INTRO TO QUANTUM INFORMATION (ECE 493-05 & 579-04)
Rutgers, Fall 2019 **Course Syllabus**

INTRODUCTION TO QUANTUM INFORMATION SCIENCE

Quantum phenomena provide computing and information handling paradigms that are distinctly different and arguably much more powerful than their classical counterparts. In the past quarter of the century, much progress has been made on the theoretical side, and experiments have been carried out in which quantum computational operations were executed on a very small number of quantum bits. The NSF has declared this general area to be one of the 10 big ideas for future investments. In June 2018, the science committee of the House of Representatives unanimously approved the National Quantum Initiative Act (H.R. 6227), which would create a 10-year federal effort aimed at boosting quantum science.

This course will provide an introduction to the theory of quantum computing and information. The topics that will be covered include 1) the fundamental elements of quantum information processing (qubits, unitary transformations, density matrices, measurements); 2) entanglement, protocols for teleportation, the Bell inequality, 3) basic quantum algorithms such as Shor's factoring and Grover's search, and 4) basic quantum data compression and error correction. The course material will be accessible to undergraduate and graduate students with a variety of backgrounds, e.g., electrical engineers, physicists, mathematicians, and computer scientists.

Learning Objective:
The students will learn the fundamentals of quantum information science, as well as a selected number of more advanced topics of their individual interests.

Instructor: Emina Soljanin (contact info on the web page)

Office hours: by appointment

Class time and place: M&W, 3:20 PM – 4:40 PM, SEC 207

Prerequisites: Calculus, linear algebra, and probability at an undergraduate level as well as familiarity with complex numbers are required. Prior exposure to quantum mechanics and information/coding theory is helpful but not essential.

Grading: homework 20%, 3 midterm exams 15% each, project 35%.

Text: N. D. Mermin, *Quantum Computer Science: An Introduction,* Cambridge Univ. Press (2007).

Recommended reading:
L. Susskind and A. Friedman, *Quantum Mechanics: The Theoretical Minimum.*
J. Preskill, *Lecture Notes for Physics 229: Quantum Information and Computation.*
F. W. Byron and R. W. Fuller, *Mathematics of Classical and Quantum Physics*

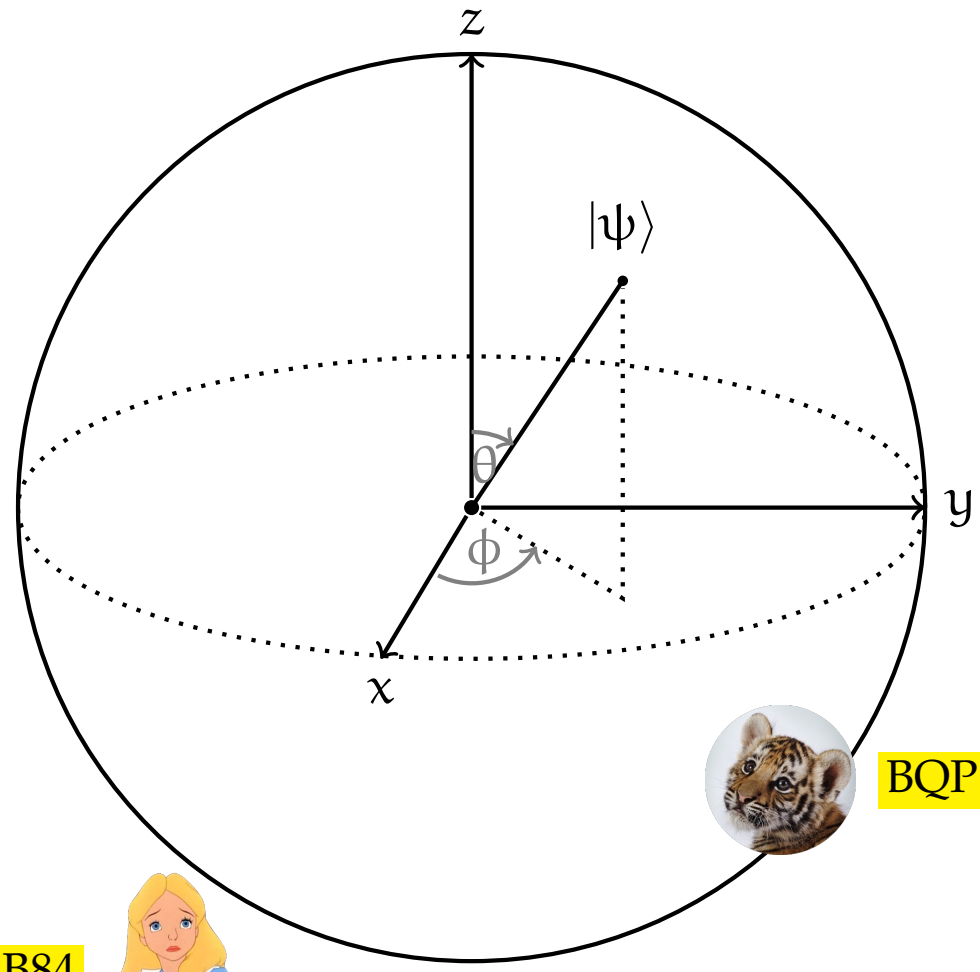
Course notes: given per week in separate documents on the class (Sakai) web page.

Remarks: The topics outlined above are very common for a quantum information science course at the advanced-undergraduate/graduate level. Such courses have been taught at several universities for many years, e.g., for almost two decades at Cornell based on the class textbook. Students are encouraged to choose their project topics according to their own (research) interests.

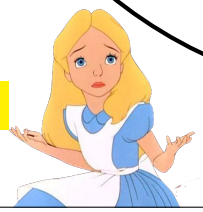
NEW COURSE ANNOUNCEMENT

CS, ECE, Math, and Physics graduate & advanced undergrad students

INTRODUCTION TO QUANTUM INFORMATION SCIENCE



BQP



BB84

For more QUBITs of information, contact

Prof. Emina Soljanin

emina.soljanin@rutgers.edu

Introduction to Quantum Information Science [1]

[1] Rutgers, ECE 579, Fall 2019

Prof. Emina Soljanin

Lecture #1, September 4

This lecture[2] informally introduces several important notions in (quantum) computing: information, measurements, algorithms. It also addresses some common misconceptions about the importance of prior knowledge in algorithm design, and shows that even classical computing can be non-intuitive.

[2] You are likely to find this class more conceptually than technically hard. In that sense, this is the hardest lecture.

Information and Measurement

Bit is a unit of information that we get when we ask a yes/no question – yes or no, true or false, on or off, 0 or 1. The assumption here is that the question concerns something we have no prior knowledge about. Suppose you want to find out the position of the black king (that can be equally likely anywhere) on a chessboard. Take a look at Fig. 1. What is the minimum number of yes/no questions you need to ask?

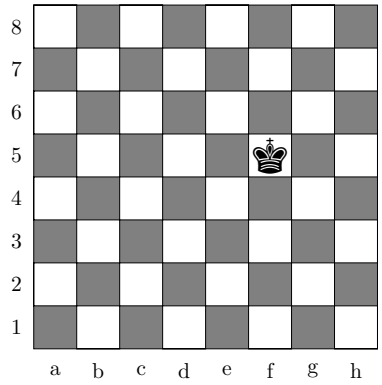


Figure 1: What is the minimum number of yes/no questions that have to be asked to locate the king on a chessboard?

To represent a bit in a computer, we need a physical entity which can exist in two distinguishable physical states. For example, magnetized cells in hard disk drives could be oriented in two different directions: "up" for 0 or "down" for 1. Flesh memory cells made from floating-gate transistors act as switches that could be open for 0 or closed for 1. (There are multi-level cell devices that can store more than one bit per cell.)

A physical system with $N = 2^k$ distinguishable physical states can represent k bits of information. Such a system can simply be a collection of k systems with two distinguishable states, i.e., a k-bit register. To specify an object in a set of N, we need $\lceil \log_2 N \rceil$ binary digits; Table 1 show how we can do that for $N = 8$.

Decimal	Binary	mod 2	Parity
0	000	0	0
1	001	1	1
2	010	0	1
3	011	1	0
4	100	0	1
5	101	1	0
6	110	0	0
7	111	1	1

Table 1: We can specify each object in a set of 8 by assigning to it a unique label, e.g., a decimal number or a binary string.

Note that distinguishable is the crucial word here. Distinguishable how? By the naked eye? By a given measuring apparatus? Is there some fundamental limit to the number of states that can be dis-

tinguished by a physical measurement regardless of whether we can build it or not? If your measuring apparatus can only tell you the last digits of the numbers in Table 1, you will get only a single bit of information telling you whether the number is even or odd (see the third column of Table 1). You will get a single but different bit of information if your measuring apparatus can only tell you the *parity*, namely, the XOR of the digits in the binary string representing the number (see the fourth column of Table 1).

Algorithms

A Penny Weighing Problem: You are given a balance scale and 8 pennies, one of which has a different weight. What is the minimum number of measurements that will always let you determine which penny has a different weight? How will you perform the measurements?

The minimum number of measurements that will always let us determine which penny has a different weight is three. Why? A possible way to perform the three measurements[3] is given in Table 2. The three rows starting with M1, M2, and M3 correspond to the three measurements. The table entry at the intersection between a column corresponding to a penny and a raw corresponding to a measurement indicates whether the penny is put on the scale in that measurement (o if it is not) and if yes, whether it is placed on the left platform L or on the right platform R.

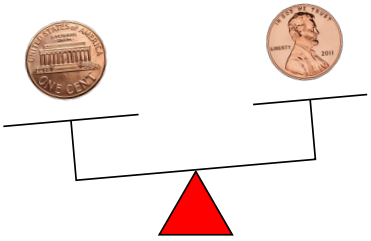


Figure 2: How would you use a balance scale to determine which of the 8 pennies has a different weight?

[3] an algorithm

		PENNY							
		0	1	2	3	4	5	6	7
ON SCALE	M1	o	o	o	o	L	L	R	R
	M2	o	o	L	L	o	o	R	R
	M3	o	L	o	L	o	R	o	R

Table 2: Pennies placement on the scale in three measurements. A penny can be placed left (L), right (R) or not at all (o).

Suppose that the penny 4 has different weight, then measurement M1 will result in an unbalanced state of the scale and M2 and M3 in the balanced state of the scale, as illustrated in Fig. 3.

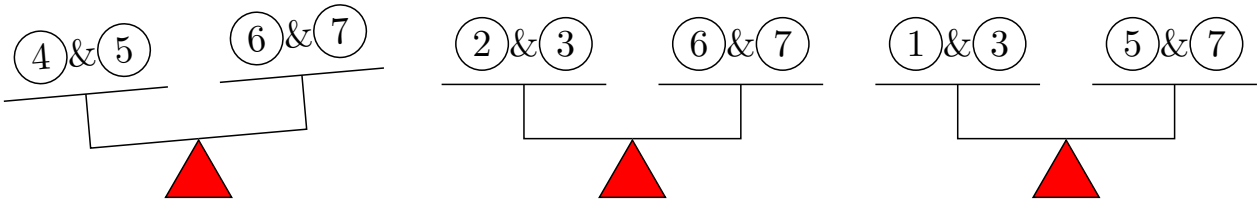


Figure 3: An example of measurement outcomes. Which penny has different weight?

Observe that since there is only one penny of different weight, a measurement will result in an unbalanced state of the scale iff the penny of different weight is placed on the scale in that measurement. Therefore, the possible measurement outcomes are as given in Table 3. In each measurement, the scale can be either balanced (0) or unbalanced (1). Not that for each of the 8 "different penny" possibilities, we have a different set of measurement outcomes. Therefore a set of measurement outcomes uniquely identifies a different penny.

		DIFFERENT PENNY							
		⓪	①	②	③	④	⑤	⑥	⑦
SCALE STATE	M1	0	0	0	0	1	1	1	1
	M2	0	0	1	1	0	0	1	1
	M3	0	1	0	1	0	1	0	1

Table 3: Scale states corresponding to measurements for each of the 8 "different panny" possibilities. The scale can be either balanced (0) or unbalanced (1).

Suppose you have a balance scale as in Fig. 2. Find a set of 3 measurements that you can use to identify the different penny if you know that it is heavier (or lighter) than the other seven.

Some Observations

1. We have committed to the way we perform the three measurements before the measuring process started. That is, we do not *adapt*[4] our measuring actions based on the results of the previous measurement, e.g., how we perform M2 does not change based on the outcome of M1.
2. Having some additional information could be helpful in designing a set of measurements, even if it cannot reduce the number of measurements. It can also be helpful in practice.
3. How we conduct measurements evidently depends on the kind of scale we have. And so does the number of measurements. What would you do if you had a scale which has the unit weight corresponding to a regular penny fixed to the right tray, as in Fig. 4, and you can only use the left tray to place pennies?

[4] Non-adaptive measuring can be as powerful as adaptive.

Problems

1. Consider the "king on the chessboard" problem. Why was it important to know that the king can be equally likely anywhere?

2. Suppose you have a balance scale as in Fig. 2. Find a set of 3 measurements that you can use to identify the different penny only if you know that it is heavier (or lighter) than the other seven.
   Hint: Consider adaptive measurements.

3. Suppose you have a fixed weight scale as in Fig. 4. How many measurements would you need *on average* to find the single penny that does not have the unit weight? [5]

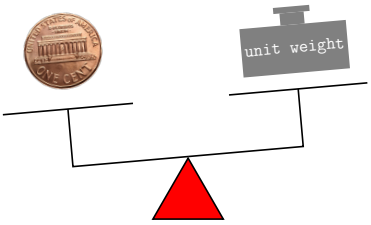


Figure 4: In this scale, there is some unit weight fixed to the right tray.

[5] We will see such "measuring scales" when we study the Grover's quantum search algorithm.

Introduction to Quantum Information Science [1]

[1] Rutgers, ECE 579, Fall 2019

Prof. Emina Soljanin

Lecture #2, September 9

This lecture 1) introduces the notion of single qubit, as the quantum computing counterpart to the (classical) bit, and 2) provides mathematical background necessary to define states of multiple qubits and explain how they can be transformed.

Bits as Mathematical Objects

In this class, we will treat bits as mathematical objects.[2] For us, bits take values in the set $\{0, 1\}$ where we can add and multiply as follows:

[2] Other classes at ECE and Physics study bits as physical systems.

XOR

$\oplus$	0	1
0	0	1
1	1	0

AND

$\cdot$	0	1
0	0	0
1	0	1

Figure 1: Binary arithmetic.

Associative and distributive laws for binary addition and multiplication are identical to those for real numbers. Strings of n bits are mathematical objects that live in the field $\mathbb{F}_{2^n}$, which is a set of 2^n elements with specially defined addition and multiplication we will formally define below.

Recall our penny weighing problem, and consider the following matrix/vector multiplication, where the arithmetic is done as defined in Fig. 1.

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

Check to see that this *classical computing* is performing the *measurements*[3] we did with a balance scale in the penny weighing problem. The result of computing is the binary representation of the number indicating the position (in this case 3) of the different bit. Multiplying (measuring) the vector with all bits equal to 1 except the one at position 3, would give the same result.

[3] We call some operations in quantum computing "measurements". Our classical balance scale did not do anything to the pennies, but quantum measurements interact with the system being measured, and are in general *irreversible* operations.

After the measuring, in order to make all bits identical, we would have to flip the bit at position 3. This flipping can be performed by e.g., 1) a NOT operation on the bit in position 3 or 2) an XOR operation

(binary addition in Fig. 1) on the bit in position 3 together with the bit of the fixed value 1. Note that both these operations are *reversible*.

Qubit as a Mathematical Object

A *qubit* is a quantum information/computing counterpart to a bit. We will treat qubits as mathematical objects as well.[4] What we learn in this class is independent of a particular physical realization.

A qubit is represented by a unit-norm vector in a two dimensional complex vector space[5]. If we denote the basis vectors of this space by

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

then a single qubit $|\psi\rangle$ is mathematically a linear combination of $|0\rangle$ and $|1\rangle$ basis vectors:

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

where α and β are complex numbers such that $|\alpha|^2 + |\beta|^2 = 1$.

In classical computing, we refer to a *bit value* or a binary value. In quantum computing, we refer to a *qubit state* or a quantum state[6]. We say that the quantum state $|\psi\rangle$ above is a superposition of the two basis states. The superposition is instrumental in enabling quantum computing speedup.

[4] Qubits (as bits) are represented by physical systems.

[5] Unfamiliar terms? Read the next section first.

[6] In the simplest case, qubit states are *pure* and we mathematically describe them as we described $|\psi\rangle$ here. There are also *mixed* states and a general way to mathematically represent both.

Math Interlude

Quantum theory is a mathematical model of the physical world. We will go over necessary mathematics as the need arises. To understand the terms and the notation we used in describing the qubit, we next review some basic algebraic notions.

