

Quantum Foundations and Quantum Computation

Seminar Notes

John Hutchinson

September 21, 2022 version

PRELIMINARY & INCOMPLETE

Introduction

Quantum Foundations and Quantum Computation

The main goal is to develop an understanding of Quantum Theory and its underlying mathematical models, particularly as it applies to quantum computation.

In Quantum Mechanics (i.e. Quantum Theory in general), we consider properties such as position and momentum which take an infinite set of values. This is modelled mathematically by considering infinite dimensional Hilbert spaces and linear operators on such spaces. This leads to many (interesting and difficult) functional analysis issues.

In Quantum Theory for quantum computing we need only consider finite dimensional Hilbert Spaces, usually the n -dimensional inner product spaces \mathbb{C}^n .¹ The functional analysis difficulties are not present.

However, all the quantum weirdness *is* present in this setting. This includes superposition and entanglement, which imply the no-cloning theorem, superdense coding, teleportation, and non-locality of quantum effects (including the famous double-slit experiment, the Einstein–Podolsky–Rosen paradox, and the results of John Bell showing quantum theory cannot be explained by additional information in the classical sense). We will see all this fairly soon!

In quantum computation, quantum “weirdness” is the essential resource utilised and exploited. We will see how this is done.

To reiterate, quantum theory in the finite dimensional setting is the optimal way to develop an intuition for quantum theory in general.

Mathematics

To understand quantum computing, you absolutely must become fluent in the mathematical model. Michael Nielsen [MN19, First Lesson, preceding “Part I: The state of a qubit”]

... it is impossible to explain honestly the beauties of the laws of nature in a way that people can feel, without their having some deep understanding of mathematics. I am sorry, but this seems to be the case. Richard Feynman [Fey, pp 39,40]

Switching from Newton’s mechanics to Einstein’s, for a mathematician, must to some extent be like switching from a good old provincial dialect to the latest Parisian slang. In contrast, switching to quantum mechanics, I imagine, is like switching from French to Chinese. Alexandre Grothendieck, *Récoltes et Semailles* (1986) (tr. from French)

DON’T PANIC Douglas Adams. *The Hitchhiker’s Guide to the Galaxy*.

¹ \mathbb{C}^n is the vector space of n -tuples $a = (a_1, \dots, a_n)$ with inner product $a \cdot b = a_1^* b_1 + \dots + a_n^* b_n$ (where a_i^* is the complex conjugate of a_i). Note that the inner product is conjugate linear in the *first* argument and linear in the second. This convention is very useful when we later use the Dirac “bra-ket” notation, see Appendix D.

The background necessary to follow these notes is some fairly basic linear algebra regarding finite dimensional complex vector spaces, and basic properties of unitary and hermitian operators. This is provided in Appendix B. Other mathematics is developed in the appendices and referred to as needed. This way you will get to very interesting quantum material very quickly!

Structure of the Notes

In the first chapter we discuss the fundamental ideas of quantum theory, the mathematical models used, and their highly nonintuitive consequences. The discussion is fairly informal – if something is unclear it will hopefully be clarified in subsequent chapters.

In Chapter 2 we begin anew and discuss the four quantum theory postulates for closed systems, the relevant mathematical framework, and from there derive the nonintuitive consequences discussed in Chapter 1.

In Chapter 3 we discuss examples of entanglement, non-cloning, superdense coding, Bell's and the CHSH inequalities and some “philosophical” considerations.

In Chapters 4 we discuss quantum computation, quantum circuits, teleportation, algorithms for quantum computers.

In Chapter 5 we discuss composite systems and some of the mathematical tools used in their analysis.

The Future for Quantum Computation

[dW19] is an insightful essay concerning the potential impact of quantum computers. [Pre18] discusses quantum computing in the near future.

Socrates on Physical Reality v. Quantum Space

And now, let me show in a figure how far our nature is enlightened or unenlightened: — Behold! human beings living in a underground den [aka: physical reality], which has a mouth open towards the light and reaching all along the den; here they have been from their childhood, and have their legs and necks chained so that they cannot move, and can only see before them, being prevented by the chains from turning round their heads.

Above and behind them a fire is blazing at a distance [aka: quantum state space], and between the fire and the prisoners there is a raised way; and you will see, if you look, a low wall built along the way, like the screen which marionette players have in front of them, over which they show the puppets.

Socrates (Plato, The Republic, Book VII (Benjamin Jowett, Tr.) [Pla0])



Figure 1: The Allegory of the Cave. (from Wiki Commons)

We, in our underground and classical world on the left, are chained and able to see but mere shadows of the quantum universe outside. Yet through mathematics — together with a little computer science, physics, and technology — enlightenment about this universe can be achieved.

Contents

1	Overview	7
1.1	Qubits	7
1.1.1	From Bits to Qubits	7
1.1.2	The State of a Qubit	8
1.1.3	Entanglement	11
1.1.4	Qubits and their Measurement	11
1.1.5	Qubits and Their Evolution	11
1.1.6	Physical Realisations of Qubits and their Measurement	11
1.2	Qubits (old)	11
1.2.1	Bits and Qubits	11
1.2.2	State Space, Physical Reality and Measuring Qubits	12
1.2.3	Superposition and Ensembles	13
1.2.4	The private world of qubits	13
1.3	Young's Two-Slit Experiment	15
1.3.1	Experimental Set-Up and Outcomes	15
1.3.2	The State Space	16
1.4	Entangled Pairs of Qubits	19
1.4.1	Quantum states for pairs of qubits	19
1.4.2	Separable qubits and entangled qubits	19
1.4.3	The Bell state	19
1.5	The EPR Paradox	21
1.5.1	What does it mean for quantum theory to be complete?	21
1.5.2	The EPR Experiment	21
1.5.3	Quantum theory <i>is</i> complete	22
2	Quantum Postulates for Closed Systems	24
2.1	State Space	25
2.1.1	State Space Postulate	25
2.1.2	Three Physical Realisations of Qubits	26
2.2	Measurement	29
2.2.1	Measurement Postulate (Orthonormal Basis Version)	29
2.2.2	Measuring Qubits	30
2.2.3	Distinguishing Relative Phase	30
2.2.4	Hermitian Operators and Measurements	31
2.2.5	Measurement Postulate (Hermitian Operator Version)	32
2.2.6	Pauli Matrices and Measurement	33
2.3	Qubits and Spin 1/2 Particles	35
2.3.1	Spin-Orientation	35
2.3.2	Stern-Gerlach Experimental Set-Up	35
2.3.3	Multiple Particles with the same Spin-Orientation	36
2.3.4	Spin-Orientation and Qubit Correspondence: Bloch Sphere Map	37
2.3.5	Spin-Orientation and Qubit Correspondence: Physical Justification	37
2.4	Evolution	38

2.4.1	Evolution Postulate (Discrete Version)	38
2.4.2	Examples of Unitary Gates	38
2.4.3	Evolution Postulate (Continuous Version)	39
2.4.4	Solution of Schrödinger's Equation	39
2.4.5	Hamiltonian Example	39
2.5	Composite Systems	41
2.5.1	Pairs of Qubits and Bipartite States	41
2.5.2	Composite System Postulate	41
2.5.3	N -Qubit Space	41
2.5.4	Inner Product for Composite Systems	42
2.5.5	Entangled Qubit Pairs	43
2.5.6	Bell States	44
3	Entanglement: Conundrum or Resource?	45
3.1	No-Cloning Theorem	45
3.2	Disentangling Entanglement	47
3.2.1	Invariance Properties of the Bell States	47
3.2.2	CNOT Gate	48
3.2.3	Preparing Bell States	49
3.2.4	Interim States in Quantum Circuits	49
3.2.5	Tensor Product of Operators	49
3.2.6	Measuring Entangled States	51
3.2.7	Measurement in the Bell Basis	53
3.2.8	Local Description for each Qubit	54
3.3	Superdense Coding	55
3.4	Teleportation	57
3.5	Bell & CHSH Inequalities	59
3.5.1	History	59
3.5.2	CHSH Experimental Setup	59
3.5.3	Preliminary Discussion of the Results	61
3.5.4	Classical Analysis; Physical Realism, Locality, Random Choice	62
3.5.5	Experimental Results	63
3.5.6	Quantum Analysis	63
3.6	GHZ	65
4	Quantum Circuits	66
4.1	Quantum Gates	66
4.2	Deutsch-Jozsa Algorithm	66
4.3	Shor's Algorithm	66
5	Composite Systems	67
5.1	Ensembles and Density Operators	67
5.2	The Bloch Ball	67
5.3	Subsystems and the Reduced Density Operator	67
5.4	Schmidt Decomposition and Purification	67
A	Visualising Higher Dimensions	68
B	Hermitian and Unitary Operators	70
B.1	Inner Product Space	70
B.1.1	Inner Product	70
B.1.2	Norm	71
B.1.3	Norms and Inner Products	71
B.1.4	Angle	71

B.1.5	Orthogonal Projections	72
B.2	Definitions in Terms of a “Good” Orthonormal Basis	72
B.2.1	Hermitian Operator	72
B.2.2	Unitary Operator	73
B.2.3	Normal Operator	74
B.3	Definitions in Terms of Adjoint Operator	74
B.3.1	Adjoint	74
B.3.2	Hermitian Operator	74
B.3.3	Unitary Operator	75
B.3.4	Normal Operator	75
B.4	2×2 Classification	75
B.5	Polar Decomposition	75
B.6	Another Characterisation	76
C	Determinant and Trace	77
C.1	Determinant	77
C.2	Trace	78
D	Dirac Bra-Ket Notation	79
D.1	Kets and Bras	79
D.2	More on Inner Products	80
D.3	Outer Products	80
D.3.1	Definition and Matrix Representation	80
D.3.2	Orthogonal Projections	80
D.3.3	Operator as a Sum of Dyads	81
D.4	Computing with Dirac Notation	81
E	Pauli Matrices	82
E.1	Definitions, Basic properties, Eigenvalues and Eigenvectors	82
E.2	As Basis Vectors	82
E.3	Pauli Vector	83
E.3.1	Definitions and Examples	83
E.3.2	Properties	83
F	The Bloch Sphere	85
F.1	Coordinate Approach	85
F.2	Pairs of antipodal points	86
F.2.1	Orthonormal Bases & Antipodal Points	86
F.2.2	Important Examples	86
F.3	Projection Mapping Approach	87
F.4	Angle Doubling	89
G	Functions of Normal Operators	90
G.1	Examples of Interest	90
G.2	Power Series Definition	90
G.3	Definition for Normal Operators	90
G.4	Matrices for the Schrödinger Equation	91
H	Tensor Products	92
H.1	Informal Presentation	92
H.1.1	Bilinear Requirements	92
H.1.2	Basis and Dimension	93
H.1.3	Entangled and Product Elements	93
H.1.4	Other Bilinear Products	93
H.1.5	Inner Product	93

H.1.6 Examples	93
H.2 Basis Dependent Definition of Tensor Products	94
H.3 Tensor Product of Operators	95
Bibliography	95

Chapter 1

Overview

Contents

1.1 Qubits	7
1.1.1 From Bits to Qubits	7
1.1.2 The State of a Qubit	8
1.1.3 Entanglement	11
1.1.4 Qubits and their Measurement	11
1.1.5 Qubits and Their Evolution	11
1.1.6 Physical Realisations of Qubits and their Measurement	11
1.2 Qubits (old)	11
1.2.1 Bits and Qubits	11
1.2.2 State Space, Physical Reality and Measuring Qubits	12
1.2.3 Superposition and Ensembles	13
1.2.4 The private world of qubits	13
1.3 Young's Two-Slit Experiment	15
1.3.1 Experimental Set-Up and Outcomes	15
1.3.2 The State Space	16
1.4 Entangled Pairs of Qubits	19
1.4.1 Quantum states for pairs of qubits	19
1.4.2 Separable qubits and entangled qubits	19
1.4.3 The Bell state	19
1.5 The EPR Paradox	21
1.5.1 What does it mean for quantum theory to be complete?	21
1.5.2 The EPR Experiment	21
1.5.3 Quantum theory <i>is</i> complete	22

1.1 Qubits

1.1.1 From Bits to Qubits

In a classical computer the basic unit of information is a *bit*. A bit takes one of two values, or equivalently is in one of two possible *states*, typically denoted by 0 and 1, but also by true/false, yes/no, +/−, etc. Thus the state of a bit is an element of the set $\{0, 1\}$.

A bit has various physical realisations such as the presence or absence of a hole in punched computer cards of old, a switch being on or off, an electric current having one of two distinct voltages (high or low), or via a flip-flop built from transistors on a computer chip. We use the terminology “bit” to refer both to the physical device as well as to its value/state at some particular time.

A one terabyte USB stick holds approximately 8×10^{12} bits of information.

In a quantum computer, on the other hand, the basic unit of information is a *quantum bit* or *qubit*¹. A qubit is the quantum generalisation of a (classical binary) bit. Compared with a classical computer, the current (in 2022) maximum number of qubits in a quantum computer is around 100. The major impediment to scaling up the size of quantum computers is that individual qubits are very sensitive to interference from the external environment.

Every two-level quantum system corresponds to a qubit. Three fundamental classes of qubit examples are particles with two spin states, the linear polarisation of a photon of light in the plane orthogonal to its line of flight, and the two lowest energy levels of an electron. But there are many variants, as well as other important but quite distinct examples. See [NC10, Chap. 7, p 277ff].

The two major qubit implementations in quantum computers currently involve trapped ion qubits or superconducting qubits. See [NAo19, Chs 2,5] for a readable discussion. Microsoft is pursuing yet another approach utilising topological qubits, which because of their potential stability and fault tolerance could more readily lead to large scale quantum computers. This is less developed than other approaches, but shows much promise for the long-term. See [here](#) and [here](#).

In a quantum computer one also needs to initialise the qubits, manipulate their states, and measure/observe the output states. All this requires extremely sophisticated and delicate devices, and has major consequences for the design of quantum computers. ***Di Vincenzo***

Finally, the power of quantum computers lies in the fact that its qubits can be “entangled” with one another. We discuss this in Section 1.1.3.

But first we need to understand what is meant by the state of a qubit.

1.1.2 The State of a Qubit

The state of a bit tells us what will be seen if we look at/observe the bit.

The *state* of a qubit is a much more sophisticated mathematical entity than the state of a bit, and takes as its possible state/value any linear *superposition* of the form

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathbb{C}^2, \quad |\alpha|^2 + |\beta|^2 = 1, \quad \alpha, \beta \in \mathbb{C}, \quad (1.1)$$

where $|0\rangle := \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle := \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ are the standard (orthonormal) basis vectors for \mathbb{C}^2 . The coefficients α and β are called *amplitudes*.

The notation $|\psi\rangle$ is due to Dirac, which is discussed in Appendix D. You can think of “ ψ ”, “0” and “1” as labels for the vectors $|\psi\rangle$, $|0\rangle$ and $|1\rangle$ respectively.

\mathbb{C}^2 is the *state space* of the qubit. Any two dimensional complex Hilbert space \mathcal{H} is isomorphic to \mathbb{C}^2 with its standard inner product, and sometimes it is more convenient to work with general Hilbert spaces \mathcal{H} . On the other hand, we usually have a fixed measurement process, and since any measurement process² determines a particular ordered orthonormal basis pair as we will see in Section 1.1.4, it is convenient to take this ordered basis to be $|0\rangle$ and $|1\rangle$ in \mathbb{C}^2 .

To gain an intuitive understanding it is sometimes sufficient to restrict considerations to $\alpha, \beta \in \mathbb{R}$ in (1.1). In this case $-1 \leq \alpha, \beta \leq 1$ with $\alpha^2 + \beta^2 = 1$, and we are restricting considerations to the unit circle in the “real” section \mathbb{R}^2 of \mathbb{C}^2 . See Figure 1.1.

The qubits

$$|+\rangle := \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \quad |-\rangle := \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle. \quad (1.2)$$

in Figure 1.1 play an important role in quantum computation and form an orthonormal basis, as is easily verified.

¹“Qubit” — pronounced “q(ueue)bit” — is a contraction of “quantum bit”.

²Except for the trivial measurement process which always gives the same output

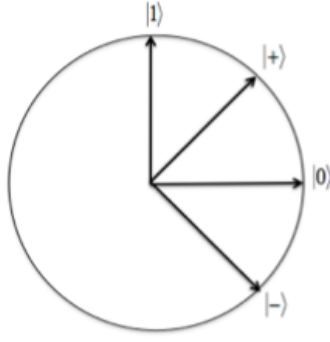


Figure 1.1: The unit circle in the “real” section of \mathbb{C}^2 . (from [Vaz12])

Interpretation And now for some of the really weird stuff, at least to our classical ways of thinking.

The significance of the coefficients α and β in (1.1) is discussed in more detail in Section 1.1.4. Their absolute values squared, $|\alpha|^2$ and $|\beta|^2$, give the respective probabilities of each of the two possible outcomes for what is called a *standard measurement*. The state of a qubit is given by (the possibly time-varying “wave” of) probability *amplitudes* (α, β) , and not just by the probabilities $(|\alpha|^2, |\beta|^2)$. In particular, the two states $|+\rangle$ and $|-\rangle$ have the same outcome probabilities when standard measurements are applied, but not when other other measurements are applied, as discussed in Section 1.1.4.

We cannot directly observe the state of a qubit. Moreover, the very act of observation must unavoidably involve some minimal physical interaction, such as by a photon of light or a phonon³ of energy, and which then dramatically changes the state. In particular, qubit states correspond to points on the unit sphere in \mathbb{C}^2 .

Every two-state physical quantum system is a qubit. We discuss examples in Section 1.1.6.

Treating qubits in a mathematical/abstract manner enables us to develop quantum theory in a manner independent of any particular physical realisation

Every finite state quantum system can be treated in an analogous manner. If there are n possible measurement outcomes then the mathematical model is obtained from \mathbb{C}^n , equivalently from the finite dimensional complex Hilbert space of dimension n , instead of \mathbb{C}^2 .

Analogously to the situation for bits, we abuse language and

- refer to the “qubit $|\psi\rangle$ ”, rather than the state of the qubit being $|\psi\rangle$,
- use the word “qubit” both for the mathematical model and for various physical realisations.

Example: energy levels of an electron in an atom. (A helpful case to keep in mind.)

It is often possible to effectively limit an electron in an atom to its two lowest energy levels. The lowest energy level (or ground state) is denoted by $|0\rangle$ and the next level (or first excited state) by $|1\rangle$. The quantum model is qubit state space \mathbb{C}^2 .

By applying a laser to the atom with the appropriate energy and direction and for the appropriate length of time, it is possible to move the electron from the ground $|0\rangle$ state to the excited $|1\rangle$ state and vice versa. The photon may then later be ejected and the qubit state will then be $|1\rangle$.

By reducing the time, the electron can be moved ‘halfway’ into the $|+\rangle$ state, or indeed into an arbitrary state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathbb{C}^2$.

A photon of light applied by the laser when the electron is in state

See [NC10, p280 Box 7.1] for some details of how this is physically achieved.

See Figure 1.2.

³See [NAo19, Ch7.6, pp309–324]

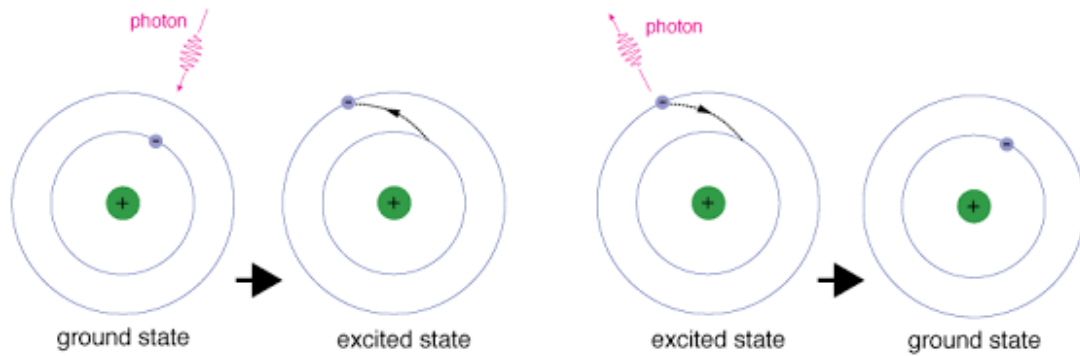


Figure 1.2: To “visualize” the electron in a quantum state which is a superposition between the ground and excited states, think of the photon itself not as a particle but as in a quantum superposition of staying and leaving.

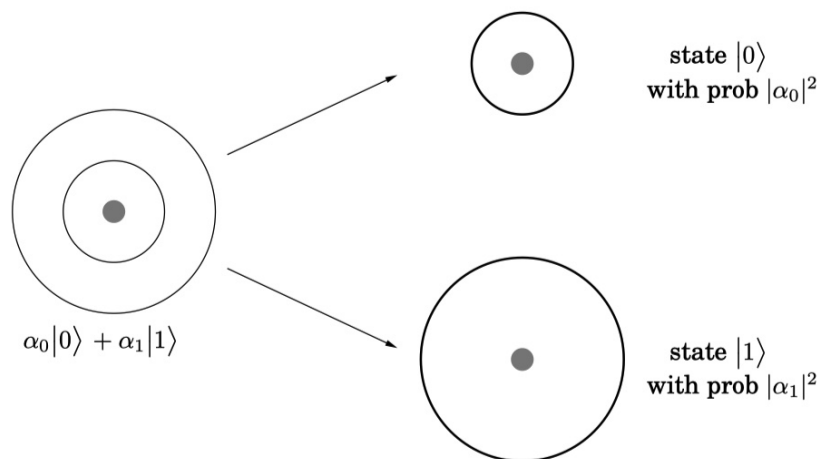


Figure 1.3: Measuring a qubit in superposition forces the qubit to move to either the ground or first excited state, with a probability given by $|\alpha_0|^2$ and $|\alpha_1|^2$ respectively.

1.1.3 Entanglement

1.1.4 Qubits and their Measurement

At least in principle, it is possible to learn the state of a classical bit either directly by indirectly by some observation or measurement process. Moreover, the measurement process can typically be unobtrusive in that it does not change the state of the bit.

The situation with qubits is completely different. The measurement process is determined by a choice of orthonormal basis in \mathbb{C}^2 . Without loss of generality and unless otherwise clear from context, we will normally take this to be the basis $\{|0\rangle, |1\rangle\}$. In quantum computing, the basis $\{|0\rangle, |1\rangle\}$ is called the *computational basis* and one speaks of measurement in the computational basis. For physical realisations of the measurement process see Section 1.1.6.

If the qubit being measured is in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ prior to measurement then after measurement it will be in either the state $|0\rangle$ or the state $|1\rangle$, with probabilities $|\alpha|^2$ and $|\beta|^2$ respectively. To be more precise, the new state will be the projection of $|\psi\rangle$ onto either the subspace spanned by $|0\rangle$ or the subspace spanned by $|1\rangle$; that is, will be either $\frac{\alpha}{\|\alpha\|}|0\rangle$ or $\frac{\beta}{\|\beta\|}|1\rangle$. Note that these probabilities are unchanged if $|\psi\rangle$ is multiplied by (what is called) a *global phase factor* $e^{i\theta}$.

The only information available as a result of the measurement process is knowledge of which of the two subspaces spanned by $|0\rangle$ or $|1\rangle$ was the projection subspace. (In physical implementations this is typically represented by a dial showing either 0 or 1 or some other appropriate labelling.)

The measurement process always involves some interference, if only through interaction with a single photon. Prior to measurement the qubit $|\psi\rangle$ is neither in state $|0\rangle$ nor in state $|1\rangle$, but is in a “superposition” of these two states. It is *not* correct to think that the qubit was in state $|0\rangle$ with probability $|\alpha|^2$ and in state $|1\rangle$ with probability $|\beta|^2$.

After measurement, it is no longer possible to obtain any further information about the state of the qubit prior to measurement. Also it is not possible to take copies of a qubit, as we will see in the “No-cloning” theorem. However, it is possible to produce an arbitrarily large number of qubits which

1.1.5 Qubits and Their Evolution

1.1.6 Physical Realisations of Qubits and their Measurement

1.2 Qubits (old)

1.2.1 Bits and Qubits

Bits: physical representations, states & mathematical model

A (classical) *bit*⁴ is the basic unit of information in computing, information theory, digital communications. A bit can take one of two values, typically 0 or 1 as in computing, but also true/false, yes/no, +/−, etc. These values are also called the possible *states* of the bit.

A bit has various physical realisations such as a bit in computer hardware or software, the presence or absence of a hole in punched computer cards of old, a switch being on or off, an electric current having one of two distinct voltages (high or low), etc.

Mathematically, a bit is modelled by the set $\{0, 1\}$ containing two distinct elements, and the state of the bit is then either 0 or 1. Often we abuse language and

- refer to the “bit 0” or the “bit 1”, rather than the state of the bit being 0 or 1,
- use the word “bit” both for the mathematical model and for various physical realisations.

⁴“Bit” is a contraction of “binary information digit”.

Qubits: states, mathematical model & physical realisations

A *quantum bit* or *qubit*⁵ is the basic unit in quantum computing. It is the quantum generalisation of a (classical binary) bit. It can take as its value/state any linear *superposition* of the form

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in \mathbb{C}^2, \quad \text{where } |\alpha|^2 + |\beta|^2 = 1, \alpha, \beta \in \mathbb{C}, \quad (1.3)$$

where $|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$. Note that $\{|0\rangle, |1\rangle\}$ is the standard/computational (orthonormal) basis for \mathbb{C}^2 . We can think of $|0\rangle$ and $|1\rangle$ as the two values 0 and 1 of a classical bit.⁶

The coefficients α and β are called *amplitudes*.

The notation $|\psi\rangle$ is due to Dirac. Dirac notation is discussed in Appendix D

Thus a qubit is a linear superposition of classical bits and is mathematically modelled by points on the unit sphere in \mathbb{C}^2 .⁷

To gain an intuitive understanding it is sometimes sufficient to take $\alpha, \beta \in \mathbb{R}$ in (1.3). In this case $-1 \leq \alpha, \beta \leq 1$ with $\alpha^2 + \beta^2 = 1$.

Treating qubits in a mathematical/abstract manner enables us to develop quantum theory in a manner independent of any particular physical realisation

Every two-state physical quantum system is a qubit. We will discuss three such realisations: the two lowest energy levels of an electron, linear polarisation of photons, and spin 1/2 particles. Quantum computers are/will be built from these and other physical realisations!

As previously for bits, we abuse language and

- refer to the “qubit $|\psi\rangle$ ”, rather than the state of the qubit being $|\psi\rangle$,
- use the word “qubit” both for the mathematical model and for various physical realisations.

1.2.2 State Space, Physical Reality and Measuring Qubits

Quantum Theory is truly weird, at least to our “classical” way of thinking.

1. Quantum states are “real”. For any unit vector $|\psi\rangle \in \mathbb{C}^2$ (*state space* for qubits) we can *prepare* multiple qubits in the state $|\psi\rangle$. Moreover, we can physically manipulate/transform these qubits into other qubits in a manner which corresponds to applying a prescribed unitary operator in \mathbb{C}^2 .
2. Given a classical bit, we can read/observe its state. This happens in a (classical) computer.

But for qubits this is not the case, the situation is completely different.

A measurement process for qubits corresponds to an orthonormal basis in \mathbb{C}^2 , also known as the *measurement basis*.⁸

- (a) If this measurement basis is $\{|0\rangle, |1\rangle\}$ and we measure one of the prepared qubits in the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, then it will give the value 0 with probability $|\alpha|^2$ and the value 1 with probability $|\beta|^2$. Moreover, after measurement the state will change/“collapse” to the state $|0\rangle$ in the first case and the state $|1\rangle$ in the second case.
- (b) In particular from (a), if the state after measurement is $|0\rangle$ then repeated applications of the same measurement of the qubit will continue (with probability 1) to give the state $|0\rangle$. Similarly for $|1\rangle$.
- (c) The qubit “decides” whether its value is 0 or 1 at the instant of measurement, and *not* prior to measurement.⁹

⁵“Qubit” — pronounced “q(ueue)bit” — is a contraction of “quantum bit”.

⁶This is consistent with the ket notation, where $|v\rangle$ is a vector with label v .

⁷This is not quite correct. Two vectors $|\phi\rangle$ and $|\psi\rangle$ on the unit sphere are said to be *equivalent* if $|\phi\rangle = e^{i\theta}|\psi\rangle$ for some $\theta \in \mathbb{R}$. Qubits correspond to *equivalence classes* of points on the unit sphere. In particular, $|\phi\rangle$ and $-|\phi\rangle$ denote the same qubit. We also sometimes refer to a non-zero vector $|v\rangle \in \mathbb{C}^2$ as a qubit. In this case we intend the normalised vector $\frac{|v\rangle}{\|v\|}$.

⁸This is not quite correct, there are more general measurement processes, but for present purposes this will suffice.

⁹With two or more *entangled* qubits the situation is more complex, as we discuss in Section 1.4.

- (d) More generally, suppose the measurement corresponds to the orthonormal basis $\{|u_1\rangle, |u_2\rangle\}$. After this measurement the state will change/collapse¹⁰ to one of these basis vectors, the “value” obtained will be the “label” u_1 or u_2 for this basis vector, and if $|\psi\rangle = \alpha_1|u_1\rangle + \alpha_2|u_2\rangle$ the respective probabilities will be $|\alpha_1|^2$ or $|\alpha_2|^2$. The obvious analogues of (a), (b) and (c) also hold.

In summary, orthonormal bases of qubit states are naturally associated with measurement processes, and conversely.

1.2.3 Superposition and Ensembles

Later we consider *ensembles*, probabilistic weightings of qubits such as $\mathcal{E} = \{(|0\rangle, p), (|1\rangle, q)\}$, where $0 \leq p \leq 1$, $0 \leq q \leq 1$ and $p^2 + q^2 = 1$. In this example the qubit is in the state $|0\rangle$ with probability p and in the state $|1\rangle$ with probability q .

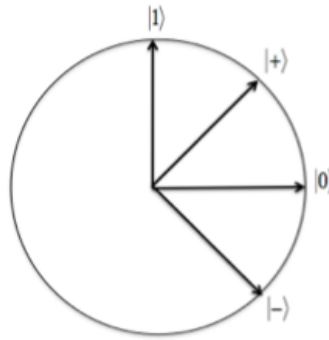


Figure 1.4: A section of \mathbb{C}^2 . (from [Vaz12])

The qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ is not the same as the ensemble $\mathcal{E} = \{(|0\rangle, |\alpha|^2), (|1\rangle, |\beta|^2)\}$. For example, let $\alpha = \beta = 1/\sqrt{2}$. Define¹¹

$$|+\rangle := \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle, \quad |-\rangle := \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle. \quad (1.4)$$

See Figure 1.4. Note $|\psi\rangle = |+\rangle$. Also see (2.2).

Measurements¹² of $|\psi\rangle$ and \mathcal{E} in the $\{|0\rangle, |1\rangle\}$ basis both give $|0\rangle$ or $|1\rangle$ with probability $1/2$. But measurement of $|\psi\rangle$ in the $\{|+\rangle, |-\rangle\}$ basis gives $|+\rangle$ with certainty and $|-\rangle$ with probability 0. On the other hand, for the ensemble \mathcal{E} measurement in the $\{|+\rangle, |-\rangle\}$ basis gives $|+\rangle$ and $|-\rangle$ each with probability $1/2$. *Exercise*

In the case of the ensemble \mathcal{E} , the state is either in state $|0\rangle$ or the state $|1\rangle$. We just do not know which. In the case of $|\psi\rangle$ the state is definitely *not* in either state $|0\rangle$ or $|1\rangle$. It is in a superposition of $|0\rangle$ and $|1\rangle$. It is also in a superposition of the states $|u_1\rangle$ and $|u_2\rangle$ for *any* orthonormal basis $\{|u_1\rangle, |u_2\rangle\}$. You will gain an intuition for this as we proceed.

1.2.4 The private world of qubits

A quantum state (or qubit) does not correspond to a physical state in the classical sense.

Qubits live in their own private \mathbb{C}^2 state space/world. This is a much “richer” world than the physical world it represents. The coefficients α_1 and α_2 in $|\psi\rangle = \alpha_1|u_1\rangle + \alpha_2|u_2\rangle$ contain information

¹⁰I think “collapse” can be misleading terminology. Every state can serve as one of the possible outcome states for *some* measurement. But on the other hand, there is only a restricted (for us — finite) set of possible outcomes for each given measurement.

¹¹These are important qubits.

¹²See the preceding discussion of measurement by projection. In the case of \mathcal{E} just treat each possibility $|0\rangle$ and $|1\rangle$ separately and weight with the appropriate probabilities, here $1/2$.

about the outcomes of measurement in the orthonormal basis $\{|u_1\rangle, |u_2\rangle\}$, as we saw in (d) above. But because, after measurement, the state of the qubit collapses to one of these basis vectors, the original state can no longer be “examined” by looking at that particular qubit.

But if someone sends us a large supply of identically prepared qubits $\alpha|0\rangle + \beta|1\rangle$, then we *can* obtain good estimates for $|\alpha|$ and $|\beta|$. *How?* In fact we can do considerably more than this, as we will later discuss.¹³

¹³If $\alpha = r_1 e^{i\theta_1}, \beta = r_2 e^{i\theta_2}$ in polar form, then we estimate $r_1 = |\alpha|^2$ and $r_2|\beta|^2$ by a simple frequency analysis on the outcomes of measurements in the $\{|0\rangle, |1\rangle\}$ basis. Although we cannot estimate θ_1 and θ_2 , we can estimate the relative phase $\theta_1 - \theta_2 \pmod{2\pi}$ by using measurements corresponding to orthonormal bases other than the standard basis. Physically, this is all that is relevant. We discuss this later.

1.3 Young's Two-Slit Experiment

(Optional) Bonus Material!

Young's experiment is the classic quantum experiment, so a brief discussion seems mandatory.

According to Richard Feynman:

...it contains the *only* mystery [in quantum theory]. We cannot make the mystery go away by “explaining” how it works. We will just *tell* you how it works. In telling you how it works we will have told you about the basic peculiarities of all quantum mechanics.

The essential element in the “telling” is the superposition principle. However, we will need to move a little beyond qubits to a different state space.

