|\beta_{00}\rangle|\psi\rangle + \frac{1}{2}|\beta_{01}\rangle(X|\psi\rangle) + \frac{1}{2}|\beta_{10}\rangle(Z|\psi\rangle) + \frac{1}{2}|\beta_{11}\rangle(XZ|\psi\rangle),$$

where $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$.

16. Consider a standard quantum teleportation circuit between Alice and Bob. The input state is $|\Psi\rangle = |q\rangle \otimes |\beta_{00}\rangle$ and the pre-measurement state is:

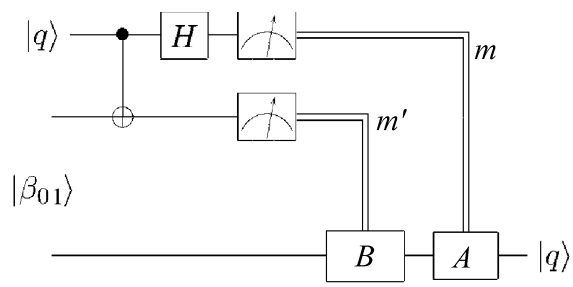
$$|0\,0\rangle\frac{\alpha|0\rangle + \beta|1\rangle}{2} + |0\,1\rangle\frac{\alpha|1\rangle + \beta|0\rangle}{2} + |1\,0\rangle\frac{\alpha|0\rangle - \beta|1\rangle}{2} + |1\,1\rangle\frac{\alpha|1\rangle - \beta|0\rangle}{2}.$$

Alice wants to teleport two type of qubits: $|q_1\rangle = |0\rangle$ and $|q_2\rangle = |+\rangle$. But the first measurement is wrong and always reads $m = 0$.

a) Is it possible that the final qubit teleported to Bob will be something different than $|q_1\rangle$ or $|q_2\rangle$? If yes, determine the different possibilities.

b) Determine the probabilities that $|q_1\rangle$ and $|q_2\rangle$ are teleported correctly.

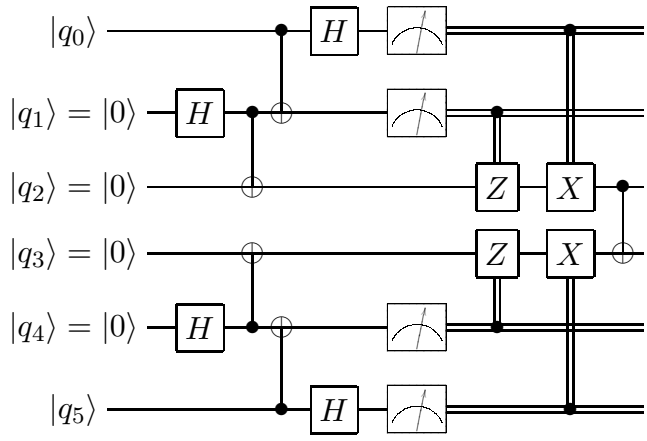
17. Consider a standard quantum teleportation circuit between Alice and Bob, as in the figure below. Alice wants to send a qubit $|q\rangle = \alpha|0\rangle + \beta|1\rangle$ to Bob while sharing the entangled state $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, also as in the figure below.



a) Determine which matrices should be used by Bob as a function of the possible values $(m,\, m')$.

b) Imagine that the entangled state $|\beta_{01}\rangle$ has suffered a decoherence process and has collapsed into the state $|11\rangle$. Determine the probability that the qubit $|q\rangle$ is now correctly teleported.

18. Alice owns the qubits $|q_0\rangle = \alpha_0|0\rangle + \alpha_1|1\rangle$ and $|q_1\rangle$. Similarly, Eve has the qubits $|q_4\rangle$ and $|q_5\rangle = \gamma_0|0\rangle + \gamma_1|1\rangle$. Finally, Bob controls the qubits $|q_2\rangle$ and $|q_3\rangle$. In some intermediate part of the circuit in the figure, Alice and Bob share the entangled Bell state $|q_1 q_2\rangle = |\beta_{00}\rangle$ while Eve and Bob share the entangled Bell state $|q_3 q_4\rangle = |\beta_{00}\rangle$.



a) What is the final 2-qubit state owned by Bob? In other words, what is the final state of the 2-qubit $|q_2 q_3\rangle$?

b) What is the operation that this circuit performs?

The Canary Island 143 km Teleportation Experiment

In 2012, an international research team led by the Austrian Academy of Sciences and the University of Vienna successfully teleported quantum information through polarized photons[1] over a distance of 143 km[2]. The experiment showed that, with current technology and under real conditions, long-distance teleportation is feasible.

The experiment began with the creation of two photons entangled as[3] $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|H\rangle|V\rangle - |V\rangle|H\rangle)$. Alice kept one photon in La Palma while the other one was sent 143 km to Bob in Tenerife. At the same time, the input photon (the one to be teleported) was prepared and sent to Alice. Alice made a joint measurement in the Bell basis of that photon and of one photon that she had entangled with Bob. The result of that measurement was sent to Bob, who applied the corresponding correction matrices and determined that his photon was in the same state as the input state. Thus, the photon had been teleported.

Note that Alice used two channels: a quantum channel to send the entangled photon to Bob and a classical one to feed her measurement information forward. Photons from both channels were sent through free space, thus subject to atmospheric attenuation -— which introduces notable losses. However, this attenuation is less sensitive than if, for instance, a fiber optic link were to be used. Despite the source of error introduced by the attenuation and other factors, the probability that a qubit had been successfully teleported was estimated to be around 71%, well above the statistical limit of 50% should Alice and Bob not share an entangled state. In summary, the Canary Island teleportation experiment represented a milestone for future quantum satellite communications and nearly achieving a quantum internet platform.

Exercises

a) Identify which of the experiment's different elements have the theoretical teleportation quantum circuit.

b) Which matrices should be used by Bob as a function of Alice's measurement?

c) In the experiment, four photon polarization states were randomly teleported. These states are equivalent to the following qubits: $|0\rangle, |1\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$. Consider now that Alice and Bob do not share an entangled state but instead share the state $|01\rangle$. Show that in this case the probability of any of the four initial qubits being correctly teleported is only 0.5.

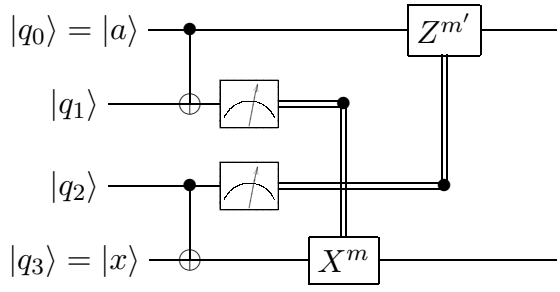
[1] Chapter 6 will introduce photon polarization.

[2] Ma, X., Herbst, T., Scheidl, T. et al. Quantum teleportation over 143 kilometres using active feed-forward. Nature **489**, 269–273 (2012). https://doi.org/10.1038/nature11472

[3] The state $|\Psi^-\rangle$ is equivalent to the Bell state $|\beta_{11}\rangle$.

3.4.5. Distributed Quantum Computing

19. Consider that qubits $|q_0\rangle$ and $|q_1\rangle$ are controlled by Alice; qubits $|q_2\rangle$ and $|q_3\rangle$ are controlled by Bob; and qubits $|q_1\rangle$ and $|q_2\rangle$ are entangled through the Bell state $|\beta_{00}\rangle$. Show that the following circuit is equivalent to a distributed CNOT gate, i.e., a CNOT gate which uses Alice's qubit $|a\rangle$ as the control and Bob's qubit $|x\rangle$ as the target. This is the quantum teleportation of a CNOT gate.
(Hint: Bob measures his qubit in the Hadamard $\{|+\rangle, |-\rangle\}$ basis).



Quantum Measurements

4.1. Definitions

– Given a quantum state $|\psi\rangle$ with n possible outcomes, the probability that we measure the outcome m ($m = 1, \ldots, n$) is

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

with M_m being a measurement operator.

– The completeness condition $\sum_m p(m) = \sum\langle\psi|M_m^\dagger M_m|\psi\rangle = 1$ implies that the set of operators shall be *complete*, i.e., $\sum_{m=1}^{n} M_m^\dagger M_m = \mathbb{I}$.

– After m is measured, the post-measurement state is $|\psi'\rangle = M_m|\psi\rangle/\sqrt{p(m)}$.

– Different kinds of quantum measurement operators fulfil the previous general definition: quantum measurement in the orthonormal basis, projective (Von Neumann) measurements and *POVM*[1] measurements.

– *Quantum measurement in an orthonormal basis:*

- The measurement operator M_m is defined as $M_m = |x_m\rangle\langle x_m|$, with $|x_m\rangle$ being one element of an orthonormal basis.
- In this case, M_m is a *projective* operator, i.e., $M_m^\dagger M_m = M_m$.
- Given an n-qubit $|\psi\rangle = |\psi_1, \ldots, \psi_n\rangle$, the basis state measurement operator of the i-th qubit and m value, E_{im}, is defined as $E_{im}|\psi\rangle = |\psi_1, \ldots, \psi_{i-1}, m, \psi_{i+1}, \ldots, \psi_n\rangle$.

– *Projective (Von-Neumann) measurements*

- An observable in quantum mechanics is represented by a *Hermitian*[2] operator A. The latter may always be decomposed as $A = \sum \lambda_m P_m$, where P_m is the projector $|\lambda_m\rangle\langle\lambda_m|$ on the eigenspace of A with eigenvalue λ_m.

[1] The acronym POVM stands for "Positive-Operator-Valued Measure".

[2] An operator A is said to be *Hermitian* if $A^\dagger = A$, where $A^\dagger$ is the conjugate-transpose (or Hermitian conjugate) of A.

- The *average value* or *mean* of an observable on a state is

$$\langle A\rangle \equiv \langle\lambda\rangle = \sum \lambda_m\, p(\lambda_m) = \sum \lambda_m \langle\psi|P_m|\psi\rangle = \langle\psi| \sum \lambda_m P_m|\psi\rangle = \langle\psi|A|\psi\rangle.$$

- The *mean-square* is defined as

$$\langle A^2\rangle \equiv \langle\lambda^2\rangle = \sum \lambda_m^2\, p(\lambda_m) = \langle\psi|A^2|\psi\rangle.$$

- While the *variance* of the observable is

$$\langle \Delta A^2\rangle \equiv \langle\lambda^2\rangle - \langle\lambda\rangle^2 = \langle A^2\rangle - \langle A\rangle^2.$$

– *POVM measurements*

- A set of operators $\{E_m\}$ define a POVM if: a) each operator E_m is positive[3]; and b) the completeness relation $\sum_m E_m = 1$ is fulfilled.

– The *density matrix* describing a quantum system that may be in one of a number of states $|\psi_i\rangle$ with probability p_i is

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$

A correctly-defined density matrix has unit trace (i.e., $\sum_i p_i = 1$) and it is Hermitian.

– The *purity* of a quantum system is defined by

$$\mathcal{P} = \mathrm{tr}(\rho^2).$$

If $\mathcal{P} = 1$, the system is said to be *pure*; while if $\mathcal{P} < 1$, the system is said to be *mixed*.

– The similiarity of the quantum system ρ to a reference pure state $|\psi\rangle$ is quantified by the *fidelity* $\mathcal{F} = \langle\psi|\rho|\psi\rangle$.

4.2. Solved Problems

1. Consider the following quantum measurement operator M_1:

$$M_1 = \frac{1}{3}\begin{pmatrix} 1 & -i & 0 & 1 \\ i & 1 & 0 & i \\ 0 & 0 & 0 & 0 \\ 1 & -i & 0 & 1 \end{pmatrix}.$$

a) Demonstrate that it is a projective operator.

b) Calculate the probability that outcome 1 is measured on the quantum state $|\Psi\rangle = \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle - \frac{1}{\sqrt{2}}|11\rangle$.

[3] E_m is a *positive* operator if $\langle\Psi|E_m|\Psi\rangle \geq 0$ for any normalized state $|\Psi\rangle$.

Solution

a) The matrix product $M_1^\dagger M_1$ equals M_1 itself, which means that the operator M_1 is projective. For this specific case, it turns out that $M_1^\dagger = M_1$ (i.e., that M is a Hermitian matrix).

b) Given $\langle\Psi| = |\Psi\rangle^\dagger = \frac{1}{2}\langle 00| + \frac{1}{2}\langle 01| - \frac{1}{\sqrt{2}}\langle 11|$, the desired probability is

$$P(|\Psi\rangle) = \langle\Psi|M_1^\dagger M_1|\Psi\rangle = \langle\Psi|M_1|\Psi\rangle = \frac{2-\sqrt{2}}{6}.$$

2. A qubit $|q\rangle$ is measured in the Hadamard basis $\{|+\rangle, |-\rangle\}$. Determine:

a) The projective measurement operators associated with states $|+\rangle$ and $|-\rangle$. Write each of those in both bra-ket and matrix notation. (Use the computational basis to express both the bra-ket and matrix notation of the operators).

b) The probability of it being measured as a $|+\rangle$, assuming that $|q\rangle = \frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle$.

Solution

a) The two projectors in bra-ket notation read as follows:

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

$$= \frac{1}{2}(|00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| + |11\rangle\langle 11|)$$

and

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

$$= \frac{1}{2}(|00\rangle\langle 00| - |01\rangle\langle 01| - |10\rangle\langle 10| + |11\rangle\langle 11|).$$

While, in matrix notation, the operators read as $P_+ = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ and $P_- = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}$.

b) The requested probability is $P(+|q) = \langle q|P_+|q\rangle$. We can use both bra-ket or matrix notation for calculating it. Using matrix notation in the computational basis, for instance, we have $P(+|q) = \langle q|P_+|q\rangle = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \end{pmatrix}\frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} \frac{1}{2} \\ -\frac{\sqrt{3}}{2} \end{pmatrix} = \frac{2-\sqrt{3}}{4} = 0.0669$.

3. A system is in the state

$$|\Psi\rangle = \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle.$$

A measurement of X is made. Evaluate the probabilities p_1 and p_2 of finding the state $|\Psi\rangle$ in each of the eigenstates of X.

Solution The eigenvalues of X are obtained from $\det|X-\lambda I|=0 \Rightarrow \lambda^2+1=0 \Rightarrow \lambda_{1,2}=\pm 1$. The corresponding normalized eigenvectors are $u_{\lambda_1}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}=|+\rangle$ and $u_{\lambda_2}=\frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}=|-\rangle$. The associated probabilities are then:

$$p_1=|\langle+|\Psi\rangle|^2=\frac{1}{8}(\sqrt{3}-1)^2=0.067$$

$$p_2=|\langle-|\Psi\rangle|^2=\frac{1}{8}(\sqrt{3}+1)^2=0.933$$

4.3. Short Questions

Indicate if the following sentences are **TRUE** or **FALSE**, and **JUSTIFY** your answers:

1. Given the following measurement operator:

$$M_+=\frac{1}{2}\begin{pmatrix}1 & -i\\ i & 1\end{pmatrix}$$

and the quantum state $|\Psi\rangle=\dfrac{|0\rangle+i|1\rangle}{\sqrt{2}}$, the probability of measuring + is 1.

2. The projective measurement operator M_R corresponding to the quantum state $|R\rangle=\frac{1}{\sqrt{2}}(|0\rangle+i|1\rangle)$ is given by the matrix:

$$M_R=\frac{1}{2}\begin{pmatrix}1 & i\\ i & -1\end{pmatrix}.$$

3. The density matrix corresponding to a 50:50 mixture of states $|0\rangle$ and $|+\rangle$ is:

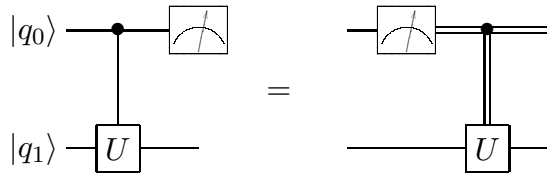
$$\rho=\frac{1}{4}\begin{pmatrix}3 & 1\\ 1 & 1\end{pmatrix}$$

4. Consider a mixture of d states. The lowest values that the purity $\mathcal{P}$ can achieve is $\mathcal{P}=1/d$.

5. The fidelity $\mathcal{F}_1$ between the pure states $|0\rangle$ and $|+\rangle$ is exactly the same as the fidelity $\mathcal{F}_2$ between $|0\rangle$ and $|-\rangle$.