Fundamental Structures in Abstract Algebra

Group $(G, \circ)$ A group is a set G together with an operation $\circ$: $G \times G \to G$ satisfying:

1. $\circ$ is associative: $(a \circ b) \circ c = a \circ (b \circ c)$
2. There is an element e in G s.t. $a \circ e = a$ and $e \circ a = a$ for every element a in G. e is called neutral element.
3. For every element a in G, there is an element a^{-1} in G s.t. $a \circ a^{-1} = a^{-1} \circ a = e$. a^{-1} is called the inverse of a.

If $\circ$ is commutative, we say that G is commutative or Abelian.

Depending on the context, we will call a group 1) *additive*, its operation $+$ addition, and its neutral element 0, or 2) *multiplicative*, its

Two examples:

1. $(\{0, 1\}, \oplus)$ is an additive group.
2. $(\{0, 1\}, \cdot)$ is not a group.

operation $*$ or $\cdot$ multiplication, and its neutral element 1 (unity).

Ring $(A, +, *)$ The most basic of the two-operation structures is called a ring: Ring is a set A with operations called addition $+$ and multiplication $*$ satisfying:

1. $(A, +)$ is an Abelian group.
2. Multiplication is associative.
3. Multiplication is distributive over addition. That is, for all a, b, and c in A, we have $a(b+c) = ab + ac$

Examples of rings:

1. set of integers $\mathbb{Z}$
2. set of $n \times n$ matrices over $\mathbb{Z}$

Natural numbers $\mathbb{N}$ is not a ring.

When the multiplication operation is commutative, we say that A is a commutative (Abelian) ring.

Field $(\mathbb{F}, +, *)$ If $(\mathbb{F}, +, *)$ is a commutative ring with unity in which every nonzero element has a multiplicative inverse, it is called a field:

1. $(\mathbb{F}, +)$ is an Abelian group.
2. $(\mathbb{F} \setminus \{0\}, *)$ is an Abelian group.

Examples of fields:

1. set of rational numbers $(\mathbb{Q}, +, \cdot)$
2. set of complex numbers $(\mathbb{C}, +, \cdot)$
3. finite field $\left(\{0, 1\}, \oplus, \cdot\right)$

A linear space over a field $\mathbb{F}$ is an additive Abelian group v together with an operation of *multiplication by scalars* $\mathbb{F} \times V \to V$. The elements of v are called vectors and the elements of $\mathbb{F}$ are called scalars. The product of $\alpha \in \mathbb{F}$ and $v \in V$ is denoted by $\alpha v \in V$. In addition, there are requirements connecting $\mathbb{F}$ and v:

For all $\alpha, \beta \in \mathbb{F}$ and $v, w \in V$, we have

1. $(\alpha\beta)v = \alpha(\beta v)$
2. $\alpha(v + w) = \alpha v + \alpha w$
3. $(\alpha + \beta)v = \alpha v + \beta v$
4. $1v = v$, where 1 is the unity in $\mathbb{F}$

Examples of linear spaces over the field of complex numbers $\mathbb{C}$:

1. $\mathbb{C}^n$ of n-tuples over $\mathbb{C}$
2. $\mathbb{C}^{k \times n}$ of $k \times n$ matrices over $\mathbb{C}$
3. All polynomials over $\mathbb{C}$

A linear combination of vectors $v_1, \ldots, v_m$ is a vector of the form

$$\alpha_1 v_1 + \cdots + \alpha_m v_m.$$

The span of vectors $v_1, \ldots, v_m$ is the set of all linear combinations of $v_1, \ldots, v_m$:

$$\operatorname{span}(v_1, \ldots, v_m) = \{\alpha_1 v_1 + \cdots + \alpha_n v_m \mid \alpha_1, \ldots, \alpha_m \in \mathbb{F}_q\}.$$

Vectors $v_1, \ldots, v_m$ are linearly independent when

$$\alpha_1 v_1 + \cdots + \alpha_m v_m = 0 \text{ only if } \alpha_1 = \cdots = \alpha_m = 0.$$

A basis of a vector space V is a set of linearly independent vectors in V that spans V.

The dimension of a vector space v is the number[7] of vectors of a basis of v over $\mathbb{F}$.

[7] Does each basis have the same number of vectors?

Let V and W be linear spaces over the same field. Then $f : V \to W$ is a linear map if for every $v, u \in V$ and $\alpha \in \mathbb{F}$, we have

1. $f(v+u) = f(v) + f(u) \quad \leftarrow$ additive
2. $f(\alpha v) = \alpha f(v) \quad \leftarrow$ homogeneous

Hilbert Space

An inner-product space is a vector space equipped with an inner product. An inner product in a complex vector space is a scalar-valued function of the ordered pair of vectors ψ and φ, such that

1. $\langle\psi|\varphi\rangle = \langle\varphi|\psi\rangle^*$
2. $\langle\alpha\psi + \beta\xi|\varphi\rangle = \alpha\langle\psi|\varphi\rangle + \beta\langle\xi|\varphi\rangle$, where $\alpha, \beta \in \mathbb{C}$.
3. $\langle\psi|\psi\rangle \geqslant 0$ for any v and $\langle\psi|\psi\rangle = 0$ iff v is the 0 vector.

The quantity $\langle\psi|\psi\rangle^{1/2} = \|\psi\|$ is often referred to as the *norm* or the *length* of the vector v.

A complex inner-product space is called a unitary space. Quantum computing deals with vectors and matrices in finite dimensional unitary spaces. The mathematical setting of quantum mechanics is the infinite dimensional generalization[8] of unitary spaces, known as the Hilbert space. Thus we say that a qubit is an element of a two dimensional Hilbert space.

[8] one needs to add completeness

Dirac's Notation

It is important to adopt a notation which let us easily distinguish between scalars and vectors. In mathematics, we usually use lower case letters for scalars and often capitals or bold face for vectors. The notation for vectors used in quantum computing literature (and preferred by physicists in general) is known as the Dirac's or bra-ket notation.

In the bra-ket notation, a column vector is denoted by $|\varphi\rangle$ and its *complex conjugate transpose* by $\langle\varphi|$. The bra-ket notation is inspired by the standard mathematical notation for the inner product

$$\langle\psi|\varphi\rangle = \langle\psi| \cdot |\varphi\rangle ,$$

where $\cdot$ denotes ordinary matrix multiplication. Here a row vector times a column vector gives a number. Bras and kets can be multiplied as matrices also as[9]

[9] the outer product

$$|\psi\rangle\langle\varphi|$$

Here a column vector times a row vector gives a matrix.

We have used 0 and 1 as labels for the basis in $\mathbb{C}^2$ above:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

There are other lables in use, e.g., $|+\rangle$ and $|-\rangle$ or $|\downarrow\rangle$ and $|\uparrow\rangle$, and even *dead* and *alive* cats.

Introduction to Quantum Information Science [1]

[1] Rutgers, ECE 579, Fall 2019

Prof. Emina Soljanin

Lecture #3, September 11

This lecture is concerned with multiple Qubits and reversible actions on single and multiple Qubits.

Reversible Acting on a Single Qubit

Recall that single Qubit is a vector in the 2D Hilbert space $\mathcal{H}_2$:

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

where $|0\rangle$ and $|1\rangle$ are the basis vectors of $\mathcal{H}_2$:

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

A quantum state can be transformed to another state only by a physical process consistent with the laws of quantum mechanics. In quantum mechanics, it is possible to act on quantum states by reversible and irreversible operations. The reversible operators will be called *gates* and irreversible will be called *measurements*.

In a closed quantum system, a single-Qubit state $|\psi\rangle \in \mathcal{H}_2$ can be transformed to some other state in $\mathcal{H}_2$, say $|\varphi\rangle$, in a reversible way only by some *unitary* operator U, i.e.,

$$|\varphi\rangle = U|\psi\rangle$$

where U is a 2×2 unitary[2] matrix. Any unitary matrix specifies a valid quantum gate.

[2] If U is real, we call it is *orthogonal*.

If we know how U acts on the basis vectors $|0\rangle$ and $|1\rangle$, then we also know how it acts on any vector $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$. To see that, recall that matrix multiplication is a linear operation:

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

Math Interlude

A unitary matrix U is a complex *square* matrix whose inverse is equal to its conjugate[3] transpose $U^\dagger$, i.e.,

[3] The conjugate of a complex number $c = x + \imath y$ is $\bar{c} = x - \imath y$.

$$U^\dagger U = U U^\dagger = I.$$

$U^\dagger$ is called the *adjoint of* U. Real unitary matrices are called *orthogonal*. If only $U^\dagger U = I$, we say that U is an isometry.

Some Single-Qubit Gates

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

Mapping the basis states

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

- Hadamard gate:

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

$$|0\rangle \text{ —H— } (|0\rangle + |1\rangle)/\sqrt{2}$$

$$|1\rangle \text{ —H— } (|0\rangle - |1\rangle)/\sqrt{2}$$

- Pauli matrices:

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

$$|0\rangle \text{ —X— } |1\rangle$$

$$|1\rangle \text{ —X— } |0\rangle$$

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

$$|0\rangle \text{ —Y— } i|1\rangle$$

$$|1\rangle \text{ —Y— } -i|0\rangle$$

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

$$|0\rangle \text{ —Z— } |0\rangle$$

$$|1\rangle \text{ —Z— } -|1\rangle$$

Math Interlude

Let A be an $m \times n$ matrix[4] and B a $p \times q$ matrix. The Kronecker product $A \otimes B$ is the $mp \times nq$ matrix given by

$$A \otimes B = \begin{bmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ a_{21}B & a_{22}B & \cdots & a_{2n}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}B & a_{m2}B & \cdots & a_{mn}B \end{bmatrix}.$$

[4] $A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$.

Some properties of the Kronecker product:

- Let A and C be $n \times n$ matrices and B and D $m \times m$ matrices. Then

$$(A \otimes B) \cdot (C \otimes D) = AC \otimes BD.$$

- (Conjugate) transposition are distributive over the Kronecker product (cf. regular matrix product):

$$(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$$

- $A \otimes B$ has the inverse iff both A and B are invertible, and then (cf. regular matrix product):

$$(A \otimes B)^{-1} = A^{-1} \otimes B^{-1}$$

Multiple Qubits

As in classical computing, we mostly operate jointly on multiple Qubits rather than deal with a single Qubit on an individual basis.[5] If we have two Qbits, one in the state $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$ and the other $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$, then the state of the pair is the Kronecker product of the individual states:

[5] How are n Qubits mathematically represented?

$$\begin{aligned}|\psi_1\rangle \otimes |\psi_2\rangle &= \big(\alpha_1|0\rangle + \beta_1|1\rangle\big) \otimes \big(\alpha_2|0\rangle + \beta_2|1\rangle\big) \\ &= \alpha_1\alpha_2\,|0\rangle \otimes |0\rangle + \alpha_1\beta_2\,|0\rangle \otimes |1\rangle + \beta_1\alpha_2\,|1\rangle \otimes |0\rangle + \beta_1\beta_2\,|1\rangle \otimes |1\rangle\end{aligned}$$

where

$$\underset{\begin{bmatrix}1\\0\\0\\0\end{bmatrix}}{|0\rangle \otimes |0\rangle} \quad \underset{\begin{bmatrix}0\\1\\0\\0\end{bmatrix}}{|0\rangle \otimes |1\rangle} \quad \underset{\begin{bmatrix}0\\0\\1\\0\end{bmatrix}}{|1\rangle \otimes |0\rangle} \quad \underset{\begin{bmatrix}0\\0\\0\\1\end{bmatrix}}{|1\rangle \otimes |1\rangle}$$

In general[6], a 2-Qubit state is any superposition of these 4 basis states, and thus cannot always be expressed as a product of single Qubit states. 2-Qubit states that can be written as a Kronecker product of two single-Qubit states are called *separable* and those than cannot are called *entangled*[7] states.

[6] separable and entangled stats

[7] Entangled states are responsible for much of "quantum magic".

The individual Qubits that make up an entangled state cannot always be characterized as having individual states of their own. To see this, consider the following two-Qubit state

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

This state is known as the Bell state or the EPR pair. [8]

[8] EPR stands for Einstein, Podolsky and Rosen, who were the first to point out the "strange" properties of this state.

A system of n Qubits is a vector in $\mathcal{H}_{2^n}$:

$$\sum_{i=0}^{2^n-1} \alpha_i |i_0\rangle \otimes |i_1\rangle \otimes \cdots \otimes |i_{n-1}\rangle,$$

where

- $\mathcal{H}_{2^n} = \underbrace{\mathcal{H}_2 \otimes \mathcal{H}_2 \otimes \cdots \otimes \mathcal{H}_2}_{n}$.
- $\alpha_i \in \mathbb{C}$, $\sum_{i=0}^{2^n-1} |\alpha_i|^2 = 1$
- $i_0 i_1 \ldots i_{n-1}$ is the binary representation of i

Several shorthand notations are used for the i-th basis vector of $\mathcal{H}_{2^n}$:

$$\begin{aligned}|i_0\rangle \otimes |i_1\rangle \otimes \cdots \otimes |i_{n-1}\rangle &\sim |i_0\rangle|i_1\rangle \ldots |i_{n-1}\rangle \\ &\sim |i_0, i_1, \ldots, i_{n-1}\rangle \\ &\sim |i_0 i_1 \ldots i_{n-1}\rangle\end{aligned}$$

If an n-Qubit state can be expressed as a Kronceker product of n single-Qubit states, we say that it is *separable*. Otherwise, we say that it is entangled.

There is a notion of *Qudit*, as a basic quantum state corresponding to a d-level physical systems. A single Qudit state is a vector in the d-dimensional Hilbert space $\mathcal{H}_d$, and an n-Qudit state is a vector in $\mathcal{H}_{d^n}$. Generalization from Qubit to Qudit systems is mathematically straightforward. Infinite dimensional systems will be left for later studies.

In general, if quantum (multi-Qubit) system A is in the state $|\Psi\rangle_A$ in the Hilbert space $\mathcal{H}_A$ and if quantum (multi-Qubit) system B is in the state $|\Phi\rangle_B$ in the Hilbert space $\mathcal{H}_B$, then the composite system's state is the product $|\Psi\rangle_A \otimes |\Phi\rangle_B$ in the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$.

By restricting attention to collections of 2-state systems (or even d-state systems for finite d) one can avoid much suffering. Of course one also loses much wisdom, but hardly any of it – at least at this stage of the art – is relevant to the basic theory of quantum computation.

David Mermin

Quantum Computer Science: An Introduction. Cambridge Univ. Press.

Reversible Acting on n Qubits

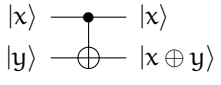
In a closed quantum system, an n-Qubit state $|\Psi\rangle \in \mathcal{H}_{2^n}$ can be transformed to some other state in $\mathcal{H}_{2^n}$, say $|\Phi\rangle$, in a reversible way only by some unitary operator U, i.e.,

$$|\Phi\rangle = U|\Psi\rangle$$

where U is a $2^n \times 2^n$ unitary matrix. As in the single-Qubit case, a unitary action on any n-Qubit state is completely described by its actions on the basis states of $\mathcal{H}_{2^n}$.

The following 2-Qubit gate is known as the *controlled* `NOT` (`CNOT`) or quantum `XOR`:

$$\texttt{CNOT} : |x, y\rangle \to |x, x \oplus y\rangle \qquad x, y \in \{0, 1\}$$



A $2^n \times 2^n$ unitary matrix U can be a Kronecker product of matrices of smaller dimensions (or not). When $U = U_0 \otimes U_1 \otimes \cdots \otimes U_{n-1}$, then its action on the basis vector of $\mathcal{H}_{2^n}$: $|i_0\rangle \otimes |i_1\rangle \otimes \cdots \otimes |i_{n-1}\rangle \in \mathcal{H}_{2^n}$ is given by

$$U\,|i_0 i_1 \ldots i_{n-1}\rangle = \boxed{U_0|i_0\rangle} \otimes \boxed{U_1|i_1\rangle} \otimes \cdots \otimes \boxed{U_{n-1}|i_{n-1}\rangle}$$

The No-Cloning Theorem

There is no reversible quantum operator that takes any state $|\psi\rangle$ to $|\psi\rangle \otimes |\psi\rangle$.