1.3.1 Experimental Set-Up and Outcomes

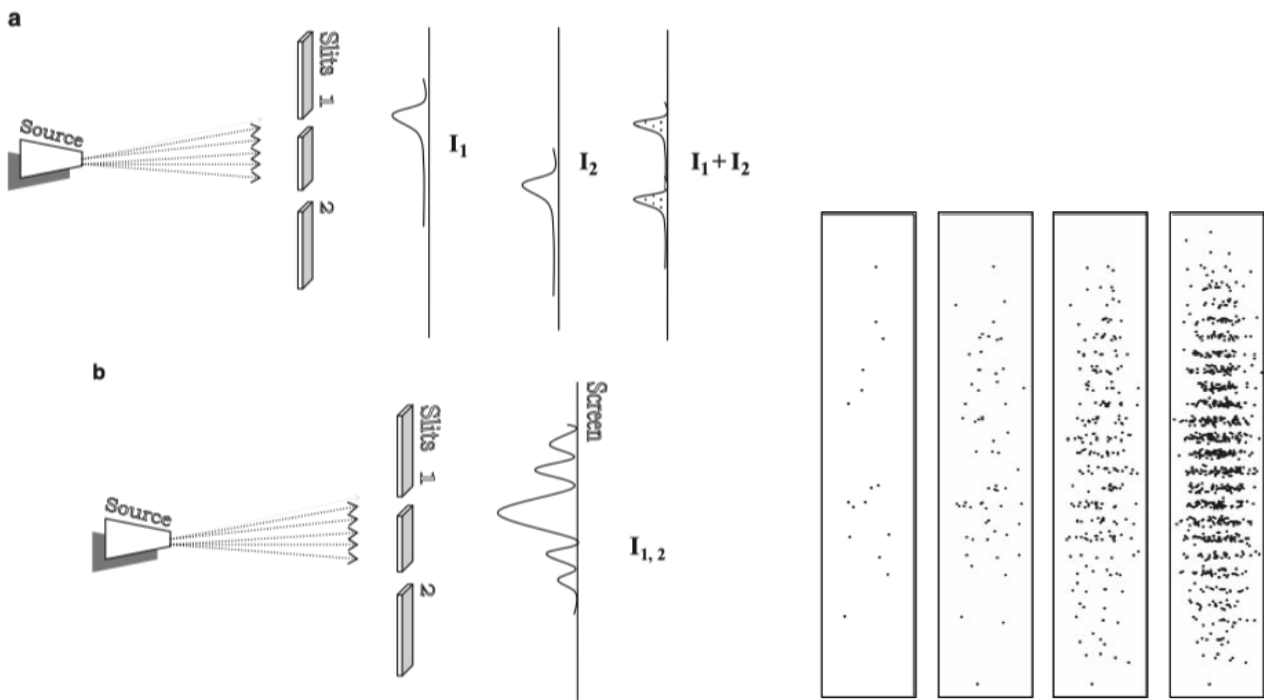


Figure 1.5: Double-slit experiment with photons/electrons or bullets. I_1 is the result *if* slit 2 is covered, I_2 is the result *if* slit 1 is covered. $I_1 + I_2$ is the result if both slits open and bullets are used, $I_{1,2}$ if photons/electrons are used ([GHW09, p 177]). The diagram on the right shows 16, 64, 256, 1024 photons strikes respectively ([SW10, p 9])

In Diagram **a** in Figure 1.5, photons/electrons or bullets are fired at a panel with two narrow slits of vertical width appropriate to the particles used. *If* slit 2 is covered those particles which are not absorbed by the panel, and so pass through slit 1, will concentrate on a screen behind the panel with an intensity in the vertical direction according to the approximately normal distribution I_1 . The dispersion is caused by interaction with the edges of the slit. Similarly, *if* slit 1 is blocked the intensity is given by I_2 .

With photons or electrons, however, the situation is quite different. If both slits are open the intensity is given by $I_{1,2}$ as in Diagram **b**. This is similar to the interference pattern obtained if a steady water wave pattern is sent towards the panel, as in Figure 1.6. The peaks of the circular waves interfere constructively, as do the troughs, to give maximum intensity (squared amplitude) along the

red lines. (The intensity peaks decrease as one moves away from the point on the screen opposite midway between the two slits.) In between peaks and troughs one obtains destructive interference.

Moreover, with photons or electrons one obtains the same interference pattern even if the photons/electrons are fired one at a time. Each electron/photon is exhibiting a wave pattern of self interference. This is very weird!

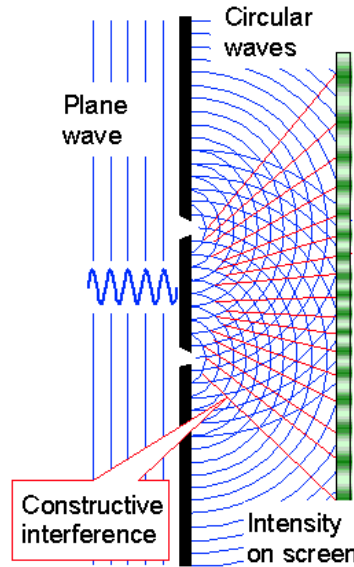


Figure 1.6: Water waves. Peaks of the circular waves (in blue) interfere additively along the red lines and destructively in between. (from https://www.tf.uni-kiel.de/matwis/amat/iss/kap_4/illustr/s4_2_2.html)

1.3.2 The State Space

To simplify matters, imagine the screen is divided into many small regions R_x , each of which is denoted by some point $\mathbf{x} = (x, y) \in R_x$. See Figure 1.7.

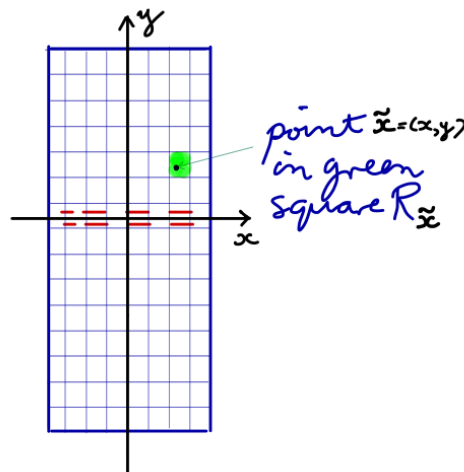


Figure 1.7: Screen as in Figure 1.5. (The dotted red lines are just to indicate that they are directly behind the two slits on the front panel.)

The possible outcomes of a particle striking the screen are given by the N possible values of \mathbf{x} .¹⁴

¹⁴So $N = 8 \times 15 = 120$ here!

Striking the screen is the measurement process. The outcomes are *mutually exclusive and regarded as exhaustive* in our set-up. For these reasons we take the state space model for a particle just prior to striking the screen to be an N -dimensional complex inner product space, not \mathbb{C}^2 as for qubits, with an orthonormal basis consisting of vectors $|\mathbf{x}\rangle$. Without loss of generality we can use \mathbb{C}^N with the standard basis vectors.

Just as an arbitrary qubit can be written $\alpha|0\rangle + \beta|1\rangle$, here the state of an arbitrary particle just prior to impacting the screen will be a superposition

$$|\psi\rangle := \sum_{\mathbf{x}} \alpha(\mathbf{x}) |\mathbf{x}\rangle, \quad \sum_{\mathbf{x}} |\alpha(\mathbf{x})|^2 = 1. \quad (1.5)$$

In particular, for a particle (electron or photon) which we *know* passed through slit j (for example, if the other slit was closed), the state will be a *unit* vector $|\psi_j\rangle \in \mathbb{C}^N$ which we write as

$$|\psi_j\rangle := \sum_{\mathbf{x}} \alpha_j(\mathbf{x}) |\mathbf{x}\rangle, \quad \alpha_j(\mathbf{x}) = |\alpha_j(\mathbf{x})| e^{i\phi_j(\mathbf{x})} \quad \text{with} \quad \sum_{\mathbf{x}} |\alpha_j(\mathbf{x})|^2 = 1. \quad (1.6)$$

The probability $p_j(\mathbf{x})$ that such a particle will arrive in $R_{\mathbf{x}}$ can be measured by repeated such experiments. It is given by $p_j(\mathbf{x}) = |\alpha_j(\mathbf{x})|^2$ according to the analogue of the discussion in Section 1.2.2, and thus $|\alpha_j(\mathbf{x})|$ can be estimated in this manner. The phase of the particle just prior to arriving at $R_{\mathbf{x}}$ is denoted by $\phi_j(\mathbf{x})$. Writing $\mathbf{x} = (x, y)$ in cartesian coordinates, where $y = 0$ is the vertical height corresponding to midway between the slits, $p_j(\mathbf{x} = (x, y))$ is a discrete approximation to a distribution which is a product of a normal distribution in y centred at height corresponding to slit j , and a constant distribution in the x (horizontal) direction for an interval roughly the length of each slit. See I_1, I_2 in Figure 1.5, showing the y dependence. The distributions I_1, I_2 are displaced vertically from each other by the distance between the two slits.

Suppose we fire electrons or photons at the panel and consider only those that are not blocked by the panel but pass through the slits and register in some way on the screen to the right in Figure 1.5. (Note that I said pass through the slits, *not* “pass through *one of* the slits”!!) Provided there was no measurement which would have enabled us to know if the particle passed through slit 1 (and equivalently in this case no measurement that would have enabled us to know if the particle passed through slit 2), the state space at any time after the particle has passed through the slits allows for both possibilities. One should *not* think: “the particle actually passed through one or the other slit but we just do not know which”.

Let s be the distance between the two slits, L the distance between the panel and the screen, and λ the wave length of the particle. The state of the particle in these circumstances just prior to striking the screen, for $L \gg s$, is approximately the equal superposition¹⁵

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|\psi_1\rangle + |\psi_2\rangle). \quad (1.7)$$

¹⁵This is not surprising, but to argue it more carefully requires considering a larger state space involving the slits. This is done, for example, in [FLS65, Vol III, Chapter 2, §§3-1,3-2]. Alternatively, it is an example of a general principle for superposition of amplitudes in such situations, see for example [GHW09, p 176].

Finally, it may seem surprising that $1/\sqrt{2}$ is the correct normalisation factor to ensure $\| |\psi\rangle \| = 1$. But note $\langle \psi | \psi \rangle = 1 + \langle \psi_1 | \psi_2 \rangle$ and $\langle \psi_1 | \psi_2 \rangle \approx 0$ due to the highly oscillatory behaviour of $\cos(\phi_1 - \phi_2)$. To pursue this point a little further,

$$\begin{aligned} \langle \psi_1 | \psi_2 \rangle &= \sum_{\mathbf{x}} r_1(\mathbf{x}) r_2(\mathbf{x}) \cos(\phi_1(\mathbf{x}) - \phi_2(\mathbf{x})) \\ &\approx \int r_1(y) r_2(y) \cos(\phi_1(y) - \phi_2(y)) dy \quad \text{where } \mathbf{x} = (x, y) \text{ and ignoring “constant” } x \text{ dependence of everything} \\ &\approx \int r_1(y) r_2(y) \cos\left(\frac{sy}{\lambda L}\right) dy \quad \text{from (1.10)} \\ &= -\frac{\lambda L}{s} \left(\int \frac{d}{dy} (r_1(y) r_2(y)) \sin\left(\frac{sy}{\lambda L}\right) dy + \text{boundary terms} \right). \end{aligned}$$

Since $\lambda \ll s$, this last term is, in effect, bounded in absolute value by constant $\times \lambda$.

Fixing \mathbf{x} and writing $\alpha_j(\mathbf{x}) = r_j e^{i\phi_j}$ in polar coordinates, the coefficient/amplitude of $|\mathbf{x}\rangle$ in $|\psi\rangle$ is

$$\frac{1}{\sqrt{2}}(\alpha_1(\mathbf{x}) + \alpha_2(\mathbf{x})) = \frac{1}{\sqrt{2}}(r_1 e^{i\phi_1} + r_2 e^{i\phi_2}), \quad (1.8)$$

and so the probability of the particle landing at \mathbf{x} is

$$\begin{aligned} \frac{1}{2} |r_1 e^{i\phi_1} + r_2 e^{i\phi_2}|^2 &= \frac{1}{2} (r_1 e^{i\phi_1} + r_2 e^{i\phi_2}) (r_1 e^{-i\phi_1} + r_2 e^{-i\phi_2}) \\ &= \frac{1}{2} (r_1^2 + r_2^2) + r_1 r_2 \cos(\phi_1 - \phi_2) \end{aligned} \quad (1.9)$$

The term $\frac{1}{2} (r_1^2 + r_2^2)$ is the probability of arriving in $R_{\mathbf{x}}$ for the *mixed* state corresponding to equal probabilities of passing through slit 1 and slit 2. The second term $r_1 r_2 \cos(\phi_1 - \phi_2)$ is the *interference term* which has a magnitude comparable to the first term but may be *additive or subtractive*.

It is not difficult to show¹⁶ that, for $s, y \ll L$, the distance between stripes in Figure 1.5 is approximately $\lambda L/s$ and

$$\phi_1(\mathbf{x}) - \phi_2(\mathbf{x}) \approx 2\pi \frac{sy}{\lambda L}, \quad (1.10)$$

This can also be used to estimate the wave length of the particles.

Remark *The fact that for the superposition of mutually exclusive events (in this case: passing through slit 1 and passing through slit 2) amplitudes add but probabilities do not, is critical to the weirdness of quantum events.*

¹⁶The distance from the bottom/top slit to the point on the screen at height y , for $s, y \ll L$, is

$$\left(L^2 + \left(y + \frac{s}{2}\right)^2\right)^{1/2} \approx L + \frac{1}{2}L^{-1} \left(y \pm \frac{s}{2}\right)^2,$$

and so the difference is $\approx sy/L$. The waves radiating out from the two slits are in phase at $y = 0$ and the next values of y for which the two waves will be in phase are given by $sy/L = \pm\lambda$, i.e. $y = \pm L\lambda/s$. Also see [BS14, p 43, §2.3.4].

Thus the distance between bands on the right of Figure 1.5 is $\approx L\lambda/s$, and so $\phi_1(\mathbf{x}) - \phi_2(\mathbf{x}) \approx 2\pi \frac{sy}{\lambda L}$.

1.4 Entangled Pairs of Qubits

1.4.1 Quantum states for pairs of qubits

We have seen how the quantum analogue of a bit with values in $\{0, 1\}$ is a qubit whose state can be any linear combination, i.e. superposition, of the *orthonormal* vectors $|0\rangle$ and $|1\rangle$ in (the unit sphere for) \mathbb{C}^2 .

Similarly, we can consider a pair of bits and the quantum analogue of a pair of qubits. For classical bits the 4 possible values of a pair of bits are $\{00, 01, 10, 11\}$ ¹⁷. In quantum mechanics these values correspond to the following *orthonormal* unit vectors in (the unit sphere for) \mathbb{C}^4 .

$$\{00\} \rightarrow |00\rangle := \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad \{01\} \rightarrow |01\rangle := \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \quad \{10\} \rightarrow |10\rangle := \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad \{11\} \rightarrow |11\rangle := \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}. \quad (1.11)$$

Mathematically, the set of all possible unit length superpositions of the four basis vectors in (1.11) is the set of all vectors/states on the unit sphere in \mathbb{C}^4 which are of the form

$$|\psi\rangle := a_{00}|00\rangle + a_{01}|01\rangle + a_{10}|10\rangle + a_{11}|11\rangle \in \mathbb{C}^4, \quad \text{where } a_{ij} \in \mathbb{C}, \quad \sum |a_{ij}|^2 = 1. \quad (1.12)$$

It is physically possible to produce pairs of qubits corresponding to any such state! This has very counterintuitive consequences.

A typical measurement basis for states in \mathbb{C}^4 uses the standard basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. This measurement is physically achieved by separate measurements on the first and second qubits, although as noted above the two qubits may be in highly separated locations.¹⁸ The squared moduli of the coefficients in (1.12) give the probabilities of the possible experimental outcomes, in a way analogous to what happens for a single qubit as discussed in Section 1.2.2. The way we read off this information is straightforward but the consequences are very weird indeed. We will discuss this for the example of the Bell state (1.14).

1.4.2 Separable qubits and entangled qubits

We can easily produce pairs of qubits of the form $\alpha|0\rangle + \beta|1\rangle$ and $\alpha'|0\rangle + \beta'|1\rangle$ respectively, which leads naturally to pairs of qubits which can be written in the product form

$$(\alpha|0\rangle + \beta|1\rangle)(\alpha'|0\rangle + \beta'|1\rangle) = \alpha\alpha'|00\rangle + \alpha\beta'|01\rangle + \beta\alpha'|10\rangle + \beta\beta'|11\rangle \in \mathbb{C}^4. \quad (1.13)$$

However, not every pair of qubits in the form (1.12) can be written in the form (1.13).

If a state can be factorised as in (1.13) it is said to be *separable*, if not it is said to be *entangled*.

1.4.3 The Bell state

A particularly instructive example of an entangled pair of qubits is the *Bell state*

$$|\Phi^+\rangle := \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle \in \mathbb{C}^4. \quad (1.14)$$

Exercise: Show the Bell state is entangled.

It is possible to physically produce many examples of the Bell state, for example where the pair of qubits is a pair of entangled polarised photons. Even though the two qubits in the Bell state (1.14) are entangled, it is possible to physically separate them by over 1,200 km, and in principle by any distance. See Section 1.5.

¹⁷It is conventional to list values in increasing binary order.

¹⁸Not all measurements can be achieved this way. The issue is whether or not the measurement is factorisable in the tensor sense, as we discuss in subsequent chapters.

The $\frac{1}{\sqrt{2}}$ coefficient in the Bell state for the $|00\rangle$ component and the implicit 0 coefficient for $|01\rangle$ together imply that when the first qubit is measured in the standard basis $\{|0\rangle, |1\rangle\}$ the result is 0 with probability $(1/\sqrt{2})^2 + 0^2 = 1/2$, and in this case the first qubit moves into the state $|0\rangle$. Similarly, the measurement result is 1 with probability¹⁹ $1/2$, and in this case the first qubit moves into the state $|1\rangle$.

Suppose the measurement outcome for the first qubit is 0. **The most astounding consequence is that the qubit pair instantaneously moves/collapses to the state $|00\rangle$, and as a consequence the second qubit instantaneously moves into the state $|0\rangle$.**²⁰ In effect, this conclusion is obtained by scratching out the $|11\rangle$ term in (1.14) (since it begins with 1 but the first qubit is actually in the state $|0\rangle$) and then normalising

¹⁹By “probability” we just mean what occurs over many experiments in a frequency analysis.

²⁰As we discuss later, using tensor notation $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \in \mathbb{C}^2 \otimes \mathbb{C}^2 = \mathbb{C}^4$, and orthogonal projection onto $\text{span}\{|0\rangle\} \otimes \mathbb{C}^2$ gives $|00\rangle$ after normalisation. That is, just scratch out any terms beginning with $|1\rangle$ and then normalise.

1.5 The EPR Paradox

1.5.1 What does it mean for quantum theory to be complete?

Einstein, Podolsky and Rosen in [EPR35] argued that quantum theory is not a complete theory. They accepted that in most quantum experiments conducted up to that time the results predicted were probabilistic, perhaps due to some random interaction with the measuring apparatus or for some other reason. This was *not* the situation they were addressing.

On the other hand, they pointed out that in certain experiments which involve entanglement (at that time thought experiments, i.e. “Gedankenexperiment”, but subsequently experimentally realised in [ADR82]), the outcome *was* determined before the measurement was conducted but quantum theory did not include this information. It was in this sense that they claimed quantum theory was not complete.

I describe the [EPR35] argument in the context of entangled qubits in the Bell state (1.14) and the 2017 Micius experiment [YCL⁺17] illustrated in Figure 1.8 (and named after the Chinese philosopher Micius or Mozi: <https://en.wikipedia.org/wiki/Mozi>).

1.5.2 The EPR Experiment

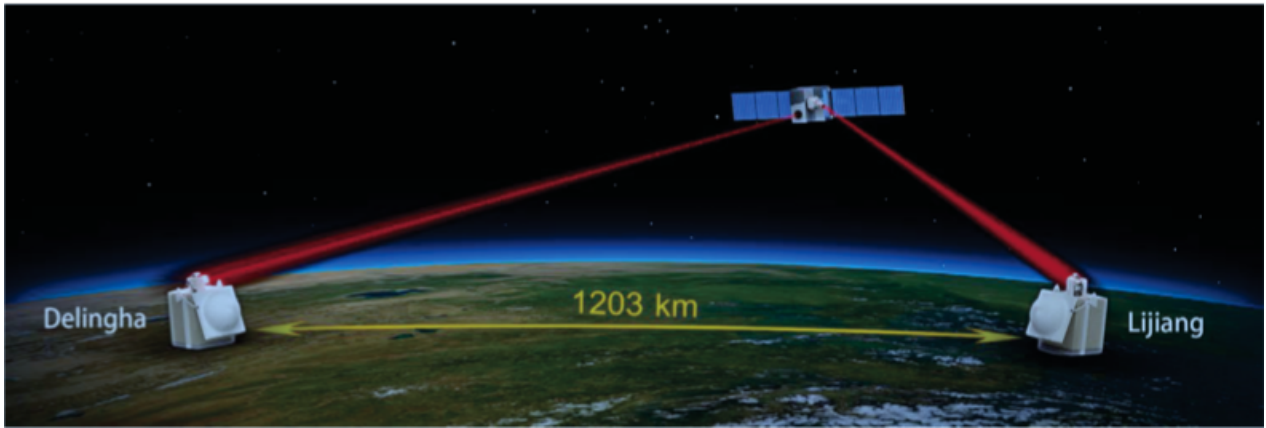


Figure 1.8: Experimental set-up of satellite-based entanglement distribution. (Arxiv version of [YCL⁺17])



Figure 1.9: Schematic representation of EPR set-up (from [RP11]). Alice and Bob are spacelike separated at measurement time. Alice and Bob are traditionally responsible for the measurements in such experiments. (From the list of authors and affiliations in [YCL⁺17] it seems unlikely either was present on this occasion.)

A pair of qubits realized as linearly polarized photons have their polarizations entangled on the

satellite into the Bell state $\frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$.²¹ After entanglement the first qubit is sent to Lijiang and the second to Delingha Lijiang. Suppose each qubit is measured in the $\{|0\rangle, |1\rangle\}$ basis immediately upon arrival.²² In the diagram, this means the Lijiang qubit before the Delingha qubit.

Suppose for sake of discussion that the first qubit arrives in Lijiang and is measured before the second qubit arrives in Delingha and is measured, but the second qubit arrives and is measured before there is time for any message (at the speed of light) to reach it regarding the measurement outcome of the first qubit. Each evening pass of the satellite produces about 300 such events.

From the previous discussion concerning the Bell state the probability of the first qubit being measured as 0 is $1/2$, of the second qubit being measured as 0 is $1/2$, and of the pair being measured as 00 is $1/2$. So the measurement results of the individual qubits are not independent, since if they were then the probability of the pair being measured as 00 would be $1/4$, and the state of the qubit pair would be the product state $\frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle \in \mathbb{C}^4$, not the Bell state. In fact the measurement outcomes of the two qubits are *perfectly correlated*, both outcomes being 0 or both being 1.

How is this perfect correlation “enforced”? Quantum theory implies the first qubit measures as 0 with probability $1/2$, as 1 with probability $1/2$, but the “decision” as to *which* of these two outcomes is the case is made at the time of measurement. For sake of argument suppose the first qubit measure as 0 — how does the second qubit know that it must also measure as 0 if it is to be consistent with the quantum theory prediction of equality of outcome?

Logically there are two possibilities:

- (a) *either* there is an interaction between the two qubits faster than the speed of light (what Einstein called “spooky action at a distance”), such that the second qubit “knows” the measurement outcome for the first qubit,
- (b) *or* there was no such interaction. In this case information about *which* one of the two shared/common outcomes will occur for an entangled pair must have been available to each particle in the pair at the time of entanglement (the last possible time for slower than speed of light interaction before measurement).

In the case of (b) this additional information is not present in the Bell state, and so quantum theory would not be a complete theory according to [EPR35].

By way of background we remark that there is indeed a simple classical model to completely explain the outcome of the version of the EPR experiment as discussed here. All that is needed is that at the time of entanglement both qubits are produced in the state $|0\rangle$ or both in the state $|1\rangle$, with probability $1/2$ for each possibility, and this choice is independent between pairs of qubits.

The difference between this model and the Bell state model shows up if we measure the individual qubits in other than the orthonormal base $\{|0\rangle, |1\rangle\}$, as we will discuss in a later section. This was done in the Micius and earlier experiments.

1.5.3 Quantum theory *is* complete

[EPR35] considered (a) to not be possible, and so came to the conclusion that (b) is true and quantum theory is *not* complete. Einstein spent much of the remaining 20 years of his life looking for such a complete theory.

However, John Bell in [Bel64] designed an experiment to decide between (a) and (b). A small modification was proposed in [CHSH69] and carried out in [ADR82], with the most recent experiment being the Micius experiment [YCL⁺17]. This has shown convincingly that quantum theory is complete, any probabilistic or deterministic extension which includes other information (known as “hidden variables”) implies correlations which are experimentally incorrect, and “spooky action at a distance” is indeed what happens.

²¹In the actual experiment the Bell state $\frac{1}{\sqrt{2}}|01\rangle - \frac{1}{\sqrt{2}}|10\rangle$ was used. This does not alter the discussion in any significant manner.

²²A more complicated experiment was conducted with additional orthonormal bases. We return to this in later discussions.

The idea that an event can be influenced by an event outside its past light cone certainly goes against our classical intuition. It is worth remarking, however, that no *classical* information is transmitted faster than the speed of light in these cases! We will return to this later in these notes.

Chapter 2

Quantum Postulates for Closed Systems

Contents

2.1 State Space	25
2.1.1 State Space Postulate	25
2.1.2 Three Physical Realisations of Qubits	26
2.2 Measurement	29
2.2.1 Measurement Postulate (Orthonormal Basis Version)	29
2.2.2 Measuring Qubits	30
2.2.3 Distinguishing Relative Phase	30
2.2.4 Hermitian Operators and Measurements	31
2.2.5 Measurement Postulate (Hermitian Operator Version)	32
2.2.6 Pauli Matrices and Measurement	33
2.3 Qubits and Spin 1/2 Particles	35
2.3.1 Spin-Orientation	35
2.3.2 Stern-Gerlach Experimental Set-Up	35
2.3.3 Multiple Particles with the same Spin-Orientation	36
2.3.4 Spin-Orientation and Qubit Correspondence: Bloch Sphere Map	37
2.3.5 Spin-Orientation and Qubit Correspondence: Physical Justification	37
2.4 Evolution	38
2.4.1 Evolution Postulate (Discrete Version)	38
2.4.2 Examples of Unitary Gates	38
2.4.3 Evolution Postulate (Continuous Version)	39
2.4.4 Solution of Schrödinger's Equation	39
2.4.5 Hamiltonian Example	39
2.5 Composite Systems	41
2.5.1 Pairs of Qubits and Bipartite States	41
2.5.2 Composite System Postulate	41
2.5.3 N -Qubit Space	41
2.5.4 Inner Product for Composite Systems	42
2.5.5 Entangled Qubit Pairs	43
2.5.6 Bell States	44

In this chapter we begin anew. The material in Chapter 1 may be considered as motivation for the more careful treatment here and we refer back to it occasionally.

The quantum postulates provide the framework for all of Quantum Theory. They are essentially due to Paul Dirac (1930) [Dir58] and John Von Neumann (1932) [vN18].

We mainly discuss the case of finite dimensional state spaces. This is what is needed for quantum computation. In addition, all the counterintuitive quantum weirdness is already present in this setting.

In this chapter we only deal with closed systems, or more precisely, systems that can be approximated by closed systems. See Remark 2 in Section 2.1.1.

The goal is to obtain an understanding of the postulates and how to apply them.

You should now read Appendices F.1 and F.2 on the Bloch sphere as they are used in the discussion of qubit measurement in Section 2.2 and provide a nice way of representing and thinking about qubits.

Throughout these notes, bases are always orthonormal unless otherwise clear.

2.1 State Space

2.1.1 State Space Postulate

Postulate 1. *Associated to any closed physical system is a complete separable¹ complex inner product space V (that is, a Hilbert space) known as the state space of the system. The system at each time is completely described by its state vector at that time, which is a unit vector in the system's state space.*

Examples

In particular, \mathbb{C}^2 is the state space for qubits. See Section 1.2.1 for some context concerning bits and qubits.

The state of a *qubit* is given by a unit vector in the state space \mathbb{C}^2 . Sometimes a qubit state is taken to be the equivalence class of unit vectors which are equal up to multiplication by an arbitrary global phase factor $e^{i\zeta}$. See Remark 3 below.

Often we say “the qubit $|0\rangle$ ” rather than the “the qubit with state/value $|0\rangle$ ”, just as we say “the bit 0” rather than “the bit with value/state 0”, etc.

Important examples of qubits are² the basis vectors

$$|0\rangle := \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle := \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad (2.1)$$

and

$$\begin{aligned} |+\rangle &:= \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle, & |-\rangle &:= \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle, \\ |i\rangle &:= \frac{1}{\sqrt{2}} |0\rangle + i \frac{1}{\sqrt{2}} |1\rangle, & |-i\rangle &:= \frac{1}{\sqrt{2}} |0\rangle - i \frac{1}{\sqrt{2}} |1\rangle. \end{aligned} \quad (2.2)$$

Each of these three pairs is an orthonormal basis for \mathbb{C}^2 . *Exercise.*

A 3-level quantum system is represented by \mathbb{C}^3 . State vectors in \mathbb{C}^3 are the standard basis vectors, usually denoted $|0\rangle$, $|1\rangle$, $|2\rangle$, and more generally are unit vectors:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle + \gamma|2\rangle \in \mathbb{C}^3, \quad \text{where } |\alpha|^2 + |\beta|^2 + |\gamma|^2 = 1, \quad \alpha, \beta, \gamma \in \mathbb{C}. \quad (2.3)$$

Similarly one uses \mathbb{C}^n for n -level systems.

¹finite dimensional spaces are always complete and separable

²“:=” means “by definition is equal to”.

Remarks

1. We only consider *finite dimensional* state spaces V , usually \mathbb{C}^n for some $n \geq 2$. This is sufficient both for quantum computation and quantum information purposes (and for understanding all the notions of “quantum weirdness”).³
2. An *isolated* or *closed* system is one which does not exchange any information, matter or energy with any other environment. This is an idealisation and there are no closed systems, except possibly for the universe itself.⁴
3. There is no physically observable difference between the physical system described by $|\psi\rangle$ and that by $e^{i\zeta}|\psi\rangle$, see Section 2.2.⁵ We call $e^{i\zeta}$ a *global phase factor*. The two vectors $|\psi\rangle$ and $e^{i\zeta}|\psi\rangle$ are said to be equivalent. To be more precise we should say that:
a state is given by an equivalence class of unit vectors.
 We later discuss *relative phase*, which is different and *is* physically significant. See Section 2.2.3.
4. Unit vectors in the state space are usually written in the ket form $|\psi\rangle$ using the Dirac notation, see Appendix D. It is usually convenient to think of ψ itself as a name or symbol representing the actual vector $|\psi\rangle$, as in the case $|0\rangle$ and $|1\rangle$.
5. As we discussed in Chapter 1, a state space in quantum theory describes physical reality in a very different manner than a state space in classical physics describes physical reality. See Section 2.2.
6. We will see in Section 2.2 that mutually exclusive outcomes of a measurement correspond to orthonormal vectors in state space. Mutually exclusive *and* exhaustive outcomes correspond to an orthonormal *basis*.

2.1.2 Three Physical Realisations of Qubits

Please look at Appendices F.1 and F.2 for the Bloch Sphere representation of qubits.

Every qubit $|\psi\rangle \in \mathbb{C}^2$, up to multiplication by a physically irrelevant phase factor $e^{i\zeta}$, can be written in the form

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\phi} |1\rangle, \quad 0 \leq \theta \leq \pi, \quad 0 \leq \phi < 2\pi, \quad (2.4)$$

and this corresponds to a unique point on the *Bloch sphere*, the unit sphere $S^2 \subset \mathbb{R}^3$ with spherical coordinates (θ, ϕ) .

Every two-level quantum system corresponds to a qubit. Here are three examples that are useful to keep in mind when dealing more abstractly with qubits. In [NC10, p. 278, Fig. 7.1] the authors list eight possible realisations of quantum bits for quantum computing, but as they note these are all variants of three fundamentally different examples: charge/energy, photon/polarisation and spin.

As with any quantum state, the energy level/polarisation/spin is not determined prior to measurement and until then the value measured/observed after measurement is only predicted probabilistically from the prior state and the particular measurement used.⁶

We give a more detailed discussion of the physical interpretation of qubit states $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and their measurement outcomes in the case of spin 1/2 in Section 2.3.

³In quantum mechanics we generally need a separable infinite dimensional Hilbert space. In this case the analogue of the state vector, such as for the position of a particle in physical space \mathbb{R}^3 , is a complex valued (“wave”) function defined over \mathbb{R}^3 and typically “peaking” at some point in \mathbb{R}^3 . Informally, the wave function is a complex superposition of Dirac measures, one at each point in \mathbb{R}^3 .

⁴And what is *the* universe? Quantum entanglement implies we need to consider events that will not come into our past light cone until some time in our future.

⁵Thus the state space is really a complex projective space, but this is usually not the most convenient/intuitive way to think about it.

⁶If the measurement is with respect to that same state as discussed in Section 2.2 then the probability is 1 and so we do have an outcome with certainty.

For further information on the physical realisation of qubits, their evolution, measurement and entanglement, directed more to mathematicians rather than physicists and experimentalists, see [CCEZ03] and particularly [ZCDH09].

The following diagrams are, of course, schematic only.

Energy levels of an electron in an atom

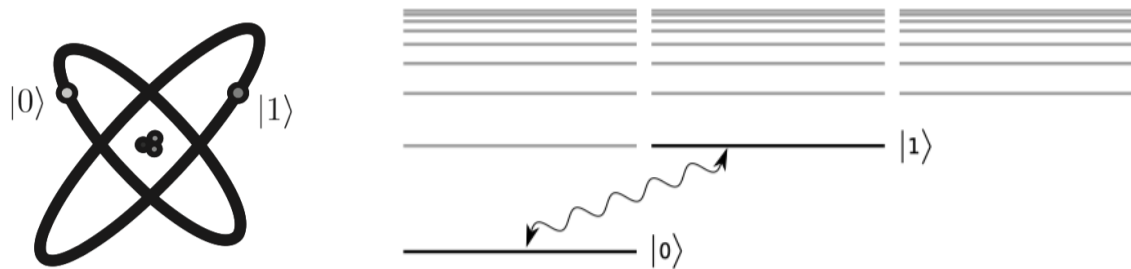


Figure 2.1: Electron energy levels of an electron in an atom. ([NC10, p14 Fig 1.2], [Vaz12, Notes Ch 1])

It is often possible to effectively limit an electron in an atom to its two lowest energy levels and to produce electrons in any (complex) superposition of these levels. The quantum model is thus qubit state space \mathbb{C}^2 . The lowest energy level state is denoted by $|0\rangle$ and the next level by $|1\rangle$.

By shining light on the atom with the appropriate energy and for the appropriate length of time, it is possible to move the electron from the $|0\rangle$ state to the $|1\rangle$ state and vice versa. By reducing the time we shine the light, an electron initially in the state $|0\rangle$ can be moved ‘halfway’ into the $|+\rangle$ state.

See [NC10, p280 Box 7.1] for details of how this is physically achieved.

Polarised photon

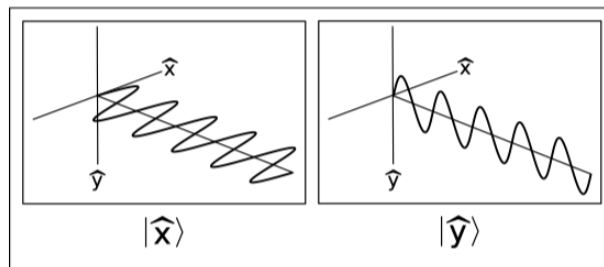


Figure 2.2: Horizontal and vertical polarisation of light. ([Vaz12, Lecture Notes Chapter 1])

Individual photons have a polarisation modelled by qubit state space \mathbb{C}^2 . The qubits $|0\rangle$ and $|1\rangle$ are conventionally assigned to horizontal and vertical linear polarisation in the plane orthogonal to the direction of propagation. See Figure 2.2.

By means of a horizontally polarised filter it is possible to produce a large supply of horizontally polarized photons which are conventionally assigned the qubit state $|0\rangle$. Similarly for $|1\rangle$. To achieve other states one passes the photons through a mixture of mirrors, phase shifters and beamsplitters. A phase shifter is a transparent slab which shifts the phase by an amount depending on the thickness and transparency of the slab.