4.4. Exercises

1. Demonstrate that the measurement commutes with controls, that is, show that the following two quantum circuits are equivalent:

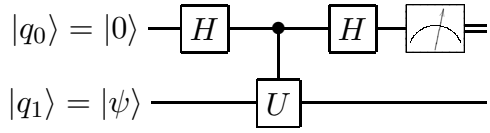


2. Write the projective measurement operator of the Bell-state $|\beta_{00}\rangle$. Then find the probability of measuring $|\psi\rangle = \frac{1}{2}\left[|00\rangle + |01\rangle + |10\rangle + |11\rangle\right]$ with the previous operator.

3. In the 143-km teleportation experiment between the Canary Islands, Alice performs a measurement in the Bell-state basis, that is, she projects her two qubits onto the four Bell states. Consider that the qubit to be teleported is $|q_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and that Alice and Bob share the state $|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Determine the probability of the first two qubits collapsing into the Bell-states $|\beta_{11}\rangle$ or $|\beta_{01}\rangle$.

4. We have the following two-qubit: $|q\rangle = \frac{1}{\sqrt{3}}\left[|00\rangle + |01\rangle + |10\rangle\right]$. If we want to measure a classical bit 0 in the first position, we use the operator E_{10}. Find $E_{10}|q\rangle$ and the corresponding probability.

5. Consider a quantum gate U with eigenstate $|\phi\rangle$, such that $U|\psi\rangle = e^{i\theta}|\psi\rangle$.



a) Demonstrate that the above quantum circuit can be used to estimate the phase θ.

b) By applying the previous circuit, will it be possible to distinguish between the states $|\psi\rangle$ and $-|\psi\rangle$? Justify your answer.

6. A system can be in one of two states: $|\psi\rangle$ or $|\phi\rangle$. The states fulfill the following condition: $\langle\psi|\phi\rangle = \cos\theta$, i.e., they are not orthogonal. Describe a POVM that can distinguish between the two states.

7. Consider the following collection of measurement operators:

$$E_1 = u|1\rangle\langle 1|,$$

$$E_2 = u|-\rangle\langle -|,$$

$$E_3 = \mathbb{I} - E_1 - E_2,$$

where $u = \sqrt{2}/(1+\sqrt{2})$. If we denote by $p(1)$ and $p(2)$ the probabilities associated with the operators E_1 and E_2, respectively, determine:

a) That the set of operators $\{E_1, E_2, E_3\}$ form a POVM.

b) The probabilities $p(1)$ and $p(2)$ when the input state is $|0\rangle$

c) The probabilities $p(1)$ and $p(2)$ when the input state is $|+\rangle \equiv \frac{|0\rangle+|1\rangle}{\sqrt{2}}$

d) If we know that the input state is either $|0\rangle$ or $|+\rangle$, can the two previous measurement operators allow us to distinguish between these two input states? Give reasons for the answer.

8. Consider the state $|\psi\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

a) If P_0 is the projection operator associated with the state $|0\rangle$, describe the action of the operator $P_0 \otimes \mathbb{I}$ on the state $|\psi\rangle$.

b) If P_1 is the projection operator associated with the state $|1\rangle$, describe the action of the operator $\mathbb{I} \otimes P_1$ on the state $|\psi\rangle$.

9. Given a measurement operator M, the probability of measuring a quantum state $|\Psi\rangle$ is $p(\Psi) = \langle\Psi|M^\dagger M|\Psi\rangle$. Consider the following measurement operator:

$$\mathbf{M} = \frac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}$$

a) Write the M operator as a product of bra-kets and check that M is a projective operator (i.e., $M^\dagger M = M$).

b) Using bra-ket notation, calculate the probabilities of measurement when the input state is $|1\rangle$ and when it is $|-\rangle$.

c) Using this measurement operator, can we distinguish if the initial state is $|1\rangle$ or $|-\rangle$? Justify your answer.

10. A system is in the state

$$|\psi\rangle = \frac{1}{2}|u_1\rangle - \frac{\sqrt{2}}{2}|u_2\rangle + \frac{1}{2}|u_3\rangle,$$

where the states $|u_1\rangle, |u_2\rangle, |u_3\rangle$ are eigenstates of the energy operator E with eigenvalues equal to $\hbar\omega, 2\hbar\omega, 3\hbar\omega$, respectively.

a) Write the projection operators corresponding to each possible measurement

b) Using the measurement operators, determine the probability of finding the system in each of the states $|u_1\rangle, |u_2\rangle, |u_3\rangle$.

c) What is the average energy of the system?

11. Find the diagonal representation of the Pauli matrix Y. What are its eigenstates?

12. A measurement with respect to a matrix means making measurements with the projection operators constructed from the eigenstates of the matrix. Now, consider a qubit in the state $|\psi\rangle = \frac{\sqrt{3}}{2}|0\rangle - \frac{1}{2}|1\rangle$, and measure it with respect to Y.

a) Determine the probability that the measurement result is $+1$, knowing that $+1$ is the eigenvalue associated with the first eigenstate.

b) Determine the probability that the measurement result is -1, knowing that -1 is the eigenvalue associated with the second eigenstate.

13. Determine if the following density operators are mixed or pure states:

a) $\rho = \frac{1}{2}[|0\rangle\langle 0| + i|0\rangle\langle 1| - i|1\rangle\langle 0| + |1\rangle\langle 1|]$

b) $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{6}|0\rangle\langle 1| + \frac{1}{6}|1\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|]$

14. A system is in the state $|\psi\rangle = \frac{1}{\sqrt{3}}|u_1\rangle + i\sqrt{\frac{2}{3}}|u_2\rangle$, where $\{|u_1\rangle, |u_2\rangle\}$ constitute an orthonormal basis.

a) Write down the density operator.

b) Show that this operator has unit trace.

15. Given the following quantum state:

$$|\Psi\rangle = \frac{1}{\sqrt{3}}(|00> -\mathrm{i}|01> -|11\rangle)$$

a) Write the matrix of the density operator $\rho = |\Psi\rangle\langle\Psi|$.

b) Determine its eigenvalues

c) Is it a mixed or a pure state?

16. A source of photons emits a one-photon wave packet each second, but alternates between horizontal, vertical and diagonal polarizations. Assuming that these polarizations correspond to the qubits $|0\rangle$, $|1\rangle$ and $|+\rangle$, respectively:

a) Write the density matrix of this mixed state

b) Any mixed state can be represented by an ensemble of only two orthogonal pure states. What are these states for the density matrix obtained in a)? (*Hint: diagonalize the matrix*).

17. Consider the pure state $|\psi\rangle = a|0\rangle + be^{i\phi}|1\rangle$ with $a^2 + b^2 = 1$. In a quantum tomography reconstruction of the state $|\psi\rangle$, we need to measure it in a different basis. We perform the measurement first in the basis $\{|0\rangle, |1\rangle\}$ and then in the basis $\{|R\rangle, |L\rangle\}$, where $|R\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$ and $|L\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$. Knowing that the probabilities of measuring the state $|0\rangle$ is 0.25, the state $|1\rangle$ is 0.75 and the state $|R\rangle$ is 0.806, obtain the density matrix of the initial state $|\psi\rangle$.

18. In a quantum entanglement experiment, we want to create the state $|\beta_{00}\rangle$. The quantum tomography reconstruction of the state gives us:

$$\rho_{real} = \begin{pmatrix} 0.501 & 0 & 0 & 0.387 \\ 0.01 & 0.02 & 0 & 0.1 \\ 0 & 0.01 & 0.01 & 0.2 \\ 0.488 & 0.01 & 0.02 & 0.412 \end{pmatrix}$$

In order to check if the created state is the theoretical one, compute the fidelity. We will consider that the theoretical and real states are the same if the fidelity is greater than 66.7%.

19. In the 143-km teleportation experiment carried out in the Canary Islands, four different quantum qubits were teleported. These qubits were $|H\rangle$, $|V\rangle$, $|P\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle)$ and $|L\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle)$. Determine:

a) The *ideal* density matrices for each of the four teleported qubits.

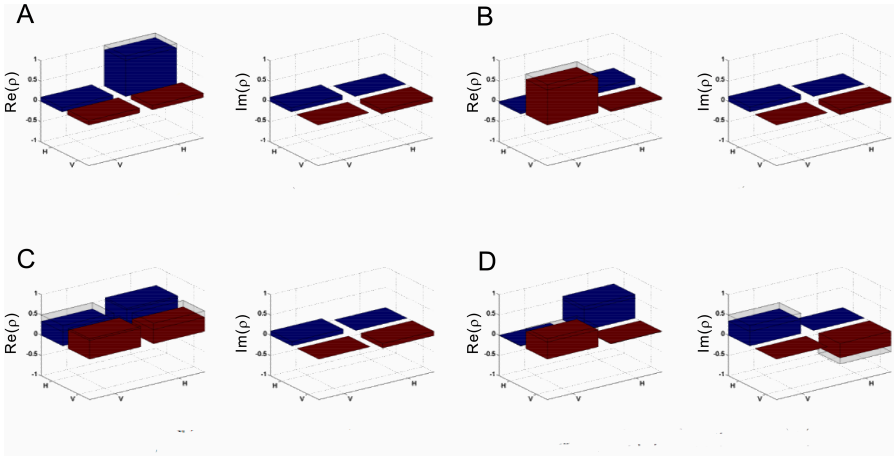


Fig. 4.2 State tomography results for the four quantum states used in the teleportation experiment of the Canary Islands. [Figure obtained from Ma, X., Herbst, T., Scheidl, T. et al. *Quantum teleportation across 143 kilometres using active feed-forward*. Nature **489**, 269–273 (2012).]

b) From the state tomography results shown in Figure **??**, estimate the measured density matrix for each of these teleported states.

c) Determine the fidelity $\mathcal{F}$ for each teleported state. What is the resulting average fidelity?

→ 5

Quantum Algorithms

– A detailed description of the Deutsch, Deutsch-Josza, Grover and Shor algorithms can be found in Chapters 19 & 20 of Desurvire, E. (2009), *Classical and Quantum Information Theory: An Introduction for the Telecom Scientist*, Cambridge: Cambridge University Press.[1]

– The quantum Fourier transform, QFT, is defined as a unitary operator acting on the state $|n\rangle$ of the N-orthonormal basis $\{|k\rangle\}_{k=0,\ldots,N-1} = \{|0\rangle, |1\rangle, \ldots, |N-1\rangle\}$, as in

$$QFT|n\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{ik\frac{2\pi n}{N}} |k\rangle.$$

– If $|\Psi\rangle$ is a qubit of dimension N, $|\Psi\rangle = \sum_{n=0}^{N-1} x_n |n\rangle$, then, the QFT of the qubit $|\Psi\rangle$ is

$$|\hat{\Psi}\rangle = QFT|\Psi\rangle = \frac{1}{\sqrt{N}} \sum_{n=0}^{N-1} \sum_{k=0}^{N-1} x_n e^{ik\frac{2\pi n}{N}} |k\rangle.$$

– The inverse of QFT is noted as QFT^{-1} and defined as:

$$|\Psi\rangle = QFT|\hat{\Psi}\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} \sum_{n=0}^{N-1} y_k e^{-in\frac{2\pi k}{N}} |n\rangle$$

– The QFT can also be implemented as a matrix $M_{N\times N}$, whose coefficients are $M_{nk} = M_{kn} = \exp(i2n\pi k/N)/\sqrt{N} \equiv \omega^{nk}/\sqrt{N}$ and $\omega \equiv e^{\frac{2\pi i}{N}}$.

[1] https://doi.org/10.1017/CBO9780511803758

– The matrix M takes the form of the Vandermonde matrix:

$$M = \frac{1}{\sqrt{N}} \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \dots & \omega^{N-1} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(N-1)} \\ 1 & \omega^3 & \omega^6 & \dots & \omega^{3(N-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{N-1} & \omega^{2(N-1)} & \dots & \omega^{(N-1)(N-1)} \end{pmatrix}$$

5.1. Solved Problems

1. Determine the quantum Fourier transform of the GHZ state:

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

Solution

The GHZ state corresponds to a 3-qubit system, i.e., $N = 2^3 = 8$. Using decimal notation: $|\Psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |7\rangle)$. We evaluate the QFT of each term separately:

$$\mathrm{Q}FT|0\rangle = \frac{1}{\sqrt{8}} \sum_{k=0}^{7} e^0 |k\rangle = \frac{1}{\sqrt{8}}(|0\rangle + \ldots + |7\rangle)$$

$$\begin{aligned} \mathrm{Q}FT|7\rangle = & \frac{1}{\sqrt{8}} \sum_{k=0}^{7} e^{ik\frac{7}{4}\pi} |k\rangle = \frac{1}{\sqrt{8}}(|0\rangle + e^{i\frac{7}{4}\pi}|1\rangle + e^{i\frac{14}{4}\pi}|2\rangle + \\ & + e^{i\frac{21}{4}\pi}|3\rangle + e^{i\frac{28}{4}\pi}|4\rangle + e^{i\frac{35}{4}\pi}|5\rangle + e^{i\frac{42}{4}\pi}|6\rangle + e^{i\frac{49}{4}\pi}|7\rangle) \end{aligned}$$

We evaluate the phase of each term:

$$\begin{aligned} e^{i\frac{7}{4}\pi} &= e^{i\frac{3}{4}\pi} = \frac{1}{\sqrt{2}}(1-i) & e^{i\frac{14}{4}\pi} &= e^{i\frac{3}{2}\pi} = -i \\ e^{i\frac{21}{4}\pi} &= e^{i\frac{5}{4}\pi} = \frac{-1}{\sqrt{2}}(1+i) & e^{i\frac{28}{4}\pi} &= e^{i\pi} = -1 \\ e^{i\frac{15}{4}\pi} &= e^{i\frac{3}{4}\pi} = \frac{1}{\sqrt{2}}(i-1) & e^{i\frac{42}{4}\pi} &= e^{i\frac{\pi}{2}} = 1 \\ e^{i\frac{49}{4}\pi} &= e^{i\frac{\pi}{4}} = \frac{1}{\sqrt{2}}(1+i) \end{aligned}$$

Finally, the QFT is the sum of both terms:

$$\begin{aligned}QFT|\Psi\rangle &= \frac{1}{\sqrt{2}}(QFT|0\rangle + QFT|7\rangle) = \\ &= \frac{1}{2}|0\rangle + \frac{1}{4\sqrt{2}}(\sqrt{2}+1-i)|1\rangle + \frac{1}{4}|(1-i)\rangle|2\rangle + \\ &+ \frac{1}{4\sqrt{2}}(\sqrt{2}-1-i)|3\rangle + \frac{1}{4\sqrt{2}}(\sqrt{2}+i-1)|5\rangle + \\ &+ \frac{1}{2}|6\rangle + \frac{1}{4\sqrt{2}}(\sqrt{2}+1+i)|7\rangle\end{aligned}$$

2. Consider an observable Ω, which defines an orthonormal basis of: N eigenstates $|x\rangle$ that are labeled $|0\rangle$, $|1\rangle$,...,$|N-1\rangle$; and of eigenvalues labeled λ_0, λ_1,...,λ_{N-1}. Consider two eigenvalues of interest, λ_{ω_1} and λ_{ω_2}, with the associated states $|\omega_1\rangle$ and $|\omega_2\rangle$, respectively. Determine:

a) The *oracle* operator U_ω and the second operator U_s, which constitute a Grover iteration: $G = U_s U_\omega$. Demonstrate that U_ω and U_s are unitary transformations.

b) Find the probability of obtaining one of the two eigenstates of interest after one Grover iteration.

Solution

a) If $|\omega_1\rangle$ and $|\omega_2\rangle$ are the eigenstates of interest, we can build the *oracle* operator as:

$$U_\omega = \mathbb{I} - 2|\omega_1\rangle\langle\omega_1| - 2|\omega_2\rangle\langle\omega_2|.$$

The second operator remains the same:

$$U_s = 2|s\rangle\langle s| - \mathbb{I},$$

where $|s\rangle$ is the superposition state $|s\rangle = \frac{1}{\sqrt{N}}\sum_{i=0}^{N}|\omega_i\rangle$.