Proof. Suppose there is a unitary U_c such that

$$\begin{aligned} U_c(|\psi\rangle \otimes |\omega\rangle) &= |\psi\rangle \otimes |\psi\rangle \\ U_c(|\varphi\rangle \otimes |\omega\rangle) &= |\varphi\rangle \otimes |\varphi\rangle \end{aligned}$$

where ω is some fixed quantum state. Note the following identities:

1. By the properties of the Kronecker product, we have

$$\big(\langle\psi| \otimes \langle\omega|\big) \cdot \big(|\varphi\rangle \otimes |\omega\rangle\big) = \langle\psi|\varphi\rangle$$

2. Since U_c is unitary, that is $U_c^\dagger \cdot U = I$, then by the properties of the Kronecker product, we have

$$\begin{aligned} \langle\psi|\varphi\rangle &= \big(\langle\psi| \otimes \langle\omega|\big) \cdot \big(|\varphi\rangle \otimes |\omega\rangle\big) \\ &= \big(\langle\psi| \otimes \langle\omega|\big) U_c^\dagger \cdot U\big(|\varphi\rangle \otimes |\omega\rangle\big) \\ &= \big(\langle\psi| \otimes \langle\psi|\big) \cdot \big(|\varphi\rangle \otimes |\varphi\rangle\big) \\ &= \langle\psi|\varphi\rangle \otimes \langle\psi|\varphi\rangle \\ &= \langle\psi|\varphi\rangle^2 \end{aligned}$$

Therefore $\langle\psi|\varphi\rangle$ is either equal to 0 or to 1. Thus if U_c can clone some state $|\psi\rangle$, then the only other state U_c can clone has to be orthogonal to $|\psi\rangle$. □

Problems – Homework due on September 18

1. Show that if U and V are unitary matrices, then $U \otimes V$ is also a unitary matrix.

2. Show that the map $|x, y\rangle \to |x, x \oplus y\rangle$ for $x, y \in \{0, 1\}$ can be achieved by the following unitary matrix:

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

3. Construct a quantum gate that performs the following map:

$$\underbrace{\alpha|0\rangle + \beta|1\rangle}_{\in \mathcal{H}_2} \quad \to \quad \underbrace{\alpha|000\rangle + \beta|111\rangle}_{\in \mathcal{H}_{23}}$$

   You are allowed to use additional fixed-state quantum systems.

Introduction to Quantum Information Science [1]

[1] Rutgers, ECE 579, Fall 2019

Prof. Emina Soljanin

Lecture #4, September 16

This lecture 1) reviews Hermitian matrices, 2) introduces the notion of quantum measurement and 3) discusses classical error correction.

Math Interlude

Rank-1 Projections and Resolutions of the Identity

Recall that $|\varphi\rangle\langle\varphi|$ is a matrix. Vector $|\varphi\rangle\langle\varphi|\cdot|\psi\rangle$ is the orthogonal[2] projection of vector $|\psi\rangle$ on vector $|\varphi\rangle$. We say that $|\psi\rangle\langle\psi|$ is a rank-1 projection matrix. (Higher rank projection matrices project vectors onto subspaces.)

[2] To check for orthogonality, consider $\langle\varphi|\left(|\psi\rangle - |\varphi\rangle\langle\varphi|\cdot|\psi\rangle\right)$.

A set of vectors $|u_1\rangle, \ldots, |u_m\rangle$ form a resolution of the identity iff

1. $\langle u_i|u_j\rangle = \delta_{ij}$
2. $|u_1\rangle\langle u_1| + |u_2\rangle\langle u_2| + \cdots + |u_m\rangle\langle u_m| = I_m$

Let $|u_1\rangle, \ldots, |u_m\rangle$ be the columns of the unitary matrix U. Then $U^\dagger U = UU^\dagger = I_m$ implies that $|u_1\rangle, \ldots, |u_m\rangle$ form a resolution of the identity. For example,

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

Eigenvectors and Eigenvalues

An eigenvector of a complex $m \times m$ matrix M is a vector $|v\rangle$ such that

$$M|u\rangle = \lambda_u |u\rangle, \quad |u\rangle \neq 0, \quad \lambda_u \in \mathbb{C}$$

where λ_u is known as the eigenvalue of M corresponding to $|u\rangle$.

Hermitian Matrices

A Hermitian matrix M (or self-adjoint matrix) is a complex square matrix that is equal to its own conjugate transpose $M^\dagger$, i.e., the element in the i-th row and j-th column is equal to the complex conjugate[3] of the element in the j-th row and i-th column, for all indices i and j:

[3] The conjugate of a complex number $c = x + iy$ is $c^* = x - iy$.

$$h_{ij} = h_{ji}^*.$$

We call real Hermitian matrices *symmetric*.

Claim:[4] Matrix M is Hermitian if and only if $\langle x|Mx\rangle$ is real for all $|x\rangle$.

[4] Very frequently useful!

If follows that the eigenvalues of a Hermitian operator are real.

Hermitian and unitary matrices are normal[5]. If A is normal, then its eigenvectors corresponding to distinct eigenvalues are orthogonal. For a Hermitian matrix M, there exists a unitary matrix U such that $U^\dagger M U$ is a diagonal matrix:

$$U^\dagger M U = \begin{bmatrix} \lambda_1 & & & & \\ & \lambda_2 & & \mathbf{O} & \\ & & \ddots & & \\ & \mathbf{O} & & \lambda_{m-1} & \\ & & & & \lambda_m \end{bmatrix}$$

Let $|u_1\rangle, \ldots, |u_m\rangle$ be the columns of U, and multiply the above equation by U from the left. $\Rightarrow$

$$\left[M|u_1\rangle \ldots M|u_m\rangle\right] = \left[\lambda_1|u_1\rangle \ldots \lambda_m|u_m\rangle\right]$$

and thus $|u_1\rangle, \ldots, |u_m\rangle$ are eigenvectors of M and $\lambda_1, \ldots, \lambda_m$ are the corresponding eigenvalues. Recall that $|u_1\rangle, \ldots, |u_m\rangle$ form a basis of $\mathcal{H}^m$ and thus a resolution of the identity.

$$|u_1\rangle\langle u_1| + |u_2\rangle\langle u_2| + \cdots + |u_m\rangle\langle u_m| = I_m$$

[5] Matrix A is normal iff $AA^\dagger = A^\dagger A$

Pauli Matrices

These matrices were introduced in the early days of quantum mechanics by Wolfgang Pauli, to describe the angular momentum associated with the spin of an electron. They often appear in both physics and mathematics for various purposes. It is interesting that they are both unitary and Hermitian, and thus can serve as quantum gates, and (as we will soon see) to define quantum measurements.

matrix	action	eigenvalue/eigenvector
$\sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\|0\rangle$ —[X]— $\|1\rangle$	$+1/(\|0\rangle + \|1\rangle)$
	$\|1\rangle$ —[X]— $\|0\rangle$	$-1/(\|0\rangle - \|1\rangle)$
$\sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	$\|0\rangle$ —[Y]— $i\|1\rangle$	$+1/(\|0\rangle + i\|1\rangle)$
	$\|1\rangle$ —[Y]— $-i\|0\rangle$	$-1/(\|0\rangle - i\|1\rangle)$
$\sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\|0\rangle$ —[Z]— $\|0\rangle$	$+1/\|0\rangle$
	$\|1\rangle$ —[Z]— $-\|1\rangle$	$-1/\|1\rangle$

Quantum Measurements

To every physical observable, there corresponds an operator defined by a Hermitian matrix. The only possible results of measuring an observable are the eigenvalues of its corresponding Hermitian matrix. The only possible states after measuring an observable are the eigenvectors of its Hermitian matrix.

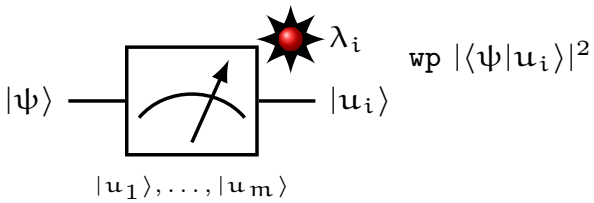


Figure 1: Quantum Measurement: When we "see" λ_i (which happens wp $|\langle\psi|u_i\rangle|^2$), we know that state $|\psi\rangle$ has collapsed to $|u_i\rangle$.

Let $|u_1\rangle, \ldots, |u_m\rangle$ be the eigenvectors of the Hermitian matrix corresponding to the observable. We also refer to $|u_1\rangle, \ldots, |u_m\rangle$ as the measurement basis. Then, after the measurement is performed on state $|\psi\rangle$, it gets projected (collapses) to state $|u_i\rangle$ with probability (wp) $|\langle\psi|u_i\rangle|^2$, $1 \leqslant i \leqslant m$.

Example: What can we get if we measure Qubit $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ in the computational basis[6] $|0\rangle$, $|1\rangle$?

Remark: The number of outcomes of a quantum measurement is finite. How many bits of information does a measurement provide?

[6] The computational basis is the one in which the Qubit is represented.

How Much Classical Information is in a Qubit?

To describe a Qubit, say $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, in a given basis, one needs to specify two complex numbers α and β. That may require a very large number of bits (depending on the chosen precision), in general, infinite.

Suppose you have acquired a Qubit. Do you posses an infinite amount of information? You would if you could read out the values of α and/or β. Is there a quantum measurement that would allow you to do that? The answer is no. Can quantum computers be more powerful than classical computers?

Figure 2: If in a 20-faced die, we can only discern if the number has one or two digits, then rolling the die is equivalent to tossing a slightly biased coin.

Error Correcting Codes

Consider the following scaled down version of the penny weighing problem we solved in our first class: How would you use a balance scale to determine which of the 3 pennies has a different weight if any? We will next use some of that reasoning to discuss the basic

principles in classical and quantum error correction. In both systems we will be concerned with *bit flips*.

Error correcting codes add redundancy to data in order to be less sensitive to errors. The most basic form of redundancy is simple replication, known as *repetition coding*. For example, if each bit is replicated 3 times, any single bit flip among the 3 replicas can be corrected by turning it to the value of the other two replicas.

We will next formally describe the process of introducing redundancy (encoding) and correcting errors (decoding) for a 1-to-3 bits repetition code, which will allow us to introduce and understand its quantum 1-to-3 Qubit counterpart, and (later in the course) study more general quantum error correction.

Correcting errors might sound like a dreary practical problem, of little aesthetic or conceptual interest. But aside from being of crucial importance for the feasibility of quantum computation, it is also one of the most beautiful and surprising parts of the subject.

David Mermin
Quantum Computer Science: An Introduction. Cambridge Univ. Press.

Classical Error Correction

- Encoding is a map that introduces redundancy. In our 1-to-3 bits repetition code example, encoding is the following map:

$$0 \to 000 \quad \text{and} \quad 1 \to 111$$

  Therefore, each bit x is mapped to a 3 bit string $x\,x\,x$.

- Error Model: In our model, at most one of the bits $x\,x\,x$ gets flipped. Such flipping is equivalent to adding (component-wise) a string in the set $\{000, 100, 010, 001\}$ to $x\,x\,x$ and getting $y_0\,y_1\,y_2$:

error	y_0	y_1	y_2
000	x	x	x
100	$x \oplus 1$	x	x
010	x	$x \oplus 1$	x
001	x	x	$x \oplus 1$

- Measurements: In a classical system, we perform the following matrix vector multiplication[7]:

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} y_0 \\ y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} y_0 \oplus y_1 \\ y_0 \oplus y_2 \end{bmatrix}$$

- Error Correction: The results of the two measurements (2 bits) instruct us how to correct errors, as follows:

y_0	y_1	y_2	$y_0 \oplus y_1$	$y_0 \oplus y_2$	add
x	x	x	0	0	000
$x \oplus 1$	x	x	1	1	100
x	$x \oplus 1$	x	1	0	010
x	x	$x \oplus 1$	0	1	001

[7] cf. Lesson # 1, penny weighing

Introduction to Quantum Information Science [1]

[1] Rutgers, ECE 579, Fall 2019

Prof. Emina Soljanin

Lecture #5, September 18

This lecture 1) introduces general von Neumann measurements, and 2) studies a simple quantum error correcting code.

Error Correcting Codes – Review

We start by reviewing our classical error correcting code example and Pauli matrices.

Classical Error Correction

- Encoding is a map that introduces redundancy. In our 1-to-3 bits repetition code example, encoding is the following map:

$$0 \to 000 \quad \text{and} \quad 1 \to 111$$

  Therefore, each bit x is mapped to a 3 bit string $x\,x\,x$.

- Error Model: In our model, at most one of the bits $x\,x\,x$ gets flipped. Such flipping is equivalent to adding (component-wise) a string in the set $\{000, 100, 010, 001\}$ to $x\,x\,x$ and getting $y_0\,y_1\,y_2$:

error	y_0	y_1	y_2
000	x	x	x
100	$x \oplus 1$	x	x
010	x	$x \oplus 1$	x
001	x	x	$x \oplus 1$

- Measurements: In a classical system, we perform the following matrix vector multiplication[2]:

[2] cf. Lesson # 1, penny weighing

$$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} y_0 \\ y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} y_0 \oplus y_1 \\ y_0 \oplus y_2 \end{bmatrix}$$

  We refer to the vector $\begin{bmatrix} y_0 \oplus y_1 \\ y_0 \oplus y_2 \end{bmatrix}$ as the *error syndrome*.

- Error Correction: The results of the two measurement (2 bits) instruct us how to correct errors, as follows:

y_0	y_1	y_2	$y_0 \oplus y_1$	$y_0 \oplus y_2$	add
x	x	x	0	0	000
$x \oplus 1$	x	x	1	1	100
x	$x \oplus 1$	x	1	0	010
x	x	$x \oplus 1$	0	1	001

Pauli Matrices – Review

These matrices were introduced in the early days of quantum mechanics by Wolfgang Pauli, to describe the angular momentum associated with the spin of an electron. They often appear in both physics and mathematics for various purposes. It is interesting that they are both unitary and Hermitian, and thus can serve as quantum gates, and (as we will soon see) to define quantum measurements.

matrix	action	eigenvalue/eigenvector
$\sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\|0\rangle$ —[X]— $\|1\rangle$	$+1/(\|0\rangle + \|1\rangle)$
	$\|1\rangle$ —[X]— $\|0\rangle$	$-1/(\|0\rangle - \|1\rangle)$
$\sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	$\|0\rangle$ —[Y]— $i\|1\rangle$	$+1/(\|0\rangle + i\|1\rangle)$
	$\|1\rangle$ —[Y]— $-i\|0\rangle$	$-1/(\|0\rangle - i\|1\rangle)$
$\sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\|0\rangle$ —[Z]— $\|0\rangle$	$+1/\|0\rangle$
	$\|1\rangle$ —[Z]— $-\|1\rangle$	$-1/\|1\rangle$

A Little More General Quantum Measurements

A simple generalization of the quantum measurement we defined in the previous lecture is known as the von Neumann's measurement.[3]. Mathematically, this type of measurement is defined by a set of $m \times m$ matrices $\{\Pi_i\}_{i=1}^{\ell}$ such that

[3] Also known as the *projective measurement*

1. $\{\Pi_i\}$ are pairwise orthogonal projection operators
2. $\{\Pi_i\}$ form a complete resolution of the identity, that is,

$$\Pi_1 + \Pi_2 + \cdots + \Pi_\ell = I_m.$$

3. The measured state $|\psi\rangle$ gets projected (collapses) to state $\frac{\Pi_i|\psi\rangle}{\|\Pi_i|\psi\rangle\|}$ with probability $\langle\psi|\Pi_i|\psi\rangle$.

Note that the only difference between this and our previous definition is that here we do not require that Π_i be rank-1 projections. This generalization comes about when we remove the requirement that all eigenvalues of the Hermitian matrix corresponding to the measured observable be distinct.

Suppose we know that a quantum system is in one of ℓ possible states, say $\{|\psi_1\rangle, \ldots, |\psi_\ell\rangle\}$. Only when the possible states are orthogonal can a quantum measurement be designed to give an unambiguous answer about the state of the system. Therefore the set of errors we can tell apart are those which take the original state to a set of orthogonal states.

A Quantum Error Correcting Code

Quantum error correction[4] has to follow the laws of quantum mechanics. Therefore each action on Qubits has to be either unitary or a measurement.

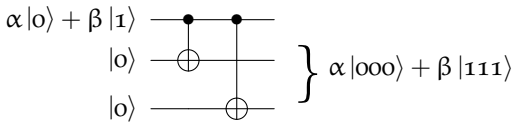
[4] *As significant as Shor's factoring algorithm may prove to be, there is another recently discovered feature of quantum information that may be just as important: the discovery of quantum error correction. Indeed, were it not for this development, the prospects for quantum computing technology would not seem bright.*

John Preskill
Quantum Computation Lecture Notes. Chapter 1, 1997/98.

- Encoding: As in the classical case, encoding is a map that introduces redundancy. In our example, a single Qubit state is mapped into a 3-Qubit state as follows:

$$\alpha|0\rangle + \beta|1\rangle \rightarrow \alpha|000\rangle + \beta|111\rangle$$

The following unitary circuit can serve as a quantum mechanically valid encoder for our code. It uses two `CNOT` gates and two ancillary Qubits, each initially in the state $|0\rangle$.



The result is an entangled 3-Qubit state.