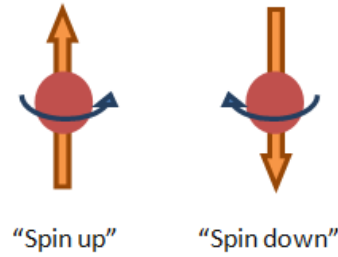


Figure 2.3: Schematic representation of spin 1/2 particle. Spin up = $|0\rangle = |\uparrow\rangle$, Spin down = $|1\rangle = |\downarrow\rangle$. (<http://www.sussex.ac.uk/physics/iqt/research/researchers/simulation.html>)

Spin 1/2 particle

All protons, neutrons, electrons, neutrinos, quarks, and certain atoms such as hydrogen and silver, have a property called *spin* 1/2⁷ which, after measurement in any direction in \mathbb{R}^3 , takes one of two values, typically denoted by $1/2$ and $-1/2$,⁸ or by \uparrow (spin up, i.e. “right hand thumb rule in the direction of the measuring device”) and \downarrow (spin down, i.e. “right hand thumb rule in the opposite direction from the measuring device”). See Figure 2.3.

In this case each possible state of the qubit corresponds to a unit vector giving the “alignment” of the spin in \mathbb{R}^3 . We discuss this in some detail in Sections 2.3 and 2.3.5.

⁷This is 2-state spin, which is the most common, but n states for any larger integer n are allowed in principle.

⁸The particular values $\pm 1/2$ are chosen essentially because they should sum to 0 from total spin conservation requirements, and they should differ by 1 in an appropriate system of units.

2.2 Measurement

2.2.1 Measurement Postulate (Orthonormal Basis Version)

Recall that we are only considering finite dimensional state spaces.

Postulate 2 (Preliminary version). *Each orthonormal basis $\{|v_1\rangle, \dots, |v_n\rangle\}$ for the state space V describes a measurement/observation as follows. If the state before measurement is*

$$|\psi\rangle = \alpha_1 |v_1\rangle + \dots + \alpha_n |v_n\rangle$$

then the state after measurement is $|v_j\rangle$ with probability $|\alpha_j|^2 = |\langle v_j | \psi \rangle|^2$. In this case we say the outcome is (the label) v_j or (the state) $|v_j\rangle$.

Remarks

1. *Notation:* See Appendix D.1. In particular, $\langle v_j | \psi \rangle$ is the inner product of $|v_j\rangle$ with $|\psi\rangle$.
2. The *projection* of $|\psi\rangle$ onto $\text{Span } |v_j\rangle$ is $\alpha_j |v_j\rangle$. When normalised to have norm 1 this gives $\frac{\alpha_j}{|\alpha_j|} |v_j\rangle$. Note that $|v_j\rangle$ and $\frac{\alpha_j}{|\alpha_j|} |v_j\rangle$ represent the same state since they agree up to the global phase factor $\frac{\alpha_j}{|\alpha_j|}$.

It is often more convenient to think of the state after measurement in this way, that is, as the normalised state after projection onto the subspace $\text{Span } |v_j\rangle$. See Appendices B.1.5 and D.3.2 for a discussion of orthogonal projections. In particular, it is then clear that changing any or some of the basis vectors $|v_j\rangle$ by a phase factor $e^{i\zeta_j}$ (which of course includes -1) does not change the probabilities or the possible final states.

3. Since $e^{i\theta} |\psi\rangle = \sum_i (e^{i\theta} \alpha_i) |v_i\rangle$ it follows from Postulate 2 that the probability of each outcome, and the state after this outcome, are invariant under multiplication of $|\psi\rangle$ by the global phase factor $e^{i\theta}$.
4. You might like to think of the outcome as a mark v_j on a screen, or a number that shows on a dial, there being only a finite number n of possibilities in the situations we are considering. We typically observe the outcome v_j rather than the state $|v_j\rangle$. But sometimes we will be loose in our language and refer to the outcome $|v_j\rangle$.
5. If the orthonormal basis $\{|v_1\rangle, \dots, |v_n\rangle\} \subset \mathbb{C}^n$ is the standard/computational basis $\{e_1, \dots, e_n\}$, which is usually written $\{|0\rangle, \dots, |n-1\rangle\}$, then we refer to *measurement in the computational basis* or *measurement in the standard basis*.
6. In \mathbb{C}^2 for example, measuring $|\psi\rangle = \alpha |0\rangle + \beta |1\rangle$ in the computational basis gives
 - (a) outcome 0, and $|0\rangle$ as the state after measurement, with probability $|\alpha|^2$,
 - (b) outcome 1, and $|1\rangle$ as the state after measurement, with probability $|\beta|^2$.
7. In the previous example, if the outcome was 0, then all subsequent measurements in the computational basis will give $|0\rangle$.⁹ *Why?*
8. Each orthonormal basis in the state space corresponds to a particular measurement in physical space which gives *mutually exclusive and exhaustive* outcomes, one outcome for each basis vector. For example, with qubits interpreted as elements of state space for spin 1/2 particles, the orthonormal basis $\{|0\rangle, |1\rangle\}$ corresponds to measurement of spin in the z -direction typically by means of a Stern-Gerlach apparatus as in Section 2.3, with outcomes spin 1/2 (i.e. spin \uparrow , i.e. new state $|0\rangle$) or spin -1/2 (i.e. spin \downarrow , i.e. new state $|1\rangle$).

⁹To be precise, this assumes the particle was not disturbed by the measurement process. Typically this would mean a detector, such as a screen of some sort, was set up to register if the outcome was $|1\rangle$. Any particle not detected will be in the state $|0\rangle$.

Similarly, as we will see later, all measurements for spin $1/2$ particles correspond to measuring spin in some direction in \mathbb{R}^3 , and the two mutually exhaustive and exclusive outcomes for each such measurement correspond to an orthonormal basis in \mathbb{C}^2 .¹⁰

For the two-slit experiment in Section 1.3, the set of orthonormal basis vectors $|\mathbf{x}\rangle$ corresponds to striking the screen in the various regions $R_{\mathbf{x}}$.

It may be the case that there are technological problems in realising the measurement process corresponding to a particular basis, but in principle there is no restriction. In the case of qubits, all possible measurements can in fact be realised, for example, with spin $1/2$ particles and a suitably oriented Stern-Gerlach apparatus.

9. Conversely to the previous remark, mutually exclusive outcomes of a measurement correspond to orthonormal vectors in state space. Mutually exclusive *and* exhaustive outcomes correspond to an orthonormal *basis*.

2.2.2 Measuring Qubits

We say a measurement is with respect to (or is measured by) the ket $|v\rangle \in \mathbb{C}^2$ if the outcome of measuring an arbitrary $|\psi\rangle$ is the state $|v\rangle$ with probability $|\langle v|\psi\rangle|^2 = \cos^2 \theta$, and so is the state $|v\rangle^\perp$ with probability $1 - |\langle v|\psi\rangle|^2 = \sin^2 \theta$, where θ is the angle in \mathbb{C}^2 between $|v\rangle$ and $|\psi\rangle$. (See Figure 2.4)

By the preliminary version of Postulate 2 this is the same as measurement w.r.t.¹¹ the (ordered) orthonormal basis $\{|v\rangle, |v\rangle^\perp\}$. Thus w.l.o.g.¹² we can consider measurements given by a single ket. Of course, this equivalence is only true in \mathbb{C}^2 .

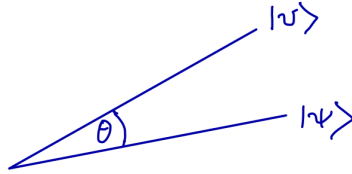


Figure 2.4: A section of \mathbb{C}^2 . $|\psi\rangle$ is measured w.r.t. $|v\rangle$ — the outcome is $|v\rangle$ with probability $\cos^2(\theta)$.

2.2.3 Distinguishing Relative Phase

We noted in Section 2.2.1 Remark 3 that measurements do not distinguish between global phase factors. However, they *can* distinguish relative phase factors such as $e^{i\phi}$ in

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\phi} |1\rangle. \quad (2.5)$$

To see this, suppose we have a large number of similarly prepared copies of $|\psi\rangle$. This may be done in the case of spin by passing a large number of spin $1/2$ particles through a Stern-Gerlach apparatus pointing in the \mathbb{R}^3 direction with spherical coordinates (θ, ϕ) and blocking those particles which come out of the apparatus with spin down. Of course, if we set up the Stern-Gerlach apparatus ourselves we know (θ, ϕ) and hence the state $|\psi\rangle$. But suppose someone else set up the apparatus and sent the

¹⁰If the measurement direction has spherical coordinates (θ, ϕ) in \mathbb{R}^3 , then the orthonormal basis in \mathbb{C}^2 is

$$\left\{ \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\phi} |1\rangle, \quad \cos \frac{\pi - \theta}{2} |0\rangle + \sin \frac{\pi - \theta}{2} e^{i(\phi + \pi)} |1\rangle = \sin \frac{\theta}{2} |0\rangle - \cos \frac{\theta}{2} e^{i\phi} |1\rangle \right\},$$

corresponding to the antipodal points in \mathbb{R}^3 with spherical coordinates (θ, ϕ) and $(\pi - \theta, \phi + \pi)$.

¹¹“w.r.t.” is an abbreviation for “with respect to”

¹²“w.l.o.g.” is an abbreviation for “without loss of generality”.

identically prepared qubits on to us. Suppose we are told all the particles are in the same state, but we are not told what is the state.

Step 1. If we measure such qubits in the computational basis $\{|0\rangle, |1\rangle\}$, the probability that after measurement the qubit will be in the state $|0\rangle$ is $\cos^2 \frac{\theta}{2}$. So we do a frequency count of what happens to a sufficiently large number of such similarly prepared qubits $|\psi\rangle$. This will give a good approximation to $\cos^2 \frac{\theta}{2}$ and hence to θ .¹³

Step 2 Such measurements in the computational basis gave no information about ϕ , only about θ . But suppose we also measure a large number of other copies of $|\psi\rangle$ in the $\{|+\rangle, |-\rangle\}$ basis.¹⁴ From (2.2)

$$|0\rangle = \frac{1}{\sqrt{2}}|+\rangle + \frac{1}{\sqrt{2}}|-\rangle, \quad |1\rangle = \frac{1}{\sqrt{2}}|+\rangle - \frac{1}{\sqrt{2}}|-\rangle. \quad (2.6)$$

So from (2.5) and (2.6)

$$|\psi\rangle = \frac{1}{\sqrt{2}} \left(\cos \frac{\theta}{2} + \sin \frac{\theta}{2} e^{i\phi} \right) |+\rangle + \frac{1}{\sqrt{2}} \left(\cos \frac{\theta}{2} - \sin \frac{\theta}{2} e^{i\phi} \right) |-\rangle =: \alpha' |+\rangle + \beta' |-\rangle. \quad (2.7)$$

Therefore

$$\begin{aligned} |\alpha'|^2 &= \frac{1}{2} \left(\cos \frac{\theta}{2} + \sin \frac{\theta}{2} e^{i\phi} \right) \left(\cos \frac{\theta}{2} + \sin \frac{\theta}{2} e^{-i\phi} \right) = \frac{1}{2} (1 + \sin \theta \cos \phi), \\ |\beta'|^2 &= \frac{1}{2} (1 - \sin \theta \cos \phi). \end{aligned}$$

So given information about θ from Step 1, we can estimate the relative phase ϕ by measuring a large number of similarly produced qubits $|\psi\rangle$ in the $\{|+\rangle, |-\rangle\}$ basis.

2.2.4 Hermitian Operators and Measurements

Every orthonormal basis $\{v_1, \dots, v_n\}$ in an n -dimensional state space V determines the eigenvectors of an hermitian operator $H : V \rightarrow V$, but not the eigenvalues. See Appendix B.2.1. The eigenvalues are essentially labels, and do not normally have a canonical physical interpretation in our setting.¹⁵

Conversely, suppose $H : V \rightarrow V$ is hermitian with distinct eigenvalues $\lambda_1, \dots, \lambda_k$ ($k \leq n$), corresponding orthogonal eigenspaces E_1, \dots, E_k , and orthogonal projection operators $P_i : V \rightarrow E_i$. Then

$$V = E_1 \oplus \dots \oplus E_k, \quad H = \sum_i \lambda_i P_i, \quad I = \sum_i P_i, \quad (2.8)$$

where $I : V \rightarrow V$ is the identity operator and $V = E_1 \oplus \dots \oplus E_k$ just says the E_i are mutually orthogonal and every $v \in V$ has a unique decomposition $v = v_1 + \dots + v_k$ with $v_i \in E_i$.

See Figure 2.7, in which case E_1 is one-dimensional and spanned by $|2\rangle$, while E_2 is two-dimensional and spanned by $|0\rangle$ and $|1\rangle$.

The other important properties of the P_i are

$$P_i = P_i^*, \quad P_i^2 = P_i, \quad P_i P_j = O \quad \text{if } i \neq j, \quad (2.9)$$

where O is the zero operator sending all vectors to the zero vector.

Choosing a set of orthonormal basis vectors for each E_i and taking the union gives a basis for V .

$$H = \begin{bmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_2 \end{bmatrix}.$$

¹³Remember that $0 \leq \theta \leq \pi$ and so in particular $\cos \frac{\theta}{2}$ is ≥ 0 .

¹⁴Not copies we have already measured in the computational basis, of course!! Those qubits will be in the $|0\rangle$ or $|1\rangle$ state, and so of no use for our purpose.

¹⁵However, in physics, where the state space is infinite dimensional, the eigenvectors may represent position or momentum for example, and the eigenvalues take on physical meaning. See Footnote 3. In the finite dimensional setting the eigenvalues could give the energy, after normalisation, of the corresponding eigenstate.

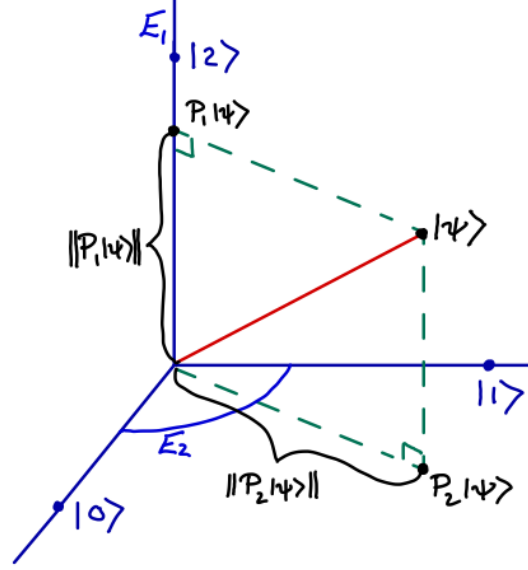


Figure 2.5: $V = \mathbb{C}^3 = E_1 \oplus E_2$ with basis $\{v_1, v_2, v_3\} = \{|0\rangle, |1\rangle, |2\rangle\}$, see (2.8).

$$|\psi\rangle = P_1 |\psi\rangle + P_2 |\psi\rangle, \quad \|\psi\|^2 = \|P_1 |\psi\rangle\|^2 + \|P_2 |\psi\rangle\|^2.$$

1-dimensional complex subspaces $\text{Span } |0\rangle$, $\text{Span } |1\rangle$ and $\text{Span } |2\rangle$ each represented by a real line.

2.2.5 Measurement Postulate (Hermitian Operator Version)

The following version of Postulate 2 is an extension of the preliminary version in Section 2.2.1, as we note subsequently in Remark 3.

Postulate 2. Suppose $H : V \rightarrow V$ is hermitian with decomposition as in (2.8). Then H describes a measurement/observation as follows. If the state before measurement is $|\psi\rangle$ then the state after measurement is $P_i |\psi\rangle / \|P_i |\psi\rangle\|$ with probability $\|P_i |\psi\rangle\|^2$. In this case we say the outcome is λ_i .

Remarks

1. It is *NOT* normally the case that the state after measurement by H of the state $|\psi\rangle$ is $H |\psi\rangle$.
2. The denominator $\|P_i |\psi\rangle\|$ in $P_i |\psi\rangle / \|P_i |\psi\rangle\|$ is needed for normalisation purposes.
3. Since

$$\begin{aligned} |\psi\rangle &= P_1 |\psi\rangle + \cdots + P_k |\psi\rangle \quad \text{by (2.8)} \\ &= \|P_1 |\psi\rangle\| \frac{P_1 |\psi\rangle}{\|P_1 |\psi\rangle\|} + \cdots + \|P_k |\psi\rangle\| \frac{P_k |\psi\rangle}{\|P_k |\psi\rangle\|}, \end{aligned} \quad (2.10)$$

it is clear by taking $k = n$ that Postulate 2 is a generalisation of the previous preliminary version.

4. Let $p_{|\psi\rangle}(\lambda_i)$ be the probability that the outcome of the measurement H is λ_i if the initial state is $|\psi\rangle$.

Since P_i is a projection operator

$$P_i^* = P_i, \quad P_i^2 = P_i. \quad (2.11)$$

Hence¹⁶

$$p_{|\psi\rangle}(\lambda_i) := \|P_i |\psi\rangle\|^2 = (P_i |\psi\rangle)^* P_i |\psi\rangle = \langle \psi | P_i^* P_i | \psi \rangle = \langle \psi | P_i | \psi \rangle. \quad (2.12)$$

Summarising, the **important** point is that

$$p_{|\psi\rangle}(\lambda_i) := \|P_i |\psi\rangle\|^2 = \langle \psi | P_i | \psi \rangle. \quad (2.13)$$

¹⁶See Appendix D.4 for the third “=”.

5. A related and important point is that *the expected outcome* $\mathbb{E}_{|\psi\rangle}(H)$ *of the measurement* H *applied to the state* ψ *is* $\langle\psi|H|\psi\rangle$.

This follows from (2.13) since

$$\mathbb{E}_{|\psi\rangle}(H) = \sum_i \lambda_i p_{|\psi\rangle}(\lambda_i) = \left\langle \psi \left| \sum_i \lambda_i P_i \right| \psi \right\rangle = \langle\psi|H|\psi\rangle.$$

This can be useful in computing the probabilities if there are just two possible outcomes.

6. Note $\sum_i p_{|\psi\rangle}(\lambda_i) = 1$. We can see this two ways:

- *Either*, from (2.13) and (2.10), $\sum_i p_{|\psi\rangle}(\lambda_i) = \sum_i \|P_i|\psi\rangle\|^2 = \langle\psi|\psi\rangle = 1$,
- *or*, from (2.13) and (2.8), $\sum_i p_{|\psi\rangle}(\lambda_i) = \sum_i \langle\psi|P_i|\psi\rangle = \langle\psi|\sum_i P_i|\psi\rangle = \langle\psi|I|\psi\rangle = 1$.

7. The type of measurements we have been discussing are known as *projective measurements* or *von Neumann measurements*. In quantum computing it is sometimes convenient to deal with more general procedures known as *generalised measurements*. However, it is also possible to realise such measurements by means of projective measurements, but sometimes not so conveniently.

Distinction between the Orthonormal Basis and Hermitian Operator Approaches

The essential aspect of both approaches is the set of eigenspaces, the eigenvalues essentially just being labels.

In the orthonormal basis approach the eigenspaces are all one dimensional. In the hermitian operator approach we allow higher dimensional eigenspaces.

In addition, it is often technically more convenient to deal with an hermitian operator rather than an orthonormal basis.

2.2.6 Pauli Matrices and Measurement

Each of the Pauli matrices (see Appendix E) gives an important example of an hermitian operator on qubits.

The matrix σ_3 corresponds to measurement in the computational basis $\{|0\rangle, |1\rangle\}$, with corresponding outcomes labelled 1 and -1 respectively.

The matrix σ_1 corresponds to measurement in the basis $\{|+\rangle, |-\rangle\}$, see (2.2), with corresponding outcomes 1 and -1 respectively.

The matrix σ_2 corresponds to measurement in the basis $\{|i\rangle, |-i\rangle\}$, see (2.2), again with corresponding outcomes 1 and -1 respectively.

Finally, the most general Pauli matrix $\hat{n} \cdot \vec{\sigma}$ corresponds to measurement in an arbitrary (orthonormal) basis.

Denoting eigenspaces by E_j and the corresponding eigenvectors and projection operators by λ_j and P_j , we have the following.

Pauli σ_3

If in (2.8) $H = \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = P_1 - P_2$, then

$$E_1 = \text{span } |0\rangle, \quad P_1 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \lambda_1 = 1; \quad E_2 = \text{span } |1\rangle, \quad P_2 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \quad \lambda_2 = -1. \quad (2.14)$$

The physical realisation of this for spin is measurement of spin in the $\Phi(|0\rangle) = Z$ direction in \mathbb{R}^3 . See Sections 2.3 and 2.3.5, and equation (F.6).

Pauli σ_1

If in (2.8) $H = \sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ then only the algebra is a little more complicated. In this case (see (2.2))

$$E_1 = \text{span } |+\rangle, \quad P_1 = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}, \quad \lambda_1 = 1; \quad E_2 = \text{span } |-\rangle, \quad P_2 = \frac{1}{2} \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}, \quad \lambda_2 = -1. \quad (2.15)$$

See Appendix E for the eigenvectors and values of σ_1 . The matrices P_1 and P_2 are the operators $|+\rangle\langle+|$ and $|-\rangle\langle-|$ (see Appendix D.3.2) and may be calculated from this. See Appendix D.3.1:

$$P_1 = |+\rangle\langle+| = \frac{1}{2}(|0\rangle\langle 0| + |0\rangle\langle 1| + |1\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2} \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix},$$

$$P_2 = |-\rangle\langle-| = \frac{1}{2}(|0\rangle\langle 0| - |0\rangle\langle 1| - |1\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2} \begin{bmatrix} 1 & -1 \\ -1 & 1 \end{bmatrix}.$$

So indeed $\sigma_1 = P_1 - P_2$.

The physical realisation of this for spin is measurement of spin in the $\Phi(|+\rangle) = X$ direction in \mathbb{R}^3 . See Section 2.3 and (F.6).

Pauli σ_2

Similarly, if $H = \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, then

$$E_1 = \text{span } |i\rangle, \quad P_1 = \frac{1}{2} \begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix}, \quad \lambda_1 = 1; \quad E_2 = \text{span } |-i\rangle, \quad P_2 = \frac{1}{2} \begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix}, \quad \lambda_2 = -1. \quad (2.16)$$

See Appendix E for the eigenvectors and values of σ_2 . The projection operators are

$$P_1 = |i\rangle\langle i| = \frac{1}{2}(|0\rangle\langle 0| - i|0\rangle\langle 1| + i|1\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2} \begin{bmatrix} 1 & -i \\ i & 1 \end{bmatrix},$$

$$P_2 = |-i\rangle\langle -i| = \frac{1}{2}(|0\rangle\langle 0| + i|0\rangle\langle 1| - i|1\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2} \begin{bmatrix} 1 & i \\ -i & 1 \end{bmatrix}.$$

So $\sigma_2 = P_1 - P_2$.

The physical realisation of this for spin is measurement of spin in the $\Phi(|i\rangle) = Y$ direction in \mathbb{R}^3 . See Section 2.3 and (F.6).

Pauli $\hat{n} \cdot \vec{\sigma}$

The most general Pauli matrix is $H = \hat{n} \cdot \vec{\sigma} := n_1\sigma_1 + n_2\sigma_2 + n_3\sigma_3 = \begin{bmatrix} n_3 & n_1 - in_2 \\ n_1 + in_2 & -n_3 \end{bmatrix}$, where $\hat{n} = (n_1, n_2, n_3) \in \mathbb{R}^3$, see Appendix E.3. From Appendix E.3.2 the unit eigenvectors are, for $n_3 \neq \pm 1$,

$$|v_1\rangle = \frac{1}{\sqrt{2(1+n_3)}} \begin{bmatrix} 1+n_3 \\ n_1+in_2 \end{bmatrix} \quad \text{with eigenvalue } +1,$$

$$|v_{-1}\rangle = \frac{1}{\sqrt{2(1-n_3)}} \begin{bmatrix} 1-n_3 \\ -(n_1+in_2) \end{bmatrix} \quad \text{with eigenvalue } -1. \quad (2.17)$$

If $n_3 = \pm 1$ then $\hat{n} \cdot \vec{\sigma} = \pm\sigma_3$; the unit eigenvectors are $|v_1\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$ with eigenvalue $+1$ and $|v_{-1}\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$ with eigenvalue -1 .

The eigenspaces, projection operators and eigenvalues are then

$$E_1 = \text{span } |v_1\rangle \quad P_1 = \frac{1}{2} \begin{bmatrix} 1+n_3 & n_1-in_2 \\ n_1+in_2 & 1-n_3 \end{bmatrix} \quad \lambda_1 = 1$$

$$E_2 = \text{span } |v_{-1}\rangle \quad P_2 = \frac{1}{2} \begin{bmatrix} 1-n_3 & -n_1+in_2 \\ -n_1-in_2 & 1+n_3 \end{bmatrix} \quad \lambda_2 = -1 \quad (2.18)$$

See Appendix E.3.2 equation (E.9) and the subsequent remarks there for the projection operators.

2.3 Qubits and Spin 1/2 Particles

For spin 1/2 particles there is a particularly nice physical interpretation of qubit states and of the measurement process, as we now discuss.

Initially we will speak of a spin 1/2 particle which *corresponds* to a qubit $|\psi\rangle$, and of the outcome *probability* of various measurements. Later we make these correspondences and probabilities “concrete” on the basis of experimental results and certain frequency counts.

A key point will be that one can produce multiple spin 1/2 particles, all spin-oriented in the same direction, see Sections 2.3.1 and 2.3.3.

2.3.1 Spin-Orientation

In the following a particle (or a qubit) is referred to as having “*spin-orientation in the direction \hat{n}* ”, or just “*spin-orientation \hat{n}* ”, where $\hat{n} \in \mathbb{R}^3$ is a unit vector. This is also referred to as spin up, spin \uparrow or spin $+1/2$, in the direction \hat{n} . Spin orientation in the direction $-\hat{n}$, as well as being referred to as spin \uparrow or spin 1/2 in the direction $-\hat{n}$, may also be referred to as spin down, spin \downarrow or spin $-1/2$ in the direction \hat{n} .

It is important to realise that a particle with “spin-orientation in the direction \hat{n} ” does *not* possess a definite property of “spin-orientation in the \hat{n} -direction” which can be discovered by means of some appropriate measurement.

To the extent such a particle with “spin-orientation \hat{n} ” has a “definite” property it is of the following *probabilistic form*. (See Section 2.3.2 for Stern-Gerlach apparatus and Section 2.3.3 for preparing a large sample of particles with the same spin-orientation.)

Experimental Observation Suppose spin 1/2 particles with the same spin-orientation \hat{n} are measured by a Stern-Gerlach apparatus oriented in direction \hat{k} , and $\eta \in [0, \pi]$ is the angle between \hat{n} and \hat{k} . Then after measurement the spin-orientation is \hat{k} with probability $\cos^2 \frac{\eta}{2}$ and is $-\hat{k}$ with probability $1 - \cos^2 \frac{\eta}{2}$. See Figure 2.6.

These probabilities have been observed repeatedly and extremely accurately.

Note that if $\hat{n} = \hat{k}$ ($\hat{n} = -\hat{k}$) then the first (second) probability is 1 and so in these cases, and only these cases, the outcome is definite.

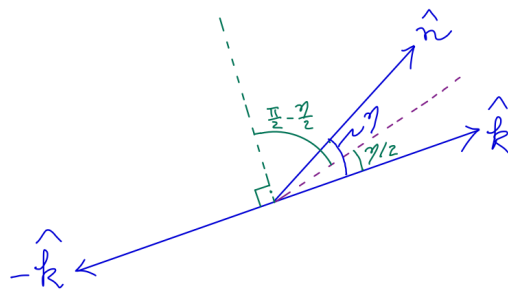


Figure 2.6: Particles with spin-orientation \hat{n} are measured by a Stern-Gerlach apparatus oriented in direction \hat{k} , with angle η between \hat{n} and \hat{k} . After measurement the spin-orientation is \hat{k} with probability $\cos^2 \frac{\eta}{2}$ and $-\hat{k}$ with probability $1 - \cos^2 \frac{\eta}{2}$.

2.3.2 Stern-Gerlach Experimental Set-Up

A Stern-Gerlach apparatus generates a non homogeneous magnetic field in some direction in \mathbb{R}^3 , as in Figure 2.7 where the field is in the vertical or z -direction.

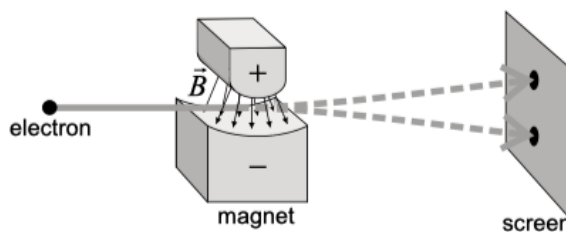


Figure 2.7: Spin 1/2 particle measured by a Stern-Gerlach apparatus. The apparatus has magnetic field, from $-$ to $+$, oriented in the z (vertical) direction, or more generally in an arbitrary \hat{k} direction ([Lvo18, p203 Fig 4.7]).

When a spin 1/2 particle is passed horizontally through this magnetic field the particle is either deflected up or down. More accurately, after passing through the field the state of the particle is in a superposition of spin up \uparrow and spin down \downarrow in the z direction in \mathbb{R}^3 , with the spin amplitudes unchanged from before passing through the field. But there is now correlation with spatial position in a larger Hilbert space — spin up is correlated with being vertically higher and spin down being vertically lower.

When the particle arrives at the screen it has to, in effect, “make a decision” whether to be spin up in the z -direction, i.e. have spin-orientation z , or to be spin down in the z -direction, i.e. have spin-orientation $-z$, and this will be indicated by which of the two possible spots on the screen register as being “hit”.

More generally, replacing z by a unit vector \hat{k} , suppose the Stern-Gerlach apparatus has magnetic field oriented in the \hat{k} direction. Suppose the particle is passed through the magnetic field in a direction orthogonal to \hat{k} . Then the particle after measurement will have spin-orientation in either the \hat{k} or $-\hat{k}$ direction.

The probability for each of the two possible outcomes $\pm\hat{k}$, assuming the initial spin-orientation \hat{n} is known, is given by the Experimental Observation in Section 2.3.1. Note that the two possible outcomes, as opposed to their probabilities, are *independent* of the particles initial spin-orientation direction. (Except that only one outcome is possible if $\hat{n} = \pm\hat{k}$.)

2.3.3 Multiple Particles with the same Spin-Orientation

From Section 2.3.2, by passing spin 1/2 particles through a Stern-Gerlach apparatus oriented in the direction \hat{k} , we can prepare particles spin-oriented in either the \hat{k} direction or $-\hat{k}$ direction.

However, once the particle hits the detection screen it is destroyed. But if we remove the upper half of the screen in Figure 2.7 then only those particles which “decide” at the time of measurement to have spin-orientation $-\hat{k}$ are destroyed, and the upper “path” gives a stream of particles with spin-orientation \hat{k} .¹⁷

If these particles with spin-orientation \hat{k} are passed through another Stern-Gerlach apparatus oriented in the direction \hat{k} ¹⁸ (or the direction $-\hat{k}$) they will remain with spin-orientation \hat{k} .

Moreover, if these particles are passed through yet another Stern-Gerlach apparatus oriented in the \hat{k}' direction then they will be observed to have spin-orientation $\pm\hat{k}'$ with probabilities in accordance with the Experimental Observation in Section 2.3.1.

¹⁷A critical point concerning quantum theory is that quantum particles do not “make a decision” re physical space until required to do so. Thus the state of the qubit is a superposition of up and down, albeit with different spatial correlations in each case, until measurement time arrives.

¹⁸You may object that after the previous (slight) deflection (in the direction of \hat{k}) the path of the particle is no longer orthogonal to the direction \hat{k} . However, it is possible to apply an intermediate magnetic field to correct for this.

2.3.4 Spin-Orientation and Qubit Correspondence: Bloch Sphere Map

In Appendix F we discuss from a *mathematical* perspective the Bloch sphere one-one correspondence Φ between qubits $|\psi\rangle \in \mathbb{C}^2$ and unit vectors $\hat{n} \in \mathbb{R}^3$. This correspondence can be given directly via spherical coordinates as in equations (F.1)–(F.3) or via the projection map $|\psi\rangle\langle\psi|$ as in (F.7) and (F.11).

For our purposes we use the projection map correspondence. From (F.7)

$$\Phi |\psi\rangle = (n_1, n_2, n_3) \quad \text{where} \quad |\psi\rangle\langle\psi| = \frac{1}{2}(I + n_1\sigma_1 + n_2\sigma_2 + n_3\sigma_3) =: \frac{1}{2}(I + \hat{n} \cdot \vec{\sigma}), \quad (2.19)$$

with $\hat{n} = (n_1, n_2, n_3) \in S^2 \subset \mathbb{R}^3$ being uniquely determined by $|\psi\rangle$, and the qubit $|\psi\rangle$ (up to a global phase) being uniquely determined by \hat{n} . Recall also that the correspondence between qubits and projection maps $|\psi\rangle\langle\psi|$ is one-one, see the first paragraph of Appendix F.3.

So after we fix an orthonormal frame in space to correspond to the unit vectors $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1) \in \mathbb{R}^3$ we also regard the Bloch Sphere map Φ as a correspondence between qubits in \mathbb{C}^2 and directions in space.

2.3.5 Spin-Orientation and Qubit Correspondence: Physical Justification

So finally we come to the key idea.

All spin measurements are essentially of the Stern-Gerlach type. By the Experimental Observation in Section 2.3.1, for a fixed measurement direction, the observable consequences (which as we have emphasised are probabilistic) are precisely determined by the measurement direction and the spin-orientation of the particle being measured.

For this reason we want to identify qubit states with spin-orientations, i.e. with unit vectors in \mathbb{R}^3 , or equivalently with directions in physical space after choosing an orthonormal frame. One candidate for such an identification is the Bloch Sphere map. The intention here is to justify on physical/experimental grounds that this must be the correct identification.

Consider two unit directions in physical space, \hat{n} and \hat{k} , and let $\eta \in [0, \pi]$ be the angle between them.

Let $|\hat{n}\rangle$ and $|\hat{k}\rangle$ be the qubits in \mathbb{C}^2 such that $\Phi |\hat{n}\rangle = \hat{n}$ and $\Phi |\hat{k}\rangle = \hat{k}$. Then *the angle between $|\hat{n}\rangle$ and $|\hat{k}\rangle$ is $\eta/2$* from the angle doubling proposition in Appendix F.4.

From Section 2.3.1 recall:

Experimental Observation. If spin 1/2 particles are prepared with spin-orientation \hat{n} and are measured by a Stern-Gerlach apparatus oriented in the direction \hat{k} , then the spin-orientation after measurement is \hat{k} with probability $\cos^2 \frac{\eta}{2}$ and is $-\hat{k}$ with probability $1 - \cos^2 \frac{\eta}{2}$. See Figure 2.6.

From the version of the measurement postulate at the end of Section 2.2.1 under the heading “Measuring Qubits” we have, since the angle between $|\hat{n}\rangle$ and $|\hat{k}\rangle$ is $\eta/2$:

Measurement Postulate Prediction. If $|\hat{n}\rangle$ is measured by (i.e. is measured w.r.t.) $|\hat{k}\rangle$, then the state after measurement is $|\hat{k}\rangle$ with probability $\cos^2 \frac{\eta}{2}$ and is $-\hat{k}$ with probability $1 - \cos^2 \frac{\eta}{2}$.