It is straightforward to check that both operators are unitary:

$$\begin{aligned}U_\omega U_\omega^\dagger &= (\mathbb{I} - 2|\omega_1\rangle\langle\omega_1| - 2|\omega_2\rangle\langle\omega_2|)(\mathbb{I} - 2|\omega_1\rangle\langle\omega_1| - 2|\omega_2\rangle\langle\omega_2|) = \\ &= \ldots = \mathbb{I}\end{aligned}$$

and

$$U_s U_s^\dagger = (2|s\rangle\langle s| - \mathbb{I})(2|s\rangle\langle s| - \mathbb{I}) = \ldots = \mathbb{I}$$

b) One Grover iteration is defined as $U_G = U_s U_\omega$. When it is applied to the superposition state, we have

$$\begin{aligned}U_g|s\rangle = U_s U_\omega|s\rangle = U_s\left(|s\rangle - \frac{2}{\sqrt{N}}|\omega_1\rangle - \frac{2}{\sqrt{N}}|\omega_2\rangle\right) = \\ = \left(1 - \frac{8}{\sqrt{N}}\right)|s\rangle + \frac{2}{\sqrt{N}}|\omega_1\rangle + \frac{2}{\sqrt{N}}|\omega_2\rangle\end{aligned}$$

,

and the probabilities of obtaining the eigenstates of interest are

$$P(\omega_1) = |\langle \omega_1 | U_G | s \rangle|^2 = \left[\left(1 - \frac{8}{N} \right) \frac{1}{\sqrt{N}} + \frac{2}{\sqrt{N}} \right]^2 = \\ = \ldots = \frac{1}{N} \left(9 - \frac{24}{N} + \frac{64}{N^2} \right) \approx \frac{9}{N}$$

Analogously, $P(\omega_2) \approx 9/N$ and the probability of finding either of the two states is just $P(\omega_1 \, or \, \omega_2) \approx 18/N$.

3. Consider $x \in \{0, 2^n - 1\}$ and $f(x) : \{0, 2^n - 1\} \mapsto \{0, 2^n - 1\}$.

a) How can we implement the function $f(x)$ within a quantum circuit? Demonstrate that it is implemented with a unitary transformation.

b) Imagine that we have $f(x) = 2^x \, mod \, 5$ and $n = 3$, and we want to create a state that is a superposition of the x values, such that $f(x) = 4$. Draw a scheme of the quantum circuit and explain how you will perform this.

Solution

a) We first create a two-register system, $|x\,,\,y\,\rangle$. The first register is also called the query register, and the second one is the result register. Both registers are n-dimensional. The function $f(x)$ is implemented with the XOR operation on the second register:

$$U_f |x\,,\,y\,\rangle \mapsto |x\,,\,y \oplus f(x)\,\rangle.$$

By simply initializing the second register to zero, $|y\rangle = |0\rangle^{\otimes n}$, we obtain the values of $f(x)$ for the different values of the query:

$$U_f |x\,,\,0\,\rangle \mapsto |x\,,\,f(x)\,\rangle.$$

It is easy to check that U_f is a unitary transformation, given that

$$U_f U_f^\dagger |x\,,\,y\,\rangle = U_f^2 |x\,,\,y\,\rangle = U_f |x\,,\,y \oplus f(x)\,\rangle = \\ = |x\,,\,y \oplus f(x) \oplus f(x)\,\rangle = |x\,,\,y\rangle \Rightarrow U_f U_f^\dagger = I$$

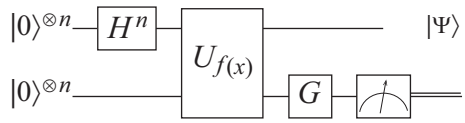
b) For this particular case, we have:

x	0	1	2	3	4	5	6	7
2^x	1	2	4	8	16	32	64	128
$f(x)$	1	2	4	3	1	2	4	3

So, the first register will be a superposition of all possible values of x: $|s\rangle = \frac{1}{\sqrt{8}} \sum_{x=0}^{7} |x\rangle$. After applying U_f, we will have in the second register a superposition of all possible values of $f(x)$. If we measure the second register, we have a probability of $\frac{1}{4}$ that it collapses into $f(x) = 4$ (see previous table), and then the first register will collapse into the desired state $|\psi\rangle = \frac{1}{\sqrt{2}}(|2\rangle + |6\rangle)|\hat{4}\rangle$. We can increase the probability that the system will collapse into $f(x) = 4$ by

applying a Grover iteration to the second register, thus defining our value of interest as 4, i.e., $|\omega\rangle = |4\rangle$.

The corresponding quantum circuit is shown below:



5.2. Short Questions

Indicate if the following sentences are **TRUE** or **FALSE**, and **JUSTIFY** your answers:

1. The Grover algorithm can be applied to find more than one qubit in a database.
2. We know that, after one Grover iteration, the probability of encountering the target qubit increases to $\frac{9}{N}$ if the number N of objects in the database is large enough. Then, for $N = 10^6$, we need $\approx N/9 \approx 1.1 \cdot 10^5$ Grover iterations to get a probability close to 1 for our target qubit.
3. The QFT of an entangled 2-qubit state is still an entangled state.
4. The quantum circuit that implements the QFT for three qubits requires two swap gates.

5.3. Exercises

5.3.1. Deutsch-Jozsa Algorithm

1. Consider a function with two inputs, such that $f(x) = 1$. Explicitly show that the Deutsch-Josza algorithm works in this case by generating the vector $|y\rangle = |00\rangle$ as the final output.
2. Suppose that $f(00) = f(01) = 0$ and $f(10) = f(11) = 1$. Apply the Deutsch-Josza algorithm and show that at least one of the first two qubits ends up as a 1.
3. *a)* Find the eigenvalues and eigenvectors of the following matrix, where x can be 0 or 1:

$$A(x) = (1 - x)I_2 + xU_{NOT}.$$

b) Show that the unitary transform

$$U_f = |0f(0)\rangle\langle 00| + |0\overline{f(0)}\rangle\langle 01| + |1f(1)\rangle\langle 10| + |1\overline{f(1)}\rangle\langle 11|,$$

where $f : \{0,1\} \to \{0,1\}$ is a boolean function and $\overline{x}$ denotes the boolean negation of x, can be written as

$$U_f = |0\rangle\langle 0| \otimes A(f(0)) + |1\rangle\langle 1| \otimes A(f(1)).$$

c) Calculate

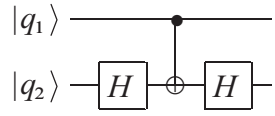
$$U_f(I_2 \otimes \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)).$$

Analyze the cases $f(0) = f(1)$ and $f(0) \neq f(1)$.

4. When, in the Deutsch algorithm, we consider U_f as a single-qubit operator, $\hat{U}_{f(x)}$, $\frac{|0\rangle - |1\rangle}{\sqrt{2}}$ is an eigenstate of $\hat{U}_{f(x)}$, whose associated eigenvalue gives us the answer to the Deutsch problem. Now, let us suppose that we are unable to prepare this eigenstate directly. Show that if we instead input $|0\rangle$ to the target qubit and otherwise run the same algorithm, we get an algorithm that gives the correct answer with probability $\frac{3}{4}$ (note that this also works if we input $|1\rangle$ to the second qubit). In addition, show that with probability $\frac{1}{2}$ we know for certain that the algorithm has produced the correct answer.
(*Hint: write* $|0\rangle$ *in the basis of eigenvectors of* $\hat{U}_{f(x)}$)

5.3.2. Grover Algorithm

5. Consider the quantum circuit in the figure below. This quantum circuit can implement the oracle operator of Grover's algorithm for a certain target qubit, $|\omega\rangle$.

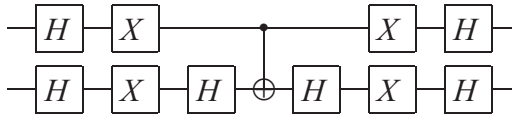


a) Determine the matrix associated with it.

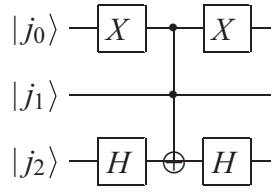
b) Find the target qubit $|\omega\rangle$ and demonstrate that, for this particular qubit, the quantum circuit acts as an oracle operator.

c) Find a simplified version of the previous quantum circuit (i.e., an equivalent quantum circuit with a smaller number of gates).

d) Finally, demonstrate that the following quantum circuit acts as the Grover diffusion operator $U_s = |s\rangle\langle s| - I$, where $|s\rangle$ is the superposition state $|s\rangle = \frac{1}{2}\sum_{x=0}^{3}|x\rangle$.



6. Consider the following 3-qubit quantum circuit that is acting as an oracle operator for a certain $|\omega\rangle$ qubit.



a) Determine $|\omega\rangle$.

b) By using as many quantum gates as needed, find a quantum circuit that acts as 3-qubit Grover diffusion operator.

7. For Grover's search algorithm, assume that we have M target states out of N total states, so the black box O takes

$$\begin{aligned} O|x\rangle &= -|x\rangle \qquad \text{if } x \text{ is a target state, and} \\ O|x\rangle &= |x\rangle \qquad \text{otherwise.} \end{aligned}$$

Suppose we find a target state with probability 1 after one iteration of the algorithm. What can you say about the ratio M/N?

8. Perform two iterations of Grover's algorithm on a system with $N = 4$ and solution indexed by $x = 0$. The state you will need to start with is $|\psi\rangle = \frac{1}{2}(|0\rangle+|1\rangle+|2\rangle+|3\rangle)$. Comment on the result.

9. Consider a system of $N = 2^3 = 8$ states. The states are equiprobable and we are searching for two of them, x_1 and x_2.

a) Find the probability of obtaining x_1 or x_2 after one Grover iteration.

b) Find the number of iterations that maximize the probability of obtaining x_1 or x_2. Also write out the quantum state after this number of iterations.

5.3.3. Quantum Fourier Transform and Shor Algorithm

10. Show that the QFT transformation is unitary. It is defined by

$$|y_n\rangle = \frac{1}{\sqrt{N}} \sum_{k=0}^{N-1} e^{ik\frac{2\pi n}{N}} |x_k\rangle,$$

and $|x_k\rangle_{k=0\ldots N-1}$ is an orthonormal basis.

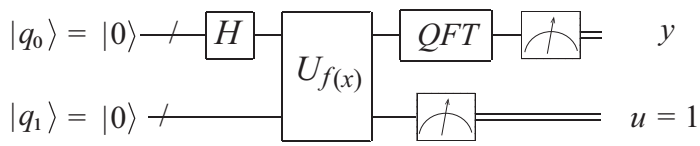
11. Demonstrate that, for $N = 2$, the QFT reduces to the Hadamard transformation.

12. Calculate the quantum Fourier transform of the qubit

$$|\psi\rangle = \frac{1}{\sqrt{14}} \left(|0\rangle + 2i|1\rangle + 3|2\rangle\right).$$

13. Calculate the QFT of the $|\beta_{01}\rangle$ EPR-Bell state. Is it still an entangled state?

14. We want to obtain the period of the function $f(x) = x \mod 2$ by using the 3-qubit quantum circuit in the figure below. Determine the possible values of the register y knowing that u has collapsed into the value 1.



15. For the following combinations of a, N, apply Shor's algorithm to find the factors of N. If the algorithm fails, clearly identify at which stage the failure occurs. Assume that each register has 15 qubits.

a) $N = 15, a = 7$

b) $N = 91, a = 4$

c) $N = 21, a = 5$

16. Consider the function $f(x) = 3^x \, mod \, 5$ and a system of 3 qubits.

a) How can we implement this function within a quantum circuit? Demonstrate that the function is implemented with a unitary transformation.

b) Now, we want the system to collapse into those values for which $f(x) = 4$. How can we achieve this? Describe the process.

17. We want to evaluate the period of the function $f(x) = 2^x \, mod \, 5$ by means of a quantum circuit. Consider the initial state as two 3-qubit registers, $|\Psi_1\rangle = |0\rangle^{\otimes n}|0\rangle^{\otimes n}$ of size $n = 3$.

a) Draw a scheme of the quantum circuit that we need in order to find the period of the previous function.

b) We obtain a value of 4 when we measure the second register. Write down the quantum state of the first register after this measurement.

c) Finally, determine the pre-measurement state of the first register.

Quantum Processors

6.1. Definitions

– *Jones vector.* When a beam of polarized light propagates along the direction $\hat{\mathbf{z}}$, the associated electric field oscillates in the plane xy. Its polarization may be characterized by the Jones vector $e^{i\Phi}\begin{pmatrix} E_{0x}e^{i\phi_x} \\ E_{0y}e^{i\phi_y} \end{pmatrix}$, where $\Phi = \omega t - kz$ is the global phase of the wave, and ϕ_x and ϕ_y are the phases in the $\hat{\mathbf{x}}$ and $\hat{\mathbf{y}}$ direction, respectively.

– If $\phi_x = \phi_y$, we have *linear polarization* while, if $\phi_x - \phi_y = \pm\pi/2$, we have *circular polarization*.

– The polarization of a photon (or, equivalently, the possible states of a qubit) may be described in terms of the two linearly-polarized states:

$$\{|H\rangle, |V\rangle\} = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}.$$

Alternatively, one may use the basis of circular states:

$$\{|R\rangle, |L\rangle\} = \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix} \right\},$$

or the Hadamard basis[1]:

$$\{|+\rangle, |-\rangle\} = \left\{ \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\}.$$

– Optical elements can be represented by a 2×2 matrix. For instance, a *linear polarizer* with transmission angle θ with respect to the horizontal axis is represented by

$$P = \begin{pmatrix} \cos^2\theta & \sin\theta\cos\theta \\ \sin\theta\cos\theta & \sin^2\theta \end{pmatrix}.$$

[1] These states are also called diagonal and antidiagonal, $\{|D\rangle, |A\rangle\}$, or plus and minus $\{|P\rangle, |M\rangle\}$, respectively.

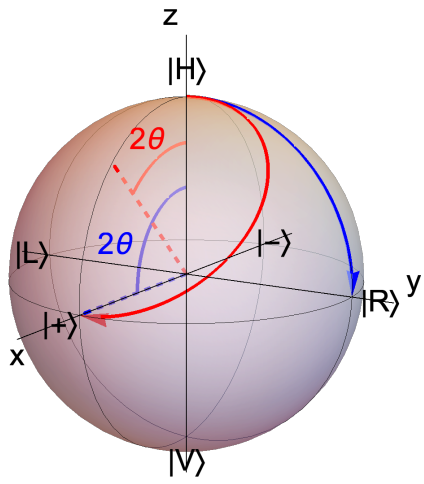


Fig. 6.1 Effect of an HWP (red) and a QWP (blue) on the Bloch sphere for a physical angle θ of the FA with respect to the horizontal direction. In the example represented: $\theta = 22.5°$ for the HWP and $\theta = 45°$ for the QWP.

– *Malus's law.* When a beam of polarized light passes through a polarizer, the intensity after the polarizer will be $I = I_0 \cos^2\theta$, where I_0 is the intensity of the beam before hitting the polarizer, and θ is the angle between the polarization direction of the incoming light and the transmission angle of the polarizer.

– A *phase retarder* or *wave-plate* is a slab of birefringent material with two characteristic refractive indices, which induces different phase delays ϵ_f and ϵ_s in the FA (fast-axis) and SA (slow-axis), respectively. By introducing $\delta = \epsilon_s - \epsilon_f$, the corresponding matrix (choosing the FA as horizontal) is

$$M_\delta = \begin{pmatrix} e^{-i\delta/2} & 0 \\ 0 & e^{i\delta/2} \end{pmatrix}.$$

– Two cases are especially important: (a) if $|\delta| = \pi/2$, we call it a *quarter-wave plate* (QWP); and (b) if $|\delta| = \pi$, we call it a *half-wave plate* (HWP).

– If the fast axis of the wave plate is twisted by an angle θ with respect to the horizontal, the Jones matrix for the wave plate is

$$M_\delta(\theta) = R(\theta) M_\delta R(-\theta),$$

where $R(\theta) = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ is a rotation matrix. The general expression for the Jones matrix of a wave-plate is therefore

$$M_\delta(\theta) = \begin{pmatrix} \cos(\delta/2) - i\sin(\delta/2)\cos(2\theta) & -i\sin(\delta/2)\sin(2\theta) \\ -i\sin(\delta/2)\sin(2\theta) & \cos(\delta/2) + i\sin(\delta/2)\cos(2\theta) \end{pmatrix}.$$

– In an ion trap[2] with j ions, a qubit $|q\rangle$ is defined as $|q\rangle = |q_1 q_2 ... q_j\rangle|n\rangle$, where the ket $|n\rangle$ represents the phononic state (or vibrational mode) of the j ions. Its possible values are $n = 0, 1, 2, 3....$

[2] A gentle introduction to ion-trap quantum computers can be found in: Michael H. Holzscheiter, Ion-Trap Quantum Computation, Los Alamos Science No. 27, 2002; https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-02-3932

Pulse Length	Initial State	Final State
2π	$\|0\rangle$	$-\|0\rangle$
	$\|1\rangle$	$-\|1\rangle$
π	$\|0\rangle$	$\|1\rangle$
	$\|1\rangle$	$\|0\rangle$
$\pi/2$	$\|0\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$
	$\|1\rangle$	$\frac{1}{\sqrt{2}}(\|0\rangle + \|1\rangle)$

– Each ion in an ion trap can be in the ground state, $|0\rangle$, or the excited state, $|1\rangle$.