- Error Model: In our model, at most one Qubit experiences the basis flip. This flipping errors result from unitary error operators as follows:

error operators	resulting state
$I \otimes I \otimes I$	$\alpha\|000\rangle + \beta\|111\rangle$
$\sigma_X \otimes I \otimes I$	$\alpha\|100\rangle + \beta\|011\rangle$
$I \otimes \sigma_X \otimes I$	$\alpha\|010\rangle + \beta\|101\rangle$
$I \otimes I \otimes \sigma_X$	$\alpha\|001\rangle + \beta\|110\rangle$

- Measurements: We perform the following two measurements:

$\boxed{M_1}$: Defined by the Hermitian operator $\sigma_Z \otimes \sigma_Z \otimes I$, i.e., the following two orthogonal projection operators:[5]

[5] M_1 compares Qubits 1 and 2.

$$\Pi_1 = |000\rangle\langle 000| + |111\rangle\langle 111| + |001\rangle\langle 001| + |110\rangle\langle 110|$$
$$\Pi_2 = |010\rangle\langle 010| + |101\rangle\langle 101| + |011\rangle\langle 011| + |100\rangle\langle 100|$$

Π_1 projects on the eigenspace of $\sigma_Z \otimes \sigma_Z \otimes I$ with eigenvalue 1, and Π_2 projects on the eigenspace of $\sigma_Z \otimes \sigma_Z \otimes I$ with eigenvalue -1.

$\boxed{M_2}$: Defined by the Hermitian operator $\sigma_Z \otimes I \otimes \sigma_Z$, i.e., the following two orthogonal projection operators:[6]

[6] M_2 compares Qubits 1 and 3.

$$\Pi_1 = |000\rangle\langle 000| + |111\rangle\langle 111| + |010\rangle\langle 010| + |101\rangle\langle 101|$$
$$\Pi_2 = |001\rangle\langle 001| + |110\rangle\langle 110| + |011\rangle\langle 011| + |100\rangle\langle 100|$$

Π_1 projects on the eigenspace of $\sigma_Z \otimes I \otimes \sigma_Z$ with eigenvalue 1, and Π_2 projects on the eigenspace of $\sigma_Z \otimes I \otimes \sigma_Z$ with eigenvalue -1.

- Error Correction: The results of the two measuremens are two eigenvalues (2 bits). As in the classical case, we refer to this result as the error syndrome, which instructs us how to correct errors, as follows:

corrupted state	M_1	M_2	apply
$\alpha\|000\rangle + \beta\|111\rangle$	$+1$	$+1$	$I \otimes I \otimes I$
$\alpha\|100\rangle + \beta\|011\rangle$	-1	-1	$\sigma_X \otimes I \otimes I$
$\alpha\|010\rangle + \beta\|101\rangle$	-1	$+1$	$I \otimes \sigma_X \otimes I$
$\alpha\|001\rangle + \beta\|110\rangle$	$+1$	-1	$I \otimes I \otimes \sigma_X$

Remark: The error detecting procedure we used 1) follows directly from classical error correction and 2) it is is useful in generalizing to other quantum codes with more Qubits. However, M_1 and M_2 are not the only measurements we can use to obtain the error syndrome that can uniquely identify the error. To see that consider the following set of projections:

$$\Pi_1 = |000\rangle\langle 000| + |111\rangle\langle 111| \text{ no error}$$
$$\Pi_2 = |100\rangle\langle 100| + |011\rangle\langle 011| \text{ bit flip on Qubit one}$$
$$\Pi_3 = |010\rangle\langle 010| + |101\rangle\langle 101| \text{ bit flip on Qubit two}$$
$$\Pi_4 = |001\rangle\langle 001| + |110\rangle\langle 110| \text{ bit flip on Qubit three}$$

Note that the (no)-error states belong to orthogonal subspaces, and therefore a von Neumann measurement defined by projectors to those subspaces can 1) unambiguously identify the error state and 2) will not disturb the measured state.

Problems – Homework due on September 23

1. Prove that orthogonal projection operators are Hermitian.

2. You are given a set of vectors $|u_i\rangle \in \mathcal{H}_m$, $i = 1, 2, \ldots, m$ that form a resolution of the identity $\langle u_i|u_j\rangle = \delta_{ij}$. Construct a Hermitian matrix which has $|u_i\rangle$ as its eigenvectors corresponding to different eigenvalues.

3. You are given a set of ℓ orthogonal projection $m \times m$ matrices that form a resolution of the identity and are pairwise orthogonal on $\mathcal{H}_m$, where $\ell \leqslant m$. Construct a Hermitian matrix whose eigienspaces corresponding to different eigenvalues are the image spaces of these projection matrices.

4. Suppose you used the 1-to-3 Qubit code and there were bit flips on Qubit 1 and on Qubit 2. Which state would you decode if you followed the measurement and correction procedure we defined in class?

Introduction to Quantum Information Science [1]

[1] Rutgers, ECE 579, Fall 2019

Prof. Emina Soljanin

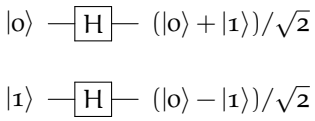
Lecture #6, September 30

This lecture 1) explains how 2-Qubit entanglement can be created by elementary gates, and 2) describes two communication protocols, dense coding and teleportation, which exploit entanglement.

Hadamard and `CNOT` Gates – Review

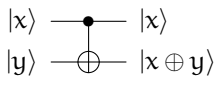
Hadamard gate is a single qubit gate:

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



`CNOT` gate is a two qubit gate:

$$\texttt{CNOT} : |x, y\rangle \to |x, x \oplus y\rangle \qquad x, y \in \{0, 1\}$$



Bell States

Recall that 2-Qubit states that can be written as a Kronecker product of 2 single-Qubit states are called *separable* and those that cannot are called *entangled*[2] states.

[2] Entangled states are responsible for much of "quantum magic".

An entangled pair of states can be created by applying a unitary transform to separable states, e.g., as shown in Fig. 1.

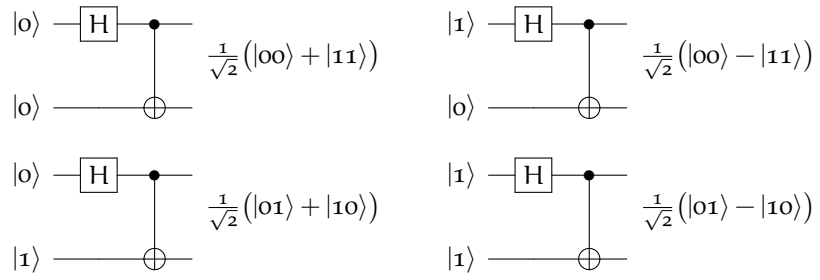


Figure 1: Creating Bell states by a 2-Qubit entanglement gate.

The 4 entangled states in Fig. 1 are known as Bell[3] states. Notice that they are orthogonal, which should not be a surprise since they are created by a unitary transform from the 4 computational basis states. Therefore, Bell states can be used to define a measurement, which is often referred to as the Bell measurement.

[3] We will learn more about John Bell and his inequalities later.

Entangled states have some "surprising" properties. To see that, we consider the EPR pair:[4]

[4] EPR stands for Einstein, Podolsky and Rosen, who were the first to point out the "strange" properties of this state.

$$\frac{1}{\sqrt{2}}\big(|00\rangle + |11\rangle\big)$$

and observe the following:

1. The individual Qubits that make up an entangled state cannot always be characterized as having individual states of their own. Consider, for example, the first Qubit, and observe that it cannot be represented in the form $\alpha|0\rangle + \beta|1\rangle$.

2. There seems to be *spooky action at a distance:*[5] What happens if we measure only the first Qubit in the computational basis? Two outcomes are possible: $|0\rangle$ with probability $1/2$, giving the post-measurement 2-Qubit state $|00\rangle$, and $|1\rangle$ with probability $1/2$, giving the post-measurement 2-Qubit state $|11\rangle$. What happens if we subsequently measure the other Qubit? Only one outcome is possible: the one that gives the same result as the measurement of the first Qubit. This behavior has been confirmed by experiment.

[5] Einstein's phrase; he was not comfortable with the notion of non-deterministic measurements and entanglement.

Dense Coding

If Alice sends a Qubit, say $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, to Bob, how many bits does he get? Recall that Bob cannot read the values of complex numbers α and/or β. He can only possibly apply some unitary transformation to $|\psi\rangle$ and then perform a measurement, which would give him at most one bit.

The most Alice can communicate to Bob by sending him a single Qubit is a single bit of information, unless they share an EPR pair.

Suppose Alice and Bob had prepared together and entangled pair of Qubits in the state

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

and then Alice took Qubit A and Bob took Qubit B. How does the state $|\Psi\rangle$ evolve if only Alice applies a unitary transformation to her Qubit? Consider the following 4 local unitary actions on the first Qubit:

$$\begin{aligned}
(I \otimes I)|\Psi\rangle &= \frac{1}{\sqrt{2}}\big(|0_A 0_B\rangle + |1_A 1_B\rangle\big)\\
(\sigma_X \otimes I)|\Psi\rangle &= \frac{1}{\sqrt{2}}\big(|1_A 0_B\rangle + |0_A 1_B\rangle\big)\\
(\sigma_Z \otimes I)|\Psi\rangle &= \frac{1}{\sqrt{2}}\big(|0_A 0_B\rangle - |1_A 1_B\rangle\big)\\
(\sigma_Z\sigma_X \otimes I)|\Psi\rangle &= \frac{1}{\sqrt{2}}\big(-|1_A 0_B\rangle + |0_A 1_B\rangle\big)
\end{aligned}$$

Note that Alice is able to create 4 orthogonal states.[6] If after performing her local action, Alice sends her Qubit to Bob, he can unambiguously identify which of the 4 orthogonal Bell states the EPR pair assumed as a result of Alice's action. He can therefore get two bits

[6] Would Alice be able to create 4 orthogonal global states by local actions if the qubits were not entangled?

of information. Alice and Bob have to have agreed on how to label Alice's actions, e.g.,

$$\begin{aligned} 00: &\quad (I \otimes I) \\ 01: &\quad (\sigma_X \otimes I) \\ 10: &\quad (\sigma_Z \otimes I) \\ 11: &\quad (\sigma_Z \sigma_X \otimes I) \end{aligned}$$

For example, if Alice wants to send two classical bits 10 to Bob, she will apply σ_Z to her Qubit before sending it to Bob. That would create the global state in Bob's possession $\frac{1}{\sqrt{2}}(|0_A 0_B\rangle - |1_A 1_B\rangle)$, which he will learn after performing the Bell measurement.

Teleportation

Suppose Alice and Bob had prepared together an entangled pair of Qubits in the state

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

and then Alice took Qubit A and Bob took Qubit B. Now, Alice has another Qubit in the state[7]

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

which she would like to send to Bob. However, there is only a classical communications channel between her and Bob. Can Alice send her Qubit to Bob by sending only classical bits of information? How many classical bits does she need to send?

To answer that question, consider the joint state of Alice's new Qubit and the entangled pair:

$$\begin{aligned} |\psi\rangle\,|\Psi\rangle &= (\alpha\,|0\rangle_a + \beta\,|1\rangle_a)\,\frac{1}{\sqrt{2}}(|0_A\rangle\,|0_B\rangle + |1_A\rangle\,|1_B\rangle) \\ &= \alpha\,|0\rangle_a\,\frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle) + \beta\,|1\rangle_a\,\frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle) \end{aligned}$$

The following protocol , known as teleportation, results in Bob's Qubit (member of the entangled pair) assuming the state $|\psi\rangle$:[8]

1. Alice first applies a `CNOT` gate to her two Qubits

$$|x\rangle_a\,|x_A\rangle \to |x_a\rangle\,|x_a \oplus x_A\rangle$$

and the 3-Qubit state becomes

$$|\Phi\rangle = \alpha\,|0\rangle_a\,\frac{1}{\sqrt{2}}(|0_A 0_B\rangle + |1_A 1_B\rangle) + \beta\,|1\rangle_a\,\frac{1}{\sqrt{2}}(|1_A 0_B\rangle + |0_A 1_B\rangle)$$

[7] We will use a (new) and A (entangled with Bob) subscripts to distinguish the two Qubits on Alice's side.

[8] Is teleportation cloning?

2. Alice then applies a Hadamard transformation H to her Qubit a, and the joint state becomes

$$\begin{aligned}(H\otimes I\otimes I)\,|\Phi\rangle &= \alpha\frac{1}{\sqrt{2}}(|0\rangle_A+|1\rangle_B)\frac{1}{\sqrt{2}}\big(|0_A0_B\rangle+|1_A1_B\rangle\big)\\ &\quad+\beta\frac{1}{\sqrt{2}}(|0\rangle_A-|1\rangle_B)\frac{1}{\sqrt{2}}\big(|1_A0_B\rangle+|0_A1_B\rangle\big)\\ &=\frac{1}{2}\,|00\rangle_{aA}\left(\alpha\,|0\rangle_B+\beta\,|1\rangle_B\right)+\frac{1}{2}\,|01\rangle_{aA}\left(\alpha\,|1\rangle_B+\beta\,|0\rangle_B\right)\\ &\quad+\frac{1}{2}\,|10\rangle_{aA}\left(\alpha\,|0\rangle_B-\beta\,|1\rangle_B\right)+\frac{1}{2}\,|11\rangle_{aA}\left(\alpha\,|1\rangle_B-\beta\,|0\rangle_B\right)\end{aligned}$$

   Observe the following:

   (a) The 4 states in the above sum are orthogonal.

   (b) For each of the 4 basis states on Alice's side, we have a corresponding state on Bob's side that can be obtained from $|\psi\rangle$ by a unitary action:

$$\begin{aligned}\alpha\,|0\rangle_B+\beta\,|1\rangle_B &= I\,|\psi\rangle\\ \alpha\,|1\rangle_B+\beta\,|0\rangle_B &= \sigma_X\,|\psi\rangle\\ \alpha\,|0\rangle_B-\beta\,|1\rangle_B &= \sigma_Z\,|\psi\rangle\\ \alpha\,|1\rangle_B-\beta\,|0\rangle_B &= \sigma_Z\sigma_X\,|\psi\rangle\end{aligned}$$

3. Alice performs a joint measurement of her two Qubits in the computational basis. Her pair of Qubits will collapse to one of the basis states and Bob's Qubit will assume[9] its corresponding state. After the measurement, Alice knows which state she is left with and thus which state Bob's Qubit is in. Bob can turn that state to $|\psi\rangle$ by applying the appropriate unitary operator. Whether that operator should be I, or σ_X or σ_Z or $\sigma_Z\sigma_X$ can be communicated to him by Alice with 2 bits of classical information. They have to have agreed on how to label the 4 operators.

   Observe that there is only one copy[10] of state $|\psi\rangle$ at the end of the protocol, the one that Bob has. Alice's 2-Qubit state collapsed to a basis state after her measurement.

[9] by the entanglement magic

[10] Teleportation is not cloning.

Introduction to Quantum Information Science [1]

[1] Rutgers, ECE 579, Fall 2019

Prof. Emina Soljanin

Lecture #7, October 2

This lecture considers several important multi-Qubit gates, and the Deutsch-Jozsa algorithm.

Some Multi-Quibit Gates

Single-Qubit Hadamard Gate

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

$$|0\rangle \text{ —}\boxed{H}\text{— } (|0\rangle + |1\rangle)/\sqrt{2}$$

$$|1\rangle \text{ —}\boxed{H}\text{— } (|0\rangle - |1\rangle)/\sqrt{2}$$

$$H|x\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + (-1)^x|1\rangle)$$

n-*Qubit Separable Hadamard Gate*

$$H^{\otimes n} = \underbrace{H \otimes H \otimes \cdots \otimes H}_{n \text{ times}}.$$

How does $H^{\otimes n}$ act on the basis state $|0\rangle^{\otimes n}$? It is easy to see that $H^{\otimes n}$ creates a uniform superposition of all basis states.

$$|0\rangle^{\otimes n} \text{ —}\boxed{H^{\otimes n}}\text{— } \tfrac{1}{2^{n/2}}\sum_{i=0}^{2^n-1}|i\rangle$$

We next look into how $H^{\otimes n}$ acts on an arbitrary base state $|x\rangle$ where $|x\rangle = |x_0\rangle \otimes |x_1\rangle \otimes \cdots \otimes |x_{n-1}\rangle$ and $x_0x_1 \ldots x_{n-1}$ is the binary representation of x:[2]

[2] Need to know for the Deutsch-Jozsa algorithm.

$$\begin{aligned} H^{\otimes n}|x\rangle &= H|x_0\rangle \otimes \cdots \otimes H|x_{n-1}\rangle \\ &= \frac{1}{\sqrt{2^n}}(|0\rangle + (-1)^{x_0}|1\rangle) \otimes \cdots \otimes (|0\rangle + (-1)^{x_{n-1}}|1\rangle) \\ &= \frac{1}{\sqrt{2^n}}\sum_{y=0}^{2^n-1}(-1)^{x\cdot y}|y\rangle \end{aligned}$$

where $x \cdot y = x_0y_0 \oplus x_1y_1 \oplus \cdots \oplus x_{n-1}y_{n-1}$ is the mod 2 sum of the bitwise product.

2-Qubit Controlled `NOT` *Gate*

The following 2-Qubit gate is known as the *controlled* `NOT` (`CNOT`) or quantum `XOR`:

$$\texttt{CNOT} : |x, y\rangle \to |x, x \oplus y\rangle \qquad x, y \in \{0, 1\}$$

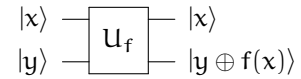
$$|x\rangle \text{ —}\bullet\text{— } |x\rangle$$

$$|y\rangle \text{ —}\oplus\text{— } |x \oplus y\rangle$$

Function Evaluation

We can evaluate an m-bit valued function f of an n-bit string x: $f : \{0,1\}^n \to \{0,1\}^m$

$$U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle \qquad x \in \{0,1\}^n,\ y \in \{0,1\}^m$$



Why is U_f a valid quantum gate?