Conclusion: Through the Bloch sphere mapping $|\hat{n}\rangle \leftrightarrow \hat{n} = \Phi |\hat{n}\rangle$, all experimental observations (for probabilities via frequency counts) agree with the measurement postulate prediction for the corresponding qubits. Since the predicted results of measurements are essentially all we can know about state space, *the Bloch sphere map is the correct and unique identification between state space for qubits and spin orientations in physical space.*

2.4 Evolution

2.4.1 Evolution Postulate (Discrete Version)

Postulate 3. *The time evolution of a closed system is described by a unitary transformation U operating on its state space V . That is, if $|\psi\rangle$ is the state of the system at time t_1 then $U|\psi\rangle$ is the state at time t_2 . The operator U depends on t_1 and t_2 but not on the state $|\psi\rangle$.*

Remarks

The requirement that U be unitary is a natural one. In particular, evolution should preserve superposition of states and map state vectors to state vectors. That is

$$U(\alpha|v\rangle + \beta|w\rangle) = \alpha U|v\rangle + \beta U|w\rangle, \quad \|U|v\rangle\| = 1. \quad (2.20)$$

These conditions imply U is a unitary transformation. See Appendix B.6.

2.4.2 Examples of Unitary Gates

Please read the first few paragraphs of Appendix E for basic information about the Pauli matrices.

In these examples we introduce the notation for quantum circuits, which is continued in Sections 3.2.2–3.2.4 and used extensively in Chapter 4.

We discuss three important examples of unitary matrices, each acting on the state space $V = \mathbb{C}^2$. It is easy to see they are unitary, for example the two columns in each case are of unit length and orthogonal to one another. (They are also hermitian, trace free and real, but these properties, do not hold for all unitary maps!)

Possible confusion to avoid: The following NOT ($\sigma_1 = X$) and phase flip ($\sigma_3 = Z$) gates are given by the same matrices as those which give measurement operators corresponding to the orthonormal bases $\{|+\rangle, |-\rangle\}$ and $\{|0\rangle, |1\rangle\}$ respectively, see the beginning of Section 2.2.6.

1. The *quantum NOT gate* is the Pauli matrix $\sigma_1 = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$. It is also called the *bit flip* matrix/gate since it takes $|0\rangle$ to $|1\rangle$ and $|1\rangle$ to $|0\rangle$.

As part of a quantum circuit it is represented as

$$\text{---}\oplus\text{---} \quad \text{or} \quad \text{---}\boxed{X}\text{---} \quad \text{where} \quad \alpha|0\rangle + \beta|1\rangle \xrightarrow{\boxed{X}} \beta|0\rangle + \alpha|1\rangle, \quad (2.21)$$

with the input and output indicated in the last case.

As for all quantum circuits, this should be interpreted as change in time, moving from left to right, rather than something necessarily moving along a wire.

2. The *phase flip gate* is the Pauli matrix $\sigma_3 = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. It leaves $|0\rangle$ unchanged and changes $|1\rangle$ to $-|1\rangle$, with the factor $-1 = e^{-i\pi}$ being the phase factor change.

As part of a quantum circuit it is represented as

$$\text{---}\boxed{Z}\text{---} \quad \text{where} \quad \alpha|0\rangle + \beta|1\rangle \xrightarrow{\boxed{Z}} \alpha|0\rangle - \beta|1\rangle. \quad (2.22)$$

3. The *Hadamard gate* is given by the matrix $H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$. It is represented by

$$\text{---}\boxed{H}\text{---} \quad . \quad \text{Note } |0\rangle \xrightarrow{\boxed{H}} |+\rangle, \quad |1\rangle \xrightarrow{\boxed{H}} |-\rangle. \quad (2.23)$$

The operator H is unitary, trace free hermitian. *Check this.* In particular $H \in \mathcal{H}_0$ and $H = \frac{1}{\sqrt{2}}(X + Z)$. See also Appendix E equation (E.4).

2.4.3 Evolution Postulate (Continuous Version)

Often we require a version of this postulate concerning evolution in continuous time.

Postulate 3. *The time evolution of a closed system is described by the Schrödinger equation*

$$\frac{d}{dt} |\psi(t)\rangle = -iH |\psi(t)\rangle, \quad (2.24)$$

where $|\psi(t)\rangle$ is the state of the system at time t . H is a time-independent hermitian operator known as the Hamiltonian of the system.

2.4.4 Solution of Schrödinger's Equation

Since the Hamiltonian H in (2.24) is *time-independent*, in terms of an orthonormal basis of eigenvectors for H we can write

$$|\psi\rangle = |\psi(t)\rangle = \begin{bmatrix} \psi_1(t) \\ \vdots \\ \psi_n(t) \end{bmatrix}, \quad H = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}. \quad (2.25)$$

It follows that (2.24) is equivalent to the following simple system of independent ordinary differential equations:

$$\frac{d}{dt} \psi_j(t) = -i\lambda_j \psi_j(t), \quad j = 1, \dots, n. \quad (2.26)$$

This has the solution

$$\psi_j(t) = e^{-i\lambda_j t} \psi_j(0). \quad (2.27)$$

That is, the solution $|\psi(t)\rangle$ of Schrödinger's equation at time t , with initial state $|\psi(0)\rangle$, is

$$|\psi(t)\rangle = U(t) |\psi(0)\rangle, \quad \text{where } U(t) := e^{-itH} = \begin{bmatrix} e^{-i\lambda_1 t} & & \\ & \ddots & \\ & & e^{-i\lambda_n t} \end{bmatrix}. \quad (2.28)$$

Note that $U(t)$ is indeed unitary. See Section G.4.

In physical realisations of quantum computing systems, the Hamiltonians, and hence the unitary gates, are obtained by applying lasers, magnetic fields, etc., appropriately oriented and turned on or off for various time intervals, typically picoseconds¹⁹. Of course, this means the quantum system under consideration is *not* closed. However, by taking it as part of a larger system which is then itself treated as closed, one can usually find a *time dependent* hermitian operator acting on the original quantum system under consideration, with parameters that can be varied as required, and which when used in Schrödinger's equation gives a good approximation to what happens in the original system.

2.4.5 Hamiltonian Example

As a prototypical example consider the Hamiltonian

$$H = -\frac{\omega}{2} \sigma_3 = \begin{bmatrix} -\frac{\omega}{2} & 0 \\ 0 & \frac{\omega}{2} \end{bmatrix}. \quad (2.29)$$

Here σ_3 is the Pauli matrix discussed briefly in Section 2.4.1 Example 2.

Since H is already in diagonal form, from (2.28),

$$U(t) = e^{-itH} = \begin{bmatrix} e^{i\frac{\omega}{2}t} & 0 \\ 0 & e^{-i\frac{\omega}{2}t} \end{bmatrix} = e^{i\frac{\omega}{2}t} \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\omega t} \end{bmatrix}. \quad (2.30)$$

The phase factor $e^{i\frac{\omega}{2}t}$ is physically irrelevant when $U(t)$ is applied to an initial state $|\psi(0)\rangle$.

Setting $t = \pi\omega^{-1}$, $U(\pi\omega^{-1}) = \sigma_3$ (up to an irrelevant global phase factor $e^{i\frac{\omega}{2}t}$).

So $Z = \sigma_3$ can be physically realised by applying the Hamiltonian $H = -\frac{\omega}{2} \sigma_3$ as an appropriate laser or magnetic field for a time interval of length $\pi\omega^{-1}$.

¹⁹A picosecond is 10^{-12} of a second.

Remarks

1. The Hamiltonian H is *not* the Hadamard matrix/gate H !
2. In (2.28) we noted the operator $U(t)$ is unitary for all t . This is consistent with the discrete time version in Section 2.4.1.
3. It is also clear from the matrix representation (G.3) that *every* unitary matrix U can be written in the form $U = \exp(-iH)$ for some Hamiltonian H . So there is a one-one correspondence between the discrete and continuous time descriptions. In understanding the theory of quantum computation, as opposed to its experimental set-up, one is usually concerned with the discrete time formulation.
4. The Schrödinger equation is usually written in the form $i\hbar \frac{d}{dt} |\psi\rangle = H |\psi\rangle$ where \hbar is *Planck's constant*. We normally choose units such that $\hbar = 1$.

2.5 Composite Systems

In this section we also introduce and motivate the notion of tensor product. But we only use the notation and what is contained in the following discussion.²⁰ In Section 3.2 there is further development of the tensor product of spaces and of operators as needed to study entanglement. A more complete mathematical development is in Appendix H.

2.5.1 Pairs of Qubits and Bipartite States

Consider first a pair of classical bits, which we refer to as the first and second bit. Their possible values are 00, 01, 10 and 11. For example, 10 is the case in which the first bit has value 1 and the second has value 0.

Guided by the State Space Postulate in Section 2.1.1, and Remarks 8 and 9 in Section 2.2.1, we hope to model the quantum situation for a pair of *qubits* by considering \mathbb{C}^4 with basis vectors

$$|00\rangle := \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix}, \quad |01\rangle := \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix}, \quad |10\rangle := \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix}, \quad |11\rangle := \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix}, \quad (2.31)$$

The state of a qubit pair, called a *bipartite state*, would be given by

$$|\psi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle = \begin{bmatrix} \alpha_{00} \\ \alpha_{01} \\ \alpha_{10} \\ \alpha_{11} \end{bmatrix}, \quad \alpha_{jk} \in \mathbb{C}, \quad \sum |\alpha_{jk}|^2 = 1. \quad (2.32)$$

Moreover, $|\psi\rangle$ and $e^{i\phi}|\psi\rangle$ should be physically indistinguishable and so represent the same qubit.

All states of the form (2.32) are physically realisable. This leads to entanglement, which is central to quantum theory. The consequences and predictions are very counterintuitive, but have been borne out in innumerable experiments.

2.5.2 Composite System Postulate

Postulate 4. Suppose we have N physical systems with state spaces V_1, \dots, V_N respectively. Then the state space V of the composite physical system is given by the tensor product $V = V_1 \otimes \dots \otimes V_N$. If the i th system is in the state $|\psi_i\rangle$ for $i = 1, \dots, N$ then the state of the composite system is $|\psi_1\rangle \otimes \dots \otimes |\psi_N\rangle$.

Tensor Products The vector space $V = V_1 \otimes V_2$ is the *tensor product* of V_1 and V_2 . The state $|\psi_1\rangle \otimes |\psi_2\rangle$ is the *tensor product* of $|\psi_1\rangle \in V_1$ and $|\psi_2\rangle \in V_2$. We give the simple examples we need in Section 2.5.3.

Just think of $|\psi_1\rangle \otimes |\psi_2\rangle$ as the state of two qubits where the first is in the state $|\psi_1\rangle \in V_1$ and the second is in the state $|\psi_2\rangle \in V_2$.

We often write $|\psi_1\rangle|\psi_2\rangle$ or $|\psi_1\psi_2\rangle$ for $|\psi_1\rangle \otimes |\psi_2\rangle$.

Similarly for $|\psi_1 \dots \psi_N\rangle = |\psi_1\rangle \dots |\psi_N\rangle = |\psi_1\rangle \otimes \dots \otimes |\psi_N\rangle$.

2.5.3 N-Qubit Space

In quantum computing we will mostly be concerned with N -qubit space

$$\mathbb{C}^{2^N} = \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2. \quad (2.33)$$

Note how the dimension 2^N grows exponentially in N .

²⁰Unfortunately, many courses on general relativity present tensors in an unnecessarily unpleasant and unintuitive manner.

The canonical basis for $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$ is in one-one correspondence with the set of all 2^N possible classical N -bits,

$$(0, \dots, 0, 0, 0), \quad (0, \dots, 0, 0, 1), \quad (0, \dots, 0, 1, 0), \quad \dots, \quad (1, \dots, 1, 1, 1), \quad (2.34)$$

here ordered lexicographically. We write the corresponding 2^N basis vectors as

$$|0 \dots 000\rangle, \quad |0 \dots 001\rangle, \quad |0 \dots 010\rangle, \quad \dots, \quad |1 \dots 111\rangle. \quad (2.35)$$

Thus for a single qubit we have canonical basis vectors $\{|0\rangle, |1\rangle\} \subset \mathbb{C}^2$. For a pair of qubits the canonical basis vectors in \mathbb{C}^4 are

$$|00\rangle, |01\rangle, |10\rangle, |11\rangle \subset \mathbb{C}^4. \quad (2.36)$$

For a triplet of qubits the canonical basis vectors in \mathbb{C}^8 are

$$|000\rangle, |001\rangle, |010\rangle, |011\rangle, |100\rangle, |101\rangle, |110\rangle, |111\rangle, \quad (2.37)$$

etc.

2.5.4 Inner Product for Composite Systems

Importance of Inner Product

Recall from Remarks 8 and 9 on page 29 that if V is the state space for a physical system then orthonormal vectors correspond to mutually exclusive outcomes of an experiment, and an orthonormal basis corresponds to a set of mutually exclusive and exhaustive outcomes. Moreover, the probabilities of various outcomes are determined by the absolute values of amplitudes, which are in turn obtained from the inner product of the state being measured and the outcome state.

Hence the importance of the inner product in the state space.

Inner Product in $\mathbb{C}^2 \otimes \mathbb{C}^2$

See footnote 1 on page 1 for the inner product in \mathbb{C}^n .

The vectors in (2.36) (similarly for (2.37) and (2.35)) are a renaming of the canonical basis vectors (2.34), *and so form an orthonormal basis with respect to this inner product*. The fact they form an orthonormal basis is also consistent with the fact they correspond to a set of mutually exclusive and exhaustive outcomes for the experiment in which each of the two qubits is measured independently in the $\{|0\rangle, |1\rangle\}$ basis.

The inner product of vectors $|\phi\rangle, |\phi'\rangle \in \mathbb{C}^n$ is often written as $\langle\phi | \phi'\rangle$. See Appendix D.1. So with $|\phi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle \in \mathbb{C}^2$ and $|\phi'\rangle = \alpha'_0 |0\rangle + \alpha'_1 |1\rangle \in \mathbb{C}^2$,

$$\langle\phi | \phi'\rangle = (\langle\phi|, |\phi'\rangle) = \alpha_0^* \alpha'_0 + \alpha_1^* \alpha'_1. \quad (2.38)$$

Moreover, with $|\psi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$ and $|\psi'\rangle = \beta'_0 |0\rangle + \beta'_1 |1\rangle$, it is straightforward to check²¹ for the inner product in $\mathbb{C}^2 \otimes \mathbb{C}^2$ that

$$(\langle\phi| \otimes \langle\psi|, |\phi'\rangle \otimes |\psi'\rangle) = \langle\phi | \phi'\rangle \times \langle\psi | \psi'\rangle. \quad (2.39)$$

²¹We have

$$\begin{aligned} & (\langle\phi| \otimes \langle\psi|, |\phi'\rangle \otimes |\psi'\rangle) \\ &= (\alpha_0 \beta_0 |00\rangle + \alpha_0 \beta_1 |01\rangle + \alpha_1 \beta_0 |10\rangle + \alpha_1 \beta_1 |11\rangle, \alpha'_0 \beta'_0 |00\rangle + \alpha'_0 \beta'_1 |01\rangle + \alpha'_1 \beta'_0 |10\rangle + \alpha'_1 \beta'_1 |11\rangle) \\ &= \alpha_0^* \beta_0^* \alpha'_0 \beta'_0 + \alpha_0^* \beta_1^* \alpha'_0 \beta'_1 + \alpha_1^* \beta_0^* \alpha'_1 \beta'_0 + \alpha_1^* \beta_1^* \alpha'_1 \beta'_1 \\ &= (\alpha_0^* \alpha'_0 + \alpha_1^* \alpha'_1) (\beta_0^* \beta'_0 + \beta_1^* \beta'_1) \\ &= \langle\phi | \phi'\rangle \times \langle\psi | \psi'\rangle. \end{aligned}$$

Inner Product in $V \otimes W$

In general, if V and W are inner product spaces, we use the extension of (2.39) to *define* the inner product on $V \otimes W$ by

$$(v_1 \otimes w_1, v_2 \otimes w_2) = (v_1, v_2) \times (w_1, w_2), \quad (2.40)$$

and extend by linearity to all of $V \otimes W$. See Appendix H.1.5.

This is consistent with what we just noted about the standard orthonormal basis for $\mathbb{C}^2 \otimes \mathbb{C}^2$ and more generally $\mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$. For example, using (2.40),

$$\begin{aligned} (|ij\rangle, |kl\rangle) &= (|i\rangle \otimes |j\rangle, |k\rangle \otimes |l\rangle) = \langle i|k\rangle \times \langle j|l\rangle \\ &= \begin{cases} 1 & \text{if } i = k, j = l \\ 0 & \text{otherwise} \end{cases} \end{aligned} \quad (2.41)$$

2.5.5 Entangled Qubit Pairs

The general *bipartite state* for a pair of qubits is a superposition of the 4 basis states (2.36):

$$\alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle, \quad \sum_{j,k} |\alpha_{jk}|^2 = 1. \quad (2.42)$$

Similarly, if $\{v, v^\perp\}$ is an orthonormal basis for the first \mathbb{C}^2 in $\mathbb{C}^2 \otimes \mathbb{C}^2$, and $\{w, w^\perp\}$ for the second \mathbb{C}^2 , then an orthonormal basis for $\mathbb{C}^2 \otimes \mathbb{C}^2$ is $\{|vw\rangle, |vw^\perp\rangle, |v^\perp w\rangle, |v^\perp w^\perp\rangle\}$, by (2.40) and as in (2.41). Using this basis, the general qubit state is

$$\begin{aligned} &a|vw\rangle + b|vw^\perp\rangle + c|v^\perp w\rangle + d|v^\perp w^\perp\rangle \\ &= a|v\rangle \otimes |w\rangle + b|v\rangle \otimes |w^\perp\rangle + c|v^\perp\rangle \otimes |w\rangle + d|v^\perp\rangle \otimes |w^\perp\rangle, \quad \text{where } |a|^2 + |b|^2 + |c|^2 + |d|^2 = 1. \end{aligned} \quad (2.43)$$

If the first qubit is prepared in the state $|\phi\rangle = \alpha_0 |0\rangle + \alpha_1 |1\rangle$ and the second in the state $|\psi\rangle = \beta_0 |0\rangle + \beta_1 |1\rangle$ then the state of the pair of qubits is

$$|\phi\rangle \otimes |\psi\rangle = (\alpha_0 |0\rangle + \alpha_1 |1\rangle)(\beta_0 |0\rangle + \beta_1 |1\rangle) = \alpha_0 \beta_0 |00\rangle + \alpha_0 \beta_1 |01\rangle + \alpha_1 \beta_0 |10\rangle + \alpha_1 \beta_1 |11\rangle. \quad (2.44)$$

This is a *product* state — we can act on and measure the two qubits independently and nothing particularly new will occur.

But not every state of the form (2.42) is a product state. If it is not a product it is said to be *entangled*.

Proposition. *A pair of qubits in the state*

$$\alpha_{00} |00\rangle + \alpha_{01} |01\rangle + \alpha_{10} |10\rangle + \alpha_{11} |11\rangle$$

is entangled if and only

$$\det \begin{bmatrix} \alpha_{00} & \alpha_{01} \\ \alpha_{10} & \alpha_{11} \end{bmatrix} = 0.$$

Proof. This is easy to see since factorisation of (2.42) as in (2.44) is possible if and only if the two rows of the matrix in the proposition are linearly dependent. \square

The analogous result similarly holds for qubits in the state (2.43).

Alice and Bob When considering a pair of qubits it is often convenient to refer to the first as *Alice's qubit* and the second as *Bob's qubit*. In (2.44), $|\phi\rangle$ refers to Alice's qubit and $|\psi\rangle$ refers to Bob's qubit. In (2.43), $|v\rangle$ and $|v^\perp\rangle$ refer to Alice's qubit, while $|w\rangle$ and $|w^\perp\rangle$ refer to Bob's qubit.

Alice and Bob may be separated by a large distance, in principle even in different galaxies. The qubits have typically been previously brought together for the entanglement process (or perhaps they were individually entangled with a previously entangled system). Alice can only measure her own qubit, unless she also has access to Bob's qubit, and similarly for Bob.

See Section 3.2.6 for measuring entangled states.

2.5.6 Bell States

Definitions Particularly important examples of entangled pairs of qubits are given by the *Bell States*:

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) & |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) & |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned} \tag{2.45}$$

These are *entangled* states by the previous proposition. It is routine to entangle pairs of qubits into Bell states and other states on a quantum computer.

Orthonormal Basis As noted in Section 2.5.4 the states $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ form an orthonormal basis for $\mathbb{C}^2 \otimes \mathbb{C}^2$. From this it is easy to check that the Bell states also form an orthonormal basis. For example, with simple cancellations,

$$\begin{aligned} \langle \Phi^+ | \Psi^- \rangle &= \frac{1}{2} (\langle 00| + \langle 11|) (|01\rangle - |10\rangle) \\ &= \frac{1}{2} (\langle 00|01\rangle - \langle 00|10\rangle + \langle 11|01\rangle - \langle 11|10\rangle) \\ &= \frac{1}{2} (0 - 0 + 0 - 0) = 0. \end{aligned}$$

Separating Entangled Qubits After entanglement the two qubits in a Bell state may be sent to different locations and remain entangled. In the EPR experiment discussed in Section 1.5 entangled photons were separated by over 1200km and remained entangled. In principle, particles could be entangled and remain entangled after one of them is sent off to a different galaxy.

Further properties of the Bell states are discussed in Section 3.2.

Chapter 3

Entanglement Conundrum or Resource ?

Contents

3.1	No-Cloning Theorem	45
3.2	Disentangling Entanglement	47
3.2.1	Invariance Properties of the Bell States	47
3.2.2	CNOT Gate	48
3.2.3	Preparing Bell States	49
3.2.4	Interim States in Quantum Circuits	49
3.2.5	Tensor Product of Operators	49
3.2.6	Measuring Entangled States	51
3.2.7	Measurement in the Bell Basis	53
3.2.8	Local Description for each Qubit	54
3.3	Superdense Coding	55
3.4	Teleportation	57
3.5	Bell & CHSH Inequalities	59
3.5.1	History	59
3.5.2	CHSH Experimental Setup	59
3.5.3	Preliminary Discussion of the Results	61
3.5.4	Classical Analysis; Physical Realism, Locality, Random Choice	62
3.5.5	Experimental Results	63
3.5.6	Quantum Analysis	63
3.6	GHZ	65

3.1 No-Cloning Theorem

The no-cloning theorem has fundamental implications for quantum computing. Although it does not involve entanglement as stated here, it has an extension to the no-broadcasting theorem for “mixed” states, which we discuss in a later section and which does involve entanglement.

Copying/cloning *classical* bits is standard, as occurs for example when files are backed up.

But copying an unknown qubit is not possible. This was originally thought to be a problem for the realisation of quantum computing, but the issue is now largely resolved by means of quantum error correction codes, see [NC10, Chapter 10].

On the other hand, the no-cloning result is essential in establishing secure quantum cryptographic transmission. A quantum system cannot be intercepted and copied in transit between the sender

and the receiver without disturbing it in some way. This disturbance can then be used to enable the intended receiver to detect the interception.

Suppose we have a quantum computer with two input slots and two output slots. An unknown state $|\psi\rangle$ and a fixed state $|\phi\rangle$ are fed into the two slots. The requirement is that a copy of $|\psi\rangle$ come out of *each* of the two output slots. See Figure 3.1.

The following shows this is not achievable by means of a unitary transformation. More general results show that applying measurement operators does not help, essentially because this leads to loss of information.

The following argument can also be easily modified to rule out the possibility of three input slots for $|\psi\rangle$ (unknown) $|\phi\rangle$ and $|\chi\rangle$ (both fixed) and three output slots delivering $|\psi\rangle$, $|\psi\rangle$ and $|\zeta\rangle$ (“junk” or “scratch work”) (*Exercise*).

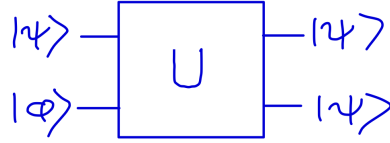


Figure 3.1: There is *no* unitary U with inputs arbitrary $|\psi\rangle$ and fixed $|\phi\rangle$, and outputs $|\psi\rangle$ and $|\psi\rangle$.

Proposition. *Suppose V is an inner product space. Then there does not exist a unitary $U : V \otimes V \rightarrow V \otimes V$ and a vector $s \in V$ such that for every unit norm vector $v \in V$, $U(v \otimes s) = v \otimes v$.*

Proof. Assume such U and s do exist. Then for any $v \in V$ and $w \in V$,

$$U : v \otimes s \mapsto v \otimes v, \quad U : w \otimes s \mapsto w \otimes w. \quad (3.1)$$

Since U preserves inner products, from (2.39) or more generally (2.40),

$$\begin{aligned} \langle v \otimes s, w \otimes s \rangle &= \langle v \otimes v, w \otimes w \rangle, \\ \text{i.e. } \langle v, w \rangle \langle s, s \rangle &= \langle v, w \rangle^2. \end{aligned}$$

Setting $v = w$ implies $\langle s, s \rangle = 1 \neq 0$. Hence $\langle v, w \rangle = 0$ or 1 for all unit v and w .

This contradiction establishes the proposition. □

(Essentially all that is being asserted here is that a general quadratic map $v \mapsto v \otimes v$ is not a linear map, in particular is not $v \mapsto U(v \otimes s)$ for some s .)

3.2 Disentangling Entanglement

In this section we look at some of the basic tools for analysing, understanding and utilising entanglement.

Although much of the discussion concerns the $|\Phi^+\rangle$ Bell state for a pair of entangled qubits, the ideas readily extend and are fundamental for all of quantum theory.

3.2.1 Invariance Properties of the Bell States

Here again are the Bell states briefly discussed in (2.45). See also Section 1.4.3.

$$\begin{aligned} |\Phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) & |\Phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ |\Psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) & |\Psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned} \quad (3.2)$$

Bell states are the key to superdense coding (Section 3.3), teleportation (Section 3.4) and the CHSH inequalities (Section 3.5).

They also have some very useful invariance properties.

For this purpose define the unitary matrix U to be a *real* rotation of \mathbb{C}^2 if its matrix has real entries, see (B.7). That is, $U = \begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix}$ with $\alpha, \beta \in \mathbb{R}$, $\alpha^2 + \beta^2 = 1$. Note $U^{-1} = U^* = \begin{bmatrix} \alpha & \beta \\ -\beta & \alpha \end{bmatrix}$.

Proposition. *Let $|v\rangle = U|0\rangle$ and $|v^\perp\rangle = U|1\rangle$ be the orthonormal basis of \mathbb{C}^2 obtained by a real rotation U of the standard basis. Then*

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|vv\rangle + |v^\perp v^\perp\rangle). \quad (3.3)$$

Proof. Let $U = \begin{bmatrix} \alpha & -\beta \\ \beta & \alpha \end{bmatrix}$. Then $|v\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|v^\perp\rangle = -\beta|0\rangle + \alpha|1\rangle$. Hence

$$\begin{aligned} \frac{1}{\sqrt{2}}(|vv\rangle + |v^\perp v^\perp\rangle) &= \frac{1}{\sqrt{2}}((\alpha|0\rangle + \beta|1\rangle)(\alpha|0\rangle + \beta|1\rangle) + (-\beta|0\rangle + \alpha|1\rangle)(-\beta|0\rangle + \alpha|1\rangle)) \\ &= \frac{1}{\sqrt{2}}((\alpha^2 + \beta^2)|00\rangle + (\alpha^2 + \beta^2)|11\rangle) = |\Phi^+\rangle. \quad \square \end{aligned}$$

Example Let $U = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$. Then $|v\rangle = U|0\rangle = |+\rangle$ and $|v^\perp\rangle = U|1\rangle = -|-\rangle$. So $|vv\rangle = |++\rangle$ and also¹ $|v^\perp v^\perp\rangle = |--\rangle$.

It follows from the proposition that $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)$.

It is straightforward to check that (3.3) does not hold for an arbitrary orthonormal basis $\{|v\rangle, |v^\perp\rangle\}$.² However, although we do not need it, for completeness we note the following for another Bell state:

¹For example, it follows from (2.44) that $(a|\phi\rangle) \otimes (b|\psi\rangle) = (ab)|\phi\rangle \otimes |\psi\rangle$.

²Using (B.7) one can write

$$|0\rangle = a|v\rangle - e^{i\zeta}b^*|v^\perp\rangle, \quad |1\rangle = b|v\rangle + e^{i\zeta}a^*|v^\perp\rangle, \quad \text{where } |a|^2 + |b|^2 = 1$$

Hence

$$\begin{aligned} \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) &= \frac{1}{\sqrt{2}}((a|v\rangle - e^{i\zeta}b^*|v^\perp\rangle) \otimes (a|v\rangle - e^{i\zeta}b^*|v^\perp\rangle) + (b|v\rangle + e^{i\zeta}a^*|v^\perp\rangle) \otimes (b|v\rangle + e^{i\zeta}a^*|v^\perp\rangle)) \\ &= \frac{1}{\sqrt{2}}((a^2 + b^2)|v\rangle|v\rangle + (a^*b - ab^*)e^{i\zeta}|v\rangle|v^\perp\rangle + (a^*b - ab^*)e^{i\zeta}|v^\perp\rangle|v\rangle + ((a^*)^2 + (b^*)^2)e^{2i\zeta}|v^\perp\rangle|v^\perp\rangle), \end{aligned}$$

after some cancellation. This does not in general equal $\frac{1}{\sqrt{2}}(|vv\rangle + |v^\perp v^\perp\rangle)$ unless $a, b \in \mathbb{R}$ and $\zeta = 0$.

Proposition. Let $\{|v\rangle, |v^\perp\rangle\}$ be any orthonormal basis of \mathbb{C}^2 . Then

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = \frac{1}{\sqrt{2}}(|vv^\perp\rangle - |v^\perp v\rangle), \quad (3.4)$$

where the second equality is up to some global phase factor. Hence both terms represent the same state.

Proof. For some unitary $U = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$, $|v\rangle = U|0\rangle = \alpha|0\rangle + \beta|1\rangle$, $|v^\perp\rangle = U|1\rangle = \gamma|0\rangle + \delta|1\rangle$. Then

$$\begin{aligned} \frac{1}{\sqrt{2}}(|vv^\perp\rangle - |v^\perp v\rangle) &= \frac{1}{\sqrt{2}}((\alpha|0\rangle + \beta|1\rangle)(\gamma|0\rangle + \delta|1\rangle) - (\gamma|0\rangle + \delta|1\rangle)(\alpha|0\rangle + \beta|1\rangle)) \\ &= \frac{1}{\sqrt{2}}(\alpha\delta - \beta\gamma)(|01\rangle - |10\rangle). \end{aligned}$$

But $\alpha\delta - \beta\gamma = \det U = e^{i\zeta}$ for some $\zeta \in \mathbb{R}$, since U is unitary and so $|\det U| = 1$.³ □



3.2.2 CNOT Gate

First review the single qubit gates discussed in Section 2.4.1, namely $\text{---}\boxed{X}\text{---}$, $\text{---}\boxed{Z}\text{---}$ and $\text{---}\boxed{H}\text{---}$.

Universality The *controlled not* or CNOT gate is applied to a *pair* of qubits, and is the key gate for producing entanglement. Its significance is that every unitary operation on n qubits is a composition of single qubit gates and the CNOT gate. Thus these gates are universal for quantum computation. See [NC10, Section 4.5].

Both qubits need to be physically present in order to apply the CNOT gate.

For the physical realisation of CNOT gates see [ZCDH09, Section 2.4, page 19], [NC10, Chapter 7] and [CCEZ03].

Representations The CNOT gate is represented by  or . In the first representation the top qubit is the *control* and the bottom qubit is the *target* (and conversely in the second). The control qubit is unchanged after the CNOT gate is applied. If the control is $|0\rangle$ then the target is also unchanged. But if the control is $|1\rangle$ then the target is flipped, as for the NOT gate (2.21). Diagrammatically,

$$\begin{array}{cccc} |00\rangle \mapsto |00\rangle & |01\rangle \mapsto |01\rangle & |10\rangle \mapsto |11\rangle & |11\rangle \mapsto |10\rangle \\ |0\rangle \text{---}\bullet\text{---}|0\rangle & |0\rangle \text{---}\bullet\text{---}|0\rangle & |1\rangle \text{---}\bullet\text{---}|1\rangle & |1\rangle \text{---}\bullet\text{---}|1\rangle \\ |0\rangle \text{---}\oplus\text{---}|0\rangle & |1\rangle \text{---}\oplus\text{---}|1\rangle & |0\rangle \text{---}\oplus\text{---}|1\rangle & |1\rangle \text{---}\oplus\text{---}|0\rangle \end{array} \quad (3.5)$$

With respect to the standard basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, CNOT has matrix

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \quad (3.6)$$

Note that CNOT is *unitary*, as are all quantum gates.

Producing Entanglement Consider the input *product* pair

$$|+\rangle|0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)|0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle). \quad (3.7)$$

³If U is unitary then $UU^* = I$ implies $\det U \det U^* = \det I = 1$. But $\det U^* = (\det U)^*$ since $\det A$ is a sum of products of the matrix entries of A for any square matrix A . Hence $|\det U|^2 = 1$ and so $|\det U| = 1$.

Then by (3.5) and linearity,

$$\left. \begin{array}{c} \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \text{ --- } \bullet \\ |0\rangle \text{ --- } \oplus \end{array} \right\} |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \quad (3.8)$$

The output is the *entangled* Bell pair $|\Phi^+\rangle$. To see this consider the input $|00\rangle + |10\rangle$ (from the actual input $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |0\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |10\rangle)$ before normalisation) and note from the properties of the CNOT gate that the first qubit from each of the two kets is unchanged (being the controls), the second 0 in $|00\rangle$ is also unchanged, but the 0 in $|10\rangle$ is flipped.

One could also see this by applying the CNOT matrix to the column vector $\frac{1}{\sqrt{2}}[1010]^t$ which corresponds to the input (3.7), but this is not the best way to gain intuition.

3.2.3 Preparing Bell States

Bell states can physically be prepared from certain atomic reactions.

The quantum circuit way is to use the CNOT gate as in the previous section, but now beginning with states $|0\rangle$ and/or $|1\rangle$ followed by a Hadamard gate as in (2.23) and then a CNOT gate. See (3.9).

$$\begin{array}{cc} \left. \begin{array}{c} |0\rangle \text{ --- } [H] \text{ --- } \bullet \\ |0\rangle \text{ --- } \oplus \end{array} \right\} |\Phi^+\rangle & \left. \begin{array}{c} |0\rangle \text{ --- } [H] \text{ --- } \bullet \\ |1\rangle \text{ --- } \oplus \end{array} \right\} |\Psi^+\rangle \\ \\ \left. \begin{array}{c} |1\rangle \text{ --- } [H] \text{ --- } \bullet \\ |0\rangle \text{ --- } \oplus \end{array} \right\} |\Phi^-\rangle & \left. \begin{array}{c} |1\rangle \text{ --- } [H] \text{ --- } \bullet \\ |1\rangle \text{ --- } \oplus \end{array} \right\} |\Psi^-\rangle \end{array} \quad (3.9)$$

The first example in (3.9) is essentially (3.8), with the Hadamard gate used to send $|0\rangle$ to $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, which is then the control for the CNOT gate, as in (3.8).

For the second example the Hadamard gate again sends $|0\rangle$ to $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ which is again the control. But the target is now $|1\rangle$ so the output is $\frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) = |\Psi^+\rangle$.

For the third example the control is $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ and the target is $|0\rangle$, so the output is $\frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\Phi^-\rangle$.

For the fourth example the control is $H|1\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ and the target is $|1\rangle$, so the output is $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) = |\Psi^-\rangle$.