– To change the state of each ion, Rabi oscillations are applied to induce coupling by rotation: $R(\theta, \phi)$, where $\theta = \Omega\tau$ is the pulse area, Ω the Rabi frequency, τ the pulse length and ϕ the phase of the laser field.

– Different Rabi oscillation pulses are then used according to the table below.

– To change the phononic state, a particular frequency of the laser should be used:

Frequency		State Change
carrier	ω_c	$\|0\rangle\|n\rangle \longleftrightarrow \|1\rangle\|n\rangle$
red	$\omega_c - \omega_z$	$\|0\rangle\|n\rangle \longleftrightarrow \|1\rangle\|n-1\rangle$
blue	$\omega_c + \omega_z$	$\|0\rangle\|n\rangle \longleftrightarrow \|1\rangle\|n+1\rangle$

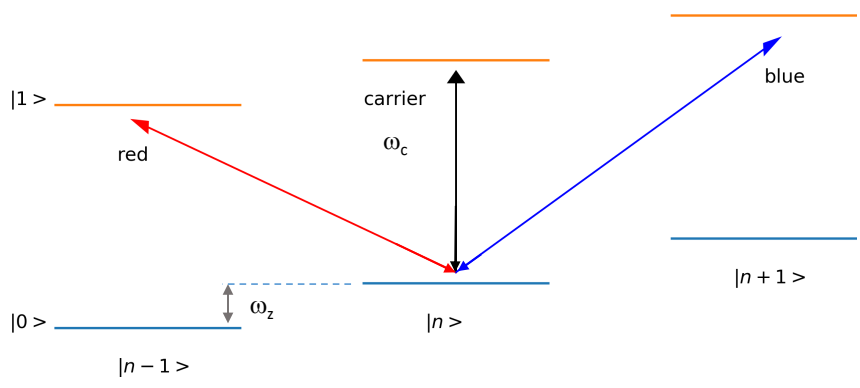


Fig. 6.2
Ion trap carrier ω_c and sideband $\omega_c \pm \omega_z$ frequencies. In the general case: $\omega_c << \omega_z$.

6.2. Solved problems

1. Demonstrate that, if the incoming light is unpolarized and with intensity I_0, the outgoing intensity after the polarizer will be $I_0/2$.

Solution

We need only to average Malus' law over all angles θ:

$$I = I_0 \frac{1}{2\pi} \int_0^{2\pi} \mathrm{d}\theta \cos^2\theta = I_0/2$$

2. A beam of unpolarized light with intensity I_0 goes through a series of polarizers P_i, whose axes are aligned, respectively, along the directions $\theta_1 = \pi/3$, $\theta_2 = 2\pi/3$, $\theta_3 = 3\pi/3$, and $\theta_4 = 4\pi/3$.

a) Determine the final intensity I_4 when all polarizers (1-2-3-4) are present.

b) Determine the final intensity I_2 when only polarizers 1 and 4 are present.

Solution

a) The intensity of unpolarized light that goes through one polarizer drops by a factor of 1/2. Subsequently, it will drop by another factor of $\cos(\pi/3)^2 = 1/4$ per polarizer. As such, $\mathrm{I}_4 = \frac{1}{4} \cdot \frac{1}{4} \cdot \frac{1}{4} \cdot \frac{1}{2} \cdot I_0 = \frac{I_0}{128}$.

b) The axes of polarizers 1 and 4 are parallel, such that light which has gone through P_1 will not be attenuated by P_4. As such, $I_2 = \frac{I_0}{2}$.

3. Find the matrix corresponding to an HWP with a physical angle of $\theta = 45°$. What is the effect when acting upon the linearly polarized photons $\{|H\rangle, |V\rangle\}$? To which quantum gate is this action equivalent?

Solution

An HWP has a retarded phase angle $\delta = \pi$, and knowing that $\theta = 45°$, we simply substitute these values in the general wave-plate matrix:

$$\mathrm{HWP}(45°) = M_{\delta=\pi}(\theta = 45°) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

When an HWP has an FA that forms an angle of $\theta = 45°$ with respect to the horizontal, then, aside from an irrelevant overall phase, it acts as an X gate in the linear polarization basis $\{|H\rangle, |V\rangle\}$:

$$|H\rangle \xrightarrow{\text{HWP } 45°} |V\rangle \xrightarrow{\text{HWP } 45°} |H\rangle.$$

4. Find the matrix corresponding to a QWP with a physical angle of $\theta = 45°$. What is the effect when it acts upon the linearly polarized photons $\{|H\rangle, |V\rangle\}$? To which quantum gate is this action equivalent?

Solution

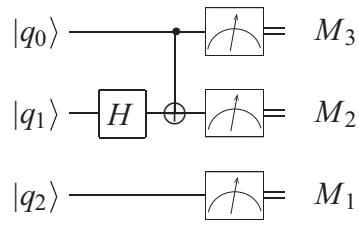
The same as in the previous example, but now with $\delta = \pi/2$ and $\theta = 45°$:

$$\text{QWP}(45°) = M_{\delta=\pi/2}(\theta = 45°) = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}.$$

A QWP with the same angle $\theta = 45°$ instead acts as a Hadamard gate, aside again from irrelevant overall phases, switching between linear and circular polarizations:

$$|H\rangle \xrightarrow{\text{QWP } 45°} |R\rangle \xrightarrow{\text{QWP } 45°} |V\rangle \xrightarrow{\text{QWP } 45°} |L\rangle \xrightarrow{\text{QWP } 45°} |H\rangle.$$

5. Consider the following quantum circuit. The polarization of qubits $|q_1\rangle$ and $|q_2\rangle$ is entangled as $|\phi\rangle = \frac{1}{\sqrt{2}}(|H\,H\rangle + |V\,V\rangle)$, and the measurements are made in the computational basis.



a) Resolve the quantum circuit for a general qubit $|q_0\rangle = \alpha|0\rangle + \beta|1\rangle$.

b) Use as many optical elements as necessary to draw a setup that implements the previous quantum circuit. You can consider both spatial and polarization modes.

c) Associate each of the measurement devices with each of the detectors in the setup.

Hint: *M_1 measures the third qubit $|q_2\rangle$. Possible values of M_1 are 0 or 1 if $|q_2\rangle$ is $|0\rangle$ or $|1\rangle$, respectively. If $M_1 = 0$, determine which detectors, D_X, light up in this case. Conduct the same analysis for $M_1 = 1$ and all the other measurement devices.*

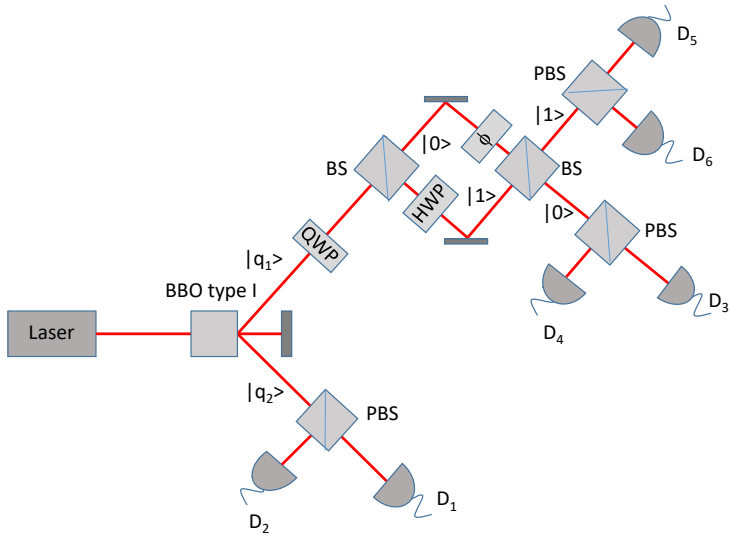
d) Determine the probabilities associated with each detector.

Hint: *Use the results obtained in point a).*

Solution

a) The shared entangled state $|\phi\rangle = \frac{1}{\sqrt{2}}(|H\,H\rangle + |V\,V\rangle)$ is equivalent to the Bell state $|\beta_{00}\rangle$. Thus, for a general qubit $|q_0\rangle = \alpha|0\rangle + \beta|1\rangle$, the initial state is $|\psi_0\rangle = |q_0\rangle \otimes |\beta_{00}\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle)$. After crossing the different gates of the quantum circuit, the pre-measurement state is $|\psi_{pre-m}\rangle = \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|001\rangle + \alpha|010\rangle - \alpha|011\rangle + \beta|100\rangle - \beta|101\rangle + \beta|110\rangle + \beta|111\rangle)$.

b) The setup is shown in the diagram below. A BBO type I crystal provides the required entanglement. The polarization state of these two photons corresponds to the qubits $|q_1\rangle$ and $|q_2\rangle$. A QWP oriented $45°$ in the $|q_1\rangle$ path acts as a Hadamard gate. The qubit $|q_0\rangle$ is implemented through the spatial mode by a Mach-Zehnder interferometer. The phase retarder ϕ provides the amplitudes α and β of $|q_0\rangle$, while a $45°$ HWP applied in path $|1\rangle$ to the polarization acts as a CNOT-gate.



c) Qubit $|q_2\rangle$ is measured by M_1, which corresponds to a polarization beam-splitter (PBS) and the detectors D_1 and D_2. The possible values of M_1 (0 or 1) are related to the polarization states of the second photon. Thus, horizontally polarized photons will reach D_1 and correspond to $M_1 = 0$, while vertically polarized photons will be detected in D_2, therefore implying $M_1 = 1$. Now, $|q_1\rangle$, which is associated with the first photon, is split into two branches, depending on the path mode of $|q_0\rangle$. Taking that into account, horizontally polarized photons can be measured in detectors D_3 or D_5, corresponding to $M_2 = 0$, while vertical ones will be detected in D_4 or D_6, implying $M_2 = 1$. Finally, $|q_0\rangle$ is implemented through a spatial model. In this case, path $|0\rangle$ is detected by D_3 or D_4, implying $M_3 = 0$, while path $|1\rangle$ is measured by D_5 or D_6.

d) In the following table we summarize which qubit state is measured by each detector and their probabilities, which were deduced from the pre-measurement state obtained in question *a)*.

heightDetector	Qubit State	Probability
D_1	$\|xy0\rangle$	$1/2$
D_2	$\|xy1\rangle$	$1/2$
D_3	$\|00x\rangle$	$\alpha^2/2$
D_4	$\|01x\rangle$	$\alpha^2/2$
D_5	$\|10x\rangle$	$\beta^2/2$
D_6	$\|11x\rangle$	$\beta^2/2$

6. We have a 2-qubit system in an ion trap in the initial state $|00\rangle|2\rangle$. Describe the state of the system if we apply to the first qubit a $\pi/2$ pulse from a laser tuned to the red sideband, followed by a π pulse from the same laser to the second qubit. Finally, we apply to the first qubit a 2π pulse, also tuned to the red sideband.

Solution

We begin with the state in $|00\rangle|2\rangle$. If we apply to the first qubit a $\pi/2$ pulse in the red sideband, we will get a superposition of the initial state and the final state. The final state has the first qubit excited and the vibrational mode will be decreased by one, as we are in the red sideband. Thus, after applying the pulse, the system will be in the state:

$$\frac{1}{\sqrt{2}}(|00\rangle|2\rangle + |10\rangle|1\rangle).$$

Now, if we apply to the second qubit a π pulse in the red sideband, the second qubit will get excited and the vibrational mode will decrease by one. As it is a π pulse, we do not obtain any extra superposition:

$$\frac{1}{\sqrt{2}}(|01\rangle|1\rangle + |11\rangle|0\rangle).$$

Finally, the action of the 2π pulse is to change the sign of the first qubit, but because the laser is tuned to the red sideband, we cannot lower the vibrational state of the second part of the above superposition and instead change only the sign of the first one. Thus, the solution is:

$$\frac{1}{\sqrt{2}}(-|01\rangle|0\rangle + |11\rangle|0\rangle).$$

6.3. Short Questions

Indicate if the following sentences are **TRUE** or **FALSE**, and **JUSTIFY** your answers:

1. We have two quantum computers. Model A has a decoherence time of $\tau_{\mathrm{Q}} = 10^{-2}$ s and an operational time of $\tau_{OP} = 10^{-3}$ s, while model B has a decoherence time of $\tau_{\mathrm{Q}} = 10^{-5}$ s and an operational time of $\tau_{OP} = 10^{-9}$ s. Model B represents a better quantum computer.

2. A beam of vertically polarized photons with an intensity I_0 goes through two polarizing filters. The first is vertically aligned and the second is at $45°$ with respect to the first one. The transmitted intensity is $I_t = I_0/\sqrt{2}$.

3. A beam of vertically polarized photons goes through a polarizing filter inclined at $60°$ with respect to the horizontal. Denote by $|0\rangle$ and $|1\rangle$ the horizontal and vertical polarizations, respectively. The resulting qubit is $|q\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|1\rangle$.

4. Entanglement may be created only between pairs of identical photons.

5. An HWP with a physical angle $\alpha = 22.5°$ turns horizontally polarized photons into diagonally polarized ones, and vertically polarized photons into anti-diagonally polarized ones.

6. Regardless of the angle α, if we twice apply an HWP to an arbitrary polarized initial state, we obtain the same initial state.

7. A π-pulse tuned to a carrier frequency always changes the qubit state, but a π-pulse tuned to sideband frequencies might not.

8. A red-detuned pulse, regardless of the pulse length, always reduces the phonon state from $|n\rangle$ to $|n-1\rangle$.

9. A π-pulse detuned to blue is applied to the initial state $|00\rangle|0\rangle$, resulting in $\frac{1}{\sqrt{2}}\left(|00\rangle|0\rangle + |10\rangle|1\rangle\right)$.

6.4. Exercises

6.4.1. Optical elements

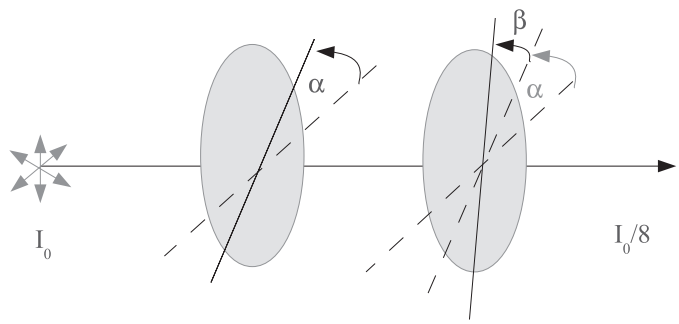
1. Non-polarized light with an intensity of $5\ \mathrm{W/m^2}$ incides on two polarizing films, with the transmission axis forming an angle of $30°$ between them. What is the intensity of the light transmitted by the second film?

2. A beam of polarized light in the horizontal direction arrives at a polarizing film. Only $25\,\%$ of the intensity of the incident light is transmitted through the film. What is the angle between the transmission axis of the film and the horizontal axis?

3. If two polarizing films have their transmission axes crossed, there is no transmitted light. If a third film is inserted between the two such that its transmission axis forms an angle θ with the first film, calculate the intensity of the transmitted light as a function of θ. Demonstrate that the transmitted intensity is maximum when $\theta = 45°$.

4. A $5\,\mathrm{mW}$ laser beam with vertical polarization impinges on two polarizing films. The first one is oriented with its transmission axis in the vertical direction. The transmission axis of the second polarizer forms an angle of $27°$ with respect to the axis of the first film. What is the power of the transmitted beam after the second film?

5. Consider a beam of unpolarized light. The beam crosses two polarizing filters as shown in the figure below. The first one forms an angle α with respect to the horizontal plane, while the second one forms an angle β with respect to the first polarizer. Determine α and β so that the final intensity is reduced to one eighth of the incident intensity.



6. Demonstrate that the superposition of two E-fields with opposite circular polarizations (i.e., $E^+ \pm E^-$) yields linearly polarized E-fields.