Quantum Parallelism

If we first create a superposition of all basis states by applying the $H^{\otimes n}$ gate to state $|0\rangle^{\otimes n}$, and then apply the U_f gate, we can simultaneously compute the value of f on its entire domain:[3]

[3] But can we see the result?

$$U_f\left(H^{\otimes n} \otimes I_m\right)\left(|0\rangle^{\otimes n} \otimes |0\rangle^{\otimes m}\right) = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle$$

The Deutsch Problem

Problem Statement

In the Deutsch Problem, we are concerned with a binary function[4]

[4] There are only 4 such functions. What are they?

$$f : \{0,1\} \to \{0,1\}$$

and know that it is either *constant* (0 on the entire domain or 1 on the entire domain) or *balanced* (1 for half of the domain and 0 for the other half). The goal is to tell whether f is constant by performing only one evaluation of the function.

An Algorithm

We begin with the two-qubit state $|0\rangle|1\rangle$ and apply a Hadamard transform to each qubit. This yields

$$\frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = |0\rangle\left(|0\rangle - |1\rangle\right) + |1\rangle\left(|0\rangle - |1\rangle\right)$$

We are given a quantum implementation of the function f that maps $|x\rangle|y\rangle$ to $|x\rangle|f(x) \oplus y\rangle$. Applying this function to our current state we obtain

$$\begin{aligned} U_f \cdot \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \\ = \frac{1}{2}\left(|0\rangle(|f(0) \oplus 0\rangle - |f(0) \oplus 1\rangle\right) + |1\rangle\left(|f(1) \oplus 0\rangle - |f(1) \oplus 1\rangle\right) \\ = \frac{1}{2}\left(|0\rangle(|f(0)\rangle - |\tilde{f}(0)\rangle\right) + |1\rangle\left(|f(1)\rangle - |\tilde{f}(1)\rangle\right) \end{aligned}$$

where $\tilde{f}(x) = 1 \oplus f(x)$ denote the complement (NOT) of $f(x)$. Observe that since f is a binary function, we have either $f(0) = f(1)$ or $f(0) = 1 \oplus f(1)$.

We further have

$$U_f \frac{1}{2}(|0\rangle + |1\rangle)(|0\rangle - |1\rangle) = \begin{cases} \frac{1}{2}(|0\rangle + |1\rangle)\big(|f(0)\rangle - |\tilde{f}(0)\rangle\big) & \text{if } f(0) = f(1) \\ \frac{1}{2}(|0\rangle - |1\rangle)\big(|f(0)\rangle - |\tilde{f}(0)\rangle\big) & \text{if } f(0) \neq f(1) \end{cases}$$

We can now perform a measurement of this 2-Qubit state according to the observable $\sigma_X \otimes I$. Recall that $|0\rangle + |1\rangle)$ and $|0\rangle - |1\rangle)$ are eigenvectors of σ_X with respective eigenvalues 1 and -1.

The Deutsch-Jozsa Problem - Homework due October 9

Be prepared to explain on the board the problem, as described below.

Problem Statement

The Deutsch-Jozsa problem is a generalization of the Deutsch problem in the sense that we are again asked to tell whether a binary function f is constant or balanced by performing only one evaluation of the function. But here, the domain of f is $\{0,1\}^n$: [5]

$$f : \{0,1\}^n \to \{0,1\}.$$

[5] Simply put, the function takes n-digit binary values as input and produces either a 0 or a 1 as output for each such value.

The algorithm 1) begins with the $(n+1)$-Qubit state $|0\rangle^{\otimes n}|1\rangle$, 2) creates a superposition by applying the Hadamard transform to each of the $n+1$ Qubits, 3) Calculates f by passing the resulting $n+1$-Qubit state through the the U_f gate, 4) performs the Hadamard transform on the first n Qubits, the and 5) measures the final state in the computational basis to get an unambiguous answer whether the function is balanced or constant. Before we look into these steps in more detail, we make the following two observations:

1. For a binary function f, we have

$$\begin{aligned} |f(x)\rangle - |1 \oplus f(x)\rangle &= \begin{cases} |0\rangle - |1\rangle & \text{if } f(x) = 0 \\ |1\rangle - |0\rangle & \text{if } f(x) = 1 \end{cases} \\ &= (-1)^{f(x)}(|0\rangle - |1\rangle) \end{aligned}$$

2. For a binary function $f : \{0,1\}^n \to \{0,1\}$, we have

$$\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} = \begin{cases} (-1)^{f(0)} & \text{if } f \text{ is constant} \\ 0 & \text{if } f \text{ is balanced} \end{cases}$$

The Algorithm

1. Set up the initial $n+1$ Qubit state to $|\psi_0\rangle = |0\rangle^{\otimes n}|1\rangle$

2. Create a superposition by using Hadamard gates to $|\psi_0\rangle$ obtain the state

$$|\psi_1\rangle = \left(H^{\otimes n} \otimes H\right) \underbrace{|0\rangle^{\otimes n}|1\rangle}_{|\psi_0\rangle} = \left(|0\rangle + |1\rangle\right)^{\otimes n}(|0\rangle - |1\rangle)$$
$$= \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle(|0\rangle - |1\rangle).$$

3. Calculate function f using U_f that maps $|x\rangle|y\rangle$ to $|x\rangle|y \oplus f(x)\rangle$:

$$U_f\,|\psi_1\rangle = \frac{1}{\sqrt{2^{n+1}}} \sum_{x=0}^{2^n-1} |x\rangle(|f(x)\rangle - |1 \oplus f(x)\rangle)$$
$$= \underbrace{\frac{1}{\sqrt{2^n}} \sum_{x=0}^{2^n-1} (-1)^{f(x)}|x\rangle}_{|\psi_2\rangle} \otimes \frac{(|0\rangle - |1\rangle)}{\sqrt{2}}$$

4. At this point the last Qubit may be ignored. We apply a Hadamard transform to each Qubit of $|\psi_2\rangle$ and obtain

$$\left|\psi_3\right\rangle = H^{\otimes n}\,|\psi_2\rangle\, \frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)} \left[\sum_{y=0}^{2^n-1} (-1)^{x\cdot y}|y\rangle\right]$$
$$= \frac{1}{2^n} \sum_{y=0}^{2^n-1} \left[\sum_{x=0}^{2^n-1} (-1)^{f(x)}(-1)^{x\cdot y}\right] |y\rangle$$
$$= \left[\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)}\right] |0\rangle + \frac{1}{2^n} \sum_{y=1}^{2^n-1} \left[\sum_{x=0}^{2^n-1} (-1)^{f(x)}(-1)^{x\cdot y}\right] |y\rangle$$

5. We now can measure $\left|\psi_3\right\rangle$ in the computational basis. Note that the probability of measuring $|0\rangle^{\otimes n}$ is

$$\left|\frac{1}{2^n} \sum_{x=0}^{2^n-1} (-1)^{f(x)}\right|^2$$

which, as we have shown above, is equal to 1 if $f(x)$ is constant or to 0 if $f(x)$ is balanced. Therefore, if the output of the measurement is $|0\rangle^{\otimes n}$, then f is constant; otherwise f is balanced.

Introduction to Quantum Information Science [1]

Prof. Emina Soljanin

Lecture #8, October 7

[1] Rutgers, ECE 579, Fall 2019

This lecture is about the Grover's search algorithm.

We have seen several quantum algorithms that achieve greater efficiency than their classical counterparts by exploiting quantum superposition and quantum entanglement. Grover's algorithm uses quantum superposition and *amplitude amplification.* In a quantum computer, amplitude amplification can be used to obtain a quadratic speedup over several classical algorithms.

Grover's Search Problem

Consider an unsorted database with $N = 2^n$ entries. The goal is to determine the index of the unique database entry that satisfies some given search criterion. We assume that we have an oracle function f that maps the database entries to 0 or 1, where $f(x) = 1$ if and only if x satisfies the search criterion. That is,

$$f : \{0,1\}^n \to \{0,1\}, \quad \text{where } f(x) = 0 \text{ iff } x = \omega.$$

Thus we need to find the unique $\omega \in \{0,1\}^n$ such that $f(\omega) = 1$. [2]

[2] As in the Deutsch-Jozsa (DJ) problem, function f takes n-digit binary values as input and produces either a 0 or a 1 as output. In the DJ problem we knew that f is either constant or balanced, and in the Grover's problem, we know that there is a unique ω s.t. $f(\omega) = 1$.

Classical Solution Complexity

Since the database is unstructured, we can not do better than evaluate the oracle function f element by element until we reach the database element ω for which $f(\omega) = 0$. Note that the probability to find the element of interest ω with a single query is $1/n$. If the first checked element is not ω, which happens with probability $(n-1)/n$, then the probability to get ω with the following query is $1/(n-1)$. Therefore, the probability to find ω with the second query is

$$\frac{n-1}{n} \cdot \frac{1}{n-1} = \frac{1}{n}.$$

Continuing in the same manner, we see that the probability that it will take k queries to find ω is $1/n$ for $k = 1, \ldots, n$. Therefore, on average, we will have to make $N/2$ queries.

Grover's Algorithm

Preliminaries

We assume that we have access to a quantum oracle capable of recognizing solutions to the search problem. The quantum oracle if our quantum function evaluation gate for the classical oracle f, defined above, that returns 1 if supplied ω, and otherwise, it returns 0.

Recall that the function evaluation gate (our oracle here) is a unitary operator acting on two qubits:

$$|x\rangle|q\rangle \xrightarrow{U_f} |x\rangle|q \oplus f(x)\rangle,$$

where $|x\rangle$ is the input n-qubit state and $|q\rangle$ is the oracle's ancillary qubit. Note that if the ancillary qubit is prepared in the state

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

we have

$$\begin{aligned} U_f\big(|x\rangle \otimes |-\rangle\big) &= \frac{1}{\sqrt{2}}\left(U_f|x\rangle|0\rangle - U_f|x\rangle|1\rangle\right) \\ &= \frac{1}{\sqrt{2}}\left(|x\rangle|f(x)\rangle - |x\rangle|1 \oplus f(x)\rangle\right) \\ &= \begin{cases} \frac{1}{\sqrt{2}}\left(|x\rangle|1\rangle - |x\rangle|0\rangle\right) = -|x\rangle \otimes |-\rangle & \text{if } f(x) = 1, \\ \frac{1}{\sqrt{2}}\left(|x\rangle|0\rangle - |x\rangle|1\rangle\right) = |x\rangle \otimes |-\rangle & \text{if } f(x) = 0 \end{cases} \end{aligned}$$

Observe that the action of U_f on the input register can be described by the following unitary operator:[3]

$$U_\omega = I - 2|\omega\rangle\langle\omega|.$$

[3] Check this claim as an exercise.

We are now ready to describe the Grover's algorithm.

Initialization

We prepare an n-qubit state $|\psi_0\rangle$ in the uniform superposition of all basis states:

$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle.$$

The following gate is known as the Grover diffusion operator:

$$U_{|\psi_0\rangle} = 2\,|\psi_0\rangle\,\langle\psi_0| - I$$

The following two-step action is known as the Grover Iteration:

Apply the operator U_ω followed by the operator $U_{|\psi_0\rangle}$.

Algorithm

1. Perform the following "Grover iteration" $O(\sqrt{N})$ times.
2. Perform the measurement in the computational basis.
3. Check the result by the oracle.
   If it does not pass the set, repeat the algorithm.

The following computations show what happens after the first iteration of the algorithm. Observe that we have start with the state $|\psi_0\rangle$ and end with the state $|\psi_1\rangle$.

$$\begin{aligned}
U_\omega|\psi_0\rangle &= (I - 2|\omega\rangle\langle\omega|)|\psi_0\rangle = |\psi_0\rangle - 2|\omega\rangle\langle\omega|\psi_0\rangle \\
&= |\psi_0\rangle - \tfrac{2}{\sqrt{N}}|\omega\rangle, \\
U_{|\psi_0\rangle}\left(|\psi_0\rangle - \tfrac{2}{\sqrt{N}}|\omega\rangle\right) &= (2|\psi_0\rangle\langle\psi_0| - I)\left(|\psi_0\rangle - \tfrac{2}{\sqrt{N}}|\omega\rangle\right) \\
&= 2|\psi_0\rangle\langle\psi_0|\psi_0\rangle - |\psi_0\rangle - \tfrac{4}{\sqrt{N}}|\psi_0\rangle\langle\psi_0|\omega\rangle + \tfrac{2}{\sqrt{N}}|\omega\rangle \\
&= 2|\psi_0\rangle - |\psi_0\rangle - \tfrac{4}{\sqrt{N}}\cdot\tfrac{1}{\sqrt{N}}|\psi_0\rangle + \tfrac{2}{\sqrt{N}}|\omega\rangle \\
&= |\psi_0\rangle - \tfrac{4}{N}|\psi_0\rangle + \tfrac{2}{\sqrt{N}}|\omega\rangle \\
&= \tfrac{N-4}{N}|\psi_0\rangle + \tfrac{2}{\sqrt{N}}|\omega\rangle \\
&= |\psi_1\rangle\,.
\end{aligned}$$

Observe that the square amplitude of the element of interest ω has increased from $|\langle\omega|\psi_0\rangle|^2 = \frac{1}{N}$ in the initial state $|\psi_0\rangle$ to

$$\left|\langle\omega|U_{|\psi_0\rangle}U_\omega|\psi_0\rangle\right|^2 = \left|\tfrac{1}{\sqrt{N}}\cdot\tfrac{N-4}{N} + \tfrac{2}{\sqrt{N}}\right|^2 = \tfrac{(3N-4)^2}{N^3} = 9\left(1 - \tfrac{4}{3N}\right)^2\cdot\tfrac{1}{N}.$$

in the end state $|\psi_1\rangle$. After $O(N)$ iterations, the amplitude will be amplified to the value close to 1. A measurement of this state in the computational basis is therefore very likely to give the state ω.

Homework - due October 14

Find an environment to simulate Grover's algorithm and be ready to explain your findings in class.

Introduction to Quantum Information Science [1]

[1] Rutgers, ECE 579, Fall 2019

Prof. Emina Soljanin

Lecture #9, October 14

This lecture discusses 1) Simon's period finding problem and 2) Shor's period finding problem and its connection with factoring.

Simon's Problem

Problem Description

In the Simon's problem, we are given a function

$$f : \{0,1\}^n \to \{0,1\}^m,$$

and know that, for some $a \in \{0,1\}^n$, we have, for all $x, y \in \{0,1\}^n$,

$$f(x) = f(y) \ \underline{\text{if and only if}} \ x \oplus y = a.$$

In other words, $f(x) = f(x \oplus a)$, for all $x \in \{0,1\}^n$, and the problem is to find a.[2]

[2] This is a period finding problem.

Observe that the above condition requires that f be a one-to-one function when $a = 0$, and two-to-one function, when $a \neq 0$. Note that $x \oplus y = 0^n$ if and only if $x = y$.

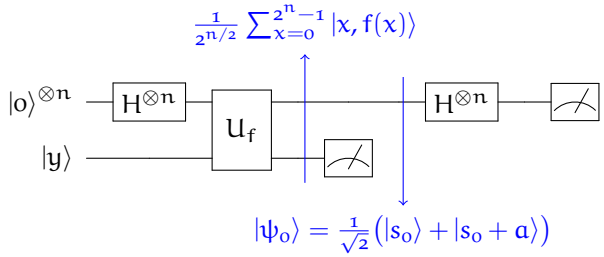


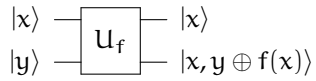
Figure 1: Steps 2, 3 and 4. This is the quantum part of the algorithm. See the sections below for more detail.

Parallel Function Evaluation

We can evaluate an m-bit valued function f of an n-bit string x:

$f : \{0,1\}^n \to \{0,1\}^m$

$$U_f : |x, y\rangle \to |x, y \oplus f(x)\rangle$$
$$x \in \{0,1\}^n,\ y \in \{0,1\}^m$$



Why is U_f a valid quantum gate?