3.2.4 Interim States in Quantum Circuits

Both here and later, it is often helpful to have a record of the state before and after each gate is applied. For the second example in 3.9 this could be written as

$$\left. \begin{array}{c} |0\rangle \text{ --- } [H] \text{ --- } \bullet \\ |1\rangle \text{ --- } \oplus \end{array} \right\} |\Psi^+\rangle \quad (3.10)$$

$\uparrow \quad \uparrow \quad \uparrow$
 $|\psi_0\rangle \quad |\psi_1\rangle \quad |\psi_2\rangle$

where

$$|\psi_0\rangle = |01\rangle, \quad |\psi_1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle), \quad |\psi_2\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \quad (3.11)$$

3.2.5 Tensor Product of Operators

Here we consider tensor products

$$S \otimes T : \mathbb{C}^2 \otimes \mathbb{C}^2 \rightarrow \mathbb{C}^2 \otimes \mathbb{C}^2, \quad (3.12)$$

since this is what is needed for the immediate applications to Bell pairs. But the key ideas are all here in this setting, so we are basically just simplifying notation.

Example

The Hadamard gate H in (3.10) is applied to the first qubit and the second qubit is unaltered. We can think of the action on the second qubit as an application of the identity map I . If we regard the two qubits together as a single system, then the action on the pair of qubits is denoted by $H \otimes I$, which we call the *tensor product of H and I* .

Then using (3.11) we have

$$\begin{aligned} (H \otimes I) |\psi_0\rangle &= (H \otimes I)(|0\rangle \otimes |1\rangle) = H|0\rangle \otimes I|1\rangle \\ &= \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \otimes |1\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |11\rangle) = |\psi_1\rangle. \end{aligned} \quad (3.13)$$

Definition

More generally, suppose $S : \mathbb{C}^2 \rightarrow \mathbb{C}^2$ (think of S as being applied to the first qubit) and $T : \mathbb{C}^2 \rightarrow \mathbb{C}^2$ (think of T as being applied to the second qubit) are linear operators (usually both hermitian or both unitary). Then the linear operator $S \otimes T : \mathbb{C}^2 \otimes \mathbb{C}^2 \rightarrow \mathbb{C}^2 \otimes \mathbb{C}^2$ is defined in the natural way on the computational basis vectors

$$(S \otimes T)|00\rangle = S|0\rangle \otimes T|0\rangle, \quad (S \otimes T)|01\rangle = S|0\rangle \otimes T|1\rangle, \quad \text{etc.}, \quad (3.14)$$

and extended by linearity

$$\begin{aligned} (S \otimes T)(\alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle) \\ = \alpha_{00}S|0\rangle \otimes T|0\rangle + \alpha_{01}S|0\rangle \otimes T|1\rangle + \alpha_{10}S|1\rangle \otimes T|0\rangle + \alpha_{11}S|1\rangle \otimes T|1\rangle. \end{aligned} \quad (3.15)$$

Moreover, it is easy to check⁴ that

$$(S \otimes T)(|\psi_1\rangle \otimes |\psi_2\rangle) = S|\psi_1\rangle \otimes T|\psi_2\rangle. \quad (3.16)$$

So for unitary operators (gates) in a quantum circuit both qubits are just operated on independently:

$$\begin{array}{ccc} |\psi_1\rangle & \text{---} \boxed{S} \text{---} & S|\psi_1\rangle \\ |\psi_2\rangle & \text{---} \boxed{T} \text{---} & T|\psi_2\rangle \end{array} \quad (3.17)$$

Finally, we remark that the definition of $S \otimes T$ in (3.15) relied on the choice of basis (the canonical basis here). But in Appendix H.3 we see that the definition does not actually depend on the choice of basis. In fact for the general definition we use (3.16) for $|\psi_1\rangle \in V_1$ and $|\psi_2\rangle \in V_2$ as part of the definition of $S \otimes T$ and show it can be extended uniquely by linearity to all of $V_1 \otimes V_2$.

Matrix Representation

Suppose $S, T : \mathbb{C}^2 \rightarrow \mathbb{C}^2$ have matrices with respect to the standard basis $\{|0\rangle, |1\rangle\}$ as follows:

$$S = \begin{bmatrix} S_{11} & S_{12} \\ S_{21} & S_{22} \end{bmatrix}, \quad T = \begin{bmatrix} T_{11} & T_{12} \\ T_{21} & T_{22} \end{bmatrix}. \quad (3.18)$$

⁴Let $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$, $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$. Then

$$\begin{aligned} (S \otimes T)(|\psi_1\rangle \otimes |\psi_2\rangle) &= (S \otimes T)(\alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle) \\ &= \alpha_1\alpha_2S|0\rangle \otimes T|0\rangle + \alpha_1\beta_2S|0\rangle \otimes T|1\rangle + \beta_1\alpha_2S|1\rangle \otimes T|0\rangle + \beta_1\beta_2S|1\rangle \otimes T|1\rangle \\ &= (\alpha_1S|0\rangle + \beta_1S|1\rangle) \otimes (\alpha_2T|0\rangle + \beta_2T|1\rangle) \\ &= S|\psi_1\rangle \otimes T|\psi_2\rangle. \end{aligned}$$

Then it follows from (3.14) that

$$\begin{aligned}
(S \otimes T) |00\rangle &= S |0\rangle \otimes T |0\rangle \\
&= (S_{11} |0\rangle + S_{21} |1\rangle) \otimes (T_{11} |0\rangle + T_{21} |1\rangle) \\
&= S_{11}T_{11} |00\rangle + S_{11}T_{21} |01\rangle + S_{21}T_{11} |10\rangle + S_{21}T_{21} |11\rangle,
\end{aligned}$$

etc. Using the standard lexicographic basis ordering $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ for \mathbb{C}^4 it follows that the matrix of $S \otimes T$ is

$$S \otimes T = \begin{bmatrix} S_{11}T_{11} & S_{11}T_{12} & S_{12}T_{11} & S_{12}T_{12} \\ S_{11}T_{21} & S_{11}T_{22} & S_{12}T_{21} & S_{12}T_{22} \\ S_{21}T_{11} & S_{21}T_{12} & S_{22}T_{11} & S_{22}T_{12} \\ S_{21}T_{21} & S_{21}T_{22} & S_{22}T_{21} & S_{22}T_{22} \end{bmatrix} = \begin{bmatrix} S_{11}T & S_{12}T \\ S_{21}T & S_{22}T \end{bmatrix}. \quad (3.19)$$

That is, multiply each entry in the matrix for S by the matrix for T , thereby obtaining the block matrix on the right.

CNOT is Not a Tensor Product

This is clear from the matrix representations in (3.19) and (3.6).

Moreover, from (3.16) it is clear that a tensor product of operators cannot produce entanglement, unlike CNOT as seen from (3.8) and the discussion which follows it.

Tensoring Preserves Hermitian and Unitary Properties

Suppose S is *hermitian* with orthonormal basis of eigenvectors $\{|v_1\rangle, |v_2\rangle\}$ and corresponding matrix $\begin{bmatrix} s_1 & 0 \\ 0 & s_2 \end{bmatrix}$, where s_1 and s_2 are real. Similarly suppose T is hermitian with eigenvectors $\{|w_1\rangle, |w_2\rangle\}$ and matrix $\begin{bmatrix} t_1 & 0 \\ 0 & t_2 \end{bmatrix}$, where t_1 and t_2 are real.

Then with respect to the orthonormal (from (2.39)) basis $\{|v_1w_1\rangle, |v_1w_2\rangle, |v_2, w_1\rangle, |v_2, w_2\rangle\}$, $S \otimes T$ has matrix $\begin{bmatrix} s_1t_1 & & & \\ & s_1t_2 & & \\ & & s_2t_1 & \\ & & & s_2t_2 \end{bmatrix}$, from (3.19). Hence $S \otimes T$ is hermitian from Appendix B.2.

$S \otimes T$ is hermitian with eigenstates $|v_1w_1\rangle, |v_1w_2\rangle, |v_2, w_1\rangle, |v_2, w_2\rangle$,
and with eigenvalues $s_1t_1, s_1t_2, s_2t_1, s_2t_2$ respectively

Suppose S is *unitary* with orthonormal basis of eigenvectors $\{|v_1\rangle, |v_2\rangle\}$ and corresponding matrix $\begin{bmatrix} e^{i\zeta_1} & 0 \\ 0 & e^{i\zeta_2} \end{bmatrix}$, where ζ_1 and ζ_2 are real. Suppose T is unitary with eigenvectors $\{|w_1\rangle, |w_2\rangle\}$ and corresponding matrix $\begin{bmatrix} e^{i\eta_1} & 0 \\ 0 & e^{i\eta_2} \end{bmatrix}$, where η_1 and η_2 are real.

Then $S \otimes T$ has matrix $\begin{bmatrix} e^{i(\zeta_1+\eta_1)} & & & \\ & e^{i(\zeta_1+\eta_2)} & & \\ & & e^{i(\zeta_2+\eta_1)} & \\ & & & e^{i(\zeta_2+\eta_2)} \end{bmatrix}$ with respect to the orthonormal basis $\{|v_1w_1\rangle, |v_1w_2\rangle, |v_2, w_1\rangle, |v_2, w_2\rangle\}$. Hence $S \otimes T$ is unitary from Appendix B.2.

$$\begin{aligned}
&S \otimes T \text{ is unitary with eigenstates } |v_1w_1\rangle, |v_1w_2\rangle, |v_2, w_1\rangle, |v_2, w_2\rangle, \\
&\text{and with eigenvalues } e^{i(\zeta_1+\eta_1)}, e^{i(\zeta_1+\eta_2)}, e^{i(\zeta_2+\eta_1)}, e^{i(\zeta_2+\eta_2)} \text{ respectively}
\end{aligned} \quad (3.21)$$

3.2.6 Measuring Entangled States

In this section we give a “hands on” approach.

Measuring a Single Unentangled Qubit

Recall that if a single qubit in the state $\alpha|v\rangle + \beta|v^\perp\rangle$ is measured with respect to the basis $\{|v\rangle, |v^\perp\rangle\}$ then the state after measurement is $|v\rangle$ with probability $|\alpha|^2$ and is $|v^\perp\rangle$ with probability $|\beta|^2$. That is, if the outcome is $|v\rangle$ we “cross out” the incompatible (orthonormal) state $|v^\perp\rangle$, obtaining $\alpha|v\rangle + \cancel{\beta|v^\perp\rangle}$, and then renormalise to get $\frac{\alpha}{|\alpha|}|v\rangle$ or equivalently $|v\rangle$. Similarly if the outcome is $|v^\perp\rangle$.

Measuring the First Qubit in an Entangled Pair

It is possible to measure just the first qubit of an entangled pair and consider the instantaneous effect on the entangled pair as a system, even though the individual qubits may be spatially separated by a large distance (say, in principle, in different galaxies). But we cannot measure the combined state of the entangled qubits unless they are both physically present. We return to this later in this section.

Consider the general entangled qubit state for $\mathbb{C}^2 \otimes \mathbb{C}^2$, see (2.43), expressed in terms of the orthonormal bases $\{v, v^\perp\}$ and $\{w, w^\perp\}$:

$$\begin{aligned} & a|vw\rangle + b|vw^\perp\rangle + c|v^\perp w\rangle + d|v^\perp w^\perp\rangle \\ &= a|v\rangle \otimes |w\rangle + b|v\rangle \otimes |w^\perp\rangle + c|v^\perp\rangle \otimes |w\rangle + d|v^\perp\rangle \otimes |w^\perp\rangle \\ &= |v\rangle \otimes (a|w\rangle + b|w^\perp\rangle) + |v^\perp\rangle \otimes (c|w\rangle + d|w^\perp\rangle). \end{aligned} \quad (3.22)$$

Suppose the first qubit is measured with respect to the basis $\{v, v^\perp\}$. By analogy with what happens when measuring a single unentangled qubit, we expect (and it is the case) that there are two possible outcomes obtained by crossing out incompatible states to get before normalising

$$\begin{aligned} & |v\rangle \otimes (a|w\rangle + b|w^\perp\rangle) + \cancel{|v^\perp\rangle \otimes (c|w\rangle + d|w^\perp\rangle)} \\ \text{or } & \cancel{|v\rangle \otimes (a|w\rangle + b|w^\perp\rangle)} + |v^\perp\rangle \otimes (c|w\rangle + d|w^\perp\rangle). \end{aligned} \quad (3.23)$$

After normalising this gives

$$\begin{aligned} & |v\rangle \otimes \left(\frac{a}{\sqrt{|a|^2 + |b|^2}} |w\rangle + \frac{b}{\sqrt{|a|^2 + |b|^2}} |w^\perp\rangle \right) \quad \text{with probability } |a|^2 + |b|^2, \\ & |v^\perp\rangle \otimes \left(\frac{c}{\sqrt{|c|^2 + |d|^2}} |w\rangle + \frac{d}{\sqrt{|c|^2 + |d|^2}} |w^\perp\rangle \right) \quad \text{with probability } |c|^2 + |d|^2. \end{aligned} \quad (3.24)$$

This process is also called the *Partial Measurement Rule*

Note that after measurement of the first qubit the system in this case is no longer entangled.

Note also that measuring just one qubit projects the original state onto one of two half-spaces. This is true more generally if we measure one qubit from a state in $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \dots \otimes \mathbb{C}^2$. But of course in this case the resulting state may still be entangled.

Measuring the Second Qubit

Subsequent measurement and normalisation of the second qubit gives

$$\begin{aligned} & |v\rangle \otimes |w\rangle \quad \text{with probability } (|a|^2 + |b|^2) \frac{|a|^2}{|a|^2 + |b|^2} = |a|^2 \\ & |v\rangle \otimes |w^\perp\rangle \quad \text{with probability } (|a|^2 + |b|^2) \frac{|b|^2}{|a|^2 + |b|^2} = |b|^2 \\ & |v^\perp\rangle \otimes |w\rangle \quad \text{with probability } (|c|^2 + |d|^2) \frac{|c|^2}{|c|^2 + |d|^2} = |c|^2 \\ & |v^\perp\rangle \otimes |w^\perp\rangle \quad \text{with probability } (|c|^2 + |d|^2) \frac{|d|^2}{|c|^2 + |d|^2} = |d|^2 \end{aligned} \quad (3.25)$$

Moreover, if the measurements of the first and second qubits were done in the reverse temporal order the possible outcome states and their probabilities are the same.

Note that the four possible states after measurement, and their probabilities, are consistent with Postulate 2 in Section 2.2 or Section 2.2.5. In the latter case the hermitian operator H is given by (2.8) where the projection operators P_1, \dots, P_4 are orthogonal projection onto $|vw\rangle$, $|vw^\perp\rangle$, $|v^\perp w\rangle$, $|v^\perp w^\perp\rangle$ respectively and the four eigenvalues just need to be distinct.

Measurement in the Computational Basis

The previous two measurements together give measurement in the basis $\{|vw\rangle, |vw^\perp\rangle, |v^\perp w\rangle, |v^\perp w^\perp\rangle\}$.

In particular, measurement for a pair of qubits in the computational basis $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ can be performed in this manner. A tensor matrix representation of this measurement is

$$T = \begin{bmatrix} \lambda_{00} & 0 & 0 & 0 \\ 0 & \lambda_{01} & 0 & 0 \\ 0 & 0 & \lambda_{10} & 0 \\ 0 & 0 & 0 & \lambda_{11} \end{bmatrix}, \quad (3.26)$$

provided $\{\lambda_{00}, \lambda_{01}, \lambda_{10}, \lambda_{11}\}$ are all distinct.

Measuring a Bell Pair For example, consider (see Section 3.2.1)

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle) + \frac{1}{\sqrt{2}}(|1\rangle \otimes |1\rangle). \quad (3.27)$$

From (3.25), measurement in the computational basis gives outcome $|00\rangle$ with probability $1/2$ and outcome $|11\rangle$ with probability $1/2$.

One strange consequence of this is that if Alice obtains $|0\rangle$ (respectively $|1\rangle$) from measuring her qubit on Earth, instantaneously it becomes the situation that Bob will definitely obtain $|0\rangle$ (respectively $|1\rangle$) even if he measures his entangled qubit on Mars.

3.2.7 Measurement in the Bell Basis

In principle, any hermitian operator T on state space should correspond to a physically realisable measurement. However, some measurements are more difficult to perform than others.

For simplicity, suppose the eigenvalues of T are all distinct, in which case T corresponds to measurement in the orthonormal basis given by the eigenspaces of T . One procedure to realise measurement with respect to T is to apply a unitary operator to the system which converts this basis into the standard computational basis, and then measure in the computational basis. Since unitary operations preserve inner products and hence preserve probabilities, this is essentially equivalent to measuring with T .

From Section 2.5.6 the Bell states form an orthonormal basis, and in some applications such as superdense coding, it is necessary to perform a measurement in this basis. See Section 3.3.

From Section 3.2.3, the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ is transformed into the Bell basis $\{|\Phi^+\rangle, |\Psi^+\rangle, |\Phi^-\rangle, |\Psi^-\rangle\}$ by the unitary operation $\text{CNOT} \circ (H \otimes I)$. The inverse operation is unitary and transforms the Bell basis into the computational basis. But the inverse of $\text{CNOT} \circ (H \otimes I)$ is just $(H \otimes I) \circ \text{CNOT}$ ⁵, which is given by application of two standard quantum gates.

So measurement in the Bell basis is physically realisable by first applying $(H \otimes I) \circ \text{CNOT}$ and then measuring in the computational basis.

⁵The inverse of CNOT is CNOT , and of $H \otimes I$ is $H \otimes I$. This is clear by a simple calculation. But better to note that since both are unitary their inverse is their adjoint, and since each is real the adjoint is the transpose, which in both cases is the original matrix.

The following shows the action of $(H \otimes I) \circ \text{CNOT}$ on the Bell basis vectors in quantum circuit notation.

$$\begin{aligned}
 |\Phi^+\rangle & \left\{ \begin{array}{c} \text{---} \bullet \text{---} \boxed{H} \text{---} |0\rangle \\ \text{---} \oplus \text{---} |0\rangle \end{array} \right. & |\Psi^+\rangle & \left\{ \begin{array}{c} \text{---} \bullet \text{---} \boxed{H} \text{---} |0\rangle \\ \text{---} \oplus \text{---} |1\rangle \end{array} \right. \\
 |\Phi^-\rangle & \left\{ \begin{array}{c} \text{---} \bullet \text{---} \boxed{H} \text{---} |1\rangle \\ \text{---} \oplus \text{---} |0\rangle \end{array} \right. & |\Psi^-\rangle & \left\{ \begin{array}{c} \text{---} \bullet \text{---} \boxed{H} \text{---} |1\rangle \\ \text{---} \oplus \text{---} |1\rangle \end{array} \right.
 \end{aligned} \tag{3.28}$$

3.2.8 Local Description for each Qubit

We know the state of the entangled pair is $|\Phi^+\rangle$, but is there some description of Alice's qubit which is local to Alice? (and similarly for Bob?) There is — but it is not obvious, yet elegant and simple.

*** (more to come)***

3.3 Superdense Coding

Background

Suppose Alice and Bob have access to a *quantum* communication channel over which they can send qubits. For example, an optical fibre over which they can send polarised photons, or a cable over which they can send spin 1/2 particles. etc.

If Alice wants to send Bob a single classical bit of information, either 0 or 1, then she can do the following. Send Bob a qubit in the state $|0\rangle$ (e.g. a spin 1/2 particle spin-oriented in the z direction) if she wants to send the bit 0, and send a qubit in the state $|1\rangle$ (e.g. a spin 1/2 particle spin-oriented in the $-z$ direction) if she wants to send the bit 1.

Bob then measures the qubit in the computational basis, (e.g. in the z direction in the case of spin 1/2 particles), and with probability 1 he will in effect obtain the correct bit of information.

This is not very interesting. But it would seem that one cannot do better, since measuring a qubit only gives one bit of information, after which there is no further pre-measurement information obtainable from the qubit.

Outline

Suppose again that Alice and Bob are at distant locations and can access a quantum communication channel as above, but now share a pair of previously prepared qubits in the (entangled) Bell state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle),$$

with Alice holding the first qubit (say) and Bob the second. The entangled pair $|\Phi^+\rangle$ can be prepared ahead of time by a third party, and does not contain any information from Alice.

We refer to the shared Bell state as a *shared resource*.

It is now possible for Alice to send Bob **one** qubit which enables him to extract **two** classical bits of information: 00, 01, 10 or 11.

The idea is as follows.

- Depending on which of the four possible values (for the two bits) that Alice wants to send Bob, Alice performs one of four operations on her qubit from their shared state $|\Phi^+\rangle$. This changes the shared state into one of the four possible Bell states $|\Phi^+\rangle$, $|\Phi^-\rangle$, $|\Psi^+\rangle$, $|\Psi^-\rangle$.
- Alice sends her (single) qubit to Bob, who now has both qubits.
- Bob measures the transformed state in the Bell basis, and from the result recovers the original two bits of information.

Summary

$$1 \text{ (shared) ebit} + 1 \text{ qubit} \xrightarrow[\text{channel}]{\text{quantum}} 2 \text{ bits} \quad (3.29)$$

The sender needs one entangled bit shared with the receiver, and to send one qubit, in order to send two bits of information.

Details

For example, if Alice wants to send the bits 01 to Bob then she applies σ_3 to her qubit. This transforms the shared Bell state via $\sigma_3 \otimes I$ into $|\Phi^-\rangle$. (See (3.13) and the discussion for $H \otimes I$. See (2.22) for the unitary operator σ_3 .)

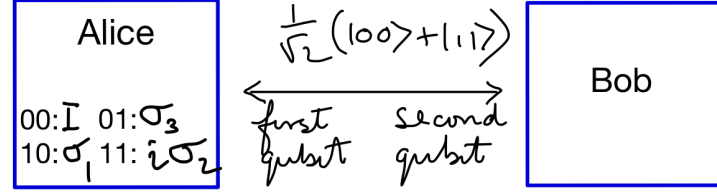


Figure 3.2: Depending on the pair of bits she wants to “send” to Bob, Alice transforms her qubit from the Bell pair $|\Phi^+\rangle$ as indicated, and then sends her qubit to Bob.

In detail, since $\sigma_3|0\rangle = |0\rangle$ and $\sigma_3|1\rangle = -|1\rangle$, i.e. σ_3 is the “phase-flip”,

$$\begin{aligned}
 (\sigma_3 \otimes I) \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) &= \frac{1}{\sqrt{2}}(\sigma_3 \otimes I)(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \\
 &= \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle - |1\rangle \otimes |1\rangle) \\
 &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\Phi^-\rangle.
 \end{aligned}$$

With a little practice one can easily do this without writing down any calculations:

$$\begin{array}{ll}
 \text{for } 00 \text{ apply } I \otimes I \text{ to } \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \text{ to get } & \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = |\Phi^+\rangle \\
 \text{for } 01 \text{ apply } \sigma_3 \otimes I \text{ to get } & \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) = |\Phi^-\rangle \\
 \text{for } 10 \text{ apply } \sigma_1 \otimes I \text{ to get } & \frac{1}{\sqrt{2}}(|10\rangle + |01\rangle) = |\Psi^+\rangle \\
 \text{for } 11 \text{ apply } i\sigma_2 \otimes I \text{ to get } & \frac{1}{\sqrt{2}}(-|10\rangle + |01\rangle) = |\Psi^-\rangle
 \end{array}$$

Note that $i\sigma_2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, and in particular is real. Also note that Alice only acts on her own qubit.

Alice then sends her qubit to Bob so that he has both qubits in the entangled pair.

Bob now performs a measurement in the orthonormal Bell basis for $\mathbb{C}^2 \otimes \mathbb{C}^2$ as described in Section 3.2.7. This gives one of four outcomes with certainty, corresponding to the 4 Bell basis vectors and in this case to the 4 classical bit pairs.

3.4 Teleportation

Outline

Alice has a qubit in an unknown state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$. She wants to send the state to Bob, but she only has a classical communication channel such as a telephone, and only time or resources to send a few bits of classical information. In particular, Alice cannot send the physical qubit to Bob.

But suppose Alice and Bob also share a pair of previously prepared qubits in the (entangled) Bell state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle),$$

There are three qubits to consider. The first qubit is the qubit with the unknown state held by Alice and whose state she wants to send to Bob. The second qubit is also held by Alice and is the first qubit in the entangled Bell pair. The third qubit is the one held by Bob, and is the second qubit in the entangled bell pair.

Alice can send the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ of her first qubit to Bob as follows:

- Alice measures her two qubits in the Bell Basis, which in particular first involves entangling her two qubits, and hence all three qubits.
- There are 4 possible measurement results for Alice, $|\Phi^+\rangle, |\Phi^-\rangle, |\Psi^+\rangle, |\Psi^-\rangle$ (which can hence be labelled by two bits of information).
- As a consequence of Alice's measurement, Bob's qubit is disentangled from the first two qubits. Moreover, it's state will be one of 4 possibilities $\alpha|0\rangle \pm \beta|1\rangle$ or $-\alpha|0\rangle \pm \beta|1\rangle$, corresponding to Alice's 4 possible outcomes.
- Alice sends Bob the two bit message stating which Bell state was her outcome. From this information Bob can apply the appropriate unitary transformation to reconstruct from his qubit the original state of Alice's qubit.

Amazing!!

Summary

$$1 \text{ (shared) ebit} + 2 \text{ bits} \xrightarrow[\text{channel}]{\text{classical}} 1 \text{ qubit} \quad (3.30)$$

The sender needs one entangled bit shared with the receiver, and to send two (classical) bits of information, in order to teleport one (unknown) qubit.

Details

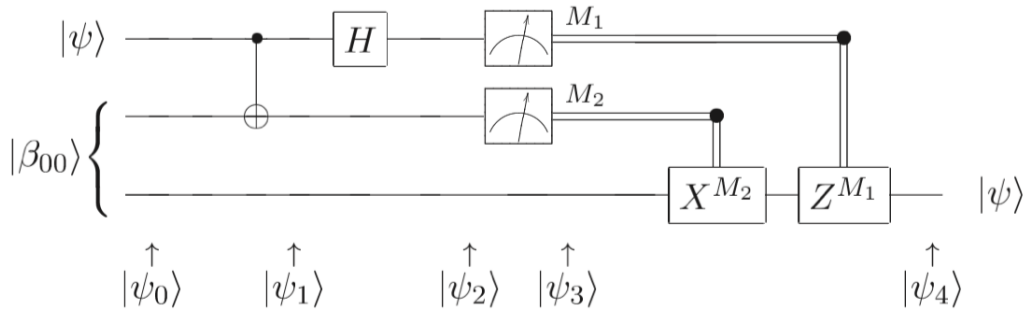


Figure 3.3: Teleportation circuit. $|\beta_{00}\rangle = |\Phi^+\rangle$, $X = \sigma_1$, $Z = \sigma_3$. See Footnote 6 for an explanation.

Following Figure 3.3, the top qubit begins in the unknown state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ and belongs to Alice.

The qubits in the second and third lines begin in the entangled state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, with the qubit on the second line belonging to Alice and that on the third belonging to Bob.

So in Figure 3.3,

$$\begin{aligned}
|\psi_0\rangle &= |\psi\rangle \otimes |\Phi^+\rangle \\
&= (\alpha|0\rangle + \beta|1\rangle) \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\
&= \frac{1}{\sqrt{2}}(\alpha|000\rangle + \alpha|011\rangle + \beta|100\rangle + \beta|111\rangle).
\end{aligned} \tag{3.31}$$

Looking from $|\psi_0\rangle$ to $|\psi_3\rangle$ in Figure 3.3 we see from (3.28) that Alice will be measuring her pair of qubits in the Bell basis. For this reason it will be useful to rewrite the state of Alice's qubits as a superposition of the Bell basis vectors. For this note from (3.2) that

$$\begin{aligned}
|00\rangle &= \frac{1}{\sqrt{2}}(|\Phi^+\rangle + |\Phi^-\rangle) & |01\rangle &= \frac{1}{\sqrt{2}}(|\Psi^+\rangle + |\Psi^-\rangle) \\
|10\rangle &= \frac{1}{\sqrt{2}}(|\Psi^+\rangle - |\Psi^-\rangle) & |11\rangle &= \frac{1}{\sqrt{2}}(|\Phi^+\rangle - |\Phi^-\rangle).
\end{aligned} \tag{3.32}$$

It follows from (3.31) that

$$\begin{aligned}
|\psi_0\rangle &= \frac{1}{2} \left(\alpha(|\Phi^+\rangle + |\Phi^-\rangle)|0\rangle + \alpha(|\Psi^+\rangle + |\Psi^-\rangle)|1\rangle \right. \\
&\quad \left. + \beta(|\Psi^+\rangle - |\Psi^-\rangle)|0\rangle + \beta(|\Phi^+\rangle - |\Phi^-\rangle)|1\rangle \right) \\
&= \frac{1}{2} \left(|\Phi^+\rangle(\alpha|0\rangle + \beta|1\rangle) + |\Phi^-\rangle(\alpha|0\rangle - \beta|1\rangle) \right. \\
&\quad \left. + |\Psi^+\rangle(\beta|0\rangle + \alpha|1\rangle) + |\Psi^-\rangle(-\beta|0\rangle + \alpha|1\rangle) \right).
\end{aligned} \tag{3.33}$$

It follows as in (3.2.6) (crossing out incompatible states) that measurement of Alice's pair of qubits in the Bell basis⁶ results in the system state $|\Phi^+\rangle(\alpha|0\rangle + \beta|1\rangle)$ with probability $\frac{1}{4}(|\alpha|^2 + |\beta|^2) = \frac{1}{4}$. In this case the state of Bob's qubit will be $\alpha|0\rangle + \beta|1\rangle$.

Similarly, if the outcome for Alice is $|\Phi^-\rangle$, $|\Psi^+\rangle$ or $|\Psi^-\rangle$, each of which also occurs with probability $\frac{1}{4}$, then the respective outcomes for Bob's state are $\alpha|0\rangle - \beta|1\rangle$, $\beta|0\rangle + \alpha|1\rangle$ and $-\beta|0\rangle + \alpha|1\rangle$ respectively. They are similar to, and in fact unitary images of, the state to be teleported.


If Alice now sends Bob the information as to which state she observed, and this information requires just two bits, then by appropriate choice of unitary gate Bob can transform his qubit into the state to be teleported.

More precisely,

- if Alice's result is $|\Phi^+\rangle$ then Bob's qubit is already in the desired state.
- If Alice's result is $|\Phi^-\rangle$ then Bob applies the phase flip gate $\sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$.
- If Alice's result is $|\Psi^+\rangle$ then Bob applies the bit flip gate $\sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$.
- And finally, if Alice's result is $|\Psi^-\rangle$ then Bob applies the gate $\sigma_3\sigma_1 = i\sigma_2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$.

Note that Alice's original qubit has now become part of one of a Bell state, and its original state is lost. So there is no cloning involved in teleportation, nor can there be by the No-Cloning result in Section 3.1.

⁶The measurement in the Bell basis includes *all* steps in going from $|\psi_0\rangle$ to $|\psi_3\rangle$ in Figure 3.3. This first involves entanglement of Alice's 2 qubits via CNOT, then Hadamard on the first qubit, then measurements in the standard computational basis on each of Alice's 2 qubits. The outcome for each qubit is a classical bit with value 0 or 1.

Figure 3.3 follows the standard convention of a single wire for qubits, a double wire for classical bits,  for a single qubit measurement in the computational basis and a superscript for the measurement label outcome.

If the outcome of the second qubit measurement by Alice is 0 then Bob will first apply $X^0 = \sigma_1^0 := I$ to his qubit, and if the outcome of the second qubit measurement by Alice is 1 then Bob will first apply $X^1 = \sigma_1^1 = \sigma_1$ to his qubit.

If the outcome of the first qubit measurement by Alice is 0 then Bob will next apply $Z^0 = \sigma_3^0 := I$ to his qubit, and if the outcome of the first qubit measurement by Alice is 1 then Bob will next apply $Z^1 = \sigma_3^1 = \sigma_3$ to his qubit.

3.5 Bell & CHSH Inequalities

3.5.1 History

We discussed in Section 1.5 how Einstein, Podolsky and Rosen argued that quantum theory was not complete. More precisely, in the context of the EPR type experiment discussed there, they would argue that 50% of the qubit pairs prepared in the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ must have been entangled in such a way that on being measured in the basis $\{|0\rangle, |1\rangle\}$ they would both give the outcome $|0\rangle$, and the other 50% of the qubit pairs would both give the outcome $|1\rangle$. This would explain the perfect correlation. Since quantum theory does not include such information, they argued quantum theory was incomplete. However, they were unsuccessful in finding a satisfactory way to extend/complete quantum theory. Neils Bohr argued that quantum theory was indeed complete and Nature operated in the precisely nondeterministic way that the theory predicted.

In 1964 John Bell [Bel64] proposed an experiment that could determine which alternative was correct. He showed that under certain circumstances the correlations predicted by quantum mechanics/theory are stronger than could be accounted for by *any* classical explanation. In 1969 Clauser, Horne, Shimony and Holt [CHSH69] proposed a variation of Bell's experiment and it was carried out by Aspect, Dalibard and Gérard in 1982 [ADR82], with many subsequent refinements closing any possible loopholes in the experiments, the latest being by Juan Yin et al. [YCL⁺17]. Quantum theory is indeed complete. For most quantum experiments there is no classical explanation for the experimentally observed correlations which are, however, predicted by quantum theory.

3.5.2 CHSH Experimental Setup

Entangled Qubits Used Many pairs of qubits are prepared in the entangled Bell state

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle), \quad (3.34)$$

see (3.3). Think of 10,000 samples.

In each case the first qubit is sent to Alice and the second to Bob, with a long distance between them, see Figure 1.8.

Correlated Qubits If Alice tests her qubit w.r.t. $|0\rangle$ then the result is either $|0\rangle$ or $|1\rangle$ each with equal probability. Moreover, according to quantum theory as discussed in Section 3.2.6, the resulting joint state of the pair after measurement is $|00\rangle$ or $|11\rangle$ respectively, each with probability $1/2$. These are product (no longer entangled) states and in particular the state of Bob's qubit is then instantaneously either $|0\rangle$ or $|1\rangle$ respectively.

Similarly, if Alice tests her qubit w.r.t. $|+\rangle$ then the result is $|+\rangle$ or $|-\rangle$ each with equal probability. the resulting joint state of the pair after measurement is $|++\rangle$ or $|--\rangle$ respectively, each with probability $1/2$. The state of Bob's qubit is then instantaneously also either $|+\rangle$ or $|-\rangle$ respectively.

So if Alice measures w.r.t. $|0\rangle$ and Bob also measures w.r.t. $|0\rangle$ then the outcomes for each experimenter will be the same, namely $|0\rangle$ or $|1\rangle$. Similarly if each experimenter measures w.r.t. $|+\rangle$.

Measurements Used Alice randomly and independently, and independent of any choices made by Bob, with probability $1/2$ in each case:⁷(see Figure 3.4)

- Measures her qubit with respect to either $|0\rangle$ or $|+\rangle$, see Section 2.2.2.
- On the Bloch sphere $S^2 \subset \mathbb{R}^3$ this corresponds to the z and x axes respectively.⁸
- In the case of spin $1/2$ particles, this corresponds to measuring spin in the z and x directions respectively. See Section 2.3.
- We denote the two possible measurements available to Alice by \hat{Q} and \hat{R} respectively.

⁷By means of a random number generator, or perhaps by exercising her free will!