7. Polarized photons are described by the two E-field components, $E = e^{\imath\phi} \begin{pmatrix} E_1 \\ E_2 \end{pmatrix} e^{\imath\omega t}$, where $\omega = 2\pi\nu$ is the oscillation frequency and ϕ the phase. Knowing that a quarter-wave plate (QWP) is oriented at $45°$ with respect to the incident polarization, this introduces a phase delay of $\Delta\phi = \pi/2$ and the output E-field becomes

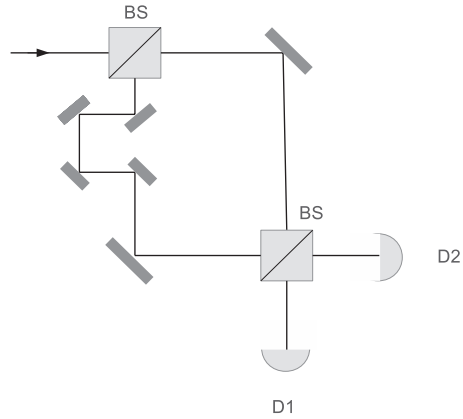
$$E = e^{\imath\phi} \frac{1}{\sqrt{2}} \begin{pmatrix} E_1 + E_2 \\ e^{\imath\Delta\phi}(E_1 - E_2) \end{pmatrix} e^{\imath\omega t}$$

Demonstrate that after traversing the QWP:

a) An incident horizontally (vertically) polarized photon becomes a right- (left-) circularly polarized photon.

b) If horizontal and vertical photons represent the quantum states $|0\rangle$ and $|1\rangle$, respectively, find the matrix that represents the QWP. Which matrix is it?

8. Consider the following unbalanced Mach-Zehnder interferometer.



The beam splitter is represented by the matrix $BS = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$, while the different lengths of the arms introduce a phase shift given by $S_\phi = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{pmatrix}$. Evaluate the probabilities for the detectors D_1 and D_2.

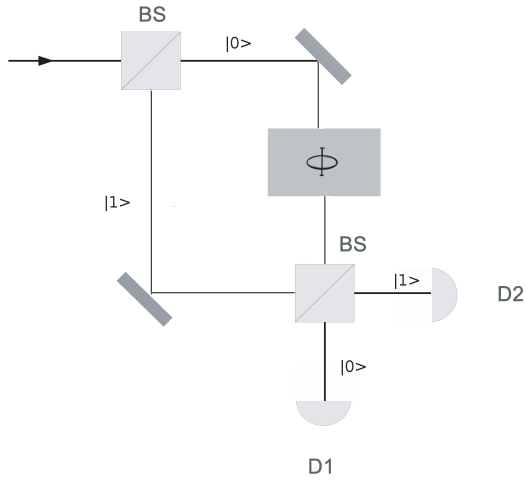
9. Consider the following unbalanced Mach-Zehnder interferometer.

The beam splitter is represented by the matrix $BS = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}$, while the different length of the arms introduce a phase shift, $e^{\mathrm{i}\phi}$, given by the retarder located at arm "$|0\rangle$".

a) Write the matrix that represents the retarder.

b) Evaluate the probabilities for the detectors D_1 and D_2.

c) Determine the values of ϕ for creating the qubits $|0\rangle$ and $|+\rangle$.

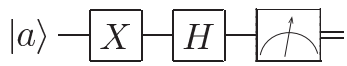


6.4.2. Optical Setups

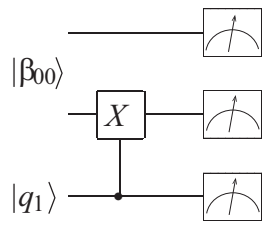
10. Consider a beam of photons in the polarized rotational states $|+\rangle$ and $|-\rangle$. Using two SPD and optical elements (for example: QWP, HWP, PBS, BBO, etc.,) design a setup for measuring these photons. What will we obtain if some photons are erroneously in the horizontally linearly polarized state $|H\rangle$?

11. Draw the optical setup needed for implementing a two-qubit controlled-Hadamard gate.

12. Given the qubit $|a\rangle = \alpha|0\rangle + \beta|1\rangle$ design the following quantum circuit using QWP, HWP and PBS. The final measurement is made in the $\{|0\rangle, |1\rangle\}$ basis.



13. Consider the following quantum circuit:



a) Using optical elements, build the setup for the previous quantum circuit.

b) Determine the probabilities for each detector and the coincidences that are possible if $|q_1\rangle = |+\rangle$.

Ground-to-Satellite Quantum Teleportation

The teleportation of arbitrary unknown quantum states is a key goal for developing a global-scale quantum internet. In an early experiment[3] performed in 2012 between two ground-stations separated by 143-km in the Canary Islands, it was demonstrated that current quantum optical technology is capable of achieving teleportation. In a more recent experiment performed in 2017 by a group of researchers from the University of Science and Technology of China and by the Chinese Academy of Science, it was demonstrated that it is also possible to teleport the information of single qubits between a ground-station and a low-Earth-orbit (LEO) satellite.

The ground-station was located in Ngari (Tibet), while the LEO satellite named Micius (as part of the Quantum Experiments at Space Scale) was launched by China to carry out different quantum experiments. Micius is in a sun-synchronous LEO at an altitude of 500 km, which established a distance of between 500–1400 km to the ground-station during the experiment. A variety of difficult technical challenges had to be faced, such as the use of: a compact ultrabright source of entangled photons; a narrow beam divergence laser; high-bandwidth; and high-accuracy data acquisition; and pointing and tracking systems. All of these had to be overcome before successfully achieving uplink communication with the satellite.

In the teleportation experiment, six different initial photon states were used: $|H\rangle, |V\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle), |R\rangle = \frac{1}{\sqrt{2}}(|H\rangle + i|V\rangle)$ and $|L\rangle = \frac{1}{\sqrt{2}}(|H\rangle - i|V\rangle)$. The experiment was successful, even though the attenuation of the communications channel was estimated to have been between 41-52 dB, mainly due to atmospheric turbulence close to the ground. An average fidelity of $\mathcal{F} = 0.80 \pm 0.01$ was achieved, thus demonstrating that quantum teleportation via satellite communication is feasible.

Exercises

a) The experiment used an ultraviolet 390 nm wavelength Ti:sapphire laser and sent a pulse width of 160 fs at a repetition rate of 80 MHz through two bismuth borate (BiBO) crystals to generate entangled photons. A photon count rate of $5.7 \times 10^5\ \mathrm{s}^{-1}$ was estimated to have left the transmitter. Give an estimate of the count rate reaching the satellite.

b) Draw a basic optical setup for creating the six different initial polarized states used in the experiment. Compare your setup with the one applied in the experiment, which can be found in Figure 1 from Ren et al. (2017).

[1] Ren, J., Xu, P., Yong, H. et al. Ground-to-satellite quantum teleportation. Nature 549, 70–73 (2017). https://doi.org/10.1038/nature23675

6.4.3. Ion Trap Quantum Computing

14. Explain how to obtain the Bell state β_{00} of two qubits in an ion trap system if the initial state is $|00\rangle|0\rangle$.

15. An ion trap with two qubits is initially in the state $|00\rangle|0\rangle$. We have a laser tuned to the blue sideband and use it to apply a π pulse on the first qubit and, later, a $\pi/2$ pulse on the second qubit. What is the final state of the system?

16. An ion trap with two qubits is initially in the state $\frac{1}{\sqrt{2}}(|00\rangle|0\rangle + |00\rangle|1\rangle)$. With a laser tuned to the carrier sideband, we apply a $\pi/2$ pulse on the first qubit and, later, we change the tuning to the blue sideband and apply a π pulse on the second qubit. What is the final state of the system?

17. An ion trap with two qubits is initially in the state $\frac{1}{\sqrt{2}}(|00\rangle|1\rangle + |01\rangle|0\rangle)$. We have a laser tuned to the carrier sideband and use it to apply a π pulse on the first qubit and, later, we change the tuning to the red sideband and apply a $\pi/2$ pulse on the second qubit. What is the final state of the system?

18. In an ion-trap quantum computer, we have m qubits and a common vibrational state n, represented by:

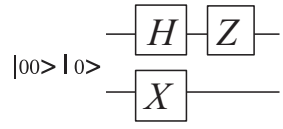
$$|\Psi\rangle = |q_1 q_2 \dots q_m\rangle|n\rangle.$$

a) Explain the sideband cooling process needed to obtain the fiducial state $|00\dots0\rangle|0\rangle$.

b) Imagine that we have the 2-qubit case $|00\rangle|0\rangle$. Define a sequence of pulses and frequencies to obtain the qubit state

$$|\Psi\rangle = \frac{1}{2}\left(|00\rangle + |01\rangle + |10\rangle + |11\rangle\right)|0\rangle.$$

19. Consider a system of two qubits based on two trapped ions and a common vibrational state. The system is initially in the zero state $|\Psi\rangle = |0\,0\rangle|0\rangle$. Define the series of pulses and frequencies that are needed to implement the following quantum circuit on the state $|\Psi\rangle$.



20. * The Cirac-Zoller controlled-not gate[4] is the implementation of the controlled-not gate using trapped ions and, together with the Pauli matrices, it is a key ingredient for building any universal set of gates. The Cirac-Zoller controlled-not gate is implemented in three steps:

[4] Cirac, J. I.; Zoller, P. (1995-05-15). Quantum Computations with Cold Trapped Ions. Physical Review Letters. **74**: 4091–4094.

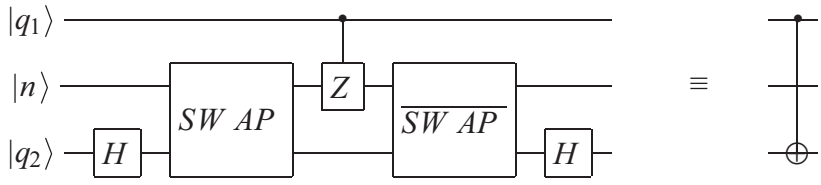
a) A controlled phase-flip gate $C_j(Z)$ is built with the help of an auxiliary qubit state $|2\rangle$. Consider the following: the frequency between the ground state $|0\rangle$ and the first excited state $|1\rangle$ is the carrier frequency ω_c; the frequency between states $|1\rangle$ and $|2\rangle$ are the auxiliary frequency ω_{aux}; and the frequency between phonon states is ω_z. Demonstrate that a 2π-pulse tuned to $\omega_{aux} - \omega_z$ is equivalent to a controlled Z-gate between the qubit and the phonon states.

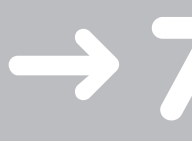
b) A swap gate, $SWAP_j$, is built with a laser tuned to the red frequency and applying a π-pulse and then a 2π-pulse with a laser tuned to the blue frequency. Demonstrate that, after preparing the phonon state in $|0\rangle$, the effect of the $SWAP_j$ gate is $|0\rangle|1\rangle \mapsto -|1\rangle|0\rangle$ and $|1\rangle|0\rangle \mapsto |0\rangle|1\rangle$. Also show that the inverse swap gate, $\overline{SWAP}_j$, acts as $|0\rangle|1\rangle \mapsto |1\rangle|0\rangle$ and $|1\rangle|0\rangle \mapsto -|0\rangle|1\rangle$.

c) Finally, demonstrate that the Cirac-Zoller CNOT gate acts as a CNOT gate between control qubit j and target k, defined by

$$CNOT_{jk} = H_k \cdot \overline{SWAP}_k \cdot C_j(Z) \cdot SWAP_k \cdot H_k,$$

when it is implemented through the following quantum circuit:





Quantum Communication

7.1. Quantum Protocol Definitions

– A *quantum key distribution* (QKD) session[1] consists of the following steps:

a) Authentication of the two parties (Alice and Bob).

b) Selection of a quantum protocol.

c) Construction of the *raw key*.

d) Construction of the *sifted key*, which after a process of checking and error correction will lead to the *reconciled key*[2].

e) Building the final *secret key* through a process of *private amplification*.

– The following notation is used:

basis			polarization 0	polarization 1
Z-basis	linear	0	$\|H\rangle \equiv \|0\rangle$	$\|\mathrm{V}\rangle \equiv \|1\rangle$
X-basis	circular	1	$\|R\rangle \equiv \frac{1}{\sqrt{2}}(\|0\rangle + i\|1\rangle)$	$\|L\rangle \equiv \frac{1}{\sqrt{2}}(\|0\rangle - i\|1\rangle)$

Strictly speaking, the eigenstates of the X matrix are $\{|+\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle \equiv \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$, while those of the Y matrix are $\{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$. These eigenstates can be associated with the diagonal $\{|D\rangle \equiv \frac{1}{\sqrt{2}}(|H\rangle + |V\rangle), |A\rangle \equiv$

[1] We recommend to the reader the report by Jane E. Nordholt, Richard J. Hughes, A New Face for Cryptography, Los Alamos Science No. 27, 2002; https://permalink.lanl.gov/object/tr?what=info:lanl-repo/lareport/LA-UR-02-3587

[2] In what follows, unless explicitly stated otherwise, we will assume no errors in the sifting process. Consequently, the sifted key will stand directly as the reconciled key.

$\frac{1}{\sqrt{2}}(|H\rangle - |V\rangle)\}$ and circular $\{|R\rangle, |L\rangle\}$ polarizations, respectively. For the quantum protocols explained here, it is irrelevant which of the two polarizations (diagonal or circular) is applied. We will generically call them X-basis and adopt the circular polarization as a reference.

– BB84 protocol[3]: an asymmetric protocol that uses four states of two orthogonal bases. The basic steps are as follows:

  a) Alice generates a random sequence $A = \{a_1, \ldots, a_N\}$ of N classical bits, which defines the basis to be used.

  b) Alice generates a second random sequence $A' = \{a'_1, \ldots, a'_N\}$, which defines the polarization of each photon.

  c) Alice transmits to Bob through a quantum channel the encoded photons.

  d) Bob generates a random sequence $B = \{b_1, \ldots, b_N\}$ for choosing the measurement basis.

  e) Bob measures the photons sent by Alice and obtains the sequence $B' = \{b'_1, \ldots, b'_N\}$.

  f) Alice and Bob communicate to each other their choice of bases (i.e., their sequences A and B) through a classical channel.

  g) In absence of errors in the sifting process, the reconciled key is composed of the bits in sequence A' (or equivalently B') which have been measured with coinciding bases (i.e., of the bits $\{a'_k\}$ $(= \{b'_k\})$ such that $\{a_k = b_k\}$. All other bits are discarded.

– B92 protocol[4]: an asymmetric protocol that uses two non-orthogonal states. The basic steps are as follows:

  a) Alice generates a random sequence $A = \{a_1, \ldots, a_N\}$ of N classical bits.

  b) For each a_k, Alice generates a photon with linear polarization $|0\rangle$ if $a_k = 0$, and with circular polarization $|+\rangle$ if $a_k = 1$.

  c) Alice transmits the encoded photons to Bob through a quantum channel.

  d) Bob generates a random sequence $B = \{b_1, \ldots, b_N\}$ for choosing the measurement basis.

  e) Bob measures the photons sent by Alice and obtains the sequence $B' = \{b'_1, \ldots, b'_N\}$.

  f) Bob communicates to Alice via a classical channel those bits whose measurement outcome was 1. Note that if $b'_k = 1$, then the basis used by Bob in the measurement process is different from the basis which Alice used to generate the photon.

  g) Alice's reconciled key is composed of those bits of A, $\{a_k\}$, for which Bob announced $b'_k = 1$. On the other hand, Bob's reconciled key is built from the subset of bits of the bitwise complement of B, $\{\bar{b}_k\} \equiv 1 - \{b_k\}$, for which $b'_k = 1$.

[3] Bennet, C.H, Brassard, G. Quantum Cryptography: Public key distribution and coin tossing. Proceedings of IEEE Int. Conf. on Computers, Systems and Signal Processing, pp.175-179 (1984).

[4] Bennet, C.H. Quantum cryptography using any two non orthogonal states, Phys. Rev. Lett. **68**, pp. 3121-3124 (1992).

– E91 or EPR protocol[5]: a symmetric protocol where the two parties share an entangled state. The basic steps are:

a) Alice and Bob share N copies of a two-photon entangled Bell state. For example: $|\beta_{00}\rangle$.

b) Alice and Bob produce two random sequences, $A = \{a_1, \ldots, a_N\}$ and $B = \{b_1, \ldots, b_N\}$, respectively, which determine the basis in which each party measures each photon.

c) Alice and Bob collect their measurements in the sequences A' and B', respectively.

d) Alice and Bob communicate to each other through a classical channel their choices of polarization basis (i.e., the sequences A and B).

e) The reconciled key is composed of those bits from A' and B' that fulfill $a_k = b_k$.