If we first create a superposition of all basis states by applying the Hadamard $H^{\otimes n}$ gate to state $|0\rangle^{\otimes n}$, and then apply the U_f gate, we can simultaneously compute the value of f on its entire domain:[3]

[3] But can we see the result?

$$U_f\left(H^{\otimes n} \otimes I_m\right)\left(|0\rangle^{\otimes n} \otimes |0\rangle^{\otimes m}\right) = \frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle$$

Measurement followed by a Hadamard Transform

What happens when we measure the right part of the register

$$\frac{1}{2^{n/2}} \sum_{x=0}^{2^n-1} |x, f(x)\rangle$$

and get the result $f(s_0)$? Then the state of the left register becomes

$$|\psi_0\rangle = \frac{1}{\sqrt{2}}\big(|s_0\rangle + |s_0 + a\rangle\big).$$

We next apply the Hadamard transform[4] on $|\psi_0\rangle$ and get $|\psi_1\rangle$:

$$\begin{aligned}
|\psi_1\rangle = H^{\otimes n}|\psi_0\rangle &= H^{\otimes n}\frac{1}{\sqrt{2}}\big(|s_0\rangle + |s_0 + a\rangle\big) \\
&= \frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} \Big((-1)^{s_0\cdot y} + (-1)^{(s_0+a)\cdot y}\Big)|y\rangle \\
&= \frac{1}{\sqrt{2^{n+1}}} \sum_{y=0}^{2^n-1} (-1)^{s_0\cdot y}\Big(1 + (-1)^{a\cdot y}\Big)|y\rangle \\
&= \frac{2}{\sqrt{2^{n+1}}} \sum_{y=0, a\cdot y=0}^{2^n-1} (-1)^{s_0\cdot y}|y\rangle
\end{aligned}$$

[4] Recall that

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

$x\cdot y = x_0y_0 \oplus x_1y_1 \oplus \cdots \oplus x_{n-1}y_{n-1}$

If we measure state $|\psi_1\rangle$ in the computational basis, the state will collapse to some $|y\rangle$ for which $a \cdot y = 0$ (to any such y with equal probability).[5]

[5] How many such y-s are there? How many of them can be linearly independent in $\mathbb{F}_2^n$?

Therefore, we get one equation with n unknowns of the form $a \cdot y_1 = 0$. We need n linearly independent equations to solve for a. We can get $n-1$ of such equations with high probability[6] by repeating the above procedure a finite number of times, and getting linearly independent[7] vectors y_i s.t. $a \cdot y_1 = 0$. We can get the n-th equation by picking any vector y_n in $\mathbb{F}_2^n$ which is not in the span of $y_1, \ldots y_{n-1}$ (and therefore not orthogonal to a). The resulting system of linearly independent equations is

[6] requires proof

[7] Check for linear independence classically!

$$\begin{aligned}
&a \cdot y_i = 0, \quad i = 1, \ldots, n-1 \\
&a \cdot y_n = 1
\end{aligned}$$

Recall that the D-J algorithm makes only a single evaluation of U_f to decide whether the function is constant or balanced. Observe that the Simon's algorithm runs the quantum part $O(n)$ times followed by classical post processing to discover the value of a. A classical algorithm would have to make $O(2^{n/2})$ calls to f.[8]

[8] A *birthday problem* argument.

Simon's algorithm is significant in multiple ways, e.g., 1) it separates certain computational complexity classes, and 2) it is a precursor of the Shor's factoring algorithm.

Introduction to Quantum Information Science [1]

[1] Rutgers, ECE 579, Fall 2019

Prof. Emina Soljanin

Lecture #10, October 16

This lecture describes the Shor's factoring algorithm.

Math Interlude – Factors and Periods

The *order* of an integer b modulo M is the smallest integer $r > 0$ such that $b^r = 1 \mod M$; if no such integer exists, the order is said to be infinite. We know that r is finite when b and M are relatively prime.[2] Consider the function

[2] Two integers are relatively prime if they have no common factors.

$$f(x) = b^x \mod M.$$

What is $f(x+r)$? Because $b^x = b^{x+r} \mod M$ if and only if $b^r = 1 \mod M$, for b relatively prime to M, the order r of b modulo M is the period of $f(x) = b^x \mod M$.

Finding the period of $f(x) = b^x \mod M$ allows us to find a factor of M. To see that, note that if $b^r = 1 \mod M$ and r is even, we have

$$(b^{r/2}+1)(b^{r/2}-1) = 0 \mod M.$$

As long as neither $b^{r/2}+1$ nor $b^{r/2}-1$ is a multiple of M, both $b^{r/2}+1$ and $b^{r/2}-1$ have nontrivial common factors with M. These factors can be found efficiently by e.g., the Euclidean algorithm.

Quantum Fourier Transform

The quantum Fourier transform (QFT) on n qubits[3] is the map that can be described by its action on the basis states $|x\rangle$ of $\mathcal{H}^n$ as follows:

[3] n-qubit states are vectors in $\mathcal{H}^n$

$$U_{FT} : |x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_N^{yx} |y\rangle.$$

where $N = 2^n$ and $\omega_N = e^{2\pi i/N}$ is a primitive[4] N-th root of unity. The $N \times N$ unitary matrix F_N of the quantum Fourier transform is given by

[4] What does primitive mean?

$$U_{FT} = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & 1 & 1 & \cdots & 1 \\ 1 & \omega_N & \omega_N^2 & \omega_N^3 & \cdots & \omega_N^{N-1} \\ 1 & \omega_N^2 & \omega_N^4 & \omega_N^6 & \cdots & \omega_N^{2(N-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega_N^{N-1} & \omega_N^{2(N-1)} & \omega_N^{3(N-1)} & \cdots & \omega_N^{(N-1)(N-1)} \end{bmatrix}.$$

The Quantum Fourier transform is related but not identical[5] to the Quantum Hadamard transform, which is given by

$$U_{HT} : |x\rangle \mapsto \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} (-1)^{yx} |y\rangle.$$

QFT can be carried out by a quantum circuit built entirely out of 1-qubit and 2-qubit gates.[6]

[5] except for $n = 1$

[6] Quantum Hadamard transform needs only 1-qubit gates.

Shor's Algorithm Outline

We want to factor $M = pq$ where p and q are odd primes.[7]

[7] Such numbers are used in RSA.

1. Pick a positive integer b smaller than M. Find the greatest common divisor (GCD)[8] y of b smaller than M. If $y > 1$, then a non-trivial factor of M has been found. Otherwise, $y = 1$ meaning that b and M are relatively prime.

[8] e.g., by the Euclidean algorithm

2. Create an n qubit superposition of all basis states in $\mathcal{H}^{2^n}$ for some n s.t. $M^2 \leqslant 2^n \leqslant 2M^2$, and use quantum parallelism to compute $f(x) = b^x \mod M$ on the superposition of inputs. The resulting state will be
$$\frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x, f(x)\rangle$$
3. Measure the target (right) register. The resulting state in the data registar will be
$$|\psi_0\rangle = \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} |x_0 + kr\rangle$$
where $f(x_0)$ is the measured value. Here x_0 is the smallest value of x ($0 \leqslant x_0 < r$) for which $f(x_0) = f_0$, and m is the smallest integer for which $mr + x_0 \geqslant 2^n$.
4. Apply the quantum Fourier transform[9] to $|\psi_0\rangle$. The resulting state is given by
$$\begin{aligned} U_{FT} |\psi_0\rangle &= \frac{1}{\sqrt{m}} \sum_{k=0}^{m-1} \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} \omega_N^{y(x_0+kr)} |y\rangle \\ &= \frac{1}{\sqrt{Nm}} \sum_{y=0}^{N-1} \omega_N^{yx_0} \sum_{k=0}^{m-1} \omega_N^{ykr} |y\rangle \end{aligned}$$

[9] Recall that the Simons algorithm was identical up to this point, where it applied the Quantum Hadamard transform to the data register.

5. Measure the data register in the computational basis. With high probability, a value v close to a multiple of $2^n/r$ will be obtained.
6. Use classical methods to obtain a conjectured period r from the value v.

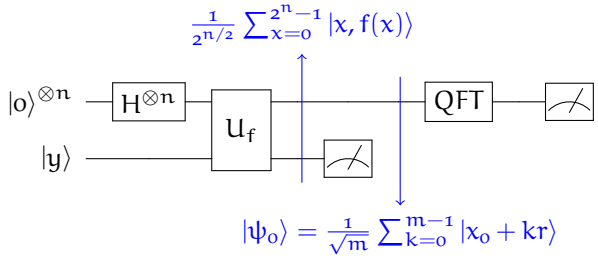


Figure 1: Steps 2 – 5. This is the quantum part of the algorithm. See the sections below for more detail.

7. If r is even, use the Euclidean algorithm to check efficiently whether $b^{r/2} + 1$ (or $b^{r/2} - 1$) has a nontrivial common factor with M.
8. Repeat steps 2–6 if necessary.

Introduction to Quantum Information Science [1]

Prof. Emina Soljanin

Lecture #11, October 21

[1] Rutgers, ECE 579, Fall 2019

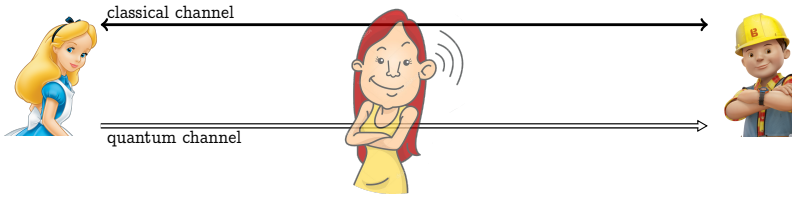
This lecture describes the BB84 quantum key distribution protocol.

The goal of a key distribution protocol is to ensure that two parties, Alice and Bob, share a secret random sequence of symbols, known as a private key. Private keys are used for, e.g., one-time pad where Alice sends to Bob her message XOR-ed with the key of the same length. The one-time pad cannot be cracked even with a Quantum computer.

The BB84 QKD Protocol

The BB84[2] protocol describes how Alice and Bob can establish a secret key by communicating over a quantum and a classical channel that can be accessed by an eavesdropper Eve. The basic observation behind this protocol is that, when nonorthogonal qubits are transmitted from Alice to Bob, then Eve cannot gain any information from the qubits without disturbing their states. Recall that since Eve cannot clone Alice's qubit, she can only gain information by measuring the original.

[2] The protocol was developed by Charles Bennett and Gilles Brassard in 1984. Hence the name.



Alice and Bob generate a secret key of $O(n)$ bits as follows:

1. Alice creates a sequence of $(4+\delta)n$ random data bits which she will map into qubits for transmission over the quantum channel between her and Bob.

2. For each data bit, Alice tosses a fair coin. If she gets a head (H), she maps her data bit into either $|0\rangle$ (if her data bit is 0) or $|1\rangle$ (if her data bit is 1). If she gets a tail (T), she maps her data bit into either $|+\rangle$ (if her data bit is 0) or $|-\rangle$ (if her data bit is 1).[3]

   We will refer to the sequence of heads and tails that Alice generated as C_A. We will call $\{|0\rangle, |1\rangle\}$ the H basis and $\{|-\rangle, |+\rangle\}$ the T basis.

[3] Recall that

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \text{ and } |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

3. Alice sends the resulting $(4+\delta)n$ qubits to Bob over their public quantum communication channel. Each qubit may be altered by the noise in the channel and/or measured by Eve. [4]
4. Upon receiving a qubit, Bob then tosses a fair coin and then, depending on the toss outcome, he measures the qubit in either the H or the T basis. If he uses the H bases and gets $|0\rangle$, or the T bases and gets $|+\rangle$, he records bit 0; otherwise he records bit 1.

   We refer to the sequence of heads and tails generated by Bob as C_B.
5. Once Bob receives $(4+\delta)n$ qubits, Alice publicly announces C_A and Bob publicly announces C_B.
6. Alice and Bob discard the bits where sequences C_A and C_B differ (that is, when Bob measured a qubit a in the different basis than Alice used for its preparation). With high probability, there are at least $2n$ bits left (if not, repeat the protocol). They keep $2n$ bits.
7. Alice selects a subset of n bits from the $2n$ remaining that will to serve as a check on Eve's interference, and tells Bob which bits she selected.
8. Alice and Bob announce and compare the values of the n check bits. If more than an acceptable[5] number disagree, they abort the protocol.
9. Alice and Bob perform information reconciliation and privacy amplification on the remaining n bits to obtain m shared key bits.

[4] Note that, at this point, Eve has no knowledge of C_A and thus what measurement basis she should use for an intercepted qubit. in order to learn the corresponding bit. She can only guess the preparation basis for a qubit, and if her guess is wrong, she will alter its state, thus leaving a proof of eavesdropping.

[5] The acceptable number is determined by the noise in the channels.

Introduction to Quantum Information Science [1]

Prof. Emina Soljanin

Lecture #12, October 30

[1] Rutgers, ECE 579, Fall 2019

This lecture introduces the density matrix formalism of quantum mechanics.

Math Interlude – The Trace of a Matrix

Let A be an $n \times n$ complex matrix. The trace of A is defined to be the sum of the elements on the diagonal of A:

$$\mathrm{tr}(A) = \sum_{i=1}^{n} a_{ii} = a_{11} + a_{22} + \cdots + a_{nn}$$

Some properties of the trace:

1. The trace is invariant under cyclic permutations:[2]

   $$\mathrm{tr}(ABCD) = \mathrm{tr}(BCDA) = \mathrm{tr}(CDAB) = \mathrm{tr}(DABC).$$

   We will often use this property of the trace.

2. The trace of the Kronecker product of two square matrices is the product of their traces:

   $$\mathrm{tr}(X \otimes Y) = \mathrm{tr}(X)\,\mathrm{tr}(Y).$$

3. The trace is a linear operator:

   $$\mathrm{tr}(\alpha X + \beta Y) = \alpha\,\mathrm{tr}(X) + \beta\,\mathrm{tr}(Y).$$

   Here X and Y are square matrices and α and β are scalars.

4. The trace is similarity-invariant. This property follows from the property 1. above:

   $$\mathrm{tr}\left(P^{-1}AP\right) = \mathrm{tr}\left(P^{-1}(AP)\right) = \mathrm{tr}\left((AP)P^{-1}\right) = \mathrm{tr}\left(A\left(PP^{-1}\right)\right) = \mathrm{tr}(A).$$

   Therefore, the trace is invariant to the change of basis, and thus

   $$\mathrm{tr}(A) = \sum_{i=1}^{n} \lambda_i. \quad \text{where } \lambda_i \text{ are the eigenvalues of } A.$$

5. Trace in Dirac's notation:[3] Let $|e_i\rangle$, $i = 1, \ldots, n$ be an orthonormal basis of $\mathbb{C}^n$. Then $a_{ii} = \langle e_i| A |e_i\rangle$, and therefore,

   $$\mathrm{tr}\, A = \sum_{i=1}^{n} \langle e_i| A |e_i\rangle$$

[2] In general, the trace is *not* permutation invariant.

[3] This property is useful for understanding the definition of the *partial trace*, which we will give later.

The Density Matrix Formalism

To describe quantum states, so far we used vectors in Hilbert spaces. Can we instead describe a quantum state, say $|\psi\rangle$, by the matrix $|\psi\rangle\langle\psi|$? We will use the notation $\rho_\psi = |\psi\rangle\langle\psi|$ and refer to ρ_ψ as the *density matrix* of state $|\psi\rangle$.[4]

[4] All we said so far can be reformulated in terms of the density matrix formalism.

Any description of a state should allow us to describe 1) how a state evolves when a unitary transformation is applied to it and 2) what happens to a state and with what probability when a measurement is performed on it.

1. Suppose that unitary operator U acts on state $|\psi\rangle$ giving the state $|\varphi\rangle = U|\psi\rangle$. We have $|\varphi\rangle\langle\varphi| = U|\psi\rangle\langle\psi|U^\dagger$. Therefore,

$$|\psi\rangle \xrightarrow{U} U|\psi\rangle \quad \Longleftrightarrow \quad \rho_\psi \xrightarrow{U} U\rho_\psi U^\dagger$$

2. Suppose a measurement defined by the matrices $\{\Pi_i\}_{i=1}^{\ell}$ is performed on the state $|\psi\rangle$. We know that the resulting state will be $|\varphi\rangle = \Pi_i|\psi\rangle / \|\Pi_i|\psi\rangle\|$ with probability $\langle\psi|\Pi_i|\psi\rangle$. Therefore,

$$\rho_\phi = \frac{\Pi_i|\psi\rangle\langle\psi|\Pi_i}{\langle\psi|\Pi_i|\psi\rangle} \text{ wp } \langle\psi|\Pi_i|\psi\rangle$$

or, in terms of density matrices,

$$\rho_\psi \to \frac{\Pi_i\rho_\psi\Pi}{\mathrm{tr}(\Pi_i\rho_\psi)} \text{ wp } \mathrm{tr}(\Pi_i\rho_\psi)$$

by observing that $\mathrm{tr}(\Pi_i\rho_\psi) = \mathrm{tr}(\Pi_i|\psi\rangle\langle\psi|) = \langle\psi|\Pi_i|\psi\rangle$.

Homework - Due November 4

Consider the quantum state described by the matrix $\rho_\varphi = |0\rangle\langle 0|$, and the quantum measurement M defined by the projections $\Pi_1 = |+\rangle\langle +|$ and $\Pi_2 = |-\rangle\langle -|$. Which states are possible as a result of measuring ρ_φ by M. Find the density matrices and the probabilities of these states.

Introduction to Quantum Information Science [1]

Prof. Emina Soljanin

Lecture #13, November 4

[1] Rutgers, ECE 579, Fall 2019

This lecture the notion of quantum mixed states the the von Neumann entropy.