⁸Note that the angle between $|0\rangle$ and $|+\rangle$ in \mathbb{C}^2 is $\pi/4$ since $(|0\rangle, |+\rangle) = (|0\rangle, \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)) = \frac{1}{\sqrt{2}} = \cos \frac{\pi}{4}$, while the angle between the z and x directions in \mathbb{R}^3 is (of course) $\pi/2$.

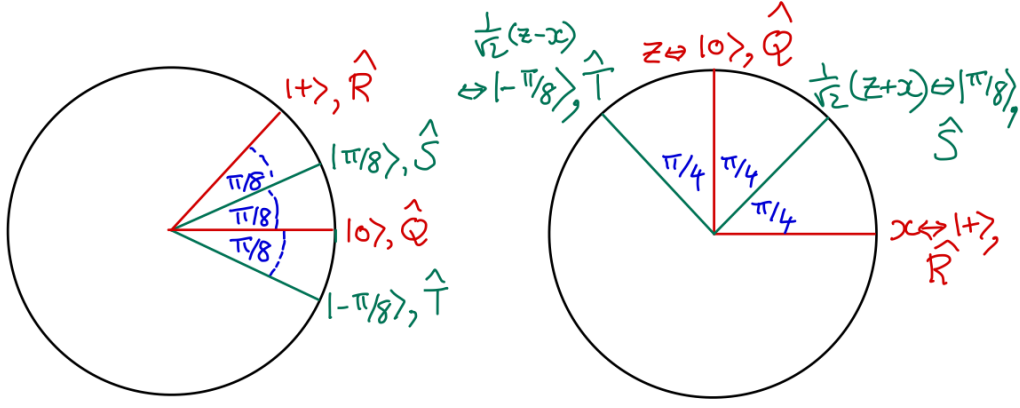


Figure 3.4: CHSH measurements, Alice red and Bob green. The left side is a section through the unit sphere $S^3 \subset \mathbb{C}^2$, the right side a section through the Bloch sphere $S^2 \subset \mathbb{R}^3$. Alice's two possible measurements are each w.r.t. one of the two red qubits on the left or equivalently the corresponding directions on the right. Bob's possible measurements are similarly given in green.

Bob similarly, randomly and independently in each experiment, and independent of any choices made by Alice, with probability $1/2$ in each case: (see Figure 3.4)

- Measures his qubit with respect to either $|\pi/8\rangle$ or $|- \pi/8\rangle$, obtained by rotating the $|0\rangle$ axis by $\pm\pi/8$ in the real section of \mathbb{C}^2 containing $|0\rangle$ and $|+\rangle$ (and $|1\rangle$). So $|\pm\pi/8\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |+\rangle)$.
- On the Bloch sphere $S^2 \subset \mathbb{R}^3$ this corresponds to the $\frac{1}{\sqrt{2}}(z \pm x)$ directions respectively, see Figure 3.4.
- In the case of spin $1/2$ particles this corresponds to measuring spin in the $\frac{1}{\sqrt{2}}(z \pm x)$ directions respectively.
- We denote the two possible measurements available to Bob by \hat{S} and \hat{T} respectively.

It follows there are four *possible* (double) experiments that could be performed on each qubit pair, denoted by $\hat{Q}\hat{S}$, $\hat{Q}\hat{T}$, $\hat{R}\hat{S}$, $\hat{R}\hat{T}$ in an obvious manner, but with one and only one such experiment performed for each such qubit pair.⁹ See Table 3.1.

	$\hat{Q}\hat{S}$	$\hat{Q}\hat{T}$	$\hat{R}\hat{S}$	$\hat{R}\hat{T}$
Alice	$\hat{Q} = 0\rangle, z$	$\hat{Q} = 0\rangle, z$	$\hat{R} = +\rangle, x$	$\hat{R} = +\rangle, x$
Bob	$\hat{S} = \frac{\pi}{8}\rangle, \frac{1}{\sqrt{2}}(z+x)$	$\hat{T} = -\frac{\pi}{8}\rangle, \frac{1}{\sqrt{2}}(z-x)$	$\hat{S} = \frac{\pi}{8}\rangle, \frac{1}{\sqrt{2}}(z+x)$	$\hat{T} = -\frac{\pi}{8}\rangle, \frac{1}{\sqrt{2}}(z-x)$

Table 3.1: **Possible Measurement Pairs.** There are four measurement pairs used for measuring a pair of entangled qubits. For example, $\hat{R}\hat{T}$ corresponds to measuring Alice's qubit with respect to $|+\rangle$ in \mathbb{C}^2 , or equivalently w.r.t. the x direction in the Bloch sphere; and measuring Bob's qubit w.r.t. $|\frac{-\pi}{8}\rangle$ or equivalently $\frac{1}{\sqrt{2}}(z-x)$.

Spatial Separation For each entangled pair of qubits, the measurement of the first qubit by Alice and of the second qubit by Bob are spatially separated. That is, there is no time (at the speed of light) for classical information regarding the choice of measurement direction by Bob, or regarding the outcome of that measurement, to reach Alice's qubit before it is measured. Similarly, analogous information regarding Alice's measurement and the outcome cannot reach Bob's qubit before it is measured.

This enforces the requirement that Alice's choice of measurement is independent of Bob's choice, and conversely.

⁹Since the qubit is changed by the measurement process, and subsequent measurement would give no further information about the qubit prior to the first measurement.

Multiple Experiments The experiment is repeated many times, say 10,000, with a different pair each time, but every pair is entangled in the same state $|\Phi^+\rangle$.

Record of the Experiments See Table 3.2. In order to agree with standard conventions, the outcome of each measurement is denoted by $+1$ if the outcome is the same as the measurement state/measurement direction and by -1 if the outcome is the orthogonal state/opposite direction.

Alice and Bob keep a record in each of the 10,000 experiments of the measurement they performed (\hat{Q} or \hat{R} for Alice, \hat{R} or \hat{S} for Bob) and of the numerical outcome (± 1). It is convenient to denote the *numerical* outcome for Alice by Q or R , and that for Bob by S or T , depending in each case on the measurement performed.

After the 10,000 experiments have all been completed, Alice and Bob get together and compare records, and in particular for each (double) experiment they obtain a number ± 1 by multiplying together their individual numerical outcomes for that experiment. This number is denoted by $Q \cdot S$, $Q \cdot T$, $R \cdot S$ or $R \cdot T$. For example, the record for the 10,000 experiments might be as in Table 3.2.

Experiment	1	2	3	4	5	6	
Alice	$Q = +1$	$R = -1$	$R = -1$	$R = +1$	$Q = -1$	$Q = 1$	
Bob	$S = +1$	$S = -1$	$S = +1$	$T = -1$	$S = -1$	$T = -1$...
Product	$Q \cdot S = +1$	$R \cdot S = +1$	$R \cdot S = -1$	$R \cdot T = -1$	$Q \cdot S = +1$	$Q \cdot T = -1$	

.....	9,998	9,999	10,000
	$R = +1$	$Q = -1$	$R = -1$
	$T = -1$	$S = -1$	$S = -1$
	$R \cdot T = -1$	$Q \cdot S = +1$	$R \cdot S = +1$

Table 3.2: **Record of CHSH Experiments.** For each experiment the table shows the measurement choices made by Alice and by Bob, the outcomes after measuring their individual qubits, and the product of the two outcomes.

3.5.3 Preliminary Discussion of the Results

We find from the results of the 10,000 experiments that there is a correlation between the outcomes Q & S , Q & T and R & S , in the sense that the product of the two values in each case is more frequently $+1$ than -1 . On the other hand there is anticorrelation between the values of R and T in the sense that the product of the two values in this case is more often -1 than $+1$.

This is not surprising! In Figure 3.4 we see that \hat{Q} is near \hat{S} , \hat{Q} is near \hat{T} , \hat{R} is near \hat{S} , but \hat{R} is near $\hat{T}^\perp = |3\pi/8\rangle$ (i.e. $\frac{1}{\sqrt{2}}(x - z)$ on the Bloch Sphere).

In fact, both experimentally and from quantum theory (Section 3.5.6) we find the following precise average/expected values:

$$\mathbb{E}(Q \cdot S) = \mathbb{E}(Q \cdot T) = \mathbb{E}(R \cdot S) = -\mathbb{E}(R \cdot T) = \frac{\sqrt{2}}{2} \approx .71. \quad (3.35)$$

If there were no correlations then the expected values would be 0 in each case.

Is it possible to explain these experimentally observed correlations from a classical perspective, e.g. by Newtonian physics? We show from (3.37) and (3.38) this is not possible. But let's make an attempt in order to see where the problems occur.

Suppose that at the time of entanglement each pair contained some information such as

$$Q = +1, R = +1; S = +1, T = -1 \quad \text{or} \quad Q = -1, R = +1; S = -1, T = -1, \text{ etc.}$$

(there are $2^4 = 16$ possibilities), but that this information is not available to us because we do not have sufficiently refined scientific instruments or knowledge or whatever. If the information for a

particular entangled pair is (for example) the second case above, and if Alice performs experiment \hat{R} and Bob performs measurement \hat{T} , then the information is interpreted as implying the outcome will be $R \cdot T = (+1) \times (-1) = -1$.

But we will see by a simple but ingenious algebraic argument in Section 3.5.4 that it is not possible by classical means to explain the correlations observed experimentally in (3.35).

We will also see in Section 3.5.6 that these correlations *are* predicted precisely by quantum theory.

3.5.4 Classical Analysis; Physical Realism, Locality, Random Choice

In the classical analysis of the CHSH experiment we assume

- physical realism,
- locality,
- the ability to make random choices concerning which of two available experiments will be performed (either by a stochastic random number generator or by exercising our free will) but in accordance with the probabilistic requirements imposed on Bob's and Alice's experimental choices.

Physical Realism For each entangled pair of qubits Alice and Bob each performed a single measurement, together giving *one* of the four possibilities $\hat{Q}\hat{S}$, $\hat{Q}\hat{T}$, $\hat{R}\hat{S}$ or $\hat{R}\hat{T}$

Although outcomes for the other *three* possibilities were not measured,¹⁰ from a classical point of view there is some value that *would* have been obtained *if* Alice and Bob had performed another pair of measurements instead of the one that *was* performed. So we make the assumption that, even though measurement may (and here does) interfere with the particle being measured, Q , R , S and T represent real physical properties of the qubits that could have been measured. This is sometimes called the assumption of *physical realism* and was essentially universal throughout science before quantum theory emerged.

A Simple Calculation Now consider for each entangled qubit pair

$$Q \cdot S + Q \cdot T + R \cdot S - R \cdot T = (Q + R) \cdot S + (Q - R) \cdot T = \pm 2 \leq 2. \quad (3.36)$$

To see the last equality note that $Q, R = \pm 1$ and so either $Q + R = 0$ or $Q - R = 0$. Since $S, T = \pm 1$ the result follows.

In particular, taking the expected (i.e. average) value over many such entangled qubits, e.g. over the 10,000 experiments previously discussed,

$$\mathbb{E}(Q \cdot S + Q \cdot T + R \cdot S - R \cdot T) = \mathbb{E}(Q \cdot S) + \mathbb{E}(Q \cdot T) + \mathbb{E}(R \cdot S) - \mathbb{E}(R \cdot T) \leq 2. \quad (3.37)$$

We are *not* claiming that the outcomes Q and S are independent. Indeed, at the time of entanglement it may have been arranged for 90% of pairs of qubits that the outcome for experiment \hat{Q} is 1 and for experiment \hat{S} is 1, while for the other 10% of qubit pairs the outcomes are 1 for \hat{Q} and -1 for \hat{S} . So there may be a *high degree of correlation* on classical grounds.

Locality / No Faster than Light Signalling As well as physical realism, we make the assumption for example, that the outcome for \hat{S} (one of the possible two measurements made by Bob) does not depend on the choice of measurement performed by Alice. Alice and Bob are performing spatially separated experiments. Assuming there cannot be faster than light communication, Bob's qubit cannot know which measurement direction (\hat{Q} or \hat{R}) was chosen by Alice.¹¹

This is what allows us to factorise in (3.36). For example, it is the same value of S in $Q \cdot S$ and $R \cdot S$. The assumption is that whether Alice had measured in the \hat{Q} or the \hat{R} direction, the result of Bob's measurement in the \hat{S} direction would be the same.

¹⁰Nor can one do so, as we know that after measuring no further information can be obtained regarding the original qubit.

¹¹We *are* however allowing for the possibility that Bob's qubit knows what the outcome for *Alice's* qubit would be *if* direction \hat{Q} was chosen by Alice and what the outcome would be *if* direction \hat{R} were chosen by Alice. This information could potentially have been available to both qubits used in experiment 1 from the time of their entanglement.

This is usually called the assumption of *locality*, or in this case *no faster than light signalling*. Events cannot be affected by other events outside their past light cone, they cannot be affected by something for which there is not sufficient time for a signal (e.g. by photons) to arrive. This assumption, like physical realism, was also essentially universal throughout science before quantum theory emerged.¹²

Random Choice The third assumption we make implicitly in our classical analysis concerns the random choice of \hat{Q} or \hat{R} available to Alice and the random choice of \hat{S} or \hat{T} available to Bob. We assume for example that in the approximately 2,500 experiments (1/4 of the 10,000 experiments) where Alice chooses experiment \hat{Q} and Bob chooses \hat{S} , the average value of $Q \cdot S$ is the same as the average value of $Q \cdot S$ over all 10,000 experiments (remember that by physical realism we are already assuming Q and S exist for all 10,000 experiments, even though we did not measure them in about 7,500 cases). We use this assumption for the equality assertion in (3.37), from which it follows that all five *expectations* (average values) can be taken over *all* 10,000 experiments.

3.5.5 Experimental Results

Repeated experiments show, to 12 or more decimal places, that

$$\mathbb{E}(Q \cdot S) + \mathbb{E}(Q \cdot T) + \mathbb{E}(R \cdot S) - \mathbb{E}(R \cdot T) = 2\sqrt{2}, \quad (3.38)$$

which contradicts (3.36).

3.5.6 Quantum Analysis

We obtain the quantum predictions as in Section 3.2.6. It is convenient to assume that Alice makes her observations just prior to Bob (but not allowing enough time for signalling in either direction at the speed of light). But exactly the same prediction and analogous argument is made if Bob is first. Quantum theory does not require that one set of measurements precedes the other.¹³

There are four possibilities for the combined choices of Alice and Bob, $\hat{Q}\hat{S}$, $\hat{Q}\hat{T}$, $\hat{R}\hat{S}$ or $\hat{R}\hat{T}$. See Figure 3.4.

In the first three cases the measurement directions differ by $\pi/8$ (or $\pi/4$ on the Bloch sphere). In the fourth case the difference is $3\pi/8$ (or $3\pi/4$ on the Bloch sphere). Recall that the entangled qubits being measured were all prepared in the state $|\Phi^+\rangle$, see (3.34).

In the first two cases, if Alice measures first then the outcome is $+1$ or -1 and the new state is $|00\rangle$ or $|11\rangle$ respectively. Since Bob's frame is just rotated by $\pm\pi/8$ from Alice's frame, with probability¹⁴

$$\cos^2 \frac{\pi}{8} = \frac{1}{2} \left(1 + \cos \frac{\pi}{4} \right) = \frac{2 + \sqrt{2}}{4} \approx .86,$$

the outcome will be the same $+1$ or -1 . But in the fourth case, the outcomes will be the same with probability $\cos^2(3\pi/8) = \sin^2(\pi/2 - 3\pi/8) = 1 - \cos^2(\pi/8)$, and hence different with probability $\cos^2(\pi/8)$.

So with probability $\frac{2+\sqrt{2}}{4} \approx .86$ we have correlation in the first 3 cases and anti-correlation in the fourth case. The same applies if Bob measures first.

It follows that

$$\mathbb{E}(Q \cdot S) = \frac{2 + \sqrt{2}}{4} \times 1 + \frac{2 - \sqrt{2}}{4} \times (-1) = \frac{\sqrt{2}}{2}.$$

Similarly,

$$\mathbb{E}(Q \cdot T) = \frac{\sqrt{2}}{2}, \quad \mathbb{E}(R \cdot S) = \frac{\sqrt{2}}{2}, \quad \mathbb{E}(R \cdot T) = -\frac{\sqrt{2}}{2}.$$

¹²Prior to the theory of relativity, one might have said informally that what is being ruled out is almost instantaneous signalling from distant galaxies!

¹³Not could it if it were to be consistent (which it is) with special relativity for spatially separated events.

¹⁴This follows from (3.3) and the corresponding discussion with $|v\rangle$ there replaced by $|0\rangle$ in the first two cases and by $|+\rangle$ in the third and fourth cases. Then apply the discussion in Section 2.2.2 or the "Experimental Observation" in Section 2.3.1.

Hence

$$\mathbb{E}(Q \cdot S) + \mathbb{E}(Q \cdot T) + \mathbb{E}(R \cdot S) - \mathbb{E}(R \cdot T) = 2\sqrt{2}, \quad (3.39)$$

in perfect agreement with experiment as noted in (3.35).

3.6 GHZ

Chapter 4

Quantum Circuits

Contents

4.1	Quantum Gates	66
4.2	Deutsch-Jozsa Algorithm	66
4.3	Shor's Algorithm	66

4.1 Quantum Gates

4.2 Deutsch-Jozsa Algorithm

4.3 Shor's Algorithm

Chapter 5

Composite Systems

Contents

5.1	Ensembles and Density Operators	67
5.2	The Bloch Ball	67
5.3	Subsystems and the Reduced Density Operator	67
5.4	Schmidt Decomposition and Purification	67

5.1 Ensembles and Density Operators

5.2 The Bloch Ball

5.3 Subsystems and the Reduced Density Operator

5.4 Schmidt Decomposition and Purification

Appendix A

Visualising Higher Dimensions

Sometimes it is convenient to try and visualise \mathbb{R}^n for $n \geq 4$ and \mathbb{C}^n for $n \geq 2$.

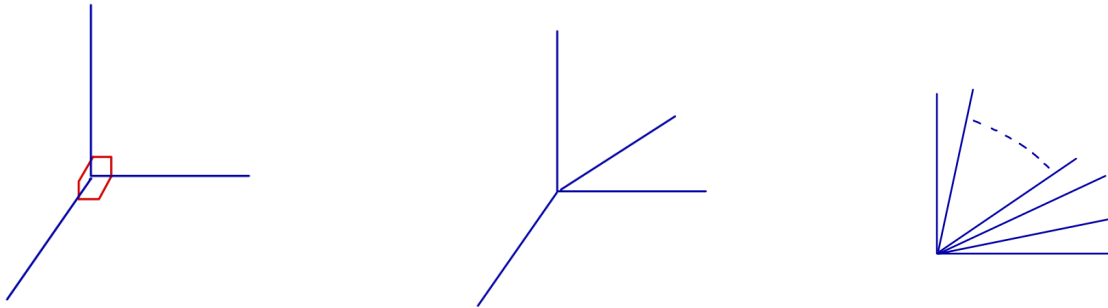


Figure A.1: 3 mutually orthogonal lines in \mathbb{R}^3 , 4 in \mathbb{R}^4 , n in \mathbb{R}^n .

Exercise: Explain to your 2-D friend *living in the 2-D plane of the paper*, why the 3 lines (segments) in the first diagram are projections into \mathbb{R}^2 of 3 mutually orthogonal lines in \mathbb{R}^3 .

In a similar manner, explain to your 3-D friend in this room, why the 4 lines in the second diagram are actually the projections into \mathbb{R}^3 (and then projected onto \mathbb{R}^2 , but forget that part) of 4 mutually orthogonal lines in \mathbb{R}^4 .

Similarly, explain why the $n \geq 6$ lines in the third diagram are actually the projections into \mathbb{R}^3 of n mutually orthogonal lines in \mathbb{R}^n .

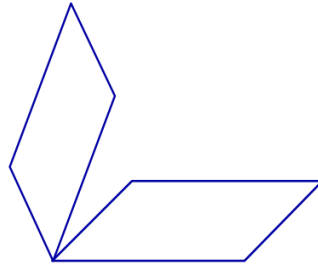


Figure A.2: 2 orthogonal 2-D real subspaces of \mathbb{R}^4 , or 2 orthogonal 1-D complex lines in \mathbb{C}^2 .

Exercise: Explain to someone why the above diagram represents (after “extending both rectangles to infinity in all directions”) two 2-D real orthogonal subspaces of \mathbb{R}^4 , whose only point of intersection is the origin.

Then explain why the diagram also represents (after again extending each rectangle) two orthogonal “complex lines”¹ (which of course are each of real dimension 2) in \mathbb{C}^2 .

¹A *complex line* in \mathbb{C}^n consists of all vectors of the form αv for some fixed non-zero $v \in \mathbb{C}^n$ and all $\alpha \in \mathbb{C}$.

Appendix B

Hermitian and Unitary Operators

Contents

B.1 Inner Product Space	70
B.1.1 Inner Product	70
B.1.2 Norm	71
B.1.3 Norms and Inner Products	71
B.1.4 Angle	71
B.1.5 Orthogonal Projections	72
B.2 Definitions in Terms of a “Good” Orthonormal Basis	72
B.2.1 Hermitian Operator	72
B.2.2 Unitary Operator	73
B.2.3 Normal Operator	74
B.3 Definitions in Terms of Adjoint Operator	74
B.3.1 Adjoint	74
B.3.2 Hermitian Operator	74
B.3.3 Unitary Operator	75
B.3.4 Normal Operator	75
B.4 2×2 Classification	75
B.5 Polar Decomposition	75
B.6 Another Characterisation	76

I summarise the main results for linear operators $T : \mathbb{C}^n \rightarrow \mathbb{C}^n$ ($T : \mathbb{R}^n \rightarrow \mathbb{R}^n$) which are related to the inner product on \mathbb{C}^n (\mathbb{R}^n).

Often I confuse the operator and the matrix of the operator with respect to some basis (the basis being understood from context).

If the proofs are not relatively straightforward I will indicate this.

I also discuss normal operators, but we will not use them in this set of notes.

B.1 Inner Product Space

Here we are interested in real or complex finite dimensional spaces V , often \mathbb{R}^n or \mathbb{C}^n .

B.1.1 Inner Product

An *inner product space* is a real or complex vector space together with an associated inner product $\langle \cdot, \cdot \rangle$. The *inner product* is a map into \mathbb{R} or \mathbb{C} with the properties

- $\langle u, v \rangle = \overline{\langle v, u \rangle}$ (*symmetry*)

- $\langle \alpha u, v \rangle = \alpha \langle u, v \rangle$ (mathematics) or $\langle u, \alpha v \rangle = \alpha \langle u, v \rangle$ (physics, computer science) (*linearity* in one of the arguments and hence conjugate linearity in the other)
- $\langle u, u \rangle \geq 0$, and $= 0$ iff $u = \mathbf{0}$

The *standard inner products* on \mathbb{R}^n and \mathbb{C}^n are

- $\langle u, v \rangle = u_1 v_1 + \cdots + u_n v_n$
- $\langle u, v \rangle = u_1 \bar{v}_1 + \cdots + u_n \bar{v}_n$ (maths) or $\langle u, v \rangle = \bar{u}_1 v_1 + \cdots + \bar{u}_n v_n$ (physics, comp sci)

B.1.2 Norm

The *norm* of u is $\|u\| = \langle u, u \rangle^{1/2}$, the *distance* between u and v is $\|u - v\|$. The distance is a metric. The *Cauchy-Schwarz inequality* is $|\langle u, v \rangle| \leq \|u\| \|v\|$.

B.1.3 Norms and Inner Products

The inner product can be defined from its norm (so norm preserving maps are inner product preserving).

- real case: $\langle u, v \rangle = \frac{1}{4}(\|u + v\|^2 - \|u - v\|^2)$
- complex case: $\langle u, v \rangle = \frac{1}{4}(\|u + v\|^2 + i\|u + iv\|^2 - \|u - v\|^2 - i\|u - iv\|^2)$

Warning: Not every norm actually defines an inner product in this way. The necessary and sufficient condition is that the norm satisfies the *parallelogram identity*: $2\|u\|^2 + 2\|v\|^2 = \|u + v\|^2 + \|u - v\|^2$.

B.1.4 Angle

The *angle* θ between u and v in a *real* inner product space is defined by $\cos \theta = \frac{\langle u, v \rangle}{\|u\| \|v\|}$ with $\theta \in [0, \pi]$, and hence by $\cos \theta = \langle u, v \rangle$ if u and v are unit vectors.

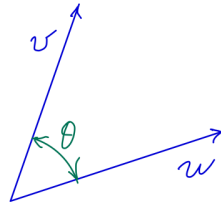


Figure B.1: $u, v \in \mathbb{R}^n$ are unit vectors, $\langle u, v \rangle = \cos \theta$ is the angle between them.

For *complex* inner product spaces the *angle* between u and v is defined by $\cos \theta = \frac{|\langle u, v \rangle|}{\|u\| \|v\|}$ with $\theta \in [0, \pi/2]$, and in particular by $\cos \theta = |\langle u, v \rangle|$ if u and v are unit vectors.

The definition of θ is invariant under replacing u by αu and v by βv for any $\alpha, \beta \in \mathbb{C}$. In particular, the definition is invariant under “phase changes”, i.e. multiplication by $e^{i\eta}$ and $e^{i\eta'}$ for u and v respectively. In fact the angle θ is the *minimum angle between unit vectors in the two dimensional real subspaces* $\text{Span } u, \text{Span } v \subset \mathbb{R}^4$ ¹, and can be regarded as the angle between the real planes $\text{Span } u$ and $\text{Span } v$.

¹Consider the natural correspondence between \mathbb{C}^n and \mathbb{R}^{2n} given by

$$\mathbb{C}^n \ni u = (x_1 + iy_1, \dots, x_n + iy_n) \longleftrightarrow (x_1, y_1, \dots, x_n, y_n) =: \tilde{u} \in \mathbb{R}^{2n}. \quad (\text{B.1})$$

B.1.5 Orthogonal Projections

For any subspace $W \subset V$, W^\perp is the set of all vectors in V that are orthogonal to every vector in W . Then W^\perp is closed under addition and scalar multiplication (*Exercise*) and so is also a subspace of V .

Every vector $v \in V$ can be written uniquely in the form $v = w + w^\perp$ where $w \in W$ and $w^\perp \in W^\perp$. We write $V = W \oplus W^\perp$. Moreover, w is the *unique* minimiser of $\{\|v - w'\| : w' \in W\}$. See Figure B.2 and just about any book on linear algebra.

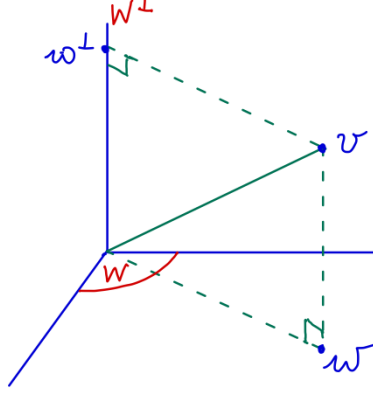


Figure B.2: $\mathbb{C}^2 = W \oplus W^\perp$, $v = w + w^\perp$, $w \in W$, $w^\perp \in W^\perp$.

The (one-dimensional complex) subspace W^\perp is represented by a real one-dimensional line.

The orthogonal projection map P given by $P(v) = w$ is a linear map from V onto W . See Appendix D.3.2 for a useful expression for P in terms of any (orthonormal) basis for W .

B.2 Definitions in Terms of a “Good” Orthonormal Basis

B.2.1 Hermitian Operator

The operator T is *hermitian* (\mathbb{C}^n case), *symmetric* (\mathbb{R}^n case) and *self-adjoint* (either case) iff it corresponds to a (real) scaling in n orthogonal directions (\mathbb{C}^n and \mathbb{R}^n case). Note that in the \mathbb{C}^n

Then it is easy to check that

$$\|u\| = \|\tilde{u}\|_{\mathbb{R}} =: \|u\|_{\mathbb{R}} \quad \text{and} \quad \operatorname{Re}\langle u, v \rangle = \langle \tilde{u}, \tilde{v} \rangle_{\mathbb{R}} =: \langle u, v \rangle_{\mathbb{R}}, \quad (\text{B.2})$$

where $\operatorname{Re}\langle u, v \rangle$ is the real part of $\langle u, v \rangle$, the vectors $\tilde{u}, \tilde{v} \in \mathbb{R}^{2n}$ correspond to $u, v \in \mathbb{C}^n$ respectively, $\|u\|_{\mathbb{R}} := \|\tilde{u}\|_{\mathbb{R}}$ is the \mathbb{R}^{2n} (real) norm, and $\langle u, v \rangle_{\mathbb{R}} := \langle \tilde{u}, \tilde{v} \rangle_{\mathbb{R}}$ is the \mathbb{R}^{2n} (real) inner product.

Proposition. Let u and v be unit vectors in \mathbb{C}^n and let $\cos \theta = |\langle u, v \rangle|$ where $\theta \in [0, \pi/2]$. Then

$$|\langle u, v \rangle| = \max_{\eta, \zeta} \langle e^{i\eta} u, e^{i\zeta} v \rangle_{\mathbb{R}}, \quad \cos \theta = \langle u', v' \rangle_{\mathbb{R}},$$

where the maximum is realised at $u' = e^{i\eta} u$ and $v' = e^{i\zeta} v$. That is, θ is the least angle $\zeta \in [0, \pi/2]$ such that $\cos \zeta = \langle u', v' \rangle_{\mathbb{R}}$ for unit vectors $u' \in \operatorname{Span} u$ and $v' \in \operatorname{Span} v$.

Proof. Just as $|z| = \sup_{\eta} \operatorname{Re}(e^{i\eta} z)$ for $z \in \mathbb{C}$, in the same manner

$$|\langle u, v \rangle| = \sup_{\eta, \eta'} \operatorname{Re}\langle e^{i\eta} u, e^{i\eta'} v \rangle = \max_{\eta, \eta'} \operatorname{Re}\langle e^{i\eta} u, e^{i\eta'} v \rangle = \max_{\eta, \eta'} \langle e^{i\eta} u, e^{i\eta'} v \rangle_{\mathbb{R}}. \quad (\text{B.3})$$

The first max is achieved, since $\operatorname{Re}\langle e^{i\eta} u, e^{i\eta'} v \rangle$ is continuous and (η, η') can be restricted to the compact set $[0, 2\pi] \times [0, 2\pi]$. The last equality is from (B.2).

Assuming the max is achieved at η and η' , let $u' = e^{i\eta} u$ and $v' = e^{i\eta'} v$, and define $\theta \in [0, \pi]$ by $\cos \theta = \langle u', v' \rangle_{\mathbb{R}}$. Note $\langle u', v' \rangle_{\mathbb{R}} \geq 0$ (why?) and so in fact $\theta \in [0, \pi/2]$. \square

case, a “direction” corresponds to a 1-complex-dimensional subspace and hence to a 2-real-dimensional subspace. A scaling corresponds to multiplying by a real number in each of these n complex subspaces.

More precisely, T is *self-adjoint* iff there is an orthonormal basis $\{v_1, \dots, v_n\}$ w.r.t. which T is a real diagonal matrix.

$$T = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix} \quad (\text{B.4})$$

(We allow negative λ_i .) Think of the unit ball at the origin being stretched into an ellipsoid.

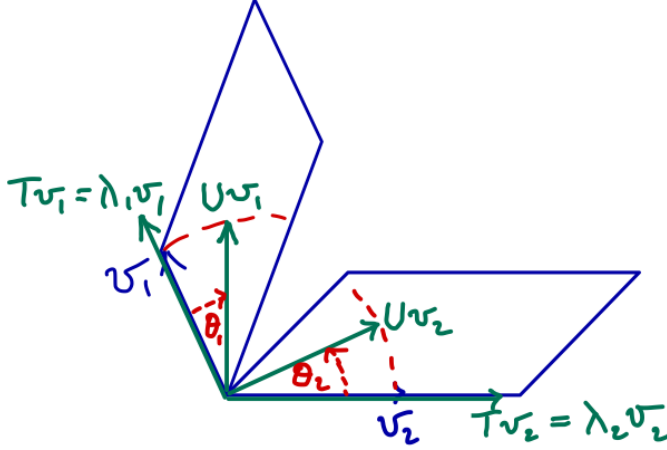


Figure B.3: Hermitian operator T and unitary operator U on \mathbb{C}^2 , $v_1 \in \text{span } |0\rangle$, $v_2 \in \text{span } |1\rangle$.

Figure B.3 shows the action of $T = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$ and $U = \begin{bmatrix} e^{i\theta_1} & 0 \\ 0 & e^{i\theta_2} \end{bmatrix}$ (see Section B.2.2) on vectors $v_1 \in \text{span } |0\rangle$ and $v_2 \in \text{span } |1\rangle$. In particular, Tv_1 is obtained by scaling v_1 with the real factor λ_1 and Uv_1 is obtained by rotating v_1 in the complex line $\text{span } |0\rangle$ (a 2 real-dimensional plane) anticlockwise² through the angle θ_1 .

B.2.2 Unitary Operator

U is *unitary* (\mathbb{C} case) iff it corresponds to a rotation (multiplication by $e^{i\theta_1}, \dots, e^{i\theta_n}$) in n orthogonal directions v_1, \dots, v_n .

More precisely, U is *unitary* iff there is an orthonormal basis w.r.t. which U is a diagonal matrix with all diagonal entries having absolute value 1.

$$U = \begin{bmatrix} e^{i\theta_1} & & \\ & \ddots & \\ & & e^{i\theta_n} \end{bmatrix}$$

The corresponding notion for orthonormal matrices (\mathbb{R} case) is not so clean. We say that O is orthonormal if there is an orthonormal basis such that O fixes some basis vectors, reflects other basis vectors, and rotates in orthogonal planes determined by pairs of the remaining basis vectors.

More precisely, O is *orthonormal* iff there is an orthonormal basis with respect to which O has

²Note that there is an orientation on $\text{span } |0\rangle$ given by complex multiplication.

matrix

$$O = \begin{bmatrix} 1 & & & & & & & & \\ & \ddots & & & & & & & \\ & & 1 & & & & & & \\ & & & -1 & & & & & \\ & & & & \ddots & & & & \\ & & & & & -1 & & & \\ & & & & & & \cos \theta_1 & -\sin \theta_1 \\ & & & & & & \sin \theta_1 & \cos \theta_1 \\ & & & & & & & & \ddots & \\ & & & & & & & & & \cos \theta_k & -\sin \theta_k \\ & & & & & & & & & \sin \theta_k & \cos \theta_k \end{bmatrix}$$

In particular, in \mathbb{R}^3 every orthonormal operator is a rotation around some vector followed perhaps by a reflection in the plane orthogonal to this vector!

Think of the unit ball at the origin being rotated into itself (perhaps there is also a reflection, thus reversing the orientation)

B.2.3 Normal Operator

T (\mathbb{C} case) is *normal* iff it corresponds to multiplication by complex numbers in each of n orthogonal directions. That is, corresponds to a stretch followed by a rotation in each of the corresponding n real 2-dimensional subspaces.

More precisely, T is *normal* iff there is an orthonormal basis with respect to which T is diagonal (with complex, not necessarily real, entries). That is, T has matrix

$$T = \begin{bmatrix} \lambda_1 e^{i\theta_1} & & \\ & \ddots & \\ & & \lambda_n e^{i\theta_n} \end{bmatrix} \quad (\text{B.5})$$

So hermitian and unitary operators are particular cases of normal operators.

B.3 Definitions in Terms of Adjoint Operator

B.3.1 Adjoint

The *adjoint* T^* of the operator T is defined by $\langle T^*u, v \rangle = \langle u, Tv \rangle$ for all $u, v \in \mathbb{C}^n$ (\mathbb{R}^n).