7.2. Solved Problems

1. The following table contains an example of the B92 protocol. The second and third rows correspond to Alice's actions, the remaining ones to Bob's. Entries that result from random choices are colored in red.

Bit number:	1	2	3	4	5	6	7	8
Alice's sequence a_k:	0	0	1	0	1	0	0	1
Photon's polarization:	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|+\rangle$	$\|0\rangle$	$\|0\rangle$	$\|+\rangle$
Bob's sequence b_k:	1	0	1	0	0	1	1	0
Bob's basis:	X	Z	X	Z	Z	X	X	Z
Possible values for b'_k:	0/1	0	0	0	0/1	0/1	0/1	0/1
Bob's measurement b'_k:	0	0	0	0	1	1	0	1

Perform the following:

a) Write down the conversation through a classical channel between Alice and Bob.

b) Determine the sifted, the reconciled and the raw keys.

c) Let us assume that Alice and Bob have initially agreed to apply the following private amplification sequence: $b_{i+j} = b_j \oplus b_{j+1}$, where $j = 1, 2, \ldots$ and i is the number of bits of the reconciled key. Determine a 1-byte secret key.

Solution

a) The conversation between Alice and Bob will be something like this:

Alice: Hi Bob.
Bob: Hi Alice.
Bob: I obtained 1 in the following bits: 5^{th}, 6^{th} *and* 8^{th}.
Alice: OK Bob. Thanks. Bye.
Bob: Bye.

[5] Ekert, A. Quantum cryptography based on Bell's theorem. Phys. Rev. Lett. **67**, pp. 661-663 (1991)

b) Alice builds her sifted key with the 5^{th}, 6^{th} and 8^{th} bits from the A sequence. That is $K_{\text{sif}} = \{a_5, a_6, a_8\} = \{1, 0, 1\}$. Bob, on the other hand, forms his sifted key from the negated bits of his B sequence. That is $K_{\text{sif}} = \{\bar{b}_5, \bar{b}_6, \bar{b}_8\} = \{\bar{0}, \bar{1}, \bar{0}\} = \{1, 0, 1\}$. In absence of transmission and measurement errors, the reconciled key is equal to the sifted key. Obviously, both parties obtain the same 3-bit reconciled key, i.e., $K_{\text{rec}} = (101)$. The raw key in the B92 protocol case corresponds to the complete Alice A sequence, that is, $K_{\text{raw}} = (00101001)$.

c) By applying the private amplification sequence, we obtain the remaining bits up to a 1-byte sequence:

$$\begin{aligned} b_4 &= b_1 \oplus b_2 = 1 \oplus 0 = 1 \\ b_5 &= b_2 \oplus b_3 = 0 \oplus 1 = 1 \\ b_6 &= b_3 \oplus b_4 = 1 \oplus 1 = 0 \\ b_7 &= b_4 \oplus b_5 = 1 \oplus 1 = 0 \\ b_8 &= b_5 \oplus b_6 = 1 \oplus 0 = 1 \end{aligned}$$

Finally, the resulting secret key is $K_{\text{sec}} = (10111001)$.

7.3. Short Questions

Indicate if the following sentences are **TRUE** or **FALSE**, and **JUSTIFY** your answers:

1. For a certain length of the raw key, the reconciled key derived from the BB84 protocol is, on average, larger than the reconciled key obtained from the B92 protocol.

2. In the BB84 protocol, if Alice and Bob use different bases for, respectively, encoding and measuring the photons, then their results are always different.

3. In the B92 protocol, it is possible to use any two non-orthogonal states for encoding the key. In other words, provided that Bob is aware of the pair of photons that Alice is going to use, she can use the pair $\{|H\rangle, |R\rangle\}$ or any other pair of non-orthogonal polarized photons, like $\{|V\rangle, |L\rangle\}$ or $\{|H\rangle, |D\rangle\}$ or $\{|D\rangle, |R\rangle\}$.

4. In a QKD session, Alice and Bob use the E91 protocol and share the Bell state $|\beta_{00}\rangle$. Alice is the first to measure a certain photon, and she obtains 1 in the Z-basis. Bob also uses the Z-basis and, consequently, also obtains 1. If Bob had been the first to measure, both parties would have achieved the same result, that is, 1.

7.4. Exercises

7.4.1. RSA Cryptography

1. Use the Diffie-Hellman algorithm with $p = 3$ and $q = 19$ to encrypt the message $m = 42$.

2. Given n, find prime numbers p and q such that $n = p \times q$:

a) $n = 15$ [6]

b) $n = 4088459$ [7]

c) $n = 15226050279225333605356183781326374297180681149613806886579$
$08494580122963258952897654000350692006139$ [8]

d) $n = 12462036678171878406583504460810659043482037465167880575481$
$87888832896668011882108550360395702725087475098647684384586210 54$
$86553797025393057189121768431828636284694840530161441643046806 68$
$75699415246993185704183030512549594371372159029236099$ [9]

e) $n = 25195908475657893494027183240048398571429282126204032027777$
$13783604366202070759555626401852588078440691829064124951508218 92$
$98559149176184502808489120072844992687392807287776735971418347 27$
$02618963750149718246911650776133798590957000973304597488084284 01$
$79742910064245869181719511874612151517265463228221686998754918 24$
$22433637259085141865462043576798423387184774447920739934236584 82$
$38242811981638150106748104516603773060562016196762561338441436 03$
$83390441495263443219011465754445417842402092461651572335077870 77$
$49817125772467962926386356373289912154831438167899885040445364 02$
$35273819513786365643912120103971228221207203 57$[10]

7.4.2. BB84 Protocol

3. Consider the quantum key distribution protocol BB84. Alice creates the following 8-bit string:

$$|+\rangle|1\rangle|+\rangle|-\rangle|0\rangle|-\rangle|+\rangle|-\rangle.$$

Use a coin to randomly determine what basis Bob uses to measure each bit position and describe the resulting bit string that Alice and Bob keep.

4. An experimental quantum key distribution session is performed between the EETAC at Castelldefels and the ETSETB at Campus Nord. The BB84 protocol is used. EETAC generates two 1-byte pseudo-random sequences, $A = (a_1, a_2, \ldots, a_8)$ and $A' = (a'_1, a'_2, \ldots, a'_8)$, for the basis and the rotation state of the photons, respectively.

a) If $A = (01101001)$ and $A' = (11001010)$, determine the quantum state $|\Psi\rangle = |q_1\rangle \otimes \ldots \otimes |q_8\rangle$ that EETAC sends to ETSETB.

b) ETSETB generates a new sequence $B = (10101100)$ in order to choose its measurement basis. Write down a possible result that ETSETB can obtain.

[6] The first number to be factorized by the Shor algorithm. This was demonstrated in 2001 using an NMR (Nuclear Magnetic Resonance) quantum computer with 7 qubits.

[7] It is claimed that the largest candidate number factorized to date was achieved in 2018 using the IBM 5-qubit quantum computer.

[8] This is RSA-100, the first number on the RSA Factoring Challenge list, which was factorized in 1991. It can be factorized in 72 minutes on a 3.5 GHz Intel Core2 using the sieve algorithm.

[9] This is RSA-240, the last RSA number to be factorized to date. This occurred in November 2019, and the estimated CPU time for finding the factors is around 900 core-years on a 2.1 Ghz Intel Xeon Gold 6130 CPU.

[10] This is RSA-2048, the largest RSA number: 617 decimal digits (2,048 bits). If you are the first person to find the two factors, contact RSA Laboratories and you will be awarded $200,000.

c) EETAC and ETSETB make a phone call. Write down explicitly what information should be transmitted between them.

d) Determine the reconcilied key.

e) Using privacy amplification, obtain a 1-byte secret key.

f) Prior to EETAC sending the 1-byte qubit to ETSETB, a spy has used a sophisticated method to access sequence A. Is this information enough to obtain the secret key? Give reasons for the answer.

5. A Quantum Key Distribution session based on the BB84 protocol is established between Alice and Bob.

a) Considering that the laser produces an unpolarized beam, make a drawing of the optical elements needed for the setups used by Alice and by Bob.

Knowing that Alice sent the sequence of polarized photons *RRLHVHLR* and that Bob used the bases *XZXZZXXZ* to measure them, determine the following (while justifying all your answers):

b) The raw (initial) key.

c) The explicit conversation through a classical channel between Alice and Bob.

d) The reconciled key.

e) A 1-byte secret key.

6. Consider a BB84 quantum key distribution protocol between Alice and Bob. The meanings of the indices are the usual ones: 0 for Z, 1 for X, 0 for H, 1 for V, 0 for R and 1 for L.

a) Fill in the gaps of the following table:

Bit number	1	2	3	4	5	6	7	8
Alice's base sequence	0	...	1	...	...	0	...	1
Alice's polarization sequence	...	...	0	0	...	...	...	0
Photon polarization	V	V	...	H	L	...	V	...
Bob's base sequence	...	0	1	1	1	0	...	...
Bob's result	1	...	...	0	...	0	0	1

b) Explicitly write the conversation that should take place between Alice and Bob:
–Alice: Hi Bob.
–Bob: Hi Alice.
–Alice: ...
...

c) Find the raw, reconciled and secret keys.

d) Consider the existence of a certain BER (Bit error rate) during the transmission of the photons. Once Alice and Bob have obtained the secret key, is there any way to check that the two keys coincide? If yes, explain the process that Alice and Bob should follow.

Photon Number Splitting Attack and the SARG04 Protocol

From a theoretical point of view, the BB84 protocol has been proven to be secure. However, its technical implementation leaves some doors open to attacks. ne example would be when using the more common attenuated laser pulses rather than single-photon sources. In a case like this, an intruder, Eve, can keep one of the photons of the pulse in a quantum memory, then send to Bob the rest of the pulse and measure that photon later, when the basis is revealed. This attack is called photon number splitting (PNS) attack and will provide to Eve the same information that Bob has.

A robust generalization of the BB84 protocol called SARG04[11] has been introduced to avoid this vulnerability. In the SARG04 protocol, Alice does not reveal the basis of each photon to Bob as she does in the BB84. Instead, Alice informs Bob of one of the following four groups: $S_{++} = \{|0\rangle|+\rangle\}$, $S_{+-} = \{|0\rangle|-\rangle\}$, $S_{-+} = \{|1\rangle|+\rangle\}$ or $S_{--} = \{|1\rangle|-\rangle\}$. Alice selects one group which contains the photon she sent to Bob. For example, Alice generates the photon $|0\rangle$ of the Z-basis and tells Bob S_{++} (she could also use S_{+-}). If Bob uses the X-basis and obtains a $|-\rangle$, he can deduce that Alice's photon has been created in the Z-basis and, consequently, is a $|0\rangle$. Bob will tell Alice to keep the bit that corresponds to this basis. This way, Eve has neither a deterministic way to deduce which basis Alice used nor any idea of which bit she should keep. In general, Bob accepts or discards (D) a bit, according to the following table:

heightAlice group \ Bob qubit	$\|0\rangle$	$\|1\rangle$	$\|+\rangle$	$\|-\rangle$
S_{++}	D	1	D	0
S_{+-}	D	1	0	D
S_{-+}	1	D	D	0
S_{--}	1	D	0	D

Exercise: Alice generates the following 1-byte sequence: $\{|+\rangle, |+\rangle, |-\rangle, |1\rangle, |1\rangle, |0\rangle, |+\rangle, |1\rangle\}$. She sends this sequence through a quantum channel, then uses a classical channel to communicate to Bob the sequence of groups: $\{S_{-+}, S_{++}, S_{--}, S_{-+}, S_{--}, S_{+-}, S_{++}, S_{-+}\}$. Bob uses a random sequence to measure this and obtains $\{|0\rangle, |+\rangle, |1\rangle, |+\rangle, |+\rangle, |-\rangle, |0\rangle, |+\rangle\}$.

a) What is the reconciled key that Alice and Bob deduce?

b) Assuming that Eve has photons that are identical to Bob's, what information can she retrieve?

c) Calculate, on average and in noiseless conditions, the percentage of bits accepted and discarded with the SAGR04 protocol.

7.4.3. B92 protocol

7. Consider the quantum key distribution protocol B92. Alice creates the following 8-bit string:

$$|0\rangle|0\rangle|+\rangle|0\rangle|+\rangle|+\rangle|0\rangle|+\rangle$$

Use a coin to randomly determine what basis Bob uses to measure each bit position and describe the bit string that Alice and Bob keep as a result.

8. A quantum key distribution session is performed between A (a ground station) and B (a LEO satellite). The protocol B92 is used. A generates an 8-bit sequence $A = (a_1, \ldots, a_8)$, such that if $a_k = 0$ then $|\Psi\rangle = |0\rangle$, and if $a_k = 1$ then $|\Psi\rangle = |+\rangle$. B also generates a 1-byte sequence $A' = (a'_1, \ldots, a'_8)$, and chooses the Z-basis or X-basis depending on whether $a'_k = 0$ or 1.

a) Knowing that $A = (00101110)$ and $A' = (01100101)$, describe the steps required to construct the sifted key between the ground station and the satellite.

b) Assuming that the reconciled key is the same as the sifted key, describe how we can obtain a 1-byte secret key by a private amplification process.

9. In 2016 China launched the Quantum Experiments at Space Scale (QUESS) satellite. Among other experiments, QUESS is going to establish a Quantum Key Distribution session based on the B92 protocol between Beijing (Alice) and Vienna (Bob).

a) Fill in the gaps of the following table:

	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8
Beijing base	...	1	1	0	...	...	1	1
Vienna base	1	...	...	1	0	0	1	...
Possible results	0/1	0/1	0	...	...	0	...	...
One result	1	1	...	0	1	...	...	1

b) Determine the polarization of the photons that are used in this experiment.

c) Write down explicitly the conversation between Beijing and Vienna.

d) Determine the reconciled and the secret key.

7.4.4. E91 Protocol

10. Consider the EPR protocol (also called E91) with a shared Bell state: $|\psi\rangle = \frac{1}{\sqrt{2^8}}(|00\rangle + |11\rangle)^{\otimes 8}$. Alice creates the following sequence a_k:

$$00010001$$

If $a_k = 0$ ($a_k = 1$) the measurement is made in the Z (X) basis. Describe the resulting byte.

[11] Scarani, V., Acín, A., Ribordy, G. and Gisin, N. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations, Phys. Rev. Lett. **92**, 057901 (2004)

11. An experimental E91 quantum key distribution session is performed between EETAC and ICFO, sharing the following 1-byte entangled-qubit:

$$|\Psi\rangle = |\beta_{00}\rangle_1 \otimes |\beta_{00}\rangle_2 \otimes \cdots |\beta_{00}\rangle_8 = \frac{1}{\sqrt{2^8}}(|0\,0\rangle + |1\,1\rangle)^{\otimes 8}.$$

a) Demonstrate that

$$|\beta_{00}\rangle = \frac{|0\,0\rangle + |1\,1\rangle}{\sqrt{2}} = \frac{|+\,+\rangle + |-\,-\rangle}{\sqrt{2}}.$$

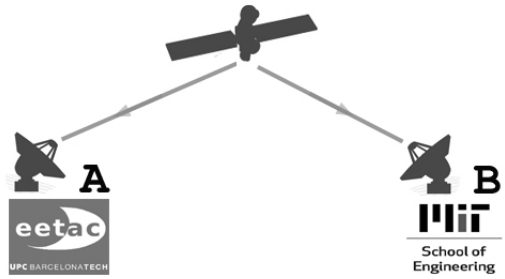
b) EETAC generates a 1-byte random sequence $A = (a_1, a_2, \ldots, a_8) = (01101010)$ and ICFO generates $A' = (a'_1, a'_2, \ldots, a'_8) = (00101011)$. They use the Z (X) basis when a 0 (1) is obtained. EETAC measures the entangled photons according to the sequence A. Write down a possible result that ICFO can obtain.

c) EETAC and ICFO make a phone call. Write down explicitly what information should be transmitted between them.

d) Determine the reconciled key.

e) Using private amplification, obtain a 1-byte secret key.

12. A quantum satellite C establishes a QKD session between A (the EETAC School in Castelldefels) and B (the MIT School of Engineering in Massachusetts). The protocol used is the E91 based on the Bell $|\beta_{00}\rangle$ state. The standard notations are used: $a_i = 0/1$ for Z/X-basis.



a) Draw the basic optical setup needed in A, B and C.

b) C uses a Titanium-sapphire laser of 404 nm wavelength and 700 mW power. The parametric down-conversion efficiency is $\nu = 10^{-12}$. For a pulse of 3 μs, determine how many photons reach A or B.

c) The EETAC School performs a 1-byte series of measurements following the sequence $A = (01110101)$ and obtaining the results $A' = (11101110)$. Some seconds later, the MIT School performs an analog series of measurements following the sequence $B = (10111001)$. Write down one possible result that can be obtained by MIT.

d) Write down explicitly the conversation between EETAC and MIT:
EETAC: Hello MIT.
MIT: Hello EETAC.
EETAC: ...
MIT: ...

e) Determine the raw key, the reconciled key, and the secret key.