Mixed States

The density matrix formalism allows us to compactly describe a quantum system about which we only know that it is in the state $|\psi_j\rangle$ with probability p_j as follows:

$$\rho = \sum_j p_j |\psi_j\rangle\langle\psi_j|$$

We refer to such quantum systems as mixed states.

The states we worked with so far that can be described by a vector, say $|\psi\rangle$, or, equivalently, the corresponding rank-1 density matrix $\rho_\psi = |\psi\rangle\langle\psi|$ are known as *pure states*.[2] In general, a density matrix ρ is a Hermitian, positive semi-definite, trace one matrix. It follows that ρ can be diagonalized by a unitary matrix, and has eigenvalues that are all real, nonnegative, and sum to one.

[2] Note that $\rho^2 = \rho$ for pure states. We will use this property when we discuss the Bloch sphere.

Unitary Evolution of Mixed States

What happens to a mixed state when a unitary transform U is applied to it? If the system described by the mixed state is actually in pure state $|\psi_j\rangle$ with the density matrix $\rho_j = |\psi_j\rangle\langle\psi_j|$, then it will evolve to the state $U\rho_j U^\dagger$. But we only know that the system is in the state ρ_j with probability p_j. Therefore, the mixed state will evolve to the state $U\rho_j U^\dagger$ with probability p_j, that is, another mixed state, whose density matrix is given by

$$\sum_j p_j U|\psi_j\rangle\langle\psi_j|U^\dagger = U\Big(\sum_j p_j|\psi_j\rangle\langle\psi_j|\Big)U^\dagger$$

Therefore, $\boxed{\rho \xrightarrow{U} U\rho U^\dagger}$.

Ensembles of States

We call the set of pure states together with the associated probabilities an *ensemble* of states. Observe that two different ensembles can have identical density matrices, and therefore quantum mechanically represent identical states. Figure 1 shows two different ensembles with the density matrix equal to I.

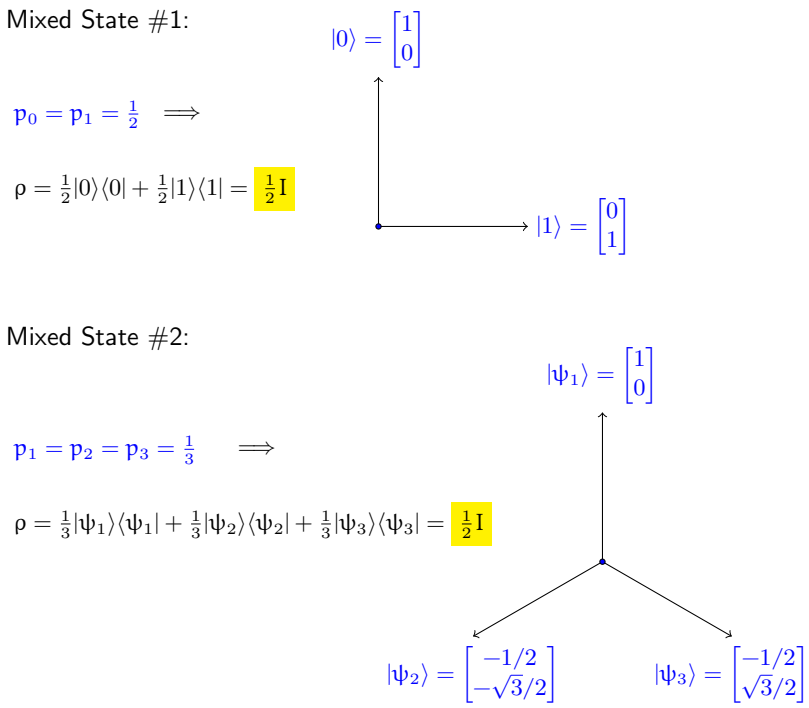


Figure 1: Two "different" mixtures of pure states with identical density matrices.

Measuring Mixed States

Measurements are also easily described in the density matrix formalism. Recall that the projective measurement is defined by a set of $m \times m$ matrices $\{\Pi_i\}_{i=1}^{\ell}$ such that

1. $\{\Pi_i\}$ are pairwise orthogonal projection operators
2. $\{\Pi_i\}$ form a complete resolution of the identity, that is,

$$\Pi_1 + \Pi_2 + \cdots + \Pi_\ell = I_m.$$

3. The measured state $|\psi\rangle$ gets projected (collapses) to state $\frac{\Pi_i|\psi\rangle}{\|\Pi_i|\psi\rangle\|}$ with probability $\langle\psi|\Pi_i|\psi\rangle$. Note that

$$\|\Pi_i|\psi\rangle\|^2 = \langle\psi|\Pi_i|\psi\rangle = \mathrm{tr}\big(\Pi_i|\psi\rangle\langle\psi|\big) = \mathrm{tr}\big(\Pi_i\rho_\psi\big)$$

Therefore, pure state $\rho_\psi = |\psi\rangle\langle\psi|$ collapses to $\frac{\Pi_i\rho_\psi\Pi_i}{\mathrm{tr}\left(\Pi_i\rho_\psi\right)}$ wp $\mathrm{tr}\big(\Pi_i\rho_\psi\big)$

We next look into what happens when we perform such a measurement on a mixed state whose density matrix is

$$\rho = \sum_j p_j|\psi_j\rangle\langle\psi_j|$$

We denote $\rho_j = |\psi_j\rangle\langle\psi_j|$. If the state being measured is $|\psi_j\rangle$ (which happens with probability p_j), then the probability of getting measurement result i is $\mathrm{tr}\big(\Pi_i|\psi_j\rangle\langle\psi_j|\big)$. Therefore, by the total probability formula, when measuring ρ, we get outcome i with probability

$$\sum_j p_j \underbrace{\mathrm{tr}\big(\Pi_i|\psi_j\rangle\langle\psi_j|\big)}_{\Pr(i|j)} = \mathrm{tr}\big(\Pi_i \sum_j p_j|\psi_j\rangle\langle\psi_j|\big) = \mathrm{tr}\big(\Pi_i\rho\big)$$

Note that different ensembles $\{\psi_j, p_j\}$ with the same ρ will give outcome i with the same probability $\mathrm{tr}\big(\Pi_i\rho\big)$, which depends only on ρ.

Is the state corresponding to outcome i pure or mixed? If the state being measured is $|\psi_j\rangle$ and the measurement result is i, then the system is in the state $\frac{\Pi_i\rho_j\Pi_i}{\mathrm{tr}\big(\Pi_i\rho_j\big)}$. Therefore, if we observe outcome i, the system is in the mixed state

$$\sum_j p_j \frac{\Pi_i\rho_j\Pi_i}{\mathrm{tr}\big(\Pi_i\rho_j\big)} = \frac{\Pi_i\rho\Pi_i}{\mathrm{tr}\big(\Pi_i\rho\big)}$$

Note that we ended up having a mixed state after the measurement resulted in outcome i, because we started with a mixed state.

Which state would we have if we[3] lost the measurement record? We saw that we get state $\frac{\Pi_i\rho\Pi_i}{\mathrm{tr}\big(\Pi_i\rho\big)}$ wp $\mathrm{tr}\big(\Pi_i\rho\big)$. We would therefore have

$$\sum_{i=1}^{\ell} \mathrm{tr}\big(\Pi_i\rho\big) \cdot \frac{\Pi_i\rho\Pi_i}{\mathrm{tr}\big(\Pi_i\rho\big)} = \sum_{i=1}^{\ell} \Pi_i\rho\Pi_i$$

Is this a valid density matrix?

[3] Here "we" is used on purpose to stress that, mathematically, the state of the system is described based on our *ignorance*.

Introduction to Quantum Information Science [1]

Prof. Emina Soljanin

Lecture #14, November 6

[1] Rutgers, ECE 579, Fall 2019

This lecture 1) introduces the Bloch sphere, 2) discusses bipartite states, and 3) describes quantum information processing.

Bloch Sphere

Any 2×2 complex matrix, and thus any density matrix ρ, can be expressed as a linear combination of the identity I and the Pauli matrices σ_X, σ_Y, and σ_Z:

$$\rho = \alpha_I I + \alpha_X \sigma_X + \alpha_Y \sigma_Y + \alpha_Z \sigma_Z$$

for some complex numbers α_I, α_X, α_Y, and α_Z. Since a density matrix is Hermitian and has trace one, these numbers will satisfy certain constraints.

Note that σ_X, σ_Y, and σ_Z have trace equal to 0. Therefore

$$\rho = \frac{1}{2}\left(I + \beta_X \sigma_X + \beta_Y \sigma_Y + \beta_Z \sigma_Z\right)$$

where β_X, β_Y, and β_Z are real numbers. To see that we write the above expression for ρ as follows:

$$\rho = \frac{1}{2}\begin{bmatrix} 1+\beta_Z & \beta_X - i\beta_y \\ \beta_X + i\beta_y & 1-\beta_Z \end{bmatrix}$$

We call $\vec{\beta} = (\beta_X, \beta_Y, \beta_Z)$ the Bloch vector of ρ. Since ρ is positive semi-definite, we have $\det(\rho) > 0$:

$$0 \leqslant \det(\rho) = 1 - (\beta_X^2 + \beta_Y^2 + \beta_Z^2) = 1 - |\vec{\beta}|^2$$

which implies $|\vec{\beta}|^2 \leqslant 1$. the set of all vectors that satisfy this condition is a ball in $\mathbb{R}^3$, known as the *Bloch sphere.*

Furthermore, for pure states, we have $\mathrm{tr}(\rho^2) = 1$, and thus

$$1 = \mathrm{tr}(\rho^2) = \frac{1}{2}\left(1 + |\vec{\beta}|^2\right) \quad \Leftrightarrow \quad |\vec{\beta}| = 1$$

As a consequence, the surface of the Bloch sphere represents all the pure states of a two-dimensional quantum system, whereas the interior corresponds to all the mixed states. In particular,

$\beta_X = \beta_Y = 0$ and $\beta_Z = 1$ gives $\rho = |0\rangle\langle 0|$

$\beta_X = \beta_Y = 0$ and $\beta_Z = -1$ gives $\rho = |1\rangle\langle 1|$

Sometimes $|\uparrow_z\rangle$ and $|\downarrow_z\rangle$ (spin up and down) are used to denote $|0\rangle$ and $|1\rangle$ respectively.

Any two diametrically opposite (antipodal) points correspond to a pair of mutually orthogonal pure state vectors. Why?

Pauli matrices:

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

$$\sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \qquad \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

form a basis for $\mathbb{C}^{2\times 2}$.

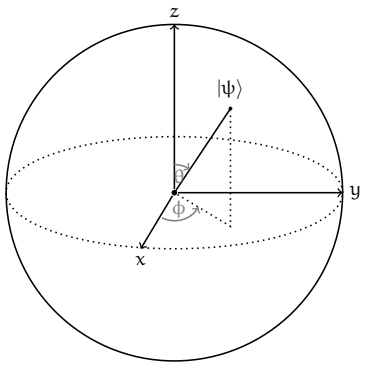


Figure 1: Bloch Sphere

Bipartite Quantum States

Let $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$. We say that $|\psi\rangle$ is a bipartite quantum state of a composite system with subsystems A and B. Let $\mathcal{H}_A$ and $\mathcal{H}_B$ be finite-dimensional Hilbert spaces with basis states $\{|a_i\rangle\}_{i=1}^n$ and $\{|b_j\rangle\}_{j=1}^m$, respectively. Then the state space of the composite system is the tensor product $\mathcal{H}_A \otimes \mathcal{H}_B$ with the basis $\{|a_i\rangle \otimes |b_j\rangle\}$, or in more compact notation $\{|a_i b_j\rangle\}$. Any pure state of the composite system can be written as

$$|\psi\rangle = \sum_{i=1}^{n} \sum_{j=1}^{m} c_{i,j}(|a_i\rangle \otimes |b_j\rangle) = \sum_{i,j} c_{i,j}|a_i b_j\rangle,$$

where $c_{i,j}$ are complex numbers. If a pure state $|\psi\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B$ can be written in the form $|\psi\rangle = |\psi_A\rangle \otimes |\psi_B\rangle$, it is said to be separable. Otherwise it is called entangled. When a system is in an entangled pure state, it is not possible to assign states to its subsystems.

Let ρ_{AB} be a density matrix in the product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. A mixed state of the bipartite system described by ρ_{AB} can be

1. a product state if $\rho_{AB} = \rho_A \otimes \rho_B$ or
2. a separable state if there exist a probability distribution $\{p_k\}$, and $\{\rho_A^k\}$ and $\{\rho_B^k\}$ which are mixed states of the respective subsystems such that
$$\rho = \sum_k p_k \rho_A^k \otimes \rho_B^k.$$

Otherwise ρ_{AB} is an entangled state. Note that, for mixed states, separable and product are different notions.

Reduced Density Operator

Recall the trace expression in Dirac's notation: Let $|e_i\rangle$, $i = 1, \ldots, n$ be an orthonormal basis of $\mathbb{C}^n$. Then $|e_i\rangle\langle e_i|A$ is a matrix whose i-th diagonal element is a_{ii} and all other elements are 0. Therefore,

$$\operatorname{tr} A = \sum_{i=1}^{n} \operatorname{tr}\big(|e_i\rangle\langle e_i|A\big) = \sum_{i=1}^{n} \langle e_i| A |e_i\rangle$$

Let ρ_{AB} be a density matrix in the product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, and let $|b_i\rangle$ be an orthonormal basis for $\mathcal{H}_B$. Then the partial trace over the Hilbert space $\mathcal{H}_B$ is defined as follows:[2]

$$\rho_A = \operatorname{tr}_B \rho_{AB} = \sum_i \big(I \otimes \langle b_i|\big)\rho_{AB}\big(I \otimes |b_i\rangle\big)$$

[2] You will often see a shorthand expression $\operatorname{tr}_B \rho_{AB} = \sum_b \langle b| \rho_{AB} |b\rangle$

Example #1 – Product State:
Suppose a quantum system is in the product state $\rho_{AB} = \rho_A \otimes \rho_B$ where ρ_A is a density operator for system A, and ρ_B is a density operator for system B. Then

$$\rho_A = \mathrm{tr}_B(\rho_A \otimes \rho_B) = \rho_A \,\mathrm{tr}\,\rho_B = \rho_A$$

Example #2 – Bell State:
Consider the bipartite state $|\phi_{AB}\rangle\,(|00\rangle + |11\rangle)/\sqrt{2}$. This is a pure state with the density operator

$$\rho_{AB} = |\phi_{AB}\rangle\langle\phi_{AB}| = \frac{1}{2}(|00\rangle\langle 00| + |00\rangle\langle 11| + |11\rangle\langle 00| + |11\rangle\langle 11|)$$

Tracing out the second qubit, we find the reduced density operator of the first qubit,

$$\begin{aligned}\rho_A = \mathrm{tr}_B \rho_{AB} &= (I \otimes \langle 0|)\rho_{AB}(I \otimes |0\rangle) + (I \otimes \langle 1|)\rho_{AB}(I \otimes |1\rangle) \\ &= \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \boxed{\frac{1}{2}I}\end{aligned}$$

Introduction to Quantum Information Science [1]

[1] Rutgers, ECE 579, Fall 2019

Prof. Emina Soljanin

Lecture #15, November 11

This lecture discusses some relations between two probability distributions and two density matrices.

Math Interlude

Majorization

Majorization is a preorder[2] relation on vectors of real numbers. We will use it to relate two probability distributions. Let $P = \{p_1, \dots, p_k\}$ and $Q = \{q_1, \dots, q_k\}$ be vectors of probabilities, and $P^{\downarrow}$ and $Q^{\downarrow}$ the vector with identical components as P and Q respectively, but sorted in descending order We write $\boxed{Q \succ P}$ say that Q majorizes P, or dominates P, or P is majorized by Q when

[2] reflexive and transitive

$$\sum_{j=1}^{i} p_j^{\downarrow} \leqslant \sum_{j=1}^{i} q_j^{\downarrow} \quad \text{for } i = 1, \dots, k-1.$$

Note that $\sum_{j=1}^{i} p_j^{\downarrow} = \sum_{j=1}^{i} q_j^{\downarrow} = 1$. Vectors P and Q do not have to have the same support, since we can pad the smaller support vector with zeros.

Schur Concavity

We say that $f : \mathbb{R}^k \to \mathbb{R}$ is *Schur concave* when we have that

$$\mathbf{a} \succ \mathbf{b} \;\text{ implies }\; f(\mathbf{a}) \leqslant f(\mathbf{b}).$$

Similarly, f is Schur convex when $\mathbf{a} \succ \mathbf{b}$ implies $f(\mathbf{a}) \geqslant f(\mathbf{b})$.

Every concave symmetric function is Schur-concave.[3]

[3] What does this say about the Shannon entropy?