With respect to any orthonormal basis, the matrix of T^* is the conjugate (not relevant of course in the \mathbb{R} case) of the transpose of T , i.e. $T_{ij}^* = \overline{T_{ji}} = T_{ji}^*$, where $\overline{T_{ji}} = T_{ji}^*$ is the complex conjugate of T_{ji} .

Note $(AB)^* = B^*A^*$.

B.3.2 Hermitian Operator

T is *hermitian* iff $T = T^*$.

The \implies case is easy but the converse requires work. It follows from the more general result for normal operators below. But in this special case it is easier to show the existence of an orthonormal basis of eigenvectors.

As noted in Section B.2.1, one often says T is *Hermitian* in the \mathbb{C} case and *symmetric* in the \mathbb{R} case.

B.3.3 Unitary Operator

U is *unitary* (O is *orthonormal*) iff $UU^* = U^*U = I$ ($OO^* = O^*O = I$).

As for hermitian/self-adjoint operators, \implies is easy, the converse requires work, but follows from the more general result for normal operators.

For arbitrary matrices, being unitary is equivalent to the columns being orthonormal (norm one and inner products of different columns equalling zero) and also equivalent to the rows having the same property.

B.3.4 Normal Operator

T is normal iff $TT^* = T^*T$. (\implies is clear from the definition. The converse requires work. The point is to show the existence of an orthonormal basis of eigenvectors. This is sketched in [NC10, p72].

B.4 2×2 Classification

Hermitian The general expression for a 2×2 hermitian matrix is clearly

$$H = \begin{bmatrix} a & c \\ c^* & b \end{bmatrix} \quad \text{where } a, b \in \mathbb{R}. \quad (\text{B.6})$$

Unitary The general expression for a 2×2 unitary matrix is

$$U = \begin{bmatrix} a & b \\ -e^{i\theta}b^* & e^{i\theta}a^* \end{bmatrix} \quad \text{where } |a|^2 + |b|^2 = 1. \quad (\text{B.7})$$

Proof. If U is in the given form then

$$UU^* = \begin{bmatrix} a & b \\ -e^{i\theta}b^* & e^{i\theta}a^* \end{bmatrix} \begin{bmatrix} a^* & -e^{-i\theta}b \\ b^* & e^{-i\theta}a \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I. \quad (\text{B.8})$$

Coversely, suppose $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ is unitary. Then

$$|a|^2 + |b|^2 = 1, \quad |c|^2 + |d|^2 = 1, \quad a^*c + b^*d = 0,$$

since the rows form an orthonormal basis.

If $a \neq 0$ and $d \neq 0$, then from the third equality $c/d = -b^*/a^*$, and so $c = -zb^*$ and $d = za^*$ for some z . Using the second and the first equalities, $1 = |c|^2 + |d|^2 = |z|^2(|a|^2 + |b|^2) = |z|^2$. Now let $z = e^{i\theta}$. This puts U in the required form.

If $a = 0$ then $|b| = 1$ from the first equality, and so $d = 0$ from the third, and so $|c| = 1$ from the second. Hence

$$U = \begin{bmatrix} 0 & e^{i\zeta} \\ e^{i\chi} & 0 \end{bmatrix} = \begin{bmatrix} 0 & e^{i\zeta} \\ -e^{i(\zeta+\chi-\pi)}e^{-i\zeta} & 0 \end{bmatrix},$$

which is in the required form.

If $d = 0$ then $a = 0$ in a similar manner, and so again the result follows. \square

B.5 Polar Decomposition

Every linear operator T (\mathbb{C} case) can be written in the form $T = UH$ where U is unitary and H is Hermitian (i.e. self-adjoint) with nonnegative e-values. That is, real nonnegative stretching in orthogonal complex directions followed by rotations in another set of orthogonal complex directions.

If the rotations are in the *same* complex directions as the stretches, then the matrix is clearly normal.

In the \mathbb{R} case, $T = OS$ where O is orthonormal and S is symmetric with nonnegative e-values. That is, T is again a nonnegative stretch in orthogonal directions and then apply orthogonal transformation.

Think of taking the unit ball sitting at the origin, stretching it to an ellipsoid, and then rotating. Similarly (\mathbb{C} case), $T = H'U$ where U is unitary and H' is self-adjoint with nonnegative e-values. Just take same U as before, and take $H' = UHU^*$. Similarly for the \mathbb{R} case.

B.6 Another Characterisation

Suppose $T : \mathbb{C}^n \rightarrow \mathbb{C}^n$. Then

1. T is *hermitian* iff $\langle Tu, u \rangle$ is real for all u .
2. T is *unitary* (orthonormal) iff $\|Tu\| = \|u\|$ for all u iff $\langle Tu, Tv \rangle = \langle u, v \rangle$ for all u, v .
3. T is *normal* iff $\|Tu\| = \|T^*u\|$ for all u .

For \Leftarrow in 1, suppose $\langle Tu, u \rangle$ is real for all u . Then

$$\langle Tu, u \rangle = \langle Tu, u \rangle^* = \langle u, T^*u \rangle^* = \langle T^*u, u \rangle.$$

So $\langle (T - T^*)u, u \rangle = 0$ for all u . But if $\langle Au, u \rangle = 0$ for all u then for all u, v

$$0 = \langle A(u + v), u + v \rangle = \langle Au, v \rangle + \langle Av, u \rangle.$$

Replacing v by iv and dividing through by i ,

$$0 = \langle Au, v \rangle - \langle Av, u \rangle.$$

Adding, $\langle Au, v \rangle = 0$ for all u, v and so $A = 0$. So $T = T^*$.

(Note: If $A : \mathbb{R}^n \rightarrow \mathbb{R}^n$ then $\langle Au, u \rangle = 0$ for all u does not imply $A = 0$. Consider rotation by $\pi/2$ in \mathbb{R}^2 .)

Appendix C

Determinant and Trace

Contents

C.1 Determinant	77
C.2 Trace	78

The following applies to both real and complex spaces, provided “vol” is defined in the same way in both cases and is allowed to be complex if necessary.

C.1 Determinant

If A is a square $n \times n$ matrix then the *determinant* $\det A$ can be defined¹, for example, by

$$\det A = \sum_{\pi \in \Pi\{1, \dots, n\}} (-1)^\pi A_{1\pi(1)} \cdot \dots \cdot A_{n\pi(n)}, \quad (\text{C.1})$$

where $\Pi\{1, \dots, n\}$ is the set of permutations of $\{1, \dots, n\}$ and $(-1)^\pi$ is $+1$ or -1 according as π is even or odd.

Important properties are

$$\det(I) = 1, \quad \det(AB) = \det(A) \det(B) \quad (\text{C.2})$$

where I is the identity matrix and A, B are square matrices of the same size.

It follows that $\det(S^{-1}AS) = \det A$, and so $\det(A)$ is *independent of choice of basis*.

In particular, if A has eigenvalues $\lambda_1, \dots, \lambda_n$ counted with multiplicities, then

$$\det(A) = \lambda_1 \cdot \dots \cdot \lambda_n. \quad (\text{C.3})$$

Moreover, if $A : V \rightarrow V$ where V is a finite dimensional vector space and A is a *linear operator*, we have shown there is a well defined notion of $\det(A)$ independent of any choice of basis.

Geometrically, and this is what footnote 1 says, $\det(A)$ is the volume change factor given by

$$\text{vol}[Av_1, \dots, Av_n] = \det(A) \times \text{vol}[v_1, \dots, v_n], \quad (\text{C.4})$$

where $[w_1, \dots, w_n]$ is the parallelpiped spanned by w_1, \dots, w_n and “vol” is the oriented volume.

¹The most natural, coordinate-free and geometric way is to use exterior algebra and define $\det A$ for an operator $A : V \rightarrow V$ to be the unique constant such that $Av_1 \wedge \dots \wedge Av_n = \det(A) v_1 \wedge \dots \wedge v_n$ for any basis $\{v_1, \dots, v_n\}$ of V .

C.2 Trace

The *trace* $\text{tr}(A)$ of the square matrix A is the sum of its diagonal elements:

$$\text{tr}(A) = \sum_i A_{ii}. \quad (\text{C.5})$$

It is straightforward to check

$$\text{tr}(I) = n, \quad \text{tr}(AB) = \text{tr}(BA). \quad (\text{C.6})$$

Here A and B need *not* be square; A is $m \times n$ and B is $n \times m$ is the general situation. In general, assuming both A and B are square of the same size so that the following three traces are all defined,

$$\text{tr}(AB) \neq \text{tr}(A) \text{tr}(B). \quad (\text{C.7})$$

However, since $\text{tr}(S^{-1}AS) = \text{tr}(AS^{-1}S) = \text{tr}(A)$, $\text{tr}(A)$ is independent of choice of basis.

Thus if $A : V \rightarrow V$ where V is a finite dimensional vector space and A is a linear operator, then there is a well defined notion of $\text{tr}(A)$ independent of any choice of basis.

In particular, if A has eigenvalues $\lambda_1, \dots, \lambda_n$ counted with multiplicities, then

$$\text{tr}(A) = \lambda_1 + \dots + \lambda_n. \quad (\text{C.8})$$

Moreover, if $A : V \rightarrow V$ where V is a finite dimensional vector space and A is a *linear operator*, we have shown there is a well defined notion of $\text{tr}(A)$ independent of any choice of basis.

For a *geometric interpretation* of $\text{tr}(A)$ suppose A has e-values $\lambda_1, \dots, \lambda_n$ (with multiplicities). Then the e-values of $I + tA$ are $1 + t\lambda_1, \dots, 1 + t\lambda_n$, and so for small t ,

$$\det(I + tA) = (1 + t\lambda_1) \cdot \dots \cdot (1 + t\lambda_n) = 1 + t \text{tr}(A) + O(t^2). \quad (\text{C.9})$$

Hence

$$\left. \frac{d}{dt} \right|_{t=0} \det(I + tA) = \text{tr}(A). \quad (\text{C.10})$$

Noting (C.4), $\text{tr}(A)$ is the rate of change of volume at $t = 0$ of a parallelpiped perturbed by tA .²

²By taking the matrix for A in the basis $\{v_1, \dots, v_n\}$ as in (C.4), we see this rate of change of volume only depends on changes in each edge of the parallelpiped in the direction of that edge.

Appendix D

Dirac Bra-Ket Notation

Contents

D.1 Kets and Bras	79
D.2 More on Inner Products	80
D.3 Outer Products	80
D.3.1 Definition and Matrix Representation	80
D.3.2 Orthogonal Projections	80
D.3.3 Operator as a Sum of Dyads	81
D.4 Computing with Dirac Notation	81

This notation is particularly useful in quantum theory where we are working with vectors, dual vectors and hermitian operators. The terminology “bra-ket” is a play on words from the bracketed expression $\langle v|w\rangle$, in which $\langle v|$ is a bra vector and $|w\rangle$ is a ket vector, see below.

Let V be an inner product space which we usually take to be finite dimensional and usually \mathbb{C}^n for some n .

D.1 Kets and Bras

An element of V is called a *ket vector*, written $|v\rangle$ for some appropriate symbol v , and pronounced “ket v ”. With respect to some orthonormal basis (understood from context, and often the standard

basis in the case of \mathbb{C}^n) we have the column vector notation $|v\rangle = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}$, $|w\rangle = \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}$, etc.

Examples in \mathbb{C}^2 are

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

The dual vector in the dual space V^* which corresponds to $|v\rangle$ is written $\langle v|$ and pronounced “bra v ”. That is, interpreting $\langle v|$ as an operator acting on $|w\rangle \in V$ in the first expression below,

$$\langle v|(|w\rangle) := (|v\rangle, |w\rangle) = v_1^* w_1 + \cdots + v_n^* w_n = [v_1^* \cdots v_n^*] \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix} = \langle v|w\rangle = \langle v|w\rangle \quad (\text{D.2})$$

where in the second expression (\cdot, \cdot) is the inner product, the third expression is just the definition of the inner product, the fourth expression is rewriting the third as matrix multiplication, the fifth is also matrix multiplication where $\langle v|$ is interpreted as the row vector $[v_1^* \cdots v_n^*]$, and the sixth expression is the standard abbreviation of the fifth in the Dirac notation.

In particular, $\langle v|w\rangle$ is the inner product of $|v\rangle$ with $|w\rangle$. Also, $\langle v| = |v\rangle^* = [v_1^* \cdots v_n^*]$ as a row vector or $1 \times n$ matrix.

D.2 More on Inner Products

Let $A : \mathbb{C}^n \rightarrow \mathbb{C}^n$ be a linear operator. We often consider expressions of the form $\langle v|A|w\rangle$. In terms of matrix multiplication this is just (from left to right) the product of the row vector $[v_1^* \cdots v_n^*]$ with

the $n \times n$ matrix A and the column vector $|w\rangle = \begin{bmatrix} w_1 \\ \vdots \\ w_n \end{bmatrix}$.

As an example of working with the Dirac notation, in the (associative) product of the three matrices $\langle v|A|w\rangle$ we can bracket the second and third terms:

$$\langle v|A|w\rangle = \langle v| (A|w\rangle) = |v\rangle^*(A|w\rangle), \quad (\text{D.3})$$

so that $\langle v|A|w\rangle$ is the inner product of the ket vector $|v\rangle$ with the ket vector $A|w\rangle$.

On the other hand, bracketing the first and second terms,

$$\langle v|A|w\rangle = (\langle v|A) |w\rangle = (A^*|v\rangle)^* |w\rangle, \quad (\text{D.4})$$

so $\langle v|A|w\rangle$ is also the inner product of the ket vector $A^*|v\rangle$ with the ket vector $|w\rangle$.

If A is hermitian then $A = A^*$, so $\langle v|A|w\rangle$ is both the inner product of $|v\rangle$ with $A|w\rangle$ and the inner product of $A|v\rangle$ with $|w\rangle$.

D.3 Outer Products

Check that you can show all assertions in the following.

D.3.1 Definition and Matrix Representation

For $|v\rangle, |w\rangle \in V$ define the *outer product*, a linear map $|v\rangle\langle w| : V \rightarrow V$, by

$$|v\rangle\langle w|(|\psi\rangle) = |v\rangle\langle w|\psi\rangle = \langle w|\psi\rangle |v\rangle, \quad \text{for } |\psi\rangle \in V. \quad (\text{D.5})$$

So $|v\rangle\langle w|$ has range $|v\rangle$ and kernel equal to the orthogonal complement of $|w\rangle$.

The operator $|v\rangle\langle w|$ is called a *dyad*.

In terms of matrices,

$$|v\rangle\langle w| = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix} [w_1^* \cdots w_n^*] = \begin{bmatrix} v_1 w_1^* & \cdots & v_1 w_n^* \\ \vdots & \ddots & \vdots \\ v_n w_1^* & \cdots & v_n w_n^* \end{bmatrix}. \quad (\text{D.6})$$

In particular, if e_1, \dots, e_n is an orthonormal basis for V then $|e_i\rangle\langle e_j|$ has matrix whose ij entry is 1 and every other entry is 0.

D.3.2 Orthogonal Projections

See also Appendix B.1.5 for information on orthogonal projections.

If $|v\rangle$ is a unit vector then

$$|v\rangle\langle v| \quad (\text{D.7})$$

is orthogonal projection onto (the space spanned by) $|v\rangle$.

If W is a subspace of V with orthonormal basis $\{|v_1\rangle, \dots, |v_k\rangle\}$ then

$$\sum_{i=1}^k |v_i\rangle\langle v_i| \quad (\text{D.8})$$

is orthogonal projection onto W .¹

Orthogonal projections are hermitian, since there exists an orthonormal base of eigenvectors and the eigenvalues are either 0 or 1.

D.3.3 Operator as a Sum of Dyads

If $\{|v_1\rangle, \dots, |v_n\rangle\}$ is an orthonormal basis for V then the identity map I satisfies

$$I = \sum_{i=1}^n |v_i\rangle\langle v_i|. \quad (\text{D.9})$$

If M has matrix elements M_{ij} w.r.t. the computational basis then

$$M = \sum_{i,j} M_{ij} |i\rangle\langle j|, \quad M_{ij} = \langle i|M|j\rangle. \quad (\text{D.10})$$

If H is hermitian with (necessarily real) eigenvalues λ_j and corresponding orthonormal eigenvectors $|v_j\rangle$ (forming a basis for V) then

$$H = \sum_j \lambda_j |v_j\rangle\langle v_j|. \quad (\text{D.11})$$

Similarly, if U is unitary with eigenvalues $e^{i\theta_j}$ and corresponding orthonormal eigenvectors $|v_j\rangle$ (forming a basis for V) then

$$U = \sum_j e^{i\theta_j} |v_j\rangle\langle v_j|. \quad (\text{D.12})$$

D.4 Computing with Dirac Notation

In computing with the bra-ket notation one is usually dealing with expressions such as $\langle v|A|w\rangle$ or $|v\rangle\langle w|\psi\rangle$ etc., and often much more complicated expressions, which can be treated as a product of matrices.

Consequence and points to note are:

- bracketing is allowed in any order consistent with the associative rule for multiplying matrices,
- expressions such as $\langle w|\psi\rangle$ are an abbreviation for the product $\langle w||\psi\rangle$,
- scalar quantities such as $\langle w|\psi\rangle$ can be moved through the expression,
- adjoints of a product are the product of the adjoints *multiplied in the reverse order*,
- adjoints of matrices are conjugate transposes, so adjoints of scalars are their complex conjugates, of hermitian matrices A are again A , of unitary matrices U are U^{-1} , of bras $\langle v|$ are kets $|v\rangle$, and of kets $|v\rangle$ are bras $\langle v|$.

There will be many examples in these notes.²

¹ $\sum_{i=1}^k |v_i\rangle\langle v_i|$ is independent of choice of orthonormal basis for W . To see this, note we can write $w \in V$ uniquely in the form $w_1 + w_2$ where $w_1 \in W$ and $w_2 \in W^\perp$. Now check $\left(\sum_{i=1}^k |v_i\rangle\langle v_i|\right)w = w_1$ by expressing w_1 and w_2 in terms of an orthonormal basis for V which extends $\{|v_1\rangle, \dots, |v_k\rangle\}$.

²See (2.12), (D.3), (D.4), (F.9), (F.12), ...

Appendix E

Pauli Matrices

Exercise: Verify all statements in the following.

E.1 Definitions, Basic properties, Eigenvalues and Eigenvectors

The Pauli matrices are ubiquitous in the theory of quantum computation. Here they are with their standard notations.

$$\begin{aligned}\sigma_0 = I &= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, & \sigma_1 = X &= \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\ \sigma_2 = Y &= \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, & \sigma_3 = Z &= \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.\end{aligned}\tag{E.1}$$

Usually σ_0 is omitted from the list. It should be clear from context when this is not the case.

They are *hermitian*. Clearly $\sigma_i = \sigma_i^*$.

They are *unitary*. It is easy to check that $\sigma_i \sigma_i^* = I$.

They are *trace free*, i.e. $\text{tr}(\sigma_i) = 0$, and $\det(\sigma_i) = -1$. It follows that they each have eigenvalues ± 1 .

They satisfy the following identities.¹

$$\begin{aligned}\sigma_i^2 &= I, & \sigma_i \sigma_j &= -\sigma_j \sigma_i \text{ if } i \neq j, \\ \sigma_1 \sigma_2 &= i\sigma_3, & \sigma_2 \sigma_3 &= i\sigma_1, & \sigma_3 \sigma_1 &= i\sigma_2.\end{aligned}\tag{E.2}$$

Using the notation of (2.2)

- σ_3 has eigenvectors $|0\rangle$ and $|1\rangle$ with eigenvalues $+1$ and -1 respectively,
- σ_1 has eigenvectors $|+\rangle$ and $|-\rangle$ with eigenvalues $+1$ and -1 respectively,
- σ_2 has eigenvectors $|i\rangle$ and $|-i\rangle$ with eigenvalues $+1$ and -1 respectively.

E.2 As Basis Vectors

Every hermitian matrix H in \mathbb{C}^2 can be uniquely represented as follows with $(n_0, n_1, n_2, n_3) \in \mathbb{R}^4$:²

$$H = \begin{bmatrix} n_0 + n_3 & n_1 - in_2 \\ n_1 + in_2 & n_0 - n_3 \end{bmatrix} = n_0 I + n_1 \sigma_1 + n_2 \sigma_2 + n_3 \sigma_3.\tag{E.3}$$

The set of all such matrices is a real vector space \mathcal{H} with basis vectors $\sigma_0, \sigma_1, \sigma_2, \sigma_3$.³

The trace free hermitian matrices form a subspace $\mathcal{H}_0 \subset \mathcal{H}$. Every $H_0 \in \mathcal{H}_0$ can be written uniquely in the form

$$H_0 = \begin{bmatrix} n_3 & n_1 - in_2 \\ n_1 + in_2 & -n_3 \end{bmatrix} = n_1 \sigma_1 + n_2 \sigma_2 + n_3 \sigma_3\tag{E.4}$$

¹Note the cyclic ordering in the second line. Clearly it follows $\sigma_1 \sigma_3 = -i\sigma_2, \sigma_2 \sigma_1 = -i\sigma_3, \sigma_3 \sigma_2 = -i\sigma_1$.

²The off diagonal entries are arbitrary complex conjugates, the main diagonal entries H_{11} and H_{22} are arbitrary reals — let $n_0 = \frac{1}{2}(H_{11} + H_{22})$, $n_3 = \frac{1}{2}(H_{11} - H_{22})$.

³In fact an inner product space with Hilbert Schmidt inner product $(A, B) := \frac{1}{2} \text{tr } A^* B = \frac{1}{2} \text{tr } AB$.

for some $(n_1, n_2, n_3) \in \mathbb{R}^3$. This gives a vector space isomorphism⁴ between \mathcal{H}_0 and \mathbb{R}^3 , which will be particularly useful in terms of the Bloch sphere map.

E.3 Pauli Vector

E.3.1 Definitions and Examples

Although one can interpret $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ as a vector of Pauli matrices called the *Pauli vector*, we just need the expression $\hat{n} \cdot \vec{\sigma}$ as an abbreviation:

$$\hat{n} \cdot \vec{\sigma} := n_1 \sigma_1 + n_2 \sigma_2 + n_3 \sigma_3 = \begin{bmatrix} n_3 & n_1 - in_2 \\ n_1 + in_2 & -n_3 \end{bmatrix}, \quad \text{where } \hat{n} = (n_1, n_2, n_3) \in \mathbb{R}^3. \quad (\text{E.5})$$

Unless otherwise clear from context, we assume

$$\hat{n} = (n_1, n_2, n_3) \text{ is a unit vector.}$$

Examples are $\hat{n} = (1, 0, 0)$ so $\hat{n} \cdot \vec{\sigma} = \sigma_1$; similarly for σ_2 and σ_3 ; and $\hat{n} = \frac{1}{\sqrt{2}}(1, 0, 1)$ which gives the Hadamard operator $H = \frac{1}{\sqrt{2}}(\sigma_1 + \sigma_3) = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$.

E.3.2 Properties

Proposition.

$$(\hat{n} \cdot \vec{\sigma})^2 = I, \quad \text{tr } \hat{n} \cdot \vec{\sigma} = 0, \quad (\text{E.6})$$

$$\det \hat{n} \cdot \vec{\sigma} = -1, \quad \text{the eigenvalues of } \hat{n} \cdot \vec{\sigma} \text{ are } \pm 1. \quad (\text{E.7})$$

Proof. Using (E.2) it follows $(\hat{n} \cdot \vec{\sigma})^2 = I$. Since $\text{tr } \sigma_i = 0$ for each i , $\text{tr } \hat{n} \cdot \vec{\sigma} = 0$.

Since $\text{tr } \hat{n} \cdot \vec{\sigma} = 0$, the eigenvalues of $\hat{n} \cdot \vec{\sigma}$ are $-\lambda$ and λ for some $\lambda > 0$. (The eigenvalues are real since $\hat{n} \cdot \vec{\sigma}$ is hermitian.) Hence $\det \hat{n} \cdot \vec{\sigma} = -\lambda^2 < 0$.

But $1 = \det I = \det(\hat{n} \cdot \vec{\sigma})^2 = (\det \hat{n} \cdot \vec{\sigma})^2$. Hence $\det \hat{n} \cdot \vec{\sigma} = -1$ (not $+1$) and the eigenvalues are ± 1 . \square

In the following we find the eigenvectors of $\hat{n} \cdot \vec{\sigma}$ (*without doing any matrix calculations!*).

Proposition. *The unit eigenvectors of $\hat{n} \cdot \vec{\sigma}$ are, for $n_3 \neq \pm 1$,*

$$\begin{aligned} & \frac{1}{\sqrt{2(1+n_3)}} \begin{bmatrix} 1+n_3 \\ n_1+in_2 \end{bmatrix} \text{ with eigenvalue } +1, \\ & \frac{1}{\sqrt{2(1-n_3)}} \begin{bmatrix} 1-n_3 \\ -(n_1+in_2) \end{bmatrix} \text{ with eigenvalue } -1. \end{aligned} \quad (\text{E.8})$$

If $n_3 = \pm 1$ then $\hat{n} \cdot \vec{\sigma} = \pm \sigma_3$; the eigenvectors are $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ with eigenvalue $+1$ and $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$ with eigenvalue -1 .

Proof. The case $\hat{n} \cdot \vec{\sigma} = \pm \sigma_3$ is immediate and already noted in Section E.1. So assume $n_3 \neq \pm 1$.

Since $\hat{n} \cdot \vec{\sigma}$ has eigenvalues $\{+1, -1\}$ respectively,

$$\frac{1}{2}(I + \hat{n} \cdot \vec{\sigma}) = \frac{1}{2} \begin{bmatrix} 1+n_3 & n_1-in_2 \\ n_1+in_2 & 1-n_3 \end{bmatrix} \quad (\text{E.9})$$

has eigenvalues $\{1, 0\}$ respectively with the *same* respective eigenvectors (*why?*).

But this matrix is then an orthogonal projection operator, so either column spans the range, and so either column is an eigenvector with eigenvalue 1. We choose the first column just because the “leading” entry is real and positive.

⁴In fact, an inner product space isomorphism.

The squared norm of $\begin{bmatrix} 1 + n_3 \\ n_1 + in_2 \end{bmatrix}$ is $(1 + n_3)^2 + n_1^2 + n_2^2 = 2(1 + n_3)$, and this then gives the first eigenvector in (E.8).

Similarly, by considering $\frac{1}{2}(I - \hat{n} \cdot \vec{\sigma})$ we get the second eigenvector. □

Appendix F

The Bloch Sphere

Contents

F.1 Coordinate Approach	85
F.2 Pairs of antipodal points	86
F.2.1 Orthonormal Bases & Antipodal Points	86
F.2.2 Important Examples	86
F.3 Projection Mapping Approach	87
F.4 Angle Doubling	89

This is a very useful way of representing qubits as points on the unit 2-dimensional sphere $S^2 \subset \mathbb{R}^3$. Recall that a qubit is just an equivalence class of points on the unit (3 real dimensional) sphere $S^3 \subset \mathbb{C}^2$, where two qubits are equivalent if they agree up to a global phase factor $e^{i\zeta}$ for some $\zeta \in \mathbb{R}$.

In fact, this map $S^3 \rightarrow S^2$, where the inverse of any point $\mathbf{x} \in S^2$ is a great circle $S^1 \subset S^3$, is the famous Hopf fibration. See, for example, [MD01, §§1,2].

F.1 Coordinate Approach

Any qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in S^3$, after using polar coordinates for α and β and multiplying through by a (irrelevant) global phase factor, can be written in the form $|\psi\rangle = r_1|0\rangle + r_2e^{i\phi}|1\rangle$ where $0 \leq r_1, 0 \leq r_2, r_1^2 + r_2^2 = 1, 0 \leq \phi < 2\pi$. Hence $|\psi\rangle$ can be written in the form

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\phi} |1\rangle, \quad 0 \leq \theta \leq \pi, \quad 0 \leq \phi < 2\pi. \quad (\text{F.1})$$

This representation is unique unless $\theta = 0$ or $\theta = \pi$.

By using (θ, ϕ) as *spherical coordinates* we obtain a *unique* correspondence between qubits (remember that qubits correspond to equivalence classes of points on the unit sphere in \mathbb{C}^2) and points on the unit sphere in \mathbb{R}^3 . See Figure F.1. (We need $\cos \frac{\theta}{2}$ with $0 \leq \theta \leq \pi$ rather than $\cos \theta$ with $0 \leq \theta \leq \pi/2$ for this.)

If $|\psi\rangle$ is a qubit then the corresponding point on the Bloch sphere is denoted by

$$\Phi(|\psi\rangle). \quad (\text{F.2})$$

In cartesian coordinates,

$$\Phi(|\psi\rangle) = (\sin \theta \cos \phi, \sin \theta \sin \phi, \cos \theta) = (\sin \theta e^{i\phi}, \cos \theta), \quad (\text{F.3})$$

where on the right side we have identified the x - y plane with the complex plane. This is often convenient for calculations.

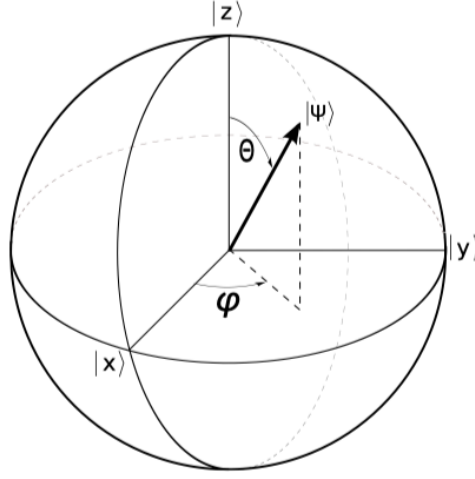


Figure F.1: Bloch Sphere. See (F.6) for notation. ([Vaz12, Notes Chapter 10, Fig. 10.1]).

F.2 Pairs of antipodal points

F.2.1 Orthonormal Bases & Antipodal Points

An arbitrary *orthonormal basis*¹

$$\begin{aligned} |\psi\rangle &= \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\phi} |1\rangle, \\ |\psi'\rangle &= \sin \frac{\theta}{2} |0\rangle - \cos \frac{\theta}{2} e^{i\phi} |1\rangle = \cos \frac{\pi - \theta}{2} |0\rangle + \sin \frac{\pi - \theta}{2} e^{i(\pi + \phi)} |1\rangle, \end{aligned} \quad (\text{F.4})$$

for \mathbb{C}^2 corresponds to a pair of *antipodal* points (θ, ϕ) and $(\pi - \theta, \pi + \phi)$ on the Bloch sphere, and conversely.

F.2.2 Important Examples

On the Bloch sphere the north pole corresponds to $|0\rangle$ (also written $|z\rangle$) since the spherical coordinates are $(0, \phi)$, and the south pole corresponds to $|1\rangle$ (also written $|-z\rangle$) since the spherical coordinates are (π, ϕ) .

In cartesian coordinates, let

$$z = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}, \quad x = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}, \quad y = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \in \mathbb{R}^3. \quad (\text{F.5})$$

¹Why can every orthonormal basis be written this way, up to a global phase factor for each basis vector?

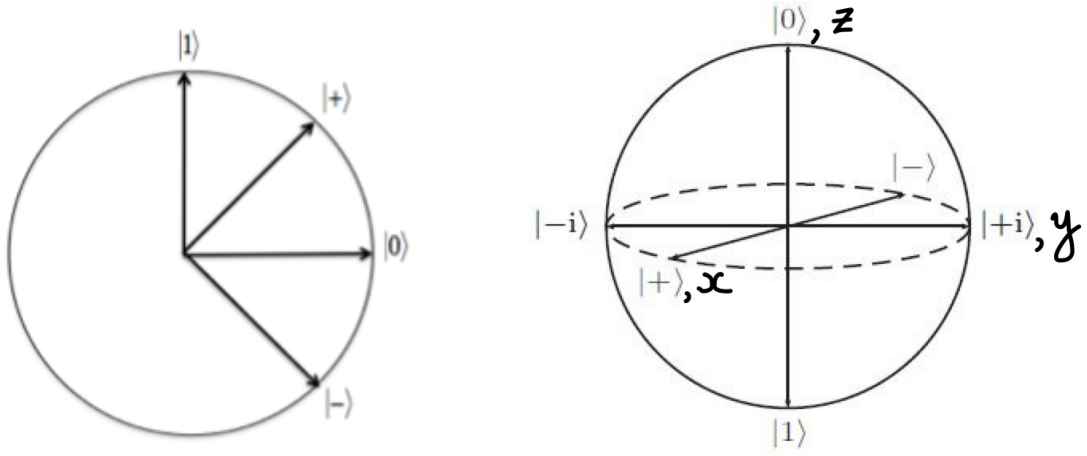


Figure F.2: A 2(real)-dim slice of \mathbb{C}^2 and the Bloch sphere $S^2 \subset \mathbb{R}^3$.

Using the notation of (2.2),

$$\begin{aligned}
|\psi\rangle &= \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\phi} |1\rangle, & (\theta, \phi) \\
|0\rangle = |z\rangle &= \cos 0 |0\rangle + \sin 0 e^{i0} |1\rangle, & (\theta, \phi) = (0, 0) \\
|1\rangle = |-z\rangle &= \cos \left(\frac{\pi}{2}\right) |0\rangle + \sin \left(\frac{\pi}{2}\right) e^{i0} |1\rangle, & (\theta, \phi) = (\pi, 0) \\
|+\rangle = |x\rangle = \frac{1}{\sqrt{2}} |0\rangle + \frac{1}{\sqrt{2}} |1\rangle &= \cos \left(\frac{\pi}{4}\right) |0\rangle + \sin \left(\frac{\pi}{4}\right) e^{i0} |1\rangle = |x\rangle, & (\theta, \phi) = \left(\frac{\pi}{2}, 0\right) \\
|-\rangle = |-x\rangle = \frac{1}{\sqrt{2}} |0\rangle - \frac{1}{\sqrt{2}} |1\rangle &= \cos \left(\frac{\pi}{4}\right) |0\rangle + \sin \left(\frac{\pi}{4}\right) e^{i\pi} |1\rangle = |-x\rangle, & (\theta, \phi) = \left(\frac{\pi}{2}, \pi\right) \\
|i\rangle = |y\rangle = \frac{1}{\sqrt{2}} |0\rangle + i \frac{1}{\sqrt{2}} |1\rangle &= \cos \left(\frac{\pi}{4}\right) |0\rangle + \sin \left(\frac{\pi}{4}\right) e^{i\pi/2} |1\rangle = |y\rangle, & (\theta, \phi) = \left(\frac{\pi}{2}, \frac{\pi}{2}\right) \\
|-i\rangle = |-y\rangle = \frac{1}{\sqrt{2}} |0\rangle - i \frac{1}{\sqrt{2}} |1\rangle &= \cos \left(\frac{\pi}{4}\right) |0\rangle + \sin \left(\frac{\pi}{4}\right) e^{i3\pi/2} |1\rangle = |-y\rangle, & (\theta, \phi) = \left(\frac{\pi}{2}, \frac{3\pi}{2}\right)
\end{aligned} \tag{F.6}$$

F.3 Projection Mapping Approach

For each qubit $|\psi\rangle$ the mapping $|\psi\rangle\langle\psi|$ is orthogonal projection onto the one dimensional subspace of \mathbb{C}^2 spanned by $|\psi\rangle$ (see Section D.3.2). Moreover, this projection map depends only on the *equivalence class* for $|\psi\rangle$.²

For $|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\phi} |1\rangle$, we defined the Bloch sphere representation $\Phi|\psi\rangle \in S^2 \subset \mathbb{R}^3$ to be (θ, ϕ) in spherical coordinates and hence $(\sin \theta \cos \phi, \sin \theta \sin \phi, \cos \theta)$ in cartesian coordinates. See (F.3). However, a frequently more convenient approach is to write the hermitian matrix $|\psi\rangle\langle\psi|$ in terms of the hermitian basis matrices $I, \sigma_1, \sigma_2, \sigma_3$ and to read off the coefficients, as in the following proposition.