Appendix A. Brief Summary of Linear Algebra

Definitions

– An operator A is said to be *Hermitian* if $A^\dagger = A$, where $A^\dagger$ is the conjugate transpose (or Hermitian conjugate) of A.

– Given a generic hermitian matrix M of size $n \times n$, its eigenvalues are given by the n solutions of the equation $\det(M - \lambda \mathbb{I}) = 0$, and the n eigenvectors are the solutions of $M|\lambda_i\rangle = \lambda_i|\lambda_i\rangle$.

– The tensor product of two vectors $|\psi_a\rangle = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ and $|\psi_b\rangle = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix}$ is the 4-vector given by $|\psi_a\rangle \otimes |\psi_b\rangle = \begin{pmatrix} a_1 b_1 \\ a_1 b_2 \\ a_2 b_1 \\ a_2 b_2 \end{pmatrix}$.

– Similarly, the tensor product of the two matrices $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ and $B = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ is the 4×4 matrix given by

$$A \otimes B = \left(\begin{array}{c|c} a_{11}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} & a_{12}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \\ \hline a_{21}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} & a_{22}\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \end{array}\right) = \begin{pmatrix} a_{11}b_{11} & \dots & \dots & a_{12}b_{12} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ a_{21}b_{21} & \dots & \dots & a_{22}b_{22} \end{pmatrix}.$$

Short Questions

Indicate if the following sentences are **TRUE** or **FALSE**, and **JUSTIFY** your answers:

1. The state of three qubits is fully described by a vector with 4 complex entries.
2. The tensor product of a 4×4 matrix multiplied by a 2×2 matrix is a 8×8 matrix.
3. If A is Hermitian and B is the inverse matrix of A, then B is also Hermitian.
4. The tensor product of two matrices (for instance, Pauli X and Z matrices) is not commutative, that is: $X \otimes Z \neq Z \otimes X$.

Exercises

Probability

1. Consider the first 25 digits in the decimal expansion of e $(2, 7, 1, 8, 2, 8, ...)$.
   a) What are the probabilities of obtaining each of the 10 digits if you select one number at random from this set?
   b) What is the most probable digit, the median digit and the average value?
   c) Find the standard deviation for this distribution.
2. Within a one-dimensional box of length L is a classical particle that can move freely between 0 and L. It has a probability distribution function $P(x) = 1/L$. Using this expression, demonstrate that $\langle x \rangle = L/2$ and $\langle x^2 \rangle = L^2/3$.
3. Consider a probability distribution that follows the Gaussian distribution $g(x) = Ce^{-\kappa(x-c)^2}$, where C, c and κ are constants.
   a) Determine C.
   b) Find $\langle x \rangle$, $\langle x^2 \rangle$, and σ.
   c) Draw the graph of $g(x)$.

Matrices and Vectors

4. Given the two matrices

$$A = \begin{pmatrix} -3 & -1 & 2i \\ 5 & -2 & 1 \\ i & 2i & 4 \end{pmatrix}, \quad B = \begin{pmatrix} -2i & i & 0 \\ 30 & 3 & 1 \\ -i & 2i & 0 \end{pmatrix},$$

compute *a)* $A + B$; *b)* AB; *c)* the commutator $[A, B] = AB - BA$; *d)* the transpose $\tilde{A}$; *e)* the complex conjugate A^*; *f)* the adjoint $A^\dagger = \tilde{A}^*$; *g)* the trace $\mathrm{Tr}(B)$; *h)* the determinant $\det(B)$; and *i)* the inverse B^{-1}. Check that $BB^{-1} = \mathbb{I}$.

5. Using the square matrices in Problem 4 and the column matrices

$$a = \begin{pmatrix} 2 \\ i \\ i \end{pmatrix}, \quad b = \begin{pmatrix} 1 \\ (1+i) \\ -1 \end{pmatrix},$$

find *a*) Aa; *b)* $a^\dagger b$; *c)* $\tilde{a}Bb$; and *d)* $ab^\dagger$.

6. Two vectors are given by

$$|a\rangle = \begin{pmatrix} -1 \\ 0 \\ 4i \end{pmatrix}, \quad |b\rangle = \begin{pmatrix} 2 \\ -2i \\ 5 \end{pmatrix}.$$

Find: a) $\langle a|$; $\langle b|$; b) $\langle a|b\rangle$; $\langle b|a\rangle$; c) $|c\rangle = |a\rangle + 2|b\rangle$; $\langle c|a\rangle$; and d) compute the norms of $|a\rangle$, $|b\rangle$ and $|c\rangle$.

7. Three states are defined by

$$|\psi_0\rangle = |0\rangle, \quad |\psi_1\rangle = -\frac{1}{2}|0\rangle - \frac{\sqrt{3}}{2}|1\rangle, \quad |\psi_2\rangle = -\frac{1}{2}|0\rangle + \frac{\sqrt{3}}{2}|1\rangle.$$

Find

$$|\langle\psi_0|\psi_1\rangle|^2, \quad |\langle\psi_1|\psi_2\rangle|^2, \quad |\langle\psi_2|\psi_0\rangle|^2.$$

8. Consider the orthonormal basis $\{|0\rangle, |1\rangle\}$ and the following matrix A:

$$A = |0\rangle\langle 0| + |1\rangle\langle 1|.$$

Find the matrix representation of A in the following cases:

a) $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

b) $|0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad |1\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix}$

c) $|0\rangle = \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}, \quad |1\rangle = \begin{pmatrix} \sin\theta \\ -\cos\theta \end{pmatrix}$

9. Calculate the tensor product of

$$|a\rangle = \frac{2}{\sqrt{3}}\begin{pmatrix} -1 \\ \frac{1}{2} \end{pmatrix} \quad \text{and} \quad |b\rangle = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 \\ \sqrt{2} \end{pmatrix}.$$

10. If $|\psi\rangle = |a\rangle \otimes |b\rangle$ and $A|a\rangle = a|a\rangle$, $B|b\rangle = b|b\rangle$. Compute $A \otimes B|\psi\rangle$.

11. Find the tensor product of the Pauli matrices X and Z.

12. Find $(X \otimes Z)|\psi\rangle$, where

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

Appendix B. Solutions to Selected Short Questions

1. Fundamentals of Quantum Physics

1 False.

3 True.

4 True: for a certain t, Ψ does not verify $\lim_{x\to\pm\infty} \Psi \to 0$.

5 False: Ψ does not verify $\lim_{x\to\pm\infty} \Psi \to 0$.

6 True: from de Broglie equation, we obtain $v = h/(m \cdot \lambda) \approx 7.3 \cdot 10^6$ m/s.

7 True.

2. Quantum Computing: Gates and Circuits

1 True: we can write $|q_2\rangle$ also as $|q_2\rangle = \frac{i}{\sqrt{2}}(|0\rangle + i|1\rangle)$, and given than global phases are unobservable, that is the same state as $|q_1\rangle$.

2 False: $\theta = \phi = \frac{\pi}{2}$ correspond to $|q\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$.

3 False: $\theta = \pi/2$ and $\phi = \pi$ correspond to $|q\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

4 False: $|q\rangle$ can be also written as $|q\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. The probability to measure 0 in the first qubit as a first measure is then $1/2$.

6 False.

7 False.

3. Quantum Computing: Applications

1 False: the circuit $(H \otimes I) \cdot CNOT \cdot (H \otimes I)$ can copy the qubits $|+\rangle$ and $|-\rangle$.

2 True: a given quantum circuit can only make copies of two orthogonal states.

3 True.

4 False.

5 False: all four outcomes are equally probable; so the probability of each measurement is always 1/4.

6 True.

4. Quantum Measurements

2 False:

$$M_R = |R><R| = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & +1 \end{pmatrix}.$$

3 True: indeed $\rho = 0.5|0\rangle\langle 0| + 0.5|+\rangle\langle +| = \frac{1}{4}\begin{pmatrix} 3 & 1 \\ 1 & 1 \end{pmatrix}$.

4 True: in the case of a mixture of equally probable states, the purity is $\mathcal{P} = 1/d$.

5 True: in both cases, we have $\mathcal{F}_1 = |\langle 0|+\rangle|^2 = \mathcal{F}_2 = |\langle 0|-\rangle|^2 = \frac{1}{2}$.

5. Quantum Algorithms

1 True.

2 False: the probability does not linearly increase as $\frac{9}{N}$. The optimum number of Grover iterations is, instead, proportional to $\sqrt{N}$. In our case, it would be $\sqrt{10^6} = 1000$.

3 False: consider, for instance, the QFT of the Bell $|\beta_{00}\rangle$ state. The resulting state is a non-entangled state.

4 False: the number of required swap gates is the integer of $k/2$, where k is the number of qubits. For a 3-qubit QFT circuit, only 1 swap gate is needed.

6. Quantum Processors

3 False.

4 False: every object, in principle, may be entangled with every other.

5 True.

6 True: indeed, multiplying matrices $HWP(\alpha) \times HWP(\alpha) = I$.

7 True.

8 False: considering the initial state $|1\rangle|n\rangle$, and after tuning a π-pulse to red, the final state is $|0\rangle|n+1\rangle$.

9 True.

7. Quantum Communication

1 True: on average, the reconciled key is 50% of the raw key for the BB84 protocol and only 25% for the B92 protocol.

2 False: even if the bases are different, the results can agree.

3 True: the only condition is that the two states generated by Alice are non-orthogonal.

4 False: the result would have been the same for both parties, but it could have been 0 or 1.

Appendix A

1 False: the state $|q_1\rangle \otimes |q_2\rangle \otimes |q_3\rangle$ of three qubits is described by a vector with 8 complex entries α_i ($i = 1, \ldots, 8$). Not all of those are independent, however. For example, the state has to be normalized so that $\sum_i |\alpha_i|^2 = 1$.

2 True.

3 True: $AB = \mathbb{I} \Rightarrow (BA)^\dagger = \mathbb{I} \Rightarrow B^\dagger A = \mathbb{I} \Rightarrow B^\dagger = A^{-1} = B$.

4 True.

Appendix C. Solutions to Selected Problems

1. Fundamentals of Quantum Physics

1 $\lambda = 34000$ Å - Infrared region

2 The photoelectric effect.

4 n=5.6×10^{16} photons/s.

5 a) $K_{\text{max}} = 8.2\,\text{eV}$ b) $V_0 = 8.2\,\text{V}$ c) $\nu_t = 1000\,\text{THz}$ d) $n = 2 \times 10^{18}\,\text{photons}/(\text{s} \cdot \text{m}^2)$.

6 a) $h = 6.621 \times 10^{-34}\,\text{kg} \cdot \text{m}^2/\text{s}$ b) $\phi_{\text{Na}} = 6.34\,\text{eV}$ and $\lambda_t = 195\,\text{nm}$.

7 $\lambda = 3820\,\text{Å}$.

9 c) In the case of electrons, we observe the characteristic interference pattern of waves, but produced by single particles (see Figure 7.1).

10 $p = 1.65 \times 10^{-24}\,\text{kg m/s}$, $E = 3.1\,\text{keV}$, and $K_{\gamma} = 330\,\text{K}_{e^-}$.

13 a) $\Delta x \geq 39.8\,\text{Å}$ b) $\Delta x \geq 0.0398\,\text{mm}$ c) $\Delta x \geq 0.0398\,\text{m}$

14 Outside the box $V(x) = +\infty$, such that $\psi(x) = 0$.
Inside the box $\partial_x^2 \psi(x) = -(2mE/\hbar^2)\psi(x) = -k^2\psi(x)$, such that $\psi(x) = A\sin(kx) +$

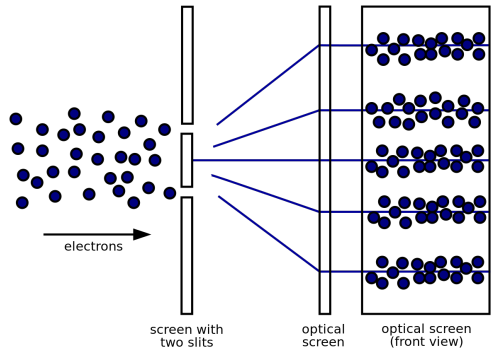


Fig. 7.1
Solution to the problem of the double slit experiment with electrons.

$B\cos(kx)$.
Imposing continuity at the edges of the box, one finds $B = 0$ and $k = \pi n/L$, with integer n, such that the energy is $E = \hbar^2 k^2/(2m) = \hbar^2\pi^2 n^2/(2mL^2)$.
Normalization $\int_{-\infty}^{\infty} |\psi(x)|^2 \mathrm{d}x = 1$ gives $A = \sqrt{2/L}$.
The complete solution inside the box is therefore $\psi_n(x) = \sqrt{2/L}\sin(\pi n x/L)$.

15 a) $n = 6.64 \times 10^{20}$, b) $\Delta x = 10\,\mu$m, $\Delta p_x = 2 \times 10^{-14}$ kg · m/s, c) $\frac{\Delta x \Delta p_x}{\hbar} = 1.9 \times 10^{15}$.

16 $\langle x\rangle = 0, \quad \langle x^2\rangle = \frac{1}{2}(\frac{1}{6} - \frac{1}{\pi^2})L^2$.

17 a) $C = \sqrt{\kappa}$ b) $\langle x\rangle = 0$, $\langle x^2\rangle = \frac{1}{2\kappa^2}$ c) $\sigma = \frac{1}{\sqrt{2}\kappa}$, $P(x \notin [-\sigma, +\sigma]) = e^{-\sqrt{2}}$.

20 a) $E_{min} = 0.54\,$eV, $\lambda_{min} = 2279\,$nm b) $\lambda_2 = 121\,$nm, $\lambda_3 = 103\,$nm, $\lambda_4 = 97$ nm.

22 Remembering that the energies allowed inside a square well of width L are $E_n = \hbar^2\pi^2 n^2/(2mL^2)$ with integer $n \geq 1$, we have a) $E = 5E_1$, b) $E = 55E_1$, and c) $E = 19E_1$.

2. Quantum Computing: Gates and Circuits

1 a) $P(|0\rangle) = \frac{2}{3}$, $P(|1\rangle) = \frac{1}{3}$, b) $P(|0\rangle) = \frac{1}{4}$, $P(|1\rangle) = \frac{3}{4}$, c) $P(|0\rangle) = \frac{1}{3}$, $P(|1\rangle) = \frac{2}{3}$

2 a) $\theta = \pi + 2k\pi$, $k \in \mathbb{N}$. b) $\theta = 0 + 2k\pi$, $k \in \mathbb{N}$ c) $e^{i\theta}$ is a global phase therefore any value of θ make the two qubits indistinguishable.

3 a) $U_{not} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, b) $U_{not} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

4 $\lambda_1 = 1$, $|\lambda_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\lambda_2 = e^{i\pi/4}$, $|\lambda_1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

5 $S = \frac{1}{2}[(1+i)\mathbb{I} + (1-i)Z]$

6 a) $|q'\rangle = -\beta|0\rangle - \alpha|1\rangle$ b) $|q'\rangle = \alpha|+\rangle - \beta|-\rangle$

9 The identity does nothing while the X, Y and Z produce rotations of $\pi\ rad$ around the x, y and z axis, respectively.

12 Taking into account that A is nilpotent, $A^2 = \mathbb{I}$, then $A^2 = A^4 = A^6 = \ldots = \mathbb{I}$ and $A = A^3 = A^5 = \ldots = A$, and applying a Tailor expansion, we have:

$$\begin{aligned}
\exp(iAx) = &\sum_{n=0}^{\infty} \frac{(iAx)^n}{n!} = \\
=&1 + \frac{iAx}{1!} - \frac{A^2x^2}{2!} - \frac{iA^3x^3}{3!} + \ldots = \\
=&1 - \frac{x^2}{2!} + \frac{x^4}{6!} - \frac{x^6}{6!} \ldots + i(x - \frac{x^3}{3!} + \frac{x^5}{5!} + \ldots)A = \\
=&\cos x\mathbb{I} + i(\sin x)A.
\end{aligned}$$

14 $H = R_x(-\pi/2)R_z(-\pi/2)R_x(-\pi/2)$.