Examples

1. For quasi-uniform vectors with d components, we have

$$\left\{\frac{1}{d}, \dots, \frac{1}{d}\right\} \prec \left\{\frac{1}{d-1}, \dots, \frac{1}{d-1}, 0\right\} \prec \cdots \prec \{1, 0, \dots, 0\}$$

2. For any probability distribution P with support size d, we have

$$\left\{\frac{1}{d}, \dots, \frac{1}{d}\right\} \prec P$$

How to Mix a Density Matrix

We have seen that different quantum ensembles $\{p_j, |\psi_j\rangle\}$ can have identical density matrices. Can we characterize ensembles that have a given density matrix? Can we characterize probability distributions that are *consistent* with a given density matrix.

Let $\{p_j\}$ be a PD, and $p_1 \geqslant p_2 \geqslant \cdots \geqslant p_k$. Let ρ be a density matrix, and $\lambda_1 \geqslant \lambda_2 \geqslant \cdots \geqslant \lambda_d$ its eigenvalues. There exist vectors $|\psi_i\rangle$ such that $\rho = \sum_{i=1}^{k} p_i |\psi_i\rangle\langle\psi_i|$ iff

$$\sum_{i=1}^{n} p_i \leqslant \sum_{i=1}^{n} \lambda_i \quad \text{for all } n < d.$$

For $\rho = \frac{1}{d} I_d$, this condition becomes $p_1 \leqslant 1/d$.

How Close are Two Quantum States?

How Close are Two Probability Vectors?

Let $P = \{p_1, \ldots, p_k\}$ and $Q = \{q_1, \ldots, q_k\}$ be vectors of probabilities. We can tell how close these vectors are by

1. *total variation*
$$D(P, Q) = \frac{1}{2} \sum_i |p_i - q_i|$$
which measures the distance, and

2. *Bhattacharyya coefficient*
$$BC(P, Q) = \sum_i \sqrt{p_i q_i}$$
which measures the amount of overlap.[4]

[4] Log of BC is *Bhattacharyya ditance.*

Fidelity and Trace Distance

To measure how faithfully mixed state σ approximates mixed state ω and vice versa, we use the so called *mixed state fidelity* F defined as

$$F(\sigma, \omega) = \left\{ \mathrm{tr}\left[(\sqrt{\sigma}\omega\sqrt{\sigma})^{1/2} \right] \right\}^2, \tag{1}$$

Besides computing the mixed state fidelity (1), one can measure how close state σ is to state ω by computing the *trace distance*

$$D(\sigma, \omega) = \frac{1}{2} \mathrm{tr} |\sigma - \omega|.$$

Here $|A|$ denotes the positive square root of $A^\dagger A$, *i.e.*, $|A| = \sqrt{A^\dagger A}$.

The trace distance and the fidelity are closely related and the following holds:

$$1 - F(\sigma, \omega) \leqslant D(\sigma, \omega) \leqslant \sqrt{1 - F(\sigma, \omega)^2}. \tag{2}$$

The trace distance is a metric on the space of density operators, and therefore the triangle inequality is true:

$$D(\sigma, \omega) \leqslant D(\sigma, \tau) + D(\tau, \omega). \tag{3}$$

It has some other useful properties, as well. When we need one of those properties, we shall switch from the fidelity to the trace distance and back by making use of the inequalities in (2).

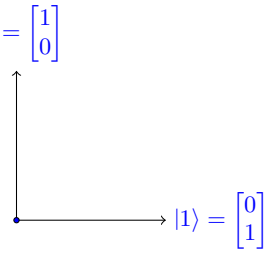
Problems - Homework Due November 20

1. Show that the following holds:

Mixed State #1:

$p_0 = p_1 = \frac{1}{2} \implies$

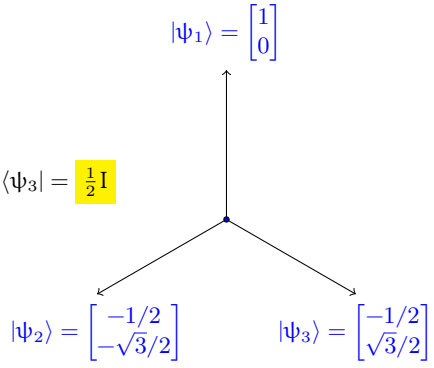
$\rho = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}I$



Mixed State #2:

$p_1 = p_2 = p_3 = \frac{1}{3} \implies$

$\rho = \frac{1}{3}|\psi_1\rangle\langle\psi_1| + \frac{1}{3}|\psi_2\rangle\langle\psi_2| + \frac{1}{3}|\psi_3\rangle\langle\psi_3| = \frac{1}{2}I$



2. Consider two density matrices σ and ω such that $\sigma\omega = \omega\sigma$. Express the fidelity and the trace distance between σ and ω in terms of their eigenvalues.

3. Consider two pure states $|\psi\rangle$ and $|\varphi\rangle$. Find the fidelity and the trace distance between ρ_ψ and ρ_φ.

4. Let ρ be a density operator. Show that $\mathrm{tr}(\rho^2) \leqslant 1$ with equality if and only if ρ is a pure state.

Introduction to Quantum Information Science [1]

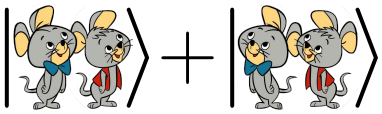
[1] Rutgers, ECE 579, Fall 2019

Prof. Emina Soljanin

Lecture #16, November 18

This lecture discusses entanglement (quantum vs. classical correlations), hidden variables theories, quantum non-locality, and Bell's inequalities.

Alice and Bob Share an EPR Pair



Consider a bipartite system consisting of two entangled qubits whose joint state is

$$|\varphi\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B\right)$$

Qubit A (Pixie) is given to Alice and qubit B (Dixie) to Bob. Note that $|\varphi\rangle$ is a Bell state (aka EPR pair) we discussed before. EPR stands for Einstein, Podolsky and Rosen, who were the first to point out the "strange" properties of this state in 1935. Recall that each individual qubit is in the mixed state $(|0\rangle\langle 0| + |1\rangle\langle 1|)/2$. We have shown earlier that if Alice measures her qubit in the computational basis, she will get either state $|0\rangle$ or $|1\rangle$, each with probability $1/2$. But if Bob then measures his qubit in the computational basis, he will get a state that is identical to Alice's. Einstain referred to this phenomenon as "spooky action at the distance" or quantum non-locality.

Einstein was not comfortable with the notion of non-deterministic measurements and entanglement. He believed that there exist some "hidden variables" that determine measurement outcomes, and in general govern the reality. He did not question the predictions of quantum mechanics, but declared it *incomplete* since it does not take into account existence of hidden variables that could explain the spooky actions at the distance.

Until John Bell's work in 1964, no circumstances were known where predictions provided by any theory with hidden variables disagreed with those provided by quantum mechanics. John Bell came up with scenarios where these predictions were not identical, and thus which one is true could be determined by experiments. In the past half a century, many such experiments were conducted, but it was only in 2015 that experiments showed non existence of hidden variables in a most complete manner possible.

We will next go over a common example (involving the state $|\varphi\rangle$ above) that shows a disagreement between the predictions provided by quantum mechanics and those provided by a hidden variable theory.

Two Measurement Scenarios

1. Suppose Alice measures her qubit in an orthonormal basis $\{|b_0\rangle, |b_1\rangle\}$ obtained by rotating the computational basis around the origin. Then $|b_0\rangle = \alpha|0\rangle + \beta|1\rangle$ where α and β are real numbers.

   If Alice gets $|b_0\rangle$ as her measurement result, then Alice's postmeasurement state is her original state multiplied by $|b_0\rangle\langle b_0|$ (and properly normalized), while the action on Bob state is described by the identity operator I. What happens to state $|\varphi\rangle$? To see that $|\varphi\rangle$ collapses to $|b_0\rangle \otimes |b_0\rangle$, consider the following:

$$\begin{aligned}(|b_0\rangle\langle b_0| \otimes I)\,|\varphi\rangle &= |b_0\rangle\,\langle b_0|0\rangle \otimes |0\rangle + |b_0\rangle\,\langle b_0|1\rangle \otimes |1\rangle \\ &= |b_0\rangle \otimes \big(\langle b_0|0\rangle\,|0\rangle + \langle b_0|1\rangle\,|0\rangle\,\big) \\ &= |b_0\rangle \otimes |b_0\rangle\end{aligned}$$

   We have used here the fact that $|b_0\rangle = \langle b_0|0\rangle\,|0\rangle + \langle b_0|1\rangle\,|0\rangle$.

2. Suppose Alice measures her qubit in an orthonormal basis $\{|b_0\rangle, |b_1\rangle\}$ obtained by rotating the computational basis by 120 degrees, that is, $|\langle b_0|0\rangle| = 1/2$. Then the probability that Alice's qubit collapses to $|b_0\rangle$ is $|\langle b_0|0\rangle|^2 = 1/4$.

Note that 1 and 2 imply that if Alice and Bob measure their entangled qubits in the identical bases they get identical results with probability 1, and if they measure their entangled qubits in the bases that are 120 degrees apart, they get identical results with probability 1/4.

A Measurement Protocol

In this protocol, Alice and Bob can perform measurements in three possible orthonormal bases: $\{|a_0\rangle, |a_1\rangle\}$, $\{|b_0\rangle, |b_1\rangle\}$, or $\{|c_0\rangle, |c_1\rangle\}$ that are 120 degrees apart, see Fig. 1. The measurement equipment is connected to a light indicator which shows a red light when the result of the measurement is either $|a_0\rangle$ or $|b_0\rangle$ or $|c_0\rangle$, and a green light when the result of the measurement is either $|a_1\rangle$ or $|b_1\rangle$ or $|c_1\rangle$.

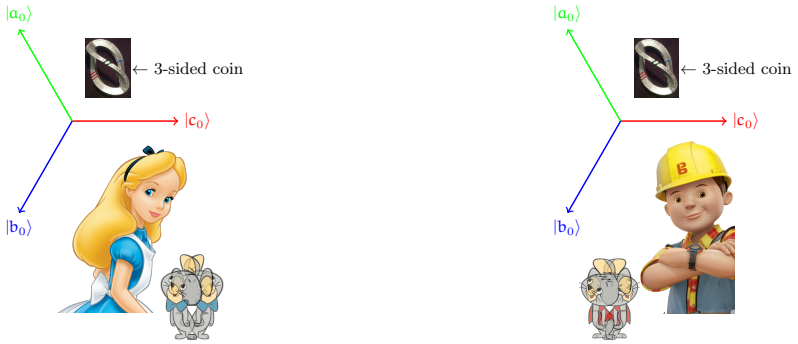


Figure 1: Alice and Bob randomly pick a basis by rolling a 3-sided die.

Alice and Bob each have a 3-sided fair die, and share a large number of entangled qubit pairs. For each entangled pair, Alice and Bob

roll their respective dice. These rolls are independent of each other and of the previous rolls. Based on their rolls outcomes, Alice and Bob choose one of the three possible basis and measure their respective qubits, and observe the light indicator. How ofthen will Alice and Bob see the lights of the same color?

Note that Alice and Bob will chose the same basis with probability 1/2, and a pair of bases that are 120 degrees apart with probability 2/3. Whenever they choose the same basis, they will see the light of the same color with probability 1. Whenever they choose different bases, they will see the the same color with probability 1/4. Therefore, Alice and Bob will see the same color with probability

$$\frac{1}{3}\cdot 1+\frac{2}{3}\cdot\frac{1}{4}=\frac{1}{2}$$

Is such outcome a result of some "spooky action at a distance" or some "hidden variables" e.g., a pre-determined light color response to each of the three basis which is somehow hidden within the particles?

Talking Mice

Can the result of the above measurement protocol be explained by assuming that the particles had agreed in advance which light will be turned on for each basis? For example, Pixie and Dixie of Fig. 2 could agree that for a measurement in bases $\{|a_0\rangle, |a_1\rangle\}$ and $\{|b_0\rangle, |b_1\rangle\}$, they will always turn the red light on, and for a measurement in basis $\{|c_0\rangle, |c_1\rangle\}$, they will always turn the green light on, as in Fig. 2.

Figure 2: Pixie and Dixie agree in advance on which light will be turned on for each of the three possible bases.

Note that there are 8 possible agreements, and 9 possible Alice and Bob basis pairs, as shown in Table 1. For each basis pair, we can check if a particular agreement will result in Alice and Bob observing the same (S) or different (D) light colors. Table 1 shows that no agreement (row in the table) results in Alice and Bob observing the same light color 50% of the time.

Pixie-Dixie Agreements	Alice and Bob Basis Pair								
	aa	ab	ac	ba	bb	bc	ca	cb	cc
RRR	S	S	S	S	S	S	S	S	S
RRG	S	S	D	S	S	D	D	D	S
RGR	S	D	S	D	S	D	S	D	S
RGG	S	D	D	D	S	S	D	S	S
GRR	S	D	D	D	S	S	D	S	S
GRG	S	D	S	D	S	D	S	D	S
GGR	S	S	D	S	S	D	D	D	S
GGG	S	S	S	S	S	S	S	S	S

Table 1: Alice and Bob can observe the same (S) or different (D) light colors depending on their choice of the basis pair and the Pixie-Dixie agreement.

Introduction to Quantum Information Science [1]

[1] Rutgers, ECE 579, Fall 2019

Prof. Emina Soljanin

Lecture #17, November 20

Quantum Information Systems – Recap & Generalization

Quantum States

Quantum states are, in the simplest case, mathematically represented as unit norm column vectors[2] in a d-dimensional Hilbert space $\mathcal{H}$. Such quantum states are called *pure*. When $d = 2$, quantum states are called *qubits*. A pure state is mathematically described by its *density matrix* equal to the outer product $|\varphi\rangle\langle\varphi|$.

[2] A column vector is denoted by $|\varphi\rangle$, its conjugate transpose by $\langle\varphi|$.

In a more complex case, all we know about a quantum state is that it is one of a finite number of possible pure states $|\varphi_i\rangle$ with probability p_i. Such quantum states are called *mixed*. A mixed state is also described by its density matrix which is equal to

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

Note that a density matrix is a $d \times d$ Hermitian trace-one positive semidefinite matrix.

Quantum Evolutions

A quantum state ρ can be transformed to another state $\mathcal{E}(\rho)$ only by a physical process consistent with the laws of quantum mechanics. Such a process is, in the simplest case, mathematically described as a *unitary* evolution:

$$\mathcal{E}(\rho) = U\rho U^\dagger \quad \text{where} \quad UU^\dagger = I,$$

and, in the general case, as an evolution by a *completely positive, trace-preserving* map:

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger \quad \text{where} \quad \sum_k E_k^\dagger E_k = I.$$

It is envisioned that a quantum computer (like a classical one) would implement such evolutions by using universal quantum gates. An example of a two-qubit quantum gate is the XOR.

$$\texttt{XOR} : |x, y\rangle \to |x, x \oplus y\rangle \quad U_{\texttt{XOR}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Quantum Measurements

A quantum measurement is a physical process applied to determine the state of the quantum system being measured. Only when the possible states, say $\{|\psi_j\rangle,\ j = 1,\ldots,k\}$, are orthogonal can a quantum measurement be designed to give an unambiguous answer.

The simplest model of quantum measurement is known as the von Neumann's measurement. Mathematically, this type of measurement is defined by a set of pairwise orthogonal projection operators $\{\Pi_i\}$ which form a complete resolution of the identity, that is, $\sum_i \Pi_i = I$. For input $|\psi_j\rangle$, the *classical* output $\Pi_i |\psi_j\rangle / \sqrt{\mathrm{tr}(\Pi_i |\psi_j\rangle)}$ happens with probability $\mathrm{tr}(\Pi_i |\psi_j\rangle)$.

In a more general case, the pairwise orthogonal projection operators $\{\Pi_i\}$ are replaced by any positive-semidefinite operators $\{E_i\}$ which form a complete resolution of the identity. This type of measurement in known as *positive operator-valued measure* (POVM).

Cloning, Broadcasting, and Deleting

Quantum information cannot be cloned, broadcast or deleted in the sense made precise below, unless we are dealing with states with commuting density matrices.

The No-Cloning Principle: There is no physical process that for all $|\psi\rangle$ leads to an evolution

$$|\phi\rangle \otimes |s\rangle \to |\phi\rangle \otimes |\phi\rangle$$

where $|\phi\rangle$ is an arbitrary state and $|s\rangle$ is a fixed state. (Approximate cloning, on the other hand, is possible.)

The No-Deleting Principle: There is no physical process that for all $|\psi\rangle$ leads to an evolution

$$|\phi\rangle \otimes |\phi\rangle \to |\phi\rangle \otimes |s\rangle$$

where $|\phi\rangle$ is an arbitrary state and $|s\rangle$ is a fixed state.

The No-Broadcasting Principle: Suppose that quantum system A is in an unknown state ρ and quantum system B is in some known or standard state ω. Then there is no physical process that for all ρ leads to an evolution

$$\rho \otimes \omega \to \sigma \ \text{ s.t. } \mathrm{tr}_A(\sigma) = \rho \text{ and } \mathrm{tr}_B(\sigma) = \rho,$$

that is, so that both subsystem A and subsystem B evolve into state ρ.