Proposition. *Let $|\psi\rangle$ be a qubit. Since the projection map $|\psi\rangle\langle\psi|$ is hermitian it has a unique expansion*

$$|\psi\rangle\langle\psi| = \frac{1}{2}(I + n_1\sigma_1 + n_2\sigma_2 + n_3\sigma_3) = \frac{1}{2} \begin{bmatrix} 1 + n_3 & n_1 - in_2 \\ n_1 + in_2 & 1 - n_3 \end{bmatrix}. \tag{F.7}$$

Then $\Phi|\psi\rangle = \hat{n} = (n_1, n_2, n_3)$ is the Bloch sphere representation of $|\psi\rangle$ in cartesian coordinates.

Proof. That the projection map $|\psi\rangle\langle\psi|$ is hermitian was noted in Section D.3.2, and the unique expansion of any hermitian matrix in terms of the Pauli matrices was noted in Appendix E equation (E.3).

²Let $|\psi'\rangle = e^{i\phi} |\psi\rangle$. Then $\langle\psi'| = e^{-i\phi} \langle\psi|$ and so $|\psi'\rangle\langle\psi'| = |\psi\rangle\langle\psi|$. See Section D.4.

Setting $|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\phi} |1\rangle$, using some basic trigonometric identities³ and (E.3)

$$\begin{aligned}
|\psi\rangle\langle\psi| &= \begin{bmatrix} \cos \frac{\theta}{2} \\ \sin \frac{\theta}{2} e^{i\phi} \end{bmatrix} \begin{bmatrix} \cos \frac{\theta}{2} & \sin \frac{\theta}{2} e^{-i\phi} \end{bmatrix} \\
&= \begin{bmatrix} \cos^2 \frac{\theta}{2} & \cos \frac{\theta}{2} \sin \frac{\theta}{2} e^{-i\phi} \\ \cos \frac{\theta}{2} \sin \frac{\theta}{2} e^{i\phi} & \sin^2 \frac{\theta}{2} \end{bmatrix} \\
&= \frac{1}{2} \begin{bmatrix} 1 + \cos \theta & \sin \theta e^{-i\phi} \\ \sin \theta e^{i\phi} & 1 - \cos \theta \end{bmatrix} \\
&= \frac{1}{2} (I + \sin \theta \cos \phi \sigma_1 + \sin \theta \sin \phi \sigma_2 + \cos \theta \sigma_3).
\end{aligned} \tag{F.8}$$

This gives (F.7) with $(n_1, n_2, n_3) = (\sin \theta \cos \phi, \sin \theta \sin \phi, \cos \theta)$, which from (F.3) is the Bloch sphere representation of $|\psi\rangle$ in cartesian coordinates. \square

Remark The fact the coefficient of I in F.7 is $\frac{1}{2}$ can be seen directly. First note that

$$\text{tr } |\psi\rangle\langle\psi| = \text{tr } \langle\psi|\psi\rangle = \langle\psi|\psi\rangle = 1. \tag{F.9}$$

The first equality is by the cyclic property of trace and the second equality because the trace of a scalar is the scalar itself. Since also

$$\text{tr } I = 2, \text{tr } \sigma_1 = \text{tr } \sigma_2 = \text{tr } \sigma_3 = 0,$$

the result follows.

Remark The fact $|\hat{n}| = 1$ can also be seen directly from (F.7). As in the proof of (F.13),

$$1 = (\langle\psi|\psi\rangle)^2 = \text{tr}(\langle\psi|\psi\rangle)^2 = \text{tr}(|\psi\rangle\langle\psi| |\psi\rangle\langle\psi|) = \frac{1}{2} (1 + |\hat{n}|^2).$$

Hence $|\hat{n}| = 1$.

Example Find $\Phi|\psi\rangle$ if $|\psi\rangle = \frac{1}{2} |0\rangle + \frac{\sqrt{3}}{2} i |1\rangle$.

Compute

$$\begin{aligned}
|\psi\rangle\langle\psi| &= \begin{bmatrix} \frac{1}{2} \\ \frac{\sqrt{3}i}{2} \end{bmatrix} \begin{bmatrix} \frac{1}{2} & -\frac{\sqrt{3}i}{2} \end{bmatrix} = \begin{bmatrix} \frac{1}{4} & -\frac{\sqrt{3}i}{4} \\ \frac{\sqrt{3}i}{4} & \frac{3}{4} \end{bmatrix} \\
&= \frac{1}{2} I + \begin{bmatrix} -\frac{1}{4} & -\frac{\sqrt{3}i}{4} \\ \frac{\sqrt{3}i}{4} & \frac{1}{4} \end{bmatrix} = \frac{1}{2} \left(I + \frac{\sqrt{3}}{2} \sigma_2 - \frac{1}{2} \sigma_3 \right)
\end{aligned}$$

Hence $\Phi|\psi\rangle = \left(0, \frac{\sqrt{3}}{2}, -\frac{1}{2}\right)$ in cartesian coordinates.

From the Bloch Sphere back to the Qubit Given a unit vector $(n_1, n_2, n_3) \in S^2 \subset \mathbb{R}^3$ we can readily find the coordinates of the ket $|\psi\rangle$ which is represented by (n_1, n_2, n_3) as follows.

From (F.7) and (E.1) we have

$$|\psi\rangle\langle\psi| = \frac{1}{2} \begin{bmatrix} 1 + n_3 & n_1 - in_2 \\ n_1 + in_2 & 1 - n_3 \end{bmatrix}. \tag{F.10}$$

We can read off the coordinates of $|\psi\rangle\langle\psi|$ directly as follows.

Since $|\psi\rangle\langle\psi|$ is a projection operator it has rank 1. Hence the two columns in its matrix must be linearly dependent and the image of $|\psi\rangle\langle\psi|$, which is $|\psi\rangle$, is spanned by either column:

$$\text{Span } |\psi\rangle = \text{Span} \begin{bmatrix} 1 + n_3 \\ n_1 + in_2 \end{bmatrix} = \text{Span} \begin{bmatrix} n_1 - in_2 \\ 1 - n_3 \end{bmatrix}.$$

³There is not much to remember, just $\sin 2\theta = 2 \sin \theta \cos \theta$, $\cos 2\theta = 2 \cos^2 \theta - 1$.

Using the first column vector since it gives a real positive coefficient for $|0\rangle$, and since its norm squared is $(1 + n_3)^2 + |n_1 + in_2|^2 = 2(1 + n_3)$, up to an arbitrary phase factor and assuming $n_3 \neq -1$,

$$|\psi\rangle = \frac{\sqrt{1 + n_3}}{\sqrt{2}} |0\rangle + \frac{n_1 + in_2}{\sqrt{2(1 + n_3)}} |1\rangle. \quad (\text{F.11})$$

If $n_3 = -1$ then $|\psi\rangle = |1\rangle$ up to a phase factor.

F.4 Angle Doubling

Let

$$|\psi\rangle = \cos \frac{\theta}{2} |0\rangle + \sin \frac{\theta}{2} e^{i\phi} |1\rangle, \quad 0 \leq \theta \leq \pi, \quad 0 \leq \phi < 2\pi,$$

as in (F.1). Since $|\langle 0|\psi\rangle| = \langle 0|\psi\rangle = \cos \frac{\theta}{2}$, the angle between $|0\rangle$ and $|\psi\rangle$ is $\frac{\theta}{2}$. See Appendix B.1.4.

On the other hand, from (F.3), $\Phi|\psi\rangle = (\sin \theta \cos \phi, \sin \theta \sin \phi, \cos \theta) =: \hat{k}$ and $\Phi|0\rangle = (0, 0, 1) := z$, so $\langle z, \hat{k} \rangle = \cos \theta$ and the angle between $\Phi|0\rangle$ and $\Phi|\psi\rangle$ is θ .

Thus there is angle doubling in passing from $S^3 \subset \mathbb{C}^2$ to $S^2 \subset \mathbb{R}^3$. We will see in the following proposition that this is always true. To prove this from the coordinate representation of qubits is very messy and not recommended.

The following proof uses a couple of important properties of trace, see Appendix C.2.

Proposition. Suppose $\Phi|\psi\rangle = \hat{n}$ and $\Phi|\phi\rangle = \hat{k}$. Let $|\langle \psi|\phi\rangle| = \cos \zeta$ with $\zeta \in [0, \pi/2]$, and let $\langle \hat{n}, \hat{k} \rangle = \cos \theta$ with $\theta \in [0, \pi]$. Then $\zeta = \theta/2$, i.e. $\theta = 2\zeta$.

Proof. First note that

$$\cos^2 \zeta = |\langle \psi|\phi\rangle|^2 = \langle \psi|\phi\rangle \langle \phi|\psi\rangle = \text{tr}(\langle \psi|\phi\rangle \langle \phi|\psi\rangle) = \text{tr}(|\psi\rangle\langle\psi| |\phi\rangle\langle\phi|). \quad (\text{F.12})$$

The third equality is just because the trace of a scalar is the scalar. The fourth is by (C.6), noting $\langle \psi|\phi\rangle = \langle \psi||\phi\rangle$ and $\langle \phi|\psi\rangle = \langle \phi||\psi\rangle$.

From (F.7), with $\hat{n} = (n_1, n_2, n_3)$ and $\hat{k} = (k_1, k_2, k_3)$,

$$\begin{aligned} \text{tr}(|\psi\rangle\langle\psi| |\phi\rangle\langle\phi|) &= \frac{1}{4} \text{tr} \begin{bmatrix} 1 + n_3 & n_1 - in_2 \\ n_1 + in_2 & 1 - n_3 \end{bmatrix} \begin{bmatrix} 1 + k_3 & k_1 - ik_2 \\ k_1 + ik_2 & 1 - k_3 \end{bmatrix} \\ &= \frac{1}{4} \text{tr} \begin{bmatrix} (1 + n_3)(1 + k_3) + (n_1 - in_2)(k_1 + ik_2) & \star \\ \star & (n_1 + in_2)(k_1 - ik_2) + (1 - n_3)(1 - k_3) \end{bmatrix} \\ &= (1 + n_3 + k_3 + n_3k_3) + (n_1k_1 + in_1k_2 - in_2k_1 + n_2k_2) \\ &\quad + (n_1k_1 - in_1k_2 + in_2k_1 + n_2k_2) + (1 - n_3 - k_3 + n_3k_3) \\ &= \frac{1}{2} (1 + \langle \hat{n}, \hat{k} \rangle) = \frac{1}{2} (1 + \cos \theta) = \cos^2 \frac{\theta}{2}. \end{aligned} \quad (\text{F.13})$$

The proposition now follows from (F.12) and (F.13). \square

Alternative Proof This is essentially just a notational change which avoids referring to matrices. In the proof of (F.13)

$$\begin{aligned} \text{tr}(|\psi\rangle\langle\psi| |\phi\rangle\langle\phi|) &= \frac{1}{4} \text{tr} \left((I + \hat{n} \cdot \vec{\sigma}) (I + \hat{k} \cdot \vec{\sigma}) \right) \quad \text{from (F.7) and (E.5)} \\ &= \frac{1}{4} \text{tr} \left(I + \hat{n} \cdot \vec{\sigma} + \hat{k} \cdot \vec{\sigma} + \langle \hat{n}, \hat{k} \rangle I \right) \quad \text{from (E.2)} \\ &= \frac{1}{2} + \frac{1}{2} \langle \hat{n}, \hat{k} \rangle = \frac{1}{2} (1 + \cos \theta) = \cos^2 \frac{\theta}{2}. \end{aligned}$$

Appendix G

Functions of Normal Operators

Contents

G.1 Examples of Interest	90
G.2 Power Series Definition	90
G.3 Definition for Normal Operators	90
G.4 Matrices for the Schrödinger Equation	91

G.1 Examples of Interest

Let V be a finite dimensional complex inner product space. For us it will be a state space. You can think of $V = \mathbb{C}^n$.

Let $T : V \rightarrow V$ be a normal operator. Recall from Appendix B.2.3 that this means T has an orthonormal basis of eigenvectors. We are interested in the case T is hermitian or unitary, but the more general case is just as straightforward.

Let $f : \mathbb{C} \rightarrow \mathbb{C}$ be some function. Then can we make sense of $f(T)$ in some useful way?

We will be particularly concerned with

$$\cos(H), \quad \sin(H), \quad \exp(i\theta H), \quad (\text{G.1})$$

where $\exp(u) = e^u$ is the exponential function and H is hermitian.

G.2 Power Series Definition

If f is the squaring function, i.e. $f(z) = z^2$, then we define $f(T) = T^2$. Similarly if $f(z) = z^k$ for some positive integer k we define $f(T) = T^k$. We can also define T^{-1} to be the inverse of T , provided T is invertible.

If $f(z) = a_0 + a_1 z + a_2 z^2 + \dots$ converges for $|z| < R$ (i.e. f is analytic) then we can define $f(T) = a_0 + a_1 T + a_2 T^2 + \dots$. This will converge if all entries in the standard matrix representation are $\leq R'$ for some R' depending on R . In particular, for the functions $\cos(z)$, $\sin z$ and e^{az} for any constant a , the series converges for all T . However, this is not the approach we take here. It is mentioned just for comparison with the literature.

G.3 Definition for Normal Operators

For normal matrices we have the following more natural and convenient approach. In particular, there are no differentiability requirements on f , and the definition of $f(T)$ depends only on the values of f for the eigenvalues of T .¹

¹This approach works for diagonalisable matrices in general. But it is not as stable under convergence of matrices as in the case of normal matrices where we are restricting to orthonormal bases. See [HJ91, §6.2.37 Theorem, p 433].

With respect to any orthonormal basis of eigenvectors we have

$$T = \begin{bmatrix} \alpha_1 & & \\ & \ddots & \\ & & \alpha_n \end{bmatrix} \implies f(T) := \begin{bmatrix} f(\alpha_1) & & \\ & \ddots & \\ & & f(\alpha_n) \end{bmatrix}. \quad (\text{G.2})$$

Note this is not a coordinate dependent definition! We are using an orthonormal basis of eigenvectors for T . Any allowable change of basis vectors for T (e.g. reordering or phase changes) will have the same effect on $f(T)$, i.e. no change on the actual operator.

G.4 Matrices for the Schrödinger Equation

If H is hermitian as in (B.4) with matrix below for some orthonormal basis of eigenvectors $\{E_1, \dots, E_n\}$ corresponding to eigenvalues $\lambda_1, \dots, \lambda_n$, then $U(t) := e^{-itH}$ has the matrix shown for the same orthonormal basis of eigenvectors (now also for e^{-itH}).

$$H = \begin{bmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{bmatrix}, \quad U(t) := e^{-itH} = \begin{bmatrix} e^{-it\lambda_1} & & \\ & \ddots & \\ & & e^{-it\lambda_n} \end{bmatrix}. \quad (\text{G.3})$$

It follows immediately that $U(t)$ is unitary.

It is also clear from its matrix representation that for any unitary operator U there is a unique hermitian operator H such that $U = \exp(-iH)$.

If t is interpreted as time then U acts on the H eigenspace E_i for λ_i by rotation with velocity λ_i , and in the clockwise direction if $\lambda_i > 0$.

In Figure G.1 let $H = \begin{bmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{bmatrix}$ and $U = \begin{bmatrix} e^{-it\lambda_1} & 0 \\ 0 & e^{-it\lambda_2} \end{bmatrix} = \exp(-itH)$.

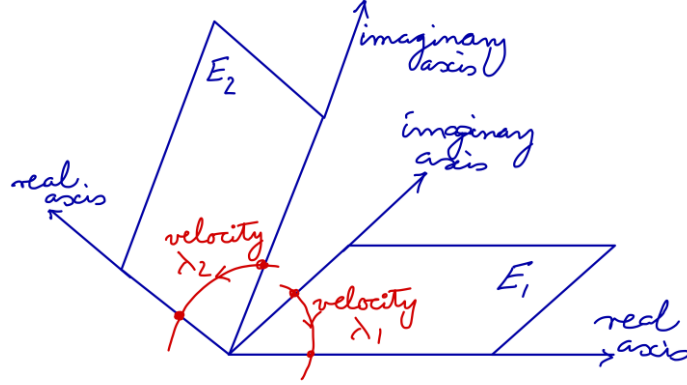


Figure G.1: Schematic representation for the 2 orthogonal eigenspaces $E_1, E_2 \subset \mathbb{C}^2$ and for the unitary operator $U = \exp(-itH)$ as it rotates vectors in these eigenspaces. The direction of rotation is shown in case $\lambda_1, \lambda_2 > 0$.

See also the Schrödinger Equation 2.24

Appendix H

Tensor Products

Contents

H.1 Informal Presentation	92
H.1.1 Bilinear Requirements	92
H.1.2 Basis and Dimension	93
H.1.3 Entangled and Product Elements	93
H.1.4 Other Bilinear Products	93
H.1.5 Inner Product	93
H.1.6 Examples	93
H.2 Basis Dependent Definition of Tensor Products	94
H.3 Tensor Product of Operators	95

H.1 Informal Presentation

H.1.1 Bilinear Requirements

Consider two finite dimensional complex¹ inner product spaces V and W , with orthonormal bases e_1, \dots, e_m and $\epsilon_1, \dots, \epsilon_n$ respectively. If $v \in V$ and $w \in W$ let

$$v = v_1 e_1 + \dots + v_m e_m, \quad w = w_1 \epsilon_1 + \dots + w_n \epsilon_n. \quad (\text{H.1})$$

We want to form a new “tensor product”² vector space $V \otimes W$ which consists of all linear combinations of elements of the form $v \otimes w$ where $v \in V$ and $w \in W$. We call $v \otimes w$ the “tensor product of v and w ” or just “ v tensor w ”. We similarly say the “tensor product of V and W ” or just “ V tensor W ” for the vector space $V \otimes W$.

We want $V \otimes W$ to “preserve” the linear vector space structure of V and of W . For example, we require

$$\begin{aligned} (2v + 3v') \otimes (w - 3w') &= 2(v \otimes (w - 3w')) + 3(v' \otimes (w - 3w')) \\ &= 2(v \otimes w) - 6(v \otimes w') + 3(v' \otimes w) - 9(v' \otimes w') \\ &= 2v \otimes w - 6v \otimes w' + 3v' \otimes w - 9v' \otimes w', \quad \text{etc.} \end{aligned}$$

In particular we unambiguously write $2v \otimes w$ since we will require $(2v) \otimes w = 2(v \otimes w)$.

More precisely, we allow repeated applications of the following rules:

$$\begin{aligned} (\alpha v + \alpha' v') \otimes w &= \alpha v \otimes w + \alpha' v' \otimes w \\ v \otimes (\beta w + \beta' w') &= \beta v \otimes w + \beta' v \otimes w' \end{aligned} \quad (\text{H.2})$$

These rules say that the map from $V \times W$ into $V \otimes W$ given by $(v, w) \mapsto v \otimes w$ is linear in v and is linear in w . In other words, the map from $V \times W$ into $V \otimes W$ is *bilinear*.

¹Essentially everything we do also applies in the real case.

²Tensor products can be defined for any two vector spaces, not necessarily complex, or finite dimensional or with an inner product.

H.1.2 Basis and Dimension

When we calculate $v \otimes w$ in this way, with v and w as in (H.1), we obtain

$$\begin{aligned} v \otimes w &= (v_1 e_1 + \cdots + v_m e_m) \otimes (w_1 \epsilon_1 + \cdots + w_n \epsilon_n) \\ &= v_1 w_1 e_1 \otimes \epsilon_1 + v_1 w_2 e_1 \otimes \epsilon_2 + \cdots + v_1 w_n e_1 \otimes \epsilon_n \\ &\quad + v_2 w_1 e_2 \otimes \epsilon_1 + \cdots + v_2 w_n e_2 \otimes \epsilon_n + \cdots + v_m w_n e_m \otimes \epsilon_n. \end{aligned} \quad (\text{H.3})$$

Thus we can write $v \otimes w$ as a linear combination of the elements $e_j \otimes \epsilon_k$. Moreover, using the rules (H.2), $v \otimes w + v' \otimes w'$ and $\alpha(v \otimes w)$ will also be a linear combination of the $e_j \otimes \epsilon_k$.

This implies $V \otimes W$ should be a vector space spanned by $\{e_j \otimes \epsilon_k : 1 \leq j \leq m, 1 \leq k \leq n\}$. Moreover, we will require that the $e_j \otimes \epsilon_k$ be linearly independent, so that they actually form a *basis* for $V \otimes W$, and $V \otimes W$ is mn -dimensional. In particular,

$$\sum_{j,k} \alpha_{jk} e_j \otimes \epsilon_k = \sum_{j,k} \beta_{jk} e_j \otimes \epsilon_k \quad \text{implies} \quad \alpha_{jk} = \beta_{jk} \text{ for all } j \text{ and } k. \quad (\text{H.4})$$

H.1.3 Entangled and Product Elements

The map from $V \times W$ into $V \otimes W$ is *not* onto. Because $V \otimes W$ is a vector space we can add its members, for example $e_1 \otimes \epsilon_1 + e_2 \otimes \epsilon_2 \in V \otimes W$.

But do there exist v and w such that $e_1 \otimes \epsilon_1 + e_2 \otimes \epsilon_2 = v \otimes w$? The answer is *NO*. To see this let v and w be as in (H.1). Then from (H.3) and (H.4),

$$v_1 w_1 = 1, v_1 w_2 = 0, v_2 w_1 = 0, v_2 w_2 = 1.$$

Since $v_1 w_2 = 0$, either $v_1 = 0$ or $w_2 = 0$. If $v_1 = 0$ this contradicts $v_1 w_1 = 1$ and if $w_2 = 0$ this contradicts $v_2 w_2 = 1$.

We say that $e_1 \otimes \epsilon_1 + e_2 \otimes \epsilon_2$ is *entangled*. On the other hand,

$$e_1 \otimes \epsilon_1 + e_1 \otimes \epsilon_2 + e_2 \otimes \epsilon_1 + e_2 \otimes \epsilon_2 = (e_1 + e_2) \otimes (\epsilon_1 + \epsilon_2),$$

We say $e_1 \otimes \epsilon_1 + e_1 \otimes \epsilon_2 + e_2 \otimes \epsilon_1 + e_2 \otimes \epsilon_2$ is a *product*.

In the quantum setting, we refer to *entangled* and *product* states.

H.1.4 Other Bilinear Products

The requirements in (H.2) are the *only* restrictions on forming the tensor product of vectors from V and W . Another way of expressing this is through the linear independence of the $e_j \otimes \epsilon_k$ as in (H.4).

To clarify this, consider (in the real case) the cross product map from $\mathbb{R}^3 \times \mathbb{R}^3$ into \mathbb{R}^3 . This *is* bilinear. But $e_1 \times e_1 = 0$ and $e_1 \times e_2 + e_2 \times e_1 = 0$, whereas $e_1 \otimes e_1 \neq 0$ and $e_1 \otimes e_2 + e_2 \otimes e_1 \neq 0$. So the cross product is not a tensor product. Moreover, the tensor product space $\mathbb{R}^3 \otimes \mathbb{R}^3$ is in fact 9-dimensional, and as we see later is unique up to an appropriate isomorphism.

H.1.5 Inner Product

H.1.6 Examples

The basis for $\mathbb{C}^2 \otimes \mathbb{C}^2$ constructed from the canonical basis $\{|0\rangle, |1\rangle\}$ for \mathbb{C}^2 consists of the four elements

$$|0\rangle \otimes |0\rangle, |0\rangle \otimes |1\rangle, |1\rangle \otimes |0\rangle, |1\rangle \otimes |1\rangle.$$

In standard abbreviated form these are written as

$$|0\rangle|0\rangle, |0\rangle|1\rangle, |1\rangle|0\rangle, |1\rangle|1\rangle; \quad \text{or} \quad |00\rangle, |01\rangle, |10\rangle, |11\rangle.$$

The basis for $\mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$ consists of the 8 elements

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

H.2 Basis Dependent Definition of Tensor Products

Definition. With V and W as above, the *tensor product* $V \otimes W$ is the mn dimensional inner product space consisting of all formal linear combinations of the form $\sum_{j,k} \alpha_{jk} e_j \otimes \epsilon_k$, with vector addition, scalar multiplications and inner product defined componentwise. In particular,

$$\left(\sum_{j,k} \alpha_{jk} e_j \otimes \epsilon_k, \sum_{j,k} \beta_{jk} e_j \otimes \epsilon_k \right) := \sum_{j,k} \overline{\alpha_{jk}} \beta_{jk}$$

and so the $e_j \otimes \epsilon_k$ form an orthonormal basis of $V \otimes W$.

Define

$$\widehat{\otimes} : V \times W \rightarrow V \otimes W, \quad \widehat{\otimes}(v, w) = v \otimes w = \sum_{j,k} v_j w_k e_j \otimes \epsilon_k.$$

Note that $\widehat{\otimes}(\cdot, \cdot)$ is bilinear, i.e. linear in each slot. But $\widehat{\otimes}$ is typically *not* onto.

Remarks Although the definition of $V \otimes W$ involves the choice of bases e_1, \dots, e_m and $\epsilon_1, \dots, \epsilon_n$, we will soon see that the tensor product is a basis independent notion. It is also possible to give a basis free definition, but it is less “concrete” than the “pedestrian” approach above.

Note that here we are just identifying $V \otimes W$ with the inner product space \mathbb{C}^{mn} , modulo a choice of orthonormal basis vectors e_1, \dots, e_m and $\epsilon_1, \dots, \epsilon_n$ and a choice of identifying the $e_j \otimes \epsilon_k$ with the standard basis vectors in \mathbb{C}^{mn} .

Proposition. If $B : V \times W \rightarrow E$ is a bilinear map into a vector space E then there is a unique linear map $L : V \otimes W \rightarrow E$ such that $B(v, w) = L(v \otimes w)$. Conversely, B can be recovered from L .

$$\begin{array}{ccc} V \times W & \xrightarrow{\widehat{\otimes}} & V \otimes W \\ B \downarrow & \swarrow L & \\ E & & \end{array}$$

Proof. Define $L(e_j \otimes \epsilon_k) = B(e_j, \epsilon_k)$ and extend to $L : V \otimes W \rightarrow E$ by linearity. It follows

$$B(v, w) = \sum_{j,k} v_j w_k B(e_j, \epsilon_k) = \sum_{j,k} v_j w_k L(e_j \otimes \epsilon_k) = L\left(\sum_{j,k} v_j w_k e_j \otimes \epsilon_k\right) = L(v \otimes w).$$

The existence and uniqueness of L are now immediate, and clearly B can be recovered from L . \square

Remark The point is that any bilinear map $B : V \times W \rightarrow E$ corresponds to a unique linear map $L : V \otimes W \rightarrow E$. We say $(\widehat{\otimes}, V \otimes W)$ satisfies the *universality property* for V and W .

We can also think of $\widehat{\otimes} : V \times W \rightarrow V \otimes W$ as the “freest” bilinear map on $V \times W$ in that the only conditions imposed are the ones of bilinearity. In particular, the bilinear maps given by scalar product and vector product on $\mathbb{R}^3 \times \mathbb{R}^3$ are not free in this sense. For example, $e_1 \cdot e_2 = 0$ but $e_1 \otimes e_2 \neq 0$, $e_1 \times e_1 = 0$ but $e_1 \otimes e_1 \neq 0$.

This leads to the following definition and proposition, which show that

Definition. Let $C : V \times W \rightarrow Z$ be a bilinear map into the vector space Z . Then (C, Z) satisfies the *universality property* for V and W if for any vector space E and bilinear map $B : V \times W \rightarrow E$ there exists a unique linear map $L_B : Z \rightarrow E$ such that the following diagram commutes:

$$\begin{array}{ccc} V \times W & \xrightarrow{C} & Z \\ B \downarrow & \swarrow L_B & \\ E & & \end{array}$$

H.3 Tensor Product of Operators

Bibliography

- [ADR82] Alain Aspect, Jean Dalibard, and Gérard Roger, *Experimental test of Bell's inequalities using time-varying analyzers*, Phys Rev Lett **49** (1982), 1804–1807, available at <https://journals.aps.org/prl/pdf/10.1103/PhysRevLett.49.1804>.
- [Bel64] John Bell, *On the Einstein Podolsky Rosen paradox*, Physics **1** (1964), 195–200, available at <https://journals.aps.org/ppf/pdf/10.1103/PhysicsPhysiqueFizika.1.195>. (Bell derives an experimentally testable inequality to distinguish between quantum predictions and Local Realism.)
- [BS14] James Binney and David Skinner, *The Physics of Quantum Mechanics*, Oxford University Press, 2014.
- [CCEZ03] G. Chen, D. A. Church, B. G. Englert, and M. S. Zubairy, *Mathematical Models of Contemporary Elementary Quantum Computing Devices*, CRM Proceedings and Lecture Notes, vol. 33, Centre de Recherches Mathématiques, 2003, available at <https://arxiv.org/pdf/quant-ph/0303163.pdf>. (A mathematical treatment of the physical implementations. See also [ZCDH09]).
- [CHSH69] J. F. Clauser, A. Horne, A. Shimony, and R. A. Holt, *Proposed experiment to test local hidden-variable theories*, Phys. Rev. Lett. **23** (1969), 880–884, available at <http://totallyrandom.info/wp-content/uploads/2018/05/Clauser.pdf>.
- [dW19] Ronald de Wolf, *The Potential Impact of Quantum Computers on Society* (2019), <https://arxiv.org/abs/1712.05380>. (An Insightful Essay).
- [Dir58] P.A.M. Dirac, *Principles of Quantum Mechanics*, fourth (revised) edition, Oxford University Press, 1958.
- [EPR35] A Einstein, B Podolsky, and N Rosen, *Can quantum mechanical description of physical reality be considered complete?*, Phys. Rev. **47** (1935), 227, available at <https://journals.aps.org/pr/pdf/10.1103/PhysRev.47.777>.
- [Fey] Richard Feynman, *The Character of Physical Law*, twelfth printing 1985, MIT Press. (1964 lectures given to Cornell students. Appear to be widely available online, see http://people.virginia.edu/~ecd3m/1110/Fall2014/The_Character_of_Physical_Law.pdf).
- [FLS65] Richard P. Feynman, Robert B. Leighton, and Matthew Sands, *The Feynman Lectures on Physics, Volume III, Quantum Mechanics*, Caltech online edition <http://www.feynmanlectures.caltech.edu>, 1965.
- [GHW09] Daniel Greenberger, Klaus Hentschel, and Friedel Weinert, *Compendium of Quantum Physics*, Springer, 2009.
- [HJ91] Roger Horn and Charles R. Johnson, *Topics in Matrix Analysis*, Cambridge University Press, 1991.
- [JS17] Des Johnston and Bernd Schroers, *Quantum Mechanics and Quantum Computing: an Introduction*, 2017, <http://www.macs.hw.ac.uk/~des/qcnotesaims17.pdf>. (A small update with a few corrections to Schroers' original notes, also in this bibliography.)
- [Lvo18] A.I. Lvovsky, *Quantum Physics: An Introduction Based on Photons*, Springer, 2018. (Well written. Emphasises the photon polarisation interpretation of qubits. Lots of problems with solutions available through the publishers web site.)
- [MD01] Rémy Mosseri and Rosen Dandoloff, *Geometry of entangled states, Bloch spheres and Hopf fibrations*, Journal of Physics A: Mathematical and General **34** (2001), no. 47, 10243, available at <https://arxiv.org/pdf/quant-ph/0108137.pdf>.
- [MN19] Andy Matuschak and Michael A. Nielsen, *Quantum computing for the very curious* (2019), <https://quantum.country/qcvc>. (A new and experimental online course by an excellent expositor. Covers much less and slower pace than these notes. Uses “spaced repetition learning” as in Anki cards. Google it!).
- [NAo19] National Academies of Sciences, Engineering, and Medicine, *Quantum Computing: Progress and Prospects* (Emily Grumbling and Mark Horowitz, eds.), National Academies Press, 2019. See <https://doi.org/10.17226/25196>.
- [NC10] Michael A. Nielsen and Isaac L. Chuang, *Quantum computation and quantum information*, Cambridge University Press, Cambridge, 2010. (Ten year Anniversary Edition of what is widely considered to be the gold standard in the field. Comprehensive. Very well written. No longer sold, but has been available free from the publisher's website and often available online for courses.)
- [Pla0] Plato, *Plato's Cave Allegory* (370 B.C.), <http://www.john-uebersax.com/plato/plato2.htm>. (Socrates on Quantum States).

- [Pre18] John Preskill, *Quantum Computing in the NISQ era and beyond*, Quantum **2** (2018), 79, available at <https://quantum-journal.org/papers/q-2018-08-06-79/pdf/>.
- [RP11] Eleanor Rieffel and Wolfgang Polak, *Quantum Computing, A Gentle Introduction*, MIT Press, Cambridge, Massachusetts, 2011. (A little slow at times, but some very interesting discussions.)
- [Sch07a] Bernd Schroers, *Quantum Computing*, 2007/8, <http://www.macs.hw.ac.uk/~bernd/F14ZD1/qcnotes.pdf>. (Goes a fair distance, globally well structured, a quick introduction to the field, follows Nielsen and Chuang. Locally not so good, some mistakes and overly complicated arguments. Some errors corrected in the slightly updated version used by Johnston).
- [Sch07b] ———, *Quantum Computing: Problem Sheets*, 2007/8, <http://www.macs.hw.ac.uk/~bernd/F14ZD1/>. (Problems vary in difficulty. Many routine ones to check background algebra. Others to check the underlying concepts.)
- [SW10] Benjamin Schumacher and Michael D. Westmoreland, *Quantum Processes, Systems, and Information*, Cambridge University Press, 2010. (A well written modern introduction to quantum processes at the advanced undergraduate level.)
- [Vaz13] Umesh Vazirani, *Quantum Mechanics and Quantum Computation* (2013), https://courses.edx.org/courses/BerkeleyX/CS-191x/2013_August/course/. (A very well presented edX MOOC.)
- [Vaz12] ———, *Chem/CS/Phys191:Qubits, Quantum Mechanics, and Computers* (2012), <http://www-inst.eecs.berkeley.edu/~cs191/sp12/>. (The Berkeley course on which the edX MOOC course was based. See the link there to the lecture notes.)
- [vN18] John von Neumann, *Mathematical Foundations of Quantum Mechanics*, new edition (Nicholas A. Wheeler, ed.), Princeton University Press, 2018.
- [YCL⁺17] Juan Yin, Yuan Cao, Yu-Huai Li, et al., *Satellite-based entanglement distribution over 1200 kilometers*, Science **356** (2017), 1140–1144, available at <http://science.sciencemag.org/content/356/6343/1140.full>. Arxiv version <https://arxiv.org/pdf/1707.01339.pdf>.
- [ZCDH09] Zhigang Zhang, Goong Chen, Zijian Diao, and Philip R. Hemmer, *NMR Quantum Computing*, Advances in Mechanics and Mathematics, vol. 17, Springer-Verlag, 2009, pp. 465–520, available at https://www.researchgate.net/profile/Zijian_Diao/publication/226605374_NMR_Quantum_Computing/links/0fcfd50887c80465a8000000/NMR-Quantum-Computing.pdf. (A treatment for mathematicians of the physical implementation of the Nuclear Magnetic Resonance approach to building quantum computers. See also [CEEZ03].)