17 The probability is $P(+1) = \frac{n_z+1}{2}$ and the post-measurament state is $|\Psi'\rangle = \frac{1}{2}\sqrt{\frac{2}{1+n_z}}\,[(n_z+1)|0\rangle + (n_x + in_y)|1\rangle]$.

18 For the Hadamard gate we have $\alpha = \pi$, $\gamma = \pi/2$ and $\hat{n} = \frac{1}{\sqrt{2}}(1,0,1)$, while for the phase gate S we get $\alpha = \pi/2$, $\gamma = \pi/4$ and $\hat{n} = (0,0,1)$.

19 a) $|\alpha_N\rangle = \frac{1}{\sqrt{39}}(3|00\rangle - 2|01\rangle + |10\rangle - 5|11\rangle)$, b) $|\alpha_N\rangle = \frac{1}{\sqrt{3}}|q_0\rangle + \sqrt{\frac{2}{3}}|q_1\rangle$, c) $P(|q_0\rangle) = \frac{1}{3}$, $P(|q_1\rangle) = \frac{2}{3}$, d) $P(|00\rangle) = \frac{9}{13}$

20 a) $b = \frac{13}{20} = 0.806$, b)$P_{2,0} = \frac{9}{10} = 0.9$, c) $P(|00\rangle) = \frac{25}{34} = 0.735$, e) $|\Psi'\rangle = \frac{1}{2}\sqrt{\frac{50}{17}}|00\rangle + \frac{3}{10}\sqrt{\frac{50}{17}}e^{i\pi}|01\rangle$

21 $|+\rangle|0\rangle$, $|-\rangle|0\rangle$,$|+\rangle|1\rangle$, $|-\rangle|1\rangle$

25 a) $CNOT_{rev} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}$ b) $A_{total} = SWAP = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

26 a) $M = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$

29 $M = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & i & 0 \\ 1 & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \end{pmatrix}$

32 $M = \begin{pmatrix} -i & 0 & 0 & 0 \\ 0 & -i & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}$

3. Quantum Computing: Applications

4 $|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $|\beta_{01}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, $|\beta_{10}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$, $|\beta_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$

6 a) $0, 0$; b) $0, 1$; c) $1, 0$; d) $1, 1$

8 If $U = \mathbb{I}$, then $m = m' = 0$. If $U = Z$, then $m = 1, m' = 0$. If $U = X$, then $m = 0, m' = 1$. If $U = ZX$, then $m = m' = 1$.

9 a) To obtain $|\beta_{00}\rangle$, $U = Z$; to obtain $|\beta_{01}\rangle$, $U = ZX$; to obtain $|\beta_{10}\rangle$, $U = I$; to obtain $|\beta_{11}\rangle$, $U = X$. b) and c):

U	pre-measurement state	(m, m')
Z	$\|00\rangle$	$0, 0$
ZX	$\|01\rangle$	$0, 1$
I	$\|10\rangle$	$1, 0$
X	$\|11\rangle$	$1, 1$

10 a) $A = H$; $B = X$; $C = Z$; $D = H$. b) $|ab\rangle = -|10\rangle$.

12 a) $|\Psi_{in}\rangle = \frac{1}{\sqrt{2}}\Big\{|0\rangle(a|-\rangle + b|+\rangle) + |1\rangle(a|-\rangle - b|+\rangle)\Big\}$. b) If $m = 0$, then $U = XH$; if $m = 1$, then $U = ZXH$.

13 If Alice measures 0, Bob applies H. If Alice measures 1, Bob applies ZH.

16 a) From the table

m	m'	Bob initial qubit	BA	Bob final qubit
0	0	$\alpha\|1\rangle + \beta\|0\rangle$	X	$\alpha\|0\rangle + \beta\|1\rangle$
0	1	$\alpha\|0\rangle + \beta\|1\rangle$	I	$\alpha\|0\rangle + \beta\|1\rangle$
1	0	$\alpha\|1\rangle - \beta\|0\rangle$	XZ	$\alpha\|0\rangle + \beta\|1\rangle$
1	1	$\alpha\|0\rangle - \beta\|1\rangle$	Z	$\alpha\|0\rangle + \beta\|1\rangle$

we deduce that the Z matrix is acting when $m = 1$, and that X is acting when $m' = 0$. Consequently, we derive $A = Z^m$ and $B = X^{\bar{m}'}$.
b) In this case, we have

m	m'	$P_{(m,m')}$	Bob initial qubit	BA	Bob final qubit
0	0	$\frac{\beta^2}{2}$	$\|1\rangle$	X	$\|0\rangle$
0	1	$\frac{\alpha^2}{2}$	$\|1\rangle$	I	$\|1\rangle$
1	0	$\frac{\beta^2}{2}$	$\|1\rangle$	XZ	$\|0\rangle$
1	1	$\frac{\alpha^2}{2}$	$\|1\rangle$	Z	$\|1\rangle$

The probability that the qubit $|q\rangle$ will be correctly teleported is $P = 2\alpha^2\beta^2$.

4. Quantum Measurements

2 The projective measurement operator is

$$M_{\beta_{00}} = |\beta_{00}\rangle\langle\beta_{00}| = \frac{1}{2}\left[|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|\right].$$

Given that a projective measurement operator is Hermitian, the probability is $P = \langle\psi|M_{\beta_{00}}|\psi\rangle = \frac{1}{2}$.

3 The probability of collapsing into any of the four Bell-states is 25%.

4 $E_{10}|q\rangle = \frac{1}{\sqrt{3}}\left[|00\rangle + |01\rangle\right]$ and the probability is $P = \langle q|E_{10}|q\rangle = \frac{2}{3}$.

5 a) The probability of measuring 0 in the first qubit is $P(0) = \cos^2(\frac{\theta}{2})$, while the probability of obtaining 1 is $P(1) = \sin^2(\frac{\theta}{2})$. Given that the probabilities depend on θ and if we perform the experiment several times, it is possible to deduce the phase θ.
b) In that case, we have $\theta = 0$ and $\theta = \pi$, respectively. For the first case, we obtain $P_{\theta=0}(0) = \cos^2(\frac{\theta}{2}) = 1$ and $P_{\theta=0}(1) = 0$; while for the second case we have $P_{\theta=\pi}(0) = 0$ and $P_{\theta=\pi}(1) = 1$. Consequently, it will be possible to distinguish between both states.

7 b) $p(1) = 0, p(2) = \frac{1}{(1+\sqrt{2})^2}$; c) $p(1) = \frac{1}{(1+\sqrt{2})^2}, p(2) = 0$; d) No.

8 a) $P_0 \otimes \mathbb{I}|\psi\rangle = |01\rangle$, b) $\mathbb{I} \otimes P_1|\psi\rangle = |01\rangle$.

9 a) $M = \frac{1}{2}(|0\rangle\langle 0| + i|0\rangle\langle 1| - i|1\rangle\langle 0| + |1\rangle\langle 1|)$; b) $p(1) = \frac{1}{2}, p(-) = \frac{1}{2}$; c) No.

10 a) $P_{\hbar\omega} = |u_1\rangle\langle u_1|$, $P_{2\hbar\omega} = |u_2\rangle\langle u_2|$, $P_{3\hbar\omega} = |u_3\rangle\langle u_3|$; b) $P(|u_1\rangle) = \frac{1}{4}$, $P(|u_2\rangle) = \frac{1}{2}$, $P(|u_3\rangle) = \frac{1}{4}$; c) $< E >= 2\hbar\omega$.

13 a) pure state, b) mixed state.

14 $\rho = \frac{1}{3}|u_1\rangle\langle u_1| - i\frac{\sqrt{2}}{3}|u_1\rangle\langle u_2| + i\frac{\sqrt{2}}{3}|u_2\rangle\langle u_1| + \frac{2}{3}|u_2\rangle\langle u_2|$

15 a) $\rho = \frac{1}{3}(|00\rangle\langle 00| + i|00\rangle\langle 01| - |00\rangle\langle 11| - i|01\rangle\langle 00| + |01\rangle\langle 01| + i|01\rangle\langle 11| - |11\rangle\langle 00| - i|11\rangle\langle 01| + |11\rangle\langle 11|)$; b) $\lambda_1 = \lambda_2 = \lambda_3 = 0, \lambda_4 = 1$; c) Pure state.

16 a) $\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{6}|0\rangle\langle 1| + \frac{1}{6}|1\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1|$ or $\rho = \frac{1}{6}\begin{pmatrix} 3 & 1 \\ 1 & 3 \end{pmatrix}$; b)$|\lambda_1\rangle = |-\rangle$, $|\lambda_2\rangle = |+\rangle$

17 $\rho = \begin{pmatrix} \frac{1}{4} & \frac{\sqrt{3}}{4}e^{-i\pi/4} \\ \frac{\sqrt{3}}{4}e^{i\pi/4} & \frac{3}{4} \end{pmatrix}$

18 $\mathcal{F} = 0.894$

19 c) $\mathcal{F}_H = 0.890(42)$, $\mathcal{F}_V = 0.865(46)$, $\mathcal{F}_P = 0.845(27)$ and $\mathcal{F}_L = 0.852(37)$, yielding an average fidelity of the teleportation process of $\hat{\mathcal{F}} = 0.863(38)$.

5. Quantum Algorithms

2 The pre-measurement state is $|\psi\rangle = |10\rangle|-\rangle$, so one of the first two qubits ends up as a 1.

3 a) Eigenvalues $\lambda_1 = +1$ and $\lambda_2 = (-1)^x$ with eigenvectors $|\lambda_1\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|\lambda_2\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, respectively. c) If $f(0) = f(1)$, the pre-measurement state is $\psi = |0\rangle|f(0)\rangle$; while if $f(0) \neq f(1)$, then $|\psi\rangle = \frac{1}{2}(|0\rangle|f(0)\rangle + |1\rangle|f(0)\rangle + |0\rangle|f(1)\rangle - |1\rangle|f(1)\rangle)$.

6 a) $|\omega\rangle = |011\rangle$

12 $QFT|\psi\rangle = \frac{1}{\sqrt{14}}\left[(2+i)|0\rangle - 2|1\rangle + (2-i)|2\rangle\right]$

14 The final state of the first register is $|\psi\rangle = \frac{1}{\sqrt{2}}\left[|0\rangle - |4\rangle\right]$, with the possible values of y being 0 and 4.

15 a) It works correctly with $r = 4$; $N = 5 \cdot 3$. b) It works correctly with $r = 6$; $N = 13 \cdot 7$. c) It fails, because $r = 4 \Rightarrow a^{r/2} \mod N \neq -1 \mod N$.

6. Quantum Processors

1 $I_t = 1.88\, W/m^2$.

2 $\theta = 60°$

3 $I_t = \frac{1}{8} I_0 \sin^2(2\theta)$

4 $P = 3.97\, mW$

5 For any value of α, $\beta = 60°$.

8 $P_{D_1} = \frac{1}{2}(1 - \cos\phi)$ and $P_{D_2} = \frac{1}{2}(1 + \cos\phi)$.

9 a) The matrix of the retarder is $\begin{pmatrix} e^{i\phi} & 0 \\ 0 & 1 \end{pmatrix}$.
b) $P_{D_1} = \frac{1}{2}(1 - \cos\phi)$ and $P_{D_2} = \frac{1}{2}(1 + \cos\phi)$. c) $\phi = \pi$ for $|0\rangle$ and $\phi = \pi/2$ for $|+\rangle$

14 First, it is necessary to apply to the first qubit a $\pi/2$ pulse from a laser tuned to the blue sideband. Then, we should apply a π pulse to the second qubit from a laser tuned to the red sideband.

15 $|\Psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle|1\rangle + |11\rangle|2\rangle)$

16 $|\Psi\rangle = \frac{1}{2}(|01\rangle|1\rangle + |11\rangle|1\rangle + |01\rangle|2\rangle + |11\rangle|2\rangle)$

7. Quantum Communication

2 a) $p = 3$, $q = 5$. b) $p = 2017$, $q = 2027$. c) $p = 61224210904935475769370373175614188412257585542531069 99$, $q = 58464182144061546788365531829791623841986105056010623 3$. d) p and q unknown.

5 b) $K_{\text{raw}} = (00101010)$. d) $K_{\text{rec}} = (01011)$.

8 *a)* $K_{\text{sifted}} = (0110)$.

9 *a)*

	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8
Beijing base	0	1	1	0	1	0	1	1
Vienna base	1	0	1	1	0	0	1	0
Possible results	0/1	0/1	0	0/1	0/1	0	0	0/1
One result	1	1	0	0	1	0	0	1

b) $HRRHRHRR$. d) $K_{\text{rec}} = (0111)$.

11 *b)* ICFO possible results: $(0, 0/1, 0, 1, 1, 0, 0, 0/1)$. *d)* $K_{\text{rec}} = (001100)$.

Appendix A

3 a) $C = \sqrt{\frac{\kappa}{\pi}}$ b) $\langle x \rangle = c, \quad \langle x^2 \rangle = c^2 + \frac{1}{2\kappa}, \sigma = \frac{1}{\sqrt{2\kappa}}$

4 a)

$$\begin{pmatrix} -3-2i & -1+i & 2i \\ 35 & 1 & 2 \\ 0 & 4i & 4 \end{pmatrix}$$

b)

$$\begin{pmatrix} -28+6i & -7-3i & -1 \\ -60-11i & -6+7i & -2 \\ 2+56i & -1+14i & 2i \end{pmatrix}$$

c)

$$\begin{pmatrix} -28-5i & -7-3i & -5-i \\ 15-12i & 30+5i & -9-60i \\ 2+43i & -1+17i & -2 \end{pmatrix}$$

d)

$$\begin{pmatrix} -3 & 5 & i \\ -1 & -2 & 2i \\ 2i & 1 & 4 \end{pmatrix}$$

e)

$$\begin{pmatrix} -3 & -1 & -2i \\ 5 & -2 & 1 \\ -i & -2i & 4 \end{pmatrix}$$

f)

$$\begin{pmatrix} -3 & 5 & -i \\ -1 & -2 & -2i \\ -2i & 1 & 4 \end{pmatrix}$$

g)

$$3-2i$$

h)

$$-3$$

i)

$$\frac{1}{3}\begin{pmatrix} 2i & 0 & -i \\ i & 0 & -2i \\ -63i & 3 & 36i \end{pmatrix}$$

9 $|a\rangle \otimes |b\rangle = \frac{2}{3}\begin{pmatrix} -1 \\ -\sqrt{2} \\ \frac{1}{2} \\ \frac{\sqrt{2}}{2} \end{pmatrix}$

10 $A \otimes B|\psi\rangle = ab|\psi\rangle$

11 $X \otimes Z = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}$

12 $(X \otimes Z)|\psi\rangle = \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle)$.

Bibliography

1. Desurvire, Emmanuel. *Classical and quantum information theory : an introduction for the telecom scientist*. Cambridge University Press, 2009.
2. Eisberg, R.M. & Resnick, R. *Quantum Physics of atoms, molecules, solids, nuclei and particles*. John Wiley & Sons, 1985.
3. Griffiths, David J. *Introduction to Quantum Mechanics*. Pearson, 2004.
4. Kaye, Phillip; Laflamme, Raymond; Mosca, Michele. *An Introduction to quantum computing*. Oxford University Press, 2007.
5. McMahon, David. *Quantum computing explained*. John Wiley & Sons, 2008.
6. Nielsen, M.A.; Chuang, I.L. *Quantum computation and quantum information*. Cambridge University Press, 2010.
7. Steeb, Willi-Hans & Hardy, Yorick. *Problems & Solutions in Quantum Computing & Quantum Information*. World Scientific Publishing Company, 2011.
8. Tipler, Paul Allen; Mosca, Gene. *Física para la ciencia y la tecnología*. Reverté, 2005.
9. Emanuel Knill, Raymond Laflamme, Howard N. Barnum, Diego A. Dalvit, Jacek J. Dziarmaga, James E. Gubernatis, Leonid Gurvits, Gerardo Ortiz, Lorenza Viola, Wojciech H. Zurek, *From Factoring to Phase Estimation: A Discussion of Shor's Algorithm*, Los Alamos Science No. 27, 2002;
10. Pedrotti, F. L.; Pedrotti, L.M; Pedrotti L,S. *Introduction to Optics*. Addison-Wesley, 2006.
11. Michael H. Holzscheiter, *Ion-Trap Quantum Computation*, Los Alamos Science No. 27, 2002;
12. Jane E. Nordholt, Richard J. Hughes, *A New Face for Cryptography*, Los Alamos Science No. 27, 2002;